Improved Spread Spectrum Schemes for Data Hiding and Their Security Analysis under Known Message Attack

by

Amir Valizadeh

B.Sc., Shiraz University, 2004
M.Sc., Shiraz University, 2007

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY
in
The Faculty of Graduate Studies
(Electrical and Computer Engineering)

THE UNIVERSITY OF BRITISH COLUMBIA
(Vancouver)
April 2013
© Amir Valizadeh 2013
Abstract

The massive production and easy use of digital media pose new challenges on protecting intellectual property of digital media. Digital data hiding, which can be defined as the procedure of embedding information into an original media host signal, is a promising technique for digital intellectual property protection. A data hiding system generally contains two major components: the encoder for embedding the hidden information and the decoder for extracting the hidden information.

This thesis focuses on spread spectrum (SS) watermarking schemes for data hiding. Watermarking techniques for data hiding can be broadly categorized into two classes: quantization index modulation (QIM) based and spread spectrum based approaches. Being robust against distortions and having simple decoder structure make SS attractive for data hiding.

First, we investigate the decoding performance of the traditional SS schemes in the DCT and DFT domains. To obtain more practical decoders, we propose using suboptimal decoders which do not need side information.

Secondly, since the interference effect of the host signal causes decoding performance degradation in the additive SS scheme, to remove this host effect efficiently, we propose the correlation-and-bit-aware concept for data hiding by exploiting the side information at the encoder side and propose two improved SS-based schemes, the correlation-aware SS (CASS) and the correlation-aware improved SS (CAISS) embedding schemes.

Thirdly, we analyze the decoding error probability and capacity of the multiplicative spread spectrum (MSS) embedding scheme, and show that the content-based MSS still suffers from the interference effect of the host signal. We then propose an improved MSS-based scheme by efficiently removing the host interference effect.

Lastly, we present the security analysis of the SS-based data hiding schemes under the Known Message Attack (KMA) scenario. Each data hiding scheme has some secret parameters and here the security of a data hiding scheme represents the difficulty of estimating the secret parameters. We employ the mutual information between the observations and the secret parameters as a security measure. Also some practical estimators for estimating the signature code are introduced and their performances are reported to illustrate the security results.
Preface

The research outline of this thesis was designed jointly by the author and Professor Z. Jane Wang. The majority of the research, including literature survey, theoretical proofs, simulation, and results was conducted by the author, with suggestions from Professor Z. Jane Wang. The manuscripts were primarily drafted by the author and then finalized with regard to the helpful comments of Professor Z. Jane Wang.

Two papers related to Chapter 2 have been published:


Three papers related to Chapter 3 have been published:


Three papers related to Chapter 4 have been published:


# Table of Contents

Abstract ................................................................. ii
Preface ................................................................. iii
Table of Contents ...................................................... v
List of Figures ........................................................... ix
List of Acronyms ......................................................... xiii
Acknowledgments ........................................................ xv
Dedication ............................................................... xvi

1 Introduction ............................................................ 1
   1.1 Watermarking and Data Hiding .................................. 2
   1.2 Applications ..................................................... 4
   1.3 Challenges of Data Hiding ....................................... 4
      1.3.1 Embedding Schemes ...................................... 5
      1.3.2 Decoding Schemes ...................................... 7
      1.3.3 Security .................................................. 8
      1.3.4 Robustness and Watermark Attacks ..................... 9
   1.4 Contributions of the Thesis ................................... 12
   1.5 Organization of the Thesis ................................... 13

2 Efficient Blind Decoders for Additive Spread Spectrum .......... 16
   2.1 Introduction .................................................... 16
   2.2 SS Schemes ..................................................... 17
      2.2.1 Additive SS Scheme .................................... 17
      2.2.2 ISS Embedding Scheme ................................ 17
   2.3 Additive SS and ISS Schemes Applied to Images ............ 18
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.4</td>
<td>Data Hiding in the DCT and the DFT Magnitude Domains</td>
<td>19</td>
</tr>
<tr>
<td>2.5</td>
<td>The ML Optimal Decoders</td>
<td>20</td>
</tr>
<tr>
<td>2.5.1</td>
<td>ML Decoders in the DFT Domain</td>
<td>20</td>
</tr>
<tr>
<td>2.5.2</td>
<td>ML Decoders in the DCT Domain</td>
<td>23</td>
</tr>
<tr>
<td>2.6</td>
<td>Suboptimal Decoders</td>
<td>24</td>
</tr>
<tr>
<td>2.6.1</td>
<td>Local Optimum Decoder</td>
<td>24</td>
</tr>
<tr>
<td>2.6.2</td>
<td>LMMSE Decoder</td>
<td>26</td>
</tr>
<tr>
<td>2.7</td>
<td>Experimental Results</td>
<td>27</td>
</tr>
<tr>
<td>2.8</td>
<td>Conclusion</td>
<td>32</td>
</tr>
<tr>
<td>3</td>
<td>Correlation-and-Bit-Aware Spread Spectrum</td>
<td>34</td>
</tr>
<tr>
<td>3.1</td>
<td>Introduction</td>
<td>34</td>
</tr>
<tr>
<td>3.2</td>
<td>Conventional Correlator as Decoder</td>
<td>35</td>
</tr>
<tr>
<td>3.3</td>
<td>Correlation-Aware SS Data Hiding Approach</td>
<td>36</td>
</tr>
<tr>
<td>3.4</td>
<td>Correlation-Aware Improved SS Data Hiding Approach</td>
<td>41</td>
</tr>
<tr>
<td>3.5</td>
<td>CASS and CAISS in the Presence of Additional Noise</td>
<td>46</td>
</tr>
<tr>
<td>3.6</td>
<td>Simulation Results</td>
<td>49</td>
</tr>
<tr>
<td>3.6.1</td>
<td>Experimental Results</td>
<td>51</td>
</tr>
<tr>
<td>3.7</td>
<td>Conclusion</td>
<td>56</td>
</tr>
<tr>
<td>4</td>
<td>Improved Multiplicative Spread Spectrum</td>
<td>57</td>
</tr>
<tr>
<td>4.1</td>
<td>Introduction</td>
<td>57</td>
</tr>
<tr>
<td>4.2</td>
<td>Conventional MSS Scheme</td>
<td>58</td>
</tr>
<tr>
<td>4.3</td>
<td>Analysis of the MSS Scheme</td>
<td>58</td>
</tr>
<tr>
<td>4.4</td>
<td>Improved Multiplicative Spread Spectrum</td>
<td>61</td>
</tr>
<tr>
<td>4.5</td>
<td>MSS and IMSS in the Presence of Additional Noise</td>
<td>67</td>
</tr>
<tr>
<td>4.6</td>
<td>Simulation Results</td>
<td>68</td>
</tr>
<tr>
<td>4.7</td>
<td>Conclusion</td>
<td>70</td>
</tr>
<tr>
<td>5</td>
<td>Security Analysis of Spread Spectrum Schemes under KMA and KMCA</td>
<td>75</td>
</tr>
<tr>
<td>5.1</td>
<td>Introduction</td>
<td>75</td>
</tr>
<tr>
<td>5.2</td>
<td>Spread Spectrum Embedding Schemes</td>
<td>76</td>
</tr>
<tr>
<td>5.2.1</td>
<td>Additive SS Scheme</td>
<td>77</td>
</tr>
<tr>
<td>5.2.2</td>
<td>ISS Scheme</td>
<td>77</td>
</tr>
<tr>
<td>5.2.3</td>
<td>CAISS Scheme</td>
<td>77</td>
</tr>
<tr>
<td>5.2.4</td>
<td>Multiplicative Spread Spectrum</td>
<td>78</td>
</tr>
<tr>
<td>5.3</td>
<td>Security Analysis of SS, ISS, and MSS Schemes under KMA</td>
<td>78</td>
</tr>
</tbody>
</table>
# Table of Contents

5.3.1 Additive SS Scheme under KMA .................................... 79
5.3.2 ISS Scheme under KMA .............................................. 79
5.3.3 MSS Scheme under KMA .............................................. 80
5.4 Security Analysis of CASS and CAISS Schemes under KMCA and KMA .... 80
  5.4.1 CASS and CAISS Schemes under KMCA ............................... 81
  5.4.2 CAISS and CASS Schemes under KMA ............................... 82
5.5 Practical Estimators of the Signature Code for SS Schemes .................... 83
5.6 Results and Discussions ................................................. 85
  5.6.1 On the Theoretical Security Results ................................ 86
  5.6.2 On the Practical Estimators ......................................... 88
  5.6.3 Important Observations .............................................. 89
5.7 Conclusion ................................................................. 93

6 Thesis Summary and Future Research Topics ..................................... 94
  6.1 Summary of Results ..................................................... 94
  6.2 Future Work ............................................................. 95
    6.2.1 Correlation-and-Bit-Aware Concept for IMSS Scheme ............... 95
    6.2.2 New Security Measure Exploiting the Decoder Structure .......... 96
    6.2.3 Data Hiding in the Encrypted Domain ................................ 96

Bibliography .............................................................................. 98

Appendices

A Corresponding Proofs for Chapter 2 .......................................... 111
  A.1 Derivations for SS Analysis in the DFT Domain ............................ 111
  A.2 Derivations for ISS Analysis in the DFT Domain ............................ 112
  A.3 Derivations for ISS Analysis in the DCT Domain ............................ 112
  A.4 Derivations for LOD Analysis in the DCT Domain ............................ 113

B Corresponding Proofs for Chapter 3 .......................................... 115
  B.1 Proof of Proposition 1 ..................................................... 115
  B.2 Derivation of Optimal Decoder for CAISS Scheme ........................ 115
  B.3 Proof of Proposition 2 ..................................................... 117
  B.4 Proof of Proposition 3 ..................................................... 118
  B.5 Proof of Proposition 4 ..................................................... 119
  B.6 Derivation of Optimal Decoder for CAISS Scheme in the Presence of Noise ... 119
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>B.7</strong> Derivation of Equation ((3.52))</td>
<td>120</td>
</tr>
<tr>
<td><strong>B.8</strong> Derivation of Equation ((3.56))</td>
<td>121</td>
</tr>
<tr>
<td><strong>C Corresponding Proofs for Chapter 4</strong></td>
<td>123</td>
</tr>
<tr>
<td><strong>C.1</strong> Derivation of Error Probability of the MSS Embedding Scheme</td>
<td>123</td>
</tr>
<tr>
<td><strong>C.2</strong> Derivation of Capacity of the MSS Embedding Scheme</td>
<td>124</td>
</tr>
<tr>
<td><strong>C.3</strong> Derivation of Equation ((4.24))</td>
<td>125</td>
</tr>
<tr>
<td><strong>C.4</strong> Derivation of Equation ((4.28))</td>
<td>127</td>
</tr>
<tr>
<td><strong>C.5</strong> Derivation of Error Probability of the IMSS Embedding Scheme</td>
<td>127</td>
</tr>
<tr>
<td><strong>C.6</strong> Derivation of Error Probability of the MSS Scheme in the Presence of Noise</td>
<td>129</td>
</tr>
<tr>
<td><strong>D Corresponding Proofs for Chapter 5</strong></td>
<td>130</td>
</tr>
<tr>
<td><strong>D.1</strong> Derivation of Upper Bound of Information Leakage for ISS Scheme</td>
<td>130</td>
</tr>
<tr>
<td><strong>D.2</strong> Derivation of Upper Bound of Information Leakage for CAISS Scheme Under KMCA</td>
<td>132</td>
</tr>
<tr>
<td><strong>D.3</strong> Derivation of Upper Bound of Information Leakage for CAISS Scheme Under KMA</td>
<td>135</td>
</tr>
<tr>
<td><strong>D.4</strong> Derivation of Inequality ((5.17))</td>
<td>136</td>
</tr>
<tr>
<td><strong>D.5</strong> Derivation of Upper Bound of Information Leakage for MSS Scheme Under KMA</td>
<td>137</td>
</tr>
<tr>
<td><strong>D.6</strong> Derivation of Estimator ((5.20))</td>
<td>138</td>
</tr>
</tbody>
</table>
List of Figures

1.1 A data hiding system includes both the encoder and the decoder. .......................... 2
1.2 An illustration of spread spectrum-based embedding schemes. .............................. 5
1.3 An illustration of quantization index modulation-based embedding schemes. ......... 6
1.4 Dither modulation with uniform step sizes. .................................................... 7

2.1 The average bit error rates versus DWR for the ML decoders, where 4,096 bits of information are embedded in the DCT domain of each of the testing images employing the SS and ISS embedding schemes. ........................................ 30
2.2 The average bit error rate versus DWR for the ML decoders, where 4,096 bits of information are embedded in the DFT magnitude domain of each of the testing images employing the modified SS and ISS embedding schemes. ........ 30
2.3 The average bit error rates versus DWR for the ML, LOD, and LMMSE decoders, where 4,096 bits of information are embedded in the DCT domain of each testing image employing the SS and ISS embedding schemes. . . . . . . . . . 31
2.4 The empirical and theoretical average bit error rate versus DWR for the LMMSE and LOD decoders, where 4,096 bits of information are embedded in the DCT domain of each testing image employing the SS and ISS embedding schemes. . . 31
2.5 The average bit error rate versus DWR for the ML, LOD, and LMMSE decoders, where 4,096 bits of information are embedded in the magnitude of the DFT domain of each testing image. ..................................................... 31
2.6 The average bit error rate versus WNR for the ML, LOD, and LMMSE decoders, where 4,096 bits of information are embedded in the DCT domain of each testing image. ..................................................... 31
2.7 The average bit error rate versus WNR for the ML and LMMSE decoders, where 4,096 bits of information are embedded in the magnitude of the DFT domain of each testing image. ..................................................... 32

3.1 Illustration of the PDFs in (3.4) and (3.3) of the test statistic $z$ in (3.2) for the SS scheme. ..................................................... 52
**List of Figures**

3.2 Illustration of the PDFs in (3.7)-(3.10) of the test statistic $z$ in (3.6) for the proposed CASS scheme. .................................................. 52

3.3 Illustration of the PDFs in (3.32)-(3.35) of the test statistic $z$ in (3.31) for the proposed CAISS scheme. ................................. 53

3.4 With additional noise: Illustration of the PDFs in (3.52), (3.55), (3.53), and (3.54) of the test statistic $z$ in (3.51) for the CAISS scheme. ......................................................................................... 53

3.5 With additional noise: Illustration of the PDFs in (3.52)-(3.55) of the test statistic $z$ in (3.51) when $\lambda_h = 0$ for the CASS scheme. .......................................................... 53

3.6 The theoretical and experimental error probabilities versus DWR for the CASS scheme with different $A_1^2$. .......................................................... 53

3.7 The theoretical and experimental error probabilities versus DWR for the CAISS scheme with different $A_1^2$. .......................................................... 54

3.8 The logarithm of EPIF versus DWR curves for evaluating of decoding performance improvements of the proposed CAISS over the ISS scheme. .......................... 54

3.9 The IRIF versus DWR curves to illustrate the improvement of the proposed CAISS over ISS. Different $A_1^2$ values are illustrated. .................................................. 54

3.10 The theoretical and experimental results of the PDF expressed in (3.52). ................. 54

3.11 The theoretical and experimental error probabilities versus DWR for the CASS scheme with different WNR. .......................................................... 55

3.12 The theoretical and experimental error probabilities versus DWR for the CAISS scheme with different WNR. .......................................................... 55

3.13 The EPIF versus DWR curves to demonstrate the improvement of the proposed CAISS over SS. Different WNR values are illustrated. .......................... 55

3.14 The EPIF versus DWR curves to demonstrate the improvement of the proposed CAISS over ISS. Different WNR values are illustrated. .......................... 55

3.15 The EPIF versus WNR curves to demonstrate the improvement of the proposed CAISS over ISS. Different DWR values are illustrated. .................................................. 56

3.16 The logarithm of EPIF versus $N$ curves to demonstrate the improvement of the proposed CAISS over ISS where DWR = 25 dB. Different WNR values are illustrated. .................................................. 56

4.1 The experimental and theoretical PDFs for the random variable $g$ defined in (4.21), where $N = 60$ and DWR = 21 dB. .......................................................... 71

4.2 The PDFs of the first coefficient of the watermarked signal for the proposed IMSS scheme (4.14), where $s_1b = -1$, $N = 60$ and DWR = 21 dB. .................................................. 71

4.3 The experimental PDF of the test statistic $z$ for the MSS scheme when a binary message is sent, where $N = 100$ and DWR = 23 dB. .................................................. 71
<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.4</td>
<td>The experimental PDF of the test statistic $z$ for the IMSS scheme when a binary message is sent, where $N = 100$, DWR = 23 dB, and $d = 2$.</td>
</tr>
<tr>
<td>4.5</td>
<td>The experimental and theoretical (4.34) distributions for the proposed IMSS scheme, where $N = 60$, DWR = 21 dB and $b = +1$.</td>
</tr>
<tr>
<td>4.6</td>
<td>The experimental and theoretical (C.4) distributions for the MSS scheme, where $N = 60$, DWR = 0 dB and $b = +1$.</td>
</tr>
<tr>
<td>4.7</td>
<td>The theoretical (4.11) and experimental error probabilities for the MSS scheme where $N = 60$.</td>
</tr>
<tr>
<td>4.8</td>
<td>The required DWRs for achieving error free decodings in IMSS when different numbers of coefficients are used for embedding.</td>
</tr>
<tr>
<td>4.9</td>
<td>The $10\log(IIR)$ versus DWR curves for the MSS and IMSS schemes, where three different values of $d$ are considered and $N = 100$.</td>
</tr>
<tr>
<td>4.10</td>
<td>The BER versus DWR curves for the MSS and IMSS schemes when $N = 100$, $d = 1, 2, 3$ are considered in IMSS.</td>
</tr>
<tr>
<td>4.11</td>
<td>The BER versus DWR curves for the MSS scheme and the proposed IMSS scheme, where WNR = 5 dB and $N = 60$.</td>
</tr>
<tr>
<td>4.12</td>
<td>The experimental and theoretical BER versus WNR curves for the IMSS scheme, where DWR = 23 dB, $N = 60$, and $d = 2$.</td>
</tr>
<tr>
<td>4.13</td>
<td>The average BER versus PSNR curves for the MSS and IMSS schemes when applied on real images.</td>
</tr>
<tr>
<td>4.14</td>
<td>The average BER versus WNR curves for the MSS and IMSS schemes when applied on real images.</td>
</tr>
<tr>
<td>4.15</td>
<td>The experimental, theoretical (4.35), and empirical BER versus DWR curves for the IMSS scheme where $d = 2$.</td>
</tr>
<tr>
<td>5.1</td>
<td>Upper bounds of information leakage per dimension versus DWR for SS and ISS schemes under the KMA scenario, when $N_0 = 100$.</td>
</tr>
<tr>
<td>5.2</td>
<td>Upper bounds of information leakage per dimension versus $N_0$ for SS and ISS schemes under the KMA scenario, when $N = 100$.</td>
</tr>
<tr>
<td>5.3</td>
<td>Upper bounds of information leakage per dimension versus $N_0$ for the ISS and CAISS schemes under the KMA scenario, when DWR = 25 dB and $N = 100$.</td>
</tr>
<tr>
<td>5.4</td>
<td>Upper bounds of information leakage per dimension versus $N_0$ for CASS and CAISS schemes under KMA and KMCA scenarios when DWR = 25 dB, $N = 100$, and $\alpha = 0.8$.</td>
</tr>
<tr>
<td>5.5</td>
<td>Upper bounds of information leakage per dimension versus $N_0$ plots for the MSS scheme under the KMA scenario, when $N = 100$.</td>
</tr>
</tbody>
</table>
5.6 Upper bounds of information leakage per dimension versus $N_0$ for the SS, ISS, and MSS, CASS, and CAISS schemes under the KMA scenario, when DWR = 25 dB, $N = 100$, and $\alpha = 0.8$. .......................................................... 91
5.7 Upper bounds of information leakage per dimension versus $N_0$ for the SS, ISS, CASS, and CAISS schemes under the KMA scenario, when DWR = 21 dB, $N = 100$, and $\alpha = 0.8$. .......................................................... 92
5.8 The average normalized correlation between the estimated and actual signature codes versus $N_0$ plots for the SS, ISS, MSS, CASS, and CAISS schemes, when DWR = 25 dB, $N = 100$, and $\alpha = 0.8$ under KMA. .................................................. 92
5.9 The average normalized correlation between the estimated and actual signature codes versus $N_0$ plots for the SS, ISS, MSS, CASS, and CAISS schemes, when DWR = 21 dB, $N = 100$, and $\alpha = 0.8$ under KMA. .................................................. 92
5.10 The average normalized correlation between the estimated and actual signature codes versus $N_0$ plots for the CASS and CAISS schemes, when DWR = 25 dB, $N = 100$, and $\alpha = 0.8$ under KMA and KMCA. .................................................. 92
5.11 The average normalized correlation between the estimated and actual signature codes versus $N_0$ plots for the SS, ISS, CASS, and CAISS schemes, when DWR = 25 dB, $N = 100$ under KMCA. .................................................. 93
List of Acronyms

CASS  Correlation-Aware Spread Spectrum
CAISS  Correlation-Aware Improved Spread Spectrum
CDF  Cumulative Distribution Function
DCT  Discrete Cosine Transform
DFT  Discrete Fourier Transform
DM  Dither Modulation
DWR  Document to Watermark Ratio
EPIF  Error Probability Improvement Factor
GGD  Generalized Gaussian Distribution
IMSS  Improved Multiplicative Spread Spectrum
IRIF  Interference Robustness Improvement Factor
ISS  Improved Spread Spectrum
KMA  Known Message Attack
KMCA  Known Message and Correlation Attack
LMMSE  Linear Minimum Mean Square Error
LOD  Local Optimum Decoder
ML  Maximum Likelihood
MSS  Multiplicative Spread Spectrum
PDF  Probability Density Function
PIF  Payload Improvement Factor
**List of Acronyms**

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>QIM</td>
<td>Quantization Index Modulation</td>
</tr>
<tr>
<td>SS</td>
<td>Spread Spectrum</td>
</tr>
<tr>
<td>STDM</td>
<td>Spread Transform Dither Modulation</td>
</tr>
<tr>
<td>WNR</td>
<td>Watermark to Noise Ratio</td>
</tr>
<tr>
<td>WOA</td>
<td>Watermark Only Attack</td>
</tr>
</tbody>
</table>
Acknowledgments

First and foremost, I would like to express my deep sincere gratitude to my advisor, Professor Z. Jane Wang, for her support and invaluable advice during my Ph.D. study. This thesis would never be possible without her guidance and support over the years. As a distinguished professor, Jane taught me how to be an independent researcher. The knowledge and attitude I learned from her benefit me forever.

I would like also to express thanks to my wonderful collaborators and fellow graduate students at UBC.
Dedication

To my lovely wife, Mahsa,
who encouraged me over the years of my study,

and

To my family,
who supported me spiritually from miles away.
Chapter 1

Introduction

The growing use of Internet has enabled the users to easily access, share, manipulate, and distribute the digital media data, and digital media has profoundly changed our daily life during the past decade. This proliferation of digital media data creates a technological revolution to the entertainment and media industries, brings new experience to users, and introduces new Internet concepts. However, the massive production and use of digital media also pose new challenges to the copyright industries and raise critical issues of protecting intellectual property of digital media, since current media sharing makes unauthorized copying and illegal distribution of the digital media much easier.

One way of protecting the digital media data is cryptography where the encrypted content is not meaningful to the third party who does not have the authorized access right. Yet, once the decryption key is known to the intruder or the content is decrypted, the content could be duplicated and distributed illegally. One promising way of providing post-delivery content protection is digital watermarking. In the digital watermarking technology, a specific signal is embedded into the host media content without significantly degrading the perceptual quality of the original media data, and the embedded information can later be extracted for desired purposes. Since this embedded watermark signal is usually not noticeable, digital watermarking could provide post-delivery protection for the digital content. Digital watermarking has many applications, and one important application is data hiding, where the embedded hidden message should be decoded accurately at the receiver side and such hidden information can be used to serve covert communications, help verifying the authenticity of the digital media data, identifying the original source, and facilitating the investigation on illegal usages and copyright violations. Below in this chapter we will provide a brief overview of data hiding using digital watermarking. In the literature, people sometimes do not distinguish the terminologies of digital watermarking and digital data hiding.

The rest of this chapter is organized as follows. In Section 1.1, we briefly review the data hiding concept. Then, in Section 1.2 some applications of digital data hiding are mentioned. Section 1.3 introduces the main challenges for designing a data hiding scheme. The contributions made in this thesis are summarized in Section 1.4 and the thesis organization is provided in Section 1.5.
1.1 Watermarking and Data Hiding

Digital data hiding using watermarking can be defined as the procedure of embedding hidden information into a certain media signal which acts as a host signal. Generally, a data hiding system generally contains two basic modules (see Figure 1.1). The first module is the encoder which is used by the system to embed the desired hidden information. The structure of the encoder depends on the specific embedding (watermarking) scheme used for hiding the information. The second module of a data hiding system is the decoder which is used to extract the hidden information at receiver side. The structure of the decoder depends on the embedding scheme which the encoder uses for information hiding. Even though data hiding was invented primarily for ownership proof, it started finding other applications because of the wide use of Internet and digital media.

Digital data hiding techniques can be applied to different types of digital media contents such as image [40, 43, 58, 63, 77, 87, 104, 122, 133, 158], audio [16, 19, 48, 64, 74, 76, 90, 144, 145, 150], and video [33, 67, 68, 75, 88, 100, 101, 115, 128, 149]. Some embedding techniques are particularly developed for a specific type of media, such as image [3] or audio [16], and other ones can be more general [28].

Depending on the application, different categories of watermarking schemes could be applied. If the integrity of the content is rather important, in order to detect any tampering of the content, fragile watermarking is preferred [23, 78, 97, 154, 157]. This kind of data hiding is sensitive to any manipulation of the data (e.g., if the content gets tampered, the hidden information can be used to detect the tampered content), and thus it could help for integrity verification. In fragile watermarking, content manipulation leads to altered watermark. For instance, it could end up with the changed watermark even under standard operations such as compression. Therefore, there is a need for watermarking schemes where the watermark could withstand certain content changes to some extent. This category of data hiding schemes is called semi-fragile watermarking where the watermark does not change under some standard operations [50, 86, 89, 132, 161]. Another category is robust watermarking schemes which should be
1.1. Watermarking and Data Hiding

robust against different distortions and attacks \cite{11, 32, 66, 130, 155}. This robust watermarking category is for applications such as copyright protection where the watermark should survive certain distortions and attacks. Watermarking schemes can also be categorized into visible and invisible schemes. Invisible watermarking is employed in most applications where the embedding schemes use perceptual masking for imperceptible watermarking \cite{8, 71, 83, 119, 156}. In some applications, for indicating ownership of the content and enhancing the copyright protection, a visible or audible watermark is added into the original contents \cite{51, 82, 125, 152, 153}.

Watermarking schemes can also be categorized into blind and non-blind cases, depending on whether the decoder has access to the original content or not. For extracting the hidden information at the receiver side, if the decoder does not have access to the original host content, the situation is referred as blind watermarking or blind data hiding, and otherwise it is called non-blind watermarking, non-blind data hiding, or non-blind decoding \cite{2, 59, 147, 151}. Since in practice, the original content is generally not provided at the decoder side, the blind schemes are more commonly applied.

Depending on different purposes, there are two main types of watermarking schemes: in one type, the embedded watermark is used to communicate a specific hidden message (e.g., binary identification numbers used for image tracking and for video distribution, or a secret hidden message represented by binary sequences) which must be extracted with sufficient decoding accuracy. In the other type of systems, the goal is only to verify whether a specific embedded watermark (e.g., representing copyright information) is presented or not, and the embedded watermark normally does not communicate a secret message that needs to be accurately decoded. Therefore current researches on watermark extraction can be categorized into two broad topics: \textit{watermark decoding} \cite{9, 15} for the case of decoding the hidden message and \textit{watermark detection} \cite{22, 54, 96, 159, 160} for the case of detecting the presence of a specific watermark. In watermark decoding, the embedded hidden message should be decoded accurately at the receiver side and therefore the bit error rate is usually used as the performance criterion to measure the accuracy of the decoder in extracting the hidden message. In watermark detection (e.g., with the applications of ownership proof or broadcast monitoring), the goal is to determine whether a specific watermark has been inserted into the original media content or not, and the detection criteria are mainly based on Neyman-Pearson Theorem (i.e., maximizing the probability of detection for a given probability of false alarm). It should be mentioned that the above two problems are formulated differently and different detection (decoding) approaches are desired to serve different performance criteria. References \cite{9, 22, 54, 121, 159, 160} explicitly have pointed out this distinction in their works.

In this thesis, we focus on SS-based data hiding since we are particularly interested in communicating hidden message and thus our work belongs to the watermark decoding category.
1.2 Applications

Data hiding using watermarking was mainly invented to protect intellectual property rights for digital contents. It can perform copyright detection by retrieving the hidden information embedded in the host content [13, 79, 84, 85]. Fingerprinting for traitor tracing is another application of data hiding. In this scenario, copyright owners distribute a uniquely watermarked copy to each client and then monitor the distribution channel. Each pirated copy is then analyzed for identifying one or more fingerprints which lead to the origin of piracy. Meta data annotation could be achieved using data hiding where useful meta data is added to the original signal. For instance in audio signals, the embedded data could describe the content by using the song title or the name of the artist and this annotation makes indexing of the database easier [5, 46]. Covert communication is another data hiding application aiming to hide secret messages into the cover signal. The hidden message should not be transmitted without arising the suspicion of the existence of secret communications [36, 52, 55, 120, 146]. Such covert communication has a long history dated back to Herodotus time when he sent a message from the prison covertly. Digital media products are regularly transmitted through communication channels in order to be broadcasted through TV and radio stations. And therefore broadcast monitoring is important. One way of achieving broadcast monitoring is using data hiding where only certain contents, indicated by their watermarks, are allowed for broadcasting [80, 81]. In order to avoid counterfeiting and forgery, data hiding technique could serve as an authentication tool. In this case, the extracted hidden information are compared with the original information in order to determine whether they are the same [20, 30, 35, 53, 131].

1.3 Challenges of Data Hiding

Each digital data hiding system should fulfill some requirements: the embedded watermark should be imperceptible, meaning that the perceptual quality of the original content should not be degraded due to watermarking. For some applications (e.g., the embedded message should be extracted accurately even after unauthorized distortions), robustness is important. Payload is another concern which arises in the applications where the number of embedded bits should be high. Security is also a critical concern in data hiding, which implies that unauthorized party should not be able to reveal the hidden message.

All the above challenges are related to the encoder and decoder structures, and they rep-
1.3. Challenges of Data Hiding

Figure 1.2: An illustration of spread spectrum-based embedding schemes.

represent conflicting requirements. More precisely, for each application, the challenges should be considered first and then based on the requirements, the appropriate encoder and decoder should be chosen or devised to achieve a good trade-off. The encoder embeds the secret message based on the embedding scheme and the decoder extracts the embedded message based on the embedding scheme. It is clear that the embedding scheme and the decoder play important roles in a data hiding scheme and in addressing the corresponding challenges.

It is worth mentioning that, despite the popularity of digital data hiding (watermarking) techniques, effective digital right protection is extremely challenging and currently there is no commonly accepted technical solution which is practically unbeatable when deployed to practical user settings. At any sense, data hiding should only be considered as one important component of an overall protection system.

Below, we will discuss the two major modules of a data hiding system, the embedding scheme and the decoding scheme. Due to the importance of the topic of data hiding security, we will also discuss the security issue in this section.

1.3.1 Embedding Schemes

Primary data hiding techniques used heuristic algorithms based on simple image processing manipulations. Passing time, more sophisticated watermarking algorithms were proposed and used in different types of media data such as audio and video. Although many embedding schemes have been proposed, they could be mainly categorized into two groups: spread spectrum and quantization based methods.

Probably the first milestone in data hiding using watermarking was accomplished by Cox et al. [28] where they proposed Spread Spectrum (SS) scheme. As a matter of fact, in [28] two versions of SS were proposed. The first one is additive SS in which the watermark is spread over the host signal uniformly. The second one is the Multiplicative Spread Spectrum (MSS) which spreads the watermark according to the host content. Figure 1.2 depicts the SS embedding scheme where the dashed line shows that it is possible to add the watermark depending (MSS...
1.3. Challenges of Data Hiding

Figure 1.3: An illustration of quantization index modulation-based embedding schemes.

scheme) or without depending (additive SS scheme) on the content. In both schemes, in order to increase the security, a secret signature code for spreading the hidden message bits is used. SS schemes generally have great robustness. Hidden messages embedded under these schemes could robustly resist against lossy compressions and many other types of distortions and attacks. In spite of their great robustness against standard signal processing operations and manipulations, the main drawback of SS-based schemes is the host interference effect. Since in the SS schemes the host signal itself acts like a noise source at the decoder side and because of the fact that the watermark has relatively small power, the host signal imposes a big interference effect which causes a serious degradation of the decoding performance. To reduce the interference effect of the host signal, Malvar and Florencio proposed the Improved Spread Spectrum (ISS) scheme [92] by exploiting the side information at the encoder side. Their result brought the hope of having a robust embedding scheme with good decoding performance.

Another important milestone in embedding schemes was presented by Chen and Wornell [18] where they introduced a new class of embedding scheme called Quantization Index Modulation (QIM). In this scheme, each message in its alphabetical set has a corresponding quantization point. Figure 1.3 shows that as opposed to the SS scheme, the watermark is not added to the host signal directly. Instead, for embedding a message bit, the host signal is quantized to the nearest point in the corresponding quantizations points. They improved the QIM idea by exploiting Costa’s approach [25] and named the new scheme as QIM with distortion compensation (DC-QIM) [18]. In order to implement the QIM computationally efficiently, a practical quantizer ensemble called Dither Modulation (DM) which uses a dither vector was proposed by them. Figure 1.4 depicts the quantization points of the DM embedding scheme (with uniform step sizes). Spread Transform Dither Modulation (STDM), another variation of the original QIM, which blends the spread spectrum and quantization idea was proposed in their work as well [18]. The QIM approach could improve the decoding performance greatly by removing the interference effect of the host signal due to its quantization embedding nature. However, it suffers from sensitivity to scaling and lacking of content based embedding. Its sensitivity to
1.3. Challenges of Data Hiding

Figure 1.4: Dither modulation with uniform step sizes.

scaling causes drastically degradation of its performance and lack of content based embedding makes it susceptible to perceptible watermark. Even though some efforts have been made to tackle these deficiencies \([1, 42, 62, 109]\), more efforts are still needed for QIM to achieve a scheme which is robust against all of these drawbacks.

1.3.2 Decoding Schemes

Once the embedding scheme is known, the encoder embeds the message bits into the host signal accordingly and then the watermarked signal is distributed. Depending on the application, different embedding schemes can be employed, as it was explained earlier. The embedded message bits should be accurately extracted at the decoder side. We assume that the original host signal is not available at the decoder side and the decoding is done blindly. Decoder structure depends on the embedding scheme and deriving the optimal decoder could lead to better decoding performance. Here decoding performance could be assessed by the ratio of incorrect extracted bits to the total number of embedded bits, and a lower value means a lower error probability and thus indicates a better decoding performance.

In SS-based schemes, the host signal acts like noise and causes degradation in decoding performance. For minimizing the error probability, the Maximum Likelihood (ML) criterion can be exploited. It maximizes the probability distribution function of the received signal given the hidden bits in order to minimize the error. Therefore, using SS scheme in different host signals which have different distributions results different optimal decoders. The traditional decoder proposed by Cox et al. \([28]\) is the correlator which extracts the hidden bit using the correlation between the received signal and the signature code. This correlator decoder is optimal only when the host signal follows an independent and identical Gaussian distribution. One important point that should be taken into account is that sometimes the ML decoder ends up with a structure
1.3. Challenges of Data Hiding

requiring additional side information such as the watermark amplitude. In practice, such side information might not be available at the decoder side and it motivates us to derive suboptimal decoders which do not require such side information.

In QIM-based schemes, the information bit is embedded by quantization of the host signal regarding with the message bit. Therefore, the characteristics of quantization embedding could be exploited for decoding. The DM scheme uses dithered quantizers which have the property that the quantization cells of any quantizer in the ensemble are shifted version of the quantization cells of any other quantizer in the ensemble. Therefore the hidden bit could be extracted by finding the minimum distance of the received signal to quantization cells. Finding the minimum distance between the received signal and the codebook words is a general way for decoding in QIM schemes. This decoder structure can help explain why the QIM schemes can achieve perfect decoding performances in the absence of any additional noise and why their performances degrade dramatically with scaling of the received signals.

1.3.3 Security

Watermarking security analysis has attracted more research attention recently [7, 38]. Even though the concept of watermark security is still in its early stage, it is generally accepted that if the secret parameters of an embedding scheme of a known data hiding technique could be estimated, then the scheme is not secure. In other words, a data hiding scheme is considered secure if it could conceal its secret parameters. An attacker can gather observations from different host signals which are watermarked with the same secret parameters in order to obtain information about the secret parameters. Therefore, the security of an embedding scheme is related to the difficulty in estimating the secret parameters using available observations.

The first major attempt to provide a theoretical framework for assessing and classification of watermarking security was proposed by Cayre et al. [17] which led to related works [24] and [10]. They exploited the principles of the cryptanalysis in order to establish the concept of watermarking security [17]. Based on Kerckhoff’s principle [61] which was primarily used in cryptanalysis, it is assumed that except the secret key (secret parameters), all other details of the data hiding scheme are known publicly. Therefore, the security of a watermarking scheme relies on the secret key, and the adversary is only interested in disclosing the secret key. It is also assumed that the owner of the secret key uses the same secret key repeatedly in watermarking and the attacker has access to the observations (watermarked contents).

In order to define security attacks, some attack scenarios were presented in [17] by following the Diffie and Hellman methodology [29]. Security attack aims to obtain information about the secret key of the embedding scheme. The first attack is the Known Message Attack (KMA) where it is assumed that the attacker has access to both the observations and the embedded messages.
1.3. Challenges of Data Hiding

The second attack is Watermark Only Attack (WOA) where it is assumed that the attacker only has access to the watermarked signals. Another one is Known Original Attack (KOA) where it is assumed that the adversary has access to both the watermarked signals and the original content. KMA and WOA are more dominant attacks because attacker rarely has access to the original content (KOA case). Cayre et al. [17] proposed using of Fisher information [26] and statistical model of the embedding scheme for measuring the security quantitatively [17]. This security measurement has a drawback related to computation of the Fisher information which needs existence and differentiability of the log-likelihood function of the observations given the secret parameters.

The second main work in watermarking security was done in [108] where a security evaluation framework based on Shannon’s [123] mutual information was introduced. Similar to the cryptanalysis, they quantified the information about the secret key which is leaked out by the observations by Shannon’s mutual information. In QIM schemes, the secret key is cast to dither vector where is used in DM to randomize the embedding and decoding functions. The security of the QIM scheme under the KMA was investigated in [108]. In SS schemes, the secret key is cast to signature code used for embedding message. Assuming Gaussian distribution for the signature code, the security analysis of the additive SS under the KMA scenario was presented in [107]. Since KMA is a more powerful attack compared with WOA, we will investigate the security of the proposed SS schemes under this attack by following the mutual information framework.

1.3.4 Robustness and Watermark Attacks

One important issue in digital watermarking that needs to be addressed is proper evaluation and watermarking benchmarking. In order to have fair performance evaluation, we need to ensure that different watermarking schemes are investigated under comparable conditions, and benchmarks are needed (e.g., Stirmark package is probably the most popular benchmark and software for testing watermark robustness).

An important aspect of any digital watermarking scheme is its robustness against attacks. In digital watermarking, an attack is any processing that may impair watermark detection or watermark decoding. Since theoretical analysis of a watermarking scheme’s performance against different attacks can be rather complicated, experimental testing results performed on some benchmark are generally reported, where the benchmark includes possible attacks into a common framework.

Since different types of digital media content (e.g., image and audio) require investigating different attacks, here we briefly describe a list of state-of-the-art attacks for a certain type of digital media content. The attacks could be malicious where the attacker intentionally tries to
1.3. Challenges of Data Hiding

remove the watermark or could be the results of standard signal processing operations applied on the digital media content (e.g., compression and signal enhancement). A list of possible attacks for data hiding in the image is as follows [28, 70, 111]:

- **Low-pass filtering**: This attack occurs when the image undergoes filters such as median and Gaussian filtering.

- **Sharpening filtering**: This filter sharpens the image, especially the edges.

- **Histogram equalization**: For compensating the illumination condition, this image processing operation is employed.

- **Gamma correction**: It is frequently used for enhancing the images and adapting them for display.

- **Additive noise**: It is common that the received image can be contaminated by noise (e.g., as the result of transmission).

- **JPEG compression**: In practice, it is quite often that the image is compressed using JPEG compression.

- **Cropping**: Images could be cropped.

- **Rotation**: Images might be rotated by a small angle, and this rotation attack usually happens together with cropping.

- **Scaling**: It usually occurs when an image is scanned.

- **Generalized geometrical transformation**: It is a combination of scaling, rotation, and shearing.

- **StirMark**: It constitutes random geometric distortions provided by a software [111]. For instance, StirMark simulates printing and rescanning of an image.

- **Geometric distortion with JPEG**: It happens when the image is geometrically distorted and compressed by JPEG compression.

- **Printing/scanning**: It introduces geometric distortion as well as noise addition.

- **Synchronization**: It happens when the location of the embedded information is lost.

Regarding applicable attacks on audio watermarking, the following list is presented [16, 19, 126]:

- **Re-sampling**: It consists of subsequent down-sampling and up-sampling, respectively.
1.3. Challenges of Data Hiding

- **Quantization**: It occurs when the received signal is quantized according to a different quantization cell.

- **Low-pass filtering**: It happens when an audio signal passes through a low pass filter such as Butterworth with a determined cut-off frequency.

- **Echo**: It happens when an imperceptible delayed version of audio signal is added to the original signal.

- **Time scaling**: It usually happens when the time is stretched or shorten.

- **Pitch scaling**: It could happen when the pitch is slightly changed.

- **Audio compression**: It is quite common to compress the audio signal using MP3, MPEG2, and AAC, etc.

- **Additive noise**: It is similar to the image case (e.g., it could be the result of transmission).

We would like to mention two important notes here. The first one is that, depending on its specific application, each embedding scheme should be tested accordingly. For example, if digital compression is the sole attack for one specific application, testing robustness of a watermarking scheme against other attacks may not be necessary. The second point is that different embedding schemes show different robustness against different attacks. For instance, QIM can be vulnerable against quantization as mentioned earlier.

Cox *et al.* [28] tested their proposed SS scheme under different attacks. They report the robustness of SS scheme against signal processing operations such as lossy compression, filtering, digital-analog and analog-digital conversion, re-quantization, and common geometric transformations such as cropping, scaling, translation, and rotation. In [6], SS scheme was applied to the DCT domain. Experimental results show that the SS watermarking is robust to several attacks including JPEG compression, low pass and median filtering, Gaussian noise, and resizing. In [116], the SS scheme was applied to the DFT domain. Results presented in the paper show the robustness of the SS watermarking against geometric attacks such as translation, cropping, and resizing. Robust image watermarking using the SS scheme and in the wavelet domain was studied in [148]. It shows the robustness of watermark against some signal processing operations such as additive noise, low pass filter, re-quantization, image enhancement, blurring, and JPEG 2000 compression. Another SS based embedding approach in the wavelet domain was proposed in [143]. Experimental results show that the watermark can be efficiently retrieved after various attacks including additive noise, JPEG compression, blurring, sharpening, and median filtering. Another study [127] shows that the embedded message using SS is recoverable after some attacks such as Gaussian noise, sinusoidal pattern, and JPEG compression. It is
1.4 Contributions of the Thesis

noted that the SS watermark can survive StirMark and the embedded message can be accurately recovered. Another study [39] conducted experiments and results show the robustness of the SS watermarking against attacks such as JPEG compression, filtering, and cropping. The robustness of SS against attacks and distortions has been mentioned in other studies as well. For instance, in [112], the robustness of SS against scaling, JPEG compression, cropping, and printing/scanning was stated. In addition, in [111], it was stated that SS is very robust against amplitude distortion and noise addition.

In spite of the SS robustness against standard signal processing operations and manipulations, SS based schemes are not so robust against synchronization attack. To address this concern, depending on the type of media context, some solutions have been suggested to deal with synchronization attack. In audio watermarking, pilot signals could be embedded into the host signal which their relative distances to the watermark signal are known. Then, at the receiver side, the pilot signals are extracted and used for synchronization estimation. In addition, other solutions for tackling this issue in the audio domain have been proposed [37, 65, 69]. In image watermarking, local invariant features are commonly used to synchronize the location of embedded information and obtain robust schemes against geometric distortions [73, 99, 114, 129].

Due to the overall robustness of SS watermarking schemes, SS-based watermarking methods are the most popular and widely used. Therefore, this thesis focuses on different SS embedding schemes for data hiding.

1.4 Contributions of the Thesis

By addressing the above mentioned major challenges, this thesis is focused on developing improved SS embedding schemes for data hiding. The main contributions of this thesis are summarized as follow.

1. We investigate the SS schemes in the DCT and magnitude of DFT domains. In order to employ SS and ISS schemes for data hiding in the magnitude of the DFT domain, we show that the conventional scheme is not directly applicable. Therefore, we propose the modified SS embedding scheme in the DFT magnitude domain. Then, the optimal decoder in this domain is proposed. SS embedding schemes in the DCT domain are considered as well and the theoretical error probability for these embedding schemes are derived. Since side information, such as the watermark amplitude, is needed at the decoder side for optimal decoding, for relaxing the decoder from this requirement, Local Optimum Decoder (LOD) and Linear Minimum Mean Square Error (LMMSE) decoder are proposed. Their decoding performances are compared to that of the optimal decoder.
1.5 Organization of the Thesis

2. We propose the correlation-and-bit-aware concept for data hiding by exploiting the side information at the encoder side. At the encoder side, the correlation-and-bit-aware concept exploits the correlation information between the host signal and the signature code, and information of the message bit to be embedded. Based on this concept and employing SS and ISS schemes, Correlation-Aware Spread Spectrum (CASS) and Correlation-Aware Improved Spread Spectrum (CAISS) embedding schemes are proposed. The error probabilities of CASS and CAISS schemes are derived theoretically and the results show that using these embedding schemes could improve the decoding performance significantly. Also, we prove that employing CASS and CAISS schemes could improve payload compared with the traditional SS scheme.

3. We derive the error probability analysis of the MSS embedding scheme for data hiding and investigate the capacity of this scheme. We note that though MSS data hiding is content based, it still suffers from interference effect of the host signal. Since we know the decoder structure at the encoder side, it motivates us to propose an improved MSS embedding scheme which could reduce the host effect. The proposed Improved Multiplicative Spread Spectrum (IMSS) employs the correlation between the host signal and the signature code, and the correlation of the host signal with itself to reduce the host effect. Simulation results illustrate that the proposed IMSS scheme could improve the decoding performance remarkably.

4. We present the security analysis of the SS data hiding schemes under the KMA scenario. Exploiting the mutual information security measure, we analyze the information leakage of SS-based schemes, including SS, ISS, CASS, CAISS, and MSS schemes, under the KMA scenario. Further, to quantitatively illustrate embedding security in a practical way, we present some practical signature code estimators and evaluate the estimation accuracy performances via simulations. In addition, for the CASS and CAISS embedding schemes, we introduce the so-called Known Message and Correlation Attack (KMCA) and show that it is more powerful than KMA.

1.5 Organization of the Thesis

In the following, we provide a brief overview of the remainder of this thesis.

Chapter 2 considers efficient blind watermark decoding approaches for hidden messages, within the framework of SS schemes for data hiding. We study SS embedding in both the Discrete Cosine Transform (DCT) and the Discrete Fourier Transform (DFT) domains. First, we show that the conventional SS scheme could not be applied directly into the magnitudes of the
DFT coefficients, and thus we present modified SS and ISS schemes and the optimal maximum likelihood (ML) decoders based on the Weibull distribution are derived. Then, we investigate the SS and ISS embedding schemes in the DCT domain and derive the corresponding optimal ML decoders. We also provide theoretical error probability for these decoders in the corresponding domains. Finally, suboptimal decoders, including local optimum decoder (LOD) and linear minimum mean square error (LMMSE) decoder, are investigated to reduce the required prior information at the receiver side, and their theoretical decoding performances are derived. Based on decoding performances and the required prior information for decoding, we discuss the preferred host domain and the preferred decoder for additive SS-based data hiding under different situations. Extensive simulations are conducted to illustrate the decoding performances of the presented decoders.

Chapter 3 [136–138] presents a correlation-and-bit-aware concept for data hiding, and based on this concept two additive SS-based improved data hiding embedding schemes are introduced. We first propose the correlation-aware spread spectrum (CASS) embedding scheme, which is shown to provide better watermark decoding performance than the traditional additive spread spectrum (SS) scheme. Further, we propose the correlation-aware improved spread spectrum (CAISS) embedding scheme by incorporating SS, improved spread spectrum (ISS), and the proposed correlation-and-bit-aware concept. Compared with the traditional additive SS, the proposed CASS and CAISS maintain the simplicity of the decoder. Our analysis shows that, by efficiently incorporating the side information, CASS and CAISS could significantly reduce the host effect in data hiding and improve the watermark decoding performance remarkably. To demonstrate the improved decoding performance and the robustness by employing the correlation-and-bit-aware concept, the theoretical bit error performances of the proposed data hiding schemes in the absence and presence of additional noise are analyzed. Simulation results show the superiority of the proposed data hiding schemes over traditional SS schemes.

Chapter 4 [134, 139, 141] analyzes the error probability of the conventional multiplicative spread spectrum (MSS) scheme and derives the corresponding channel capacity. It is noted that the interference effect of the host signal causes the distribution leakage and contributes to the decoding performance degradation. Since the host signal and the decoder structure information are available at the encoder side, an improved multiplicative spread spectrum (IMSS) embedding scheme for data hiding is proposed. Since the host signal and the decoder structure information are available at the encoder side, the proposed IMSS scheme exploits both the correlation between the host signal and the watermark signal and the decoder structure in embedding the bit information to reduce the host interference effect. We show that, compared with MSS, the proposed IMSS maintains the simple decoder structure and does not require additional information for decoding. We also analyze the decoding performances of MSS and IMSS in the presence of
1.5. Organization of the Thesis

additional Gaussian noise. Simulation results depict the superiority of the proposed IMSS data hiding scheme over the conventional MSS scheme.

Chapter 5 presents the security analysis of ISS, CASS, CAISS, and MSS schemes under the KMA scenario. The amount of information about the secret key which leaks out from the observations is quantified by Shannon’s mutual information. Exploiting this security measure, we analyze the information leakage of ISS, CASS, CAISS, and MSS under the KMA scenario. Further, to quantitatively illustrate embedding security in a practical way, we present some practical signature code estimators and evaluate the estimation accuracy performances via simulations. Based on our security analysis, from a designer’s point of view, we show that it is possible to design an embedding scheme with both enhanced security and decoding performance, e.g., the CAISS scheme can both be more secure (measured by less information leakage) and provide better decoding performance when compared with the ISS scheme. Further, from an attacker’s point of view, we show that it is possible to devise a more effective attack. For instance, we introduce the so-called known message and correlation attack (KMCA) and show that it is more powerful attack than KMA.

Chapter 6 summarizes the contributions of this thesis and outlines a few future topics. Finally, Appendices include the proofs of some expressions stated in the thesis body.
Chapter 2

Efficient Blind Decoders for Additive Spread Spectrum

2.1 Introduction

In this chapter, our main purpose is to provide a watermark decoding framework for data hiding using spread spectrum embedding in the DCT domain and the DFT magnitude domain. DCT and DFT domains are widely used for compression and thus embedding in these domains is appealing. In addition, embedding in the frequency domain could help to improve the perceptual quality of the watermarked signal. In the literature, there is lack of investigation on the optimal decoder using the additive SS in the DFT magnitude domain and we will fill this gap in this chapter. We will show that the conventional SS scheme could not be applied directly in the DFT magnitude domain and thus we will propose a modified SS embedding scheme. In order to provide a guidance on the preferred domain for information hiding using additive SS embedding, based on the derived decoders, we will discuss which domain is preferred under different circumstances. In addition, we present a theoretical framework of optimal decoders for additive SS and ISS schemes in the DCT and DFT magnitude domains. We note that optimal decoders using ISS provide better decoding performances than the traditional additive SS. As the optimum ML decoder requires the distribution parameters of the host image and the watermark strength information, to address this concern, we also investigate several suboptimal watermark decoders. By invoking the Taylor series, the local optimum decoder (LOD) which is independent of watermark amplitude is proposed. Further, due to simplicity and good performance, we employ the linear minimum mean square error (LMMSE) criterion and derive the LMMSE decoders. Moreover, we derive the theoretical performance analysis of the suboptimal decoders.

The rest of this chapter is organized as follows. In Section 2.3, the traditional additive SS and ISS embedding schemes are briefly reviewed for data hiding and communicating hidden message. Host probability distribution functions for DCT and DFT domains are described in Section 2.4. The optimal ML decoders are derived in Section 2.5 and the corresponding bit-error-rate analyses are presented. In Section 2.6, the suboptimal decoders, including LOD and
LMMSE decoders are presented and their theoretical performance analyses will be provided. The simulation results are demonstrated in Section 2.7 to validate the analysis. Finally, the discussions and concluding remarks are given in Section 2.8.

2.2 SS Schemes

As it has been indicated in Chapter I, additive SS and ISS are two major SS embedding schemes. In the following subsections, the signal model of these embedding schemes are presented.

2.2.1 Additive SS Scheme

In the conventional SS scheme, the bit message $b$ with amplitude $A > 0$ is embedded into the host signal. The information bit to be hidden in the host signal is usually taken from the binary set $b \in \{ -1, +1 \}$. The binary message bit is embedded into the host signal $x = [x_1, x_2, \ldots, x_N]^T$. Here, $N$ is the number of the host coefficients used for conveying one information bit. The SS scheme employs a signature code $s = [s_1, s_2, \ldots, s_N]^T$ for the sake of security and this key is assumed to be selected from a binary set $s_i \in \{ -1, +1 \}$. Based on the SS embedding, the watermarked signal $r = [r_1, r_2, \ldots, r_N]^T$ can be represented in the following form

$$r_i = x_i + s_i A b, \quad i = 1, 2, \ldots, N. \quad (2.1)$$

Generally, the distortion due to any watermark embedding can be defined as

$$D = \frac{1}{N} E\{||r - x||^2\}, \quad (2.2)$$

where $E\{ . \}$ means the expectation operator and $\| . \|$ is defined as the norm of a vector. In the additive SS scheme the distortion is equal to $A^2$. Additive SS embedding scheme could be written in the vector form as $r = x + sA b$.

2.2.2 ISS Embedding Scheme

The traditional additive SS, where the host signal acts as a noise source, is a non rejected host method which does not use the host signal information in the decoder. It was shown in [92] that ISS, which reduces the interference effect of the host signal, leads to significant performance improvements. The signal model for ISS data hiding is defined as

$$r = s A b + t, \quad (2.3)$$
where

\[ t = (I_N - \lambda ss^T)x, \]  

(2.4)

where \( I_N \) denotes the identity matrix and \( \lambda \) is obtained usually by maximizing the watermark to data ratio or by minimizing the probability of error. The distortion for ISS embedding can be obtained as follows

\[ D = \frac{1}{N} E\{\|sAb - \lambda ss^T x\|^2\} = A^2 + \lambda^2 s^T R_x s, \]  

(2.5)

where \( R_x \) is the correlation matrix of the host signal. When the host signal coefficients’ are uncorrelated with variance \( \sigma_x^2 \), (2.5) becomes \( D = A^2 + \lambda^2 N\sigma_x^2 \).

### 2.3 Additive SS and ISS Schemes Applied to Images

In this section, we consider the additive SS and ISS schemes in order to embed the information in the images.

Suppose a host image \( I \in \mathcal{M}^{m \times n} \) is supposed to be watermarked, where \( \mathcal{M} \) means the image alphabet, e.g., \( \mathcal{M} = \{0, 1, \ldots, 255\} \) for a gray scale image, and \( m \) and \( n \) represent the size of the image in the pixel (spatial) domain. Here for simplicity we assume \( m = n \), though the results could be extended to the general case of having unequal \( m \) and \( n \). The additive SS embedding procedure for a host image is summarized as follows. First, the image \( I \) is partitioned into \( \frac{m}{p} \times \frac{m}{p} \) sub-blocks of size \( p \times p \). Then, each block is usually transformed to a domain which is insensitive to tampering, i.e., \( \mathcal{T}(I) \in \mathbb{R}^{p \times p} \) where \( \mathcal{T} \) denotes the transform function transforming the host image into the new domain called host domain. For the total \( q = \left(\frac{m}{p}\right)^2 \) sub blocks, each of them conveys one hidden information bit for one-message embedding or multiple hidden information bits for multi-message information embedding. A perfect transform should be insensitive against operations such as translation, lowpass filtering, compression, and other standard signal processing manipulations. In the context of image processing, two popular transform domains include the DCT and DFT which are of interest of this Chapter.

For each block of size \( p \times p \) in the transformed domain, a subset of host coefficients with length \( N \leq p^2 \) is selected to be the carrier vector for embedding. Such selected vectors \( x_i \in \mathbb{R}^N, i = 1, 2, \ldots, q \), are used for information embedding employing the signature code.

The point that should be taken into account is that different domain host signals may affect the procedure of adding the information. Using the DCT domain makes no restriction on the additive SS watermarking. Employing the DFT and explicitly embedding the information in the magnitude of DFT coefficients limit the set of coefficients to be watermarked, since the watermarked DFT coefficients are required to be positive. We will discuss about the embedding
scheme in the magnitude of the DFT domain more precisely when the optimal decoders are explained in Section 2.5.

### 2.4 Data Hiding in the DCT and the DFT Magnitude Domains

As it was explained in Section 2.3 the message bits could be embedded in the DCT and DFT domains. In order to find the optimal decoders, the distributions of the DCT and DFT coefficients are needed to be known. The authors in [47] suggested that the heavy tailed property for low and mid frequency of DCT coefficients can be modeled by the zero mean Generalized Gaussian Distribution (GGD) as

\[
fx(x) = \alpha e^{-|\beta x|^c}, \quad (2.6)
\]

where

\[
\alpha = \frac{\beta c}{2\Gamma\left(\frac{1}{c}\right)}, \quad \beta = \frac{\Gamma(3/c)}{\Gamma(1/c)} \sigma_x, \quad (2.7)
\]

and \(\sigma_x\) means the standard deviation of the host signal and \(\Gamma(.)\) means the Gamma function defined as \(\Gamma(x) = \int_0^{\infty} t^{x-1} e^{-t} dt\). The power exponent \(c\) is the shape parameter where its smaller value leads to the more impulsive shape and heavier tail. The scale parameter \(\beta\) and the shape parameter \(c\) can be estimated from the host signal [98].

The DFT is another popular transform domain for image analysis, where the DFT magnitude could be used to represent the host signal. Since the magnitude of the DFT coefficient is real and positive, the Weibull distribution was suggested [9] to model the Probability Density Function (PDF), because of its flexibility and consistency with the DFT magnitude, as follows

\[
fx(x) = \frac{1}{\eta} \left(\frac{|x|}{\eta}\right)^{\gamma-1} \exp\left[-\left(\frac{|x|}{\eta}\right)^\gamma\right] u(x), \quad (2.8)
\]

where \(u(.)\) determines the step function which returns one where its argument is positive and returns zero when its argument is negative. Moreover, the parameters \(\eta > 0\) and \(\gamma > 0\) represent the scale and the shape parameters of the Weibull distribution.
2.5 The ML Optimal Decoders

The optimal decoder obtains an estimate $\hat{b}$ of $b$ such that the probability error $P_e = Pr\{\hat{b} \neq b\}$ is minimized. This can be done with the ML decoder as follows

$$\hat{b} = \arg \max_{b \in \{\pm 1\}} f(r|b, s), \quad (2.9)$$

where $f(r|b, s)$ represents the conditional PDF of $r$ when given $b$ and $s$. It is clear that the distribution of the host signal plays an important role in the ML decoder structure and thus, distribution of the DCT and magnitude of DFT domains were introduced in Section 2.4. As discussed in Section 2.4, the PDF of the host signal can be different depending on the transform domain. In practice, due to different desired properties, different transform domains could be used for data hiding. Derivation and performance analyses of the ML decoder for SS embedding require the distribution of the host signal in a specific domain. In the following subsections, the ML decoders for SS and ISS embedding schemes in DCT and magnitude of DFT domains are derived. It is worth mentioning that the ML decoder for the SS scheme in the DCT domain has been already proposed in [47].

2.5.1 ML Decoders in the DFT Domain

One possible host signal for information hiding is the DFT magnitude domain. However, it is important to note that the SS (2.2) and ISS (2.5) embedding schemes cannot be applied directly in this domain because of the special property of the magnitudes of the DFT coefficients, i.e., they should be always positive. To ensure the intuition that the watermarked signal should be always positive, we propose a modified SS embedding scheme in the DFT magnitude domain as follows

$$r = x + sAb + e, \quad (2.10)$$

where the insurance vector $e = [e_1, e_2, \ldots, e_N]^T$ is designed to make $r_i$’s positive. More specifically, if $x_i + s_iAb$ is positive, its corresponding element $e_i$ is set to be zero; If $x_i + s_iAb$ is negative, $e_i = -s_iAb$ is set to make $r_i$ equal to $x_i$, which is consequently positive. In summary, $e_i$ in (2.10) can be formulated as

$$e_i = (-s_iAb)u(-(x_i + s_iAb)). \quad (2.11)$$

The modified SS embedding scheme (2.10) and the vector $e$ defined in (2.11) reveal that, for those coefficients where $e_i > 0$, the watermarked signal becomes $r_i = x_i$. However, because of the structure of the optimal decoder, which will be derived shortly, such $r_i$’s still could help for decoding. We also note that, for the modified SS scheme (2.10), by increasing the watermark
amplitude $A$, the number of coefficients with $e_i > 0$ increases. Generally, the goal of this modified SS embedding scheme is to make all the watermarked coefficients positive.

Having proposed the modified SS embedding scheme for information hiding in the magnitude of the DFT domain, we can derive the optimal decoder using the distribution of the host signal. Based on (2.9), the decoder decides $\hat{b} = 1$ if (see Appendix A.1)

$$
\frac{\exp\left\{-\sum_{i=1}^{N} \left(\frac{|r_i - s_i A|}{\eta_i}\right)^{\gamma_i}\right\}}{\exp\left\{-\sum_{i=1}^{N} \left(\frac{|r_i + s_i A|}{\eta_i}\right)^{\gamma_i}\right\}} \prod_{i=1}^{N} \left(\frac{|r_i - s_i A|}{\eta_i}\right)^{\gamma_i-1} u(r_i - s_i A) > 1.
$$

(2.12)

Investigating the ML decoder in the DFT magnitude domain reveals that the information bit amplitude as well as the PDF parameters should be provided at the receiver side. Now, we proceed to show that the decoding procedure is error free for two cases. For one case that $b = +1$ and there is at least one coefficient with $r_i + s_i A < 0$ at the decoder side, we can see that the left side in (2.12) goes to infinity and thus the decoder definitely decides $\hat{b} = +1$. More precisely, in this case, $u(r_i - s_i A)$ is positive and $u(r_i + s_i A)$ equals to zero, and thus the left side in (2.12) goes to infinity. Similarly, for the other case that $b = -1$ and at the decoder side there is at least one coefficient with $r_i - s_i A < 0$, the left side in (2.12) is equal to zero and thus the decoder definitely decides $\hat{b} = -1$.

As mentioned earlier, the coefficients that $e_i > 0$ could help error free decoding. To explain this better, let assume that $b = +1$ and $x_i + s_i A < 0$, thus the corresponding coefficient becomes $r_i = x_i$ at the embedding side. At the decoder side we will have $r_i + s_i A < 0$, which based on the above discussion, leads to the decision $\hat{b} = +1$. Similarly, let assume that $b = -1$ and $x_i - s_i A < 0$, thus the corresponding coefficient becomes $r_i = x_i$ at the embedding side. At the decoder side we will have $r_i + s_i A < 0$, which leads to decision $\hat{b} = -1$. In both cases, the decoder performance would be error free and therefore, coefficients with $e_i > 0$ could contribute to accurate decoding.

Deriving an analytic expression for the probability of error is always desirable, because it could help to analyze the behavior of the error. In Appendix A.1 has been shown that the error probability could be approximated as

$$
P_e = \frac{1}{2} \text{erfc}\left(\sqrt{\frac{m_z^2}{2\sigma_z^2}}\right),
$$

(2.13)

where

$$
m_z = \sum_i \left\{ \frac{1}{2} \left(\frac{|x_i + 2A|}{\eta_i}\right)^{\gamma_i} + \frac{1}{2} \left(\frac{|x_i - 2A|}{\eta_i}\right)^{\gamma_i} + \frac{1}{2} (\gamma_i - 1) \ln \left(\frac{x_i^2}{|x_i^2 - 4A^2|}\right) - \left(\frac{x_i}{\eta_i}\right)^{\gamma_i}\right\}.
$$

(2.14)
2.5. The ML Optimal Decoders

\[ e_z^2 = \frac{1}{2} \left( \sum_i \left\{ \frac{1}{2} \left( \frac{|x_i + 2A|}{\eta_i} \right)^{\gamma_i} - \left( \frac{x_i}{\eta_i} \right)^{\gamma_i} + (\gamma_i - 1) \ln \left( \frac{x_i}{|x_i + 2A|} \right) \right\}^2 \right. \]
\[ + \frac{1}{2} \left( \sum_i \left\{ \frac{1}{2} \left( \frac{|x_i - 2A|}{\eta_i} \right)^{\gamma_i} - \left( \frac{x_i}{\eta_i} \right)^{\gamma_i} + (\gamma_i - 1) \ln \left( \frac{x_i}{|x_i - 2A|} \right) \right\}^2 \right. \], \quad (2.15) \]

and \( \sigma_z^2 = e_z^2 - m_z^2 \). Therefore, the theoretical error probability of the modified SS scheme is expressed as (2.13) when the mean and variance could be achieved using (2.14) and (2.15).

Having introduced information embedding using the modified SS scheme in the DFT magnitude domain, we now present the modified ISS scheme. Similar to the modified SS scheme, to avoid having negative watermarked coefficients, we propose a modified ISS embedding scheme as

\[ r = sA\beta + t + e, \] \quad (2.16) \]

where the insurance vector \( e \) is determined as follows. If \( t_i + s_iA \) is positive then the corresponding \( e_i \) is set to zero; If \( u_i + s_iA \) is negative, then \( e_i = -s_iA + \lambda s_i\beta^T x \) to ensure that \( r_i \) is positive. Therefore \( e_i \) in the modified ISS scheme could be expressed as

\[ e_i = (-s_iA + \lambda s_i\beta^T x)u(-(t_i + s_iA)). \] \quad (2.17) \]

Similar to the decoder (2.12), it has been shown in Appendix [A.2] that the ML decoder for the ISS scheme is obtained as

\[
\exp \left\{ \frac{-\sum_{i=1}^N \left| m_i (r - sA) \right|^{\gamma_i}}{\eta_i} \right\} \prod_{i=1}^N \left[ \frac{\left| m_i (r - sA) \right|^{\gamma_i - 1} u(r_i - s_iA + \lambda s_i\beta^T x)}{\left| m_i (r + sA) \right|^{\gamma_i - 1} u(r_i + s_iA + \lambda s_i\beta^T x)} \right] > 1. \] \quad (2.18) \]

which \( m_i \) is the \( i \)th row of \( M^{-1} \) where \( M = I - \lambda \beta \beta^T \).

According to the modified embedding scheme (2.16) the watermarked signal lies in the positive domain. Therefore, similar behavior to the SS scheme could be observed in ISS scheme as well. So, we will apply the modified ISS scheme in (2.16) for embedding, and use the decoder in (2.18) for extracting the hidden information.

Similar to the SS case, the error probability could be approximated by (2.13) where (cf. Appendix [A.2])

\[ m_z = \sum_i \left\{ \frac{1}{2} \left( \frac{|a_i|}{\eta_i} \right)^{\gamma_i} + \frac{1}{2} \left( \frac{|d_i|}{\eta_i} \right)^{\gamma_i} + \frac{1}{2} (\gamma_i - 1) \ln \left( \frac{x_i^2}{|a_i d_i|} \right) - \left( \frac{x_i}{\eta_i} \right)^{\gamma_i} \right\}, \] \quad (2.19) \]
2.5. The ML Optimal Decoders

\[ e_z^2 = \frac{1}{2} \left( \sum_i \left\{ \frac{1}{2} \left( \frac{|a_i|}{\eta_i} \right)^{\gamma_i} - \left( \frac{x_i}{\eta_i} \right)^{\gamma_i} + (\gamma_i - 1) \ln \left( \frac{x_i}{|a_i|} \right) \right\} \right)^2 + \]
\[ \frac{1}{2} \left( \sum_i \left\{ \frac{1}{2} \left( \frac{|d_i|}{\eta_i} \right)^{\gamma_i} - \left( \frac{x_i}{\eta_i} \right)^{\gamma_i} + (\gamma_i - 1) \ln \left( \frac{x_i}{|d_i|} \right) \right\} \right)^2 , \] (2.20)

where \( a_i = x_i + 2A(N\mu + 1) \), \( d_i = x_i - 2A(N\mu + 1) \), and \( \mu = (\lambda^{-1} - N)^{-1} \).

The remaining point is determining the parameter \( \lambda \) in ISS embedding which could be achieved using the probability of error. This parameter should take the value which minimizes the theoretical probability of error. Thus, regarding to the obtained probability for the ISS, \( \lambda \) is obtained as

\[ \lambda_k = \arg\max_{\lambda} \frac{m_i^2}{\sigma_z^2} . \] (2.21)

2.5.2 ML Decoders in the DCT Domain

As opposed to the SS and ISS schemes in the magnitude of DFT which suffered from lack of optimal decoder, the optimal decoder in the DCT domain exploiting SS scheme has been accomplished in [47]. It has been shown [47] that the test statistic of the ML is in the form

\[ z = \sum_{i=1}^{N} \left[ \left( \frac{r_i + s_iA}{\sigma_{x_i}} \right)^c \right] - \left[ \left( \frac{r_i - s_iA}{\sigma_{x_i}} \right)^c \right] . \] (2.22)

We can see that the ML decoder requires knowledge of the information bit amplitude and the shape parameter. For practical implementation, the receiver should either have prior information about the shape parameter or estimate it. One way to avoid estimating the shape parameter is to use a general value for all images, hoping it could describe the distribution of the DCT coefficients relatively well [12, 91].

Now, we extend this work to obtain the ML decoder for ISS embedding scheme in the DCT domain to achieve better decoding performance. Exploiting the ML criterion leads to the test statistic of the optimal decoder for ISS scheme as follows (see Appendix A.3)

\[ z = \sum_{i=1}^{N} \left[ \left( \frac{m_i(r + sA)}{\sigma_{x_i}} \right)^c \right] - \left[ \left( \frac{m_i(r - sA)}{\sigma_{x_i}} \right)^c \right] . \] (2.23)

Having proposed the optimal decoder of the ISS scheme in the DCT domain, the error
2.6 Suboptimal Decoders

probability is obtained by (2.13) where the mean and variance are determined as follow:

\[ m_z = \sum_{i=1}^{N} \left( \frac{1}{\sigma_{x_i}} \right)^c \left( \frac{1}{2} |x_i + 2A(\lambda \mu + 1)|^c + \frac{1}{2} |x_i - 2A(\lambda \mu + 1)|^c - |x_i|^c \right), \tag{2.24} \]

\[ \sigma_z^2 = \sum_{i=1}^{N} \left( \frac{1}{\sigma_{x_i}} \right)^{2c} \left( \frac{1}{4} [ |x_i + 2A(\lambda \mu + 1)|^c - |x_i - 2A(\lambda \mu + 1)|^c ]^2 \right). \tag{2.25} \]

Similar to the ISS embedding in the magnitude of the DFT domain, the parameter \( \lambda \) could be determined using the constrained maximization (2.21) taking into account the mean and variance defined in (2.24) and (2.25).

2.6 Suboptimal Decoders

As shown in Section 2.5, the ML decoder requires the host distribution parameters as well as the watermark amplitude. Assuming low distortion due to watermark, we could estimate the host signal parameters using the received signal, while estimating the watermark amplitude is not easy because of the complex structure of the embedding scheme. Therefore, to reduce the dependency on such prior information, in this section, we will investigate two suboptimal decoders. In addition, since it was shown that the ML decoder for embedding in the magnitude of the DFT domain is sensitive to watermark amplitude, we hope that the suboptimal decoders in this domain could decrease this sensitivity and lead to good performances in the presence of additional noise.

2.6.1 Local Optimum Decoder

To make the hidden information imperceptible, the watermark amplitude should be small. This motivates us to explore the LOD idea of using Taylor expansion of the test statistic around zero. The Taylor series of \( f(x) \) around the point \( x = a \) excluding the second and higher orders can be expressed as

\[ f(x) = f(a) + \dot{f}(a)(x - a), \tag{2.26} \]

where \( \dot{f}(a) \) is the first order derivative of \( f(.) \) at the point \( x = a \).

Having introduced this approximation, we first consider the LOD for SS embedding in the DCT domain. Taking into account the point that the test statistic (2.22) at \( A = 0 \) equals to zero, and deriving the Taylor series around \( A = 0 \), the LOD for SS embedding in the DCT
2.6. Suboptimal Decoders

domain is achieved by
\[
\hat{b} = \text{sign} \left\{ \sum_{i=1}^{N} \frac{s_i |r_i|^{(c-1)} \text{sign}\{r_i\}}{\sigma_{x_i}^c} \right\}. \tag{2.27}
\]

The provided above decoder expression reveals that it is independent of the watermark amplitude and appropriate for the cases which there is no access to the watermark amplitude.

Having obtained the test statistic of LOD for SS embedding, the error probability can be analyzed using (2.13) where it could be shown that the mean and the variance are as follow
\[
m_z = \sum_{i=1}^{N} \left[ \frac{1}{\sigma_{x_i}^c} \left( |x_i + A|^{(c-1)} \text{sign}\{x_i + A\} - |x_i - A|^{(c-1)} \text{sign}\{x_i - A\} \right) \right], \tag{2.28}
\]
\[
\sigma_z^2 = \sum_{i=1}^{N} \left[ \frac{1}{\sigma_{x_i}^2} \left( |x_i + A|^{(c-1)} \text{sign}\{x_i + A\} + |x_i - A|^{(c-1)} \text{sign}\{x_i - A\} \right)^2 \right]. \tag{2.29}
\]

We follow the same procedure provided for LOD using the SS scheme to obtain its counterpart using the ISS scheme. In Appendix A.4 has been shown that the LOD for ISS embedding scheme is obtained by
\[
\hat{b} = \text{sign} \left\{ \sum_{i=1}^{N} \left[ \frac{1}{\sigma_{x_i}^c} (N\mu + 1)\mu s_i \sum_{j \neq i} s_j r_j + (1 + \mu) r_i \right]^{(c-1)} \text{sign}\left\{ \mu s_i \sum_{j \neq i} s_j r_j + (1 + \mu) r_i \right\} \right\}. \tag{2.30}
\]

Finally, similar procedure could be taken to obtain the LOD in the DFT magnitude domain. Referring to the test statistic (A.3), we can obtain the LOD decoder for SS embedding in the DFT magnitude domain as
\[
\hat{b} = \text{sign} \left\{ \sum_{i} \left[ \frac{r_i^{\gamma_i - 1} s_i \gamma_i}{\eta_i^{\gamma_i}} - (\gamma_i - 1) \frac{s_i}{r_i} \right] \right\}. \tag{2.31}
\]

It is worthy mentioning that, since LOD is independent of the watermark amplitude \(A\), decoding performance degradation is observed in LOD compared with ML, especially for the high watermark amplitude cases. As discussed in Section 2.5, the watermarked coefficients with \(x_i - s_i A < 0\) or \(x_i + s_i A < 0\) help accurate decoding in the ML decoder. From the LOD in (2.31), it is clear that with no access to the watermark amplitude information, all the received coefficients are exploited for extracting the hidden information even though some of them do not convey any information. This is the source of the decoding performance degradation of LOD.
2.6. Suboptimal Decoders

2.6.2 LMMSE Decoder

In Section 2.5, we focused on the optimal ML decoders, which require the PDF parameters as well as the watermark strength and signature code. Since providing the watermark strength information to the decoder is not always possible, the LOD decoder was proposed in Section 2.6 to make the decoders independent of this information. However, the PDF parameters are still required by these decoders. This motivated us to develop suboptimal decoders which depend neither on PDF parameters nor on the watermark strength information. Here, we introduce the LMMSE decoder which requires only the signature code as prior information at the decoder side.

In signal processing, the mean square error (MSE) is a common measure of estimation and the MMSE estimator minimizes the mean square error in a Bayesian setting. More specifically, let $\theta$ be an unknown random variable to be estimated, and let $y$ be the measurement, the MMSE estimator is to find a function $\hat{\theta} = g(y)$ such that it minimizes the MSE $E\{ (\theta - g(y))^2 | y \}$. In many cases, the minimum mean square error estimator could not be achieved, since we may not know the distributions $f(\theta | y)$ and $f(\theta, y)$ or the conditional expectation can be difficult to compute. Therefore, in practice the LMMSE estimator which has a linear structure and could be achieved more easily [60], is usually applied. The LMMSE decoder takes a linear combination of the received signal $r_i$ and some coefficients $w_i$ as follows

$$ z = \hat{\mathbf{w}}^T \mathbf{r}, $$

(2.32)

which the latter coefficients should be determined, and the hidden information is extracted using sign of the test statistic. The weight vector $\mathbf{w}$ is obtained by minimizing the MSE as

$$ \hat{\mathbf{w}} = \arg\min_{\mathbf{w}} E\{ \| A\mathbf{b} - \mathbf{w}^T \mathbf{r} \|^2 \}. $$

(2.33)

It could be shown that the result of this minimization leads the LMMSE decoder to the following conventional [60] form

$$ \hat{\mathbf{w}} = \mathbf{R}_r^{-1} \mathbf{s}, $$

(2.34)

where the autocorrelation matrix $\mathbf{R}_r$ defined as $\mathbf{R}_r = E\{ \mathbf{r}\mathbf{r}^T \}$, can be estimated at the receiver side. Therefore, from the former expression, we can see that only the signature code is required at the receiver side. Although the LMMSE decoder has the same structure for information embedding in the DCT and magnitude of the DFT, its performance varies in these host domains. As explained earlier for LOD in the magnitude of the DFT domain, all the coefficients do not convey the information. On the other hand, the autocorrelation matrix is estimated using all the coefficients of the received signal and thus it causes degradation in the decoding performance.
To obtain a closed form expression of the error probability for the LMMSE decoder when SS scheme is exploited for information hiding in the DCT domain, by assuming that the test statistic $z$ in (2.32) follows a Gaussian distribution, we can show that the probability of error would be in the form of (2.13) when

$$m_z = A s^T R_r^{-1} s, \quad \sigma_z^2 = s^T R_r^{-1} R_x R_r^{-1} s,$$  \hspace{1cm} (2.35)

where $R_r = A^2 s s^T + R_x$. In a similar way, the theoretical error probability of LMMSE decoder for ISS embedding in the DCT domain, using (2.13), is obtained as

$$m_z = A s^T R_r^{-1} s, \quad \sigma_z^2 = s^T R_r^{-1} (I_N - \lambda s s^T) R_x (I_N - \lambda s s^T) R_r^{-1} s,$$  \hspace{1cm} (2.36)

where $R_r = A^2 s s^T + (I_N - \lambda s s^T) R_x (I_N - \lambda s s^T)$. 

As it was discussed before, by minimizing the error probability parameter $\lambda$ is achieved. By applying the minimization, the parameter $\lambda$ is obtained as

$$\lambda = \frac{(s^T R_x s + DN^2) - \sqrt{(s^T R_x s + DN^2)^2 - 4DN^2 s^T R_x s}}{2Ns^T R_x s}. \hspace{1cm} (2.37)$$

It should be pointed out that, as opposed to other decoders, the LMMSE leads to a closed form expression for $\lambda$.

## 2.7 Experimental Results

In this section, simulations on real images are conducted to illustrate the performance of the proposed watermark decoders for decoding hidden message. A set of 100 testing images with size $512 \times 512$ are employed for information embedding. Testing images include images collected by the UBC’s Digital Multimedia Lab and some standard images such as “Boat”, “Lena”, “Peppers”, “Barbara” and other ones. These standard images are commonly used for testing different aspects of watermarking schemes and are widely used in watermarking papers for evaluating watermarking schemes [132, 153, 154, 157].

For information embedding in the DCT domain, for each $8 \times 8$ block of the image, the DCT coefficients are calculated and all coefficients except the $dc$ one are used as the host signal to convey the hidden information, therefore, 63 coefficients are used for conveying of one bit of information. For information hiding in the DFT domain, since the coefficients should remain conjugate symmetric, 31 coefficients are employed. For the DCT-domain data hiding, shape parameter is set to $c = 0.8$. Since each block with size $8 \times 8$ is used for hiding one bit, the total number of embedded bits is $512^2/8^2 = 4096$ in each test image.
We first verify the theoretical error probabilities when employing the ML decoders proposed in Section 2.5 for both traditional SS and ISS embedding. For data hiding in the DCT domain, both the simulation results and the theoretical results are shown in Figure 2.1 where the bit error rate (BER) is plotted as a function of the Document to Watermark Ratio (DWR) defined in the form of 
\[ \text{DWR} = 10 \log \left( \frac{\sigma^2_x}{\sigma^2} \right) \]
It should be mentioned that the average of the BER for test images has been calculated as the final result. From Figure 2.1 it is clear that the theoretical analysis and the simulated BER result match closely with each other, and this verifies the theoretical analysis of the error probability. Also, comparing the performances of SS and ISS, as expected, we note that ISS clearly outperforms the traditional SS.

Similar to the DCT-domain results, we also investigate the performances of ML decoders when the magnitude of the DFT-domain is exploited for information hiding. The average BER performance based on testing images and the theoretical performance derived in Section 2.5 are shown in Figure 2.2. The consistency between the simulated and theoretical results proves the correctness of the provided error analysis in Section 2.5. From Figures 2.1 and 2.2 we note that, at low DWR, the theoretical results of the DCT domain data hiding are more accurate than that of the DFT magnitude domain. The reason is most likely due to the assumed Gaussian distribution of the test statistic, which is more true when more random variables are added together. Since the total number of available coefficients for information hiding in the DFT magnitude domain is only half of that of the DCT domain and, as explained in Section 2.5 and more DFT coefficients do not convey information when the DWR decreases, the Gaussian assumption imposed on the test statistic in (2.22) and (2.23) for the DCT domain embedding is more accurate than their counterparts in the DFT magnitude domain. From Figures 2.1 and 2.2 we also note that data hiding in the magnitude DFT domain yields better decoding performances than that of the DCT domain. This observation could be explained by the special structure of the test statistic which is error free when \( r_i + s_i A < 0 \) or \( r_i - s_i A < 0 \) and thus leads to better decoding performances.

To gain more insight into the optimal and suboptimal decoders derived in Sections 2.5 and 2.6 the decoding performances of the ML, LOD, and LMMSE decoders are compared in Figure 2.3 where the DCT-domain SS and ISS embedding schemes are studied. It is noted from this figure that the ML decoder outperforms the suboptimal ones. The ML decoder uses the watermark amplitude information to make the decision, while the LOD and LMMSE decoders do not require this information and provide close, slightly worse performance to that of ML. The other point observed is that the LMMSE decoder yields slightly better decoding performance than the LOD one, which could be intuitively justified by the structure of LOD. In deriving LOD, it is assumed that the watermark amplitude is small, and the LOD shows close decoding performance to that of ML as long as this assumption is satisfied. As it is seen from Figure 2.3
2.7. Experimental Results

the performance gap between the ML and the LOD gets bigger as the DWR decreases. This is because, by decreasing the DWR, the watermark amplitude gets larger and the LOD derived by truncating the second and higher orders of Taylor’s series results in a coarser approximation of the ML decoder. The LMMSE does not impose any constraint on the watermark amplitude, and this might be one reason that LMMSE is slightly better than LOD. In addition, the LMMSE decoder does not need to estimate parameters of the host signal and this simplicity makes it attractive for decoding. Therefore, we suggest that the LMMSE decoder is generally a good choice for extracting the information hidden in the DCT domain, in the sense that it needs less information than the ML decoder yet yields close decoding performance.

To verify the derived theoretical decoding performance analysis in Section 2.6, the BER curves of the LOD and LMMSE decoders in the DCT domain are shown in Figure 2.4. We observe close matches between the theoretical BER performances and the performances calculated based on the experimental results.

To compare the performances of the suboptimal decoders for the DFT magnitude domain embedding, Figure 2.5 is reported. From Figure 2.5, we note that, for the SS embedding, the LOD decoder does not provide comparable BER performances when compared with other decoders. As discussed in Section 2.6, though not all DFT coefficients convey hidden information, the LOD and LMMSE decoders use all the received coefficients for decoding and thus have degraded decoding performances from that of ML. More specifically, at lower DWR, since less DFT coefficients can be used for conveying the information bit, the decoding performance gap is larger, as observed in Figure 2.5. It is observed from the Figure 2.5 that the slope of decoding performance of LOD becomes smaller as the DWR decreases, and the same behavior is observed for the LMMSE decoder in Figure 2.5. From the Figure 2.5, we note that overall the LMMSE decoder outperforms other suboptimal decoders.

To examine the performances of the proposed decoders in the presence of additional distortions/attacks, we consider a scenario where an additive Gaussian noise is added into the watermarked images, and the decoders’ performances are shown in Figures 2.6 and 2.7 for the DCT and the DFT magnitude domain embedding, respectively. In these figures, the Watermark to Noise Ratio (WNR) changes, where $WNR = 10 \log \left( \frac{D}{\sigma_n^2} \right)$ and $\sigma_n^2$ denotes the noise variance. From Figure 2.6, we note that the ISS scheme has better performance than SS, and that all suboptimal decoders yield close decoding performances to each other. One observation in Figure 2.7 is that the LMMSE decoder outperforms ML. Even though in the absence of any additional attack, ML in the DFT magnitude domain provides the best decoding performance, its performance in the presence of additional noise degrades significantly. This could be explained by the sensitivity of the ML decoder to the watermark amplitude. In the presence of additional noise, the received coefficients can be changed, and thus are wrongly exploited for decoding and
2.7. Experimental Results

Figure 2.1: The average bit error rates versus DWR for the ML decoders, where 4,096 bits of information are embedded in the DCT domain of each of the testing images employing the SS and ISS embedding schemes. The theoretical performances are also depicted.

Figure 2.2: The average bit error rate versus DWR for the ML decoders, where 4,096 bits of information are embedded in the DFT magnitude domain of each of the testing images employing the modified SS and ISS embedding schemes. The theoretical performances are also depicted.

consequently degrade the performance of the ML decoder. On the other hand, the LMMSE decoder does not depend on the watermark amplitude and can yield better performances than ML under additional noise.

In summary, some useful observations can be concluded from the experimental results: with the watermark amplitude information available at the receiver side, the DFT magnitude domain data hiding could result in better performances when the ML decoder is employed; With no access to the watermark amplitude information, the information embedding in the DCT domain data hiding is preferred, and the LMMSE decoder is preferred; When considering additional noise, data hiding in the DCT domain with ISS is preferred than the DFT magnitude domain ISS embedding. However, for SS embedding, the LMMSE decoder in the magnitude of the DFT domain provides fairly comparable performances to that of LMMSE in the DCT domain.
2.7. Experimental Results

Figure 2.3: The average bit error rates versus DWR for the ML, LOD, and LMMSE decoders, where 4,096 bits of information are embedded in the DCT domain of each testing image employing the SS and ISS embedding schemes.

Figure 2.4: The empirical and theoretical average bit error rate versus DWR for the LMMSE and LOD decoders, where 4,096 bits of information are embedded in the DCT domain of each testing image employing the SS and ISS embedding schemes.

Figure 2.5: The average bit error rate versus DWR for the ML, LOD, and LMMSE decoders, where 4,096 bits of information are embedded in the magnitude of the DFT domain of each testing image. The modified SS and ISS embedding schemes are employed.

Figure 2.6: The average bit error rate versus WNR for the ML, LOD, and LMMSE decoders, where 4,096 bits of information are embedded in the DCT domain of each testing image. The SS and ISS embedding schemes are employed.
2.8 Conclusion

In this chapter, the optimal and suboptimal decoders for additive spread spectrum data hiding were investigated. Overall, we presented decoding analysis framework of additive SS and ISS data hiding when the information bit is embedded into the DCT and the magnitude of the DFT domains. Generalized Gaussian distribution and Weibull distribution were used for deriving the maximum likelihood decoders in the different domains. To improve the accuracy of the extracted hidden message, we employed improved spread spectrum embedding and presented the optimal ML decoders. The theoretical error analyses of SS and ISS embedding in the DCT domain and in the magnitude of the DFT domain were derived. Experimental results showed that, when the watermark amplitude is available at the decoder side, data hiding in the magnitude of the DFT domain could yield better decoding performances than that of the DCT domain.

Though theoretically the ML decoder achieves the decoding performance upper bound, it requires additional prior information such as the watermark amplitude. To relax the requirements on such prior information, the LOD and LMMSE decoders were derived for practical data hiding applications in the DCT domain. The LOD decoder is independent of the watermark amplitude, though it still requires the host signal parameters. The LMMSE decoder provides a linear decoder in terms of the received signal which is independent of the watermark amplitude. The LOD and LMMSE decoders yield performances close to that of the ML decoder, with the LMMSE being slightly better than the LOD, especially at lower DWR. For the proposed suboptimal decoders, we also provided the theoretical analysis of the bit error rate decoding performances. The suboptimal LOD was also proposed in the DFT magnitude domain. However
2.8. Conclusion

LOD does not provide close performances to that of the ML decoder, probably because that LOD uses all the received coefficients for decoding. The LMMSE decoder in the DFT magnitude domain shows better performance than that of the LOD decoder.

The experimental results suggest that, with no access to the watermark amplitude information at the decoder side, the suboptimal decoders in the DCT domain are more reliable than their counterparts in the DFT magnitude domain. Among the proposed suboptimal decoders, overall the LMMSE decoders are preferred. As expected, the ISS embedding scheme outperforms SS in both the DCT and the DFT magnitude domains, and thus is preferred. Experiments in the presence of additional noise showed that ISS embedding in the DCT domain is preferred. The LMMSE decoder is preferred in the presence of additional noise than the ML one for data hiding in the magnitude of DFT domain.
Chapter 3

Correlation-and-Bit-Aware Spread Spectrum

3.1 Introduction

In Chapter 2, it was shown that the ISS has better decoding performance than the conventional SS scheme. In this chapter, our main purpose is to propose an improved embedding scheme based on SS which could efficiently decrease the interference effect of the host signal. Inspired by the success of ISS, we propose a correlation-and-bit-aware concept for data hiding by exploring the correlation between the host signal and the signature code as well as the information bit to be embedded into the host signal as the side information at the encoder. The proposed approach is referred as correlation-aware data hiding approach. By incorporating the correlation-and-bit-aware concept with the SS scheme, a new correlation-aware SS (CASS) data hiding scheme is proposed. Our theoretical analysis shows that CASS is superior to the SS counterpart in terms of watermark decoding performance. To further improve the decoding performance of ISS, a correlation-aware improved spread spectrum (CAISS) data hiding scheme is proposed which is a combination of the SS, ISS, and the correlation-and-bit-aware concept. Having introduced the CAISS scheme, we will show theoretically that it outperforms the ISS scheme by yielding higher decoding performance. In addition, we will prove that the proposed CASS scheme is more robust against the interference effect than the traditional SS. Similarly, better robustness of the proposed CAISS over the ISS will be shown. Moreover, it will be shown that employing the proposed CASS and CAISS schemes could increase the payload.

Further assuming additional Gaussian noise is added to the received signal, we derive the corresponding test statistic distribution at the decoder side. Based on the derived distributions, the error probability of the CASS and CAISS schemes in the presence of noise will be presented. The simulation results verify the integrity of the derived theoretical decoding performances and support the claim that the proposed correlation-aware schemes can provide better decoding performances in the presence or absence of additional noise. It is worth emphasizing that, comparing with the traditional blind SS scheme, the proposed correlation-aware data hiding approaches do not require additional information at the decoder side and do not change the
3.2 Conventional Correlator as Decoder

In Chapter 2, the SS and ISS embedding schemes were introduced. Since the correlation-aware concept is a data hiding scheme that is applicable for any context (image, video, and audio), we generally assume that the host signal follows Gaussian independent and identical distribution (IID) with zero mean and variance $\sigma^2_x$, i.e., $x \sim \mathcal{N}(0_N, \sigma^2_x I_N)$, where $I_N$ and $0_N$ are the $N \times N$ identity matrix and zero vector with dimension $N$, respectively.

Since the host coefficients are assumed to be Gaussian IID’s, the optimal decoder is the correlation between the received data and the signature code. The correlator estimates the hidden information bit as

$$\hat{b} = \text{sign}\{z\},$$

where

$$z = r^T s.$$ (3.2)

$r$ and $s$ are the received signal and signature code, respectively. $\text{sign}\{\cdot\}$ function returns $+1$ and $-1$ when its argument is positive and negative, respectively.

Given $b = +1$ and $b = -1$, the PDFs of the sufficient statistic $z = r^T s$ could be determined as follow

$$f_Z(z|b = +1) = \mathcal{N}(NA, N\sigma^2_x),$$ (3.3)

$$f_Z(z|b = -1) = \mathcal{N}(-NA, N\sigma^2_x).$$ (3.4)

From the above PDFs, it is clear that the SS embedding scheme is not error free even in the absence of any additional noise. The explanation of this phenomenon is that the host signal is actually treated as noise in SS embedding. Since the host signal power is generally much higher than the embedding signal (watermark) power due to the imperceptibility requirement of data
hiding, this noise effect of the host signal results in a degradation in the decoding performance of SS.

To reduce the interference effect of the host signal, Malvar and Florencio proposed the improved spread spectrum embedding [92] by modulating the energy of the inserted signal. It should be mentioned that by assuming the Gaussian distribution of the host signal, the optimal ML decoder is in the form of (3.1) where the test statistic is as (3.2).

### 3.3 Correlation-Aware SS Data Hiding Approach

As introduced in Section 3.2 in SS embedding, the host signal is the source of uncertainty at the decoder side. The fundamental reason is that, as implied in Eqns. (3.1) and (3.3), the PDF leakage causes the decoding error. The leakage means that the test statistic given in Eqn. (3.2) could get negative and positive values when we send the bit \( b \) of +1 and -1, respectively. This phenomenon has been demonstrated clearly in Figure 3.1. To reduce this interference effect of the host signal, the correlation-and-bit-aware concept is introduced in this section. The SS-based correlation-and-bit-aware concept is motivated by the prior knowledge that we know the decoder structure is the correlation between the received signal and the signature code. Such correlation is a summation of the correlation between the host signal and the signature code and the correlation between the signature code and the modulated hidden information.

As the encoder side, since we know the correlation between the host signal and the signature code and the bit message \( b \) to be embedded in advance, we could exploit such side information in a smart way to reduce the original PDF leakage in SS. By exploring the correlation-and-bit-aware concept in SS embedding, we therefore propose an embedding scheme, referred as correlation-aware spread spectrum (CASS), as follows

\[
\mathbf{r} = \begin{cases} 
\mathbf{x} + sA_1 & \text{if } \mathbf{s}^T\mathbf{x} \geq 0, \quad b = +1, \\
\mathbf{x} - sA_2 & \text{if } \mathbf{s}^T\mathbf{x} \geq 0, \quad b = -1, \\
\mathbf{x} - sA_1 & \text{if } \mathbf{s}^T\mathbf{x} < 0, \quad b = -1, \\
\mathbf{x} + sA_2 & \text{if } \mathbf{s}^T\mathbf{x} < 0, \quad b = +1,
\end{cases}
\]

(3.5)

where \( A_1 \) and \( A_2 \) (\( 0 < A_1 < A_2 \)) are two amplitude levels determined with respect to the allowed distortion.

The intuitive idea behind the CASS embedding scheme is to modulate the bit message of information by two amplitude levels based on the correlation between the host signal and the signature code as well as the bit message to be embedded. More specifically, suppose that the message bit +1 needs to be embedded: if the correlation between the host signal and the signature code is positive then the smaller amplitude \( A_1 \) should be used for modulation; if
the correlation is negative then the larger amplitude $A_2$ should be employed. Suppose the bit message -1 is to be embedded: if the correlation of the host signal and the signature code is negative then the smaller amplitude is used, and if the correlation is positive then the larger amplitude is used. The underlying advantage of the proposed CASS embedding is cleared when the sufficient statistic of the decoder is investigated shortly.

We can prove that, with the assumption that the host signal follows Gaussian IID, the optimal decoder for the CASS embedding scheme (3.5) is the correlator as defined in Eqn. (3.1) with the test statistic $z$ defined in Eqn. (3.2). The detailed proof is omitted here since CASS can be treated as a particular case of CAISS with $\lambda_h = 0$, while we will describe CAISS and provide the proof of CAISS in Section 3.4.

With the optimal decoder in Eqn. (3.1), the sufficient statistic $z$ in Eqn. (3.2) using CASS embedding in (3.5) can be expressed by the following form

$$ z = \begin{cases} 
  s^T x + NA_1 & \text{if } s^T x \geq 0, \ b = +1, \\
  s^T x - NA_2 & \text{if } s^T x \geq 0, \ b = -1, \\
  s^T x - NA_1 & \text{if } s^T x < 0, \ b = -1, \\
  s^T x + NA_2 & \text{if } s^T x < 0, \ b = +1.
\end{cases} \quad (3.6) $$

Since the host signal is assumed to follow Gaussian distribution, given the bit message $b$ and the sign of the correlation between the host signal and the signature code, the sufficient statistic $z$ consists of four conditional half-Gaussian PDFs as follows

$$ f_Z(z|s^T x \geq 0, b = +1) = 2N(NA_1, N\sigma_x^2)u(z - NA_1), \quad (3.7) $$

$$ f_Z(z|s^T x < 0, b = +1) = 2N(-NA_2, N\sigma_x^2)u(-z - NA_2)), \quad (3.8) $$

$$ f_Z(z|s^T x \geq 0, b = -1) = 2N(-NA_2, N\sigma_x^2)u(z + NA_2), \quad (3.9) $$

$$ f_Z(z|s^T x < 0, b = -1) = 2N(-NA_1, N\sigma_x^2)u(-z + NA_1)), \quad (3.10) $$

where $u(.)$ defines the step function.

The above PDFs of the sufficient statistic $z$ provide us more insight into the underlying advantages of the proposed CASS embedding scheme and the superiority of CASS over SS. The PDFs in Eqn. (3.7)-(3.10) of the sufficient statistic are shown in Figure 3.2. It depicts how CASS embedding could reduce the host-interference effect. It is seen that when the message bit is +1 and the correlation between the host signal and the signature code is positive, there is
3.3. Correlation-Aware SS Data Hiding Approach

no PDF leakage. Similarly, when the bit message is -1 and the correlation is negative, there is no PDF leakage. For the cases that the bit message is +1 and the correlation is negative and that the bit message is -1 and the correlation is positive, there might still be some PDF leakage. Therefore, from comparing Figures 3.1 and 3.2 it is justified intuitively that the PDF leakage for the CASS scheme is less than the conventional SS where the message bit is modulated by a single amplitude level regardless of the correlation between the host signal and the signature code.

Having intuitively explained the underlying advantage of CASS data hiding, we now proceed to analyze the decoding performance of CASS by deriving the bit error rate (BER). The probability of error of CASS data hiding is defined as

\[
P_e = \Pr \{ \hat{b} \neq b \} = \frac{1}{4} \times \Pr \{ \hat{b} = +1 | b = -1, s^T x > 0 \} + \frac{1}{4} \times \Pr \{ \hat{b} = +1 | b = -1, s^T x < 0 \} + \frac{1}{4} \times \Pr \{ \hat{b} = -1 | b = +1, s^T x < 0 \} + \frac{1}{4} \times \Pr \{ \hat{b} = -1 | b = +1, s^T x > 0 \},
\]

(3.11)

where \( \hat{b} \) is the decoded bit. As discussed earlier, the second and the fourth terms are zero since there are no PDF leakages. Therefore, the error probability is simplified to the following expression

\[
P_{e-CASS} = Q \left( \frac{N A_2}{\sqrt{N \sigma_x^2}} \right),
\]

(3.12)

where \( Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty \exp(-u^2/2) \, du \). To fairly compare different data hiding algorithms, the same distortion \( D \) due to embedding, should be assumed. The distortion defined in (2.2) due to CASS embedding in (3.5) can be expressed as

\[
D = (A_1^2 + A_2^2)/2.
\]

(3.13)

Thus, using (3.12) and (3.13), the error probability of CASS in terms of the distortion \( D \) is expressed as

\[
P_{e-CASS} = Q \left( \frac{N \sqrt{2D - A_1^2}}{\sqrt{N \sigma_x^2}} \right).
\]

(3.14)

It is noteworthy that, since \( 0 < A_1 < A_2 \), according to the distortion expression in (3.13), the amplitudes \( A_1 \) and \( A_2 \) always satisfy the following inequalities

\[
0 < A_1 < \sqrt{D} < A_2 < \sqrt{2D}.
\]

(3.15)

To compare the error probability of CASS with that of SS, we need to provide the error proba-
3.3. Correlation-Aware SS Data Hiding Approach

bility of SS scheme in terms of $D$. We can show that

$$P_{e-SS} = Q \left( \frac{N\sqrt{D}}{\sqrt{N\sigma^2_x}} \right),$$  \hspace{1cm} (3.16)

The superiority of the proposed CASS over SS is presented as a proposition as follows.

**Proposition 1:** With the assumption that the host signal follows Gaussian IID, the proposed CASS scheme in (3.5) yields smaller error probability (3.14) than the traditional SS in (3.16).

**Proof:** The proof details are given in the Appendix B.1. The superiority of the CASS over SS scheme in the sense of decoding has been proved so far. In the rest of this section, we aim at quantitatively investigating the improvement of CASS in terms of error probability, robustness, and payload. We attempt to answer the question of how much improvement is obtained by employing the CASS scheme.

We define the Error Probability Improvement Factor (EPIF) as follows

$$EPIF_{1-2} \triangleq \frac{P_1}{P_2},$$  \hspace{1cm} (3.17)

where $P_1$ and $P_2$ are two probability of error functions to be compared. EPIF represents the improvement ratio and a smaller value implies a better improvement. In data hiding, it is more appropriate to express EPIF as a function of the document to watermark ratio (DWR) defined in the following form

$$DWR \triangleq 10 \log \left( \frac{\sigma^2}{D} \right),$$  \hspace{1cm} (3.18)

When comparing the error probabilities of CASS (3.14) and SS (3.16), we have the EPIF as

$$EPIF_{CASS-SS} = Q \left( \frac{\frac{N\sqrt{2D-A_1^2}}{\sqrt{N\sigma^2_x}}}{\sqrt{N\sigma^2_x}} \right) / Q \left( \frac{N\sqrt{D}}{\sqrt{N\sigma^2_x}} \right).$$  \hspace{1cm} (3.19)

Since $0 < A_1 < \sqrt{D}$, it could be shown that the EPIF$_{CASS-SS}$ is bounded as follows

$$\frac{Q(10^{-DWR/20}\sqrt{2N})}{Q(10^{-DWR/20}\sqrt{N})} < EPIF_{CASS-SS} < 1.$$  \hspace{1cm} (3.20)

The lower bound represents the best achievable improvement given the DWR and the number of host coefficients.

We proposed using of EPIF as a measure to investigate the error probability improvement of the CASS over SS under a fixed distortion. As discussed earlier, the host signal is an interference source for decoding. It is important to measure the robustness of the embedding schemes against interference. We now proceed to investigate how much more host-interference
3.3. Correlation-Aware SS Data Hiding Approach

CASS could tolerate comparing with the SS scheme, given a fixed error probability and distortion due to embedding. It should be clarified that the robustness discussed here is referred to the interference effect of the host signal and not to other additional noise. To quantify the robustness, assuming equal error probability and equal distortion due to embedding, we define the Interference Robustness Improvement Factor (IRIF) as

$$\text{IRIF}_{2-1} = \frac{\sigma_1^2}{\sigma_2^2},$$

(3.21)

where $\sigma_1^2$ and $\sigma_2^2$ represent the corresponding host signal powers of two embedding schemes to be compared. Let us denote $\sigma_{x-CASS}^2$ and $\sigma_{x-SS}^2$ the host signal powers in CASS and SS, respectively, when the error probability and the distortion are assumed to be the same in two embedding schemes. With equal error probability and equal distortion due to embedding, referring to the error probabilities in (3.14) and (3.16), we have

$$\frac{2D - A_1^2}{\sigma_{x-CASS}^2} = \frac{D}{\sigma_{x-SS}^2}. \tag{3.22}$$

According to the IRIF definition in (3.21), we have

$$\text{IRIF}_{CASS-SS} = \frac{1}{2 - \alpha}, \tag{3.23}$$

where

$$A_1^2 = \alpha D, \quad 0 < \alpha < 1. \tag{3.24}$$

It is straightforward to show that since $0 < \alpha < 1$ the $\text{IRIF}_{CASS-SS}$ is bounded as

$$\frac{1}{2} < \text{IRIF}_{CASS-SS} < 1. \tag{3.25}$$

The IRIF robustness in (3.25) reveals that CASS is more robust to the host interference than SS, and CASS can tolerate the interference power up to twice of the conventional SS scheme.

Another advantage of the CASS scheme is its increased payload. Given the same error probability and distortion due to embedding, more information bits could be embedded into the host signal in the CASS scheme than SS. We define the Payload Improvement Factor (PIF) as a payload measure in the following

$$\text{PIF}_{2-1} = \frac{N_1}{N_2}, \tag{3.26}$$

where $N_1$ and $N_2$ are the numbers of host coefficients used for conveying one bit of information where the error probability and the distortion are assumed to be same in the embedding schemes.
3.4 Correlation-Aware Improved SS Data Hiding Approach

Referring to the PIF definition and the error probabilities in (3.14) and (3.16), we have the following expression

\[ N_{\text{CASS}}(2D - A_1^2) = N_{\text{SS}}D, \]  

where \( N_{\text{CASS}} \) and \( N_{\text{SS}} \) are the required numbers of host coefficients for the CASS and SS schemes. This expression results in the following PIF using (3.24)

\[ \text{PIF}_{\text{CASS-SS}} = 2 - \alpha. \]  

We can see that the obtained PIF is always greater than one, meaning that the CASS scheme could increase the payload of data hiding in comparison with SS.

3.4 Correlation-Aware Improved SS Data Hiding Approach

In this section, we proceed to exploit the correlation-and-bit-aware concept for designing an improved embedding scheme based on ISS. As mentioned earlier, the ISS embedding scheme [92] was introduced to improve the decoding performance of the traditional SS. We plan to incorporate the ISS with the correlation-and-bit-aware idea to further improve the decoding performance of ISS.

By taking a look at Figure 3.2, we can see that the main source of decoding error is the PDF leakage from two cases: one is that \( b = +1 \) and \( s^T x \) is negative, and the other is that \( b = -1 \) and \( s^T x \) is positive. Intuitively, squeezing the two PDFs involving the leakage (e.g., as in ISS) could improve the decoding performance. Therefore, the basic idea of the CAISS scheme is to combine CASS and ISS: for the cases that there is no PDF leakage (i.e., when \( b = +1 \) and \( s^T x \) is positive, and when \( b = -1 \) and \( s^T x \) is negative), employ the CASS scheme because there is no interference effect at the decoding side; for the left two cases that there is leakage, the ISS embedding is employed since ISS can modulate the embedding energy to compensate for the host signal interference. We describe the proposed CAISS embedding scheme as follows

\[ r = \begin{cases} 
  x + sA_1 & \text{if } s^T x \geq 0, \quad b = +1, \\
  x - sA_2 - \lambda_h s(s^T x) & \text{if } s^T x \geq 0, \quad b = -1, \\
  x - sA_1 & \text{if } s^T x < 0, \quad b = -1, \\
  x + sA_2 - \lambda_h s(s^T x) & \text{if } s^T x < 0, \quad b = +1, 
\end{cases} \]  

where \( \lambda_h \) is a parameter determined by the allowed distortion. We will later show that the following bound on \( \lambda_h \) holds

\[ 0 \leq \lambda_h \leq \frac{1}{N}. \]
3.4. Correlation-Aware Improved SS Data Hiding Approach

Before we can show why the CAISS scheme can yield better decoding performance than that of both CASS and ISS, we need first to obtain the optimal decoder.

With the assumption of Gaussian IID host signal samples, the optimal decoder for the CAISS scheme (3.29) which minimizes the error probability is the correlator defined in Eqn. (3.1) with the test statistic \( z \) in Eqn. (3.2). The proof details are given in the Appendix B.2.

By comparing the embedding schemes in (3.5) and (3.29), it is clear that CASS is a particular case of CAISS with \( \lambda_h = 0 \). Therefore, we can similarly show that the same correlator decoder is optimal for CASS, and the performance analysis of the CASS scheme presented in Section 3.3 can be considered a special case of CAISS.

We have shown that the correlator is the optimal decoder for the CAISS scheme. One important issue is to determine an appropriate value of the parameter \( \lambda_h \) in CAISS. We propose determining \( \lambda_h \) by minimizing the error probability. For CAISS in (3.29), the test statistic \( z \) in (3.2) can be expressed as

\[
z = \begin{cases} 
  s^T x + NA_1 & \text{if } s^T x \geq 0, \quad b = +1, \\
  s^T x(1 - \lambda_h N) - NA_2 & \text{if } s^T x \geq 0, \quad b = -1, \\
  s^T x - NA_1 & \text{if } s^T x < 0, \quad b = -1, \\
  s^T x(1 - \lambda_h N) + NA_2 & \text{if } s^T x < 0, \quad b = +1,
\end{cases}
\]  

(3.31)

Given \( b \) and the correlation between signature code and the host signal, the conditional PDFs of the test statistic \( z \) are in the following form

\[
f_Z(z|s^T x \geq 0, b = +1) = 2N(NA_1, N\sigma_x^2)u(z - NA_1),
\]  

(3.32)

\[
f_Z(z|s^T x < 0, b = +1) = 2N(-NA_2, N\sigma_x^2(1 - \lambda_h N)^2)u(-z - NA_2),
\]  

(3.33)

\[
f_Z(z|s^T x \geq 0, b = -1) = 2N(-NA_2, N\sigma_x^2(1 - \lambda_h N)^2)u(z + NA_2),
\]  

(3.34)

\[
f_Z(z|s^T x < 0, b = -1) = 2N(-NA_1, N\sigma_x^2)u(-z + NA_1)).
\]  

(3.35)

Now we proceed to derive the theoretical BER performance of the proposed CAISS data hiding scheme. The distortion (2.2) due to CAISS embedding (3.29) is expressed as

\[
D = \frac{1}{2}(A_1^2 + A_2^2 + \lambda_h^2 N\sigma_x^2).
\]  

(3.36)

Referring to the distributions of the statistics given in (3.32)-(3.35), the distortion in (3.36), and
3.4. Correlation-Aware Improved SS Data Hiding Approach

the bit error probability defined in (3.11), we can show that the bit error rate of the CAISS scheme is obtained as

$$P_{e-CAISS} = Q\left(\frac{N\sqrt{2D - A^2 - \lambda_h^2 N \sigma_x^2}}{\sqrt{(1 - \lambda_h N)^2 N \sigma_x^2}}\right).$$  (3.37)

We now can determine the optimal value of the parameter $\lambda_h$ by minimizing the above error probability. Since the $Q$ function is monotonically decreasing, it is equivalent to maximizing its argument. Taking the derivative of the argument and letting it to be zero and some simplifications lead us to

$$\lambda_h = \begin{cases} \frac{1}{N} & \text{if } D > \frac{\sigma_x^2 + A^2 N}{2N}, \\ \frac{2D - A^2}{\sigma_x^2} & \text{if } D \leq \frac{\sigma_x^2 + A^2 N}{2N}. \end{cases}$$  (3.38)

To provide more insight into the parameter $\lambda_h$, we further show that the inequality in (3.30) always holds. From (3.38), it is clear that $\lambda_h$ is a function of the distortion $D$, i.e., $\lambda_h(D)$. To prove the inequality in (3.30), we show that when the distortion approaches zero and infinity, $\lambda_h$ approaches zero and $\frac{1}{N}$, respectively, and that $\lambda_h(D)$ is a monotonically increasing function of the distortion $D$. It is pretty easy to verify that

$$\lim_{D \to 0} \lambda_h = 0, \quad \lim_{D \to \infty} \lambda_h = \frac{1}{N}. \quad (3.39)$$

To show that $\lambda_h(D)$ is a monotonically increasing function of $D$, the derivative of (3.38) with respect to $D$ is taken and we see that $\frac{d\lambda_h}{dD} \geq 0$. Thus, we can conclude that $\lambda_h$ is an increasing function of the distortion. Therefore, together with (3.39), the inequality in (3.30) is verified.

From the monotonically increasing behavior of $\lambda_h(D)$ and the PDFs in (3.33) and (3.34), we can see that increasing the embedding distortion could decrease the variance in the related PDFs and thus improve the decoding performance. To intuitively explain the superior performance of CAISS over CASS, we plot the PDFs of the test statistic $z$ in (3.32)-(3.35) in Figure 3.3. Compared with the PDFs in Figure 3.2, we can see that, similar to CASS, the correlation-and-bit-aware concept could separate two PDFs completely in CAISS, and that the left two PDFs are better separated in CAISS than in CASS due to smaller variances in the related distributions. Therefore, substantial reduction of PDF leakage is observed in CAISS and thus leads to the reduced interference effect of the host signal.

We have shown in Section 3.3 that the proposed CASS is superior to SS. Here similarly, we show that the proposed CAISS outperforms both SS and ISS, with more details provided in the following Proposition.
3.4. Correlation-Aware Improved SS Data Hiding Approach

**Proposition 2:** With the assumption of Gaussian IID host signal samples, the error probability of the CAISS embedding scheme in (3.37) is smaller than that of ISS, i.e., \( P_{e-CAISS} < P_{e-ISS} \).

**Proof:** The proof details are given in the Appendix B.3. It should be noted that since SS is a particular case of ISS and has worse performance than that of ISS, the above proposition implies that the error probability of CAISS is smaller than that of SS.

So far, we have proved that the proposed CAISS data hiding scheme provides better decoding performance than that of the SS and ISS schemes. We now proceed to quantify the performance improvement of CAISS over SS and ISS in terms of error probability, robustness, and payload. We first examine the EPIF measure for BER performance improvement of CAISS over SS. According to the error probabilities in (3.37) and (3.16), the EPIF is obtained as

\[
\text{EPIF}_{CAISS-SS} = Q\left(\frac{N\sqrt{2D - A_1^2 - \lambda_h^2 N\sigma_x^2}}{\sqrt{(1 - \lambda_h N)^2 N\sigma_x^2}}\right) / Q\left(\frac{N\sqrt{D}}{N\sigma_x}\right).
\]

(3.40)

Since \( 0 < A_1 < \sqrt{D} \) and \( 0 \leq \lambda_h \leq \frac{1}{N} \), it could be shown that the above EPIF is bounded as

\[
0 \leq \text{EPIF}_{CAISS-SS} < 1.
\]

(3.41)

By comparing (3.41) with (3.20) for the CASS scheme, a smaller lower-bound is observed for CAISS, implying a further improvement of CAISS over SS. Similarly, referring to the error probabilities in (3.37) and (B.12), the improvement of CAISS over ISS can be described by

\[
\text{EPIF}_{CAISS-ISS} = Q\left(\frac{N\sqrt{2D - A_1^2 - \lambda_h^2 N\sigma_x^2}}{\sqrt{(1 - \lambda_h N)^2 N\sigma_x^2}}\right) / Q\left(\frac{N\sqrt{D - \lambda^2 N\sigma_x^2}}{\sqrt{(1 - \lambda N)^2 N\sigma_x^2}}\right).
\]

(3.42)

We can show that the above EPIF is bounded as

\[
0 \leq \text{EPIF}_{CAISS-ISS} < 1.
\]

(3.43)

We now proceed to investigate the robustness of CAISS against the host signal effect. With a fixed error probability, we have the following proposition, which shows that the CAISS scheme is more robust against the interference effect of the host signal than ISS.

**Proposition 3:** With the assumption that the host signal follows Gaussian IID, the IRIF for the CAISS and ISS schemes is less than one, i.e., \( \text{IRIF}_{CAISS-ISS} < 1 \), where

\[
\text{IRIF}_{CAISS-ISS} = \frac{\sigma_x^2_{-ISS}}{\sigma_x^2_{-CAISS}}.
\]

(3.44)
The parameters $\sigma^2_{x-ISS}$ and $\sigma^2_{x-CAISS}$ are the corresponding variances of the host signal in the ISS and CAISS schemes, with the error probability and the distortion being assumed the same in both embedding schemes. It could be shown that, referring to the error probabilities in (3.37) for CAISS and in (B.12) for ISS, and assuming equal error probability, we further have

$$\text{IRIF}_{\text{CAISS-ISS}} = \frac{D(1 - \lambda hN)^2}{2D(1 - \lambda N)^2 - A_1^2(1 - \lambda N)^2 - \lambda hN\sigma^2(1 - \lambda N)^2 + \lambda^2 N\sigma^2(1 - \lambda hN)^2},$$

(3.45)

where we have used $\sigma^2$ to denote $\sigma^2_{x-CAISS}$ for notation simplicity.

Proof: The proof details are given in the Appendix B.4. Based on above proposition, it is straightforward to show that, with the assumption of IID Gaussian host signal samples, $\text{IRIF}_{\text{CAISS-SS}}$ is less than one where

$$\text{IRIF}_{\text{CAISS-SS}} = \frac{\sigma^2_{x-SS}}{\sigma^2_{x-CAISS}}. \quad (3.46)$$

The parameter $\sigma^2_{x-SS}$ and $\sigma^2_{x-CAISS}$ are the variances of the host signal in the SS and CAISS schemes, respectively, with the error probability and the distortion being assumed the same. Using (3.45) leads us to the following expression

$$\text{IRIF}_{\text{CAISS-SS}} = \frac{D(1 - \lambda hN)^2}{2D - A_1^2 - \lambda hN\sigma^2}, \quad (3.47)$$

where we use $\sigma^2$ to denote $\sigma^2_{x-CAISS}$.

We further prove that the CAISS scheme can increase the payload in data hiding in comparison with both SS and ISS schemes. Referring to the error probabilities in (3.16) and (3.37) and the PIF definition in (3.26), we can show that

$$\text{PIF}_{\text{CAISS-SS}} = \frac{2D - A_1^2 - \lambda hN\sigma^2}{D(1 - \lambda hN)^2},$$

(3.48)

where for notation simplicity we use $N$ to denote $N_{\text{CAISS}}$. Since the PIF in (3.48) is the inverse of the IRIF for the CAISS and SS scheme, it is larger than one, meaning that the CAISS scheme increases the payload in data hiding.

The proof of the superiority of the CAISS scheme over ISS in terms of payload is not as easy as the case of SS. We provide the following proposition, with the proof details given in the Appendix B.5.

Proposition 4: With the assumption of Gaussian IID host signal samples, for a given error probability and embedding distortion, the PIF for the CAISS and the ISS schemes is larger than
one, i.e., \( \text{PIF}_{\text{CAISS-ISS}} > 1 \), where by using (3.24) we have

\[
\text{PIF}_{\text{CAISS-ISS}} = 2 - \alpha. \tag{3.49}
\]

In summary, we have shown that the proposed correlation-and-bit-aware concept could improve the performance of the conventional SS and ISS schemes from several aspects: given a fixed embedding distortion, CASS and CAISS yield better decoding performances; for a fixed error probability, CASS and CAISS are more robust against the interference effect of the host signal; and they can increase the payload of data hiding.

### 3.5 CASS and CAISS in the Presence of Additional Noise

In Sections 3.3 and 3.4, the concept of correlation-and-bit-aware data hiding was introduced and two versions of correlation-aware embedding schemes, called the CASS and CAISS schemes, were presented. We so far have proved the superiority of CASS and CAISS over the SS and ISS schemes in the absence of additional noise. In practice, the received watermarked-signal might be contaminated with additional noise and thus its effects on the proposed correlation-aware data hiding schemes should be investigated. Therefore, in this section, we first show that the optimal decoder for both CASS and CAISS in the presence of additional Gaussian noise is still in the form of the correlator defined in (3.1) and (3.2). Then, the decoding performances of the proposed CASS and CAISS schemes in the presence of additional Gaussian noise are analyzed.

Since CASS can be considered as a particular case of CAISS with \( \lambda_b = 0 \), we only need to prove the optimality of the correlator decoder for CAISS. The optimality of the correlator for CASS could be simply shown by assuming \( \lambda_b = 0 \) in CAISS.

With additional Gaussian noise, the received noisy signal in the CAISS scheme could be described as

\[
r = \begin{cases} 
  x + sA_1 + n & \text{if } s^T x \geq 0, \ b = +1, \\
  x - sA_2 - \lambda_b s(s^T x) + n & \text{if } s^T x \geq 0, \ b = -1, \\
  x + sA_1 + n & \text{if } s^T x < 0, \ b = -1, \\
  x + sA_2 - \lambda_b s(s^T x) + n & \text{if } s^T x < 0, \ b = +1,
\end{cases} \tag{3.50}
\]

where \( n = [n_1, n_2, \ldots, n_N]^T \) includes the IID Gaussian noise samples with zero-mean and variance of \( \sigma_n^2 \). In Appendix B.6 has been shown that the optimal decoder is in the form of (3.1) where the test statistic is as (3.2).

Having obtained the correlator as the optimal decoder, we proceed to analyze the error probability of the CAISS and CASS schemes in the presence of the noise. The probability of
error for the CAISS scheme is first derived, and the corresponding error probability for the CASS embedding scheme can be obtained by substituting \( \lambda_h = 0 \) in the analysis.

Applying the correlator for the received signal of the CAISS embedding scheme (3.50), leads the test statistic \( z \) be expressed in the following form

\[
z = \begin{cases} 
    s^T x + N A_1 + s^T n, & \text{if } s^T x \geq 0, \; b = +1, \\
    s^T x(1 - \lambda_h N) - N A_2 + s^T n, & \text{if } s^T x \geq 0, \; b = -1, \\
    s^T x - N A_1 + s^T n, & \text{if } s^T x < 0, \; b = -1, \\
    s^T x(1 - \lambda_h N) + N A_2 + s^T n, & \text{if } s^T x < 0, \; b = +1.
\end{cases}
\] (3.51)

Since the test statistic in (3.51) is a sum of one Gaussian random variable and one random variable with half-Gaussian distribution, it is non-Gaussian distributed. This is the distinct point making the analysis of the CAISS scheme in the presence of additional noise different from the noise-free scenario in Sections 3.3 and 3.4. We first derive the PDF for the case that \( s^T x \geq 0, b = +1 \). Similarly, the PDF for other cases can be derived. In Appendix B.7 has been shown that under above constraints, we have the following conditional PDF

\[
f_Z(z|s^T x \geq 0, b = +1) = \frac{2}{\sqrt{2\pi N (\sigma_n^2 + \sigma_n^2)}} \exp \left\{ \frac{-(z - NA_1)^2}{2N (\sigma_n^2 + \sigma_n^2)} \right\} \left[ 1 - Q \left( \frac{(z - NA_1)\sigma_n}{\sigma_n\sqrt{N(\sigma_n^2 + \sigma_n^2)}} \right) \right].
\] (3.52)

Applying a similar derivation to (B.26) and regarding the test statistic (3.50), the following distributions are obtained

\[
f_Z(z|s^T x < 0, b = +1) = \frac{2}{\sqrt{2\pi N (\sigma_n^2 + \sigma_n^2)(1 - \lambda_h N)^2}}} \exp \left\{ \frac{-(z - NA_2)^2}{2N (\sigma_n^2 + \sigma_n^2)(1 - \lambda_h N)^2}} \right\} \times Q \left( \frac{(z - NA_2)\sigma_n}{\sigma_n\sqrt{N(\sigma_n^2 + \sigma_n^2)(1 - \lambda_h N)^2}}} \right),
\] (3.53)

\[
f_Z(z|s^T x \geq 0, b = -1) = \frac{2}{\sqrt{2\pi N (\sigma_n^2 + \sigma_n^2)(1 - \lambda_h N)^2}}} \exp \left\{ \frac{-(z + NA_2)^2}{2N (\sigma_n^2 + \sigma_n^2)(1 - \lambda_h N)^2}} \right\} \times \left[ 1 - Q \left( \frac{(z + NA_2)\sigma_n}{\sigma_n\sqrt{N(\sigma_n^2 + \sigma_n^2)(1 - \lambda_h N)^2}}} \right) \right].
\] (3.54)

\[
f_Z(z|s^T x < 0, b = -1) = \frac{2}{\sqrt{2\pi N (\sigma_n^2 + \sigma_n^2)}} \exp \left\{ \frac{-(z + NA_1)^2}{2N (\sigma_n^2 + \sigma_n^2)} \right\} Q \left( \frac{(z + NA_1)\sigma_n}{\sigma_n\sqrt{N(\sigma_n^2 + \sigma_n^2)}} \right).
\] (3.55)

Figure 3.4 shows the above distributions of \( z \) and it is observed from it that in the presence of
3.5. CASS and CAISS in the Presence of Additional Noise

In practice, one issue is to determine the parameters $A_1$ and $\lambda_h$ in the presence of additional noise. Due to the complex expression of the error probability in (3.56) for CAISS, finding a closed form solution of the parameters is not feasible and numerical approach should be employed. The parameters $A_1$ and $\lambda_h$ can be obtained by solving the following constrained two

$$P_{e-CAISS} \approx P_1(A_1, \sigma_x^2) - P_1(A_2, \sigma_x^2(1 - \lambda_h N)^2) + P_2(\sigma_x^2(1 - \lambda_h N)^2) + P_3(n - 1, 2, A_1, \sigma_x^2)$$

$$- P_3(2, 1, A_2, \sigma_x^2(1 - \lambda_h N)^2).$$

(3.56)

where

$$P_1(A_i, \sigma^2) = \sqrt{\frac{\sigma_n^2}{\sigma_n^2 + \sigma^2}} Q \left( \frac{NA_i}{\sqrt{N\sigma_n^2}} \right) c_1 + \frac{NA_i^2 \sigma_n^2}{\sqrt{2\pi N(\sigma_n^2 + \sigma^2)}} \exp \left\{ -\frac{NA_i^2}{2\sigma_n^2} \right\},$$

(3.57)

$$P_2(\sigma^2) = Q \left( \frac{NA_2}{\sqrt{N(\sigma_n^2 + \sigma^2)}} \right),$$

(3.58)

$$P_3(k_1, k_2, A_i, \sigma^2) = \frac{1}{\sqrt{2\pi}} \sum_{n \in \{3, 5, \ldots, n_a - 1\}} c_n (-1)^{k_1} [N(\sigma^2 + \sigma_n^2)]^{-\frac{n}{2}} \times$$

$$\sum_{r=1}^{n-2} [(NA_i)^{2r-1}(N\sigma_n^2)^{\frac{n+1}{2}-r} \exp \left\{ -\frac{NA_i^2}{2\sigma_n^2} \right\} \prod_{t=0}^{n-1-r} (n - 2 - 2t)] +$$

$$\sqrt{2\pi}(N\sigma_n^2)^{\frac{n}{2}} \left\{ \prod_{t=0}^{n-3} (n - 2 - 2t) + (NA_i)^{n-2}(N\sigma_n^2) \exp \left\{ -\frac{NA_i^2}{2\sigma_n^2} \right\} \right\} -$$

$$\frac{(-1)^{k_2}}{\sqrt{2\pi}} (N\sigma_n^2) \exp \left\{ -\frac{NA_i^2}{2\sigma_n^2} \right\} \sum_{n \in \{4, 6, \ldots, n_a\}} c_n (-1)^{k_1} [N(\sigma^2 + \sigma_n^2)]^{-\frac{n}{2}} \times$$

$$\sum_{r=1}^{n-2} [(NA_i)^{2r-2}(N\sigma_n^2)^{\frac{n+1}{2}-r} \prod_{t=0}^{n-2-r} (n - 2 - 2t)] + (NA_i)^{n-2}.$$

(3.59)
dimensional minimization problem

\[(A_1, \lambda_h) = \arg \min_{A_1, \lambda_h} P_{e-CAISS}(\bar{A}_1, \bar{\lambda}_h). \tag{3.60}\]

We can employ standard numerical methods to solve the above minimization problem and obtain the desired parameters.

With \(\lambda_h = 0\), referring to the error probability for the CAISS scheme, we could obtain the corresponding error probability for the CASS scheme as follows

\[P_{e-CASS} \approx P_1(A_1, \sigma_x^2) - P_1(A_2, \sigma_x^2) + P_2(\sigma_x^2) + P_3(n - 1, 2, A_1, \sigma_x^2) - P_3(2, 1, A_2, \sigma_x^2). \tag{3.61}\]

Figure 3.5 depicts the distribution of the test statistic for the CASS scheme. It is clear that CASS leads to more PDF leakage when compared with CAISS in Figure 3.4.

3.6 Simulation Results

In this section, we conduct extensive simulations to verify the analysis results derived for the proposed CASS and CAISS schemes. The simulation results have been obtained by employing the Monte Carlo simulations using \(N = 100\) unless stated otherwise. For the noiseless cases, the value of the parameter \(\lambda_h\) is determined for each DWR based on the expressions in Eqn. (3.38), and for the additional Gaussian noise cases, \(\lambda_h\) is obtained by numerically solving the minimization problem in (3.60).

To show the preciseness of the obtained error probability for the CASS scheme in (3.14), both the theoretical and simulation results versus DWR are shown in Figure 3.6 where different values of the amplitude \(A_1\) are investigated. From this figure, excellent matches between the theoretical and simulation results are observed. It also reveals that a smaller value of the amplitude \(A_1\) yields a better decoding performance. In the absence of any additional noise, given a fixed embedding distortion, a smaller value of \(A_1\) would save embedding distortion and thus lead to a larger value of \(A_2\). Since for the noise-free case the PDFs relating to \(A_1\) have no leakage, intuitively a larger value of \(A_2\) makes the PDFs leading to leakage be further apart from each other and thus reduces the decoding error.

Figure 3.7 illustrates the theoretical (3.37) and experimental error probabilities for the CAISS scheme. Almost perfect match between the results is observed, which verifies the correctness of the theoretical derivations. Similar to the CASS case, we can see that a smaller \(A_1\) yields better decoding error probability in CAISS. We also evaluate the decoding improvement of CAISS using the EPIF measure in (3.42). Figure 3.8 clearly shows a substantial decoding performance improvement of the CAISS data hiding scheme over ISS. Though not reported specifically,
3.6. Simulation Results

we would like to mention that the proposed CAISS yields significant decoding performance improvement over the SS scheme as well. It is also noted from Figure 3.8 that the EPIF has an asymptotic behavior for high DWR, which represents the low embedding distortion region. Basically, it means that when the embedding distortion is very small, CAISS and CASS yield similar decoding performances. Based on Eqn. (3.39), it is noted that \( \lambda_h \) approaches zero for a small embedding distortion (i.e., for a high DWR), and a similar observation for \( \lambda \) is noted. Therefore, by taking this into consideration and referring to the expression in (3.42), we can show that in the asymptotic case (i.e., for high DWR), the EPIF of CAISS over ISS approaches

\[
Q \left( \frac{N\sqrt{2D-A_1^2}}{\sqrt{N}\sigma_x} \right) / Q \left( \frac{N\sqrt{D}}{\sqrt{N}\sigma_x} \right)
\]

which is close to one for a small distortion. Thus, the observed asymptotic behavior is intuitively explained. It is also worth mentioning that, since both \( \lambda_h \) and \( \lambda \) approach zero in the asymptotic case, CAISS performs similarly as CASS and ISS performs similarly as SS asymptotically for a small embedding distortion.

The result of IRIF defined in (3.45) for comparing CAISS and ISS is shown in Figure 3.9. It is clear that the CAISS scheme is more robust against the interference than the ISS scheme. Based on the expression of (3.45), it could be shown that the IRIF of CAISS and ISS asymptotically approaches \( D/(2D - A_1^2) \) for the high DWR region. In Figure 3.9 it is noted that a smaller value of \( A_1 \) leads to better robustness against the interference effect of the host signal. Once again, intuitively this is because that in the absence of noise, a smaller value of \( A_1 \) reduces the PDF leakage and thus allows the correlation-aware schemes to tolerate more host-interference effect for a fixed error probability and embedding distortion. Even though the result of IRIF for the CAISS and ISS scheme has been reported here, since the ISS scheme outperforms the SS scheme, we can easily show that the CAISS scheme enhances the robustness against the interference effect of the host signal when compared with SS. In addition, because of the inverse relationship between IRIF and PIF for the CAISS and SS scheme, it is clear that the proposed CAISS scheme improves the payload for data hiding.

To verify the derivation of the distributions of the test statistic \( z \) in the presence of additional Gaussian noise, Figure 3.10 plots both the theoretical PDF in (3.52) and the experimental one. In this figure, we have used the notion watermark-to-noise ratio (WNR) defined as WNR = \( 10\log(\frac{D}{\sigma_n^2}) \), and have set WNR = 0 dB. The simulation results in Figure 3.10 demonstrate the accuracy of the theoretical derivation of the PDF and thus support the correctness of the derivation.

To verify the derived decoding performances for CASS (3.61) and CAISS (3.56) in the presence of additional Gaussian noise, the error probability versus DWR curves are plotted in Figure 3.11 and Figure 3.12, respectively, where \( n_o = 30 \) and different WNR are studied. The figures illustrate the consistence between the theoretical and empirical results and prove the correctness of the theoretical analysis.
3.6. Simulation Results

To demonstrate the decoding performance improvements of CAISS over both SS and ISS even in the presence of additional Gaussian noise, the EPIF curves are shown in Figure 3.13 and Figure 3.14. We can see that the proposed CAISS scheme is still superior to the SS and ISS schemes. It is observed that the EPIF does not demonstrate a monotonic behavior in these figures: as the DWR decreases, the EPIF decreases first and then increases. For Figure 3.13 we can show that the corresponding EPIF is a complicated function, where the error probability of the CAISS scheme is expressed in Eqn. (3.56) and the error probability of SS can be derived as $Q\left(N\sqrt{D}/\sqrt{N(\sigma_x^2 + \sigma_n^2)}\right)$, and thus theoretical justification of this behavior is not easy. Numerically, we note that at the minimal point, the parameter $\lambda_h$ tends to take the extreme value of $1/N$ in order to maximally reject the effect of the host signal. An intuitive explanation of the observed non-monotonic behavior is as follows. With additional Gaussian noise, there are two conflicting factors contributing to the overall decoding performance: the embedding distortion $D$ and the additional noise with variance $\sigma_n^2$. A larger distortion, which means a higher watermark power, leads to a smaller decoding error rate, while a larger noise variance $\sigma_n^2$ results in more PDF leakage and thus increases the decoding error rate. Since for each curve in Figure 3.13 we fix the WNR, $D$ and $\sigma_n^2$ increase or decrease simultaneously. Given a WNR, as we first decrease the DWR (i.e., increasing $D$), the factor of $D$ is dominant and thus the performance measure EPIF decreases (until the parameter $\lambda_h$ approaches $1/N$); as we further decrease the DWR, $\lambda_h$ does not change anymore, while the noise variance $\sigma_n^2$ is larger and causes more PDF leakage, and thus becomes the dominant factor and leads to the increased EPIF measure. The behavior in Figure 3.14 can be similarly explained. We also want to mention that, to provide a good trade-off between decoding performance and imperceptibility in practical data hiding, the DWR can not be too large and meanwhile it can not be too small.

To study the performance of CAISS against WNR, three different values of DWR are studied in Figure 3.15. It is noted that the CAISS scheme consistently yields better performance, even at a low WNR. Figure 3.16 shows the logarithm of the EPIF measure as a function of the number of host coefficients when DWR = 25 dB. We can see clear improvements of the CAISS scheme over ISS, especially when $N$, the number of the host coefficients, increases.

3.6.1 Experimental Results

Recently, in [44], a study was conducted for investigating the performance of the proposed CAISS scheme on real images. Real images with size of 512x512 were tested and the SS, ISS, and CAISS schemes were applied to the DCT coefficients of the images. All the results in the paper were obtained from image tests conducted on the BOWS2 original database [49]. In their study, 800 message bits were embedded into DCT coefficients of each image, and the robustness against JPEG compression was investigated. It shows that the proposed CAISS significantly
3.6. Simulation Results

outperforms the SS and ISS schemes under the JPEG compression distortion. For instance, from Table 1 in [44] by testing on 9997 images, their study shows that appropriate choice of CAISS parameters results in two orders of magnitude smaller BER as compared with SS under medium JPEG compression (i.e., JPEG quality level 75%) and specific Peak Signal-to-Noise Ratio (PSNR) level (i.e., 37.0 +/- 0.3dB). From Fig. 5 in [44] by testing 500 images for SS and 2000 images for ISS and CAISS, it is noted that CAISS can perform approximately two times better than ISS after JPEG compression.

However, it is worth clarifying that this thesis does not evaluate explicitly how the proposed modifications to the original SS scheme affect CASS’s robustness against StirMark and possibly other distortion attacks, not studied in [44].

Figure 3.1: Illustration of the PDFs in (3.4) and (3.3) of the test statistic $z$ in (3.2) for the SS scheme.

Figure 3.2: Illustration of the PDFs in (3.7)-(3.10) of the test statistic $z$ in (3.6) for the proposed CASS scheme.
3.6. Simulation Results

Figure 3.3: Illustration of the PDFs in (3.32)-(3.35) of the test statistic $z$ in (3.31) for the proposed CAISS scheme.

Figure 3.4: With additional noise: Illustration of the PDFs in (3.52), (3.55), (3.53), and (3.54) of the test statistic $z$ in (3.51) for the CAISS scheme.

Figure 3.5: With additional noise: Illustration of the PDFs in (3.52)-(3.55) of the test statistic $z$ in (3.51) when $\lambda_n = 0$ for the CASS scheme.

Figure 3.6: The theoretical and experimental error probabilities versus DWR for the CASS scheme with different $A_t^2$. 
3.6. Simulation Results

Figure 3.7: The theoretical and experimental error probabilities versus DWR for the CAISS scheme with different $A_1^2$.

Figure 3.8: The logarithm of EPIF versus DWR curves for evaluating of decoding performance improvements of the proposed CAISS over the ISS scheme.

Figure 3.9: The IRIF versus DWR curves to illustrate the improvement of the proposed CAISS over ISS. Different $A_1^2$ values are illustrated.

Figure 3.10: The theoretical and experimental results of the PDF expressed in (3.52).
3.6. Simulation Results

Figure 3.11: The theoretical and experimental error probabilities versus DWR for the CASS scheme with different WNR.

Figure 3.12: The theoretical and experimental error probabilities versus DWR for the CAISS scheme with different WNR.

Figure 3.13: The EPIF versus DWR curves to demonstrate the improvement of the proposed CAISS over SS. Different WNR values are illustrated.

Figure 3.14: The EPIF versus DWR curves to demonstrate the improvement of the proposed CAISS over ISS. Different WNR values are illustrated.
3.7. Conclusion

In this chapter, the correlation-and-bit-aware concept for spread spectrum embedding has been introduced. We have shown that the proposed CASS and CAISS data hiding schemes can improve the performance of the traditional SS and ISS schemes by taking into consideration the correlation between the host signal and the signature code and the bit message to be embedded. Thorough theoretical analysis on decoding error probability has been provided to prove that the CASS scheme outperforms the SS scheme and that the CAISS scheme outperforms the ISS scheme. We have also proved the superior robustness of the proposed CASS and CAISS data hiding schemes against the interference effect of the host signal. Furthermore, our analysis shows that using the proposed correlation-and-bit-aware data hiding schemes could increase the payload. In addition, the theoretical BER performances of the proposed schemes in the presence of additional noise have been derived. Extensive simulation results confirm the theoretical analysis and demonstrate the superiority of the the proposed CAISS scheme over the traditional SS and ISS schemes.
Chapter 4

Improved Multiplicative Spread Spectrum

4.1 Introduction

In the previous chapters, the additive SS scheme was presented which spreads the watermark uniformly over the host signal. In order to have imperceptible watermark, the multiplicative spread spectrum (MSS) could be used which spreads the watermark according to the host signal. Although MSS ends up with better perceptual quality than the SS, its decoding performance has not been analyzed yet. In addition, similar to the SS scheme, the interference effect of the host signal causes performance degradation. A few improved MSS schemes have been developed for reducing the interference effect. An enhanced MSS was proposed in [159] to improve the watermark detection rate, and a similar embedding scheme was developed in [21] for watermark decoding applications. Even though the scheme in [21] could provide better decoding performance than the conventional MSS, it can not completely remove the host interference effect.

Following the aforementioned motivations, this chapter serves two main goals. The first one is to provide the theoretical performance analysis of MSS. Although MSS has been proposed in [28], the exact analysis of its decoding performance, and capacity have not been provided yet. We will fill this gap in this chapter. The second goal of this chapter is to present an improved MSS (IMSS) scheme which could improve the decoding performance while maintaining the multiplicative embedding structure. We propose exploiting the correlation between the host signal and the watermark signal and exploring the decoder structure of the conventional MSS scheme at the embedding side to remove the interference effect of the host signal, where the introduced parameters will be efficiently determined to achieve a trade off between decoding performance and watermark-introduced distortion. We will then provide the theoretical error probability analysis of the proposed IMSS. It is worth mentioning that the proposed IMSS for data hiding has the same decoder structure as the conventional MSS and does not require additional information at the decoder side. To be complete, we will also provide the decoding error analysis for MSS and the proposed IMSS in the presence of additional noise.
4.2. Conventional MSS Scheme

The rest of this chapter is organized as follows. The MSS scheme is introduced briefly in Section 4.2, and its performance analysis is provided in Section 4.3. The proposed IMSS scheme is presented in Section 4.4. The decoding performance analysis of MSS and IMSS under additional noise are provided in Section 4.5, and the simulation results are reported in Section 4.6.

4.2 Conventional MSS Scheme

For the MSS scheme [28], the watermarked signal \( r = [r_1, r_2, ..., r_N]^T \) is represented as

\[
r_i = x_i + s_i x_i A b, \quad i = 1, 2, ..., N,
\]

(4.1)

where the information bit \( b \) is modulated and added into \( N \) host coefficients \( x = [x_1, x_2, ..., x_N]^T \) corresponding to the host coefficient values. Here \( b \) is assumed to be taken from a binary set \( b \in \{-1, +1\} \) and it is assumed that the host signal follows Gaussian distribution, such as Chapter 3, with zero mean and unit variance.

To extract the hidden information \( b \) from the received signal, we can employ the optimal decoder based on the maximum likelihood (ML) criterion. Based on (4.1), the conditional PDFs for the \( i \)th coefficient are given by

\[
  f_R(r_i | b = +1, s_i) = \mathcal{N} (0, (1 + s_i A)^2), \quad f_R(r_i | b = -1, s_i) = \mathcal{N} (0, (1 - s_i A)^2).
\]

(4.2)

With the Gaussian IID assumption on the host signal coefficients, the ML decoder is in the form of (2.9) where the test statistic \( z \) is expressed as

\[
z = r^T S_d r = \sum_{i=1}^{N} r_i^2 s_i,
\]

(4.3)

where \( S_d = \text{diag}\{s_1, s_2, ..., s_N\} \) means the diagonal matrix embracing the signature code coefficients.

4.3 Analysis of the MSS Scheme

In this section, the decoding performance of the optimal ML decoder based on (4.3) for MSS is analyzed. With the assumption of equal probability for the message bit, the probability of bit decoding error can be expressed as

\[
  P_{e-MSS} = Pr \left\{ \hat{b} \neq b \right\} = 0.5 Pr \left\{ \hat{b} = +1 | b = -1 \right\} + 0.5 Pr \left\{ \hat{b} = -1 | b = +1 \right\}.
\]

(4.4)
4.3. Analysis of the MSS Scheme

To obtain the error probability (4.4), we first need to derive the distribution of the host signal. Since $s_i$’s take their values from +1 and -1, the test statistic (4.3) can be expressed as

$$z = v - y,$$  

(4.5)

with the independent random variables $v$ and $y$ being

$$v = (1 + Ab)^2 \sum_{i \in C_p} x_i^2, \quad y = (1 - Ab)^2 \sum_{i \in C_n} x_i^2$$  

(4.6)

where the sets of $C_p$ and $C_n$ are defined as the set of indices which $s_i = +1$ and $s_i = -1$, respectively. Both sets have $N/2$ elements. It is straightforward to show that the terms $\sum_{i \in C_p} x_i^2$ and $\sum_{i \in C_n} x_i^2$ follow chi-square distribution with $N/2$ degrees of freedom. Therefore we have the following distributions

$$f_V(v) = \frac{1}{(1 + Ab)^2 2^{N/4} \Gamma(N/4)} \left[ \frac{v}{(1 + Ab)^2} \right]^{N/4 - 1} \exp \left\{ \frac{-v}{2(1 + Ab)^2} \right\} u(v),$$  

(4.7)

$$f_Y(y) = \frac{1}{(1 - Ab)^2 2^{N/4} \Gamma(N/4)} \left[ \frac{y}{(1 - Ab)^2} \right]^{N/4 - 1} \exp \left\{ \frac{-y}{2(1 - Ab)^2} \right\} u(y).$$  

(4.8)

where $u(.)$ returns +1 or 0 when its argument is positive or negative respectively, and $\Gamma(.)$ denotes the Gamma function. Based on (4.7) and (4.8), since the random variables $v$ and $y$ are positive and independent, the distribution of $z$ in (4.5) can be obtained as \[103\]:

$$f_Z(z) = \int_{-\infty}^{\infty} f_V(z + y) f_Y(y) dy.$$

(4.9)

We can show that the mean $m_z$ and variance $\sigma_z^2$ of the test statistic $z$ are as follows:

$$m_z = 2AbN, \quad \sigma_z^2 = 2N (A^4 + 6A^2 + 1).$$  

(4.10)

Having obtained the distribution of the test statistic, we could proceed to calculate the theoretical error probability of the MSS scheme. To this end, in Appendix C.1 it has been shown that the error probability is expressed as

$$P_{e-MSS} = \frac{1}{(1 - D)^{N/2} 2^{N/4} \Gamma^2(N/4)} \times \sum_{k=0}^{n} \left[ \binom{n}{k} \sum_{i=0}^{2n-k} (-1)^k \binom{2n-k}{i} i! \left[ \frac{(1 - D)^2}{(1 + D)} \right]^{i+1} (2n-i)! \left[ 2(1 - \sqrt{D})^2 \right]^{2n-i+1} \right]^{i+1}.$$  

(4.11)
4.3. Analysis of the MSS Scheme

Based on the derived error probability \( (4.11) \) for MSS, we note that the MSS can be error free. More specifically, it could be shown that the error probability is equal to zero when \( D = 1 \). In other words, the decoder does not make any wrong decoding decision when the DWR is 0 dB. This observation could also be verified by considering the conditional PDF of \( f_Z(z|b = +1, z < 0) \) when \( D = 1 \). An error decision is made when a PDF leakage happens, i.e., when the test statistic \( (4.3) \) becomes negative or positive while the bit \( b +1 \) or \( -1 \) is sent, respectively. It is clear that when \( f_Z(z|b = +1, z < 0) \) is not zero, there will be decoding errors due to PDF leakage. When \( D = 1 \), the conditional PDF can be shown to be zero, implying that there is no PDF leakage.

The analysis of the error probability of MSS can provide some insight into the decoding behavior of MSS at different DWR and can be used to explain the motivation of the proposed IMSS. We can rewrite \( (4.11) \) in terms of DWR as

\[
P_{e-MSS}(DWR) = \frac{\left(1 - 10^{\frac{DWR}{20}}\right)^{N/2}}{\left(1 + 10^{\frac{DWR}{20}}\right)^{N/2} 2^{N/2} \Gamma^2(N/4)} \times 
\sum_{k=0}^{n} \binom{n}{k} \left[\sum_{i=0}^{2n-k} (-1)^k \binom{2n-k}{i} \frac{1 + 10^{\frac{DWR}{20}} + 2 \times 10^{\frac{DWR}{20}}}{1 + 10^{\frac{DWR}{20}}} i! (2n-i)! (2^{2n-i+1})\right].
\]

From \( (4.12) \), we note that \( P_{e-MSS}(DWR) = P_{e-MSS(-DWR)} \), meaning that \( P_{e-MSS}(DWR) \) is an even function of DWR. It is clear that \( P_{e-MSS}(DWR) \) is not a monotonically decreasing function of DWR. More precisely, the error probability decreases first as the DWR decreases until the DWR reaches 0 dB (which leads to error free decoding), and further decreasing the DWR leads to the increase of the error probability. This non-monotonic behavior could also be explained by the statistics of the test statistic in \( (4.10) \), i.e., increasing the watermark amplitude increases both the mean and the variance of the test statistic. In fact, the power of the information to the interference could be expressed as \( \frac{n_z^2}{\sigma_z^2} \). Referring to \( z \) in \( (4.10) \) and taking the derivative of above expression with respect to \( D \), we can show that this function has a Gaussian-like curve with the maximum at one. Thus, the non-monotonic behavior of the error probability is justified. This observation in MSS is different from additive SS, where increasing the watermark amplitude increases the mean of the test statistic while the variance is fixed, and thus a higher watermark amplitude in additive SS leads to a better decoding performance.

Since information (data) hiding could be interpreted as a communication channel, we also study the channel Shanon capacity of MSS, i.e., the maximum host payload in bit that allows information recovery with arbitrary small probability of error \[26\]. As the received signal \( r \) conveys the information bit in MSS \( (4.1) \), the capacity is expressed by \( C = \max_{f_b} I(b;r) \), where \( I(b;r) \) denotes the mutual information conveyed by the received signal \( r \) and the maximization
is taken over all possible distribution $f_b$. The mutual information is defined as

$$I(b; r) = h(r) - h(r|b)$$

where $h(r)$ and $h(r|b)$ represent the differential entropy and conditional differential entropy, respectively. Therefore, it could be shown (see Appendix C.2) that under reasonably high DWR, the capacity of the MSS scheme is expressed as

$$C_{MSS}(DWR) = \frac{N}{2} \log_2 \left( \frac{1 + 10^{-\frac{DWR}{10}}}{1 - 10^{-\frac{DWR}{10}}} \right).$$

(4.13)

It could be seen that by approaching DWR towards zero, the channel capacity increases which is consistent with the behavior of the error probability.

### 4.4 Improved Multiplicative Spread Spectrum

In Section 4.3, we observed that the MSS scheme is error free when the DWR is 0 dB. In MSS, the host signal itself is one source of decoding errors because the host signal is treated as noise at the decoder. Since the structure of the decoder (4.3) is known at the encoder side, it motivates us to propose an improved MSS (IMSS) scheme by exploiting the decoder structure during the multiplicative based embedding to remove the interference effect of the host signal. Specifically, we propose the following IMSS embedding scheme:

$$r = x + S_d Ab + g S_d x,$$

(4.14)

where $g$ denotes a function to be described shortly. The basic idea behind the proposed IMSS is to take advantage of the decoder structure in (4.3) for MSS and introduce the term $g S_d x$ to compensate the host interference effect.

We now explain the IMSS intuition with more details. Since the IMSS scheme has a similar embedding structure to MSS, we can heuristically employ the ML decoder for MSS in (4.3) and (3.1) for extracting the bit $b$. As a result, for IMSS (4.14), the decoder can be expressed as (3.1) with the test statistic $z$ as

$$z = 2b \left( Ag x^T S_d x + A x^T x \right) + \left[ x^T S_d x \left( 1 + A^2 + g^2 \right) + 2 x^T x g \right].$$

(4.15)

The test statistic (4.15) consists of two terms, where the first one contains the information bit $b$ and the second one contains the interference and is the source of decoding errors. Ideally, if we can remove the second term and make $(Ag x^T S_d x + A x^T x)$ of the first term be positive, the decoder (3.1) can be decoding error free. Therefore, we propose determining the desired
4.4. Improved Multiplicative Spread Spectrum

function $g$ by making the interference term zero, i.e.

$$g^2 x^T S_d x + 2g x^T x + (x^T S_d x + A^2 x^T S_d x) = 0. \quad (4.16)$$

Finding the roots of the above quadratic equation shows that function $g$ should be as

$$g = \frac{-x^T x + \sqrt{(x^T x)^2 - (x^T S_d x)^2(1 + A^2)}}{x^T S_d x}, \quad (4.17)$$

which satisfies the requirement that $(Ag x^T S_d x + Ax^T x) > 0$. Therefore, by exploiting IMSS in (4.14), using $g$ in (4.17) at the encoder side and employing the decoder (4.3) as in MSS at the receiver side, the proposed IMSS could yield error free decoding performance.

For watermarking methods, we normally need to calculate the total watermark-introduced distortion due to watermark embedding and we would prefer a closed form expression of the distortion, e.g., especially for performance comparisons of different embedding schemes. Referring to the distortion definition, for IMSS (4.14), we have the distortion as

$$D = A^2 + \frac{1}{N} E \{g^2 x^T x\}. \quad (4.18)$$

Since $g$ is in the form of (4.17), computing the distortion (4.18) in a closed form directly is rather difficult. To avoid this complexity, we rewrite the expression of $g$ (4.17) as

$$g = -x^T x + (x^T x) \left[ 1 - \left( \frac{x^T S_d x}{x^T x} \right)^2 (1 + A^2) \right]^{1/2} / (x^T S_d x). \quad (4.19)$$

Now, we employ the binomial series, i.e., the Taylor series at $x = 0$ for the function $(1 + x)^\alpha$ where $\alpha$ is positive, described as

$$(1 + x)^\alpha = 1 + \sum_{k=1}^{\infty} \left[ \frac{x^k}{k!} \prod_{j=0}^{k-1} (\alpha - j) \right]. \quad (4.20)$$

Substituting the binomial series (4.20) into $g$ in (4.19) leads to the following approximation

$$g(u) = \sum_{k=1}^{d} \left[ \left( \frac{x^T S_d x}{x^T x} \right)^{2k-1} (u)^k \frac{(-1)^k}{k!} \prod_{j=0}^{k-1} \left( \frac{1}{2} - j \right) \right], \quad (4.21)$$

where we have $u = 1 + A^2$. Here, the parameter $d$ determines the accuracy of the binomial series. As $d$ increases, the difference between the approximated $g$ and its exact value (4.17) decreases. We can show that when $d = 1$, the proposed IMSS scheme is reduced to the scheme in [21],
meaning that the scheme in [21] for the Gaussian host signal is a special case of the proposed IMSS. \( d = 1 \) represents a coarse approximation and thus may not be able to efficiently remove the host interference effect. Our later simulations show that a higher value of \( d \), e.g., \( d = 2 \), provides better decoding performances.

Now, with the approximation of \( g \) in (4.21), to explicitly express the distortion of IMSS, we need to define a variable which could also help our analysis in the rest of the chapter. Let define \( H(m, n, q, u) \) and \( h(m, n, q, u) \) as follow

\[
H(m, n, q, u) = g^m(u) \left( x^T x \right)^n \left( x^T S d x \right)^q, \tag{4.22}
\]

\[
h(m, n, q, u) = E\{H(m, n, q, u)\}. \tag{4.23}
\]

In Appendix [C.3] we will show that, for non-negative integers of \( m, n, \) and \( q \), we have

\[
h(m, n, q, u) = \sum_{k_1=1}^{d} \ldots \sum_{k_m=1}^{d} \left[ (-u)^{(\sum_{i=1}^{m} k_i)} \prod_{r=k_1}^{k_m} \prod_{j=0}^{r-1} \left( \frac{1}{2} - j \right) \prod_{i=1}^{m} k_i ! \right] \times \sum_{n=0}^{p} \left[ (-1)^{n} 2^{p-n} \frac{\Gamma(p - n + N/4) \Gamma(n + N/4) \Gamma(p - l + N/2) \Gamma(p + N/2)}{\Gamma^2(N/4) \Gamma(p + N/2)} \right], \tag{4.24}
\]

where

\[
p = 2 \sum_{i=1}^{m} k_i - m + q, \quad l = 2 \sum_{i=1}^{m} k_i - m - n. \tag{4.25}
\]

Now, according to (4.18), (4.22) and (4.24), we have the distortion of IMSS as

\[
D = A^2 + \frac{1}{N} h(2, 1, 0, 1 + A^2). \tag{4.26}
\]

The distortion expression (4.26) is a useful measure, because it determines that, for fixed watermark parameters, how much distortion is introduced in IMSS to remove the host interference effect.

We have shown that applying the IMSS scheme (4.14) with \( g(1 + A^2) \) expressed in (4.21) could lead to error free decoding.

Even though the proposed IMSS with \( g(1 + A^2) \) in (4.17) could provide decoding error free performance, it introduces a specific degree of distortion into the watermarked signal, as described in (4.26). For some practical watermarking applications, if it is desirable to have less distortion, it is preferred to employ IMSS (4.14) with using \( g(\lambda) \) instead of \( g(1 + A^2) \) where the
4.4. Improved Multiplicative Spread Spectrum

free parameter \( \lambda \) provides a trade off between the distortion and the decoding performance. In other words, when a larger distortion is allowed, a larger magnitude of \( \lambda \) can be used to achieve a better decoding performance; and when a lower distortion is allowed, a smaller \( \lambda \) should be used. This free parameter allows us working at each individual DWR. Using \( g(\lambda) \) as long as the parameter \( \lambda \) is less than 1 can partially achieve host rejection while there is still PDF leakage; and when \( \lambda \) is larger than 1, the host signal effect can be removed completely. While for the former case there is still PDF leakage, therefore developing the optimal decoder is crucial to minimize the leakage effect, and the watermarked signal distribution is needed for obtaining the optimal decoder.

As mentioned earlier, similar to MSS, the decoder (3.1) with the test statistic (4.3) can be heuristically exploited for extracting the hidden bits in the proposed IMSS. However, one should note that this decoder is optimal only for Gaussian watermarked signal. For the proposed IMSS, to derive the ML optimal decoder, we first need to investigate the distribution of the watermarked signal (4.14), where the distribution of the random variable \( g \) is needed. Based on our simulations, we observed that the distribution of \( g \) approaches Gaussian when \( N \) is increased. It should be mentioned that \( g \) has zero mean and variance \( h(2,0,0,\lambda) \). Figure 4.1 illustrates the experimental and theoretical PDF results of the random variable \( g(u) \) when \( N = 60 \) and DWR = 21 dB. We clearly see a close match between the experimental and theoretical results, and thus the Gaussian assumption of the random variable \( g(u) \) is valid. To further validate the assumed Gaussian distribution, we also conduct the Kolmogorov-Smirnov test which verifies whether two different samples belong to the same distribution or not by exploiting the difference of the Cumulative Distribution Function (CDF) of the samples. Our analysis based on the Kolmogorov-Smirnov test reveals that the Gaussian approximation is valid for the random variable \( g(u) \). Given the Gaussian distribution of \( g \), we can derive the distribution of the watermarked signal in IMSS (4.14), where the \( i \)th coefficient could be interpreted as the multiplication of two Gaussian random variables \( x_i \) and \( y_i \), with

\[
y_i = 1 + s_i Ab + s_i g. \tag{4.27}
\]

In Appendix C.4 we show the PDF of the watermarked signal \( r \) in IMSS (4.14) is expressed as

\[
f_R(r) = \frac{1}{(\sqrt{\pi} \sigma_y^2)^N} \exp \left\{ \frac{-N(1 + A^2)}{2\sigma_y^2} \right\} \prod_{i=1}^{N} \sum_{n=0}^{\infty} \frac{1}{n! \Gamma(n + 1/2)} \left( \frac{(1 + s_i Ab)^2 |r_i|}{4\sigma_y^3} \right)^n K_n \left( \frac{|r_i|}{\sqrt{\sigma_y^2}} \right) \tag{4.28}
\]

where \( \sigma_y^2 = h(2,0,0,\lambda) \) and \( K_n(\cdot) \) denotes the modified Bessel function of the second kind.

Based on (4.28), applying the maximum likelihood criterion (2.9), we can derive the ML
Improved Multiplicative Spread Spectrum

decoder in the form of (3.1) with the test statistic $z$ being

$$
z = \prod_{i=1}^{N} \left[ \sum_{n=0}^{\infty} \frac{1}{n! \Gamma(n+1/2)} \left( \frac{|r_i|}{4\sigma_y^3} \right)^n K_n \left( \frac{|r_i|}{\sqrt{\sigma_y^2}} \right) \left[ (1 + s_i A)^{2n} - (1 - s_i A)^{2n} \right] \right]. \quad (4.29)
$$

From the above test statistic (4.29), it is noted that the watermark amplitude $A$ is required for the ML decoder. However, in practice, such watermark amplitude information is generally not available at the decoder side, and thus it will be preferred to find a practical approximation of the distribution in (4.28) and obtain a simpler decoder without requiring $A$. Our study showed that the exact distribution of the watermarked signal in (4.28) at relatively moderate and high DWR could be well approximated by a Gaussian distribution. Figure 4.2 shows the experimental, exact theoretical (4.28), and Gaussian approximation of the first coefficient of the watermarked signal when $s_1 b = -1$, i.e., $f_R(r_1|A, s_1 b = -1)$, $N = 60$ and DWR = 21 dB. The figure clearly illustrates the good match between the experimental result and the exact PDF in (4.28) and the close match between the theoretical PDF and the Gaussian approximation. Once again, we investigated the Kolmogorov-Smirnov test to verify the results.

Replacing (4.28) using the approximated Gaussian distribution, we can have the ML decoder as the decoder of (3.1) with the test statistic being in the form of (4.3) and (4.15). For IMSS, compared with the optimal decoder (3.1) with $z$ in (4.29), the decoder (3.1) with $z$ in (4.3) has a much simpler structure and, more important, is independent of the watermark amplitude. Also, it is noted that the decoder (3.1) with $z$ in (4.3) for IMSS is the same as the optimal decoder for MSS.

In practice, for the proposed IMSS, we may need to determine the generalized free parameter $\lambda$ for a given allowed distortion. For the IMSS scheme, using the free parameter $\lambda$, the test statistic (4.15) consists of two terms, where the first one $(2A g(\lambda) x^T S_d x + 2A x^T x)$ contains the bit information and the other term $(x^T S_d x (1 + A^2 + g^2(\lambda)) + 2g(\lambda) x^T x)$ represents the interference and causes the decoding errors. The powers of the information bit and the interference at the decoder side can be correspondingly defined as $P_{inf} = E \left\{ 4A^2 (g(\lambda) x^T S_d x + x^T x)^2 \right\}$ and $P_{int} = E \left\{ (x^T S_d x (1 + A^2 + g^2(\lambda)) + 2g(\lambda) x^T x)^2 \right\}$, respectively. In order to determine the value of $\lambda$, we define the information to interference ratio (IIR), which is the ratio of the power of bit information to the power of the interference term, as

$$
IIR \triangleq \frac{P_{inf}}{P_{int}}. \quad (4.30)
$$

It is obvious that a higher IIR leads to more host interference rejection, and consequently better decoding performance. Using the distortion expression (4.26) and the definition of $h(m, n, q, u)$
4.4. Improved Multiplicative Spread Spectrum

In (4.24), the information and interference powers can be expressed as

\[ P_{inf} = 4 \left( D - \frac{1}{N} h(2, 1, 0, \lambda) \right) \left[ h(2, 0, 2, \lambda) + 2h(1, 1, 1, \lambda) + \frac{4\Gamma(2 + N/2)}{\Gamma(N/2)} \right], \quad (4.31) \]

\[ P_{int} = 2N \left( 1 + D - \frac{1}{N} h(2, 1, 0, \lambda) \right) h(2, 0, 2, \lambda) + 4h(2, 2, 0, \lambda) + 4h(3, 1, 1, \lambda) + 2 \left( 1 + D - \frac{1}{N} h(2, 1, 0, \lambda) \right) h(2, 0, 2, \lambda) + 4 \left( 1 + D - \frac{1}{N} h(2, 1, 0, \lambda) \right) h(1, 1, 1, \lambda). \quad (4.32) \]

Since a higher IIR leads to more host rejection, based on the IIR expression using (4.30)-(4.32), we propose determining the parameter \( \lambda \) by solving the following maximization problem,

\[ \hat{\lambda} = \arg\max_{\lambda} \text{IIR}. \quad (4.33) \]

As a summary, for an allowed fixed distortion, exploiting IMSS (4.14) with \( g(\lambda) \) and \( \lambda \) being obtained using (4.21) and (4.33), respectively, could efficiently reduce the host interference effect. To further explain the advantage of the proposed IMSS and to provide more insight into why the IMSS could help removing the host interference effect, we study the PDFs of the test statistics for MSS and IMSS schemes. The experimental PDFs of the test statistic \( z \) for MSS and IMSS are illustrated in Figures 4.3 and 4.4 where \( N = 100 \) and DWR = 23 dB. Each figure shows two peaks corresponding to the information bit -1 and +1 respectively. Comparing Figures 4.3 and 4.4 for the same DWR reveals that IMSS leads to better distinguishing capability between \( b = -1 \) and \( b = +1 \). More precisely, the PDFs \( f_Z(z|b = +1) \) and \( f_Z(z|b = -1) \) for IMSS are taller and farther apart than their counterparts for the MSS scheme. This example demonstrates that IMSS has less PDF leakage.

We now proceed to analyze the decoding error probability for IMSS. As mentioned earlier, the distribution of the watermarked signal (4.28) can be approximated by a Gaussian distribution and thus the decoder is in the form of (3.1) where the test statistic \( z \) is as in (4.15). We need the distribution of the test statistic (4.15). However, finding the exact distribution of \( z \) in (4.15) is very difficult due to its complex structure and an appropriate approximation of the distribution is needed to simplify the analysis. Investigating (4.15) reveals that the coefficient of the information bit regarding (4.17) is always positive and the interference term could take either positive or negative values and thus, the resulted distribution is skew, as seen in Figure 4.4. Thus, we propose to approximate the distribution of \( z \) given the information bit as skew
normal in the following form

$$f_Z(z) = \frac{2}{\omega \sqrt{2\pi}} \exp \left\{ -\left(\frac{z - \zeta}{2\omega^2}\right)^2 \right\} \left[ 1 - Q\left(\alpha \left(\frac{z - \zeta}{\omega}\right)\right) \right],$$ (4.34)

where the function $Q(.)$ is defined as $Q(x) = \frac{1}{2\pi} \int_x^\infty \exp \left\{ -\frac{u^2}{2} \right\} du$, $\zeta$ and $\omega$ are the location and scale parameters, respectively, and $\alpha$ represents the skewness of the distribution. To illustrate the matching between the experimental distribution and the theoretical approximation (4.34) of the IMSS test statistic $z$ in (4.15), Figure 4.5 is shown where $N = 60$ and DWR = 21 dB. We can see that the difference between the experimental PDF and the fitted skew normal distribution is very subtle. With regard to the skew normal distribution of the test statistic (4.34), in Appendix C.5, it has been shown that the error probability is obtained as

$$P_{e-IMSS} = Q\left(\frac{\zeta}{\omega}\right) - \frac{1}{\pi} \tan^{-1} \alpha - \frac{1}{\pi} \sum_{n=1}^\infty \left[ \frac{1}{n!} \left( -\frac{\zeta^2}{2\omega^2} \right)^n \sum_{k=0}^{n-1} \frac{(n-1)}{k} \frac{\alpha^{2k+1}}{2k+1} \right],$$ (4.35)

where the corresponding parameters have been obtained in the same Appendix.

As discussed earlier, there could be a subtle difference between the true PDF and the skew normal distribution of the test statistic. This skew normal approximation could affect the accuracy of the bit error probability analysis, especially at the very low bit error rates.

### 4.5 MSS and IMSS in the Presence of Additional Noise

In Section 4.4, we proved that the proposed IMSS could decrease the PDF leakage and consequently improve the decoding performance when compared with MSS in the absence of additional noise. In practice, the received watermarked signal can be contaminated with additional noise. In this section, we will investigate the decoding performances of MSS and the proposed IMSS in the presence of additional noise. For IMSS, the received noisy signal is described as

$$r = x + S_d x A b + g S_d x + n,$$ (4.36)

where $n = [n_1, n_2, ..., n_N]^T$ represents the Gaussian noise coefficients with zero-mean and variance of $\sigma_n^2$. Note that MSS can be considered as a special case of the IMSS scheme with $g = 0$. We first analyze the MSS scheme and then analyze IMSS in the presence of additional noise.

For MSS, it is obvious that now the received signal follows Gaussian distribution as $f_R(r_i|b, s_i) = \mathcal{N}\left(0, (1 + s_i A b)^2 + \sigma_n^2\right)$. The ML decoder is still in the form of (3.1) where the
test statistic is described in (4.3). The test statistic can be expressed in the form of (4.5) with

\[ v = [(1 + Ab)^2 + \sigma_n^2] \sum_{i \in C_p} u_i, \quad y = [(1 + Ab)^2 + \sigma_n^2] \sum_{i \in C_p} w_i \]  

(4.37)

and where random variables \( u_i \) and \( w_i \) have zero mean and unit variance, with \( u_i = x_i / \left[(1 + Ab)^2 + \sigma_n^2\right]^{1/2} \) and \( w_i = x_i / \left[(1 - Ab)^2 + \sigma_n^2\right]^{1/2} \). Since the distribution of the test statistic would be in the form of (4.9), the error probability can be obtained, similar to the noiseless case, in the following form (see Appendix C.6)

\[ P_{e-MSS} = \frac{1}{\left[(1 - D)^2 + 2\sigma_n^2(1 + D) + \sigma_n^4\right]^{N/4}} 2^{N/2} \Gamma^2(N/4) \sum_{k=0}^{n} \left[ \binom{n}{k} \left[ \sum_{i=0}^{2n-k} (-1)^k \binom{2n-k}{i} \right] \frac{2^{n-i}}{(2n-i)!} \left( \frac{(1 - D)^2 + 2\sigma_n^2(1 + D) + \sigma_n^4}{(1 + \sqrt{D})^2 + \sigma_n^2} \right)^{2n-i+1} \right]. \]

(4.38)

For IMSS, referring to (4.3) and (4.36), we can express the test statistic as

\[ z = 2Ab (gx^T s_d x + x^T x + x^T n) + x^T s_d x (1 + A^2 + g^2) + 2x^T x g + (2x^T s_d n + 2g x^T n + n^T s_d n), \]

(4.39)

where the parameter \( \lambda \) is determined by the result of (4.33) where IIR \( \triangleq \hat{P}_{inf}/\hat{P}_{int} \). The information and interference powers in the presence of additional noise regarding the test statistic (4.39) are expressed as

\[ \hat{P}_{inf} = P_{inf} + 4N\sigma_n^2 \left( D - \frac{1}{N} h(2, 1, 0, \lambda) \right), \quad \hat{P}_{int} = P_{int} + 2\sigma_n^2 \left( 2N + 2h(2, 1, 0, \lambda) + N\sigma_n^2 + 4h(1, 0, 1, \lambda) \right) \]

(4.40)

where \( P_{inf} \) and \( P_{int} \) have been defined in (4.31) and (4.32), respectively. Accordingly, the bit error probability of IMSS could be described as in (4.35) with the parameters determined in (C.26)-(C.28), where in (C.26) \( P_{inf} \) and \( P_{int} \) should be replaced by \( \hat{P}_{inf} \) and \( \hat{P}_{int} \), respectively.

### 4.6 Simulation Results

In this section, we conduct extensive simulations to illustrate the decoding performances of the proposed IMSS scheme and to verify the derived error probability analysis. The results are obtained based on Monte Carlo simulations. We set \( N = 60 \) in all simulations, unless stated otherwise.

To validate the derived theoretical PDF for the test statistic \( z \) in (4.34), in Figure 4.5, we can
4.6. Simulation Results

see an excellent matching between the empirical result based on simulations and the theoretical result based on the analysis provided in Section 4.3. To show that the MSS scheme is decoding error free for DWR = 0 dB, the conditional PDF \((C.4)\) of the test statistic \((4.3)\) with \(D = 1\) and \(b = +1\) is depicted in Figure 4.6. It is clear that the PDF is zero for negative \(z\), proving that there is no PDF leakage and thus no decoding error when DWR = 0 dB.

To investigate the validity of the derived error probability in (4.11) for the MSS scheme, the theoretical and experimental results are shown in Figure 4.7, where we see excellent matches between the theoretical results and the ones based on simulations.

For the proposed IMSS in Section 4.4, \(g\) is determined as in (4.17) to achieve decoding error free, and the corresponding distortion can be calculated in (4.26). Figure 4.8 is shown to provide more insight into the required DWR for error free decoding for a fixed number of coefficients \(N\). For example, if \(N = 50\), then if we are allowed to have DWR below 20 dB, the decoder will not make any false decision.

As mentioned in Section 4.4, introducing \(\lambda\) can make a trade off between the allowed distortion and the decoding performance. The parameter \(\lambda\) is determined by maximizing the IIR as (4.30), where a higher IIR value means a more efficient interference host effect rejection. The parameter \(d\) introduced in (4.21) represents the approximation precision of the optimal \(g(u)\), i.e., a higher value of \(d\) leads to a more accurate approximation. The \(10\log(\text{IIR})\) measures for MSS and IMSS with different values of \(d\) are calculated and shown in Figure 4.9. It could be seen that IMSS yields higher IIR values than MSS and that increasing \(d\) could result in more host interference effect rejection as expected.

To compare the decoding performance of the proposed IMSS against the MSS, the bit error rates of MSS and IMSS with \(d = 1\), \(d = 2\), and \(d = 3\) are shown in Figure 4.10, where \(N = 100\). It is clear that IMSS consistently yields better decoding performance than MSS and that employing the IMSS with a higher value of \(d\) could lead to better decoding performance. As the behavior of the IIR for different embedding schemes are demonstrated in Figure 4.9, and the relationship between the IIR and the interference host effect rejection have been explained already, the decoding performances provided in Figure 4.10 are expected. Our simulations show that increasing \(d\) to be larger than 3 does not further improve the decoding performance significantly, so we use \(d\) up to 3 in our simulations. It is worth mentioning that by decreasing the DWR, the free parameter \(\lambda\) can be larger and consequently remove the host effect more. When the allowed distortion reaches the desirable amount shown in Figure 4.8, the IMSS could completely reject the interference host effect and thus be decoding error free for a lower DWR.

To investigate the effect of additional noise on the performance of the proposed IMSS, Figure 4.11 shows that the decoding performance of IMSS and MSS when \(N = 60\) and WNR = 5dB where WNR is defined as WNR = \(10\log \left( \frac{P}{\sigma_n^2} \right)\). This figure depicts that the IMSS consistently
4.7 Conclusion

provides better decoding performances than the MSS in the presence of additional Gaussian noise and also, bigger value of \( d \) results in better performance. Figure 4.12 depicts the theoretical and experimental decoding performance of the IMSS scheme versus different WNRs. This figure shows the integrity of the error analysis for the IMSS in the presence of the noise.

We also conduct experiments to evaluate the proposed embedding scheme on real images. A set of testing images with size 768 \( \times \) 1024 are investigated for information embedding. Since peak signal to noise ratio (PSNR) is a common measurement for evaluating the perceptual quality of the images, the figures are plotted against the PSNR values. Also, we run our algorithm for PSNR of 37 dB for the experiments. For investigating the decoding performance of the proposed IMSS on real images, the average BER for the images is shown in Figure 4.13. It depicts that the IMSS has better performance than the conventional MSS and increasing the parameter \( d \) improves the performance, as we expected. To investigate the decoding performance of the IMSS for real images against the additional noise attack, the average BER curve is shown in Figure 4.14. We can see that the decoding performance of the proposed IMSS outperforms MSS.

The worth mentioning point is that there are two assumptions that are not completely fulfilled when examining real images. The first one is that the distribution of the host signal (e.g., DCT coefficients) does not follow the Gaussian distribution. The second one is that the coefficients are not necessarily IID. To demonstrate the effect of these violations from our assumptions, the empirical error probability (based on real images) is compared with the theoretical one (4.35) in Figure 4.15. One can see that there is a difference between the experimental (based on simulations) and empirical results, which is probably mainly due to non-Gaussian IID samples in real images.

4.7 Conclusion

In this chapter, we first derived the theoretical decoding performance analysis of the conventional MSS embedding scheme. To this end, we provided the theoretical error probability and channel capacity. We also showed that the interference effect of the host signal causes decoding performance degradation in the MSS scheme. Therefore, we proposed an improved MSS scheme by taking advantage of the decoder structure during embedding to remove the host signal interference effect. A thorough theoretical analysis of bit error probability for the proposed IMSS scheme was provided and the simulations were used to validate the derivations. Simulation results showed that the IMSS consistently outperforms the conventional MSS. The decoding performance analysis of the MSS and the IMSS in the presence of additional Gaussian noise were also provided and simulations showed the superiority of the IMSS scheme.
4.7. Conclusion

Figure 4.1: The experimental and theoretical PDFs for the random variable $g$ defined in (4.21), where $N = 60$ and DWR = 21 dB.

Figure 4.2: The PDFs of the first coefficient of the watermarked signal for the proposed IMSS scheme (4.14), where $s_1 b = -1$, $N = 60$ and DWR = 21 dB.

Figure 4.3: The experimental PDF of the test statistic $z$ for the MSS scheme when a binary message is sent, where $N = 100$ and DWR = 23 dB.

Figure 4.4: The experimental PDF of the test statistic $z$ for the IMSS scheme when a binary message is sent, where $N = 100$, DWR = 23 dB, and $d = 2$. 

71
4.7. Conclusion

Figure 4.5: The experimental and theoretical \((4.34)\) distributions for the proposed IMSS scheme, where \(N = 60\), DWR = 21 dB and \(b = +1\).

Figure 4.6: The experimental and theoretical \((C.4)\) distributions for the MSS scheme, where \(N = 60\), DWR = 0 dB and \(b = +1\).

Figure 4.7: The theoretical \((4.11)\) and experimental error probabilities for the MSS scheme where \(N = 60\).

Figure 4.8: The required DWRs for achieving error free decodings in IMSS when different numbers of coefficients are used for embedding.
4.7. Conclusion

Figure 4.9: The $10\log(IIR)$ versus DWR curves for the MSS and IMSS schemes, where three different values of $d$ are considered and $N = 100$.

Figure 4.10: The BER versus DWR curves for the MSS and IMSS schemes when $N = 100$. $d = 1, 2, 3$ are considered in IMSS.

Figure 4.11: The BER versus DWR curves for the MSS scheme and the proposed IMSS scheme, where WNR = 5 dB and $N = 60$.

Figure 4.12: The experimental and theoretical BER versus WNR curves for the IMSS scheme, where DWR = 23 dB, $N = 60$, and $d = 2$.
Figure 4.13: The average BER versus PSNR curves for the MSS and IMSS schemes when applied on real images.

Figure 4.14: The average BER versus WNR curves for the MSS and IMSS schemes when applied on real images.

Figure 4.15: The experimental, theoretical, and empirical BER versus DWR curves for the IMSS scheme where \( d = 2 \).
Chapter 5

Security Analysis of Spread Spectrum Schemes under KMA and KMCA

5.1 Introduction

In this chapter, we present security analysis based on the mutual information measure for ISS, CASS, CAISS, and MSS schemes.

The definition of watermarking security has been evolved during the last two decades in the field of digital watermarking and data hiding. In the literature, people actually referred to different properties of digital watermarking when using the term security.

In early era of watermarking and data hiding, different concepts of watermarking security were used. For instance, the ability of the attacker to extract the hidden message could be defined as a security breach. One thing that was considered as a way of increasing the watermarking security was hiding the location of the embedded information [112, 113]. It is worth mentioning that, in early era of digital watermarking, the issue of watermarking security was mainly discussed and studied in a non-mathematical way and there was lack of quantitative studies for watermarking security.

In recent era, the first rigorous definition of watermark security was proposed in [57]. Kalker defined the watermark security as the inability of the attacker to have access to the original signal. It led researchers to come up with a specific definition of watermark security. In the new watermark security definition, similar to the cryptography concept, it is assumed that the attacker has access to all information except the key and his/her final objective is to estimate it. With this definition and in order to quantify watermark security, different attacks and security measures were proposed in [107].

In this chapter, we employ the Shannon’s framework [108] and therefore use the mutual information between the observations and the signature code given the embedded messages measures the information leakage about the signature code. Since the CASS and CAISS embedding schemes [138] rely not only on the signature code but also on the sign of the correlation
between the host signal and the signature code, to behave as a more powerful attacker, we introduce a new adversary attack, the known message and correlation attack (KMCA), and analyze the security of the CASS and CAISS schemes under KMCA. Later we will show that CASS and CAISS are less secure under the KMCA scenario than the KMA one. In order to illustrate how an adversary could attack the watermarked content by estimating the signature code, we present some practical estimators for different SS schemes and study their corresponding estimation performances to correlate the estimation performance with the security measure. One important issue for any data hiding scheme is the robustness-security trade-off. Robustness shows how accurate an embedding scheme could extract the hidden messages and it is usually evaluated by decoding performance. The robustness-security trade-off implies that generally enhancing one will degrade the other. However, we will show via the simulations that the CAISS scheme could enhance both the security and the robustness simultaneously when compared with the ISS scheme.

The rest of this chapter is organized as follows. In Section 5.2, different SS-based embedding schemes are briefly introduced. Section 5.3 provides the security analysis for the SS embedding schemes under the KMA scenario. In Section 5.4 the KMCA attack is introduced for the CASS and CAISS schemes and the security analysis under this attack is studied. The practical estimators of the signature code for SS schemes are described in Section 5.5. Simulation results are reported and explained in Section 5.6. Section 5.7 draws the conclusions.

5.2 Spread Spectrum Embedding Schemes

In this section, different spread spectrum embedding schemes are presented briefly. Throughout this chapter, it is presumed that the host signal vector with length $N$, $\mathbf{x} = [x_1, x_2, ..., x_N]^T$, conveys one message bit $b$. In addition, it is assumed that the host signal follows Gaussian independent and identical distribution (IID) with zero mean and variance $\sigma_x^2$, i.e., $\mathbf{x} \sim \mathcal{N}(0_N, \sigma_x^2 \mathbf{I}_N)$, where $\mathbf{I}_N$ and $0_N$ mean the $N \times N$ identity matrix and the zero vector with length $N$, respectively. Here, $N$ is the number of the host coefficients conveying one bit information. The SS schemes employ the watermark signature code $\mathbf{s} = [s_1, s_2, ..., s_N]^T$ to embed the message bit $b$. In this chapter, like the other ones, we assume that the signature code consists of binary random variables from the set $s_i \in \{-1, +1\}$. Each embedding scheme introduces a watermark-induced distortion $D$, which is defined as (2.2). Since we will investigate the security of the SS schemes in this chapter, in the following subsections, the SS embedding schemes are briefly reviewed.
5.2. Spread Spectrum Embedding Schemes

5.2.1 Additive SS Scheme

The additive spread spectrum is probably the most popular embedding scheme in the SS category. The additive SS adds the message bit over the host coefficients uniformly, expressed as

\[ y = x + sAb, \]  \hspace{1cm} (5.1)

where \( A > 0 \) is the watermark amplitude. Based on the additive SS embedding scheme (5.1) and the distortion definition (2.2), the amplitude \( A \) could be expressed as \( A = \sqrt{D} \). Additive SS is a non-host rejection scheme due to the interference effect of the host signal.

5.2.2 ISS Scheme

In order to reduce the interference effect of the host signal, Malvar and Florencio [92] proposed the ISS scheme in the following form

\[ y = x + sAb - \lambda ss^T x \]  \hspace{1cm} (5.2)

where \( \lambda \) is a free parameter which can be determined as

\[ \lambda = \begin{cases} \frac{1}{N} & \text{if } D > \frac{\sigma^2}{N}, \\ \frac{D}{\sigma_x^2} & \text{if } D \leq \frac{\sigma^2}{N}. \end{cases} \]  \hspace{1cm} (5.3)

Based on the distortion definition (2.2) and the ISS embedding scheme (5.2), the amplitude \( A \) can be expressed as \( A = \sqrt{D - \lambda^2 N \sigma_x^2} \). It should be recalled that ISS scheme exploits a host rejection procedure which could reduce the host signal’s effect.

5.2.3 CAISSERT Scheme

The main drawback of the SS scheme is the interference effect of the host signal, and ISS was an attempt to reduce this interference effect. Motivated by the success of ISS, in Chapter 3 we introduced the correlation aware concept to remove the interference effect of the host signal more efficiently by determining the embedding based on both the message bit and the correlation between the host signal and the signature code. The correlation aware concept leads to two embedding schemes, the CASS and CAISSERT schemes. The CASS is expressed as:

\[ y = \begin{cases} x + sA_1, & \text{if } s^T x \geq 0, \quad b = +1, \\ x - sA_2, & \text{if } s^T x \geq 0, \quad b = -1, \\ x - sA_1, & \text{if } s^T x < 0, \quad b = -1, \\ x + sA_2, & \text{if } s^T x < 0, \quad b = +1, \end{cases} \]  \hspace{1cm} (5.4)

77
5.3 Security Analysis of SS, ISS, and MSS Schemes under KMA

where the amplitudes \( A_1 = \sqrt{\alpha D} \) and \( A_2 = \sqrt{(2 - \alpha)D} \), with \( 0 < \alpha \leq 1 \).

Since CAISS leads to less probability distribution function (PDF) leakage, it yields better decoding performances than that of ISS. The CAISS scheme is described as follows

\[
y = \begin{cases}
x + sA_1, & \text{if } s^T x \geq 0, \ b = +1, \\
x - sA_2 - \lambda_h s(s^T x), & \text{if } s^T x \geq 0, \ b = -1, \\
x - sA_1, & \text{if } s^T x < 0, \ b = -1, \\
x + sA_2 - \lambda_h s(s^T x), & \text{if } s^T x < 0, \ b = +1,
\end{cases}
\] (5.5)

where \( A_1 = \sqrt{\alpha D}, \ A_2 = \sqrt{D(2 - \alpha) - \lambda^2_h N \sigma_x^2} \), and the parameter \( \lambda_h \) is determined as

\[
\lambda_h = \begin{cases}
\frac{1}{N} \frac{D(2 - \alpha)}{\sigma_x^2}, & \text{if } D > \frac{\sigma_x^2}{N(2 - \alpha)}, \\
D, & \text{if } D \leq \frac{\sigma_x^2}{N(2 - \alpha)},
\end{cases}
\] (5.6)

5.2.4 Multiplicative Spread Spectrum

In order to make the watermark more imperceptible, the MSS scheme can be employed \([28]\). Since the MSS scheme embeds the message bit according to the content of the host signal, it generally yields a content-based watermarked signal. The MSS embedding scheme can be expressed as:

\[
y = x + S_d x Ab
\] (5.7)

where \( S_d \) is a diagonal matrix denoted as \( S_d = diag\{s_1, ..., s_N\} \). According to the distortion definition \((2.2)\) and the MSS scheme \((5.7)\), we have \( A = \sqrt{D/\sigma_x^2} \).

5.3 Security Analysis of SS, ISS, and MSS Schemes under KMA

In the following sections, the security analyses of different SS embedding schemes are investigated. According to \([17]\), one popular scenario for security assessment is known-message attack, where it is assumed that the attacker has access to the embedded messages in the host signal.

In this chapter, we focus on KMA because it has many applications \([108]\) and it generally results in worse information leakage than the watermark only attack (WOA) scenario. Here, we employ the framework used in \([108]\) and \([106], [105]\) for assessing the security of the SS schemes. The information about the signature code leaked out by the observations is quantified by the mutual information between the observations and the signature code \([26]\).
When \( N_0 \) watermarked signals \( Y = [y_1, ..., y_{N_0}] \) which are obtained by watermarking \( N_0 \) host signals \( X = [x_1, ..., x_{N_0}] \), and the associated \( N_0 \)-bit message \( b = [b_1, ..., b_{N_0}]^T \) are observed, the information leakage about the signature code \( s \) could be calculated, as the mutual information between the observations \( Y \) and the signature code \( s \) given the embedded message bits \( b \), in the following form

\[
I(Y; s|b) = h(Y|b) - h(Y|b, s),
\]

(5.8)

where \( I(.) \) and \( h(.) \) denote the mutual information and differential entropy operations, respectively.

As explained earlier, the above Shannon’s mutual information represents the leakage about the signature code from the observations. One could compute Shannon’s equivocation about the signature code given the observations and the embedded message to represent the remaining uncertainty about the signature code. For the KMA scenario, the equivocation defined as \( h(s|Y, b) = h(s) - I(Y; s|b) \) implies the uncertainty of the signature code given observations and message bits.

### 5.3.1 Additive SS Scheme under KMA

Based on the additive SS embedding scheme (5.1), assumed Gaussian distribution of the signature code, the mutual information for the KMA scenario has been obtained in [107]. It is straightforward to show that for the binary signature code, the information leakage could be bounded as

\[
I(Y; s|b)_{SS} \leq \frac{N}{2} \log \left( 1 + \frac{N_0 D}{\sigma_x^2} \right).
\]

(5.9)

The information leakage per dimension for additive SS, defined as \( I(Y; s|b)/N \), reveals that it is independent of the dimension \( N \). Also as we expected, it is clear that increasing the number of observations \( N_0 \) will increase the information leakage.

### 5.3.2 ISS Scheme under KMA

As explained earlier, ISS is a host rejection algorithm. It is known that the decoding performance of ISS is generally better than that of the SS scheme. The security level is another factor that should be considered when comparing SS and ISS schemes. In Appendix D.1, we can show that...
5.4 Security Analysis of CASS and CAISS Schemes under KMCA and KMA

the information leakage for the ISS scheme under the KMA scenario is bounded as:

\[
I(Y; s|b)_{ISS} \leq \frac{N}{2} \log \left( 1 + \frac{(D - \lambda^2 N \sigma^2_x) N_0}{[(1 - \lambda)^2 + (N - 1)\lambda^2]\sigma^2_x} \right) - N_0 \log(1 - \lambda b N) + \frac{NN_0}{2} \log \left( (1 - \lambda)^2 + (N - 1)\lambda^2 \right) - N_0 \log(1 - \lambda h N) + NN_0 \log \left( (1 - \lambda)^2 + (N - 1)\lambda^2 \right). \tag{5.10}
\]

Since SS is a special case of ISS with \( \lambda = 0 \), it is clear that, when \( \lambda = 0 \), the information leakage of the ISS scheme (5.10) is the same as the mutual information of the SS scheme (5.9). From (5.10), we also note that, when \( \lambda \) approaches to \( 1/N \), the information leakage approaches infinity. Different from the additive SS where the information leakage per dimension is independent of \( N \), increasing \( N \) leads to more information leakage per dimension in ISS. In terms of the information leakage per dimension, the behavior of the ISS scheme is affected by several factors such as the distortion \( D \), \( N \) and \( N_0 \), and we will investigate its behavior in Section 5.6.

5.3.3 MSS Scheme under KMA

MSS is another popular SS-based scheme which employs Eqn. (5.7) for data hiding. Referring to MSS embedding in (5.7) and the mutual information definition in (5.8), we can express the upper bound of information leakage of MSS as follows

\[
I(Y; s|b)_{MSS} \leq \frac{N N_0}{2} \log \left( \sigma^2_x + \frac{D}{\sigma^2_x - D} \right). \tag{5.11}
\]

The proof details can be found in Appendix D.5.

From (5.11), we note that, similar to the SS scheme, the information leakage per dimension for MSS is independent of \( N \). On the other hand, in contrary to the SS scheme, the information leakage for MSS has a linear relationship with the number of observations, \( N_0 \). Also, the analysis in (5.11) suggests that the mutual information goes to infinity when DWR tends to be 0 dB, though it is worth mentioning that the DWR is always much higher than 0 dB in practical watermarking applications.

5.4 Security Analysis of CASS and CAISS Schemes under KMCA and KMA

For security analysis of the SS, ISS, and MSS embedding schemes, we can consider the KMA scenario since KMA is a powerful attack for SS, ISS and MSS. However, for the CASS (5.4) and CAISS (5.5) embedding schemes, since both the embedded information bit and the sign of the correlation between the signature code and the host signal are used for embedding, while
the attacker is assumed to only have access to the embedded message bits in KMA, the KMA scenario is not sufficiently powerful. To better understand the security limit of the CASS and CAISS schemes, we therefore need to propose a more powerful attack by taking advantage of the specific properties of CASS and CAISS embedding (e.g., both the embedded bits and the correlation information are explored in CASS and CAISS embedding). More specifically, since both the host signal and the signature code are assumed to be random variables, the sign of their correlation is a random variable as well, we introduce a new attack for the CASS and CAISS schemes, called the known message and correlation attack (KMCA), where the attacker knows not only the information about the embedded messages but also the signs of the correlations between the host signals and the signature code. If the attacker does not know the correlation information, the KMCA is reduced to the conventional KMA. It is worth noting that, since the attacker is assumed to have no access to the signature code, in practice he/she generally has no access to the sign information of the correlation between the host signal and the signature code. Here, we assume that such correlation information is provided to the attacker in KMCA.

5.4.1 CASS and CAISS Schemes under KMCA

Under the KMCA scenario, for $N_0$ watermarked signals $Y = [y_1, ..., y_{N_0}]$, we further assume that the associated $N_0$-bit message $b = [b_1, ..., b_{N_0}]^T$ and the signs of the correlations between the $N_0$ host signals and the signature code are available to the attacker. We can define the information leakage about the signature code as the mutual information between the observation $Y = [y_1, ..., y_{N_0}]$ and the signature code $s$ given $b = [b_1, ..., b_{N_0}]$ and $g = [g_1, ..., g_{N_0}]^T$ as:

$$I(Y; s|b, g) = h(Y|b, g) - h(Y|b, g, s),$$  \hspace{1cm} (5.12)

where the $i$th element of $g$ is defined as the sign of the correlation between the $i$-th host signal vector and the signature code, i.e., $g_i = \text{sign}\{s^T x_i\}$.

In Appendix D.2, we can derive that the information leakage of CAISS under the KMCA scenario is expressed as:

$$I(Y; s|b, g)_{CAISS} \leq -\frac{N_0}{2} \log(1 - \lambda_h N) + N_0 \log(2) + \frac{N}{2} \sum_{i=0}^{N_0} \log \left( (1 - 2\lambda_h + \lambda_h^2 N)^i \left[ 1 + \frac{1}{\sigma_x^2} \left( \frac{i(D(2-\alpha) - \lambda_h^2 N \sigma_x^2)}{1 - 2\lambda_h + \lambda_h^2 N} + (N_0 - i)\alpha D \right) \right] \right) \left( \begin{array}{c} N_0 \\ i \end{array} \right).$$  \hspace{1cm} (5.13)

When $\lambda_h = 0$, CAISS is reduced to the CASS scheme, and the corresponding information leakage
for the CASS embedding can be expressed as:

\[
I(Y; s|b, g)_{CASS} \leq \frac{N}{2} \left( \frac{1}{2} \right)^{N_0} \sum_{i=0}^{N_0} \log \left( 1 + \frac{N_0}{\sigma_x^2} \left( 2i - 2i\alpha + N_0\alpha \right) \right) \left( \begin{array}{c} N_0 \\ i \end{array} \right) + N_0 \log(2). \quad (5.14)
\]

### 5.4.2 CAISS and CASS Schemes under KMA

In this subsection, for considering the security of the CAISS scheme under the conventional KMA scenario, it is assumed that the attacker only has access to the embedded message \( b \). In the previous subsection, the information leakage of the CAISS scheme under KMCA is derived, where the attacker has access to both the embedded message bits \( b \) and the signs of the correlations between the host signals and the signature code. In Appendix D.3 has been shown that the information leakage of the CAISS scheme under the KMA is expressed as

\[
I(Y; s|b)_{CAISS} \leq \frac{NN_0}{2} \log \left( \frac{1}{2} \left( 2 - 2\lambda_h + \lambda_h^2 N \right) + \frac{1}{4\sigma_x^2} \left[ \sqrt{\alpha D} - \sqrt{D(2 - \alpha) + \lambda_h^2 N\sigma_x^2} \right]^2 \right) + \\
\frac{N}{2} \log \left( 1 + \frac{N_0}{\sigma_x^2} \left( 2 - 2\lambda_h + \lambda_h^2 N \right) + \frac{1}{4} \left[ \sqrt{\alpha D} - \sqrt{D(2 - \alpha) - \lambda_h^2 N\sigma_x^2} \right]^2 \right) - \frac{N_0}{2} \log(1 - \lambda_h N). \quad (5.15)
\]

By replacing \( \lambda_h \) with zero in (5.15), the information leakage of the CASS scheme under the KMA is obtained as

\[
I(Y; s|b)_{CASS} \leq \frac{NN_0}{2} \log \left( 1 + \frac{1}{4\sigma_x^2} \left[ \sqrt{\alpha D} - \sqrt{D(2 - \alpha)} \right]^2 \right) + \\
\frac{N}{2} \log \left( 1 + \frac{N_0}{\sigma_x^2} \left[ \sqrt{\alpha D} + \sqrt{D(2 - \alpha)} \right]^2 \right). \quad (5.16)
\]

In order to know the relation between the information leakage of the CASS and CAISS schemes in the KMA and KMCA, in Appendix D.4 it has been shown that

\[
I(Y; s|b)_{CAISS} < I(Y; s|b, g)_{CAISS} \quad , \quad I(Y; s|b)_{CASS} < I(Y; s|b, g)_{CASS}. \quad (5.17)
\]

In (5.17), the left side of the inequalities are the information leakage under the KMA scenario and the right side of the inequalities are the information leakage under the KMCA scenario. Thus, it reveals that the information leakage of the CASS and CAISS schemes under the KMCA is more than the leakage under the KMA scenario. As a result, it suggests that KMCA is a more powerful attack for CAISS and CASS embedding. This phenomenon could be intuitively
explained as follows: When the attacker has access to both the embedded message and the signs of the correlations between the host signals and the signature code, he/she has more information about the signature code when compared with the KMA case where he/she only has access to the embedded message. It is thus expected that there is more information leakage of the signature code under KMCA than under the KMA scenario.

Analytical comparison of the information leakages of the ISS (5.10) and CAISS (5.15) under KMA is complicated and the superiority of one over the other is not clear. Therefore, the behaviors of them will be illustrated through numerical simulations in section 5.6.

The point that should be mention is that for high values of DWR, the exact information leakage of the indicated SS schemes approaches to the provided upper bounds.

### 5.5 Practical Estimators of the Signature Code for SS Schemes

Having analyzed the information leakage of different SS embedding schemes, we proceed to consider the practical estimators of the signature code under the KMA and KMCA scenarios. In practice, to have a practical quantitative understanding of the security level associated with each embedding scheme, one important issue raised regarding the information-theoretic expression of the information leakage is that how well the leaked information can be useful for accurately estimating the unknown signature code. Generally, the accuracy of the estimation depends on the specific signature code estimator and the available information to the attacker. The importance of the first factor is obvious since different estimators could yield different estimation accuracy. The second factor is the available information on the attacker’s side that he could use to estimate the signature code. Such information could include the side information (e.g., the embedded message bits) and the leaked information (e.g., observations of the watermarked signals). For instance, the side information available to the attacker is the embedded messages under KMA, while both the embedded messages and the signs of the correlations between the host signals and the signature code are available under KMCA. Since the attacker in the KMCA has more side information than in the KMA scenario, the attacker is possible to design a more accurate estimator in KMCA than in the KMA scenario. It is important to note the above factors jointly contribute to the overall estimation accuracy, and relying on only one factor could be misleading.

For the additive SS embedding scheme (5.1) under the KMA scenario, it has been in [17] shown that the maximum likelihood (ML) estimator of the signature code $s$ has the following form:

$$\hat{s} = \text{sign}(Y^Tb). \quad \text{(5.18)}$$

For the ISS embedding scheme (5.2) under the KMA scenario, we could not get a closed-
form expression of the ML estimator using \( f(Y|s, b) \), i.e., the PDF of the observations given the signature code and the information bits. Thus, we consider the test statistic of the decoder, i.e., \( z_i = y_i^T s \), which leads to the PDF of the test statistic given the signature code and information bits in the form of \( f(Y^T s|s, b) \). The ML estimator of the signature code based on this PDF has been obtained in [117] under the KMA scenario as:

\[
\hat{s} = \text{sign} \left\{ (YY)^{-1} Y^T b \right\}.
\]  

(5.19)

For the MSS embedding scheme (5.7) under the KMA scenario, we show in Appendix D.6 that the ML estimator can be expressed as:

\[
\hat{s} = \text{sign} \left\{ \frac{1}{\sigma^2} \sum_{i=1}^{N_0} (Y_i \odot Y_i)b_i - (1 + \frac{D}{\sigma^2})(1^T b)1 \right\},
\]  

(5.20)

where \( 1 = [1, \ldots, 1]^T \) and \( \odot \) denotes the element by element multiplication operation.

For the CAISS embedding scheme (5.5) under the KMCA scenario, we could not get a closed form solution of the ML estimator of the signature code. In order to find a practical and efficient estimator, we propose exploring the constrained least squares estimation. Based on the CAISS embedding (5.5) and the test statistic at the decoder side (\( z_i = y_i^T s \)), we can define a cost function as

\[
J = \sum_{i \in \{N_2, N_4\}} (y_i^T s - NA_2 b_i)^2 + \sum_{i \in \{N_1, N_3\}} (y_i - sA_1 b_i)^T (y_i - sA_1 b_i),
\]  

(5.21)

where \( N_1, N_2, N_3, \) and \( N_4 \) are the subsets of the signal indices where \( s^T x > 0 \) and \( b = 1 \), \( s^T x < 0 \) and \( b = 1 \), \( s^T x < 0 \) and \( b = -1 \), and \( s^T x > 0 \) and \( b = -1 \), respectively. With some simplifications, we show that the estimator can be obtained by solving the following minimization problem,

\[
\hat{s} = \underset{s}{\text{argmin}} \left( \frac{1}{2} s^T Q s + c^T s \right) \quad , \quad \text{subject to} \quad Hs \leq p,
\]  

(5.22)

where

\[
Q = \sum_{i \in \{N_2, N_4\}} y_i y_i^T + 2A_1^2 I, \quad c = - \sum_{i \in \{N_2, N_4\}} NA_2 y_i b_i - \sum_{i \in \{N_1, N_3\}} A_1 y_i b_i
\]

\[
H = [-Y_{N_1}^T; Y_{N_2}^T; Y_{N_3}^T; -Y_{N_4}^T], \quad p = [-NA_1 1_{1 \times N_1} - NA_1 1_{1 \times N_3} NA_2 1_{1 \times N_2} NA_2 1_{1 \times N_4}]^T.
\]  

(5.23)
where \( l_{N_1}, l_{N_2}, l_{N_3}, \) and \( l_{N_4} \) are the numbers of the observations within the subsets \( N_1, N_2, N_3, \) and \( N_4, \) respectively. In addition, \( Y_{N_1}, Y_{N_2}, Y_{N_3}, \) and \( Y_{N_4} \) are the matrices containing the observations in the subsets \( N_1, N_2, N_3, \) and \( N_4, \) respectively. It should be mentioned that the constraints represented above are the results of the a priori information about the signs of the correlations between the host signals and the signature code. In order to explain it, the test statistic at the decoder side (\( z_i = y_i^T s \)) according to the embedding scheme (5.5) should be considered. Regarding the test statistic and for different subsets of the observations, we should have \( Y_{N_1}^T s > NA_1 1_{l_{N_1} \times 1}, Y_{N_2}^T s < -NA_1 1_{l_{N_1} \times 1}, \) and \( Y_{N_2}^T s < NA_2 1_{l_{N_2} \times 1}. \) The matrix form of these constraints can be expressed in (5.22) and (5.23).

For the CAISS embedding scheme (5.5) under the KMA scenario, since information about the correlations between the signature code and the host signals is not available to the attacker, there is no closed-form solution for the ML estimator. With only the embedded message bits are available to the adversary, we can employ a heuristic cost function as:

\[
J = \sum_{i=1}^{N_0} [(y_i - sA_1 b_i)^T (y_i - sA_1 b_i) + (y_i - sA_2 b_i)^T (y_i - sA_2 b_i)].
\]

It leads to a practical estimator for the CAISS scheme under the KMA scenario, which has the form of (5.18).

In order to find an estimator for the CASS scheme (5.4) under the KMCA scenario, similar to the CAISS case, we propose exploring the constrained least squares estimation. Based on the CASS scheme (5.4), we define a cost function as:

\[
J = \sum_{i \in \{N_2, N_4\}} (y_i - sA_2 b_i)^T (y_i - sA_2 b_i) + \sum_{i \in \{N_1, N_3\}} (y_i - sA_1 b_i)^T (y_i - sA_1 b_i).
\]

We can show that minimizing this cost function subject to the constraints related to the available correlation information can be formulated as a constrained minimization problem as in (5.22), where \( Q = [(l_{N_1} + l_{N_3}) A_1^T + (l_{N_2} + l_{N_4}) A_2^T] I, \)
\( c = -0.5 \sum_{i \in \{N_2, N_4\}} A_2 y_i b_i - 0.5 \sum_{i \in \{N_1, N_3\}} A_1 y_i b_i, \) and \( H \) and \( p \) are defined the same as (5.23).

For the CASS scheme under the KMA scenario, since information about the correlations between the signature code and the host signals are not available, similar to the CAISS case, we employ the estimator in the form of (5.18).

The performance of the estimators described above will be investigated next in section 5.6.

### 5.6 Results and Discussions

In this section, we first investigate the information leakage behaviors of different SS schemes presented in Sections 5.3 and 5.4 and their information leakages are compared under the KMA and KMCA scenarios. Further, the performances of the estimators of the signature code described in Section 5.5 are presented and compared.
5.6. Results and Discussions

5.6.1 On the Theoretical Security Results

In general, for different SS schemes, we note that the mutual information security measure is a function of several factors including DWR, $N$, and $N_0$. We therefore investigate the effects of different factors on the security of the SS schemes. The information leakage per dimension plots are reported in this section.

First, we compare the information leakage per dimension for the SS (5.9) and ISS (5.10) schemes. Figure 5.1 reports the effects of DWR on the information leakage per dimension result for different values of $N$ when $N_0 = 100$. Our theoretical analysis reveals that the information leakage per dimension for the SS scheme is independent of the dimension of the received signal $N$, and this conclusion is supported by Figure 5.1. We also observe that the ISS scheme always yields higher information leakage than that of the SS scheme, and increasing $N$ leads to higher information leakage in ISS. From our previous analysis of information leakage for the ISS scheme in Section 5.3, we note that when $\lambda$ tends to $1/N$, the information leakage theoretically goes to infinity. Intuitive explanation of this behavior could shed some lights on different behaviors of the SS and ISS schemes. This observation can be explained by exploiting the decoder structure of the ISS scheme: To decode the embedded message bits, the decoders for the SS, ISS, and CAISS schemes all use a test statistic as $z = y^T \cdot s$ where $z$ follows Gaussian distribution with fixed variance for the SS scheme for all DWR values. For the ISS scheme, the test statistic $z$ follows a Gaussian distribution whose variance depends on the parameter $\lambda$. When $\lambda$ gradually approaches $1/N$, the variance of $z$ becomes smaller and smaller and its PDF is squeezed more and more. This is indeed the motivating idea behind the host rejection of ISS which tries to squeeze the distribution of the test statistic $z$ as much as possible to avoid PDF leakage and thus improve the decoding performance. Once $\lambda$ is $1/N$, the test statistic $z$ becomes a deterministic value $NAb$. Therefore, suppose the attacker tries to estimate the signature code when $\lambda = 1/N$ based on $N_0$ observations. He could verify the estimated signature code by multiplying the estimate with the observations to check whether the result is equal to $NAb$ or not. In other words, the security level of ISS is very low $\lambda = 1/N$ while when the parameter $\lambda$ is less than $1/N$, the test statistic $z$ is a random variable, not a fixed deterministic value. The above discussion clearly shows that there is a trade-off between the security level and decoding performance for the ISS scheme: On one hand, approaching $\lambda$ to $1/N$ can avoid PDF leakage and improve the decoding performance; On the other hand, less PDF leakage makes the attack (estimating the signature code) simpler and more efficient. The SS scheme does not exploit any host rejection method and thus less information leaks out from the watermarked observations. However, though SS’s security level is higher than that of ISS, its decoding performance is generally worse than that of ISS.

Figure 5.2 investigates the effects of the number of observations $N_0$ on the information leakage
5.6. Results and Discussions

per dimension. As expected, increasing the number of observations leads to more information leakage for both SS and ISS schemes. In other words, when more watermarked observations are available, the attacker could estimate the signature code more accurately. Different DWRs are studied in Figure 5.2, where a smaller DWR yields more information leakage. This behavior is expected because a smaller DWR means larger watermark. We also note from Figure 5.2 that the difference between the leakages for the ISS scheme at different DWRs is larger than that of the SS scheme. This is because, as the DWR decreases, the parameter $\lambda$ in the ISS scheme is closer to $1/N$ which causes more information leakage. Decreasing the DWR in the SS scheme does not have such PDF squeezing effect on the test statistic and therefore the difference between the information leakages of the SS scheme at different DWRs is smaller than in the ISS scheme.

Both the CASS and CAISS embedding schemes contain the parameter $\alpha$, which affects the security measure under the KMA scenario. To investigate the effects of $\alpha$, with DWR = 25 dB and $N = 100$, Figure 5.3 shows the upper bound of information leakage of the CAISS scheme when employing different values of $\alpha$ (5.15), and the results are compared with the information leakage of ISS under the KMA scenario (5.10). It is clear that the information leakage of the CAISS scheme changes as a function of the parameter $\alpha$. As $\alpha$ increases, the information leakage of CAISS decreases and can be smaller than that of ISS. It is worth recalling that, for all values of $\alpha$, the CAISS scheme consistently provides a better decoding performance than that of ISS.

We now try to intuitively explain the security behavior of CAISS when different $\alpha$ is employed. Similar to the ISS case, exploiting the test statistic of the decoder could help explain the information leakage behavior of CAISS. Recalling the embedding structure of the CAISS scheme in (5.5), it is noted that the CAISS scheme is a combination of the SS and ISS schemes according to the correlation between the host signal and the watermark signature code. This conditional embedding of the CAISS scheme has two effects: On one hand, since $\lambda_h$ is always greater than or equal to $\lambda$, CAISS results in more host rejection than that of ISS. In other words, when $b = 1$ and $x^T s < 0$, or when $b = -1$ and $x^T s > 0$, CAISS squeezes the PDF of the test statistic more than ISS does and thus CAISS could result more information leakage than ISS. However, on the other hand, when $b = 1$ and $x^T s > 0$, or when $b = -1$ and $x^T s < 0$, CAISS employs SS embedding (i.e., no PDF squeezing occurs) and thus CAISS in these two situations results in less information leakage than ISS. In summary, the total information leakage for the CAISS scheme is contributed by the above two opposite cases. The parameter that could adjust the overall information leakage is $\alpha$. More specifically, a smaller value of $\alpha$ results in a larger $\lambda_h$ which leads to more host rejection and thus more information leakage. A larger value of $\alpha$ results in a smaller $\lambda_h$ which leads to less host rejection and thus less information leakage. Therefore, a larger $\alpha$ could result in a CAISS scheme which is more secure than ISS. Since
CAISS consistently outperforms ISS for all values of $\alpha$, it means that with certain $\alpha$, CAISS can be both more secure and provide better decoding performance than ISS. It suggests that one could design an embedding scheme (such as CAISS) which could enhance the security and robustness at the same time.

The important observation of Figure 5.3 is that the information leakage of the CAISS scheme could be less than its counterpart in ISS scheme under the KMA scenario. Since CAISS has better decoding performance than the ISS, it reveals that it is possible to design an embedding scheme which could enhance the decoding performance and security at the same time.

In order to get some rough idea about the information leakage of the CASS and CAISS schemes under the KMA and KMCA scenarios, Figure 5.4 is presented. It depicts the upper bounds of the CASS and CAISS scheme under the KMCA (5.13)-(5.14) and KMA (5.15)-(5.16) scenarios when $DWR = 25$ dB, $\alpha = 0.8$, and $N = 100$. We could see that upper bounds under the KMCA are above the bounds under the KMA scenario as we expected. Thus, from this figure it could be implied that the KMCA is a more powerful attack than the KMA one for the CASS and CAISS schemes.

Figure 5.5 shows the information leakage per dimension plots for the MSS scheme when $N = 100$. It could be seen from this figure that, as we expected, the information leakage increases when the DWR decreases.

To compare the information leakages of different SS schemes under the KMA scenario, Figure 5.6 is reported where $DWR = 25$ dB, $N = 100$, and $\alpha = 0.8$. It can be seen from this figure that the SS scheme has slightly less information leakage than the CASS scheme. It is also observed that MSS has the most information leakage, and ISS and CAISS lie between. To illustrate that the security behaviors of the SS schemes are complicate and affected by factors such as DWR, we consider a different DWR setting. Keeping $N$ and $\alpha$ be the same as in Figure 5.6, Figure 5.7 reports the information leakage plots of different SS schemes when $DWR = 21$ dB. In this figure, CASS and SS still yields the comparable, least information leakage, while MSS leads to less information leakage than ISS and CAISS has the most leakage. In summary, we could see that the SS and CASS schemes generally yield the least information leakage, however, the security comparisons between other SS schemes are parameter dependent.

5.6.2 On the Practical Estimators

As a practical assessment of the security levels of different SS schemes, we now investigate the estimation performances of the signature code estimators for different SS schemes described in Section 5.5. The performances of the estimators are evaluated based on the absolute value of the normalized correlation between the real and estimated signature codes. The performances of these estimators under the KMA scenario are shown in Figure 5.8 where $N = 100$ and DWR
= 25 dB. From this figure, we can see that the signature code estimator of MSS outperforms that of ISS, and the estimator of ISS generally outperforms that of SS. These observations are consistent with Figure 5.6 where the leakage of the MSS is more than that of the ISS and SS schemes. Figure 5.9 shows the results under the same settings except that DWR = 21 dB. We can see that in this case the estimator of ISS yields the best estimation performance, followed by that of MSS and SS (together with CASS and CAISS). This is consistent with Figure 5.7 where the ISS and CASS schemes have the most and least leakages under the KMA scenario, respectively. From this figure, we can see that the performances of the estimators of the SS, CASS, and CAISS schemes are very close to each other.

In order to investigate the performances of the proposed signature code estimators of the CASS and CAISS schemes under the KMCA scenario, Figure 5.10 is illustrated. It shows that the estimator of the CAISS scheme yields better performance than that of CASS. This observation is also consistent with Figure 5.4 which shows more information leakage of CAISS. Comparing Figure 5.8 and Figure 5.10 we note that the performances of the signature code estimators of the CASS and CAISS schemes under the KMCA scenario are better than the corresponding estimators under the KMA scenario. This could be because of the additional information (correlations between the host signals and the signature code) provided to the attacker under KMCA and thus KMCA is more powerful than KMA.

5.6.3 Important Observations

It has been proved that when \( \alpha < 1 \), the CASS and CAISS schemes yield better decoding performances than that of the SS and ISS ones. From Figures 5.8 and 5.9 one could see that the performance of estimators in the SS and CASS schemes are almost the same. In addition, we could observe that the estimator in the ISS scheme could end up with better accuracy than the CAISS scheme. It implies that ISS could have more information leakage than the CAISS scheme. Therefore, it is possible to design an embedding scheme (e.g., CAISS) which not only improves the decoding performance but also decreases the information leakage.

One point that should be taken into account is that even though the KMCA scenario was proposed for CASS and CAISS embedding scheme, it is possible that attacker uses this attack for obtaining information about the signature code for other SS schemes such as SS and ISS. Investigating the SS under the KMCA is straightforward because when \( \alpha = 1 \) the CASS scheme becomes SS scheme. Thus, we could use the estimator for CASS scheme under the KMCA when \( \alpha = 1 \). In order to get estimator of the ISS under the KMCA, we follow the approach that was used to obtain the estimator for CAISS scheme. Following (5.21), we could employ the cost function

\[
J = \sum_{i=1}^{N_0} (y_i^T s - N A_2 b_i)^2.
\]

It leads to the constrained minimization (5.22) where

\[
Q = \sum_{i=1}^{N_0} y_i y_i^T + 2 A^2 I, \quad c = -\sum_{i=1}^{N_0} N A y_i b_i, \quad p = N A [ -1_{1 \times N_1} - 1_{1 \times N_3} 1_{1 \times N_2} 1_{1 \times N_4} ]^T,
\]

and
5.6. Results and Discussions

Figure 5.1: Upper bounds of information leakage per dimension versus DWR for SS and ISS schemes under the KMA scenario, when $N_0 = 100$.

Figure 5.2: Upper bounds of information leakage per dimension versus $N_0$ for SS and ISS schemes under the KMA scenario, when $N = 100$.

$\mathbf{H}$ has the form of (5.23). It should be recalled that $A$ is the watermark amplitude in the ISS scheme.

Figure 5.11 depicts the performance of the signature code estimators for the SS, ISS, CASS, and CAISS schemes under the KMCA scenario. The first point that is observed is that the estimator for the SS scheme is better than its counterpart for CASS scheme. The other observed point is that the performance of the estimator for CAISS scheme, depending on $\alpha$, could be better or worse than its counterpart for ISS scheme. Therefore, this figure leads us to the conclusion that while the CASS and CAISS schemes have better decoding performance than the SS and ISS schemes could be more secure as well.
5.6. Results and Discussions

Figure 5.3: Upper bounds of information leakage per dimension versus $N_0$ for the ISS and CAISS schemes under the KMA scenario, when DWR = 25 dB and $N = 100$.

Figure 5.4: Upper bounds of information leakage per dimension versus $N_0$ for CASS and CAISS schemes under KMA and KMCA scenarios when DWR = 25 dB, $N = 100$, and $\alpha = 0.8$.

Figure 5.5: Upper bounds of information leakage per dimension versus $N_0$ plots for the MSS scheme under the KMA scenario, when $N = 100$.

Figure 5.6: Upper bounds of information leakage per dimension versus $N_0$ for the SS, ISS, and MSS, CASS, and CAISS schemes under the KMA scenario, when DWR = 25 dB, $N = 100$, and $\alpha = 0.8$. 
5.6. Results and Discussions

Figure 5.7: Upper bounds of information leakage per dimension versus $N_0$ for the SS, ISS, CASS, and CAISS schemes under the KMA scenario, when DWR = 21 dB, $N = 100$, and $\alpha = 0.8$.

Figure 5.8: Performance illustrations of different estimators of the signature code under KMA: The average normalized correlation between the estimated and actual signature codes versus $N_0$ plots for the SS, ISS, MSS, CASS, and CAISS schemes, when DWR = 25 dB, $N = 100$, and $\alpha = 0.8$.

Figure 5.9: Performance illustrations of different estimators of the signature code under KMA: The average normalized correlation between the estimated and actual signature codes versus $N_0$ plots for the SS, ISS, MSS, CASS, and CAISS schemes, when DWR = 21 dB, $N = 100$, and $\alpha = 0.8$.

Figure 5.10: Performance illustrations of different estimators of the signature code under KMA and KMCA: The average normalized correlation between the estimated and actual signature codes versus $N_0$ plots for the CASS and CAISS schemes, when DWR = 25 dB, $N = 100$, and $\alpha = 0.8$. 
5.7 Conclusion

By exploiting Shannon’s mutual information between the watermarked observations and the signature code given the embedded message bits, we provided the security analysis of the SS-based embedding schemes, including ISS, MSS, CASS, and CAISS schemes. More specifically, we derived the upper bound of information leakage about the signature code from the observations under the KMA scenario. To better understand the security behavior of the CASS and CAISS schemes, a more powerful attack, the known message and correlation attack, was introduced in this chapter. We proved that, measured by the information leakage measure, the information leakage of the CASS and CAISS schemes under the KMCA is more than the counterparts in the KMA scenario which implies that KMCA is a more powerful attack for the correlation-aware schemes. We also described several estimators of the signature code for different embedding schemes, and we investigated the estimation accuracy of the signature code estimators. We used the simulation to show that for some values of $\alpha$, the CAISS has less information leakage than its counterpart ISS scheme, while CAISS generally provides better decoding performances than that of ISS. This observation suggests that it is possible to design an embedding scheme (such as CAISS scheme) which could both enhance the decoding performance and the security level.

Figure 5.11: Performance illustrations of different estimators of the signature code under KMCA: The average normalized correlation between the estimated and actual signature codes versus $N_0$ plots for the SS, ISS, CASS, and CAISS schemes, when DWR = 25 dB, $N = 100$. 

93
Chapter 6

Thesis Summary and Future Research Topics

In this chapter, in Section 6.1, we summarize our results and highlight the contributions of this thesis. Then, in Section 6.2, we point out some directions for future research.

6.1 Summary of Results

This thesis focused on different SS embedding schemes for data hiding, named as the additive SS, ISS, and MSS. We investigated these SS embedding schemes, and further developed improved SS schemes to improve the decoding performances.

In Chapter 2, we proposed modified SS and ISS embedding schemes for embedding in the DFT magnitude domain. We then presented the optimal decoders for the corresponding schemes in the DCT and DFT magnitude domains. Based on the decoder structures, we presented decoding performance analysis of the SS and ISS schemes in these domains. Experimental results showed that in the absence of additional attack and having access to the watermark amplitude, embedding in the magnitude of DFT domain ends up with better decoding performance. In addition, in order to have a more practical decoders which do not need watermark amplitude at the cost of performance degradation, suboptimal decoders of LOD and LMMSE were proposed. Experimental results showed that suboptimal decoders in the DCT domain are preferred to their counterparts in the magnitude of DFT domain. Moreover, LMMSE decoder provides better performance than the LOD.

In Chapter 3, we introduced the concept of correlation-and-bit-aware for additive SS schemes. We showed that exploiting the information about the correlation of the host signal and signature code could help removing the interference effect of the host signal more effectively. Based on this concept, we proposed CASS and CAISS embedding schemes. Through theoretical error probability analysis, we proved that the CASS scheme outperforms SS scheme and CAISS scheme outperforms SS and ISS schemes. Simulation results showed that the CAISS scheme could improve the decoding performance significantly. Furthermore, we proved that using CASS and CAISS schemes could increase the payload compared with traditional SS schemes. In order to
have a comprehensive investigation on the CASS and CAISS schemes, their theoretical error probability in the presence of additional noise was derived and the simulation results depicted the superiority of the proposed schemes over the traditional ones.

In Chapter 4, we presented the theoretical performance analysis of the MSS scheme. We showed that even though the MSS scheme could provide a content based watermark, it suffers from interference effect of the host signal and this is the cause of its performance degradation. We exploited the decoder structure in order to come up with the MSS-based scheme which could remove the interference effect efficiently. Based on this idea, we proposed IMSS which could improve the decoding performance greatly. We showed that IMSS uses some available information, such as correlation between the host signal and the signature code and correlation of the host signal with itself, at the encoder side to remove the host effect and improve the performance. We also presented the theoretical decoding performance of the IMSS scheme in the presence of additional noise and ran the simulations for showing the superiority of the proposed IMSS over the conventional one.

In Chapter 5, we exploited Shannon’s mutual information to study the security of the SS schemes. More specifically, we provided upper bounds of information leakage for the ISS, MSS, CASS, and CAISS schemes under the KMA scenario. Since the CASS and CAISS schemes use the correlation between the host signal and signature code, we proposed the KMCA scenario. We showed that KMCA is a more powerful attack than the KMA and could provide more information about the signature code for the attacker. In order to provide some practical understanding of the information leakage, we presented some signature code estimators that could be exploited by the attacker in the KMA and KMCA scenarios. We showed that it is possible to tune the parameters in the CAISS scheme to have less leakage than the ISS one. It implies that it might be possible to design an embedding scheme to improve the decoding performance and enhance the security at the same time.

6.2 Future Work

In the following, we propose some ideas for further research that can be accomplished based on the work of this thesis.

6.2.1 Correlation-and-Bit-Aware Concept for IMSS Scheme

In Chapter 4, we considered the MSS scheme and proposed the IMSS scheme to improve the decoding performance. The proposed IMSS scheme reduces the interference effect of the host signal to improve the decoding performance. However, it is possible that we could further remove the host signal effect more efficiently. In Chapter 5, we introduced the correlation-and-bit-aware
concept which helps removing the interference effect by splitting the PDF of the test statistic at the decoder side. CASS and CAISS were designed by exploiting the decoder structure and the correlation-and-bit-aware concept. We could apply the same correlation-and-bit-aware concept to remove the host signal in IMSS more effectively. More specifically, since we have access to the decoder structure of the IMSS and the message bits at the encoder side, it is possible to develop two modified MSS-based schemes, similar to CASS and CAISS, which can remove the host effect and improve the decoding performance.

6.2.2 New Security Measure Exploiting the Decoder Structure

In Chapter 5, we considered the security of the SS schemes using the mutual information between the observations and the signature code. Since the observations represent the embedding scheme, the mutual information based security analysis only exploits the embedding side information. We know that there is also a relationship between the extracted bits and the decoder, since the decoder by invoking the signature code could extract the hidden bits correctly. On the other hand, in the KMA, the attacker has access to the embedded bits. Therefore, the attacker could examine the integrity of the signature code by employing it in the decoder structure. Therefore we could see that the decoder also could play an important role for watermarking security attack. The current security measure, i.e., Shannon’s mutual information, does not exploit the decoder structure. We believe that proposing a security measure which could exploit both the embedding side and the decoder side structures may lead to more meaningful watermarking security analysis. Since the test statistic comprises both the observations and the decoder structure, it might be used to define a security measure that takes into account both sides of embedding and decoding. More specifically, one such measure could include the mutual information between the test statistic at the decoder side and the signature code.

6.2.3 Data Hiding in the Encrypted Domain

Although this thesis focused on data hiding as a post-decryption protection scheme, there are some applications that data hiding alone is not sufficient. For instance, there are military and medical applications that we need to have a confidential transmission and thus cryptography is necessary. Therefore, it is interesting to develop a joint cryptography - data hiding system which could protect the contents from unauthorized parties. The encryption side of the system scrambles the data to make it unreadable for unauthorized parties and thus can provide pre-delivery protection and the data hiding side could provide post-delivery protection. This ensemble protection system has attracted research attentions recently [14]. This system should be able to embed a message in the encrypted domain such that the corresponding decrypted domain contains the message. It could help to enhance the security of the applications where the
6.2. Future Work

content should be processed by a non-trusted third party. One application for data hiding in the encrypted domain is for buyer-seller watermarking protocols [94] which prevents the seller from obtaining the watermarked copy of the buyer. The content containing the buyer’s watermark can not be distributed illegally to the third parties by the seller. We plan to pursue this direction by developing a joint cryptography - data hiding system by incorporating the ideas proposed in this thesis.
Bibliography


Appendix A

Corresponding Proofs for Chapter 2

A.1 Derivations for SS Analysis in the DFT Domain

Referring to expression (2.8), assuming the independent and identical distribution of the coefficients, we have the joint PDF of the host data as

\[ f(x) = \exp\left\{-\sum_{i=1}^{N} \left(\frac{|x_i|}{\eta_i}\right)^{\gamma_i}\right\} \prod_{i=1}^{N} \left[\left(\frac{\gamma_i}{\eta_i}\right)^{\gamma_i-1} u(x_i)\right]. \]  \hspace{1cm} (A.1)

Based on the ML decoder structure (2.9), it decides \( \hat{b} = +1 \) if

\[ \frac{f(r|b = +1)}{f(r|b = -1)} = \frac{\exp\left\{-\sum_{i=1}^{N} \left(\frac{|r_i-s_iA|}{\eta_i}\right)^{\gamma_i}\right\} \prod_{i=1}^{N} \left(\frac{\gamma_i}{\eta_i}\right)^{\gamma_i-1} u(r_i-s_iA)}{\exp\left\{-\sum_{i=1}^{N} \left(\frac{|r_i+s_iA|}{\eta_i}\right)^{\gamma_i}\right\} \prod_{i=1}^{N} \left(\frac{\gamma_i}{\eta_i}\right)^{\gamma_i-1} u(r_i+s_iA)} > 1. \]  \hspace{1cm} (A.2)

It is straightforward to see that the (A.2) leads to (2.12).

In order to derive the error probability, first we show that the test statistic used for decoding could be modeled as Gaussian random variable. Taking logarithm from both sides of (2.12) leads to \( \hat{b} = \text{sign}\{z\} \). Doing some manipulations on test statistic \( z \) when \( r_i > A \) results

\[ z = \sum_{i=1}^{N} \left[\left(\frac{|r_i+s_iA|}{\eta_i}\right)^{\gamma_i} - \left(\frac{|r_i-s_iA|}{\eta_i}\right)^{\gamma_i} + (\gamma_i-1) \ln\left(\frac{r_i-s_iA}{r_i+s_iA}\right)\right]. \]  \hspace{1cm} (A.3)

It is noted that the test statistic (A.3) is the sum of \( N \) random variables, which with the assumption of independent host signal samples and with the knowledge of signature codes, by employing the central limit theorem, it could be approximated as a normal random variable. Assuming that the signature code accepts values \(+1\) and \(-1\) with the equal probability, one could show that the conditional PDFs of the test statistic are approximately symmetric and expressed as \( f_Z(z|b = +1) = N(m_z, \sigma_z^2) \) and \( f_Z(z|b = -1) = N(-m_z, \sigma_z^2) \) where \( m_z \) and \( \sigma_z^2 \) represent the mean and the variance of the test statistic. Therefore, assuming the equal prior probability for the information bit, the probability of error can be expressed as (2.13) where \( \text{erfc}(x) = \frac{2}{\sqrt{\pi}} \int_{x}^{\infty} e^{-t^2} dt \) is the complementary error function. Since the test statistic is symmetric
A.2 Derivations for ISS Analysis in the DFT Domain

In order to obtain the ML decoder, the conditional distribution of the received signal \( r \) should be exploited. To do so, it is straightforward to show that the distribution of the vector \( r \) regarding (2.3) could be given by

\[
f(r) = \frac{1}{|M|} f_x(M^{-1}(r - sA b)), \tag{A.4}
\]

where \( M \) is defined as \( M = I - \lambda s s^T \).

Exploiting the ML criterion (2.9) and Weibull distribution (2.8) lead to decoder which decides \( \hat{b} = +1 \) when the following inequality holds

\[
\frac{f_R(r|b = +1)}{f_R(r|b = -1)} = \frac{\exp\left\{-\sum_{i=1}^{N} \left( \frac{|m_i(r-sA)|}{\eta_i} \right)^{\gamma_i} \right\} \prod_{i=1}^{N} \left[ \left( \frac{\gamma_i}{\eta_i^{\gamma_i}} \right) \left( |m_i(r-sA)| \right)^{\gamma_i-1} u(r_i - s_iA + \lambda s_i s^T x) \right]}{\exp\left\{-\sum_{i=1}^{N} \left( \frac{|m_i(r+sA)|}{\eta_i} \right)^{\gamma_i} \right\} \prod_{i=1}^{N} \left[ \left( \frac{\gamma_i}{\eta_i^{\gamma_i}} \right) \left( |m_i(r+sA)| \right)^{\gamma_i-1} u(r_i + s_iA + \lambda s_i s^T x) \right]} > 1. \tag{A.5}
\]

where \( m_i \) is the \( i \)th row of \( M^{-1} \). It is straightforward to show that (A.5) results (2.18). □

In order to obtain the error probability, first by applying some simplifications, decoder (A.5) turns to \( \hat{b} = \text{sign}\{z\} \). Then, the test statistic is expressed as follows

\[
z = \sum_{i=1}^{N} \left[ \left( \frac{|m_i(r+sA)|}{\eta_i} \right)^{\gamma_i} - \left( \frac{|m_i(r-sA)|}{\eta_i} \right)^{\gamma_i} \right] + (\gamma_i - 1) \ln \left( \frac{|m_i(r-sA)|}{|m_i(r+sA)|} \right). \tag{A.6}
\]

Similar to the justification brought in Appendix A.1, the error probability could be expressed in the form of \( \text{erfc} \) function. Without loss of generality it is assumed that \( b = 1 \), and thus, it is straightforward to have the mean and mean of the square of the test statistic (A.6) as (2.19) and (2.20).

A.3 Derivations for ISS Analysis in the DCT Domain

For obtaining the optimal ML decoder, we should first obtain the PDF of the vector \( t \) defined in (2.4). To this end, the PDF of generalized Gaussian is rewritten in the following vector form

\[
f(x) = \frac{\lambda^N}{\prod_{i=1}^{N} \sigma_{x_i}} \exp\left\{- \left[ \sqrt{\frac{\Gamma(\frac{3}{c})}{\Gamma(\frac{1}{c})}} \left\| x^T R_x^{-\frac{1}{2}} \right\|_{\frac{1}{c}} \left\| R_x^{-\frac{1}{2}} x \right\|_{\frac{1}{c}} \right] \right\}, \tag{A.7}
\]
where
\[
\bar{\lambda} = \frac{c}{2\Gamma\left(\frac{1}{c}\right)} \sqrt{\frac{\Gamma\left(\frac{3}{c}\right)}{\Gamma\left(\frac{1}{c}\right)}}.
\] (A.8)

and \( \mathbf{R}_x = \text{diag}\{\sigma_{x_1}^2, \sigma_{x_2}^2, \ldots, \sigma_{x_l}^2\} \). In addition, we define \( \| [a_1, a_2, \ldots, a_N] \|_c = \| [a_1]^c, [a_2]^c, \ldots, [a_N]^c \|_c \).

Regarding to the ISS signal model (2.3), it is shown [103] that the PDF of \( t \) can be expressed as
\[
f(t) = \frac{\bar{\lambda}^N}{|M| \prod_{i=1}^{N} \sigma_{x_i}} \exp\left\{ -\left[ \sqrt{\frac{\Gamma\left(\frac{2}{3}\right)}{\Gamma\left(\frac{2}{4}\right)}} \right] \left[ t^T \mathbf{M}^{-1} \mathbf{R}_x^{-\frac{1}{2}} \right] \left[ \left| \mathbf{R}_x^{\frac{1}{2}} \mathbf{M}^{-1} \right|_2 \right] \right\}.
\] (A.9)

Then, likelihood ratio for ISS (2.3) leads the decoder decides \( \hat{b} = +1 \) when
\[
\frac{f(r|b = +1)}{f(r|b = -1)} = \frac{\exp\left\{ -\left[ (r - s \mathbf{A})^T \mathbf{M}^{-1} \mathbf{R}_x^{-\frac{1}{2}} \right] \left[ \left| \mathbf{R}_x^{\frac{1}{2}} \mathbf{M}^{-1} (r - s \mathbf{A}) \right|_2 \right] \right\}}{\exp\left\{ -\left[ (r + s \mathbf{A})^T \mathbf{M}^{-1} \mathbf{R}_x^{-\frac{1}{2}} \right] \left[ \left| \mathbf{R}_x^{\frac{1}{2}} \mathbf{M}^{-1} (r + s \mathbf{A}) \right|_2 \right] \right\}} > 1.
\] (A.10)

Having accomplished some algebraic simplifications, the test statistic of the ML decoder for ISS embedding scheme is obtained as (2.23).

**A.4 Derivations for LOD Analysis in the DCT Domain**

To derive the LOD for ISS in the DCT domain, the test statistic (2.23) should be rewritten in a more tractable form. After some algebraic manipulations, we have the following form of the test statistic
\[
z = \sum_{i=1}^{N} \left[ \frac{\mu s_i \sum_{j \neq i} s_j r_j + (1 + \mu)r_i + (N\mu + 1)s_i \mathbf{A}}{\sigma_{x_i}} \right]^c - \left[ \frac{\mu s_i \sum_{j \neq i} s_j r_j + (1 + \mu)r_i - (N\mu + 1)s_i \mathbf{A}}{\sigma_{x_i}} \right]^c.
\] (A.11)
Taking the derivative of above expression results

\[
z = \sum_{i=1}^{N} \frac{c}{\sigma_{x_i}} (N\mu + 1)s_i \left[ \mu s_i \sum_{j \neq i} s_j r_j + (1 + \mu)r_i + (N\mu + 1)s_i A \right]^{(c-1)} \text{sign} \left\{ \mu s_i \sum_{j \neq i} s_j r_j + (1 + \mu)r_i + (N\mu + 1)s_i A \right\} + \\
\sum_{i=1}^{N} \frac{c}{\sigma_{x_i}} (N\mu + 1)s_i \left[ \mu s_i \sum_{j \neq i} s_j r_j + (1 + \mu)r_i - (N\mu + 1)s_i A \right]^{(c-1)} \text{sign} \left\{ \mu s_i \sum_{j \neq i} s_j r_j + (1 + \mu)r_i - (N\mu + 1)s_i A \right\}.
\]

By replacing \( A = 0 \) into (A.12) and regarding the Taylor series (2.26), the optimal decoder is obtained as (2.30).
Appendix B

Corresponding Proofs for Chapter 3

B.1 Proof of Proposition 1

For CASS to have better decoding performance than that of SS, the error probability of the CASS scheme should always be smaller than that of SS. In other words, we should have

\[ Q\left(\frac{N\sqrt{2D - A_1^2}}{\sqrt{N\sigma^2_x}}\right) < Q\left(\frac{N\sqrt{D}}{\sqrt{N\sigma^2_x}}\right). \]  

(B.1)

Since \(Q(.)\) is a monotonic decreasing function, to satisfy aforementioned expression, we need to show that \(\sqrt{2D - A_1^2} > \sqrt{D}\). It is pretty straightforward to show that it requires \(0 < A_1 < \sqrt{D}\). From (3.15), it is obvious that this constraint is always satisfied. Therefore, it is concluded that the CASS always outperforms the SS scheme in decoding performance.

B.2 Derivation of Optimal Decoder for CAISS Scheme

The optimal decoder minimizing the error probability \(P_e = Pr\{\hat{b} \neq b\}\) is obtained by the maximum likelihood (ML) criterion. The ML estimate \(\hat{b}\) is expressed as

\[ \hat{b} = \arg\max_{b \in \{\pm 1\}} f_R(r|b, s), \]  

(B.2)

where \(f_R(r|b, s)\) represents the conditional PDF of \(r\) given the bit message, amplitudes, and the signature code. Therefore, the decoder decides \(\hat{b} = +1\) if

\[ f_R(r|b = +1, s) > f_R(r|b = -1, s). \]  

(B.3)

It is clear that the conditional PDFs are needed to obtain the decision rule. Assuming that the host signal coefficients are Gaussian IID with zero-mean and variance \(\sigma^2_x\), we can show that
the conditional PDFs regarding the CAISS embedding in (3.29) are in the following form

\[ f_R(r|b = +1, s) = \frac{1}{2(\sqrt{2\pi\sigma_x^2})^N} \exp \left\{ \frac{-1}{2\sigma_x^2} (r - sA_1)^T (r - sA_1) \right\} + \frac{1}{2 |M| (\sqrt{2\pi\sigma_x^2})^N} \exp \left\{ \frac{-1}{2\sigma_x^2} (r - sA_2)^T M^{-2} (r - sA_2) \right\}, \quad (B.4) \]

\[ f_R(r|b = -1, s) = \frac{1}{2(\sqrt{2\pi\sigma_x^2})^N} \exp \left\{ \frac{-1}{2\sigma_x^2} (r + sA_1)^T (r + sA_1) \right\} + \frac{1}{2 |M| (\sqrt{2\pi\sigma_x^2})^N} \exp \left\{ \frac{-1}{2\sigma_x^2} (r + sA_2)^T M^{-2} (r + sA_2) \right\}, \quad (B.5) \]

where

\[ M = I_N - \lambda h ss^T, \quad (B.6) \]

and \(|.|\) denotes the determinant operator. By plugging the conditional PDFs (B.4) and (B.5) into the decoder in (B.3), with some calculations, we have that the decoder decides \( \hat{b} = +1 \) if

\[
\exp \left\{ \frac{2r^T sA_1}{\sigma_x^2} \right\} + \frac{1}{|M|} \exp \left\{ \frac{r^T (A_1 I_N + A_2 M^{-2}) s}{\sigma_x^2} - \frac{r^T (M^{-2} - I_N) r}{2\sigma_x^2} - \frac{s^T (A_2^2 M^{-2} - A_1^2 I_N) s}{2\sigma_x^2} \right\} > 1 + \frac{1}{|M|} \exp \left\{ \frac{r^T (A_1 I_N - A_2 M^{-2}) s}{\sigma_x^2} - \frac{r^T (M^{-2} - I_N) r}{2\sigma_x^2} - \frac{s^T (A_2^2 M^{-2} - A_1^2 I_N) s}{2\sigma_x^2} \right\}.
\]

(B.7)

Now, we want to show that if \( r^T s \) is positive then the above inequality holds. If \( r^T s > 0 \), then the first term in the left hand side of (B.7) would be larger than one. To show that the second term in the left side is larger than the second term in the right side of inequality (B.7), we need to prove that

\[ r^T (A_1 I_N + A_2 M^{-2}) s > r^T (A_1 I_N - A_2 M^{-2}) s. \]

(B.8)

With (B.6) and using Woodbury equation, we have

\[ M^{-2} = I_N + \beta ss^T, \quad (B.9) \]

where

\[ \beta = \alpha^2 N - 2\eta \quad \text{and} \quad \eta = \frac{1}{N - \frac{1}{\lambda h}}. \quad (B.10) \]
Therefore, with (B.9) and (B.10), now (B.8) becomes
\[ r = A_1 + A_2(1 + \beta N) > r = A_1 - A_2(1 + \beta N). \] (B.11)

To satisfy (B.11), the parameter \(1 + \beta N\) is required to always be positive. It is easy to show that \(1 + \beta N = (\alpha N - 1)^2\) and thus is always positive.

Therefore, the decoder decides \(\hat{b} = +1\) when \(r > 0\). Similarly, we can show that the decoder decides \(\hat{b} = -1\) when \(r < 0\). We thus conclude that the optimal decoder is the correlator defined in (3.1) with the test statistic \(z\) in (3.2).

### B.3 Proof of Proposition 2

To compare the proposed CAISS scheme with the ISS scheme, we recall that the error probability of the ISS \([92]\) can be obtained as
\[
P_{e-ISS} = Q\left(\frac{N\sqrt{D - \lambda^2 N\sigma_x^2}}{\sqrt{N\sigma_x^2(1 - \lambda N)^2}}\right),
\] (B.12)
where
\[
\lambda = \begin{cases} 
\frac{1}{N}, & \text{if } D > \frac{\sigma^2}{\sigma_x^2} \\
\frac{D}{\sigma_x^2}, & \text{if } D \leq \frac{\sigma^2}{\sigma_x^2}
\end{cases}
\] (B.13)

To prove that the proposed CAISS provides a better decoding performance, referring to the error probabilities in (3.37) and (B.12), we should prove that
\[
\frac{D - \lambda^2 N\sigma_x^2}{(1 - \lambda N)^2} \leq \frac{2D - A_1^2 - \lambda_h^2 N\sigma_x^2}{(1 - \lambda_h N)^2}. 
\] (B.14)

We can show that (B.14) can be equivalently expressed as \(g \geq 0\) where
\[
g = \lambda^2(2DN^2 - A_1^2N^2 + N\sigma_x^2) - \lambda_h^2(N\sigma_x^2 + DN^2) + \lambda(2A_1^2N - 4DN) + 2\lambda_hDN \\
+ 2\lambda \lambda_h N^2 \sigma_x^2(\lambda_h - \lambda) + (D - A_1^2). \] (B.15)

With \(\lambda_h\) in (3.38) and \(\lambda\) in (B.13), three cases may occur: the first one is when \(D \leq \frac{\sigma^2 + A_1^2 N}{2N}\); the second one is when \(\frac{\sigma_1^2 + A_1^2 N}{2N} < D \leq \frac{\sigma^2}{N}\); and the third one is when \(D > \frac{\sigma^2}{N}\). We now prove the inequality in (B.14) for each of the three cases.

**Case I:** With \(D \leq \frac{\sigma^2 + A_1^2 N}{2N}\), referring to (3.38) and (B.13), we have \(\lambda_h = (2D - A_1^2)/\sigma_x^2\) and \(\lambda = D/\sigma_x^2\). So, we have \(g = 2N^2(D - A_1^2)(D - \frac{A_1^2 + \sigma^2}{2N})(D - \frac{\sigma^2}{2N})\). Based on the assumption that
\( D \leq \frac{\sigma^2 + A_1^2 N}{2N} \) and the fact that \( 0 < A_1 < \sqrt{D} \), it could be concluded that \( g \geq 0 \) and thus the inequality in (B.14) holds for Case I.

**Case II:** With \( \frac{\sigma^2 + A_1^2 N}{2N} < D \leq \frac{\sigma^2}{N} \), referring to (3.38) and (B.13), we have \( \lambda_h = 1/N \) and \( \lambda = D/\sigma_x^2 \). So, now \( g \) in (B.15) becomes \( g = 2N^2(D - \frac{\sigma^2 + A_1^2 N}{2N})(D - \frac{\sigma^2}{N})^2 \). Based on the assumption on \( D \) in this case, we can see that \( g \geq 0 \) and thus the inequality (B.14) is hold for Case II.

**Case III:** With \( D > \frac{\sigma^2}{N} \), referring to (3.38) and (B.13), we have \( \lambda_h = 1/N \) and \( \lambda = 1/N \). It is straightforward to show that \( g = 0 \) for this case.

Based on the above three cases, we can conclude that \( g \geq 0 \) and thus the CAISS embedding scheme has better decoding performance than the ISS scheme.

## B.4 Proof of Proposition 3

To prove that \( \text{IRIF}_{\text{CAISS-ISS}} < 1 \), referring to (3.45), it is equivalently to show that \( h \geq 0 \) with

\[
\begin{aligned}
h &= \lambda_h^2(-DN^2 + 2\lambda N^2\sigma_x^2 - N\sigma_x^2) - \lambda_h(2N^2\lambda^2\sigma_x^2 + 2ND) + \\
&\quad \lambda^2\sigma_x^2N + 2N^2D\lambda^2 - N^2A_1^2\lambda^2 + D - 4ND\lambda + 2NA_1^2\lambda + A_1^2.
\end{aligned}
\]  

(B.16)

We need to prove \( h \geq 0 \) for two cases as follows.

**Case I:** In this case, it is assumed that \( D \leq \frac{\sigma^2 + A_1^2 N}{2N} \) and thus \( \lambda_h = \frac{2D - A_1^2}{\sigma_x^2} \). We now can write \( h \) as

\[
h = -(D - \frac{\sigma^2 + A_1^2 N}{2N})g(A_1),
\]

(B.17)

where

\[
g(A_1) = A_1^2(4\lambda N^2\sigma^2 - 2DN^2 - 2N\sigma^2) + 2\lambda^2N^2\sigma^4 - 8DN^2\sigma^2\lambda + 4D^2N^2 + 2DN\sigma^2.
\]

To prove \( h \geq 0 \), it is equivalent to prove that \( g(A_1) \) is positive. From (B.18), it is noticed that \( g(A_1) \) is a quadratic function in the form of \( g(A_1) = aA_1^2 + c \). Therefore, to prove that \( g(A_1) \) is positive, we need to show that both \( g(0) \) and \( g(\sqrt{D}) \) are positive. For \( A_1 = 0 \), we can write \( g(0) = f(\lambda) = 2\lambda^2N\sigma^4 - 8DN\sigma^2\lambda + 4D^2N + 2D\sigma^2 \). Since \( f(\lambda) \) is a quadratic convex function, to show that it is always positive, it is equivalent to prove that \( f(\lambda) \) has no real root. Referring to \( f(\lambda) \), we have \( \Delta = (4DN\sigma^4)^2 - 4(2N^2\sigma^4)(4D^2N + 2D\sigma^2) = 4DN\sigma^4(2DN - \sigma^2) \). Since it is assumed \( D \leq \frac{\sigma^2 + A_1^2 N}{2N} \) and \( A_1 = 0 \), we have \( D < \frac{\sigma^2}{2N} \). Therefore the discriminator \( \Delta \) is negative and consequently \( f(\lambda) \) and \( g(0) \) are positive.

It is pretty straightforward to show that we have \( g(\sqrt{D}) = 2(\lambda N\sigma^2 - DN)^2 \), which is positive always. Therefore we complete the proof that \( h \geq 0 \) for Case I.
Case II: $D > \frac{\sigma_x^2 + A_1^2}{2N}$ is assumed for Case II and thus $\lambda_h = \frac{1}{N}$. Therefore, referring to (3.45), we have $h > 0$ where $h = (1 - \lambda N)^2(2D - A_1^2 - \frac{\sigma_x^2}{N})$.

### B.5 Proof of Proposition 4

In order to derive PIF, let denote $M = N_{ISS}$ and $N = N_{CAISS}$ for simplicity. Assuming an equal error probability for the CAISS and ISS schemes, referring to (3.37) and (B.12), we have

$$\frac{M(D - \lambda^2 M\sigma_x^2)}{(1 - \lambda M)^2} = \frac{N(2D - A_1^2 - \lambda_h^2 N\sigma_x^2)}{(1 - \lambda_h N)^2}. \tag{B.19}$$

The above expression can be rewritten as

$$M^2(-\lambda^2 \sigma_x^2 + 2\lambda_h N\lambda^2 \sigma_x^2 - 2ND\lambda^2 + N A_1^2 \lambda^2) + M(D + D\lambda_h^2 N^2 - 2\lambda_h ND + 4ND\lambda - 2NA_1^2 \lambda - 2\lambda_h^2 N^2 \sigma_x^2) - 2ND + NA_1^2 + \lambda_h^2 N^2 \sigma_x^2 = 0 \tag{B.20}$$

Two cases are proved here to complete the proof this proposition.

**Case I:** $\lambda_h = (2D - A_1^2)/\sigma_x^2$ and $\lambda = D/\sigma_x^2$ are assumed for Case I. Based on these assumptions and (B.20), we can have PIF as in (3.49) and thus $\text{PIF}_{CAISS-ISS} > 1$.

**Case II:** We have $\lambda_h = 1/N$ for Case II. To have (B.20) still holds, $\lambda$ should tend to be $1/M$. Referring to (3.38) and (B.13), it could be seen that we should have $M = (2 - \alpha)N$ which implies the PIF expression as in (3.49).

### B.6 Derivation of Optimal Decoder for CAISS Scheme in the Presence of Noise

We can show that the PDF of the received signal model in Eqn. (3.50) has the following form

$$f_R(r|b = +1, s) = \frac{1}{2(\sqrt{2\pi\sigma_x^2})^N} \exp \left\{ -\frac{1}{2\sigma_x^2} (r - sA_1)^T(r - sA_1) \right\} + \frac{1}{2\sqrt{(2\pi\sigma_x^2)^N|C_y|}} \exp \left\{ -\frac{1}{2} (r - sA_2)^T C_y^{-1} (r - sA_2) \right\}, \tag{B.21}$$
B.7. Derivation of Equation (3.52)

\[ f_R(r|b = -1, s) = \frac{1}{2(\sqrt{2\pi}\sigma_x^2)^N} \exp \left\{ -\frac{1}{2\sigma_x^2} (r + sA_1)^T (r + sA_1) \right\} + \frac{1}{2\sqrt{(2\pi\sigma_x^2)^N |C_y|}} \exp \left\{ -\frac{1}{2} (r + sA_2)^T C_y^{-1} (r + sA_2) \right\}, \tag{B.22} \]

where

\[ C_y = \sigma_n^2 I_N + M^2 \sigma_x^2. \tag{B.23} \]

By plugging (B.21) and (B.22) into (B.3), we can show that the optimal decoder decides \( \hat{b} = +1 \) if \( r^T C_y^{-1} s > 0 \). Referring to (B.23) and Woodbury equation, the aforementioned decision expression changes to \( (r^T s) / ((\lambda h N - 1)^2 + \sigma_x^2 \sigma_n^2) > 0 \). Since the denominator is positive, the decision rule becomes the correlator defined in (3.2).

B.7 Derivation of Equation (3.52)

We let \( v = w + x \) where \( x = s^T n \) and \( w = s^T x, w > 0 \). It can be shown that the distribution of \( v \) could be obtained as

\[ f_V(v) = B_1 + B_2 = \int_0^\infty (2\pi N \sigma_n^2)^{\frac{1}{2}} \exp \left\{ -\frac{(v - y)^2}{2N \sigma_n^2} \right\} \left(2\pi N \sigma_x^2\right)^{\frac{1}{2}} \exp \left\{ -\frac{y^2}{2N \sigma_x^2} \right\} dy + \int_{-\infty}^0 \left(2\pi N \sigma_n^2\right)^{\frac{1}{2}} \exp \left\{ -\frac{(v + y)^2}{2N \sigma_n^2} \right\} \left(2\pi N \sigma_x^2\right)^{\frac{1}{2}} \exp \left\{ -\frac{y^2}{2N \sigma_x^2} \right\} dy. \tag{B.24} \]

Because of the symmetric characteristics of the integrals \( B_1 \) and \( B_2 \), we have \( B_1 = B_2 \). We can show that \( B_2 \) has the following form

\[ B_2 = (4\pi^2 N^2 \sigma_n^2 \sigma_x^2)^{\frac{1}{2}} \exp \left\{ -\frac{v^2}{2N(\sigma_n^2 + \sigma_x^2)} \right\} \int_{-\infty}^{\frac{v \sigma_x}{\sigma_n \sqrt{N(\sigma_n^2 + \sigma_x^2)}}} \exp \left\{ -\frac{(\sigma_n^2 + \sigma_x^2)t^2}{2N \sigma_n^2 \sigma_x^2} \right\} dt. \tag{B.25} \]

Using the definition of \( Q \) function and combining (B.24) and (B.25), we have the distribution of \( v \) as

\[ f_V(v) = \frac{2}{\sqrt{2\pi N(\sigma_n^2 + \sigma_x^2)}} \exp \left\{ -\frac{v^2}{2N(\sigma_n^2 + \sigma_x^2)} \right\} \left[ 1 - Q\left( \frac{v \sigma_x}{\sigma_n \sqrt{N(\sigma_n^2 + \sigma_x^2)}} \right) \right]. \tag{B.26} \]

Therefore, regarding the test statistic (B.25) and above expression, we have the conditional PDF \( f_Z(z|s^T x > 0, b = 1) \).
B.8 Derivation of Equation (3.56)

Referring to the distributions in (3.52)-(3.55) and the probability of error expressed in (3.11), we can calculate the bit error probability of CAISS in the presence of additional Gaussian noise as

\[
P_{e-CAISS} = \int_{-\infty}^{-N_{A1}} \frac{1}{\sqrt{2\pi N(\sigma_n^2 + \sigma_x^2)}} \exp \left\{ \frac{-z^2}{2N(\sigma_n^2 + \sigma_x^2)} \right\} \left[ 1 - Q\left( \frac{z\sigma_x}{\sqrt{N(\sigma_n^2 + \sigma_x^2)}} \right) \right] dz + \int_{N_{A2}}^{\infty} \frac{1}{\sqrt{2\pi N(\sigma_n^2 + \sigma_x^2)}} \exp \left\{ \frac{-z^2}{2N(\sigma_n^2 + \sigma_x^2)} \right\} \times \\
\left[ 1 - Q\left( \frac{z\sigma_x(1 - \lambda_h N)}{\sigma_n \sqrt{N(\sigma_n^2 + \sigma_x^2)(1 - \lambda_h N)^2}} \right) \right] dz.
\]

(B.27)

It should be noted that the second and the fourth terms of (3.11) are no longer zero and thus also contribute to decoding errors. The error probability could be rewritten in the following form

\[
P_{e-CAISS} = -\int_{-\infty}^{-N_{A1}} \frac{1}{\sqrt{2\pi N(\sigma_n^2 + \sigma_x^2)}} \exp \left\{ \frac{-z^2}{2N(\sigma_n^2 + \sigma_x^2)} \right\} Q\left( \frac{z\sigma_x(1 - \lambda_h N)}{\sigma_n \sqrt{N(\sigma_n^2 + \sigma_x^2)(1 - \lambda_h N)^2}} \right) dz + \\
\int_{-\infty}^{-N_{A2}} \frac{1}{\sqrt{2\pi N(\sigma_n^2 + \sigma_x^2)}} \exp \left\{ \frac{-z^2}{2N(\sigma_n^2 + \sigma_x^2)(1 - \lambda_h N)^2} \right\} \\
\left[ 1 - Q\left( \frac{z\sigma_x(1 - \lambda_h N)}{\sigma_n \sqrt{N(\sigma_n^2 + \sigma_x^2)(1 - \lambda_h N)^2}} \right) \right] dz + Q\left( \frac{N_{A1}}{\sqrt{N(\sigma_n^2 + \sigma_x^2)}} \right).
\]

(B.28)

It is worth mentioning that the error probability in (B.28) does not have a closed form expression and should be calculated numerically. To simplify the calculation, an approximation for \( Q \) function can be used. Using the approximation in [56], we have the following

\[
P_{e-CAISS} \approx Q\left( \frac{N_{A1}}{\sqrt{N(\sigma_n^2 + \sigma_x^2)}} \right) + Q\left( \frac{N_{A2}}{\sqrt{N(\sigma_n^2 + \sigma_x^2)(1 - \lambda_h N)^2}} \right) - \int_{-\infty}^{-N_{A1}} \frac{1}{\sqrt{2\pi N(\sigma_n^2 + \sigma_x^2)}} \times \\
\exp \left\{ \frac{-z^2}{2N(\sigma_n^2 + \sigma_x^2)} \right\} \left[ 1 - \exp \left\{ \frac{-z^2 \sigma_x^2}{2\sigma_n^2 N(\sigma_n^2 + \sigma_x^2)} \right\} \sum_{n=1}^{n_a} c_n \left( -1 \right)^{n-1} \left( \frac{\sigma_x(1 - \lambda_h N)}{\sigma_n \sqrt{N(\sigma_n^2 + \sigma_x^2)(1 - \lambda_h N)^2}} \right)^{n-1} z^{n-1} \right] dz - \\
\int_{N_{A2}}^{\infty} \frac{1}{\sqrt{2\pi N(\sigma_n^2 + \sigma_x^2)}} \exp \left\{ \frac{-z^2}{2N(\sigma_n^2 + \sigma_x^2)(1 - \lambda_h N)^2} \right\} \\
\left[ 1 - \exp \left\{ \frac{-z^2 \sigma_x^2}{2\sigma_n^2 N(\sigma_n^2 + \sigma_x^2)} \right\} \sum_{n=1}^{n_a} c_n \left( -1 \right)^{n-1} \left( \frac{\sigma_x(1 - \lambda_h N)}{\sigma_n \sqrt{N(\sigma_n^2 + \sigma_x^2)(1 - \lambda_h N)^2}} \right)^{n-1} z^{n-1} \right] dz,
\]

(B.29)
where $c_n = \frac{(-1)^{n+1}(1.98)^n}{1.135 \sqrt{\pi} (\sqrt{2})^{n+1} n!}$. The parameter $n_a$ determines the approximation accuracy, i.e., a higher value of $n_a$ means a more accurate approximation of $Q$ function. Without loss of generality, $n_a$ is assumed to be odd and consequently the error probability in (B.29) has the closed form expression as (3.56).
Appendix C

Corresponding Proofs for Chapter 4

C.1 Derivation of Error Probability of the MSS Embedding Scheme

To obtain the error probability in (4.4) for the ML decoder (3.1), we can rewrite it in terms of the test statistic \( z \) as \( P_{e-MSS} = Pr\{z < 0|b = +1\} \). To calculate the probability of error, the conditional PDF of \( z \) which causes error, i.e., \( f_Z(z|b = +1, z < 0) \), can be derived as

\[
f_Z(z|b = +1, z < 0) = \frac{1}{(1 - A^2)^{N/4}2^{N/4}2\Gamma^2(N/4)} \exp \left\{ -\frac{z}{2(1 + A)^2} \right\} \times 
\int_{-\infty}^{\infty} (zy + y^2)^{N/4 - 1} \exp \left\{ -\frac{-y(1 + A^2)}{(1 - A^2)^2} \right\} dy.
\] (C.1)

To find a closed form result for the above integral, for simplicity, we assume that \( N \) is a multiple of 4. Before calculating the integral expressed in (C.1), we provide two useful equations:

\[
\int (\tau^2 - t\tau)^n \exp(\beta \tau)d\tau = \sum_{k=0}^{n} \binom{n}{k} (-t)^k \int \tau^{2n-k} \exp(\beta \tau)d\tau,
\] (C.2)

\[
\int \tau^p \exp(\beta \tau)d\tau = \exp(\beta \tau) \sum_{i=0}^{p} (-1)^i \tau^{p-i} \binom{p}{i} i!(\frac{1}{\beta})^{i+1},
\] (C.3)

where \( n \) and \( p \) are non-negative integers, and (C.2) can be obtained using the binomial formula. Using (C.2) and (C.3), we can rewrite (C.1) as

\[
f_Z(z|b = +1, z < 0) = \frac{1}{(1 - A^2)^{N/4}2^{N/4}2\Gamma^2(N/4)} \exp \left\{ -\frac{z}{2(1 + A)^2} \right\} \times 
\sum_{k=0}^{M} \binom{M}{k} z^k \exp \left\{ \frac{(1 + A^2)z}{(1 - A^2)^2} \right\} \left[ \sum_{i=0}^{2M-k} (-1)^{i-k} z^{2M-k-i} \binom{2M-k}{i} i! \left[ \frac{(1 - A^2)^2}{(1 + A)^2} \right]^{i+1} \right],
\] (C.4)

where \( M = N/4 - 1 \).
C.2. Derivation of Capacity of the MSS Embedding Scheme

Based on the error probability expression and the above conditional PDF (C.4), we have

\[ P_{e-MSS} = \int_{-\infty}^{0} f(z|b = +1, z < 0)dz = \frac{1}{(1 - A^2)^{N/22N/2\Gamma^2(N/4)}} \times \sum_{k=0}^{M} \binom{M}{k} (-1)^{i-k} \left[ \sum_{i=0}^{2M-k} \binom{2M-k}{i} i! \left( \frac{(1 - A^2)^2}{1 + A^2} \right)^{i+1} \left( \int_{-\infty}^{0} z^{2M-i} \exp \left\{ \frac{z}{2(1 - A^2)} \right\} dz \right) \right] \]  

(C.5)

In watermarking, it is more convenient to express the error probability in terms of the watermark-induced distortion rather than the watermark amplitude. The watermark-induced distortion is defined as

\[ D = E \left\{ \| r - x \|^2 \right\} / N \]

where \( E\{\cdot\} \) means the expectation operator. To facilitate the further discussions, we also define the document to watermark ratio (DWR) as DWR = 10 log \( \left( \sigma^2_x \right) \). Since the power of the host signal is assumed to be one, in our case, we have DWR = -10 log \( D \).

For MSS in (4.1), since the host signal is assumed to have unit variance, the distortion for the MSS scheme equals to the square of the watermark amplitude, i.e., \( D = A^2 \). Employing the equation (C.3), we can show that the probability of error for MSS, in terms of the distortion, is expressed as (4.11).

C.2 Derivation of Capacity of the MSS Embedding Scheme

Since the MSS scheme (4.1) assumes Gaussian distribution of the host signal, the watermarked signal follows the Gaussian distribution under reasonably high DWR. We can show that the power of each element \( r_i \) is \( E\{r_i^2\} = (1 + D) \). Therefore we have the differential entropy as

\[ h(r) = \frac{N}{2} \log_2 \left( 2\pi e \right) . \]  

(C.6)

Similarly, the conditional differential entropy could be written as

\[ h(r|b) = - \sum_{b\in\{-1,+1\}} P(b) \int f_R(r|b) \log(f_R(r|b))dr, \]  

(C.7)

where \( P(b) = 0.5 \). For MSS, we have

\[ f_R(r|b) = \frac{1}{|I_N + S_d Ab|} f_X \left( (I_N + S_d Ab)^{-1} r \right), \]  

(C.8)

where \(|\cdot|\) denotes the determinant operator. Substituting (C.8) into (C.7), we can have

\[ h(r|b) = \frac{N}{2} \log_2 \left( (2\pi e)|1 - D| \right). \]  

(C.9)
Therefore, using expressions (C.6) and (C.9), we have the channel capacity for MSS embedding as (4.13).

### C.3 Derivation of Equation (4.24)

Based on the definition of \( g(u) \) in (4.21), \( H(m, n, q, u) \) in (4.22) could be written as

\[
H(m, n, q, u) = \sum_{k_1=1}^{d} \ldots \sum_{k_m=1}^{d} (-u)^{(\sum_{i=1}^{m} k_i)} \left( \frac{\prod_{r=k_1}^{k_m} \prod_{j=0}^{r-1} \left( \frac{1}{2} - j \right)}{\prod_{i=1}^{m} k_i!} \right) \left( \frac{(x^T S_d x)^p}{(x^T x)^l} \right), \tag{C.10}
\]

where the parameters \( p \) and \( l \) are defined as in (4.23). Since \( h(m, n, q, u) \) is defined as the expectation of \( H(m, n, q, u) \), we have

\[
h(m, n, q, u) = \sum_{k_1=1}^{d} \ldots \sum_{k_m=1}^{d} \left[ (-u)^{(\sum_{i=1}^{m} k_i)} \left( \frac{\prod_{r=k_1}^{k_m} \prod_{j=0}^{r-1} \left( \frac{1}{2} - j \right)}{\prod_{i=1}^{m} k_i!} \right) \left( \frac{(x^T S_d x)^p}{(x^T x)^l} \right) \right], \tag{C.11}
\]

Since the signature code \( s \) contains equal elements of +1 and -1, we have

\[
(x^T S_d x)^p = \left( \sum_{i \in C_p} x_i^2 - \sum_{i \in C_n} x_i^2 \right)^p = \sum_{k=0}^{p} \left( \begin{array}{c} p \\ k \end{array} \right) (-1)^k \left( \sum_{i \in C_p} x_i^2 \right)^{p-k} \left( \sum_{i \in C_n} x_i^2 \right)^{k}, \tag{C.12}
\]

where the binomial formula has been used to obtain this equality. Therefore, we have

\[
E \left\{ \frac{(x^T S_d x)^p}{(x^T x)^l} \right\} = \sum_{k=0}^{p} \left( \begin{array}{c} p \\ k \end{array} \right) (-1)^k E \left\{ \left( \sum_{i \in C_p} x_i^2 \right)^{p-k} \left( \sum_{i \in C_n} x_i^2 \right)^{k} / \left( \sum_{i=1}^{N} x_i^2 \right)^l \right\}. \tag{C.13}
\]

Since \( \sum_{i \in C_p} x_i^2 \) and \( \sum_{i \in C_n} x_i^2 \) follow chi-square distributions, it could be shown that \( \left( \sum_{i \in C_p} x_i^2 \right) / \left( \sum_{i=1}^{N} x_i^2 \right) \) and \( \left( \sum_{i \in C_n} x_i^2 \right) / \left( \sum_{i=1}^{N} x_i^2 \right) \) are independent of \( \left( \sum_{i=1}^{N} x_i^2 \right) \). Thus, we have

\[
E \left\{ \frac{\left( \sum_{i \in C_p} x_i^2 \right)^{p-k} \left( \sum_{i \in C_n} x_i^2 \right)^{k}}{\left( \sum_{i=1}^{N} x_i^2 \right)^l} \right\} = E \left\{ \left( \sum_{i \in C_p} x_i^2 \right)^{p-k} \left( \sum_{i \in C_n} x_i^2 \right)^{k} \right\} E \left\{ \left( \sum_{i=1}^{N} x_i^2 \right)^{p-l} \right\}. \tag{C.14}
\]
Also, based on the stated fact, we have

\[
E \left\{ \left( \sum_{i \in C_p} x_i^2 \right)^{p-k} \left( \sum_{i \in C_n} x_i^2 \right)^k \right\} = E \left\{ \left( \frac{\sum_{i \in C_p} x_i^2}{\sum_{i=1}^N x_i^2} \right)^{p-k} \left( \frac{\sum_{i \in C_n} x_i^2}{\sum_{i=1}^N x_i^2} \right)^k \right\} E \left\{ \left( \frac{\sum_{i=1}^N x_i^2}{\sum_{i=1}^N x_i^2} \right)^p \right\} \quad \text{(C.15)}
\]

Substituting (C.15) into (C.14) and using the fact that \( \sum_{i \in C_p} x_i^2 \) and \( \sum_{i \in C_n} x_i^2 \) are independent, we have

\[
E \left\{ \frac{\left( \sum_{i \in C_p} x_i^2 \right)^{p-k} \left( \sum_{i \in C_n} x_i^2 \right)^k}{\left( \sum_{i=1}^N x_i^2 \right)^l} \right\} = E \left\{ \left( \frac{\sum_{i \in C_p} x_i^2}{\sum_{i=1}^N x_i^2} \right)^{p-k} \right\} E \left\{ \left( \frac{\sum_{i \in C_n} x_i^2}{\sum_{i=1}^N x_i^2} \right)^k \right\} E \left\{ \left( \frac{\sum_{i=1}^N x_i^2}{\sum_{i=1}^N x_i^2} \right)^{p-l} \right\} E \left\{ \left( \frac{\sum_{i=1}^N x_i^2}{\sum_{i=1}^N x_i^2} \right)^p \right\}.
\]

(C.16)

It is noted that right side of the equation (C.16) involves different moments of chi-square random variables where the \( m \)th moment of a chi-square random variable with \( N \) degrees of freedom is expressed as

\[
E \left\{ \left( \sum_{i=1}^N x_i^2 \right)^m \right\} = 2^m \frac{\Gamma(m+N/2)}{\Gamma(N/2)}. \quad (C.17)
\]

Since \( \sum_{i \in C_p} x_i^2 \) and \( \sum_{i \in C_n} x_i^2 \) are chi-square random variables with \( N/2 \) degrees of freedom, equation (C.16) could be rewritten as

\[
E \left\{ \left( \sum_{i \in C_p} x_i^2 \right)^{p-k} \left( \sum_{i \in C_n} x_i^2 \right)^k \left( \sum_{i=1}^N x_i^2 \right)^l \right\} = \frac{2^{p-l} \Gamma(p-k+N/4) \Gamma(k+N/4) \Gamma(p-l+N/2)}{\Gamma^2(N/4) \Gamma(p+N/2)}.
\]

(C.18)

Substituting Equation (C.18) into Equation (C.13) yields

\[
E \left\{ \left( x^T S_d x \right)^p / \left( x^T x \right)^l \right\} = \sum_{k=0}^p \binom{p}{k} (-1)^k \frac{2^{p-l} \Gamma(p-k+N/4) \Gamma(k+N/4) \Gamma(p-l+N/2)}{\Gamma^2(N/4) \Gamma(p+N/2)} \quad \text{(C.19)}
\]

Therefore, the expression of \( h(m, n, q, u) \) as in (4.24) can be finally proved by substituting (C.19) into (C.11).
C.4 Derivation of Equation (4.28)

We have the PDF of the multiplication of two random variables \( x \) and \( y \), i.e., \( r = xy \), where \( y \) is defined as in (4.27), as below [103]

\[
f_R(r) = \int_{-\infty}^{+\infty} \frac{1}{|y|} f_X(r/y) f_Y(y) dy = \frac{1}{\pi \sigma_y} \int_0^{+\infty} \frac{1}{y} \exp \left\{ -\frac{r^2}{2y^2} - \frac{(y - m_y)^2}{2\sigma_y^2} \right\} dy, \tag{C.20}
\]

where \( \sigma_y^2 = h(2,0,0,\lambda) \) and \( m_y = 1 + s_i Ab \). Calculating the above integral directly does not provide us a closed form solution. Instead, the characteristic function [103] defined as

\[
\phi_X(\omega) = \int_{-\infty}^{+\infty} \exp \{j\omega x\} f_X(x) dx
\]

is employed. We can have the characteristic function of \( r \) as

\[
\phi_R(\omega) = \left( \frac{1}{\sqrt{1 + \omega^2 \sigma_y^2}} \right) \exp \left\{ -m_y^2 \omega^2 / 2(1 + \omega^2 \sigma_y^2)^2 \right\}. \tag{C.21}
\]

Now employing the inverse relation in the form of 

\[
f_X(x) = \frac{1}{2\pi} \int_{-\infty}^{+\infty} \exp \left\{ -\frac{r^2}{2\sigma_y^2} \right\} \sum_{n=0}^{\infty} \frac{1}{n!} \Gamma(n + 1/2) \left( \frac{m_y^2 |r|}{4\sigma_y^2} \right)^n K_n \left( \frac{|r|}{\sqrt{\sigma_y^2}} \right), \tag{C.22}
\]

where \( K_n(.) \) denotes the modified Bessel function of second kind. Since the coefficients of the watermarked signal \( r \) are assumed IID, the numbers of +1 and -1 in the signature code are assumed equal, based on the expressed PDF of (C.22), the PDF of the watermarked vector \( r \) can be expressed as in (4.28).

C.5 Derivation of Error Probability of the IMSS Embedding Scheme

Assuming the skew normal distribution (4.34) for \( z \) given the message bits in (4.15), we have the error probability of IMSS as

\[
P_{e-IMSS} = \int_{-\infty}^{0} f_Z(z|b = +1) dz = Q \left( \frac{\zeta}{\omega} \right) - 2T \left( \frac{-\zeta}{\omega}, \alpha \right), \tag{C.23}
\]

where \( T(.,.) \) represents the Owen’s \( T \) function defined as

\[
T(h, a) = \frac{1}{2\pi} \int_{0}^{a} \exp \left\{ \frac{-h^2}{2} (1 + x^2) \right\} \frac{dx}{1 + x^2}. \tag{C.24}
\]

127
C.5. Derivation of Error Probability of the IMSS Embedding Scheme

Using \( \exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!} \) for the exponential function and the binomial theorem, and with some algebraic simplifications, we can rewrite the expression \( (C.24) \) as

\[
T(h, a) = \frac{1}{2\pi} \tan^{-1} a + \frac{1}{2\pi} \sum_{n=1}^{\infty} \frac{1}{n!} \left[ \frac{-h^2}{2} \right] \sum_{k=0}^{n-1} \binom{n}{k} \frac{a^{2k+1}}{2k+1}.
\]

(C.25)

Therefore, we have the bit error probability as \( (4.35) \).

By applying the method of moments, we have the following closed-form expressions for the desired parameters as \( [4] \)

\[
\omega = \sqrt{P_{inf}(\hat{\lambda}) + P_{int}(\hat{\lambda}) + 4h(3, 0, 2, \hat{\lambda})A - 4A^2 \left( h(1, 0, 1, \hat{\lambda}) + N \right)^2} \frac{1}{1 - 2\delta^2 / \pi},
\]

(C.26)

\[
\zeta = 2A \left( h(1, 0, 1, \hat{\lambda}) + N \right) - \omega \delta \sqrt{2 / \pi}, \quad \alpha = \frac{\delta}{\sqrt{1 - \delta^2}}
\]

(C.27)

where

\[
\delta = \text{sign}\{\gamma\} \sqrt{\frac{\pi |\gamma|^{2/3}}{2|\gamma|^{2/3} + 2((4 - \pi)/2)^{2/3}}}
\]

(C.28)

The parameter \( \gamma \) denotes the skewness of the test statistic and could be obtained as follows.

The skewness for the case of \( b = +1 \) is defined as \( \gamma = (E\{z^3|b = +1\} - 3\mu\sigma^2 - \mu^3)/\sigma^3 \) where \( \mu \) and \( \sigma^2 \), the mean and variance of the test statistic \( z \) in \( (4.15) \) when \( b = +1 \), can be expressed as

\[
\mu = 2A \left( h(1, 0, 1, \hat{\lambda}) + N \right) + h(2, 0, 1, \hat{\lambda}) + 2h(1, 1, 0, \hat{\lambda}), \quad \sigma^2 = \hat{P}_{inf}(\hat{\lambda}) + \hat{P}_{int}(\hat{\lambda}) - \mu^2
\]

(C.29)

To calculate the expression of \( \gamma \), based on \( (4.15) \), we first approximate \( E\{z^3|b = +1\} \) as

\[
E\{z^3|b = +1\} = 8A^3 \left[ h(3, 0, 3, \hat{\lambda}) + 8\Gamma(3 + N/2)/\Gamma(N/2) + 3h(2, 1, 2, \hat{\lambda}) + 3h(1, 2, 1, \hat{\lambda}) \right] + 6A \left[ (1 + A^2)h(1, 0, 3, \hat{\lambda}) + h(5, 0, 3, \hat{\lambda}) + 2(1 + A^2)h(3, 0, 3, \hat{\lambda}) + 8h(3, 2, 1, \hat{\lambda}) + 6(1 + A^2)h(2, 1, 2, \hat{\lambda}) + 5h(4, 1, 2, \hat{\lambda}) + 4h(2, 3, 0, \hat{\lambda}) + 4(1 + A^2)h(1, 2, 1, \hat{\lambda}) \right].
\]

(C.30)

Thus, the skewness can be obtained by using the expression for \( \gamma \) and equations \( (C.29) \) and \( (C.30) \).
C.6 Derivation of Error Probability of the MSS Scheme in the Presence of Noise

The distribution of the test statistic of the MSS in the presence of additional noise and regarding to expressions (4.37) is in the form of (4.9). Similar to the derivation in Appendix C.1, we have the conditional PDF

\[
 f_Z(z|b = +1, z < 0) = \frac{1}{[(1 - A^2)^2 + 2\sigma_n^2(1 + A^2) + \sigma_n^4]^{N/4}2^{N/2}\Gamma^2(N/4)} \exp \left\{ -\frac{z}{2[(1 + A^2) + \sigma_n^2]} \right\} \\
 \times \sum_{k=0}^{n} \left( \begin{array}{c} n \\ k \end{array} \right) z^k \exp \left\{ \frac{(1 + A^2 + \sigma_n^2) z}{[(1 - A^2)^2 + 2\sigma_n^2(1 + A^2) + \sigma_n^4]} \right\} \times \\
 \left[ \sum_{i=0}^{2n-k} (-1)^{i-k} z^{2n-k-i} \left( \begin{array}{c} 2n - k \\ i \end{array} \right) \frac{i!}{(1 - A^2)^2 + 2\sigma_n^2(1 + A^2) + \sigma_n^4} \right]^{i+1}.
\]

(C.31)

Based on the above conditional PDF of \( z \) and by applying expressions (C.2)-(C.3), similar to Appendix C.1, the error probability is expressed in the form of (4.38).
Appendix D

Corresponding Proofs for Chapter 5

D.1 Derivation of Upper Bound of Information Leakage for ISS Scheme

In order to calculate the mutual information (5.8), two terms \( h(Y|b) \) and \( h(Y|b,s) \) need to be computed. The distribution of the observations when the message bits are known is not Gaussian, therefore, the differential entropy is bounded by

\[
h(Y|b)_{ISS} \leq \frac{1}{2} \log \left( (2\pi e)^N N_0 |C(Y|b)| \right),
\]

where \( C(Y|b) \) means the covariance matrix of the observations given the embedded message bits \( b \). To obtain the mentioned covariance matrix, we revisit the ISS embedding scheme (5.2) by defining

\[
y_m = [y_{1m}, y_{2m}, \ldots, y_{Nm}]^T \quad \text{and} \quad x_m = [x_{1m}, x_{2m}, \ldots, x_{Nm}]^T,
\]

where

\[
y_{ij} = (1 - \lambda)x_{ij} - \lambda s_i \sum_{k=1, k\neq i}^N s_k x_{kj} + s_i Ab_j \quad , \quad i = 1, 2, \ldots, N \quad , \quad j = 1, 2, \ldots, N_0. \tag{D.2}
\]

We thus have

\[
E\{y_{ii}^2\} - E^2\{y_{ii}\} = (1 - \lambda)^2 \sigma_x^2 + \lambda^2 (N - 1) \sigma^2_x + A^2,
\]

\[
E\{y_{ij}y_{ik}\} - E\{y_{ij}\}E\{y_{ik}\} = A^2 b_j b_k \quad , \quad j \neq k,
\]

\[
E\{y_{ij}y_{kl}\} - E\{y_{ij}\}E\{y_{kl}\} = 0 \quad , \quad i \neq k. \tag{D.3}
\]

Therefore, \( C(Y|b) \) has the block diagonal structure in the following form

\[
C(Y|b) = \begin{bmatrix}
F & 0 & \cdots & 0 \\
0 & F & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & F
\end{bmatrix}, \tag{D.4}
\]
D.1. Derivation of Upper Bound of Information Leakage for ISS Scheme

where the $N_0 \times N_0$ matrix $F$ is defined as

$$F = [(1 - \lambda)^2 \sigma_x^2 + \lambda^2 (N - 1) \sigma_x^2]I + A^2 bb^T,$$  \hspace{1cm} (D.5)

where $I$ means the $N_0 \times N_0$ identity matrix. Based on the covariance matrix in (D.4) and $F$ in (D.5), we can have the determinant of $C$ as [41]:

$$|C(Y|b,s)| = \left(1 + \frac{N_0 A^2}{[(1 - \lambda)^2 + (N - 1) \lambda^2 \sigma_x^2]}\right)^N \left(1 - \lambda^2 (N - 1) \sigma_x^2\right)^{N_0 N}.$$  \hspace{1cm} (D.6)

We now calculate the second item $h(Y|b,s)$. For ISS, when both the embedded message and the signature code are given, the observations follow the independent and identical Gaussian distribution. Thus, the differential entropy of the observations given the embedded message and the signature code can be expressed as:

$$h(Y|b,s)_{ISS} = \frac{1}{2} \log \left(\frac{(2\pi e)^{N_0}}{|C(Y|b,s)|}\right),$$  \hspace{1cm} (D.7)

We need to compute the covariance of the observations given $b$ and $s$. Referring to the ISS embedding scheme (D.2) and given a particular realization, we have the following observations

$$E\{y_{ii}^2\} - E^2\{y_{ii}\} = (1 - \lambda)^2 \sigma_x^2 + \lambda^2 (N - 1) \sigma_x^2,$$

$$E\{y_{ij}y_{ik}\} - E\{y_{ij}\}E\{y_{ik}\} = 0, \hspace{0.5cm} j \neq k,$$

$$E\{y_{ij}y_{kl}\} - E\{y_{ij}\}E\{y_{kl}\} = 0, \hspace{0.5cm} i \neq k, j \neq l,$$

$$E\{y_{ij}y_{kj}\} - E\{y_{ij}\}E\{y_{kj}\} = \lambda \sigma_x^2 (\lambda N - 2) s_i s_j b_i b_k, \hspace{0.5cm} i \neq k.$$  \hspace{1cm} (D.8)

Therefore, $C(Y|b,s)$ has the same block diagonal structure as in (D.4), with the difference that $F$ is now a $N \times N$ matrix defined as

$$F = \sigma_x^2 I + \lambda \sigma_x^2 (\lambda N - 2)(b \odot s)(b \odot s)^T$$  \hspace{1cm} (D.9)

where $\odot$ denotes the element by element product of two vectors. It is straightforward to show that the determinant of the covariance matrix $C(Y|b,s)$ can be expressed as

$$|C(Y|b,s)| = (\sigma_x^{2N}(1 - \lambda N)^2)^{N_0}.$$  \hspace{1cm} (D.10)

Using the above obtained determinants of the covariance matrices as in (D.6) and (D.10), and referring to the differential entropy definitions in (D.1) and (D.7), we can derive the upper bound of mutual information for ISS as in Eqn. (5.10).
D.2 Derivation of Upper Bound of Information Leakage for CAISS Scheme Under KMCA

To calculate the mutual information for CAISS under the KMCA scenario (5.12), we need to compute the entropies \( h(Y|b, g) \) and \( h(Y|b, g, s) \). According to the CASS (5.4) and CAISS (5.5) embedding schemes, one could observe that having the signature code \( (s) \) and the correlation information \( (g) \) imply that the \( x \) lies in half space. For more clarification, we rewrite the CAISS embedding scheme in the following form

\[
y_{ij} = \begin{cases} 
  y_{ij1} = x_{ij} + s_i A_1 & \text{if } s^T x_j \geq 0, \ b_j = +1, \\
  y_{ij2} = (1 - \lambda_h)x_{ij} - \lambda_h s_i \sum_{k=1, k \neq i}^N k x_{kj} - s_i A_2 & \text{if } s^T x_j \geq 0, \ b_j = -1, \\
  y_{ij3} = x_{ij} - s_i A_1 & \text{if } s^T x_j < 0, \ b_j = -1, \\
  y_{ij4} = (1 - \lambda_h)x_{ij} - \lambda_h s_i \sum_{k=1, k \neq i}^N k x_{kj} + s_i A_2 & \text{if } s^T x_j < 0, \ b_j = +1,
\end{cases}
\]  

(D.11)

where \( i = 1, 2, \ldots, N \) and \( j = 1, 2, \ldots, N_0 \). When the signature code, message bits, and the correlation information are known, the observations are independent. Without loss of generality, we assume that \( b_j = 1 \) and \( g_j = 1 \). Having signature code and correlation information lead to the fact that \( x_j \) lies in the half space. In other words, the distribution of the observation \( y_j \) under the aforementioned conditions is as \( f(y_j | b_j = 1, g_j = 1, s) = 2N(0_N, \sigma_x^2 I_N)|I(s^T x_j > 0)\) where \( I(s^T x_j > 0) \) returns one when \( x_j \) lies on the corresponding half space, i.e., \( s^T x_j > 0 \), and returns zero otherwise.

Since we have assumed that the host signal follows Gaussian distribution, we could conclude that the random variable \( y_{ij} \) given \( b, g, \) and \( s \) follows half Gaussian. The point that should be taken into account is that if \( x \) follows the Gaussian distribution with covariance matrix \( C \), then the corresponding half normal random vector \( y \) has the entropy of \( h(y) = 0.5 \log((2\pi e)^N |C|) - \log(2) \).

According to the CAISS embedding scheme (D.11), when \( b, s, \) and \( g \) are known, the observations are uncorrelated and we have the following statistics

\[
E\{y_{ij1}y_{kl1}\} - E\{y_{ij1}\}E\{y_{kl1}\} = 0 \quad , \quad i \neq k,
\]

\[
E\{y_{ij1}y_{kl4}\} - E\{y_{ij1}\}E\{y_{kl4}\} = 0 \quad , \quad i \neq k, j \neq l,
\]

\[
E\{y_{ij1}y_{ik1}\} - E\{y_{ij1}\}E\{y_{ik1}\} = 0 \quad , \quad j \neq k,
\]
D.2. Derivation of Upper Bound of Information Leakage for CAISS Scheme Under KMCA

\[ E\{y_{ij} y_{ik}\} - E\{y_{ij}\} E\{y_{ik}\} = 0, \quad j \neq k, \]

\[ E\{y_{ij1} y_{ik}\} - E\{y_{ij}\} E\{y_{ik}\} = 0, \quad j \neq k, \]

\[ E\{y_{ij4} y_{kj}\} - E\{y_{ij}\} E\{y_{kj}\} = \lambda h \sigma_x^2 (\lambda h N - 2) s_i s_k, \quad i \neq k, \]

\[ E\{y_{ii1}\} - E^2\{y_{ii}\} = \sigma_x^2, \]

\[ E\{y_{ii4}\} - E^2\{y_{ii}\} = (1 - \lambda h)^2 \sigma_x^2 + \lambda h^2 (N - 1) \sigma_x^2. \]  

(D.12)

We define \( q \) as the number of observations which satisfying \( b = 1 \) and \( g = -1 \). From (D.12), we can see that the vector observations are uncorrelated and the covariance matrix \( C(Y|b, g, s) \) is in the form of (D.4) with the \( N \times N \) matrix \( F \). Thus, when \( q = 0 \) and \( q = N_0 \), we have \( F = \sigma_x^2 I \) and \( F = \sigma_x^2 I + \sigma_x^2 \lambda h (\lambda h N - 2) s s^T \), respectively.

Without loss of generality, we assume that \( b_1 = 1 \) and therefore, based on the independent half Gaussian observations, \( h(Y|b, g, s) \) could be expressed as

\[ h(Y|b, g, s)_{CAISS} = N_0 h(y_1|b_1 = 1, g_1 = 1, s) + h(y_1|b_1 = 1, g_1 = -1, s) = \]

\[ \frac{N_0}{4} \log \left( (2\pi e \sigma_x^2)^N \right) + \frac{N_0}{4} \log \left( (2\pi e \sigma_x^2)^N (1 - \lambda h N)^2 \right) - N_0 \log(2) = \]

\[ \frac{N_0}{2} \log \left( (2\pi e \sigma_x^2)^N (1 - \lambda h N) \right) - N_0 \log(2). \]  

(D.13)

It should be mention that the term \( \log(2) \) in above entropy is due to the effect of the half Gaussian distribution of the observations when message bits, signature code, and the correlation information are known.

To complete the security analysis of the KMCA scenario, we also need to obtain \( h(Y|b, g) \).
When the message bits and the correlations are known, we can have the following statistics:

\[
E\{y_{ij1}y_{k1}\} - E\{y_{ij1}\}E\{y_{k1}\} = 0, \quad i \neq k
\]
\[
E\{y_{ij1}y_{k1}\} - E\{y_{ij1}\}E\{y_{k1}\} = 0, \quad i \neq k
\]
\[
E\{y_{ij1}y_{ik1}\} - E\{y_{ij1}\}E\{y_{ik1}\} = A_1^2 b_j b_k, \quad j \neq k
\]
\[
E\{y_{ij4}y_{ik4}\} - E\{y_{ij4}\}E\{y_{ik4}\} = A_2^2 b_j b_k, \quad j \neq k
\]
\[
E\{y_{ij1}y_{ik4}\} - E\{y_{ij1}\}E\{y_{ik4}\} = A_1 A_2 b_j b_k, \quad j \neq k
\]
\[
E\{y_{ii1}\}^2 - E^2\{y_{ii1}\} = (1 - \lambda_h)^2 \sigma_x^2 + \lambda_h^2(N - 1)\sigma_x^2 + A_1^2.
\]

(D.14)

The entropy \(h(\mathbf{Y}|\mathbf{b}, \mathbf{g})\) could be expressed as

\[
h(\mathbf{Y}|\mathbf{b}, \mathbf{g})_{\text{CAISS}} = \sum_i h(\mathbf{Y}|q = i)p(q = i), \quad (D.15)
\]

where \(q\) is the number of observations which satisfying \(b = 1\) and \(g = -1\) and follows the binomial distribution as \(p(q = i) = 0.5^{N_0}\binom{N_0}{i}\). It is known that \(h(\mathbf{Y}|q = i)\) depends on \(C(\mathbf{Y}|q = i)\), which has the block diagonal structure presented in (D.4) with \(\mathbf{F}\) being a \(N_0 \times N_0\) matrix. When \(q = 0\) the matrix \(\mathbf{F}\) is in the form of \(\mathbf{F} = \sigma_x^2 \mathbf{I} + A_1^2 \mathbf{bb}^T\), and when \(q = N_0\) the matrix has the form \(\mathbf{F} = \sigma_x^2(1 - 2\lambda_h + \lambda_h^2 N)\mathbf{I} + A_2^2 \mathbf{bb}^T\). When \(q \neq 0\) and \(q \neq N_0\), the matrix \(\mathbf{F}\) has the following structure

\[
\mathbf{F} = \text{diag}\{\sigma_x^2, \ldots, \sigma_x^2, (1 - \lambda_h)^2 \sigma_x^2 + \lambda_h^2(N - 1)\sigma_x^2, \ldots, (1 - \lambda_h)^2 \sigma_x^2 + \lambda_h^2(N - 1)\sigma_x^2\} + \begin{bmatrix} \mathbf{F}_{11} & \mathbf{F}_{12} \\ \mathbf{F}_{12}^T & \mathbf{F}_{22} \end{bmatrix} \quad (D.16)
\]

where \(\text{diag}\{\cdot\}\) represents the diagonal matrix with the first \(N_0 - i\) elements being \(\sigma_x^2\) and the rest being \((1 - \lambda_h)^2 \sigma_x^2 + \lambda_h^2(N - 1)\sigma_x^2\). Moreover, the elements of matrices \(\mathbf{F}_{11}, \mathbf{F}_{12},\) and \(\mathbf{F}_{22}\) are as

\[
\mathbf{F}_{11}^{ij} = A_1^2 b_i b_j,
\]
\[
\mathbf{F}_{12}^{ij} = A_1 A_2 b_i b_j,
\]
\[
\mathbf{F}_{22}^{ij} = A_2^2 b_i b_j. \quad (D.17)
\]

When \(q = 0\) and \(q = N_0\), the determinants of the matrix \(\mathbf{F}\) are \(\sigma_x^{2N_0}(1 + \frac{N_0 A_1^2}{\sigma_x^2})\) and \(\sigma_x^{2N_0}(1 - 2\lambda_h + \lambda_h^2 N)^{N_0}(1 + \frac{N_0 A_2^2}{\sigma_x^2(1 - 2\lambda_h + \lambda_h^2 N)})\), respectively. When \(q = k\) \((k \neq 0\) and \(k \neq N_0\)), the determinant of \(\mathbf{F}\) is equal to \(\sigma_x^{2N_0}(1 - 2\lambda_h + \lambda_h^2 N)^{k}(1 + \frac{1}{\sigma_x^2(1 - 2\lambda_h + \lambda_h^2 N)} + (N_0 - k)A_2^2)\)).

Since \(C(\mathbf{Y}|q = i)\) is in the form of (D.4) with the \(N_0 \times N_0\) matrix \(\mathbf{F}\), \(h(\mathbf{Y}|q = i)\) is bounded
D.3. Derivation of Upper Bound of Information Leakage for CAISS Scheme Under KMA

as \( h(Y|q = i) \leq 0.5 \log((2\pi e)^{N_0}|C(Y|q = i)|) \). Therefore, according to (D.15) and the above analysis, we have

\[
\frac{N}{2} \left( \frac{1}{2} \right)^{N_0} \sum_{i=0}^{N_0} \log \left( (2\pi e\sigma_x^2)^{N_0} (1 - 2\lambda_h + \lambda_h^2 N) \right) \left[ 1 + \frac{1}{\sigma_x^2} \left( \frac{i(D(2 - \alpha) - \lambda_h^2 N\sigma_x^2)}{1 - 2\lambda_h + \lambda_h^2 N} + (N_0 - i)(N_0 - i) \alpha D \right) \right] \left( \frac{N_0}{i} \right)
\]

(D.18)

Substituting (D.18) and (D.13) into (5.12) leads to (5.13), as the upper bound for information leakage of the CAISS scheme under the KMCA scenario.

D.3 Derivation of Upper Bound of Information Leakage for CAISS Scheme Under KMA

In order to calculate the information leakage of the CAISS scheme under the KMA scenario, we need to compute the entropies \( h(Y|b) \) and \( h(Y|b, s) \). When the message bits and the signature code are available, the observations are independent which leads to \( h(Y|b, s) = N_0 h(y_1|b_1, s) \). Entropy \( h(y_1|b_1, s) \) depends on the \( f(y_1|b_1 = 1, s) \) which without loss of generality it has been assumed that message bit is equal to 1. According to (D.11), the distribution \( f(y_1|b_1 = 1, s) \) could be written as

\[
f(y_1|b_1 = 1, s) = f_p I(x^T s > 0) + f_n I(x^T s < 0), \tag{D.19}
\]

where \( I(x^T s > 0) \) and \( I(x^T s < 0) \) return one when \( x \) satisfy \( x^T s > 0 \) and \( x^T s < 0 \), respectively, and return zero otherwise. In addition, here, we have \( f_p = f(y_1|b_1 = 1, g_1 = 1, s) \) and \( f_n = f(y_1|b_1 = 1, g_1 = -1, s) \). According to (D.19), since \( f_p \) and \( f_n \) are defined in complement spaces, it is straightforward to show that \( h(Y|b, s) \) could be expressed as

\[
h(y|b, s)_{CAISS} = N_0 \left[ - \int_{x^T s > 0} f_p \log(f_p) dx - \int_{x^T s < 0} f_n \log(f_n) dx \right] = \frac{N_0}{4} \log \left( (2\pi e\sigma_x^2)^N \right) + \frac{N_0}{4} \log \left( (2\pi e\sigma_x^2)^N (1 - \lambda_h N) \right) = \frac{N_0}{2} \log \left( (2\pi e\sigma_x^2)^N (1 - \lambda_h N) \right), \tag{D.20}
\]

where we have used \( \mathbf{F} = \sigma_x^2 \mathbf{I} \) and \( \mathbf{F} = \sigma_x^2 \mathbf{I} + \sigma_x^2 \lambda_h (\lambda_h N - 2) \mathbf{s}s^T \) to obtain the entropies.

The entropy \( h(Y|b)_{CAISS} \) is bounded as \( h(Y|b)_{CAISS} \leq 0.5 \log((2\pi e)^{N_0}|C(Y|b)|) \). When
D.4. Derivation of Inequality (5.17)

the message bits are known, regarding to (D.14), we can have the following statistics

\[ E\{y_{ij}y_{kl}\} - E\{y_{ij}\}E\{y_{kl}\} = 0, \ i \neq k \]

\[ E\{y_{ij}y_{ik}\} - E\{y_{ij}\}E\{y_{ik}\} = \frac{1}{4}(A_1^2 + A_2^2 + 2A_1A_2)b_jb_k, \ j \neq k \]

\[ E\{y_{ii}\}^2 - E^2\{y_{ii}\} = \frac{\sigma_x^2}{2}(2 - 2\lambda_h + \lambda_h^2N) + \frac{1}{2}(A_1^2 + A_2^2). \] (D.21)

Thus, \( C(Y|b) \) is in the form of (D.4) with the \( N_0 \times N_0 \) matrix \( F \) where

\[
F = \left[ \frac{\sigma_x^2}{2}(2 - 2\lambda_h + \lambda_h^2N) + \frac{1}{4}(A_1 - A_2)^2 \right] \mathbf{I} + \frac{1}{4}(A_1 + A_2)^2 \mathbf{b}\mathbf{b}^T. \] (D.22)

Therefore, according to above results, we have the following entropy for CAISS scheme as

\[
h(Y|b)_{CAISS} \leq \frac{N}{2} \log \left( (2\pi e)^{N_0} \left[ \frac{\sigma_x^2}{2}(2 - 2\lambda_h + \lambda_h^2N) + \frac{1}{4} \left( \sqrt{\alpha D} - \sqrt{D(2 - \alpha) - \lambda_h^2N}\sigma_x^2 \right)^2 \right]^{N_0} \right) +
\]

\[
\frac{N}{2} \log \left( 1 + \frac{N_0}{4} \left[ \sqrt{\alpha D} - \sqrt{D(2 - \alpha) + \lambda_h^2N}\sigma_x^2 \right]^2 \right) \] (D.23)

Substituting (D.20) and (D.23) into (5.8) leads to upper bound of information leakage of CAISS scheme under KMA scenario as (5.15).

D.4 Derivation of Inequality (5.17)

Based on the definition of the mutual information for \( I(Y; s|b) \), it is straightforward to show that the mutual information of CAISS under KMA can be expressed as:

\[
I(Y; s|b)_{CAISS} = h(Y|b)_{CAISS} - h(Y|b, s)_{CAISS} = [h(Y|b)_{CAISS} - h(Y|b, g, s)_{CAISS}] - [h(Y|b, s)_{CAISS} - h(Y|b, g, s)_{CAISS}] = I(Y; g, s|b)_{CAISS} - I(Y; g|b, s)_{CAISS} = I(Y; s|b, g)_{CAISS} + I(Y; g|b)_{CAISS} - I(Y; g|b, s)_{CAISS}, \] (D.24)

where the third equality comes from the definition of the mutual information and the fourth one comes from the chain rule of mutual information.

In order to show that the mutual information of CAISS under KMA is less than that of
D.5 Derivation of Upper Bound of Information Leakage for MSS Scheme Under KMA

In order to calculate the information leakage for the MSS scheme (5.7) under KMA, we rewrite MSS embedding as

\[ y_{ij} = x_{ij} (1 + s_i A b_j), \quad i = 1, 2, ..., N, \quad j = 1, 2, ..., N_0. \]  

We first compute the differential entropy \( h(Y|b)_{MSS} \). Based on MSS embedding (D.26), the observations have the following statistics

\[ E\{y_{ij}y_{kl}\} - E\{y_{ij}\} E\{y_{kl}\} = 0, \quad i \neq k, \]
\[ E\{y_{ii}^2\} - E\{y_{ii}\} E\{y_{ii}\} = \sigma_x^2 (1 + A^2). \]  

Therefore, we have

\[ h(Y|b)_{MSS} \leq \frac{1}{2} \log \left( (2\pi e\sigma_x^2)^{NN_0} (1 + D/\sigma_x^2)^{NN_0} \right). \]  

For MSS embedding (5.7), the observations are independent and follow identical Gaussian
D.6 Derivation of Estimator (5.20)

When the embedded messages and the signature code are known, without loss of generality, we assume that the embedded message bit is 1, and thus we have

\[ h(Y|b,s)_{MSS} = \frac{N_0}{2} \log ((2\pi e) |C(y_1|b_1 = 1, s)|). \] (D.29)

When the embedded messages and the signature code are fully known, we could use \( h(BX) = h(X) + \log(|B|) \) where \( B = I + S_dA \) for the MSS scheme. Since the numbers of +1 and -1 in the signature code are equal, the determinant of \( B \) is \( |B| = |1 - A^2|^{N/2} \). Therefore, we have the conditional differential entropy

\[ h(Y|b,s)_{MSS} = \frac{N_0}{2} \log \left( (2\pi e\sigma_x^2)^N |1 - D/\sigma_x^2|^N \right). \] (D.30)

Finally, using (D.28) and (D.30), we can have the upper bound of information leakage of the MSS scheme under KMA as described in (5.11).

D.6 Derivation of Estimator (5.20)

For the MSS embedding scheme (5.7), the distribution of the watermarked signals conveying the message bits using \( s_j \) is as below

\[ f(y|b,s_j) = \frac{1}{\sqrt{(2\pi\sigma_x^2)^N_0}} \prod_{i=1}^{N_0} \left( \frac{1}{1 + s_jAb_i} \right) \exp \left\{ \sum_{i=1}^{N_0} \frac{-y_{ji}^2}{2\sigma_x^2(1 + s_jAb_i)^2} \right\}, \] (D.31)

where \( y = [y_{j1}, ..., y_{jN_0}] \) is the \( j \)th element of the observations. The ML estimator of the \( j \)th element of the signature code can be obtained by maximizing the PDF \( f(y|b,s_j) \). By taking the derivative of (D.31) with respect to \( s_j \) and letting it to be zero, we can obtain the ML estimator of \( s_j \) as

\[ \hat{s}_j = \text{sign} \left\{ \frac{1}{\sigma^2_x} b^T (y \odot y) - (1 + A^2) b^T 1 \right\}. \] (D.32)

It is straightforward to show that this result leads to the ML estimator of the signature code in the form of (5.20).