ENHANCED IMAGE WATERMARKING TECHNIQUES WITH CONTOUR COMPRESSION METHODS

MAJDI FARAG MOHAMMED EL BIREKI

A thesis submitted in
fulfillment of the requirement for the award of the
Degree of Doctor of Philosophy in Electrical Engineering

Faculty of Electrical and Electronic Engineering
Universiti Tun Hussein Onn Malaysia

MAY, 2017
This thesis is dedicated to my beloved mother, father, my dear siblings and friends who are always supportive when I needed them, for without their understanding, I would not be able to complete my dissertation.
ACKNOWLEDGEMENT

First, I deeply thank Allah, for his guidance and blessing.

I would like to express my appreciation and sincere gratitude to my supervisor, Prof. Dr. Mohammed Faiz Liew Bin Abdullah and co-supervisor Assoc. Prof. Dr. Ali Abdhrhman M. Ukhsha for their continuous support, encouragement and endless patience towards completing the course of this PhD research. I am thankful for their aspiring guidance, invaluable constructive criticism and friendly advice during the project work. I am sincerely grateful to them for sharing their truthful and illuminating views on several issues related to the project.

I also thank all my friends, particularly to Rachel R. Polancos, who motivated me to strive towards my goal, for giving me ideas, moral support and feedbacks in this research. I would also like to thank my friends and colleagues at Universiti Tun Hussein Onn Malaysia (UTHM) for all the help and advice received from you.

Finally, my great thanks and gratitude to my parents, for the sacrifices that you have made on my behalf all my life. Your prayers for me were what sustained me thus far. My sincere thanks to my sisters and brothers for your continuous assistance, patience and wonderful support.

May God bless all of us!
ABSTRACT

Techniques that hide information have undoubtedly become valuable and useful in commercial, public or private application areas. However, the fast-developing technologies have also caused numerous downsides e.g. illegal transmission, copying, manipulation or duplication of data contents, loss of revenues because of worldwide piracy and copyright problems. Thus, digital watermarking algorithms that provide imperceptibility, robustness and security to combat these problems are highly desirable. Problems that are related to image recognition after watermarking are examined and tested through the attacked watermarked image using a well-defined curve approximation of active contours by compression. The proposed watermarking algorithms embed watermark bits into a cover image using zonal sampling methods in the frequency domains DCT, DWT and joint DWT-DCT. Comparative results show that the proposed watermarking methods are imperceptible, robust and secure against various signal/image processing attacks with PSNR values of 30-35 dB and above, with NCC values of 0.60 and above. Experimental and comparative results for contour compression show that the proposed Adaptive Triangle method has a high compression ratio greater than or equal to 94%. The method’s simplicity with accepted level of reconstruction is its main advantage. The combination of contour extraction and contour compression using the Adaptive triangle method from the attacked watermarked image increases value to image recognition ability and security of the proposed method.
ABSTRAK

Teknik-teknik penyembunyian maklumat tidak diragukan lagi telah menjadi bernilai tinggi dan berguna dalam bidang aplikasi komersial, awam atau swasta. Walau bagaimanapun, pembangunan teknologi yang pesat juga telah menyebabkan banyak kelemahan, contohnya; penghantaran terlarang, penyalinan, manipulasi atau penduaan kandungan-kandungan data serta kerugian hasil-hasil akibat daripada cetak rompak di seluruh dunia dan pelbagai masalah hak cipta. Oleh itu, algoritma-algoritma tera air digital yang mempunyai nilai ketakbolehkelihatan, keteguhan dan keselamatan dalam menangani masalah-masalah tersebut adalah sangat diperlukan. Masalah-masalah yang berkaitan dengan pengecaman imej setelah ditera air diperiksa dan diuji menggunakan imej yang ditera air yang telah diserang, dengan menggunakan satu anggaran lengkung yang tepat daripada kontur-kontur aktif oleh pemampatan. Algoritma-algoritma tera air yang dicadangkan membenamakan bit tera air ke dalam satu imej penutup dengan menggunakan kaedah-kaedah persampelan zon dalam domain frekuensi DCT, DWT dan DWT-DCT yang bergabung. Keputusan-keputusan perbandingan menunjukkan kaedah-kaedah tera air yang dicadangkan adalah tidak boleh dilihat, teguh dan selamat daripada serangan pelbagai isyarat / imej pemprosesan dengan nilai-nilai PSNR 30-35 dB dan ke atas, dengan nilai NCC 0.60 dan ke atas. Keputusan-keputusan eksperimen dan perbandingan bagi pemampatan kontur menunjukkan bahawa kaedah Adaptive Triangle yang dicadangkan mempunyai nisbah mampatan yang tinggi iaitu bersamaan atau lebih besar daripada 94%. Keringkasan kaedah beserta tahap pembinaan semula yang munasabah adalah kelebihannya yang utama. Gabungan pengekstrakan kontur dan pemampatan kontur yang menggunakan kaedah Adaptive Triangle daripada imej yang ditera air yang telah diserang meningkatkan nilai terhadap keupayaan pengesanan imej dan keselamatan daripada kaedah yang dicadangkan.
# Table of Contents

**Declaration**

v

**Dedication**

vi

**Acknowledgement**

vii

**Abstract**

viii

**Abstrak**

ix

**Table of Contents**

x

**List of Tables**

xviii

**List of Figures**

xxii

**List of Appendices**

xxx

**List of Symbols and Abbreviations**

xxxi

**List of Publications**

xxxv

## Chapter 1 Introduction

1

1.1 Introduction

1

1.2 Research Background

1

1.2.1 The evolution of information hiding

3

1.2.2 General watermarking system

4

1.3 Problem statement and significance

5

1.4 Research questions

6

1.5 Research objectives

6

1.6 Research scopes and limitations

7

1.7 Research novelty and contribution

8

1.8 Thesis organization

10

## Chapter 2 Literature Review

11

2.1 Introduction

11

2.2 General framework of digital watermarking

11

2.2.1 Digital watermarking

12

2.2.2 Digital watermarking requirements

15
2.2.3 Purposes and applications of digital watermarking 16
2.3 Digital image watermarking categories 17
2.4 Digital watermarking techniques 19
   2.4.1 Spatial domain 19
   2.4.2 Frequency domain 20
      2.4.2.1 Discrete wavelet transform (DWT) 21
      2.4.2.2 Discrete cosine transform (DCT) 26
2.5 The hybrid watermarking technique 29
2.6 Zonal sampling method (ZSM) 33
2.7 The Arnold Transform 34
2.8 Watermark attacks 35
2.9 An overview on image’s edges and contours 37
   2.9.1 Edge detection 37
   2.9.2 Contour extraction methods in different windows 39
      2.9.2.1 Object contour following (OCF) 41
      2.9.2.2 Multiple step contour extraction (MSCE) 42
      2.9.2.3 Object-oriented contour extraction (OCE) 43
      2.9.2.4 Single step parallel contour extraction (SSPCE) 44
2.9.3 Methods of contour approximation and compression in spatial domain 46
   2.9.3.1 Ramer method 47
   2.9.3.2 Trapezoid method 48
   2.9.3.3 Triangle method 49
2.10 Previous related works 50
   2.10.1 Discrete cosine transform-based watermarking 51
   2.10.2 Discrete wavelet transform-based watermarking 52
   2.10.3 Joint watermarking techniques 53
   2.10.4 Contour extraction and compression in spatial domain 56
CHAPTER 3  RESEARCH METHODOLOGY AND IMPLEMENTATION  61

3.1 Introduction  61
3.2 Overview of the research work  61
3.3 Proposed area of research methodology and implementation  63
  3.3.1 Zonal sampling algorithms in DCT and DWT watermarking schemes  65
    3.3.1.1 Embedding process  65
    3.3.1.2 Watermark attacks  66
    3.3.1.3 Extraction process  67
  3.3.2 Hybrid watermarking scheme using DCT-DWT and Arnold Transform  67
  3.3.3 Contour extraction and contour approximation/compression  68
    3.3.3.1 Contour extraction using SSPCE method  69
    3.3.3.2 Contour compression using Adaptive Triangle method  70
    3.3.3.3 Contour compression using Ramer method  79

3.4 Research performance criteria  85
  3.4.1 Performance criteria used on image  85
    3.4.1.1 Mean Square Error (MSE)  86
    3.4.1.2 Imperceptibility  86
    3.4.1.3 Robustness  86
    3.4.1.4 Correlation coefficient  87
    3.4.1.5 Compression ability  87
    3.4.1.6 Histograms  88
  3.4.2 Performance criteria used on contour  88
    3.4.2.1 Compression ability  89
    3.4.2.2 Quality measurement  89

3.5 Summary  90
CHAPTER 4  RESULTS AND DATA ANALYSIS FOR DIGITAL IMAGE WATERMARKING METHODS IN DCT AND DWT WITH ZONAL SAMPLING ALGORITHM  

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1</td>
<td>Introduction</td>
<td>91</td>
</tr>
<tr>
<td>4.2</td>
<td>Block diagram of the proposed enhanced digital watermarking method</td>
<td>91</td>
</tr>
<tr>
<td>4.2.1</td>
<td>Embedding process of the proposed enhanced watermarking method</td>
<td>93</td>
</tr>
<tr>
<td>4.2.2</td>
<td>Watermark extraction process of the proposed method</td>
<td>94</td>
</tr>
<tr>
<td>4.3</td>
<td>Test results and discussions for DCT</td>
<td>95</td>
</tr>
<tr>
<td>4.3.1</td>
<td>Test results of blurred and compressed watermarked image using DCT with zonal sampling algorithm I</td>
<td>96</td>
</tr>
<tr>
<td>4.3.2</td>
<td>Test results of blurred and compressed watermarked image using the DCT with zonal sampling algorithm II</td>
<td>98</td>
</tr>
<tr>
<td>4.3.3</td>
<td>Digital watermark extraction results using DCT with zonal sampling I</td>
<td>101</td>
</tr>
<tr>
<td>4.3.3.1</td>
<td>Robustness against Gaussian blurring using DCT with zonal sampling I</td>
<td>102</td>
</tr>
<tr>
<td>4.3.3.2</td>
<td>Robustness against LoG blurring using DCT with zonal sampling I</td>
<td>103</td>
</tr>
<tr>
<td>4.3.3.3</td>
<td>Robustness against sharpening using DCT with zonal sampling I</td>
<td>104</td>
</tr>
<tr>
<td>4.3.4</td>
<td>Digital watermark extraction results using DCT with zonal sampling II</td>
<td>105</td>
</tr>
<tr>
<td>4.3.4.1</td>
<td>Robustness against Gaussian blurring using DCT with zonal sampling II</td>
<td>106</td>
</tr>
<tr>
<td>4.3.4.2</td>
<td>Robustness against LoG blurring using DCT with zonal sampling II</td>
<td>107</td>
</tr>
<tr>
<td>4.3.4.3</td>
<td>Robustness against sharpening using DCT with zonal sampling II</td>
<td>108</td>
</tr>
</tbody>
</table>
4.4 Experimental results of various host images using DCT with zonal sampling methods I & II  
4.4.1 Experimental results using DCT with zonal sampling I  
4.4.2 Experimental results using DCT with zonal sampling II  
4.4.2.1 Experimental results with various intensified attacks on watermarked images using DCT with zonal sampling I and II  
4.4.2.2 Discussion and analysis for various intensified attacks on watermarked images using DCT with zonal sampling I and II  
4.5 Comparative results on robustness using DCT with zonal sampling I & II against other watermarking methods  
4.6 The proposed enhanced watermarking method using DWT  
4.6.1 Embedding procedure using DWT with zonal sampling I & II  
4.6.2 Extracting procedure using DWT with zonal sampling I & II  
4.7 Test results and discussions for DWT  
4.7.1 Digital watermark extraction results using DWT with zonal sampling I  
4.7.2 Digital watermark extraction results using DWT with zonal sampling II  
4.8 Experimental results using DWT with zonal sampling methods I & II  
4.8.1 Experimental results using DWT with zonal sampling I  
4.8.2 Experimental results using DWT with zonal sampling II
4.8.2.1 Experimental results with various intensified attacks on watermarked images using DWT with zonal sampling I and II

4.8.2.2 Discussion and analysis for various intensified attacks on watermarked images using DWT with zonal sampling I and II

4.9 Comparative results between BPNN and the proposed method

4.10 Comparative results between DCT and DWT using zonal sampling I & II

4.11 Summary

CHAPTER 5 RESULTS AND DATA ANALYSIS OF THE WATERMARKING DESIGN USING JOINT DCT-DWT TECHNIQUES

5.1 Introduction

5.2 Block diagram of the proposed joint DWT-DCT watermarking scheme and Arnold Transform

5.2.1 The watermark embedding procedure

5.2.2 The watermark extraction procedure

5.3 Experimental results and discussion

5.4 Summary

CHAPTER 6 RESULTS AND DATA ANALYSIS FOR CONTOUR EXTRACTION AND CONTOUR COMPRESSION METHODS

6.1 Introduction

6.2 The proposed contour extraction method

6.2.1 Proposed gray image encryption and decryption using SSPCE

6.2.1.1 Generation of Key images

6.2.1.2 Encryption process

6.2.1.3 Decryption process

6.2.2 Results and discussion for the proposed method
6.3 The proposed Adaptive Triangle method for contour compression
  6.3.1 Experimental results of SSPCE and Adaptive Triangle methods
  6.3.2 Comparative results of the different contour compression methods against the proposed Adaptive Triangle method

6.4 Contour extraction and compression from watermarked image in frequency domain DCT and DWT using zonal sampling methods
  6.4.1 Results in frequency domain DCT/DWT using zonal sampling methods, SSPCE and Ramer contour compression method
    6.4.1.1 Contour extraction and compression results and discussion in frequency domain DCT, Ramer and zonal sampling
    6.4.1.2 Results in frequency domain DWT using zonal sampling methods, SSPCE and Ramer contour compression method
  6.4.2 Results and discussion in the frequency domain DCT/DWT using zonal sampling methods, SSPCE and Adaptive Triangle contour compression method
    6.4.2.1 Contour extraction and compression results and discussion in frequency domain DCT, Adaptive Triangle and zonal sampling
    6.4.2.2 Contour extraction and compression results and discussion in frequency domain DWT, Adaptive Triangle and zonal sampling

6.5 Summary
<table>
<thead>
<tr>
<th>CHAPTER 7</th>
<th>CONCLUSION AND FUTURE WORK</th>
<th>190</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.1</td>
<td>Conclusion and contribution</td>
<td>190</td>
</tr>
<tr>
<td>7.2</td>
<td>Future work</td>
<td>191</td>
</tr>
<tr>
<td>REFERENCES</td>
<td></td>
<td>193</td>
</tr>
<tr>
<td>APPENDIX A</td>
<td></td>
<td>205</td>
</tr>
<tr>
<td>APPENDIX B</td>
<td></td>
<td>210</td>
</tr>
<tr>
<td>APPENDIX C</td>
<td></td>
<td>216</td>
</tr>
<tr>
<td>APPENDIX D</td>
<td></td>
<td>218</td>
</tr>
<tr>
<td>VITA</td>
<td></td>
<td>222</td>
</tr>
</tbody>
</table>
LIST OF TABLES

2.1 Research findings and weaknesses of various watermarking techniques 59
3.1 Contour sequence table 73
3.2 Sequence of the points for the curve segment of the straight line $l_1$ 74
3.3 Sequence of the points for the lower curve segment of the straight line $l_1$ 81
3.4 Sequence of the points for the upper curve segment of the straight line $l_1$ 83
4.1 Results of the distorted test images using DCT with zonal sampling I 97
4.2 Results of the distorted test images using DCT with zonal sampling 99
4.3 Results after the motion blurring attack using DCT with zonal sampling I 102
4.4 Results after Gaussian blurring attacks using DCT with zonal sampling I 103
4.5 Results after LoG blurring attack using DCT with zonal sampling I 104
4.6 Results after sharpening attack using DCT with zonal sampling I 105
4.7 Results of the motion blurring attack using DCT with zonal sampling II 105
4.8 Results after Gaussian blurring attack using DCT with zonal sampling II 106
4.9 Results after LoG blurring attack using DCT with zonal sampling II 107
4.10 Results after sharpening attack using DCT with zonal sampling II
4.11 DCT with zonal sampling I experimental results without attack, salt and peppers and JPEG attacks
4.12 DCT with zonal sampling I experimental results with Gaussian noise, blurring attacks motion and LoG
4.13 DCT with zonal sampling I experimental results with sharpening, LPF and median filter attacks
4.14 DCT with zonal sampling II experimental results without attack, salt and peppers and JPEG attacks
4.15 DCT with zonal sampling II experimental results with Gaussian noise, blurring attacks motion and LoG
4.16 DCT with zonal sampling II experimental results with sharpening, LPF and median filter attacks
4.17 Expanded experimental results with salt and peppers, JPEG and LPF attacks using DCT with zonal sampling I
4.18 Expanded experimental results with median filter, sharpening and motion blurring attacks using DCT with zonal sampling I
4.19 Expanded experimental results with Gaussian noise, LoG and histogram attacks using DCT with zonal sampling I
4.20 Expanded experimental results with salt and peppers, JPEG and LPF attacks using DCT with zonal sampling II
4.21 Expanded experimental results with median filter, sharpening and motion blurring attacks using DCT with zonal sampling II
4.22 Expanded experimental results with Gaussian noise, LoG and histogram attacks using DCT with zonal sampling II
4.23 Comparative results between FIS and the proposed method
4.24 Comparative results between Neural Networks method and the proposed method
4.25 Results after the motion blurring attack using DWT with zonal sampling I
4.26 Results after the motion blurring attack using DWT with zonal sampling II
4.27 DWT with zonal sampling I experimental results with no attack, salt and peppers and JPEG attacks
4.28 DWT with zonal sampling I experimental results with Gaussian noise, motion and LoG blurring attacks
4.29 DWT with zonal sampling I experimental results with sharpening, LPF and median filtering attacks
4.30 DWT with zonal sampling II experimental results with no attack, salt and peppers and JPEG attacks
4.31 DWT with zonal sampling II experimental results with Gaussian noise, motion and LoG blurring attacks
4.32 DWT with zonal sampling II experimental results with sharpening, LPF and median filtering attacks
4.33 Expanded experimental results with salt and peppers, JPEG and LPF attacks using DWT with zonal sampling I
4.34 Expanded experimental results with median filtering, sharpening and motion blurring using DWT with zonal sampling I
4.35 Expanded experimental results with Gaussian noise, LoG and histogram attacks DWT with zonal sampling I
4.36 Expanded experimental results with salt and peppers, JPEG and LPF attacks using DWT with zonal sampling II
4.37 Expanded experimental results with median filtering, sharpening and motion blurring using DWT with zonal sampling II
4.38 Expanded experimental results with Gaussian noise, LoG and histogram attacks DWT with zonal sampling II
4.39 Comparative results between BPNN and the proposed method
4.40 Comparative results between DCT and DWT with ZS1 and ZS2
5.1 Results of the applied measures achieved using DWT-DCT-Arnold Transform
6.1 MSE, PSNR and NCC of JPEG attacked and reconstructed gray level images
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2</td>
<td>MSE, PSNR and NCC of salt and peppers attacked and reconstructed gray level images</td>
<td>168</td>
</tr>
<tr>
<td>6.3</td>
<td>Contour approximation results from the test images using Adaptive Triangle method</td>
<td>170</td>
</tr>
<tr>
<td>6.4</td>
<td>Contour approximation results for Yes word image</td>
<td>172</td>
</tr>
<tr>
<td>6.5</td>
<td>Contour approximation results for Serpent image</td>
<td>173</td>
</tr>
<tr>
<td>6.6</td>
<td>Comparative results using different methods of contour approximation</td>
<td>176</td>
</tr>
<tr>
<td>6.7</td>
<td>Contour compression results in frequency domain DCT using SSPCE, Ramer method and zonal sampling I &amp; II</td>
<td>181</td>
</tr>
<tr>
<td>6.8</td>
<td>Contour compression results in frequency domain DWT using SSPCE, Ramer method and zonal sampling I &amp; II</td>
<td>183</td>
</tr>
<tr>
<td>6.9</td>
<td>Contour compression results in frequency domain DCT using SSPCE, Adaptive Triangle method and zonal sampling I &amp; II</td>
<td>185</td>
</tr>
<tr>
<td>6.10</td>
<td>Contour compression results in frequency domain DWT using SSPCE, Adaptive Triangle method and zonal sampling I &amp; II</td>
<td>185</td>
</tr>
</tbody>
</table>
## LIST OF FIGURES

1.1 Standard 2D grey level image “Lena” .................................................. 2
1.2 General watermarking technique ....................................................... 4
1.3 Digital watermarking system ............................................................ 4
1.4 Flow chart of the research objectives .................................................... 7
1.5 Scope of study using key charts ......................................................... 9
2.1 Block diagram of a watermark encoder ............................................... 13
2.2 Block diagram of a watermark decoder ............................................... 14
2.3 Block diagram of a comparator .......................................................... 15
2.4 Types of watermarks and watermarking techniques ............................. 19
2.5 Standard one level 2D image decomposition using DWT ..................... 22
2.6 Standard representation of 3-level 2D image decomposition using DWT 22
2.7 Flowchart 2-D DWT compression analysis .......................................... 24
2.8 Flowchart 2-D DWT reconstruction analysis ....................................... 25
2.9 Generalized DWT watermarking scheme ........................................... 26
2.10 DCT basic functions ......................................................................... 26
2.11 Definition of DCT regions .................................................................. 27
2.12 a) 2D DCT compression algorithm; b) 2D DCT reconstruction algorithm 29
2.13 Generalized DWT–DCT based watermarking ........................................ 30
2.14 Example block diagram using zonal sampling ...................................... 33
2.15 Attacks on watermarks ....................................................................... 36
2.16 Edge detection using Canny method applied to Lena image ............... 38
2.17 Edge detection using the Sobel method applied to Lena image ........... 38
2.18 The object contour follower (OCF) contour extraction method .......... 42
2.19 Block diagram of the multiple step contour extraction (MSCE) method 43
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.20</td>
<td>Block diagram of object-oriented contour extraction method</td>
</tr>
<tr>
<td>2.21</td>
<td>The eight rules to extract closed contour using the SSPCE method [4]</td>
</tr>
<tr>
<td>2.22</td>
<td>Chain coding using the (a) 8-Connectivity scheme and (b) 4-Connectivity scheme, (3x3 window)</td>
</tr>
<tr>
<td>2.23</td>
<td>Example of polygonal approximation</td>
</tr>
<tr>
<td>2.24</td>
<td>Example of contour approximation using Ramer method</td>
</tr>
<tr>
<td>2.25</td>
<td>Example of contour approximation using the trapezoid method</td>
</tr>
<tr>
<td>2.26</td>
<td>Flowchart of the Trapezoid method</td>
</tr>
<tr>
<td>2.27</td>
<td>Approximation by using Triangle method</td>
</tr>
<tr>
<td>2.28</td>
<td>Flowchart of the Triangle method</td>
</tr>
<tr>
<td>2.29</td>
<td>Combined DWT-DCT watermark embedding procedure</td>
</tr>
<tr>
<td>2.30</td>
<td>Multi-resolution DWT sub-bands of the original image</td>
</tr>
<tr>
<td>2.31</td>
<td>Combined DWT-DCT watermark extraction procedure</td>
</tr>
<tr>
<td>2.32</td>
<td>Joint DWT-DCT watermark embedding procedure</td>
</tr>
<tr>
<td>2.33</td>
<td>(a) Four multi-resolution DWT coefficient sets of the original image in level 2 to apply DWT to another level; (b) four selected multi-resolution DWT coefficient sets of the host image in level 3</td>
</tr>
<tr>
<td>2.34</td>
<td>Joint DWT-DCT watermark extraction procedure</td>
</tr>
<tr>
<td>3.1</td>
<td>Research design and methodology</td>
</tr>
<tr>
<td>3.2</td>
<td>Flowchart of the proposed area of research</td>
</tr>
<tr>
<td>3.3</td>
<td>Zonal sampling (a) algorithm I; (b) algorithm II</td>
</tr>
<tr>
<td>3.4</td>
<td>Example of zonal sampling algorithm I showing coefficient values of the HPF after applying DCT</td>
</tr>
<tr>
<td>3.5</td>
<td>Example of zonal sampling algorithm II showing coefficient values of the HPF after applying DCT</td>
</tr>
<tr>
<td>3.6</td>
<td>Binary watermark (a) logo CS, (b) Scrambled 1 time and (c) Scrambled 8 times</td>
</tr>
<tr>
<td>3.7</td>
<td>Host images (a) Tools; (b) Fruits</td>
</tr>
<tr>
<td>3.8</td>
<td>Curve approximation using the proposed Adaptive Triangle method</td>
</tr>
<tr>
<td>3.9</td>
<td>Flowchart of the proposed Adaptive Triangle method</td>
</tr>
<tr>
<td>3.10</td>
<td>The original contour using Adaptive Triangle method</td>
</tr>
</tbody>
</table>
3.11 The maximum distance for the curve segment from the straight line \( l_1 \)

3.12 The computation of the perpendicular distance between point \((x_p, y_p)\) and a line segment \( l_1 \)

3.13 The computation of the perpendicular distance between point \((43, 93)\) and a straight line \( l_1 \)

3.14 The curve segments for the new triangle

3.15 Curve approximation using the Ramer method

3.16 The original contour using the Ramer method

3.17 The curve segment of straight line \( l_1 \)

3.18 Computation the perpendicular distance between points in the lower curve segment and a line segment \( l_1 \)

3.19 The maximum distance for the lower curve segment from the straight line \( l_1 \)

3.20 The lower curve segments for the two new straight lines \( l_2 \) and \( l_3 \)

3.21 Computation of the perpendicular distance between points in the upper curve segment and a line segment \( l_1 \)

3.22 The maximum distance for the upper curve segment from the straight line \( l_1 \)

3.23 The upper curve segments for the two new straight lines \( l_2 \) and \( l_3 \)

3.24 The original and approximated contours

4.1 Embedding process of the proposed enhanced watermarking method

4.2 Extraction process of the proposed enhanced watermarking method

4.3 Host image (a) Tools; (b) Watermark image

4.4 (a) Watermarked image; (b) Blurred watermarked image

4.5 Extracted watermarks using DCT (a) zonal sampling I; (b) zonal sampling II
4.6 Test results of the host image using DCT with zonal sampling I (a) Watermarked image without attack; (b) Blurred watermarked image; (c) Compressed watermarked image; (d) Image after watermark extraction

4.7 The original host image before and after histogram equalization using DCT with zonal sampling I

4.8 Histogram of the original and watermarked image using DCT with zonal sampling I

4.9 Test results of the host image using DCT with zonal sampling II (a) Watermarked image without attack; (b) Blurred watermarked image; (c) Compressed watermarked image; (d) Image after watermark extraction

4.10 The original host image before and after histogram equalization using DCT with zonal sampling II

4.11 Histogram of the original and watermarked image using DCT with zonal sampling II

4.12 (a-d) Extracted watermarks using DCT with zonal sampling I

4.13 Extracted watermark using DCT with zonal sampling I after Gaussian attack

4.14 Extracted watermark using DCT with zonal sampling I after LoG attack

4.15 Extracted watermark using DCT with zonal sampling I after sharpening attack

4.16 (a-d) Extracted watermarks using DCT with zonal sampling II after motion attacks

4.17 Extracted watermark using DCT with zonal sampling II after Gaussian attack

4.18 Extracted watermark using DCT with zonal sampling II after LOG attack

4.19 Extracted watermark using DCT with zonal sampling II after sharpening attack

4.20 Various test host images for DCT (a) Tools; (b) Cameraman; (c) Rice; (d) Fruits; (e) Lena; (f) Baboon

4.21 The original watermark for DCT
4.22 Original host image (a) Lena and (b) Watermark “JNTU ACEA”  
4.23 Bar plots of the proposed method versus FIS  
4.24 Original host image (a) Mandrill; (b) Watermark “JNTU”  
4.25 Bar plots of the proposed method versus Neural Networks method  
4.26 (a-d) Extracted watermarks using DWT with zonal sampling I after motion attacks  
4.27 (a-d) Extracted watermarks using DWT with zonal sampling II after motion attacks  
4.28 The original watermark for DWT  
4.29 Histogram of the original and watermarked image using DWT with zonal sampling I  
4.30 Histogram of the original and watermarked image using DWT with zonal sampling II  
4.31 Bar plots of the proposed method versus BPNN method  
4.32 Original host image (a) Tools; (b) Watermark CS logo  
4.33 Bar plots of DCT and DWT with ZS1 and ZS2  
5.1 Proposed watermark embedding procedure  
5.2 (a) Cover object (Tools); (b) Watermark image (CS)  
5.3 Four multi-resolution DWT coefficient sets of the original image in level 1 to apply DWT to another level  
5.4 Four multi-resolution DWT coefficient sets of the original image in level 2 to apply DWT to another level  
5.5 Four selected multi-resolution DWT coefficient sets of the host image in level 3  
5.6 Binary watermark (a) CS logo; (b) Scrambled eight times  
5.7 Proposed watermark extraction procedure  
5.8 Original host image (a) Tools; (b) Fruits; (c) Cameraman; (d) Crowd  
5.9 Binary watermark (a) CS logo; (b) Scrambled one time; (c) Scrambled eight times  
5.10 (a) Watermarked image Tools without attack; (b) Extracted watermark image from the image Tools
5.11 (a) Watermarked image Fruits without attack; (b) Extracted watermark image from the image Fruits

5.12 Motion blurring attack (a) Blurred attacked watermarked image Tools; (b) Restored watermarked image; (c) Extracted watermark

5.13 Motion blurring attack (a) Blurred attacked watermarked image Fruits (b) restored watermarked image; (c) extracted watermark

5.14 Salt and Peppers attack on watermarked image Tools (a) Salt and Peppers; (b) Restored watermarked image after using filter; (c) Extracted watermark

5.15 Salt and Peppers attack on watermarked image Fruits (a) Salt and Peppers (b) Restored watermarked image after using filter; (c) Extracted watermark

5.16 JPEG attack on watermarked image Tools (a) JPEG attack (b) Extracted watermark

5.17 JPEG attack on watermarked image Fruits (a) JPEG attack (b) extracted watermark

5.18 Bar plots of the proposed method versus Amirgholipour et al method

6.1 Block diagram of the encryption and decryption process using SSPCE

6.2 Original and key images

6.3 Original biplane decomposition of the gray level Tools image

6.4 Results using JPEG compression (NCC=0.9955)

6.5 Results using Salt and Peppers noise (NCC=0.9979)

6.6 Binary test images a) Arabic letter; b) English letter; c) Hand; d) Man; e) Yes word; f) Serpent

6.7 Test results on a) Arabic letter; b) English letter; c) Hand; d) Man

6.8 Approximation results for Yes word image

6.9 Approximation results for Serpent image

6.10 Contour approximation results for several images using: a) Ramer method, b) Trapezoid method, c) Adaptive Triangle method
6.11 Comparison between the Adaptive Triangle method with Ramer and Trapezoid methods for MSE versus CR for a) Arabic letter; b) English letter; c) Hand; d) Man; e) Yes word; f) Serpent

6.12 Comparison between the Adaptive Triangle method with Ramer and Trapezoid methods for SNR Versus CR for a) Arabic letter; b) English letter; c) Hand; d) Man; e) Yes word; f) Serpent

6.13 Block diagram of contour extraction and compression using SSPCE and Ramer/Adaptive Triangle method

6.14 Extracted contours from the attacked watermarked image Tools in frequency domain DCT using SSPCE with (a) zonal sampling I and (b) zonal sampling II

6.15 Compressed contours from the attacked watermarked image Tools in frequency domain DCT using zonal sampling I and Ramer method

6.16 Compressed contours from attacked watermarked image Tools in frequency domain DCT using zonal sampling II and Ramer method

6.17 Extracted contours from the attacked watermarked image Tools in frequency domain DWT using SSPCE with (a) zonal sampling I and (b) zonal sampling II

6.18 Compressed contours from the attacked watermarked image Tools in frequency domain DWT using zonal sampling I and Ramer method

6.19 Compressed contours from the attacked watermarked image Tools in frequency DWT using zonal sampling II and Ramer method

6.20 Compressed contours from the attacked watermarked image Tools in frequency domain DCT using Adaptive Triangle method and zonal sampling I

6.21 Compressed contours from the attacked watermarked image Tools in frequency domain DCT using Adaptive Triangle method and zonal sampling II
6.22 Compressed contours from the attacked watermarked image
Tools in frequency domain DWT using Adaptive Triangle
method and zonal sampling I

6.23 Compressed contours from the attacked watermarked image
Tools in frequency domain DWT using Adaptive Triangle
method and zonal sampling II
| APPENDIX A | A.1 Embedding process of DCT | 205 |
| APPENDIX A | A.2 Extraction process of DCT | 208 |
| APPENDIX B | B.1 Embedding process of DWT | 210 |
| APPENDIX B | B.2 Extraction process of DWT | 213 |
| APPENDIX C | C.1 Calculating NCC | 216 |
| APPENDIX C | C.2 Calculating PSNR for image | 216 |
| APPENDIX C | C.3 Calculating MSE for image | 217 |
| APPENDIX C | C.4 Calculating (NL) Find Indices of largest coefficients values | 217 |
| APPENDIX D | D.1 Adaptive Triangle process | 218 |
| APPENDIX D | D.2 Calculating MSE for contour | 221 |
| APPENDIX D | D.3 Calculating length between two points | 221 |
| APPENDIX D | D.4 Calculating distance from the straight line | 221 |
LIST OF SYMBOLS AND ABBREVIATIONS

b  The length of the base of the Triangle

c  The comparator

C₀  The comparator function

d_{\text{max}}  Maximum distance between the point on the curve and the line

E₀  The computationally feasible function

f  The length between each two points of the Adaptive Triangle

ff  Segment length of the vertex point of the Adaptive Triangle

F_H  The high frequency components

F_L  The low frequency components

F_M  The mid frequency components

\tilde{G}  Low pass filter

h  The height of the Triangle

\bar{H}  High pass filter

I₀  The original Image

I_w  The watermarked Image

L_C  The input contour length of the Triangle

L_{CC}  The input contour length of the trapezoid

\ell_1  First straight line between the SP and EP

\ell_2  Second straight line between the SP and EP

\ell_3  Third straight line between the SP and EP

n  Time

r_{xy}  Correlation Coefficient

th  Threshold

th₁  Threshold 1

th₂  Threshold 2
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>W'</td>
<td>The extracted watermark</td>
</tr>
<tr>
<td>x</td>
<td>The correlation of the two signatures</td>
</tr>
<tr>
<td>α</td>
<td>The parameter that determines the coefficient value</td>
</tr>
<tr>
<td>σ</td>
<td>key security factor</td>
</tr>
<tr>
<td>δ</td>
<td>Threshold at comparator function</td>
</tr>
<tr>
<td>φ</td>
<td>The scaling function</td>
</tr>
<tr>
<td>ψ</td>
<td>The scaling a wavelet function</td>
</tr>
<tr>
<td>AC</td>
<td>Approximating Contour</td>
</tr>
<tr>
<td>BPNN</td>
<td>Back Propagation Neural Network</td>
</tr>
<tr>
<td>BPP</td>
<td>Bit Per Pixel</td>
</tr>
<tr>
<td>C</td>
<td>Sequence of the contour input</td>
</tr>
<tr>
<td>CC</td>
<td>Cartesian Co-ordinates</td>
</tr>
<tr>
<td>CR</td>
<td>Compression Ratio</td>
</tr>
<tr>
<td>D</td>
<td>The decoder function</td>
</tr>
<tr>
<td>DCT</td>
<td>Discrete Cosine Transform</td>
</tr>
<tr>
<td>DE</td>
<td>Difference Expansion</td>
</tr>
<tr>
<td>DFT</td>
<td>Discrete Fourier Transformation</td>
</tr>
<tr>
<td>DKT</td>
<td>Discrete Kekre Transformation</td>
</tr>
<tr>
<td>DWT</td>
<td>Discrete Wavelet Transform</td>
</tr>
<tr>
<td>E</td>
<td>The encoder function</td>
</tr>
<tr>
<td>EP</td>
<td>End Point</td>
</tr>
<tr>
<td>FFT</td>
<td>Fast Fourier Transform</td>
</tr>
<tr>
<td>FIS</td>
<td>Fuzzy Inference Systems</td>
</tr>
<tr>
<td>GIF</td>
<td>Graphics Interchange Format</td>
</tr>
<tr>
<td>GRNN</td>
<td>Generalized Regression Neural Network</td>
</tr>
<tr>
<td>HDR</td>
<td>High Dynamic Range</td>
</tr>
<tr>
<td>HL</td>
<td>High-Low</td>
</tr>
<tr>
<td>HH</td>
<td>High-High</td>
</tr>
<tr>
<td>HPF</td>
<td>High-Pass Filters</td>
</tr>
<tr>
<td>HVS</td>
<td>Human Visual System</td>
</tr>
<tr>
<td>I</td>
<td>Image</td>
</tr>
<tr>
<td>IntDCT</td>
<td>Integer Discrete Cosine Transform</td>
</tr>
<tr>
<td>K</td>
<td>The length between each two points of the Trapezoid</td>
</tr>
</tbody>
</table>
L The input contour length of the Adaptive Triangle
LH Low-High
LL Low-Low
LN Real distance between start & end point of vertex segment
LO Direct distance between start & end point of vertex segment
LPF Low-Pass Filters
LoG Laplacian of Gaussian
LSB Least-Significant-Bits
LSODE Linear Second order Ordinary Differential Equation
MPAA Motion Picture Association of America
MSCE Multiple Step Contour Extraction
MSE Mean Square Error
NCC Normalize Correlation Coefficient
NL Largest coefficients values
NOZ Number of the Zero Coefficients
NROI Non-Region of Interest
OCE Object-oriented Contour Extraction
OCF Object Contour Following
PN Point Number
PRN Pseudo Random Numbers
PSNR Peak Signal-to-Noise Ratio
QF Quality Factor
ROI Region of Interest
SNR Signal-to-Noise Ratio
SP Start Point
SSPCE Single Step Parallel Contour Extraction
STFT Short Time Fourier Transform
SVD Singular Value Decomposition
T The length between each two points of the Triangle
TT Segment length of the vertex point of the Triangle
VA Sequence of indices of the final vertices
W Watermark
WT Wavelet Transform
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZSM</td>
<td>Zonal Sampling Methods</td>
</tr>
<tr>
<td>ZS I</td>
<td>Zonal Sampling algorithm I</td>
</tr>
<tr>
<td>ZS II</td>
<td>Zonal Sampling algorithm II</td>
</tr>
<tr>
<td>1D</td>
<td>One-Dimensional</td>
</tr>
<tr>
<td>2D</td>
<td>Two-Dimensional</td>
</tr>
<tr>
<td>3D</td>
<td>Three-Dimensional</td>
</tr>
</tbody>
</table>
LIST OF PUBLICATIONS

Journals:


Conferences:


CHAPTER 1

INTRODUCTION

1.1 Introduction

In recent times, most valuable files and records are stored in digital formats to conveniently store, process or retrieve them for later use. The fast-phased communication systems, networks and the advent of the Internet made access to and manipulation of digital data a lot easier. For these reasons, an increasing need to use digital watermark for copyright protection, ownership assertion, content authentication, among others, have aroused. The author was motivated to meet the challenge that an ideal image watermarking algorithm requires namely imperceptibility, robustness, complexity and security with sufficient satisfaction.

Another challenge that this study faces is integrating contour compression on attacked watermarked image. The representation of extracted and compressed contours is very useful in solving problems like retrieval, recognition, matching shapes and medical image analysis. Both extraction and contour compression problems are challenging due to artifacts and noise. This study is interested in contour compression and its image detection ability.

1.2 Research Background

The basic idea of digital watermarking is to embed data (the watermark) or digital signature into a multimedia object such that the watermark can be detected or extracted later on to make an assertion, authenticity verification or ownership identification about that object. The embedded data can be of different formats. For
example, it can either be a pattern of bits or arbitrary real or integer number inserted into a digital media, pseudo random numbers (PRN), logos, digital signature or an encoded text. Not only should the embedded watermark be imperceptible, it should also be robust enough to survive to most common signal distortions and distortions caused by malicious attacks.

The digital signal to be protected may be audio, picture, song, 3D graphics, text, video, etc. As this research focuses on image (picture) as the signal and object for watermarking, it is found necessary to know some of its characteristics. According to [1], an image is defined as a representation, likeness or imitation of an object or thing; a graphic or clear description of something to represent something else. It can be kept in any representation, provided there is an algorithm that can convert it to a form usable by a display. Being characterized as a continuous two-dimensional (2D) function \( f(x, y) \), this real image's function must be digitized to become a digital image. This can be achieved by measuring the function’s value at a fixed number of locations (spatial sampling) and limiting the result to a fixed set of values (amplitude quantization) [2]. A standard grey level image representation “Lena” is shown in Figure 1.1.

![Figure 1.1 Standard 2D grey level image “Lena”](image)

Digital image frequency content plays a vital role in digital noise filtering, digital image restoration and digital image compression. Digital image transforms are used to obtain the digital image frequency content. The transforms used are two-dimensional, because the digital image itself is a two-dimensional signal. Their computation requires many numerical operations. Therefore, the construction of fast transform algorithms is an important task. Digital images require a large memory amount for their storage, thus, a reduction of the memory requirements is of utmost
importance. In many applications, digital image coding and compression take advantage of the information redundancy existing in the image to reduce its information content and to compress the image. Large compression ratios can be obtained by proper exploitation of information redundancy and excessive image compression results in image degradation [3].

An image can be processed to detect and recognize any information within the image. Hence, the information that corresponds to shape objects can be found in the contour of that object (image). The important step to obtain some features of recognizing an object is by using contour extraction from a given 2D-digital image. Contour extraction and compression is an important tool in pattern recognition and computer vision (through applications of shape description and representation) because it can be used in visual tasks such as contour matching in medical images or cartography or to enhance security on a visual task such as information hiding [4].

1.2.1 The evolution of information hiding

The idea of information hiding can be traced back to the middle ages. The earliest use has been to record the manufacturer's trademark on the product so that authenticity could be easily established. It has a long history of being associated with methods of secret communication. Ancient cryptographic technique processes information into an unintelligible form (encrypted) in order to transmit the information securely [5] [6]. The receiver then uses a "key" so that the encrypted message can be decoded (decrypting) to obtain back the original message. In the later years, this encryption method is used to prevent unauthorized access to digital content. However, this method has a drawback: it protects the data only as long as it is transmitted from one source of destination. The moment the data has been transmitted and received at its destination, it is no long secure and protected.

Steganography evolved as a complement to cryptography. Steganography is used to hide encrypted messages in mediums less likely to attract attention; it does not immediately arise the suspicion of something secret or valuable. It hides an important message in an unimportant medium instead but then again, it has encountered the same drawback as cryptography. Over time, these primitive cryptographic techniques improved, increasing speed, capacity and security of the
transmitted message. Then emerged a new information hiding technique: digital watermarking [6]. This technique embeds or hides information within a digital file without noticeably changing the file itself. Through technological advancements, this method has extended its use in texts, images, audio, video and other multimedia data.

1.2.2 General watermarking system

The basic elements of a simple watermarking system [7] are illustrated in block diagram of Figure 1.2. The watermark information is embedded into the host data in the encoding stage to produce watermarked data. In the decoding stage the watermark information is extracted from the watermarked data. The extracted watermark is compared with the original watermark for authentication.

![Figure 1.2 General watermarking technique](image)

A more expanded general watermarking system [8] is illustrated in the block diagram of Figure 1.3 where noise or attacks are applied to the watermarked image A, producing a noised or attacked watermarked image B, through a communication channel. A watermark key is required to embed and detect watermark.

![Figure 1.3 Digital watermarking system](image)
1.3 Problem statement and significance

Internet and other multimedia technologies have tremendously developed throughout the years. However, these fast-developing technologies have made it possible and easier for anybody to transmit, copy, distribute and create digital data. Contents manipulations or duplications of these data by various means are no longer that difficult. In last decade, revenue losses on motion pictures due to worldwide piracy amounted to 6.1$ billion a year [9]. Copyright protection is a very important subject but not the only one- in which watermarking appears as one of the very promising solutions. Although digital watermarking offers solutions, it does not have the same capacity or level of security as data encryption. It does not prevent the viewing or listening of content and is not immune to attacks, unintentionally or intentionally [10]. This raises the awareness of the copyright problems in the e-commerce age. There are several problems that are sought in this research. The need for digital watermarking methods that will enhance copyright protection, among others, are highly desirable; worthwhile improvements can be made in extension to the existing digital image watermarking schemes considering the aspects particularly on the embedding and extracting domains, coefficient selection, possible attacks and the human visual system. The content’s imperceptibility and robustness requirements influence watermarking designs. The problem is to design a watermark embedding algorithm which provides an imperceptible watermark, that is, one which does not noticeably degrade or destroy the original host image or signal. Using perceptual models appropriate for the different media types should be adapted. The other problem for designing watermarking schemes for multimedia is the type of degradations that the watermark is expected to survive and system requirements for media specific applications. An application that strengthens image data security, for example, can be integrated by utilizing their contours for better image recognition and detectability. There are also existing fundamental issues in this field which include problems related to image restoration, image enhancement, image segmentation, image recognition, etc. These contours can be compressed and transmitted in a shorter time constraints (speed). Therefore, to design a contour compression algorithm that enhances security on a visual task in information hiding is needed.
1.4 Research questions

Digital information technology is constantly looking for answers to the question: can any technique ensure copyright protection, security and tamper-resistance of digital contents by processing, transmitting and storing information encoded in systems where digital content can easily be transferred through communication channels? It is then the purpose of this research to present robust and imperceptible watermarking schemes with contour extraction and compression techniques that will provide a larger security and image detectability. Will these proposed enhanced schemes answer the necessities? Will these enhanced methods lead to good quality performance?

1.5 Research objectives

The objectives which are considered in this research that will ensure copyright protection, security and a tamper-resistance watermarking scheme are to develop designs for a robust and imperceptible watermarking technique. Furthermore, a scrambling technique is added for security measures. Contour compression will be used for approximation of active contours for quick transmission of information that enhances security on a visual task in information hiding from the attacked watermarked image. The objectives are illustrated in Figure 1.4 and are written down as follows:

1. To develop an enhanced algorithm using zonal sampling methods (ZSM) for digital watermarking.

2. To improve algorithms using DWT, DCT and a watermarking technique based on joint DWT-DCT transforms for embedding and extracting digital watermark.

3. To verify the effect of the watermarking methods DCT, DWT with ZSM, each method using different host images and different image sizes.

4. To measure the performance of the robustness and imperceptibility of the proposed watermarking algorithms and compare them with some well-known methods using mean square error (MSE), peak signal-to-noise ratio (PSNR), and Normalize Correlation Coefficient (NCC).
5. To introduce a design that can be used to describe and compress any contour in time and spectral domain.

6. To compare the designed enhanced contour compression algorithm with the existing compression methods using mean square error (MSE), signal-to-noise ratio (SNR) and compression ratio (CR).

Figure 1.4 Flow chart of the research objectives

1.6 Research scopes and limitations

It quickly becomes apparent that by considering these three digital watermarking requirements, i.e. robustness, imperceptibility and security, each of which having been the subject of several research works, the scope of this research is focused on the following integrating techniques:
1) Transform domain techniques DCT and DWT
2) Arnold Transform scrambling technique
3) Contour extraction and contour compression techniques

All input images used for watermarking will be grey level images and invisible watermark. The types of watermarks used are texts and logo/image of different sizes depending on the type of tests conducted. Attacks such as lossy compression and geometrical distortions are applied to the watermarked image. This research limits its application for digital images only. The scope of this research is illustrated in a key chart in Figure 1.5. There are a lot of existing established algorithms for a lot of problems concerning digital image watermarking, contour extraction and compression, but, only appropriate existing methods will be used in this research.

1.7 Research novelty and contribution

To the author's knowledge, there has been no study done using zonal sampling method in digital watermarking with contour compression. Thus, this research contributes:

1. An enhanced watermarking algorithm using zonal sampling methods (ZSM). It has the advantage of defining the region where the most important information is concentrated in an image and thus providing a more imperceptible watermark.

2. An efficient watermarking scheme with DCT, DWT and joint DWT-DCT transforms with good quality performance in terms of imperceptibility and robustness.

3. A combination of contour extraction and contour compression techniques from the attacked watermarked image add value to image detection ability and security. It can be used with a minimum level of image distortion thus giving a better image information and analysis.

4. A new method for contour compression called Adaptive Triangle is introduced. The short computational time of operations, good approximation quality and its simple implementation both in terms of memory requirement and fit criterion are its main advantages.
Figure 1.5 Scope of study using key charts
1.8 Thesis organization

This research is composed of seven chapters, which are as follows:

Chapter 2 provides the literature review. It describes the framework and principles of digital watermarking and reviews on various research studies related to this research. Chapter 3 describes the methodology of the proposed enhanced watermarking algorithms based on:

(i) DCT, DWT and zonal sampling methods.
(ii) Joint DWT-DCT with Arnold transform.
(iii) Contour extraction and contour compression techniques.

Chapter 4 describes the proposed enhanced watermarking algorithms DWT and DCT only. Its implementation and experimental results are discussed and analyzed. Chapter 5 describes the joint watermarking algorithm DWT-DCT using the pre-treatment method-Arnold transform. Its implementation, experimental results are discussed and analyzed. Chapter 6 describes the proposed Adaptive Triangle method on contour compression and how it is carried out or implemented. Experimental results of the proposed method are discussed and analyzed. Conclusions that can be drawn in this research and ideas for future work appear in Chapter 7.
CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This chapter presents a survey of literature providing a general background on digital watermarking, image’s edges and contours, contour extraction/approximation and contour compression methods. Related works relevant in this research are found in Section 2.9.

2.2 General framework of digital watermarking

In this section, a general framework [11, 12, 13, 14, 15, 16, 17 and 18] of digital watermarking and the basic parts of watermarking are discussed, especially for the case of image watermarking. Embedding information within the host signal is the essence of watermarking. For the sake of simplicity, image as watermarking content is chosen; most of the discussion applies to audios and videos as well. The embedding process can be considered successful only if the recipient of the watermarked image can reliably identify the very modification performed by the sender. Thus, the watermarking pattern is not much different than a digital communication system, whose main task is to ensure reliable information sharing between the sender and receiver. There are requirements to be met in order to have a little or less degradation of the host or cover object. Furthermore, this section provides information why digital watermarking technique is essential, what requirements are to be met and how they are used or what their applications are [11].
The subject to be embedded is called the digital watermark which is either a pattern of bits or arbitrary real or integer number inserted into a digital media. One of the most known digital watermarks is the pseudo-random-numbers (PRN) sequence of unique random numbers generated with a seed or a secret key value. The use of logo or small images as a watermark is gaining more popularity day by day as they are easy to identify by bare eyes. However, the most commonly used watermarks are sequence of 0s and 1s (binary bits), digital signature, encoded text, small binary Image, small grey scale/color image or logo [12, 13].

2.2.1 Digital watermarking

According to [14], digital watermarking is the practice of imperceptibility altering a “work” to embed a message about that “work”- either a copyright notice, digital rights information or identification notice. “Work” here is referred to as multimedia object. It is a process that embeds data (the watermark) or digital signature into a multimedia object such that the watermark can be detected or extracted later on to make an assertion about that object [15]. A message (digital watermark), once embedded into a digital signal, may be used to verify its authenticity or the identity of its owners, just as a paper bearing a watermark for visible identification [16]. The signal may be picture, song, 3D graphics, audio, text, video, etc. If the signal is copied, then, the information also is carried in the copy.

Like digital communication system, frameworks for image watermarking schemes are generally based on three parts [17, 18]: 1) The watermark to be embedded which is unique to the owner; 2) The encoder for embedding the watermark into the data (embedding algorithm) and 3) The decoder for extracting and verifying the embedded watermark. Fitting watermarking schemes to this model is often useful for comparing the likenesses and differences between two schemes simplifying the discussion of more complex digital watermarking schemes [11]. The encoding procedure is illustrated in Figure 2.1.
The watermark embedding process of inserting the watermark in the original host image is performed by the encoder. The decoder, on the other hand, performs the extraction and verification process to determine and trace the embedded watermark previously processed.

More specifically, the encoder takes the host image and the original watermark as inputs and produces the watermarked image. Inside the encoder, after the original image and the desired watermark have been selected, the first step is to choose an appropriate representation of the image for embedding the watermark. The data representation could be pixels, transform coefficients or some image features. The watermark is then transferred to the values (coefficients, pixels) and coordinates of the host image to determine its embedding place. The watermark can be placed anywhere within the image or throughout the image. Depending on the embedding rule, it can be placed in block by block manner or in some locations of the host image.

Denoting an image by $I$, a watermark by $W$ and the watermarked image by $I_w$. An encoder function $E$ takes an image $I$ and a watermark $W$ which then generates a new image which is called watermarked image $I_w$, mathematically expressed as [11]:

$$E(I, W) = I_w$$

The decoder inputs include the original watermark and the received (i.e., watermarked but possibly distorted or attacked) image. In some watermarking methods, a watermark can be extracted in its accurate form (watermark extraction procedure) while in other cases, it can be detected only if a specific given watermarking signal is existing in an image (watermark detection procedure).
Distinguishing factor between these procedures is that watermark extraction can prove ownership whereas watermark detection can only be used to verify ownership.

The decoder function $D$ takes the watermarked image $I_w$ ($I_w$ can either be a watermarked image or distorted watermarked image) whose ownership is to be determined. For recovering the watermark $W'$ from the host image, an additional $I_o$ (which is the original version of $I_w$) can also be included. The reason behind this is that some decoding methods may make use of the original image(s) in the watermarking process in order to provide extra robustness against unintentional or malicious attacks (12). Mathematically:

$$D(I_w, I_o) = W'$$  \hspace{1cm} (2.2)

The extracted watermark $W'$ will then be compared with the original watermark sequence by a comparator function $C_\delta$ and a binary output decision will be generated. It is 1 if there is a match and 0 otherwise, presented in the equation (18):

$$C_\delta(W', W) = \begin{cases} 
1, & c \leq \delta \\
0, & \text{otherwise} 
\end{cases}$$ \hspace{1cm} (2.3)

Where $c$ is the comparator, $x = C_\delta(W', W) \times c$ is the correlation of the two signatures and $\delta$ is a threshold. Not losing its generality, watermarking methods can be treated as a 3-tuple $(E, D, C_\delta)$. Figure 2.2 and Figure 2.3 demonstrate the decoder and comparator respectively.

![Figure 2.2 Block diagram of a watermark decoder [12]](image-url)
2.2.2 Digital watermarking requirements

The digital watermark has a bright future in many commercial applications. The type and form of the watermark as well as the amount of embedded information, depends on the target application. However, for digital watermarking schemes to be effective and deployed within the next-generation e-commerce infrastructure, they have to satisfy several requirements [15, 16, 17, 18 and 19]:

*Imperceptibility:* The imperceptibility of the watermark depends on the embedding algorithm used. After embedding, the quality of the original image should not be affected after it is watermarked and it should be invisible to the human eyes [15].

*Robustness:* Once embedded, the watermark should permanently reside in the host content throughout its lifetime and should be difficult to be extracted or detected without a proper key. For applications related to copyright protection, the definition of robustness is augmented to require that the watermark be extractable or detectable even if the watermarked content undergoes some form of manipulation or malicious attack. Since there are numerous ways that pirates can modify or tamper with the watermarked content, how to design a robust watermark for copyright protection is a very challenging task [16, 17].

*Security:* The watermark should only be detected by authorized person. It should be able to carry enough information to represent the uniqueness of the image, meaning, it has enough capacity or data payload [18].
From the above discussion, it is clear that the watermarking system has to satisfy many requirements for various applications and some of the requirements often contradict the other. For instance, the imperceptibility and the robustness requirements are two conflicting factors. From a signal processing point of view, imperceptibility limits the strength of the embedded watermark. On the other hand, it is important to encode a relatively strong watermark for it to be resistant to content manipulation and attacks. A similar conflict may hold for the requirements of information capacity and efficiency. Hence, certain trade-offs (or compromises) are involved in the design of an effective watermarking system [19].

2.2.3 Purposes and applications of digital watermarking

Over the years, watermarks added to digital content serve number purposes. One of which is ownership assertion aiming to establish ownership of the content i.e. image. It serves as a fingerprint to keep away unauthorized duplication and distribution of media content which are accessible to the public. It is used for authentication and integrity verification purposes, wherein the authenticator is inseparably bound to the content, whereby the author has a unique key associated with the content and can verify integrity of that content by extracting the watermark. Any change in digital content will be detected through content authentication using fragile or semi-fragile watermark known for its low robustness to modification in an image [20].

Furthermore, watermark is added as usage control to limit the number of copies created and at some point, would no longer create any more copies (e.g. DVD). It is also used for content labeling which embed bits into the data that gives further information about the content such as graphic image in time and place information. Lastly, for content protection, wherein the content is marked with a visible mark that is hardly removable so that it can be distributed publicly and freely.

One of the applications is in copyright protection systems which are intended to prevent or determine unauthorized copying of digital media [9]. In this use, a copy device retrieves the watermark from the signal before making a copy. The device makes a decision whether to copy or not, depending on the contents of the watermark. When a work is produced, copyright information can be inserted as a watermark. In case of dispute of ownership, this ownership can provide evidence.
Another application is in the source tracing. A watermark is embedded into a
digital signal at each point of distribution. If a copy of the work is found later, then
the watermark may be retrieved from the copy and the source of the distribution
known. This technique reportedly has been used to detect the source of illegally
copied movies. As broadcast monitoring application [21], digital watermarking is
used to monitor unauthorized broadcast stations. It can verify whether the content is
really broadcasted or not. Fragile watermarks are used for tamper detection. If the
watermark is destroyed or degraded, it indicates the presence of tampering and hence
digital content cannot be trusted. Unfortunately, there is not a universal
watermarking technique to satisfy all these purposes [22]. The content in the
environment that it will be used determines the digital watermarking technique.

2.3 Digital image watermarking categories

Watermarking techniques can be divided into four categories according to the type of
document to be watermarked: image watermarking, video watermarking, audio
watermarking and text watermarking. According to the human perception, the digital
watermarks can be divided into three different types: visible watermark, invisible-
robust watermark/ invisible-fragile watermark and dual watermark [23].

Visible watermark is a secondary translucent overlaid into the primary image.
The watermark appears visible to a casual viewer on a careful inspection. The
invisible-robust watermark is embedded in such a way that alternations made to the
pixel value are perceptually not noticed and it can be recovered only with appropriate
decoding mechanism. The invisible-fragile watermark is embedded in such a way
that any manipulation or modification of the image would alter or destroy the
watermark. Dual watermark is a combination of a visible and an invisible watermark.
In this type of watermark, an invisible watermark is used as a backup for the visible
watermark. An invisible robust private watermarking scheme requires the original or
reference image for watermark detection; whereas the public watermarks do not. The
class of invisible robust watermarking schemes that can be attacked by creating a
“counterfeit original” is called invertible watermarking scheme [12, 23].
The watermark extraction/detection process of an imperceptible robust blind watermarking method does not need to be aided by the original for watermark extraction/detection. However, non-blind watermarking methods do require the original image to help extracting them. The class of invisible invertible robust watermarking method is one where the original image can be obtained by reversing the watermarking procedure.

A watermarking scheme \((E, D, C_\delta)\) is called quasi-invertible, if for any watermarked image \(I_w\), there exists a function \(E^{-1}\) such that:

\[
E^{-1}(I_w) = (I_o, W) \tag{2.4}
\]

\[
C_\delta (D(I_w), W') \tag{2.5}
\]

Where, \(E^{-1}\) is a computationally feasible function, \(W\) belongs to the set of allowable watermarks and the images \(I_o\) and \(I_w\) are perceptually similar. Otherwise, the watermarking scheme is non-quasi-invertible.

Digital watermark can be also classified in terms of application as sourced-based or destination-based watermarks [12]. Source-based watermarks are desirable for ownership identification or authentication where a unique watermark identifying the owner (seller) is introduced to all the copies of a particular image being distributed.

A source-based watermark could be used for content authentication and to determine whether a received image or other electronic data has been tampered with or not. The watermark could also be destination based where each distributed copy gets a distinctive watermark identifying the particular buyer. In legal selling cases, the destination based watermark can be used to track the buyer. Refer to Figure 2.4 for illustration.
2.4 Digital watermarking techniques

Watermarking techniques can be divided into various categories in various ways. The watermarks can be applied in spatial domain. An alternative to spatial domain watermarking is frequency domain watermarking. In this section, various watermarking techniques that are used in the watermarking process are discussed.

2.4.1 Spatial domain

Spatial domain techniques such as LSB [24, 25] are the most straight-forward method of steganography (information hiding) and watermark embedding which embeds the watermark into the least-significant-bits of the cover object. However,
Despite its simplicity, their works bring a host of drawbacks. It lacks basic robustness, is vulnerable to noise and it can be attacked easily. Watermark casting is performed in the spatial domain by slightly modifying the intensity of randomly selected image pixels [26]. Watermark detection does not require the existence of the original image and is carried out by comparing the mean intensity value of the marked pixels against that of the pixels not marked. Statistical hypothesis testing is used for this purpose. In [27], one of the watermarks is based on image features in the spatial domain and the other one is based on image features in the frequency domain. Both of the watermarks complement each other. A tolerance to modifications, below a threshold, is obtained by protecting the spatial domain edge features using approximate message authentication codes, which are able to tolerate minor modifications. By protecting the frequency domain transform coefficients with error correcting codes, errors or modifications are located and corrected if possible. Other spatial domain techniques such as the predictive coding, correlation-based techniques and patchwork techniques [28] have been proposed but the robustness, image quality and data payload have been greatly compromised.

2.4.2 Frequency domain

In several applications, it might be essential to analyze a given signal. The structure and features of the given signal may be better understood by transforming the data into another domain [29, 30, 31, 32, 33 and 34]. There are several transforms available like the Fourier transform, Hilbert transform, wavelet transform, etc. The Fourier transform is probably the most popular transform. However, the Fourier transform gives only the frequency-amplitude representation of the raw signal losing the time information. Therefore, it is not wise to use the Fourier transform in applications which require both time as well as frequency information at the same time.

The Short Time Fourier Transform (STFT) was developed to overcome this drawback. However, the STFT gives a fixed resolution at all times and this shortcoming was overcome by the development of the wavelet transform. The frequency component of a signal at a particular time instant cannot be exactly determined. This follows directly from the Heisenberg's Uncertainty Principle
which states that the momentum and position of a moving particle cannot be exactly determined. Thus, the best method to do is to investigate which frequency components exist in any given interval of time. The high frequency components are better resolved in time and low frequency components are better resolved in frequency. This is the reason why the wavelet transform has overtaken the STFT [8, 31 and 32]. Other wavelet transforms such as Discrete Fourier Transformation (DFT), the Haar wavelet, which is the simplest of all wavelets and its operation is easy to understand but have their limitations too. They are piecewise constant and hence produce irregular, blocky approximations. There are several other wavelets available like the Daubechies wavelet, Donoho’s wavelet, Meyer wavelet, etc [29, 33]. However, these wavelets are not easy to comprehend and are also computationally intensive. In [34], discrete cosine transform (DCT) and discrete wavelet transform (DWT) are used for embedding and extracting watermark and concluded that DWT gives better image quality than DCT.

In the following two sub-sections, Discrete Wavelet Transform and Discrete Cosine Transform will be thoroughly discussed since the scope of this research mainly concerns these two frequency domain (image compression) techniques.

2.4.2.1 Discrete wavelet transform (DWT)

Image compression is one of the most important applications of wavelets. Wavelets are mathematical functions that satisfy certain properties and can be used to transform one function representation into another [35] while [36] explains: “Wavelet transform performs multi-resolution analysis. Multi-resolution analysis is simultaneous representation of image on different resolution levels”. Wavelet Transform (WT) represents an image as a sum of wavelet functions with different locations and scales. DWT has become researchers’ focus for watermarking as it is very similar to the theoretical model of Human Visual System (HVS) [3]. Moreover, it offers multi-resolution representation of an image or signal and gives perfect reconstruction of decomposed image. Image itself is considered as two dimensional signals [2]. When image is passed through series of low pass and high pass filters, DWT decomposes the image into sub bands of different resolutions. Decompositions can be done at different DWT levels or scales.
As images are treated as 2D signals, they change horizontally and vertically, thus, 2D wavelet analysis should be used for images [37]. Wavelet compression technique uses the wavelet filters for image decomposition; image is divided into approximation and detail sub-images. First, filter is applied along the rows and then applied along the columns, thus, the operation results in four bands: low-low (LL), low-high (LH), high-low (HL) and high-high (HH) as illustrated in its standard form in Figure 2.5 [31]. The low-low frequency part can be further processed so it is again subdivided into four bands. At every level, four sub-images are obtained: the approximation, the vertical sub-image, the horizontal sub-image and the diagonal sub-image. This is shown in Figure 2.6 which is a standard representation of 3-level decomposition of a 2D image [38].

![Figure 2.5 Standard one level 2D image decomposition using DWT][31]

![Figure 2.6 Standard representation of 3-level 2D image decomposition using DWT][38]
Any decomposition of an image into wavelets involves a pair of waveforms: one to represent the high frequencies corresponding to the detailed parts of an image and one for the low frequencies or smooth parts of an image [39, 40]. At the resolution level \( j \), the approximation of the one-dimensional level (1-D) function \( f_j(t) \) and its details denoted by \( d_k(t) \) are included in approximation at resolution level \( j+1 \):

\[
f_{j}(c+1) = f_j(t) + d_k(t)
\]  

(2.6)

This procedure can be repeated several times and function \( f(t) \) can be given as:

\[
f(t) = f_j(t) + \sum_{k=j}^{m} d_k(t)
\]  

(2.7)

DWT for an image as a 2-D signal can be derived from 1D DWT. The easier way for obtaining scaling and wavelet function for two dimensions is by multiplying two 1-D scaling function:

\[
\varphi(x,y) = \varphi(x)\varphi(y)
\]  

(2.8)

where \( \varphi \) = the scaling function

Wavelet functions for 2-D DWT can be obtained by multiplying two wavelet functions and scaling function for 1-D analysis. Three wavelet functions that scans in horizontal direction \( \psi(x,y) = \varphi(x)\psi(y) \), vertical direction \( \psi(x,y) = \psi(x)\varphi(y) \) and diagonal \( \psi(x,y) = \psi(x)\psi(y) \) direction [41, 42 and 43].

Each row of an \( M \times N \) image is filtered and then down sampled which gives two \( N\times M/2 \) images. Then, each column is filtered and sub-sampled which gives four \( N/2 \times M/2 \) images. Of these four sub-images, the one obtained by low pass filtering rows and columns is referred as LL image; the one obtained by low pass the rows and high pass filtering the columns is referred to as the LH image and the other two are HL and HH images. Each of these sub-images can be further decomposed (compressed) in similar manner as shown in Figure 2.7 [43]. The reconstruction (decompression) analysis flowchart for this method is shown in Figure 2.8 [43].
The DWT is defined [43] as:

$$W_\varphi(j_0, k) = \frac{1}{\sqrt{M}} \sum_x f(x) \varphi_{j_0,k}(x)$$  \hspace{1cm} (2.9)$$

$$W_\psi(j, k) = \frac{1}{\sqrt{M}} \sum_x f(x) \psi_{j,k}(x)$$  \hspace{1cm} (2.10)$$

Where \(j \geq j_0\). The Inverse DWT (IDWT) is defined [43] as:

$$f(x) = \frac{1}{\sqrt{M}} \sum_k W_\varphi(j_0, k) \varphi_{j_0,k}(x) + \frac{1}{\sqrt{M}} \sum_{j=j_0}^{J-1} \sum_k W_\psi(j, k) \psi_{j,k}(x)$$  \hspace{1cm} (2.11)$$

Where \(f(x)\) is the host signal, \(\varphi_{j_0,k}(x)\) and \(\psi_{j,k}(x)\) are two basic functions of the discrete variable. Normally we let \(j_0 = 0\) and select \(M\) to be a power of 2 (i.e. \(M = 2^J\)) so that the summations in equation (2.9), equation (2.10) and equation (2.11) are performed over \(x = 0, 1, 2, J-1, j = 0, 1, 2, \ldots, J-1\) and \(k = 0, 1, 2, \ldots, 2^J-1\). The coefficients defined in equation (2.9) and equation (2.10) are respectively called approximation and detail coefficients.
REFERENCES


