

Multimedia Systems and Applications

Series editor

Borko Furht

More information about this series at: <http://www.springer.com/series/6298>

Amit Kumar Singh • Basant Kumar
Ghanshyam Singh • Anand Mohan
Editors

Medical Image Watermarking

Techniques and Applications

 Springer

Editors

Amit Kumar Singh
Department of Computer Science
and Engineering
Jaypee University of Information
Technology
Waknaghat, Solan, Himachal Pradesh, India

Basant Kumar
Department of Electronics and
Communication Engineering
Motilal Nehru National Institute
of Technology
Allahabad, Uttar Pradesh, India

Ghanshyam Singh
Department of Electronics and
Communication Engineering
Jaypee University of Information
Technology
Waknaghat, Solan, Himachal Pradesh, India

Anand Mohan
Department of Electronics Engineering
Indian Institute of Technology (BHU)
Varanasi, Uttar Pradesh, India

Multimedia Systems and Applications

ISBN 978-3-319-57698-5

ISBN 978-3-319-57699-2 (eBook)

DOI 10.1007/978-3-319-57699-2

Library of Congress Control Number: 2017947800

© Springer International Publishing AG 2017

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Printed on acid-free paper

This Springer imprint is published by Springer Nature

The registered company is Springer International Publishing AG

The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

Information and communication technology (ICT) has been potentially useful for cost-effective and speedy transmission of electronic patient record (EPR) over open channels for telemedicine applications. However, attempts of malicious attacks or hacking for unauthorized access, alteration, modification, deleting, or even preventing the transfer of EPR possess challenging tasks in the implementation of dependable telemedicine systems. Therefore, the authenticity of EPR and related medical images is of prime concern as they form the basis of inference for diagnostic purposes. In such applications, tamperproofing and guaranteed originality of EPR/medical images is achieved by embedding some kind of watermark(s) which must be secure and robust against malicious attacks. Although numerous robust watermarking algorithms have been proposed, there has been a rat race situation between the robustness of watermark and malicious attacks, making robust watermarking an interesting challenging area for researchers.

In view of addressing the above challenges of telemedicine systems concerned with the authenticity and security aspects of transmitted EPR/medical image(s) over open channels for telemedicine, this book presents the state-of-the-art medical image watermarking techniques and algorithms for telemedicine and other emerging applications. The book begins with a conceptual introduction of digital watermarking, important characteristics, novel applications, different watermarking attacks, and benchmark tools followed by a detailed literature review on spatial and transform domain medical image watermarking techniques, their merits, and limitations. Subsequently, an in-depth analysis of available techniques of medical image watermarking is highlighted with their limitations. Further, the book presents improved/novel methods of watermarking for e-health applications which offer higher robustness, better perceptual quality, increased embedding capacity, and a secure watermark. For telemedicine, tele-ophthalmology, telediagnosis, and tele-consultancy services, medical images play a prominent role for instant diagnosis and understanding of crucial diseases as well as to avoid the misdiagnosis. In order to overcome this problem, the book includes some improved/novel medical image watermarking methods. The book also explores the important spatial and transform domain techniques followed by the major performance matrices. Finally, the book includes

emerging trends and research challenges in robust watermarking and watermark security with special reference to telemedicine applications.

The authors believe that the book would provide a sound platform for understanding the medical image watermarking paradigm and prove as a catalyst for researchers in the field and shall be equally beneficial for professionals. In addition, the book is also helpful for senior undergraduate and graduate students, researchers, and industry professionals working in the area as well as other emerging applications demanding robust watermarking.

The book contains ten chapters. Chapter 1 presents a brief introduction of digital watermarking techniques, their classification, important characteristics, and emerging applications of digital watermarks followed by the essential requirements of medical image watermarking.

Chapter 2 contains a detailed review of the literature on medical image watermarking techniques and algorithms using medical image(s) as covers because they offer higher data embedding capacity. It includes both, the computationally simple but fragile watermarking in “spatial domain” and computationally expensive “transform domain” techniques that offer robust watermarking. The spatial domain watermarking using least significant bit (LSB) substitutions and the correlation-based and spread-spectrum techniques are discussed wherein the watermark data is embedded directly by manipulating the pixel values, bit stream, or code values of the host signal (cover media). The transform domain watermarking modulates the coefficients of a transform, e.g., discrete Fourier transform (DFT), discrete cosine transform (DCT), discrete wavelet transform (DWT), and singular value decomposition (SVD). Computationally complex transform domain watermarking techniques offer superior robustness of watermarked data as compared to spatial domain techniques. The chapter specially focuses on wavelet-based watermarking because it offers major benefits of space-frequency localization, multi-resolution representation, multi-scale analysis, reducing blocking artifact, adaptability, and linear complexity besides being compatible with JPEG 2000 image coding.

Chapter 3 describes detailed techniques of watermarking in spatial and transform domains along with major performance evaluation parameters: peak signal-to-noise ratio (PSNR), weighted peak signal-to-noise ratio (WPSNR), mean square error (MSE), universal image quality index, structural similarity index measure (SSIM), normalized correlation (NC), noise visibility function (NVF), and bit error rate (BER) of the watermarking algorithms. In addition, this chapter also discusses important watermark attacks and the use of a standard benchmark tool to measure the robustness of watermarking algorithms.

Chapter 4 presents a new robust hybrid watermarking technique using fusion of DWT, DCT, and SVD instead of applying these techniques individually or in combination thereof. It is based on initially decomposing the host image into first-level DWT followed by transformation of low-frequency band (LL) and watermark image using DCT and SVD. Then, the singular vector of the watermark image is embedded in the singular component of the host image, and the watermarked image is generated by inverse SVD on modified singular vector and original orthonormal matrices, followed by inverse DCT and inverse DWT. The proposed method has been extensively

tested and analyzed against known attacks such as JPEG, Gaussian, Salt-and-Pepper, Speckle, and Poisson. The experimental results have revealed that the proposed technique achieves superior performance in respect of imperceptibility, robustness, and capacity as compared to the techniques reported in literature. Watermark robustness has been checked using the benchmarking software “Checkmark,” and it is found that the suggested algorithm is robust against the “Checkmark” attacks. Further, the performance of the proposed watermarking method by applying encryption on patient text data before embedding the watermark has been investigated.

Chapter 5 addresses the issue of faulty watermark due to channel noise distortions which may result into inappropriate disease diagnosis in telemedicine environment. The effect of channel noise distortions in creating faulty watermark has been minimized by encoding the watermark using error correction codes (ECCs) before embedding. The effects of Hamming, BCH, Reed–Solomon, and hybrid ECC consisting of BCH and repetition code on the robustness of text watermark and the cover image quality have been investigated. It is found that the hybrid ECC code has better performance as compared to that of the other three codes, and the suggested method is robust against known attacks without significant degradation of the cover image quality. Further, the performance of the proposed watermarking method by applying Reed–Solomon ECC on encrypted patient data before embedding the watermark has been presented. The robustness of this method has been checked using “Checkmark” and is found that the proposed method is robust against the “Checkmark” attacks.

Chapter 6 discusses the solution to the growing concern of medical identity theft. This is based on the development of new secure watermarking techniques of medical data/image using multiple watermarking where patient identity reference and telemedicine center logo are used as text watermark and image watermark, respectively, for identity authentication. The embedding of watermark is based on DWT and spread-spectrum where pseudorandom noise (PN) sequences are generated corresponding to each watermark bit of the image watermark. The spread-spectrum has been used to secure the image watermark, and enhancement in robustness of the text watermark has been achieved using BCH-based ECC before embedding. The performance of this watermarking method has been tested against known attacks. Subsequently, simultaneous embedding of three watermarks, i.e., doctor code, image reference code, and patient record using multilevel watermarking of cover medical image, has been proposed to address the issues of data security, data compaction, unauthorized access, and tamperproofing. The suggested method uses wavelet-based spread-spectrum watermarking where the encrypted text watermarks are embedded at multiple levels of the DWT sub-bands of the cover image. The performance of the developed scheme is evaluated and analyzed against known attacks by varying watermark sizes and the gain factor. It is reported that the suggested multilevel watermarking enhances the security of the patient data and thus it can be potentially useful in the prevention of patient identity theft.

In chapter 7, the authors proposed new secure multiple watermarking techniques using eye image as cover for secure and compact medical data transmission in teleophthalmology applications. The method is based on initially embedding of four

different watermarks using fusion of DWT and SVD. A secure hash algorithm (SHA-512) is used for enhancing the security feature of the proposed watermarking technique. The performance in terms of “NC” and “BER” of the developed scheme is evaluated and analyzed against known signal processing attacks and “Checkmark” attacks. The method is found to be robust against all the considered attacks.

Chapter 8 contains an algorithm for multiple watermarking based on DWT, DCT, and SVD which can be extremely useful in the prevention of patient identity theft in medical applications. The proposed method uses three different watermarks in the form of medical lump image watermark, doctor signature, identification code, and diagnostic information of the patient as the text watermark for identity authentication purpose. In order to improve the robustness performance of the image watermark, back propagation neural network (BPNN) is applied to the extracted image watermark to reduce the noise effects on the watermarked image. The security of image watermark is also enhanced by using Arnold transform before embedding into the cover. Further, the symptom and signature text watermarks are also encoded by lossless arithmetic compression technique and Hamming error correction code, respectively. The compressed and encoded text watermark is then embedded into the cover image. The experimental results are examined by varying the gain factor, different sizes of text watermarks, and different cover image modalities. The results are provided to illustrate that the proposed method is able to withstand different signal processing attacks and has been found to give an excellent performance for robustness, imperceptibility, capacity, and security simultaneously. The robustness performance of the method is also compared with other reported techniques. Finally, the visual quality of the watermarked image is also evaluated by the subjective method. This shows that the visual quality of the watermarked images is acceptable for diagnosis at different gain factors.

In chapter 9, the authors presented a robust and secure multiple watermarking method using a combination of DWT, DCT, SVD, selective encryption, error correcting codes, and neural network. The proposed technique initially decomposes the host image into third-level DWT where the vertical frequency band at the second-level and low frequency sub-band at the third-level DWT are selected for embedding image and text watermark, respectively. Further, the proposed method addresses the issue of ownership identity authentication; multiple watermarks are embedded instead of a single watermark into the same multimedia objects simultaneously, which offer the extra level of security and reduced storage and bandwidth requirements in important applications areas. Moreover, the robustness image watermark is also enhanced by using “BPNN,” which is applied on extracted watermark to minimize the distortion effects on the watermarked image. In addition, the method addresses the issue of channel noise distortions in identity information. This has been achieved using ECCs for encoding the text watermark before embedding into the host image. The effects of Hamming and BCH codes on the robustness of personal identity information in the form of text watermark and the cover image quality have been investigated. Recently, selective encryption is computationally fast for large size multimedia documents offering secure document dissemination for various multimedia applications. In order to reduce the computation time and

enhance the security of the documents, selective encryption is applied on watermarked image, where only the important multimedia data is encrypted. The proposed method has been extensively tested and analyzed against known attacks. Based on experimental results, it is established that the proposed technique achieves superior performance in respect of robustness, security, and capacity with acceptable visual quality of the watermarked image as compared to reported techniques. Finally, we have evaluated the image quality of the watermarked image by subjective method.

Finally, chapter 10 discusses the recent trends and potential research challenges of the state-of-the-art watermarking techniques in brief. It includes medical image watermarking, 3D model watermarking, watermarking in cloud computing and multi-core environment, biometric watermarking, watermarking using mobile device, and securing online social network contents. The chapter also reviews several aspects about digital watermarking in different domains. Meanwhile, it discusses the requirements and potential challenges that the watermarking process faces.

This book is an extension of the Ph.D. thesis of Dr. Amit Kumar Singh submitted to the Department of Computer Engineering, National Institute of Technology (Institution of National Importance), Kurukshetra, Haryana, 2015, under the supervision of Dr. Mayank Dave and Prof. Anand Mohan.

First and foremost, the author is heartily thankful to *Prof. Borko Furht*, series editor, Multimedia Systems and Applications, for his guidance, promotion, encouragement, and support in every stage of my research work. His knowledge, kindness, patience, sincerity, and vision have provided me with lifetime benefits.

I am grateful to *Prof. S. P. Ghreera*, head of the Department of Computer Science & Engineering, Jaypee University of Information Technology, Wagnaghat, Solan, Himachal Pradesh, for his consistent support, encouragement, and invaluable suggestions throughout the manuscript preparation. It is his enlightened guidance and vision and generous support that made it possible for me to finish this work within the stipulated time.

The authors are indebted to numerous colleagues for valuable suggestions during the entire period of the manuscript preparation.

We would also like to thank the publishers at Springer, in particular *Susan Lagerstrom-Fife*, senior publishing editor/CS Springer, for their helpful guidance and encouragement during the creation of this book.

We are sincerely thankful to all authors, editors, and publishers whose works have been cited directly/indirectly in this manuscript.

The authors would not justify their work without showing gratitude to their family members who have always been the source of strength to tirelessly work to accomplish the assignment. I owe my deepest gratitude toward my wife, *Sweta Singh*, for her continuous support and understanding of my goals and aspirations. Her infallible love and support has always been my strength. Her patience and sacrifice will remain my inspiration throughout my life. I am thankful to my daughters, *Anandi* and *Anaya*, for loving me and not complaining for their share of time I devoted for carrying out my work. I owe a lot to my parents, who encouraged and

helped me at every stage of my personal and academic life and longed to see this achievement come true.

The second author, Dr. Basant Kumar, is also thankful to his wife, Dr. Namrata Parashar, and daughters, Anushka and Pragya, for sparing their time for this work. Further, the author wants to pay a deep sense of respect and gratitude to his grandfather (maternal) Sri Ram Uchit Singh for his life long support and his consistent encouragement and motivation for writing a book.

The third author, Prof. Ghanshyam Singh, is also thankful to his wife, Swati Singh; daughter, Jhanvi; and son, Shivam, for sparing their time for this work.

The fourth author, Prof. Anand Mohan, is also thankful to his wife, *Sudha Mohan*; daughter, *Amrita Mohan*; and son, *Ashish Mohan*, for their sparing time for this work.

Waknaghat, Solan, India
Allahabad, India
Waknaghat, Solan, India
Varanasi, India

Amit Kumar Singh
Basant Kumar
Ghanshyam Singh
Anand Mohan

Special Acknowledgments

We gratefully acknowledge the authorities of Jaypee University of Information Technology, Wagnaghat, Solan, Himachal Pradesh, India, for their kind support to come up with this book.

Contents

1 Digital Image Watermarking: Concepts and Applications	1
Amit Kumar Singh, Basant Kumar, Ghanshyam Singh, and Anand Mohan	
2 Medical Image Watermarking Techniques: A Technical Survey and Potential Challenges	13
Amit Kumar Singh, Basant Kumar, Ghanshyam Singh, and Anand Mohan	
3 Analytical Study and Performance Evaluation of Medical Image Watermarking Techniques.....	43
Amit Kumar Singh, Basant Kumar, Ghanshyam Singh, and Anand Mohan	
4 Robust and Imperceptible Hybrid Watermarking Techniques for Medical Images.....	61
Amit Kumar Singh, Basant Kumar, Ghanshyam Singh, and Anand Mohan	
5 Robust and Secure Multiple Watermarking for Medical Images.....	95
Amit Kumar Singh, Basant Kumar, Ghanshyam Singh, and Anand Mohan	
6 Secure Spread Spectrum Based Multiple Watermarking Technique for Medical Images	125
Amit Kumar Singh, Basant Kumar, Ghanshyam Singh, and Anand Mohan	
7 Robust and Secure Multiple Watermarking Technique for Application in Tele-Ophthalmology	159
Amit Kumar Singh, Basant Kumar, Ghanshyam Singh, and Anand Mohan	

8 Secure Multiple Watermarking Technique Using Neural Networks.....	175
Amit Kumar Singh, Basant Kumar, Ghanshyam Singh, and Anand Mohan	
9 Securing Patient Data Through Multiple Watermarking and Selective Encryption	195
Amit Kumar Singh, Basant Kumar, Ghanshyam Singh, and Anand Mohan	
10 State-of-the-Art Techniques of Image Watermarking: New Trends and Future Challenges	227
Amit Kumar Singh, Basant Kumar, Ghanshyam Singh, and Anand Mohan	

List of Abbreviations

AES	Advanced Encryption Standard
ASCII	American Standard Code for Information Interchange
BCH	Bose, Chaudhuri, and Hocquenghem
BER	Bit error rate
CDMA	Code division multiple access
CS	Compressed sensing
DCT	Discrete cosine transform
DFT	Discrete Fourier transform
DIBR	Depth-image-based rendering
DICOM	Digital Imaging and Communications in Medicine
DWPT	Discrete wavelet packet transform
DWT	Discrete wavelet transform
ECC	Error-correcting codes
EPR	Electronic patient record
GA	Genetic algorithm
HMM	Hidden Markov model
HVS	Human visual system
ICA	Independent component analysis
ICT	Information and communication technology
IWT	Integer wavelet transform
LSB	Least significant bit
LZW	Lempel–Ziv–Welch
MPEG	The Moving Picture Experts Group
MSE	Mean square error
NC	Normalized correlation
NROI	Non-region of interest
NVF	Noise visibility function
PCA	Principal component analysis
PN	Pseudorandom noise
PSNR	Peak signal-to-noise ratio
QF	Quality factor

ROI	Region of interest
SNR	Signal-to-noise ratio
SPIHT	Set partitioning in hierarchical trees
SVD	Singular value decomposition
SVM	Support vector machine
WBCT	Wavelet-based contourlet transform

List of Figures

Fig. 1.1	The prisoner’s problem	2
Fig. 1.2	Classification of watermarking techniques	4
Fig. 1.3	The watermark process (a) embedding and (b) extraction	6
Fig. 1.4	Potential applications of watermarking	7
Fig. 1.5	Main advantages of medical image watermarking	9
Fig. 1.6	Major security requirements for EPR data.....	10
Fig. 3.1	Pyramid structure of three levels DWT.....	48
Fig. 3.2	Four level sub-band decomposition of CT test image	48
Fig. 3.3	Definition of DCT regions	49
Fig. 3.4	Classification of possible attacks in digital watermarking.....	55
Fig. 4.1	Image (a) cover (b) watermark and (c) watermarked	70
Fig. 4.2	NC performance of the proposed method against known attacks at gain factor (α) = 0.9	73
Fig. 4.3	Comparison of NC values with other reported method at gain factor (α) = 0.5	73
Fig. 4.4	Comparison of NC values with other reported methods against known attacks	74
Fig. 4.5	Robustness performance of the proposed method against ‘Checkmark’ attacks	76
Fig. 4.6	Multiple watermarks (a) embedding and (b) extraction process	77
Fig. 4.7	(a) Cover CT Scan image and Watermarked CT Scan images at (b) α = 0.05 (c) α = 0.5 and (d) α = 1.0	78
Fig. 4.8	Watermarks (a) Image and (b) Text	78
Fig. 4.9	NC and BER performance of the proposed method against different attacks.....	81
Fig. 4.10	PSNR, NC and BER performance of the proposed method using different cover images	81
Fig. 4.11	Multiple watermarks (a) embedding process and (b) extraction process.....	84

Fig. 4.12 (a) Cover image and (b) Watermarked Barbara images at gain factor = 0.05, (c) 0.1 and (d) 0.9 85

Fig. 4.13 Original (a) image and (b) text watermark of size 50 characters 85

Fig. 5.1 The watermark (a) embedding and (b) extraction process 99

Fig. 5.2 Original and watermarked MRI images (a) original image and watermarked images at gain factor (b) 0.01 (c) 0.05 and (d) 0.5 103

Fig. 5.3 EPR data as (a) image and (b) text watermark 104

Fig. 5.4 NC performance with different ECCs against known attacks at gain factor (α) = 0.05 114

Fig. 5.5 BER performance with different ECCs against known attacks at gain factor (α) = 0.05 114

Fig. 5.6 PSNR performance of the proposed method for different cover images using hybrid error correcting code at gain factor (α) = 0.05 115

Fig. 5.7 NC performance of the proposed method for different cover images using hybrid error correcting code at gain factor (α) = 0.05 115

Fig. 5.8 Encryption based watermark (a) embedding and (b) extraction process 116

Fig. 5.9 Original and watermarked MRI images (a) original image and watermarked images with gain factor; (b) 0.01; (c) 0.05 and (d) 0.5 116

Fig. 5.10 EPR data as text watermark 117

Fig. 5.11 NC performance of the proposed method against ‘Checkmark’ attacks 121

Fig. 5.12 NC performance of the proposed method against ‘Checkmark’ attacks 122

Fig. 6.1 Embedding process of PN sequence in the proposed method 131

Fig. 6.2 Original and watermarked MRI images (a) original image and watermarked images with gain factor; (b) 1.0; (c) 1.5 and (d) 5.0 135

Fig. 6.3 Image watermark (a) original and recovered watermark with gain factor α = (b) 0.5; (c) 1.0; (d) 2.5; (e) 4.0 and (f) 5.0 136

Fig. 6.4 Recovered watermark of different size at gain factor = 5 (a) 64×20 ; (b) 80×25 ; (c) 99×31 136

Fig. 6.5 BER performance of the proposed method at different gain factors 138

Fig. 6.6 BER performance of the proposed method against different attacks 139

Fig. 6.7 Comparison results under NC values at different gain factors 139

Fig. 6.8 (a) Cover image (b) Watermarked image at gain factor (α) = 15 140

Fig. 6.9 Extracted text watermark at gain factor (α) = 15 140

Fig. 6.10 Cover and watermarked CT Scan images **(a)** original image and watermarked images with gain factor; **(b)** 5; **(c)** 15 and **(d)** 40 145

Fig. 6.11 EPR data as text watermark 145

Fig. 6.12 PSNR performance of proposed method using different cover images 147

Fig. 6.13 BER performance of the proposed method using different cover images 147

Fig. 6.14 BER performance of the proposed method against known attacks..... 148

Fig. 6.15 Proposed dual watermark embedding method 149

Fig. 6.16 **(a)** Cover MR and **(b)** watermark logo image 151

Fig. 6.17 Watermarked MR image at **(a)** Gain = 1 **(b)** Gain = 5 and **(b)** Gain = 15 151

Fig. 6.18 Patient information as text watermark 152

Fig. 7.1 Image **(a)** cover eye and **(b)** watermarked 167

Fig. 7.2 Extracted Signature, Index and Caption watermark 168

Fig. 7.3 Reference **(a)** original and **(b)** extracted watermark..... 168

Fig. 8.1 Watermark **(a)** embedding and **(b)** extraction process..... 180

Fig. 8.2 BPNN training process 183

Fig. 8.3 **(a)** CTscan cover image **(b)** lump image watermark **(c)** watermarked image..... 185

Fig. 8.4 Signature and Symptoms text watermarks..... 185

Fig. 8.5 Extracted Lump watermark **(a)** without and **(b)** with BPNN training..... 185

Fig. 8.6 PSNR, NC and BER performance of the proposed method at different gain factor 188

Fig. 8.7 PSNR, NC and BER performance of the proposed method for different cover image..... 189

Fig. 8.8 PSNR, NC and BER performance of the proposed method for different size of text watermark..... 189

Fig. 8.9 NC and BER performance of the proposed method for known attacks 190

Fig. 9.1 Image and text watermark **(a)** embedding and **(b)** extraction process 202

Fig. 9.2 BPNN Training Process for image watermark..... 203

Fig. 9.3 Cover Images **(a)** kidney **(b)** Lena and **(c)** PDGC_logo 208

Fig. 9.4 Watermark images **(a)** stone **(b)** signature **(c)** logo 209

Fig. 9.5 Personal information using as text watermark 209

Fig. 9.6 Corresponding watermarked images..... 209

Fig. 9.7 Corresponding selective encrypted watermarked images 209

Fig. 9.8 Corresponding selective decrypted watermarked images 210

Fig. 9.9 Extracted watermark images without using BPNN 210

Fig. 9.10 Extracted watermark images using BPNN 210

Fig. 9.11 Histogram for (a) watermarked image (b) encrypted
and (c) decrypted watermarked image 211

Fig. 9.12 NC performance comparison with Xing and Tan 219

Fig. 9.13 NC performance comparison with Ghafoor and Imran 219

Fig. 9.14 NC performance comparison with Santhi and Thangavelu 220

Fig. 9.15 NC performance comparison with Zhao and Dang 220

Fig. 9.16 NC performance comparison with Xiong 221

Fig. 9.17 NC performance comparison with Shi et al. 221

Fig. 10.1 Emerging areas of image watermarking and its related
potential issues 228

List of Tables

Table 2.1	Summary of inspiring and pioneering robust image watermarking algorithms.....	28
Table 4.1	Effect of attacks on robustness (determined using NC values) at different wavelet decomposition levels	71
Table 4.2	Effect of Salt and pepper noise on robustness (determined using NC values) at different wavelet decomposition levels	71
Table 4.3	Effect of Gaussian noise on robustness (determined using NC values) at different wavelet decomposition levels	72
Table 4.4	Effect of Speckle noise on robustness (determined using NC values) at different wavelet decomposition levels	72
Table 4.5	Comparison of robustness (determined using NC values) performance with other reported methods.....	74
Table 4.6	Effect of ‘Checkmark’ attacks on robustness (determined using NC values) at gain factor (α) = 0.09.....	75
Table 4.7	Effect of encryption on PSNR, NC and BER at different gain factors	79
Table 4.8	NC and BER performance of the proposed method against different attacks at gain factor (α) = 0.05.....	80
Table 4.9	PSNR and NC performance using different cover images at gain factor (α) = 0.05.....	80
Table 4.10	Performance comparison of robustness (determined using NC values) performance under different attacks	82
Table 4.11	Subjective measure of the watermarked image quality at different gain factors.....	82
Table 4.12	Comparison under PSNR, NC and BER with other reported technique at different gain factor	86

Table 4.13	Comparison under NC and BER with other reported technique against attacks	87
Table 4.14	Effect of cover image at gain = 0.05	88
Table 4.15	Effect of size of the text watermark at gain = 0.01.....	88
Table 4.16	Performance comparison results under NC value	89
Table 5.1	The effect of Hamming code on PSNR, NC and BER at different gain factor (α)	105
Table 5.2	The effect of Hamming code on NC and BER against different attacks at gain factor (α) = 0.05	106
Table 5.3	The effect of BCH code on PSNR, NC and BER at different gain factors.....	107
Table 5.4	The effect of BCH code on NC and BER against different attacks at gain factor (α) = 0.05	108
Table 5.5	The effect of Reed-Solomon code on PSNR, NC and BER at different gain factor.....	109
Table 5.6	The effect of Reed-Solomon code on NC and BER against different attacks at gain factor (α) = 0.05	110
Table 5.7	Hybrid code performance under PSNR, NC and BER at different gain factors.....	111
Table 5.8	Performance comparison of different ECCs against signal processing attacks at gain factor (α) = 0.05	112
Table 5.9	Effect of cover images on PSNR, NC and BER values using hybrid error correcting code at gain factor (α) = 0.05	113
Table 5.10	Comparison of NC values with other reported methods	113
Table 5.11	Effect of gain factor on PSNR, NC and BER performance with varying text watermark sizes	118
Table 5.12	Effect of encryption and ECC on NC and BER against different attacks at gain factor (α) = 0.05	119
Table 5.13	Effect of cover image on PSNR, NC and BER at gain factor (α) = 0.05	119
Table 5.14	Comparison of NC and BER values with other reported method.....	120
Table 5.15	Effect of 'Checkmark' attacks at gain factor (α) = 0.05.....	122
Table 6.1	Allocation of watermarks according to robustness and capacity criteria at different sub-band	130
Table 6.2	Effect of BCH coding on PSNR and BER at different gain factors	136
Table 6.3	Effect of BCH coding on NC and BER against different attacks at gain factor (α) = 5.....	137
Table 6.4	Effect of different size of image watermark on PSNR, NC and BER at gain factor (α) = 1.5.....	137
Table 6.5	Effect of different cover image on PSNR, NC and BER at gain factor (α) = 1.5	138

Table 6.6	The comparison results under PSNR and NC value at different gain factors.....	138
Table 6.7	PSNR and BER performance of the proposed method with and without BCH code	141
Table 6.8	BER performance of proposed method with and without BCH code against different attacks at gain factor (α) = 10.....	141
Table 6.9	Effect of cover images on PSNR and BER performance at different gain factors.....	142
Table 6.10	The comparison results under PSNR and BER value	142
Table 6.11	Allocation of watermarks according to robustness and capacity criteria at different sub-band	143
Table 6.12	Effect of gain factor on PSNR and BER for different sizes of watermark.....	146
Table 6.13	Effect of encryption on BER for different attacks at gain factor (α) = 15	146
Table 6.14	PSNR and BER performance using different cover images at gain factor (α) = 15.....	146
Table 6.15	PSNR, NC and BER Performance of the proposed method at different gain factors.....	153
Table 6.16	PSNR, NC and BER Performance of the proposed method at different size of the image watermark	154
Table 6.17	PSNR, NC and BER Performance of the proposed method for different cover image	154
Table 6.18	NC and BER performance of the proposed method against different attacks.....	154
Table 6.19	NC and BER performance of the proposed method for different attacks.....	155
Table 7.1	Comparison between two important hashing algorithms	163
Table 7.2	Allocation of watermarks according to robustness and capacity criteria at different DWT sub-band	164
Table 7.3	PSNR, BER and NC performance at different factor.....	168
Table 7.4	BER and NC performance for JPEG attacks at different quality factors (QF)	169
Table 7.5	BER and NC performance for ‘Checkmark’ attacks.....	169
Table 7.6	Comparison of PSNR and NC values with other reported method.....	170
Table 8.1	Allocation of different watermarks according to robustness and capacity criteria at different sub-band	179
Table 8.2	PSNR, NC and BER performance of the proposed method at different gain.....	185
Table 8.3	PSNR, NC and BER performance for different no of characters in Symptoms watermark at different gain.....	186
Table 8.4	PSNR, NC and BER performance for different cover images at gain = 0.08.....	186

Table 8.5	PSNR and NC and BER performance for different text watermark size at gain 0.08	186
Table 8.6	BER and NC performance of the proposed method for different attacks at gain = 0.08.....	187
Table 8.7	Comparison results under NC value.....	190
Table 8.8	Subjective measure of the watermarked image quality at different gain factor	191
Table 9.1	Important difference between cryptography, steganography and watermarking	196
Table 9.2	Summary of considered techniques and corresponding objectives	200
Table 9.3	Allocation of watermarks according to robustness and capacity criteria at different DWT sub-band	201
Table 9.4	Performance of YCbCr model (kidney, stone, 40 characters)	212
Table 9.5	Performance of YIQ model (kidney, stone, 40 characters).....	212
Table 9.6	Performance of YCbCr model for different size of text watermark.....	213
Table 9.7	Performance of YCbCr model at different gain factors.....	213
Table 9.8	Performance of YCbCr model for different cover and watermark images at gain 0.07 (64 characters)	213
Table 9.9	Performance of YCbCr model for different attacks at gain 0.07 (64 characters)	214
Table 9.10	Encryption and Decryption time for different cover	215
Table 9.11	The performance comparison under NC with watermark size of 128×128	215
Table 9.12	The performance comparison under NC watermark size of 64×64	216
Table 9.13	Visual quality of the watermarked by subjective methods	217
Table 10.1	Summary of existing state-of-the-art watermarking techniques.....	229