A NEW ROBUST IMAGE WATERMARKING APPROACH USING TWO-LEVEL INTERMEDIATE SIGNIFICANT BITS COUPLED WITH HISTOGRAM INTERSECTION TECHNIQUE

Mir Shahriar Emami

A thesis submitted in fulfilment of the
requirements for the award of the degree of
Doctor of Philosophy (Computer Science)

Faculty of Computer Science and Information System
Universiti Teknologi Malaysia

MAY 2012

To my beloved father and mother

To my beloved Narges and Arshia

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to my supervisor, Professor Dr. Ghazali Bin Sulong, for his supports and valuable guidance during my research.

I would like thank Universiti Technologi Malaysia (UTM), for awarding me the International Doctoral Fellowship (IDF) an also for supporting me with the Research University Grant Scheme (RUGS) during my study.

I also gratefully acknowledge the suggestions made by anonymous journal reviewers that have enhanced the quality of my PhD thesis.

I would like to thank my parents for offering their support and love through my life.

I want to express my great appreciation to my dearest Narges and Arshia for their understanding of my situations during each period of my studies.

ABSTRACT

Nowadays, due to the explosive growth of the internet and multimedia technologies, digital multimedia assets are mostly vulnerable to redistribution and replication via accessible networks. Hence, digital watermarking techniques have become widely recognized as effective solutions for ownership identification and copyright protection of the digital assets. Experimental investigations have shown that current digital image watermarking approaches are prone to be impacted by watermarking attacks which originated from image processing or signal processing common operations. Even worst, some attacks with unknown or complex behaviours can be emerging in near future that able to destroy partially or completely the embedded watermarks. In such a situation, providing a universal model for the watermarking attacks is almost impossible. Beside the robustness, it is important to provide high visual quality and embedding capacity. Therefore, creating an effective watermarking technique which provides a balanced trade-off between robustness and visual quality, and at the same time attain reasonable capacity is a challenging task. To take up this challenge, a two-level Intermediate Significant Bit watermarking technique called BiISB is introduced in which two interrelated watermarks namely, main watermark and sub-watermark which is formed from statistical information of the main watermark using binary bit-patterns, are embedded concurrently in the host image. After an attack, the remnant information of both main watermark and sub-watermark in the form of bit-pattern histograms are used for the ownership identification of the property using Histogram Intersection technique. In addition, in order to measure the trade-off among above requirements, two techniques namely, Threshold based approach and Fuzzy approach are introduced. Experiments have been conducted using arbitrary watermarks, 10 standard host images, 10 different attacks, and 10 different embedding capacities. The experimental results revealed that the proposed technique successfully identified the ownership of the watermarked images even after the embedded watermarks were totally corrupted. The results also revealed that the technique introduced has successfully balanced the trade-off between robustness and quality, and at the same time attained high capacity. This is realized by obtaining ownership probabilities of higher than 0.95, qualities beyond 40dB, and 12.5% capacities.

ABSTRAK

Kebelakangan ini, disebabkan oleh perkembangan internet dan teknologi multimedia yang semakin pesat, aset multimedia digital adalah sangat mudah terdedah kepada replikasi dan pengedaran semula melalui rangkaian yang diakses. Dalam situasi ini, teknik digital tera air diiktiraf secara meluas sebagai cara penyelesaian yang efektif untuk mengenalpasti pemilikan dan perlindungan hak cipta aset digital. Siasatan eksperimen menunjukkan bahawa pendekatan imej tera air digital yang terkini adalah terdedah kepada serangan tera air yang berasal daripada operasi biasa pemprosesan imej dan pemprosesan isyarat. Memburukan lagi keadaan dimana beberapa serangan yang tidak diketahui perlakuannya atau berkelakuan kompleks dijangka akan muncul dalam masa terdekat yang mampu untuk memusnahkan sama ada sebahagian atau keseluruhan tera air yang terbenam. Dalam situasi yang demikian, adalah mustahil untuk menyediakan satu model tera air yang universal. Disamping kekukuhan tersebut, adalah penting untuk menyediakan kualiti visual dan kapasiti pembenaman yang tinggi. Oleh itu untuk mencipta satu teknik tera air yang efektif dan mampu mengimbangi diantara kekukuhan dan kualiti visual serta pada masa yang sama mencapai kapasiti yang berpatutan adalah satu tugas yang mencabar. Demi menyahut cabaran tersebut, satu teknik Bit Bererti Pertengahan yang digelar *BiISB* dikemukakan, dalam mana dua tera air yang berkaitan iaitu tera air utama dan sub-tera air yang terbentuk daripada maklumat statistik tera air utama menggunakan corak bit binari, dibenamkan didalam imej hos secara serentak. Selepas suatu serangan, sisa maklumat daripada kedua-dua tera air utama dan sub-tera air dalam bentuk histogram corak bit digunakan untuk mengenali pemilik harta menggunakan teknik Persilangan Histogram. Selanjutnya, untuk mengukur kesan kompromi diantara keperluan diatas, dua teknik iatu pendekatan berasaskan Ambang dan pendekatan Kabur dikemukakan. Eksperimen telah dijalankan menggunakan pelbagai tera air, 10 hos imej piawai, 10 jenis serangan dan 10 kapasiti yang berbeza. Keputusan kajian menunjukkan bahawa teknik yang dicadangkan telah berjaya mengenal pasti pemilik imej tera air walaupun imej tera air yang terbenam telah rosak sepenuhnya. Keputusan tersebut juga menunjukkan bahawa teknik tesebut berjaya mengimbangi kesan kompromi diantara kekukuhan dan kualiti dan pada masa yang sama kapasiti pembenaman yang tinggi diperolehi. Ini direalisasikan dengan memperolehi kebarangkalian pemilikan melebihi 0.95, kualiti melampaui 40dB dan kapasiti sebanyak 12.5%.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

BCR	-	Bit Correct Rate
dB	-	Decibel
DCT	-	Discrete Cosine Transform
DFT	-	Discrete Fourier Transform
DWT	-	Discrete Wavelet Transform
EISB	-	Enhanced Intermediate Significant Bit
FFT	-	Fast Fourier Transform
FIS	-	Fuzzy Inference System
HH	-	High-High frequency band
HL	-	High-Low frequency band
HRT	-	Histogram Relationship Triangle
IDCT	-	Invert Discrete Cosine Transform
IDFT	-	Invert Discrete Fourier Transform
IDWT	-	Invert Discrete Wavelet Transform
IP	-	Inverted Pattern
ISB	-	Intermediate Significant Bit
JPEG	-	Joint Photographic Expert Groups
LH	-	Low-High frequency band
LL	-	Low-Low frequency band

LPAP	-	Local Pixel Adjustment Process
LSB	-	Least Significant Bit
MFRB	-	Mamdani Fuzzy Rule Based
MSB	-	Most Significant Bit
MSE	-	Mean Square Error
NCC	-	Normalized Cross Correlation
OPAP	-	Optimal Pixel Adjustment Process
OSR	-	Optimal Similarity Rate
PSNR	-	Peak Signal to Noise Ratio
PVD	-	Pixel Value Differencing
SR	-	Set Removal
RR	-	Reset Removal
TIBV	-	Thresholds based on Intermediate Bit Values
VBA	-	Visual Basic for Applications
WMSE	-	Worst case Mean Square Error

CHAPTER 1

INTRODUCTION

1.1. Background of the Study

In the past few years, digital multimedia has proliferated with the rapid advancements of multimedia and communication technologies. In spite of the several advantages of these advancements, multimedia assets are largely vulnerable to replication and redistribution via simply popular accessible networks particularly the Internet. According to recent statistics, billions of dollars have been lost to multimedia piracy. These may bring about hindering the offer of digital distributions of intellectual properties by their owners as they worry about the copyright protection of their digital assets.

In such a situation, digital watermarking approaches have become widely used as effective mechanisms for ownership protection. In actual fact, digital watermarking as an approach for ownership identification of digital property is a new area of research in computer science which has attracted the interest of several researches both in industry and academia. Moreover, due to the explosive growth of the Internet and multimedia technologies in this digital era, digital watermarking has become one of the hottest topic in image/signal processing researches in order to protect digital contents against intentional or unintentional unauthorized replacements and manipulations. Watermarking schemes have been identified as effective approaches to cope with protection of digital multimedia intellectual properties.

Moreover, several varieties of attacks against watermarking approaches have been recognized and of course, many new kinds of them may emerge in the near future. Experimental investigations have shown that the proposed watermarking approaches are prone to be impacted severely by several attacks. This makes them unable to extract the embedded watermark to identify the ownership of the digital media. Therefore, a universal watermarking algorithm which can withstand all kinds of attacks and simultaneously satisfy the imperceptibility requirement does not seem to exist. Thus, new solutions must be devised to tackle this problem (Licks and Jordan, 2005).

Furthermore, digital watermarking process requires a rapid and low computational power particularly for real-time applications. Currently, there is a time lap between image creation and watermarking embedding. This gap as a security hole will provide good opportunities to the attackers to exploit the delay of original image transformation to watermarked version of the image. In such a situation, there is a need of low complexity watermarking mechanism for many of todays' applications. For example, digital photographs need to be watermarked as soon as they are taken by the digital phone cameras (Sohn, et al., 2006). This brings about the identification of those photographs to a particular digital phone camera or to its owner immediately after they are taken.

In general, the quality of the digital image after the watermark embedding process is degraded. Thus, the degradation level of a watermarking algorithm should be given serious attention in the evaluation of a watermarking scheme performance. Some of the proposed watermarking algorithms may be robust enough but they may drastically degrade the quality of the digital media. In actual fact, there is a trade-off among watermarking performance requirements including visual imperceptibility, robustness and embedding capacity but to address this trade-off, a strategy is needed to measure it. Although, there are several metrics to evaluate watermarking performance requirements, none of these watermarking metrics gave concrete attention to measure this trade-off.

In addition, digital watermarking schemes with respect to the information taken into account through extracting can be categorized as blind and non-blind approaches. In non-blind watermarking approaches, both data for actual host image and data statistics about watermarked image are known in the time of watermark detection and extraction (Tao and Eskicioglu, 2004). In contrast, in blind approach retrieving the watermark without referring to the original image is preferred (Al-Otum and Samara, 2010). There are several difficulties concerning the blind watermarking approaches. On the one hand, high effectiveness of blind watermarking is also proven. Therefore, a new technique called semi-blind watermarking was introduced. In this kind of watermarking approach, only the original watermark or the watermarked multimedia statistics are known (Tao and Eskicioglu, 2004; Shieh, 2006; Eugene, 2007). Paunwala, and Patnaik, (2011), applied semi-blind strategy in their approach in which principal direction of the subject watermarked image as statistical information is available at the time of watermark extraction to avoid the use of the original host image. Consequently, in the non-blind approaches in the original host data is needed after the extraction time to identify the rightful owner. On the other hand, in blind approaches detecting and extracting the watermark information will become very difficult if the watermarked image is highly attacked either intentionally or unintentionally. Therefore, the semi-blind approach as a key solution is more robust than the blind approach and more effective than the non-blind approach.

In conclusion, in the previous watermarking approaches, the ownership of the attacked image cannot be identified against all types of intentional and unintentional attacks and preserve the quality of the watermarked image at the same time. Moreover, several intentional attacks with the purpose of removing or replacing of the embedded watermarks may appear in the near future. In addition, a general purposed attack modelling is complicated as some severe attacks cannot be simply modelled or the behaviour of other watermarking attacks may be unknown. In such a situation, obtaining a balanced trade-off among the robustness, the visual imperceptibility and the embedding capacity has become a challenge in the digital watermarking research area.

1.2 Problem Statement

Instantaneous digital image watermarking is an urgent need for many of today's applications such as digital cameras and digital phone cameras. Comparing two of the watermarking techniques, transform domain watermarking approaches requires higher computational complexity than spatial domain techniques (Wolfgang et al., 1999; Wu and Hwang, 2007; Burdescu et al., 2007; Larijani and Rad; 2008, Mehemed et al.; 2009, and Kougianos et al., 2009). This is due to the forward and inverse transformations of the transform-domain watermarking approaches. Nonetheless, there are problems with spatial-domain techniques. For example, high embedding errors in ISB bit-planes results in many researchers employing low-order bit-planes such as LSB for data hiding, for example in Maity and Kundu (2002) Chan and Cheng (2004), and Yang (2008). However, the low-order bit-planes techniques does not contain visually significant information so, the embedded watermark may be simply corrupted or replaced by unauthorized users without influencing visual effects. For example, Abolghasemi et al. (2010) proposed a technique using co-occurrence matrix and bit-plane clipping which can detect the hidden data in LSB.

Hence, other researchers used ISB bit-planes in both spatial and spectral domains to improve this drawback, such as in Habes (2006), Zeki and Manaf (2007). However, the selecting higher bit-planes in ISB schemes results in higher visual degradation effects in the watermarked image quality. This decreases the imperceptibility of the watermarked image which is one of the major goals of the invisible digital watermarking. According to Kefa Rabah (2004), watermarked image would look identical to its original host image if the used bit-planes for data hiding are not higher than the 5th. Later on, Habes (2006) concluded the same result in his latest research. He mentioned that using each of the low order bit-planes (5th to 8th) for embedding the watermark guarantees the performance of the imperceptibility. Instead, choosing high order bit-planes (1^{st} to 4^{th}) could bring about higher robustness. Thus, when we choose higher bit-planes for watermark embedding, the image quality degrades but the robustness increases and vice versa.

On the other hand, a watermarking attack may bring about much degradation effects for the watermarked image quality and make the watermarked image useless and unproductive for piracy. This can be interpreted as a higher robustness. Therefore, selecting lower bit-planes results in lower visual degradation effects and lower robustness because the embedded watermark can be simply corrupted or replaced by malicious users without any visual effects. To overcome this drawback, Zeki and Manaf (2009) proposed an enhanced technique based on ISB approach, which can be called as EISB for simplicity. This approach allows the use of higher ISB bit-planes with low perceptible visual effects. Although EISB improved ISB scheme in terms of watermarking visual degradation effects, there is still robustness weaknesses in this approach. For example, JPEG2000 attack can simply corrupt the embedded watermark(s) in the EISB approach. Zeki and Manaf (2011) introduced the Block-based Biased-EISB approach in order to overcome this drawback. However, there are still three main weaknesses in this approach. Firstly, the biased-based strategy degrades the watermarked image quality drastically. Secondly, some common image processing attacks such as rotating, skewing, etc. can simply influence on the continuity of the structure of the blocks so the embedded watermark can be corrupted easily. Thirdly, as each bit of the watermark information is embedded in a block of pixels instead of one single pixel, so this approach suffers from low embedding capacity.

Meanwhile, many researchers, for example Wolfgang et al. (1999) Cox, Miller and Bloom (2002), Fazli and Khodaverdi (2009), Song et al. (2010), emphasized that robustness, imperceptibility and capacity conflict with each other. In other words, there is a trade-off among these requirements. For example, there is still a trade-off between visual imperceptibility, robustness and embedding capacity in spatial domain watermarking schemes such as biased-EISB, Aliwa et al. (2010) and Block-based Biased-EISB approaches. In biased-EISB approach, the bias strategy is used to increase the robustness but the bias strategy degrades the quality of the image. In Aliwa et al. (2010) approach, a high-order bit-plane (the 3^{rd} bit-plane) is used to increase the robustness but using a high order bit-plane degrades the quality and restricts the embedding capacity. In block-based biased-EISB approach, both the bias strategy and the blocking strategy are used in order to improve the robustness but bias strategy decrease the quality and the blocking strategy decrease the capacity. Fazli and Khodaverdi (2009) in their latest research on the LSB watermarking concluded similar results. Similarly, in real-time applications such as digital cameras and digital phone cameras, the mentioned requirements are also in trade-off but the simplicity of the watermarking technique is another requirement in such applications. Hence, new approaches are required to obtain a balanced trade-off among quality, robustness and capacity in order to enable the EISB-based watermarking approaches to be applied for real-time applications. Now the question is: Is it possible to obtain a technique to balance a trade-off among visual imperceptibility, robustness and embedding capacity in EISB-based watermarking approaches?

Finally, numerous diversities of attacks against watermarking approaches have been documented, for example in Song et al. (2010), and of course a number of new varieties may emerge in the near future. Experimental investigations have shown that the previous watermarking approaches are prone to be impacted severely by several kinds of such attacks. This makes them unavailable to extract the embedded watermark(s) in order to identify the ownership of the digital media. In addition, many of the attacks against watermarking schemes may be too complex to model, so an effective analysis of their behaviour is not simple (Cox et al., 1997). Consequently, a universal watermarking approach that can withstand against several varieties of attacks and, at the same time, satisfies the quality and the embedding capacity requirements with a low complexity has not been discovered yet. In this situation, approximation approaches can be employed in order to identify the ownership of the attacked watermarked image with low computational complexity. Now the question is: How to come up with a solution that can withstand against many varieties of attacks without knowing their exact behaviours?

1.3. Purpose of the Study

In general, no watermarking scheme is immune to all kinds of attacks and, at the same time, preserves the host image quality with a high embedding capacity. According to Bender et al. (1996), all of the watermarking approaches encounter restrictions. Therefore, several techniques must be employed simultaneously to attain the acceptable degree of trade-off among robustness, imperceptibility and capacity. The main aim of this study is to introduce an approximation approach based on the statistical information in terms of both the embedding watermark and the extracting watermark which provides a balanced trade-off among robustness, visual imperceptibility and embedding capacity.

This can be realized by proposing a new robust image watermarking technique based on two-level ISB using the remnant information of the embedded watermarks in order to identify the ownership of the watermarked image even after severe attacks. The proposed approach should achieve a balanced trade-off among the visual imperceptibility, robustness and embedding capacity.

1.4. Objectives

In order to achieve the goal, the following objectives are to be performed:

I. To propose new severe attacks.
II. To propose measurement schemes in order to evaluate the trade-off among imperceptibility, robustness and capacity requirements.
III. To propose a new technique for owner identification.
IV. To propose a new watermarking technique in order to obtain a balanced trade-off among robustness, imperceptibility, and capacity.

1.5. Scope of the Study

The focus of this study is as in the followings:

I. Invisible Semi-blind Robust Digital Watermarking
II. Spatial Domain Watermarking

III. 8-bit gray-scale still image

IV. JPEG, JPEG2000, Rotating, Vertical Skewing, Horizontal Skewing , Pepper & Salt, and Cropping Attacks

1.6. Contributions of the Study

The contributions of this study can be categorized as: (I) new attacks, (II) new measurement techniques to evaluate balanced trade-off, (III) new owner identification technique, (IV) new watermarking technique. For each category the contributions are as follows:

I. Two new attacks which are severer than most popular attacks such as JPEG, JPEG2000, and Skewing. Unlike the popular attacks, the attacks introduced impacts directly on the embedded watermarks and remove the embedded watermarks partially or totally.

II. Two new measurement techniques namely, Threshold-based and Fuzzy-based approaches. Unlike the popular measures such as BCR, NCC, and PSNR which merely evaluate one of the main watermarking requirements, the techniques introduced measure the balanced trade-off among robustness, imperceptibility, and capacity.

III. New ownership identification method utilizing L2Norm technique for the ownership identification. The technique introduced identifies the ownership of the property using the remnant information after the attack totally destroys the embedded watermarks.

IV. New watermarking technique using two-level ISB coupled with Histogram Intersection technique in which a low-order bit-plane for maintaining high imperceptibility and a high-order bit-plane for obtaining high robustness were used to embed main watermark and its interrelated sub-watermark, respectively. This technique identifies the ownership of the property exploiting the remnant information after the embedded watermarks are totally destroyed by the attacks. The technique introduced is better than other techniques as it obtains a balanced trade-off among robustness, imperceptibility, and capacity.

1.7. Significance of the Study

The proposed watermarking scheme can be applied for real-time applications such as digital camera, digital phone camera, human interacting-robots, etc. in order to protect the ownership of the attacked watermarked images regardless the behaviour of the attacks. Moreover, the proposed scheme highly preserves the quality of the watermarked image such that it can be used in clinical studies, medical applications, photography, etc.

1.8. Research Framework

Watermarking and steganography are two main branches of information hiding research area. The watermark object may be visible or invisible. The invisible watermarking has been more challenging in comparison with the visible watermarking. A watermarking scheme can be robust, fragile or semi-fragile. Among the three mentioned categories, robust watermarking scheme is used for copyright protection and ownership identification. Any watermarking process can be implemented in spatial domain, transform-domain or hybrid domain. In the spatial domain approach, the secret information is embedded directly within the host media pixels. In contrast, in the transform domain approach the secret information is embedded within the transform domain coefficients. Figure 1.1 shows the framework for the information hiding.

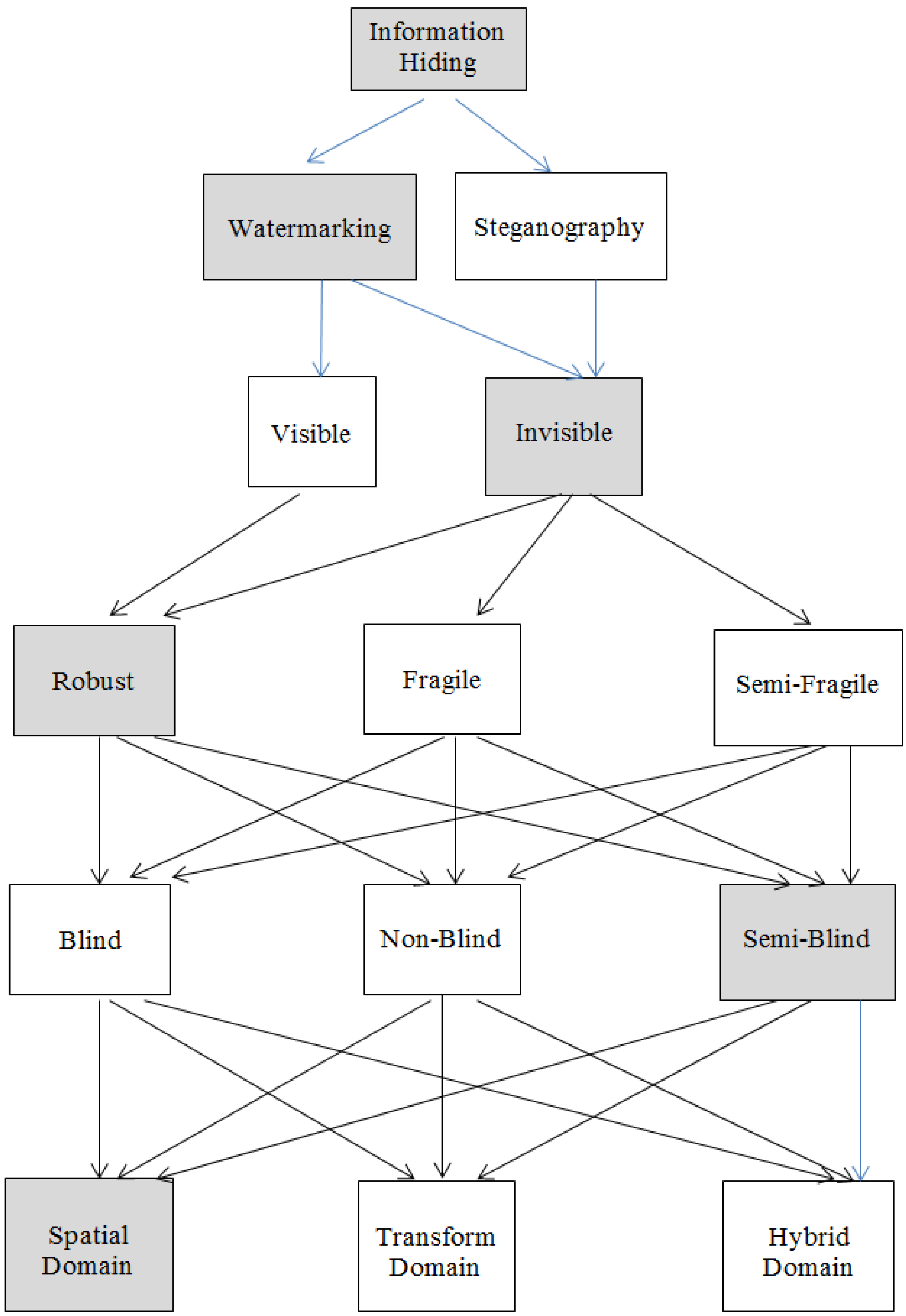

Figure 1.1.Diagram of the Approach of the study In this diagram, the gray boxes show the path of this study.

There are four key concepts in digital robust watermarking viz: watermark attacking, performance measurement, watermark embedding, and watermark extracting.

First of all, in the case of watermark attacks, the behaviours of some kinds of previous attacks and future unknown attacks against watermarking techniques may be either complex or unknown. Meanwhile, most watermarking attacks originated from either signal or image processing common operations. However, there are also other watermarking attacks that originated from an attacker's mind. Such attacks can be severe enough that the attacked watermarked image can no longer be identified (Chapter 3 introduces the two of such attacks.). Thus, a universal watermarking technique which is compatible with all forms of known and unknown attacks has not appeared yet. Meanwhile, several robust digital watermarking techniques have been proposed by researchers which are able to withstand certain attacks. However, in order to obtain a precise assessment, all of the above attacks should be considered.

Secondly, in the case of performance measurement, there are at least three main requirements viz: quality (visual imperceptibility), robustness, and embedding capacity that should be fulfilled in a robust watermarking technique. Unfortunately, these requirements conflict with each other which means there is a trade-off among them. In order to assess the effectiveness of a watermarking technique, it is important to measure this trade-off by means of an effective mechanism. In order to fulfill this need, two different approaches are proposed in Chapter 4 viz: an effective technique based on three Threshold conditions, and a Fuzzy based model.

Thirdly, during the extracting process, each pixel of the extracted watermark is constructed based on the respective pixels in the watermarked image which has the same positions as those in the original host image. For this reason, many severe attacks such as JPEG2000 lossy compression, rotating, skewing, etc. can either modify some pixel values or displace the embedded watermark positions. This results in corrupting the embedded watermarks and the continuity of the embedded bits, respectively. Subsequently, it is not possible for exact methods such as BCR to identify the ownership of the watermarked image after such severe attacks as the extracted watermark is not similar to the original embedded watermark. To overcome this problem, a statistical approach utilizing the L2Norm technique is introduced in Chapter 5 for ownership identification of the watermarked image. However, there is still no guarantee for this approach as certain attacks may be so severe that the ownership of the attacked watermarked image cannot be recognized. To overcome this drawback, a new strategy is required in the embedding process.

Fourthly, in the embedding stage, both the main watermark and statistical information regarding the main watermark in the form of bit-pattern histogram (called sub-watermark) can be embedded in the host image concurrently. A new watermarking technique, namely BiISB, is introduced in Chapter 6 in which both the high-order and the low-order bit-planes are used for embedding the sub-watermark and main watermark, respectively. This approach couples a two-level ISB approach with the Histogram Intersection technique in order to produce a high imperceptibility and, at the same time, withstand several kinds of attacks. Thus, the proposed technique can provide strong and probabilistic guarantees on the proof of ownership of the host image.

Finally, arbitrary watermarks, and several standard test images as the host image namely, Lena, Pirate, Baboon, Woman Blonde, Fishing Boat, Peppers, Jet, Crowd, Camera Man, and Living Room were used. Some of these standard images like Baboon and Crowd comprised of several edges and some others such as Jet and Peppers comprised of a lot of smooth areas. In addition, in order to test the robustness, several severe attacks namely, JPEG2000, JPEG, Vertical Skewing, Horizontal Skewing, Rotating, Cropping, Set Removal, Reset Removal, and Pepper & Salt were used. In addition, PSNR metric, and BCR and NCC metrics were used to evaluate visual imperceptibility and robustness, respectively.

1.9. Thesis Organization

The remaining of this thesis is organized as follows. In chapter 2, watermarking performance measures, attacks on watermarking schemes, and watermarking techniques in transform-domain, spatial-domain and hybrid-domain are reviewed. In chapter 3, two new watermarking attacks are proposed. Chapter 4 introduces novel techniques in order to measure the trade-off among watermarking performance measures. Chapter 5 introduces a new owner identification approach using statistical distribution of the remnant information after severe attacks. In chapter 6 a complete watermarking technique is introduced. Finally, chapter 7 provides thesis conclusions and future work recommendations.

REFERENCES

Abolghasemi, A., Aghaeinia, H., Faez, K., Mehrabi, M. A. (2010), "Detection of $LSB \pm 1$ Steganography based on Co-occurrence Matrix and Bit-plane Clipping", Journal of Electronic Imaging, Vol.19, No.1

Adelson, E. H. (1990), "Digital signal encoding and decoding apparatus," U.S. Patent 4939515

Ahire, V. K. and Kshirsagar, V. (2011), "Robust Watermarking Scheme Based on Discrete WaveletTransform (DWT) and Discrete Cosine Transform (DCT) for Copyright Protection of Digital Images", International Journal of Computer Science and Network Security, Vol..11, No.8

Al-Haj A. (2007), "Combined DWT-DCT digital image Watermarking", Journal of Computer Science, Vol 3, PP. 740-746

Aliwa, M. B., El-Tobely, T. E. and Fahmy, M. M., (2010), "A New Novel Fidelity Digital Watermarking Based on Adaptively Pixel- Most-Significant-Bit-6 in Spatial Domain Gray Scale Images and Robust", American Journal of Applied Sciences vol.7, no.7, pp.987-1022

Al-Otum , H. M. and Samara, N. A. (2010), "A robust blind color image watermarking based on wavelet-tree bit host difference selection", Signal Processing, Elsevier, Vol :90, PP 2498-2512

Amirgholipour, S. K. and Naghsh-Nilchi, A. R., (2009)," Robust Digital Image Watermarking Based on Joint DWT-DCT", International Journal of Digital Content Technology and its Applications, Volume 3, No.2

Atawneh, S. (2006), "A New Algorithm for Hiding Gray Images Using Blocks", Proc of IEEE Computer Society

Baba, S., Krikor, L. Z., Arif, T. and Shaaban, Z. (2010)," Watermarking of digital images in Frequency Domain", International Journal of Automation and Computing, 7(1), PP. 17-22

Bender, W., Gruhl, D., Morimoto, N. and Lu, A. (1996), "Techniques For Data Hiding", IBM System Journal, Vol. 35, NOS 3&4, PP. 313-336

Bennour, J., Dugelay, J,., and Matta, F (2007)., "Watermarking Attack (BOWS contest)", Security, Steganography, and Watermarking of Multimedia Contents, Proceedings of SPIE-IS&T Electronic Imaging, Vol. 6505, pp. 650518-1 - 650518-6, SPIE-IS&T

Burdescu, D. D., Stanescu, L., Ion, A., and Mihaescu, C. M. (2007), "A Spatial Watermarking Algorithm for Video Images", Computer Network Security-Communications in Computer and Information Science, Vol 1, Part 7, Part 12, Springer-Verlag, PP. 402-407

Chan, C. and Cheng, L. M., (2001), Improved Hiding Data in Images by Optimal Moderate Significant Bit Replacement, IEE Electronics Letters, vol.37, no.16, pp.1017-1018

Chan, C., and Cheng, L.M., (2004), "Hiding data in images by simple LSB substitution", Pattern Recognition 37, Elsevier, PP 469 – 474

Chang, C., and Tseng, H. (2004), "A Stenganographic Method for Digital Images using Side Match", Pattern Recognition Letters, vol.25, pp.1431–1437

Chang, C., Lin, C. and Hu, Y. (2007), "An SVD Oriented Watermark Embedding Scheme with High Qualities for the Restored Images", International Journal of Innovative Computing, Information and Control, Vol. 3, No. 3

Chang, K., Huang, P. Tu, S., T., and Chang, C. (2007), "Adaptive image steganographic scheme based on Tri-way Pixel-Value Differencing ", IEEE International Conference on Systems, Man and Cybernetics, pp. 1165 - 1170, IEEE Computer Society

Chang, C., Lin, C., and Hu, Y. (2007), "An SVD Oriented Watermark Embedding Scheme with High Qualities for the Restored Images", International Journal of Innovative Computing, Information and Control, Vol. 3, No. 3

Cheung, W. N. (2000), "Digital Image Watermarking in Spatial and Transform Domains", Proceedings TENCON 2000, pp. III-374 – III-378, IEEE Computer Society

Cooley, J. and Tukey, J. (1965), "An Algorithm for the Machine Calculation of Complex Fourier Series", Math. Comp., 19, PP. 297-301

Cox, I. J., Kilian, J. and Shamoon, T. (1997), "Secure Spread Spectrum Watermaking for Multimedia", IEEE Transaction of Image Processing, Vol. 6, No. 12, PP. 1673-1687, IEEE Computer Society

Cox, J., Miller, M. L., and Bloom, J. A. (2002), “Digital Watermarking”, Morgan Kaufmann, San Francisco

Chu, S., Jain, L. C., Huang, H. and Pan, J. (2010), “Error-Resilient Triple-Watermarking with Multiple Description Coding”, Journal of Networks, Vol. 5, No. 3, pp. 267-274, IEEE Computer Society

Daubechies, I. (1992), Ten lectures on wavelets, SIAM Press, Philadelphia, PA., USA

Dejun, Y., Rijing, Y., Yuhai, Y. and Huijie, X. (2009), “Blind Digital Image Watermarking Technique Based On Intermediate Significant Bit and Discrete Wavelet Transform”, Proc, International Conference on Computational Intelligence and Software Engineering, CISE 2009. IEEE Computer Soceity

Devapriya, M. and Ramar, K. (2010), ” Statistical Image Watermarking In DWT with Capacity Improvement”, Global Journal of Computer Science and Technology, Vol. 10, Issue 2, Ver 1.0

Eggers, J. J., Su, J. K. and Girod, B. (2000), ”Robustness of a Blind Image Watermarking Scheme’, International Conference on Image Processing, pp. 17-20, IEEE Computer Society

El-Ghoneimy, M. M. (2008), “Coparison Between Two WatermarkingAlgorithms Using DCT Coefficient, And LSB Replacement ”, Journal of Theoretical and Applied Information Technology, JATIT

Elbasi, E. and Eskicioglu, A. M. (2006), “A Semi-Blind Watermarking Scheme for Images using a Tree Structure ”, Proc, 2006 IEEE Sarnoff Symposium, PP. 1-4, IEEE Computer Society

Eugene, P.G. (2007), “Digital watermarking of bitmap images”, Proc, International Conference on Computer Systems and Technologies, June 14-15, ACM Press, Rousse, Bulgaria, pp: 1-6

Fazli, S. and Khodaverdi, G. (2009), “Trade-off between Imperceptibility and Robustness of LSB Watermarking using SSIM Quality Metrics”, Proc, Second International Conference on Machine Vision, IEEE Computer Society

Fourati, W. and Bouhlel, M. S. (2006), “Amelioration of the JPEG2000 by a Variable Window Pretreatment”, proc, Information and Communication Technologies (ICTTA2006) , pp. 1824-1829

Ganesanl, K. and Guptha (2010), T. K., “Multiple Binary Images Watermarking in Spatial and Frequency Domain”, Signal & Image Processing : An International Journal(SIPIJ), Vol.1, No.2, PP 148-159

Ghannam, S. and Abou-Chadi, F., (2008), F., “Enhancing Performance of Image Watermarks Using Wavelet Packet”, International Conference on Computer Engineering & Systems, ICCES 2008, IEEE Computer Society

Ghannam, S. and Abou-Chadi, F. E. Z., (2009), “WPT versus WT for a Robust Watermarking Technique”,International Journal of Computer Science and Network Security, Vol.9 No.1, pp. 236-241

Habes, A. (2006), “Information Hiding in BMP image Implementation, Analysis and Evaluation”, Information Trnsmissions In Computer Networks, Tom. 6, No. 1

Hameed, K., Mumtaz, A. and Gilani, S. A. M. (2006), “Digital image watermarking in the wavelet transform domain”, Proc. World Academy of Science, Engineering and Technology, Vol . 13: PP. 86-89

Honsinger, C. (2000), “Data Embedding using Phase Dispersion”, IEE Seminar on Secure Images and Image Authentication , pp. 5/1 - 5/7, IEEE Computer Society

Hore, A. and Ziou, D. (2010), “ Image Quality Metrics_PSNR vs SSIM”, International Conference on Pattern Recognition, IEEE Computer Society, pp.2366-2369

Hsu, C. and Wu, J. (1996), “Hidden Signatures in Images”, Proc, International Conference on Image Processing, Vol.3, PP. 223 - 226 , IEEE Computer Society

Huang, H., Chu, C., and Pan, J. (2009), ”Genetic Watermarking for Copyright Protection”, Information Hiding and Applications, SCI 227, pp. 1–19, Springer-Verlag

Istepanian, R. S. H., Philip, N., Martini, M. G., Amso, N. and Shorvon, P. (2008), ”Subjective and Objective Quality Assessment in Wireless TeleUltrasonography”, *pr*oc, International IEEE EMBS Conference, Vancouver, Canada, pp.20-24

Ji-jiang, T., Feng-ling, W. and Liang-tao, Z. (2010), “A Low Power and Complexity Watermarking Algorithm in DS-CDMA Communication”, 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT), PP. 547 - 551 , IEEE Computer Society

Jin, C., Zhang, Z., Jiang, Y., Qu, Z. and Ma, C., (2007), "A Blind Watermarking Algorithm Based on Modular Arithmetic in the Frequency Domain", Advances and Innovations in Systems, Computing Sciences and Software Engineering, pp. 543–547, Springer

Jou, F., Fan, K., Chang, Y. (2004), "Efficient Matching Large Size Histograms", Pattern Recognition Letters, Vol. 25, pp. 277–286

Kailasanathan, C., (2003), "Fragile Watermark based Polarity of Pixel Points", proc, 3rd International Symposium on Image and Signal Processing and Analysis, pp. 860-865, USA

Kamran, H., Mumtaz, A. and Gilani, S. A. M. (2006), "Digital image watermarking in the wavelet transform domain", Proc. World Academy of Science, Engineering and Technology, Vol . 13: pp..86-89

Kao, C. H. and Hwang, R. J. (2005), Information Hiding in Lossy Compression Gray Scale Image", Tamkang Journal of Science and Engineering, Vol. 8, No 2, pp. 99_108

Kluska, J. (2009) Analytical Methods in Fuzzy Modeling and Control, Studies in Fuzziness and Soft Computing, Springer-Verlag

Kothari, A.M., Suthar, A. C. and Gajre, R. S. (2010), "Performance Analysis of Digital Image Watermarking Technique–Combined DWT–DCT over individual DWT", International Journal of Advanced Engineering & Applications

Kougianos, E., Mohanty, S. P. and Mahapatra, R. N. (2009), "Hardware Assisted Watermarking for Multimedia", Computers and Electrical Engineering 35, PP. 339–358, Elsevier

Kumar, S. P., Anusha, K., Ramana, R. V. (2011), "A Novel Approach to Enhance Robustness in Steganography Using Multiple Watermark Embedding Algorithm", International Journal of Soft Computing and Engineering, Vol.1, Issue 1, pp.50-56

Larijani, H. H. and Rad, G. R. (2008), "A New Spatial Domain Algorithm for Gray Scale Images Watermarking", Proc, International Conference on Computer and Communication Engineering, PP. 157-161, Kuala Lumpur, Malaysia

Li, M., Narayanan, S. and Poovendran, R. (2004), "Tracing Medical Images Using Multi-BandWatermarks", 26th Annual International Conference of the IEEE

Engineering in Medicine and Biology Society, pp. 3233 – 3236, IEEE Computer Society

Li, S. , Leung K., Cheng, L.M. and Chan C. (2006),” Data Hiding in Images by Adaptive LSB Substitution based on the Pixel-value Differencing”, First International Conference on Innovative Computing, Information and Control, China, Beijing, pp. 58 - 61

Licks, V. and Jordan, R. (2005), “Geometric Attackes on Image Watermarking Systems”, IEEE Multimedia, PP. 68-78, IEEE Computer Society

Lie, W. and Chang, L. C., (1999), “Data hiding in images with adaptive numbers of least significant bits based on the human visual system”, International Conference on Image Processing, vol.1, pp.286 – 290

Liujuang, Q., and Ding, Z. (2008), “Spread Spectrum Watermark for color Image ”, Based on Wavelet Tree Structure”, Proc, International Conference on Computer Scienece and Software Engineering, PP 692-695

Maity S. P. and Kundu, M. K. (2002),” Robust and blind spatial watermarking in digital image”, proc, 3rd Indian Conf. on Computer Vision, Graphics and Image Processing (ICVGIP '2002), pp. 388 -393

MaruthuPerumal, S. and VijayaKumar, V., (2011), “A Wavelet based Digital Watermarking Method using Thresholds on Intermediate Bit Values”, International Journal of Computer Applications,Vol. 15, No.3, pp.29-36

Meerwald, P. and Pereira, S. (2002), “Attacks, applications, and evaluation of known watermarking algorithms with Checkmark”, *Proc*, Security and Watermarking of Multimedia Contents IV, Vol. 4675, PP. 293-304, SPIE

Mehemed, B.A., El-Tobely, T.E.A., Fahmy, M.M., Naser, M.E.L.S. and El-Aziz, M.H.A. (2009), "Robust digital watermarking based falling-off boundary in corners board-MSB-6 gray scale images", International Journal of Computer Science and Network Security,Vol.9, No.8, PP.227-240

Mohan, B. C., Kumar, S. S. and Chatterjee, B. N. (2006), “Digital Image Watermarking in Dual Domains ”, *Proc*, IET International Conference on Visual Information Engineering, PP. 410 – 415, IEEE Computer Society

Mohanty, S.P. (1999), “Digital Watermarking: A Tutorial Review”., www.cs.unt.edu/~smohanty/research/Reports/MohantyWatermarkingSurvey1999.pdf.

Nishchal, N. K. (2009), “Optical image watermarking using fractional Fourier transform”, Journal of Optics 38 (1), Springer

Ozturk, M., Akan, A. and Cekic, Y. (2010), “A Robust Image Processing in the Joint Time-Frequency Domain”, EURASIP Journal on Advances in Signal Processing, Hindawi Publishing Corporation, Vol.2010

Pan, G., Wu, Z. and Pan Y. (2002), “A Data Hiding Method for Few-color Images”, proc, IEEE International Conference on Acoustics, Speech and Signal Processing, IEEE Computer Society, pp. 3469-3472, USA

Paunwala, M. C. and Patnaik, S (2011), Biometric Template Protection With Robust Semi–Blind Watermarking Using Image Intrinsic Local Property, International Journal of Biometrics and Bioinformatics (IJBB), Vol.5, Issue 2

Perumal S. M. and Kumar V. V. (2011), A Wavelet based Digital Watermarking Method using Thresholds on Intermediate Bit Values, International Journal of Computer Applications, vol.15, no.3, pp.29-36

Potdar, V. M., Han, S. and Chang, E. (2005),“ A Survey of Digital Image Watermarking Techniques”, 3rd International Conference on Industrial Informatics(INDIN), PP. 709 – 716, IEEE Computer Society

Qi, H., Zheng, D., and Zhao, J. (2008),” Human visual system based adaptive digital image watermarking”, Signal Processing , vol.88, pp.174–188

Rabah K. (2004), “Steganography -- The Art of Hiding Data”, Information Technology Journal, Vol.3, No. 3, PP. 245-269

Rabie, T. and Guerchi, D. (2007), “Magnitude Spectrum Speech Hiding ”, *Proc*, IEEE International Conference on Signal Processing and Communications , PP. 1147 – 1150, IEEE Computer Society

Rafigh, M. and Moghaddam, M. E. (2010),” A Robust Evolutionary Based Digital Image Watermarking Technique in DCT Domain”, PP 105-109. , Seventh International Conference on Computer Graphics, Imaging and Visualization, IEEE Computer Society

Ramkumar, M., Akansu, A. and Alatan , A. (1999), “A Robust data hiding scheme for images using DFT”, Proc, IEEE International Conferenece on Image Processing, IEEE Computer Society, PP. 211-215

Reddy, A. A. and Chatterji, B.N. (2005), “A new wavelet based logo-watermarking scheme”, Pattern Recognition Letters 26, PP. 1019–1027, Elsevier

Sakawa, M. (1983), Interactive computer programs for fuzzy linear programming with multiple objectives. Intern.J. Man-Machine Stud., 18, PP. 489–503

Schyndel, R. G. V., Trike, A. Z. and Osborne, C. F. (1994), "A Digital Watermark", proc, 1st International IEEE Image Processing Conference, RMIT, Houston, USA

Seshadrinathan, K. and Bovik, (2008), A. C.," Unifying Analysis of Full Reference Image Quality Assessment", 15th IEEE International Conference on Image Processing, pp.1200 - 1203

Shapiro, J. M. (1993), "Embedded Image Coding Using Zerotrees of Wavelet Coefficients", IEEE Transactions on Signal Processing, Vol. 41 No. 12, IEEE Computer Society

Shieh, J., Lou, D., and Chang, M. (2006), "A Semi-blind digital watermarking scheme based on singular value decomposition", Elsevier, Computer Standards & Interfaces 28, PP 428– 440

Senthil, V. and Bhaskaran, R. (2008)," Robustness Analysis of Blind and Non-Blind Multiple Watermarking using Edge Detection and Wavelet Transforms ", 16th International Conference on Advanced Computing and Communications, ADCOM, PP. 106 – 111, IEEE Computer Society

Shih, F. Y., Wu, S. Y. T. (2003), "Combinational Image Watermarking in the Spatial and Frequency Domains", Pattern Recognition 36, PP. 969 -975, Elsevier

Sohn, J. S., Lee, S. I., Lee, S. H., Kwon, K. R. and Kim, D. G. (2006), "Blind Image Watermarking Technique for Digital Phone Camera", IEEE Sensors, IEEE Computer Society, *Conf*, Daegu, Korea

Song, C., Sudirman, S., Merabti, M. and Jones, D. L. (2010), "Analysis of Digital Image Watermark Attacks", Proc, Consumer Communications and Networking Conference (CCNC), 2010 7th IEEE , IEEE Computer Society

Sun Q. and Zhang, Z. (2006), "A Standardized JPEG2000 Image Authentication Solution based on Digital Signature and Watermarking", China Communications, pp. 71-80

Swain, M. J. and Ballard D. H. (1991). Color indexing. International Journal of Computer Vision, 7(1):11–32

Tao, P. and Eskicioglu, A. M. (2004), "A robust multiple watermarking scheme in the Discrete Wavelet Transform domain", Proc, SPIE, Internet Multimedia Management Systems V, Vol. 5601, 133, Philadelphia, PA, USA

Temi, C., Choomchuay, S., and Lasakul, A. (2005), "A Robust Image Watermarking using Multiresolution Analysis of Wavelet", Proc, IEEE International Symposium on Communications and Information Technology, 2005. ISCIT 2005. Vol. 1, IEEE Computer Society

Voloshynovskiy, S., Pereira, S., Iquise V. and Pun, T. (2001)," Attack Modeling: towards a second generation watermarking benchmark", Signal Processing Vol. 81, pp. 1177-1214, Elsevier

Wang, J. and Liu, R. (2009) , "Low Complexity DCT-Based Distributed Source Coding for Hyperspectral Image", 4^{th} International Conference on Communications and Networking, ChinaCOM, PP. 1-5, IEEE Computer Society

Wang, R., Lin, C. and Lin, J., (2000), "Hiding data in images by optimal moderately significant bit replacement", IEE Electronics Letters, vol.36, no.25, pp.2069-2070

Wang, S. (2005), "Steganography of capacity required using modulo operator for embedding secret image, (2005)", Applied Mathematical and Computation, Applied Mathematics and Computation, vol.164, pp. 99–116

Wang, S., Zheng, D., Zhao , J., Tam, W. J., and Speranza, F. (2005)," An accurate method for image quality evaluation using digital watermarking", IEICE Electronics Express, vol.2, no.20, pp.523-529

Wang, Y., and Pearmain, A., (2004), "Blind Image Data Hiding based on Self Reference", Pattern Recognition Letters, vol. 25, pp.1681–1689

Westfeld, A., and Pfitzmann, A. (1999), "Attacks on Stenganographic Systems Breaking the Stenganographic Utilities EzStego, Jsteg, Stegnos, and S-Tools and Some Lessons Learned ", Proc, International Workshop Information Hiding, Dresden, Germany

Wolfgang, R. B., Podilchuk, C. I., and Delp, E. J. (1999), "Perceptual Watermarks for Digital Images and Video," Proceedings of the IEEE, Vol. 87, No. 7, PP. 1108-1126

Wu, D.C. and Tsai, W.H. (2000) "Spatial-domain image hiding using image differencing", IEE Proc.-Vcs. hncige Signal Process 147, No.1, pp.29-37

Wu, H.-C., Wu, N., Tsai, (2003), "A Stegnographic Method for Images by Pixel-value Differencing", Pattern Recognition Letters, vol.24, pp.1613-1626

Wu, H.-C., Wu, N.-I., Tsai, C.-S. and Hwang, M.-S. (2005), ‘Image steganographic scheme based on pixel-value differencing and LSB replacement methods”, Visual and Image Signal Processing, Vol. 152, No. 5, IEE

Wu, N., (2004), A Study on Data Hiding for Gray-Level and Binary Image, Master Thesis, Chaoyang University of Technology, Taiwan

Wu, N. I., and Hwang, M. (2007), “Data Hiding: Current Status and Key Issues”, International Journal of Network Security, Vol.4, No.1, PP.1–9

Wu, X., Guan, Z. (2007), “A Novel Digital Watermark Algorithm based on Chaotic Maps”, Physics Letters A, Vol.365, pp.403–406

Wu, X. , Guan, Z. and Wu, Z. (2007), ”A Chaos Based Robust Spatial Domain Watermarking Algorithm”, Lecture Notes in Computer Science, Vol.4492/2007, pp.113-119

Xuan, M., and Jiang, J. (2009), “A Novel Watermarking Algorithm in Entropy Coding Based on Image Complexity Analysis ”, proc, International Conference on Multimedia Information Networking and Security, MINES'09, PP 128-129

Yang, C. (2008), “Inverted pattern approach to improve image quality of information hiding by LSB.”, Pattern Recognition 41, Elsevier, PP. 2674 – 2683

Yin, C. Y., Wu, D. C. and Tsai W. H. (2002), “New Data Hiding Methods for Copyright Protection, Annotation and Authentication of BMP Archive Images in Digital Libraries and Museums”, proc, 1st Workshop on Digital Achieves Technologies, pp. 168-183, Taiwan

Yoo, J., Choi, B. and Choi, H. (2010), “1-D fast normalized cross-correlation using additions”, Digital Signal Processing 20, PP. 1482–1493, Elsevier

Yoshida, M., Fujita, T. and Fujiwara, T. (2006), “A New Optimum Detection Scheme for Additive Watermarks Embedded in Spatial Domain”, proc, International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IEEE Computer Society

You, X., Du, L., Cheung, Y. and Chen Q., (2010), “A Blind Watermarking Scheme Using New Nontensor Product Wavelet Filter Banks”, IEEE TRANSACTIONS ON IMAGE PROCESSING, Vol. 19, No. 12

Zeki, A. M., and Manaf A. A. (2007), “Robust Digital Watermarking Method based on Bit-Plane Ranges”, Studies in Informatics and Control Journal, Romania

Zeki, A. M. and Manaf, A. A. (2009), " A Novel Digital Watermarking Technique Based on ISB (Intermediate Significant Bit), International Journal of Information Technology, vol:5:3

Zeki, A. M. and Manaf, A. A. (2011), "ISB Watermarking Embedding: A Block Based Model", Information Technology Journal, Vol.10, No.4, pp.841-848

Zhang, D., Xu, J., Li, H. and Li, H. (2009), "A Novel Image Watermarking Algorithm with Fast Processing Speed", International Conference on Information Engineering and Computer Science, IEEE Computer Society, pp.1-4

Zhang, X., and Wang, S., (2004), "Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security", Pattern Recognition Letters, vol.25, pp. 331–339

Zhao, X. and Ho, A. T. S. (2010), "An Introduction to Robust Transform Based Image Watermarking Techniques", Studies in Computational Intelligence, Volume 282, Intelligent Multimedia Analysis for Security Applications, PP. 337-364

Zimmermann, H.J. (1978), Fuzzy programming and linear programming with several objective functions. Fuzzy Sets and Systems, 1, PP. 44–55