

國立交通大學

資訊管理研究所

碩士論文

以小波為基礎並利用雙浮水印與人類視覺系統之多
功能彩色浮水印技術

Wavelet Based Multipurpose Color Image Watermarking by Using
Dual Watermarks with Human Vision System Models

研究生：林志文

指導教授：蔡銘箴 博士

中華民國九十六年六月

以小波為基礎並利用雙浮水印與人類視覺系統之多功能彩色浮
水印技術

Wavelet Based Multipurpose Color Image Watermarking by Using Dual
Watermarks with Human Vision System Models

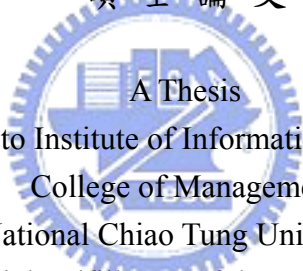
研究生：林志文

Student : Chih-Wen Lin

指導教授：蔡銘箴

Advisor : Min-Jen Tsai

國立交通大學
資訊管理研究所
碩士論文



A Thesis
Submitted to Institute of Information Management
College of Management
National Chiao Tung University
in Partial Fulfillment of the Requirements
for the Degree of
Master of Science
in

Information Management

June 2007

Hsinchu, Taiwan, Republic of China

中華民國九十六年六月

以小波為基礎並利用雙浮水印與人類視覺系統之多功能彩色浮水印技術

學生：林志文

指導教授：蔡銘箴 博士

國立交通大學資訊管理研究所碩士班

摘 要

本論文中，我們提出一套完整的數位浮水印架構，以同時解決數位內容所有權保護與驗證之議題，我們將可視與半易碎型浮水印(雙浮水印)結合並嵌入彩色圖片數位內容之中，可視浮水印將對所有權保護產生效用，半易碎型浮水印則在驗證浮水印圖片的完整性與一致性，防止有心人對可視浮水印圖片進行破壞，使其失去所有權保護之效能。

在設計可視浮水印系統時，比較重要的條件和需求為半透明性與強韌性，但這兩者互為取捨，本研究中，我們發現人類視覺系統 HVS (Human Visible System)-對比敏感函數 CSF (Contrast Sensitive Function) 與 雜訊可見函數(Noise Visibility Function) 可以在兩者之間取得一個適當的平衡點，透過 CSF 與 NVF 可以得知圖片全域與區域性的特性以便進行可視浮水印的嵌入，同時加入小波雜訊可視門檻值(DWT Noise Visibility thresholds) 調整浮水印加入的權重，使可視浮水印有較佳的視覺效果並兼任強韌性。在半易碎型浮水印系統中，此演算法可以正確判斷竄改之位置，並可以容忍無意間的攻擊類型(例如:JPEG 壓縮與 Additive White Gaussian Noise 加成性白色高斯雜訊)，達到驗證之功能。實驗結果顯示，我們產生出來的可視浮水印圖片比其他提出演算法有較好的視覺品質並有較佳的強健性，對於近年藉由影像重建理論(Image Recovery)抹除可視浮水印，也有較佳的抵抗能力。

關鍵詞 — 人類視覺系統，半易碎型浮水印，竄改偵測，可視浮水印。

Wavelet Based Multipurpose Color Image Watermarking by Using Dual Watermarks with Human Vision System Models

Student: Chih-Wen Lin

Advisor: Dr. Min-Jen Tsai

Institute of Information Management
National Chiao Tung University

ABSTRACT

In this study, we propose a complete architecture based on digital watermarking techniques to solve the issue of copyright protection and authentication for digital contents. We apply visible and semi-fragile watermarks as dual watermarks where visible watermarking is used to establish the copyright protection and semi-fragile watermarking authenticates and verifies the integrity of the watermarked image.

In order to get the best tradeoff between the embedding energy of watermark and the perceptual translucence for visible watermark, the contrast-sensitive function (CSF) and noise visible function (NVF) of perceptual model is applied which characterizes the global and local image properties and identifies texture and edge regions to determine the optimal watermark locations and strength at the watermark embedding stage. In addition, the perceptual weights according to the basis function amplitudes of DWT coefficients is fine tuned for the best quality of perceptual translucence in the design of the proposed watermarking algorithm. Furthermore, the semi-fragile watermark can detect and localize malicious attack effectively yet tolerate mild modifications such as JPEG compression and channel additive white Gaussian noise (AWGN). From the experimental results, our proposed technique not only improves the PSNR values and visual quality than other algorithms but also preserves the visibility of the watermark visible under various signal processing and advanced image recovery attacks.

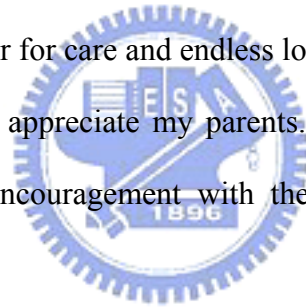
Index Terms — HVS, semi-fragile watermark, tamper detection, visible watermarking.

ACKNOWLEDGMENT

I would like to express my sincere appreciation to my advisor, Dr. Min-Jen Tsai for his valuable guidance and patience during the two years period in Chiao-Tung University, and the three orals commissioners Dr. Long-Wen Chang, Dr. Suh-Yin Lee, and Dr. Chun-Shien Lu for their helpful comments and guidance. In addition, I am very thankful to my faculty members, Chih-Cheng Chien, Yuan Fu Luo, Ching Ting Lin, Yin Kai Hung, for their discussions, suggestions and help at all times.

Then, I want to give my deepest love and gratitude to my girl friend, Joahanna Lee. Without her support and patience, this thesis might not achieve on time and even could not be accomplished. I really thank her for care and endless love.

Finally, I want to deeply appreciate my parents. They are the most important support behind me. Their love and encouragement with them were very constructive for me to accomplish this work.

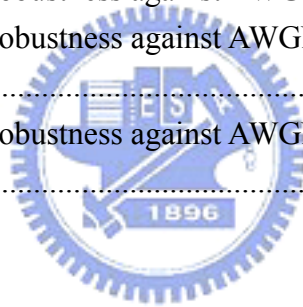


Contents

摘 要	ii
ABSTRACT	iii
ACKNOWLEDGMENT	iv
List of Tables	vi
List of Figures.....	vii
I. Introduction	1
1.1 Intellectual Property	1
1.2 Digital Watermarking	2
1.3 Organization of the Dissertation.....	7
II. Related Works	8
2.1 Visible watermarking.....	8
2.2 Image Authentication and Temper Detection	11
III. Proposed Algorithm for Copyright Protection and Image Authentication	14
3.1 Human Visual System Model	14
3.1.1 CSF (Contrast Sensitive Function)	15
3.1.2 NVF (Noise Visibility Function).....	18
3.2 DWT noise detection thresholds.....	20
3.3 Visible watermarking Algorithm	21
3.4 Image Authentication (Semi -Fragile watermark) Algorithm	25
IV. Experimental Results and Discussion.....	30
4.1 Visual Effect	34
4.2 PSNR (Peak Signal-Noise Ratios).....	36
4.3 JPEG 2000 Compression.....	37
4.4 Median Filter	40
4.5 ICA (Independent component analysis) Image recovery Attack.....	43
4.6 Tamper Detection.....	49
V. Conclusion and future work	59
References	60

List of Tables

Table 1	The basic function amplitudes for a five-level 9/7 DWT	20
Table 2	PSNR summary of watermarked color images.....	36
Table 3	PSNR summary of watermarked color images before and after JPEG 2000 Compression	38
Table 4	PSNR summary of watermarked color images before and after Median Filter	41
Table 5	Lena (NCTU logo): Robustness against AWGN and JPEG compression.	54
Table 6	Lena (IIM logo): Robustness against AWGN and JPEG compression.....	54
Table 7	Baboon (NCTU logo): Robustness against AWGN and JPEG compression.....	54
Table 8	Baboon (IIM logo): Robustness against AWGN and JPEG compression.	54
Table 9	lake (NCTU logo): Robustness against AWGN and JPEG compression.	54
Table 10	lake (IIM logo): Robustness against AWGN and JPEG compression.	55
Table 11	Peppers (NCTU logo): Robustness against AWGN and JPEG compression.	55
Table 12	Peppers (IIM logo): Robustness against AWGN and JPEG compression.	55
Table 13	Lena (NCTU logo): Robustness against AWGN and JPEG compression by using Bi18/10 Filter.....	57
Table 14	Lena (NCTU logo): Robustness against AWGN and JPEG compression by using Bi9/7 Filter.....	57



List of Figures

Fig. 1	Watermark embedding process.....	6
Fig. 2	Watermark extraction process.....	6
Fig. 3	Luminance CSF.....	15
Fig. 4	DWT CSF mask with 11 unique weights.....	16
Fig. 5	The adequate modulation rate for each subband.....	17
Fig. 6	$\beta_{\lambda,\theta}$ in different DWT level and orientation.....	22
Fig. 7	The flow chart of the proposed visible watermarking approach.....	24
Fig. 8	The flow chart of the proposed semi-fragile watermark approach.....	27
Fig. 9	The flow chart of authentication and tamper detection algorithm approach.....	29
Fig. 10	Two watermark images : (a) NCTU logo (b) IIM logo.....	31
Fig. 11	(a) original Lena image (b) watermarked Lena image by the method in Huang and Tang (c) watermarked Lena image by the proposed algorithm.....	31
Fig. 12	(a) original Lena image (b) watermarked Lena image by the method in Huang and Tang (c) watermarked Lena image by the proposed algorithm.....	31
Fig. 13	(a) original Baboon image (b) watermarked Baboon image by the method in Huang and Tang (c) watermarked Baboon image by the proposed algorithm.....	32
Fig. 14	(a) original Baboon image (b) watermarked Baboon image by the method in Huang and Tang (c) watermarked Baboon image by the proposed algorithm.....	32
Fig. 15	(a) original Lake image (b) watermarked Lake image by the method in Huang and Tang (c) watermarked Lake image by the proposed algorithm.....	32
Fig. 16	(a) original Lake image (b) watermarked Lake image by the method in Huang and Tang (c) watermarked Lake image by the proposed algorithm.....	33
Fig. 17	(a) original Peppers image (b) watermarked Peppers image by the method in Huang and Tang (c) watermarked Peppers image by the proposed algorithm.....	33
Fig. 18	(a) original Peppers image (b) watermarked Peppers image by the method in Huang and Tang (c) watermarked Peppers image by the proposed algorithm.....	33
Fig. 19	The visual comparison of close-ups for images to figure 11 through 18 (a) close-ups of the original images (b) close-ups of the watermarked images by the method in Huang and Tang (c) close-ups of the watermarked images by the proposed algorithm.....	35
Fig. 20	The visual quality comparison of close-ups of watermarked image after jpeg 2000 compression ratio of 100:3 (a) original image (b) watermarked images by the Huang and Tang's method (c) watermarked image by the proposed algorithm.....	39
Fig. 21	The visual quality comparison of close-ups of 7x7 median filtering of watermarked image (a) original image (b) watermarked images by the Huang and Tang's method	

(c) watermarked image by the proposed algorithm	42
Fig. 22 Recovering the public domain image (a) watermarked image (b) recovered image (c) watermarked image (d) recovered image	44
Fig. 23 Recovering the watermarked images from our method (a) watermarked image with NCTU logo (b) recovered image from watermarked image with NCTU logo (c) watermarked image with IIM logo (d) recovered image from watermarked image with IIM logo	45
Fig. 24 Recovering the watermarked images from our method (a) watermarked image with NCTU logo (b) recovered image from watermarked image with NCTU logo (c) watermarked image with IIM logo (d) recovered image from watermarked image with IIM logo	46
Fig. 25 Recovering the watermarked images from our method (a) watermarked image with NCTU logo (b) recovered image from watermarked image with NCTU logo (c) watermarked image with IIM logo (d) recovered image from watermarked image with IIM logo	47
Fig. 26 Recovering the watermarked images from our method (a) watermarked image with NCTU logo (b) recovered image from watermarked image with NCTU logo (c) watermarked image with IIM logo (d) recovered image from watermarked image with IIM logo	48
Fig. 27 (a) Result (watermarked) image (b) Tampered image (c) Tampering detection.....	49
Fig. 28 (a) Result (watermarked) image (b) Tampered image (c) Tampering detection.....	50
Fig. 29 (a) Result (watermarked) image (b) Tampered image (c) Tampering detection.....	50
Fig. 30 (a) Result (watermarked) image (b) Tampered image (c) Tampering detection.....	50
Fig. 31 Tamper detection for mixing tampering operations and AWGN (a) watermarked image (b) tampered image (c) $\sigma^2 = 6$ (d) $\sigma^2 = 12$ (e) $\sigma^2 = 18$ (f) $\sigma^2 = 24$ (g) $\sigma^2 = 30$ (h) $\sigma^2 = 36$	52
Fig. 32 Tamper detection for mixing tampering operations and JPEG compression (a) QF=100 (b) QF=90 (c) QF=80 (d) QF=70 (e) QF=60 (f) QF=50	52
Fig. 33 (a) Dual watermarked image of Lena (b) Tampered dual watermarked image with watermark removal attack (c) Tampering Detection	53
Fig. 34 (a) Dual watermarked image of Baboon (b) Tampered dual watermarked image with watermark removal attack (c) Tampering Detection	53
Fig. 35 (a) Dual watermarked image of Lake (b) Tampered dual watermarked image with watermark removal attack (c) Tampering Detection	53
Fig. 36 (a) Dual watermarked image of Peppers (b) Tampered dual watermarked image with watermark removal attack (c) Tampering Detection	53
Fig. 37 Tamper Detection after JPEG compression using different filters (QF) (a) QF=80 by using Bi 18/10 Filter (b) QF=70 by using Bi 18/10 Filter (c) QF=60 by using Bi 18/10 Filter (d) QF=80 by using Bi 9/7 Filter (e) QF=70 by using Bi 9/7 Filter (f)	

QF=60 by using Bi 9/7 Filter.....	56
Fig. 38 Tamper Detection after AWGN using different filters (a) $\sigma^2 = 6$ by using Bi 18/10 Filter (b) $\sigma^2 = 12$ by using Bi 18/10 Filter (c) $\sigma^2 = 18$ by using Bi 18/10 Filter (d) $\sigma^2 = 6$ by using Bi 9/7 Filter (e) $\sigma^2 = 12$ by using Bi 9/7 Filter (f) $\sigma^2 = 18$ by using Bi 9/7 Filter	57
Fig. 39 (a) Dual watermarked image of Lena and the size is 512×480 (b) Tampered dual watermarked image and the size is 512×480 (c) Tampering Detection.....	58

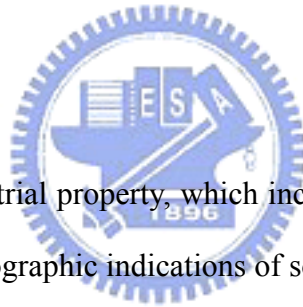


I. Introduction

1.1 Intellectual Property

We are now in an era of knowledge-based economy. At the core of such an economy, intellectual property becomes the critical issue we concerned. Intellectual property acts like real property and surrounds us in nearly everything we do. Books, music, digital multimedia, and any kind of arts actually belong to the authors who made it, and the authors have the rights to restrict access to intellectual property [1].

Intellectual property refers to creations of the mind: inventions, literary and artistic works, and symbols, names, and images used in commerce. Intellectual property is divided into two categories [1]:



- **Industrial Property:** Industrial property, which includes inventions (patents), trademarks, industrial designs, and geographic indications of source.
- **Copyright:** Copyright, which includes literary and artistic works such as novels, poems and plays, films, musical works, drawings, paintings, photographs and sculptures, and architectural designs.

There are several compelling reasons for promoting and protecting intellectual property. First, the progress and well-being of humanity rests on its capacity for new creations in the areas of technology and culture. Second, the legal protection of these new creations encourages the expenditure of additional resources, which leads to further innovation. Third, the promotion and protection of intellectual property spurs economic growth, creates new jobs and industries, and enhances the quality and enjoyment of life.

1.2 Digital Watermarking

Because of the advantages of digital media and rapid development of digital signal processing, a variety of multimedia contents have been digitalized and easily distributed or duplicated without any reduction in quality through both authorized and unauthorized distribution channels. With the ease of editing and reproduction, protection of the copyright and authentication of digital multimedia become an important topic in these years.

Over the last two decades, software, multimedia, and all digital content-driven industries, whether on the Internet or not, have also come to rely on effective copyright protection, especially as a revolution is underway in digital entertainment and marketing.

In the beginning, conventional encryption algorithms such as DES or RSA are directly adopted to protect digital media. In these cryptographic systems, only the valid users who have the correct decryption key can decrypt the encrypted content and use it. But once such content is decrypted the users can duplicate and retransmit it again and again, the authors still have no way to track. Therefore, conventional cryptography is not a good way to solve this issue.

Digital watermarking [2] has been extensively researched and regarded as a potentially effective means for protecting copyright of digital media in recent years, since it makes possible to embed secret information in the digital content to identify the owner of it. Digital watermarking describes methods and technologies that allow hiding information, for example a number sequence or recognizable pattern, in digital media, such as images, video and audio. A lot of digital watermarking techniques have been proposed by many researchers and can be divided into various categories and in various ways [3]. One important classification is to divide digital watermarking algorithms into visible and invisible ones according to the perceptivity of watermark data in watermarked contents.

Visible watermarking schemes protect copyrights in a more active method. They not only prevent pirates but also recognize the copyright of multimedia data. Digital contents embedded with visible watermarks will overlay recognizable but unobtrusive copyrights patterns identifying its ownership. Therefore, a useful visible watermarking technique should remain details of contents and ensure embedded patterns difficult or even impossible to be removed, and no one could use watermarked data illegally.

An effective visible watermarking algorithm usually requires meeting a set of requirements [4]. These requirements include:

- The watermark in the marked digital contents should be obvious and recognizable to any person having normal or corrected visual accommodation, even if that person is color-blind. Clearly, the visible watermark should be visible in both color and monochrome images
- It should be possible to adjust the strength of embedding applied to digital contents by referring to the characteristics of the digital contents, so the watermark could be made as obtrusive or unobtrusive as desired and didn't introduce any artifacts. It should not only protect the digital contents from unauthorized uses but also not make it so unattractive that no one is interested in viewing it.
- The patterns of the watermark in the embedded contents should be visible, and should form a recognizable symbol to identify contents owners or providers.
- All details of the unmarked digital contents should be preserved in the marked digital ones. It means that corresponding pixel values in marked regions between with original and watermarked digital contents should be different in brightness, but be the same in hue and saturation.
- The watermark should be very difficult to remove or robust to attacks. This is the meaning of robustness. Watermark removal, at a minimum, should be more costly and labor intensive than purchasing rights to use the digital data.

On the other hand, invisible watermark schemes can be broadly classified into three types: robust watermarks, fragile (or semi-fragile) watermarks and captioning watermarks [5]. For copyright protection and ownership verification, robust watermarks are adopted because they should be nearly resistant to any image processing operations as desired. For content authentication and integrity verification, fragile (or semi-fragile) watermarks are used because they are fragile to certain alterations and modifications of the authenticated multimedia. Semi-fragile watermarks are more practical than fragile watermarks, since they are robust to some mild modifications such as JPEG compression and channel AWGN (additive white Gaussian noise) causing by exchange and storage but fragile to malicious attacks like image cropping which crops objects from a source and pastes them onto a target. Captioning watermarks are mainly used for conveying side information, so the algorithms are required to convey more information than robust watermarks.

According to the conveyance of authentication data, fragile (or semi-fragile) watermarks can be classified into two main categories: labeling-based authentication scheme and watermarking-based authentication scheme. The watermarking-based authentication schemes embed the data into the original multimedia contrast to labeling-based authentication ones that store the authentication data in a separate file. Consequently, the authentication data becomes the integral part of the original multimedia and can be transmitted more efficiently and securely [6] [7]. In this paper, we focus on the semi-fragile watermarking based authentication scheme and some necessary requirements as follows [8]:

- The semi-fragile watermarks should satisfy robustness and fragility objectives simultaneously and have a quantitative mechanism to tradeoff between these objectives.
- For security, the semi-fragile watermarks should be secure to intentional tampering and be impossible for the opponent to create a fraudulent message.

- In the hiding processes, the semi-fragile watermarks must ensure the modifications of the media are imperceptible.
- For authentication embedding and verifying processes, the semi-fragile watermarks must be computationally efficient, especially for real time applications.

Regardless of exploiting the digital watermarking techniques, Fig. 1 and Fig. 2 describe the generic structure for watermark embedding and extraction processes. First, a host image (original image) directly embeds watermark in spatial domain or is transformed into frequency domain through the well-known spread spectrum approach, i.e. DFT (Discrete Fourier Transform), DCT (Discrete Cosine Transform) or DWT (Discrete Wavelet Transform). However, the algorithms using transform domain offer more robust than directly embedding watermark into spatial domain. Then, coefficients are passed through a perceptual analysis block that determines how strong of the watermark in embedding algorithm so that the resulting watermarked image is imperceptible. The secret key uses to generate watermark and watermark embedding location more. The watermark is embedded using a specific well-designed algorithm based on mathematical or statistical model. If the coefficients in frequency domain, the inverse spread spectrum approach is then adopted to obtain a watermarked image. The watermark extraction applies the similar operations in embedding processes. It employs the inverse operations or uses the mathematical or statistical characteristic to extract the embedded watermark. Watermark detection decides whether an image has been watermarked and the watermark exists or not by calculating the correlation between the embedded watermark and the extracted one.

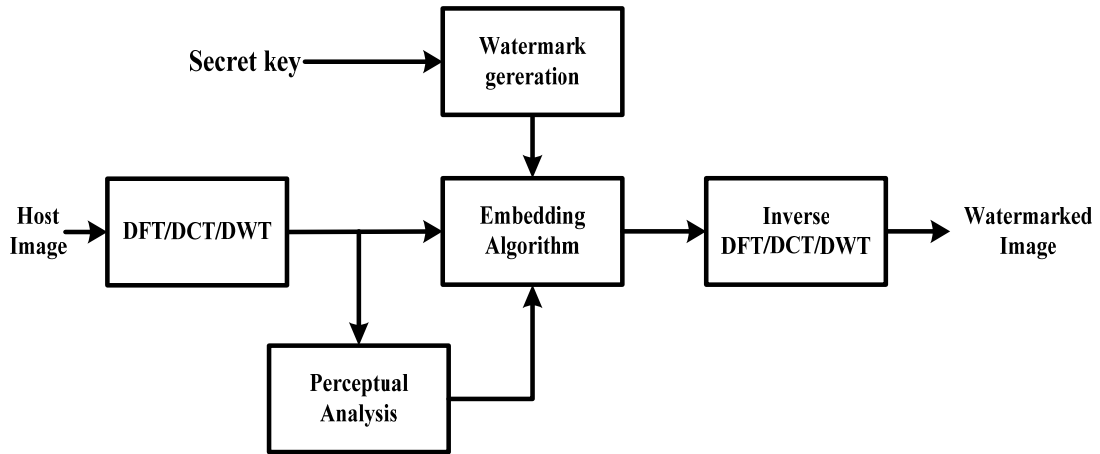


Fig. 1 Watermark embedding process.

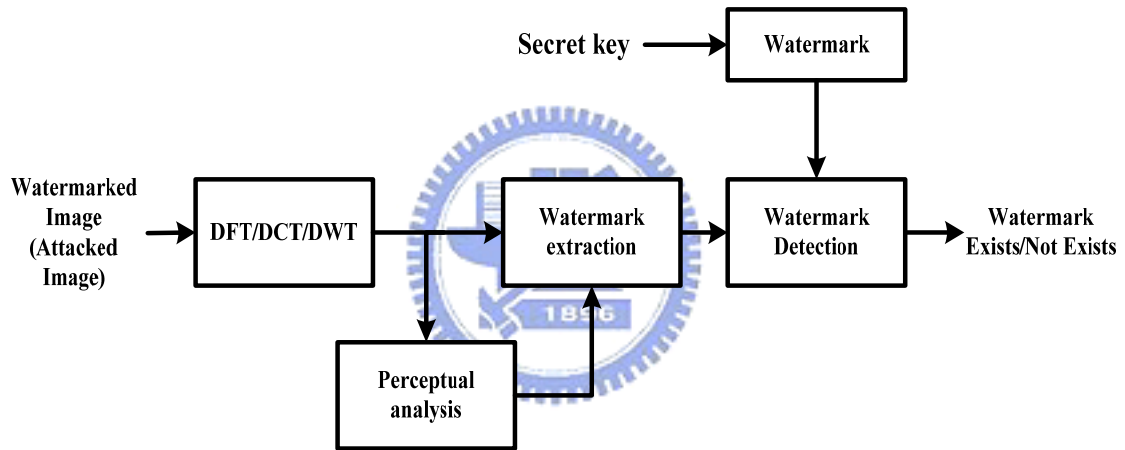


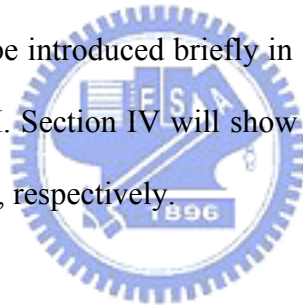
Fig. 2 Watermark extraction process.

The goal of this paper is to propose a novel scheme for copyright protection and authentication of color images by using visible watermark and semi-fragile watermark. For copyright protection, we present a differential visible watermarking algorithm based on noise reduction and Human Visible System (HVS) model to get the best tradeoff between the embedding energy of watermark and the perceptual translucence for visible watermark. The collaboration of CSF and NVF for HVS models is leveraged with the noise reduction of the visibility thresholds for HVS in DWT domain. The perceptual weights is fine tuned for

watermark embedding which results significant improvement over the watermarked images by CSF only algorithms regarding the image quality, translucence and robustness of the watermarking. For authentication and verifying the integrity of the watermarked images, we applied a semi-fragile watermark algorithm which can detect and localize malicious attack effectively yet tolerate mild modifications such as JPEG compression and channel additive white Gaussian noise (AWGN). In our algorithm, the order of embedding is visible watermark first and semi-fragile watermark next.

1.3 Organization of the Dissertation

The rest of this paper is organized as follows. Related works about visible watermarking and image authentication will be introduced briefly in Section II. The details of the algorithm will be explained in Section III. Section IV will show the experiments results and discussion and conclusion is in Section VI, respectively.



II. Related Works

2.1 Visible watermarking

Visible watermarking techniques are used to protect copyright of digital multimedia (audio, image or video) that have to be delivered for certain purpose, such as digital multimedia used in exhibition, digital library, advertisement or distant learning web, while illegal duplicate is forbidden. From the literature survey, the visible watermarking has captured greater attention than the invisible one [9] since there are not only different visible watermarking approaches either in spatial or transform domain but also various visible watermark removal schemes. We will briefly address different visible watermark techniques here and the removal schemes will be further discussed in Section IV.

Braudaway et al. [4] proposed one of the early approaches for visible watermarking by formulating the nonlinear equation to accomplish the luminance alteration in spatial domain. In this scheme, dimensions of watermark image are equal to those of the host image. There is a one-to-one correspondence between pixel locations in the watermark image and those in the host image. According to their brightness, pixels in the watermark image can be divided into transparent and nontransparent ones. The brightness of each pixel in the host image in proportion to the nontransparent regions of the watermark will be increased or reduced to a perceptually equal amount by using nonlinear equation while the brightness of each pixel in proportion to the transparent regions of the watermark will remain the same after watermark embedding. They formulate the nonlinear equation by using an approximately color space, such as the CIE 1976 ($L^*u^*v^*$) space and the CIE ($L^*a^*b^*$) space and various parameters of the nonlinear equation are applied to make the watermark difficult to remove.

Meng and Chang [10] applied the stochastic approximation for Braudaway's method in

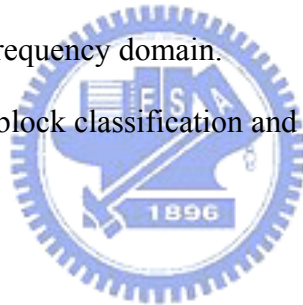
the discrete cosine transform (DCT) domain by adding visible watermarks in video sequences. Mohanty et al. [11] proposed a watermarking technique called dual watermarking by combining of a visible watermark and an invisible watermark in the spatial domain. The visible watermark adopted to establish the owner's right to the image and invisible watermark to check the intentional and unintentional tampering of the image. Chen [12] has proposed a visible watermarking mechanism to embed a gray level watermark into the host image based on a statistic approach. First, the host image is divided into equal blocks and the standard deviation in each block is calculated. The standard deviation value will determine the amount of gray value of the pixel in the watermark to be embedded into the corresponding host image.

Kankanhalli et al. [13] proposed a visible watermarking algorithm in the discrete cosine transform (DCT) domain. First, the host image and the watermark image are divided into 8x8 blocks. Then, they classify each block into one of 8 classes depending on the sensitivity of the block to distortion and adopted the effect of luminance to make a final correction to the block scaling factors. The strength of the watermark is added in varying proportions depending on the class to which the image block belongs. Kankanhalli et al. [14] proposed a modification to their above watermark insertion technique to make the watermark more robust.

Hu and Kwong [15-16] implemented an adaptive visible watermarking in the wavelet domain by using the truncated Gaussian function to approximate the effect of luminance masking for the image fusion. Based on image features, they first classify the host and watermark image pixels into different perceptual classes. Then, they use the classification information to guide pixel-wise watermark embedding. In high-pass subbands, they focus on image features, while in the low-pass subband, they use truncated Gaussian function to approximate the effect of luminance masking. Yong et al. [17] also proposed a translucent digital watermark in the DWT domain and use error-correct code to improve the ability to anti-attack.

Each of above schemes wasn't devoted to better feature-based classification and the use of sophisticated visual masking models, so Huang and Tang [9] presented a contrast sensitive visible watermarking scheme with the assistance of HVS. They first compute the CSF mask of the discrete wavelet transform domain. Secondary, they use square function to determine the mask weights for each subband. Third, they adjust the scaling and embedding factors based on the block classification with the texture sensitivity of the HVS. However, their scheme doesn't consider the following issues:

1. The basis function of the wavelet transform plays an important role during the application of CSF for the HVS in the wavelet transform domain.
2. The embedding factors emphasize more weights in the low frequency domain instead of the medium-to-high frequency domain.
3. The interrelationship of block classification and the characteristics of the embedding location.



For issues one, the direct application of CSF for the HVS in the wavelet transform domain needs to be further studied [18, 19, 20] while the basis function of the wavelet transform is a critical factor to affect the visibility of the noise in the DWT domain. For issue two, the watermark embedding in the low frequency components results high degradation of the image fidelity. In addition, the high frequency components of the watermarked image easily suffer common image signal processing attacks with low robustness. For issue 3, the plane, edge and texture block classification in [9] is a genuine approach should the local and global characteristics of wavelet coefficients be further considered.

2.2 Image Authentication and Tamper Detection

Many content authentication schemes which are based on digital watermarking have been proposed and can be classified as watermarking-based authentication schemes contrast to labeling-based ones [7]. Some fragile watermarking techniques [7], [21], [22], [23], [24] were usually based on the concept of checksum produced by secure hash functions (e.g. MD5, SHA160) to verify the completeness of an image. They can detect and localize tamper correctly, but they treat admissible manipulations such as JPEG compression and channel AWGN as malicious attacks. Therefore, fragile watermarks are less practical than semi-fragile watermarks, so we focus on semi-fragile watermarking techniques in this paper.

Some semi-fragile watermarking schemes have been proposed to verify the integrity of digital contents and tolerate some degree of mild modifications. For have a better understanding of what have been already presented, some semi-fragile methods can be seen and reviewed in [8] [25] representing the state of the art, image content authentication. The fragile (semi-fragile) watermarks can be embedded in the spatial domain or the transformed domain. The schemes using spatial domain are simpler than the ones using transformed by utilizing the least significant bit (LSB) of data. However, the schemes that embed watermark in the transformed domain offer a higher degree of robustness [2]. Recently, many semi-fragile methods are based on wavelet transform domain since it suffers simple image processing operations to obtain a highest degree of robustness and allows the method to have spatial and frequency localization of digital data by the nature of multiresolution discrete wavelet decomposition.

Kundur and Hatzinakos [26] proposed one of the first approaches to semi-fragile watermarking called telltale tamper proofing. They embed a watermark in the discrete wavelet

domain of the image by quantizing the corresponding coefficients. They claim their tamper detection determined both in localized spatial and frequency regions is unlike previously proposed techniques embed a watermark in the spatial domain; They only provide information on the spatial location of the changes but fail to give a more general characterization of the type of distortion applied to the signal. They also use a statistics-based tamper assessment function as measurement for tamper proofing and authentication.

H.P. Alexandre et al. [27] proposed a novel technique for content authentication of digital images by quantizing wavelet packet coefficients and adopting characteristics of the human visual system to maximize the embedding weights for improving good imperceptibility of watermarked image. According to the experiment results, their method is able to detect and localize malicious image modifications while offering a certain degree of robustness to image compression. A similar concept was also proposed in [28], where they proposed a discrete wavelet transform-based image semi-fragile watermarking scheme based on fusion of multi-resolution. The Watson's quantization matrix [20] and the features of the human visual system are clearly adopted in the quantization process to get good quality of watermarked image. Z.M Liu et al. [29] presented a semi-fragile image watermarking technique based on index constrained vector quantization (VQ). However, the peak signal-to-noise ratio (PSNR) of their watermarked image is low and their scheme would waste storage and be not flexible for the codebook of vector quantization that should be known in both watermark embedding and extraction process.

Hua Yuan and Xiao-Ping Zhang [30] proposed a novel semi-fragile watermarking method based on image model using the Gaussian mixture model (GMM) in the wavelet domain. They modify selected wavelet coefficients according to the GMM parameters obtained through an EM algorithm. In experiment results, their scheme achieves minimum watermarking distortion and identifies mild modification from malicious attacks, but it treats AWGN as malicious attack.

Ding et al. [31] propose a wavelet-based chaotic semi-fragile watermarking scheme based on chaotic map and odd-even quantization. Their scheme can detect and localize malicious attacks with high peak signal-to-noise ratio (PSNR), while allowing more JPEG compression and channel additive white Gaussian noise (AWGN) tolerance. In [32], the authors presented a semi-fragile watermarking scheme for authenticating region of interest (ROI) of image. First, the reference mask is obtained by Poisson matting. Then, they embed watermark according to the reference mask, representing the region of interest of the image.

Since [31] is superior in obtaining high PSNR and resisting JPEG and AWGN attacks among other semi-fragile approaches, we further modify the scheme and integrate it into the proposed dual watermark approach which will explained in the next section.



III. Proposed Algorithm for Copyright Protection and Image Authentication

3.1 Human Visual System Model

The most important requirements in the visible watermarking scheme are the robustness and translucence, but unfortunately these are in conflict with each other. If we increase the energy of watermark to improve its robustness, the problem we get is perceptual translucence and vice versa. Therefore, we have to decrease the energy of the watermark to get good perceptual translucence and so the embedded watermark will not be robust to signal processing, intentional and unintentional attacks. HVS (Human Visual System) is the key factor we have found in providing the good translucence of the watermarked image and a better robustness.

A lot of work has been devoted to understanding HVS and offering mathematical models of how humans see the world. Psychovisual studies have shown that human vision has different sensitivity from various spatial frequencies (frequency subbands). Recently, many researchers have applied this knowledge to digital watermarking techniques. In digital watermarking schemes there has been a need of a good perceptual analysis for image quality that incorporates properties of the HVS and of a good strength of the watermark to provide a better robustness. Common HVS models are composed of image dependent or independent Just Noticeable Difference (JND) thresholds, so the HVS by using the contrast sensitive function (CSF) and noise visibility function (NVF) is integrated in this study and will be explained in brief as following:

3.1.1 CSF (Contrast Sensitive Function)

The contrast sensitive function (CSF) describes human's sensitivity to spatial frequencies. Mannos and Sakrison [33] originally presented a model of the CSF for luminance (or grayscale) images is given as follows:

$$H(f) = 2.6 * (0.0192 + 0.114 * f) * e^{-(0.114 * f)^{1.1}} \quad (1)$$

where $f = \sqrt{f_x^2 + f_y^2}$ is the spatial frequency in cycles/degree of visual angle (f_x and f_y are the spatial frequencies in the horizontal and vertical directions, respectively). Fig. 3 depicts the CSF curve which characterizes luminance sensitivity of the HVS as a function of normalized spatial frequency. According to the CSF curve, we can see that the HVS is most sensitive to normalized spatial frequencies between 0.025 and 0.125 and less sensitive to low and high frequencies. Therefore, this knowledge from CSF can be used to develop a simple image independent HVS model.

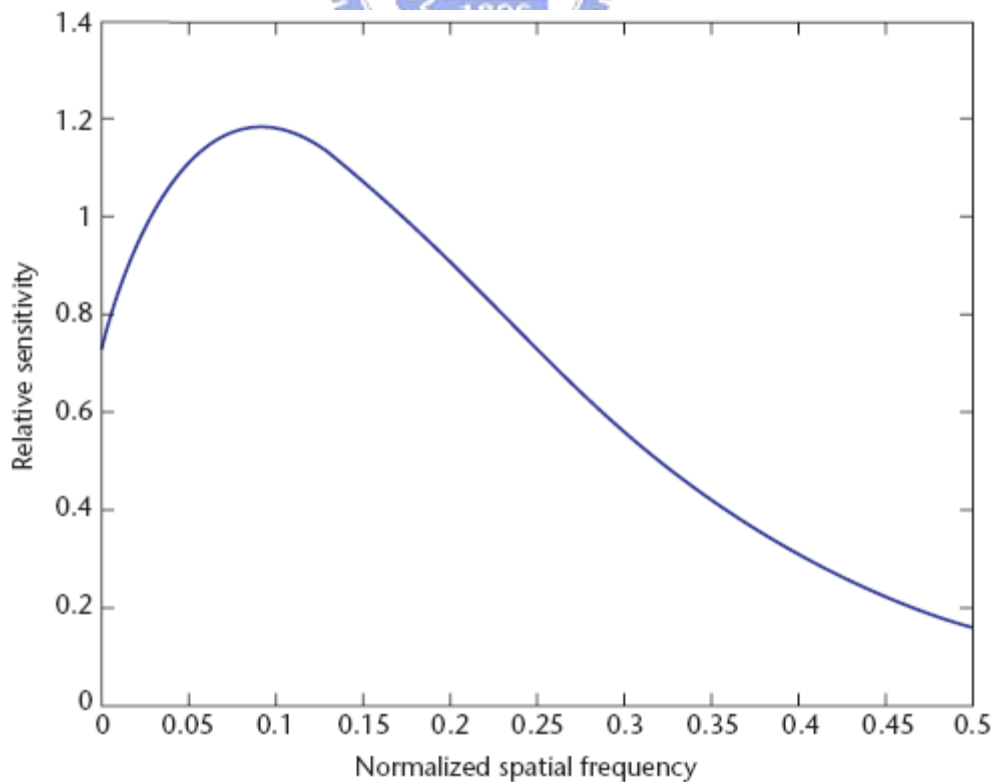


Fig. 3 Luminance CSF.

CSF masking [18] [19] is one way to apply the CSF in the discrete wavelet domain. CSF masking refers to the method of weighting the wavelet coefficients according to their perceptual importance. Some well-designed CSF masks which transform the CSF curve in Fig. 3 into perceptual importance weight are presented in [18]. Huang and Tang [9] use the same method led to 11-weight DWT CSF mask in the five-level wavelet transform. Fig. 4 illustrates the 11-weight DWT CSF mask with the weights shown for each subband.

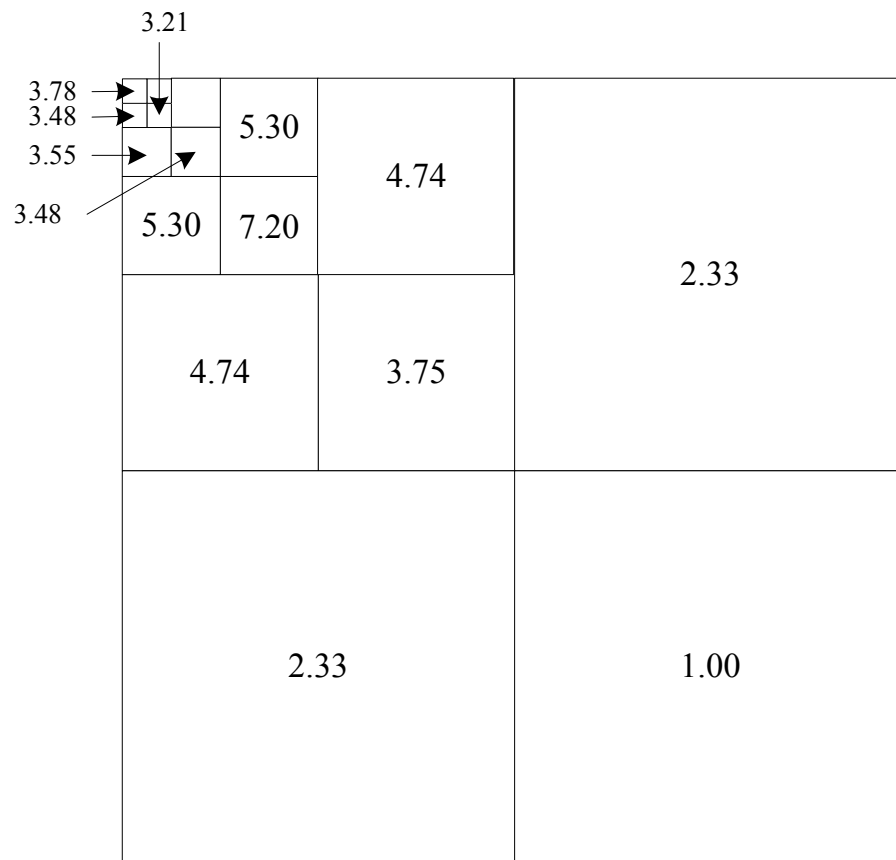


Fig. 4 DWT CSF mask with 11 unique weights.

For a five-level pyramidal DWT decomposition, the HVS is most sensitive to the distortion in mid-frequency regions (level 3) and sensitivity falls off as the frequency value drifts on both sides (level 1, 2, 4 and 5). The square function (2) in [9] is applied to approximate the effect of CSF masking.

The adequate modulation rate β^λ for each subband is determined by:

$$\beta^\lambda = 0.01 + \frac{(7.20 - r^\lambda)^2}{7.20^2} \quad (2)$$

where λ denotes the decomposed level and r^λ represents the wavelet coefficient CSF of the perceptual importance weight as shown in Fig. 4. The adequate modulation rate β^λ for each subband as shown in Fig. 5. The level 3 has the smallest rate for modulation.

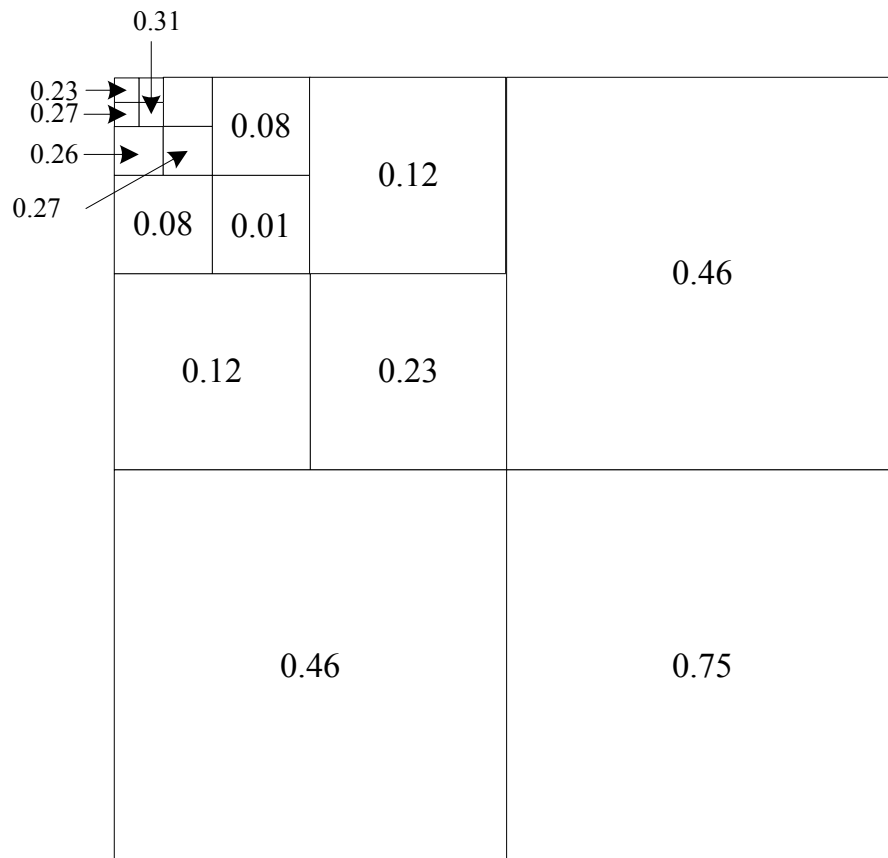


Fig. 5 The adequate modulation rate for each subband.

3.1.2 NVF (Noise Visibility Function)

Many schemes embedded the watermark as random noise in the whole host image with the same strength regardless of the local properties of the host image, so the visible artifacts are easy taken placed at flat regions. S.Voloshynovskiy et al. [34] presented a stochastic approach based on the computation of a NVF (Noise Visibility Function) that characterizes the local image properties and identifies texture and edge regions. Accordingly, when the local variance is small, the image is flat, and a large enough variance indicates the presence of edges or highly texture areas.

Because human eyes are sensitive to changes in flat than edges regions of the image, ones can increase the energy of watermark in the edges and high textured areas of the image, and reducing it in smooth regions in similar peak-signal noise rate (PSNR). This allows us to determine the optimal watermark locations and strength for the watermark embedding stage. Therefore, this concept from NVF can be used to develop a simple image dependent HVS model.

They developed three such NVF Functions:

1. NVF Function with Non-Stationary Gaussian Model

$$NVF(i, j) = \frac{1}{1 + \sigma_x^2(i, j)} \quad (3)$$

With

$$\sigma_x^2(i, j) = \frac{1}{(2L+1)^2} \sum_{k=-L}^L \sum_{l=-L}^L (x(i+k, j+l) - \bar{x}(i, j))^2$$

$$\bar{x}(i, j) = \frac{1}{(2L+1)^2} \sum_{k=-L}^L \sum_{l=-L}^L x(i+k, j+l)$$

where L as width of window, $\sigma_x^2(i, j)$ denotes the local variance in a window centered on the wavelet coefficient with coordinates (i, j) . Therefore, the NVF is

inversely proportional to the local image properties defined by the local variance.

2. NVF Function with Stationary GG (Generalized Gaussian) Model

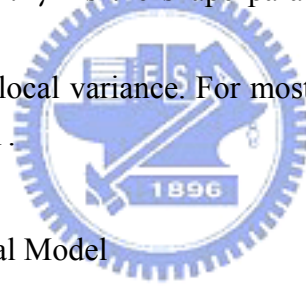
$$NVF(i, j) = \frac{w(i, j)}{w(i, j) + \sigma_x^2} \quad (4)$$

where $w(i, j) = \gamma[\eta(\gamma)]^\gamma \frac{1}{\|r(i, j)\|^{2-\gamma}}$ and σ_x^2 is the global variance of host

image. $\eta(\gamma) = \sqrt{\frac{\Gamma(\frac{3}{\gamma})}{\Gamma(\frac{1}{\gamma})}}$, $\Gamma(t) = \int_0^\infty e^{-u} u^{t-1} du$ (gamma function) and

$r(i, j) = \frac{x(i, j) - \bar{x}(i, j)}{\sigma_x}$. γ is the shape parameter and $r(i, j)$ is determined by

the local mean and the local variance. For most of real images, the shape parameter is in the range $0.3 \leq \gamma \leq 1$.



3. NVF Function with Empirical Model

$$NVF(i, j) = \frac{1}{1 + \theta \sigma_x^2(i, j)} \quad (5)$$

where $\theta = \frac{D}{\sigma_{x \max}^2}$ is a tuning parameter and $\sigma_x^2(i, j)$ is the local variance. $\sigma_{x \max}^2$ is the

maximum local variance and $D \in [50, 100]$ is an experimentally determined parameter.

3.2 DWT noise detection thresholds

In order to further improve the HVS model for better image quality, the knowledge of detection thresholds for DWT coefficients should be also studied. A.B. Watson, et al. [20] proposed a mathematical model for DWT noise detection thresholds which is a function of level, orientation, and display visual resolution. The model is given by:

$$\log Y = \log a + K (\log f_\lambda - \log g_\theta f_0)^2 \quad (6)$$

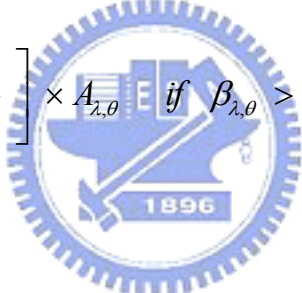
Where a is the minimum threshold is occurs at spatial frequency $g_\theta f_0$, f_λ is the spatial frequency of decomposition level λ , and g_θ shifts the minimum thresholds by an amount that is a function of orientation. Table 1 shows the basic function amplitudes for a 5-level DWT. In this paper, we use $A_{\lambda,\theta}$ indicating the basic function amplitudes, λ as DWT Level, and θ as Orientation.

Table 1 The basic function amplitudes for a five-level 9/7 DWT

Orientation	Level				
	1	2	3	4	5
LL	0.62171	0.345374	0.18004	0.0914012	0.0459435
HL	0.672341	0.413174	0.227267	0.117925	0.0597584
LH	0.672341	0.413174	0.227267	0.117925	0.0597584
HH	0.727095	0.494284	0.286881	0.152145	0.0777274

3.3 Visible watermarking Algorithm

From above discussion, we have implemented the CSF based visible watermarking and found the direct application of CSF square function in [9] emphasizes more weights in the low DWT frequency domain. Subsequently, the watermark embedding in the low frequency components results high degradation of the image fidelity. In addition, this approach affects the quality of watermarked images and their PSNR values are often below 30dB for 512x512 color images. According to this observation, the concept of DWT noise detection threshold is adopted here to fine tune the perceptual weights by the basis function amplitudes $A_{\lambda,\theta}$ from [20]. Therefore, the perceptual weighting is modified as following:

$$\begin{cases} \beta_{\lambda,\theta} = \left[0.4 + \frac{(7.20 - r^\lambda)^2}{7.20^2} \right] \times A_{\lambda,\theta} & \text{if } \beta_{\lambda,\theta} > 0.2 \\ \beta_{\lambda,\theta} = 0.2 \end{cases} \quad (7)$$


Here, $\alpha_{\lambda,\theta}$ and $\beta_{\lambda,\theta}$ are scaling and embedding factors, λ as DWT Level, and θ as Orientation where γ^λ is the wavelet coefficient CSF of the perceptual importance weight, as Figure shown in Fig. 4. Fig. 6 shows $\beta_{\lambda,\theta}$ in different DWT level and orientation.

Meanwhile $\alpha_{\lambda,\theta}$ and $\beta_{\lambda,\theta}$ are the global characteristics of the host image, and they are independent to digital images.

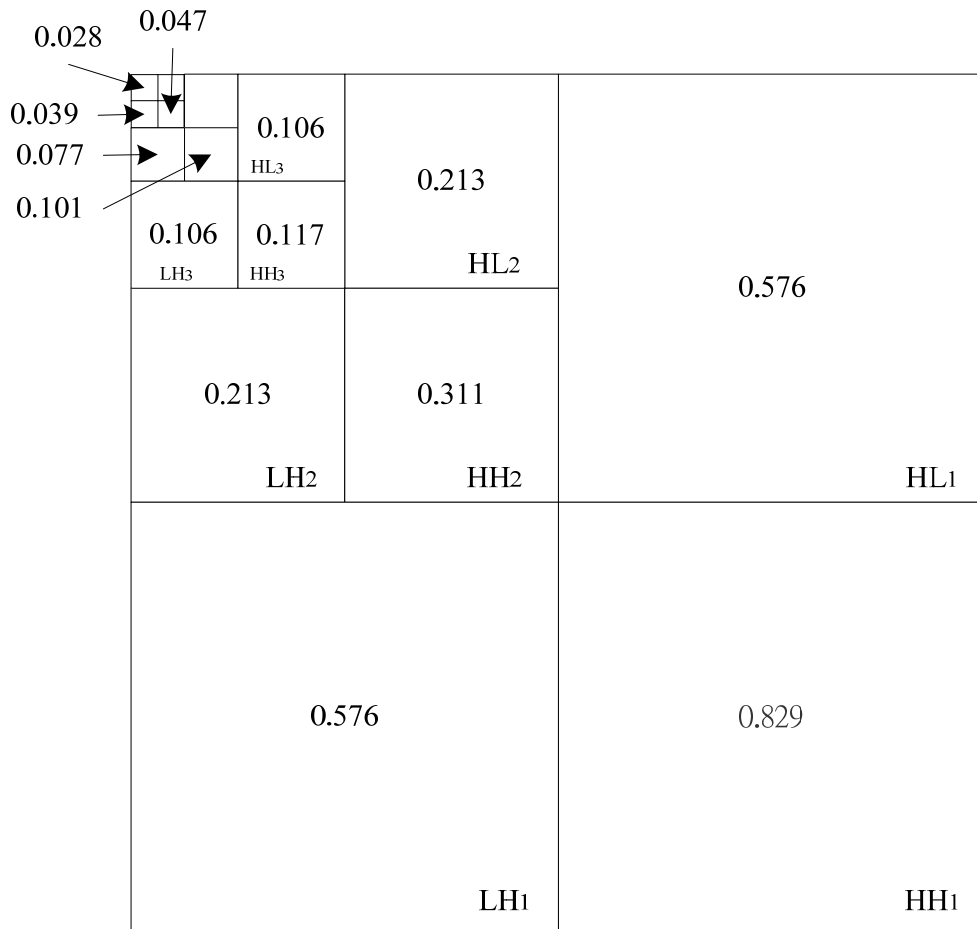


Fig. 6 $\beta_{\lambda,\theta}$ in different DWT level and orientation

To further improve the application of block classification by simply categorizing three type blocks in [9], the local characteristics in DWT domain is considered. In our content adaptive scheme, a stochastic image model for watermark embedding is adopted by using the NVF which characterizes the local image properties and identifies texture and edge regions. In our scheme, we have found the stationary GG model is the most appropriate approximation in the embedding stage and the estimated shape parameter for $\gamma = 0.65$ and width of window is 1. The complete design of the visible watermarking algorithm is summarized as following and the flow chart is shown in Fig. 7:

Visible Watermarking embedding algorithm:

- (1) The host color image is converted in the color space domain from RGB to YCrCb.
- (2) By using Bi9/7 filter from [20], compute the 5-level 2-D wavelet coefficients of Y component from host color image and grayscale watermark image. If the width of watermark is not the same as the one of the host image, it should be proportionally scaled to the host image.
- (3) Modify the DWT coefficients of the host image by using the following equation

$$Y_{i,j} = \alpha_{\lambda,\theta} \times X_{i,j} + (1 - NVF_{i,j}) \times S_{i,j} \times \beta_{\lambda,\theta} + NVF_{i,j} \times K \times S_{i,j} \quad (8)$$

Note: (i, j) indicates the spatial location. X and S are the decomposed wavelet coefficients of the host image and the watermark image. NVF is defined in formula (4) and the relationship of $\alpha_{\lambda,\theta}$ and $\beta_{\lambda,\theta}$ is defined in formula (7). The constant of k denotes the embedding watermark strength for flat regions and the value 0.08 is adopted for this algorithm.

- (4) Inverse transform the DWT coefficients of the host image to obtain a watermarked image (Y component).

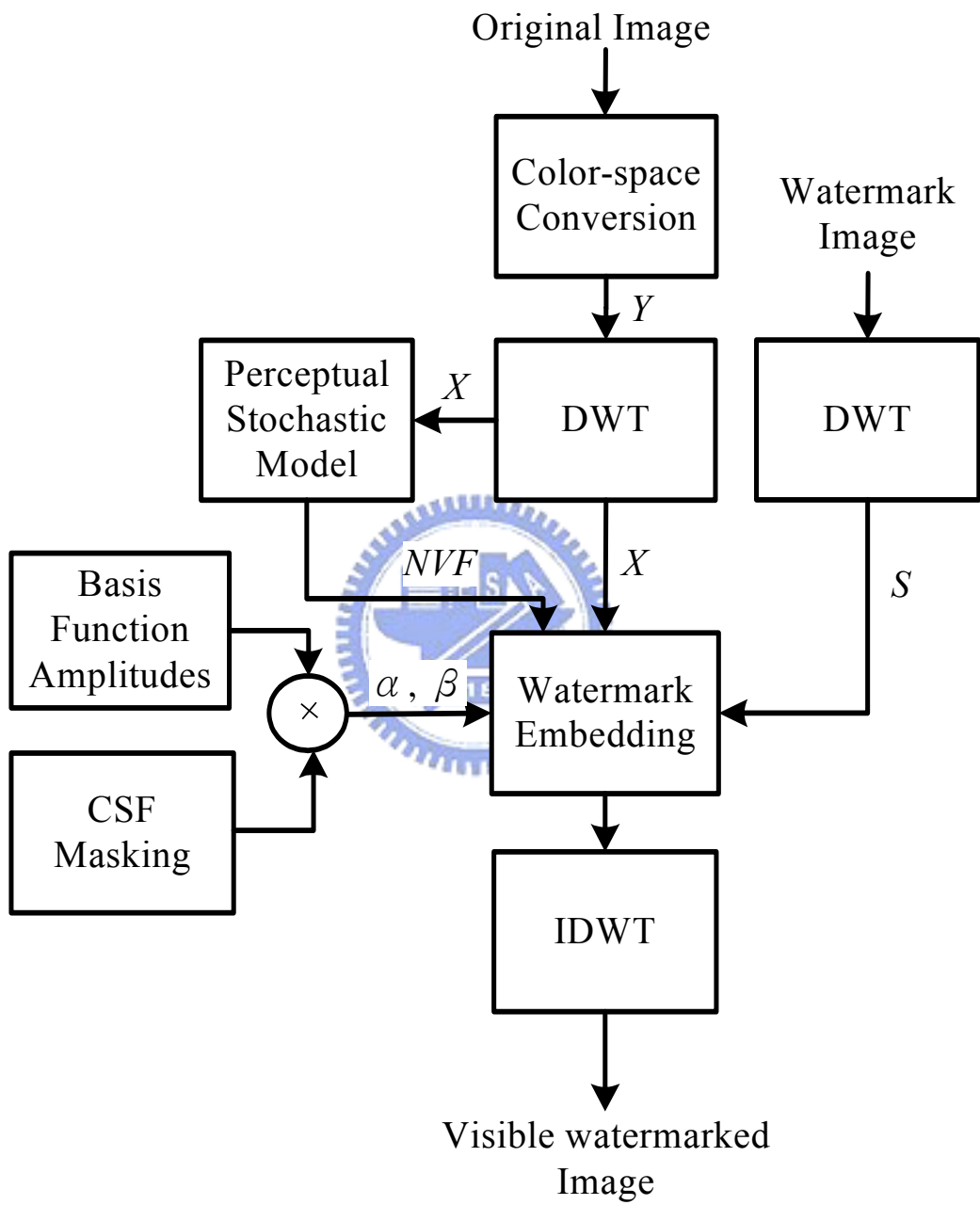


Fig. 7 The flow chart of the proposed visible watermarking approach

3.4 Image Authentication (Semi-Fragile watermark) Algorithm

It is difficult to develop a visible watermarking algorithm that can avoid the watermark to be destroyed maliciously by expensive human labors using any software, especially while the texture content of the host image is uncomplicated. In order to detect such kind of tampering and verify the integrity of the visible watermarked images, we modified the image authentication (semi-fragile watermark) algorithm from [31] into the proposed visible watermarked image as a dual watermarking scheme for our complete architecture.

Semi-Fragile Watermark Generation and Embedding Algorithm:

The flow chart of semi-fragile watermark embedding is shown in fig. 8. The semi-fragile watermark embedding procedure are as following:



- (1) Select parameters: K_1 and K_2 are the private keys of the scheme. q_1 and q_2 are the quantization parameters.
- (2) Select the Y (Luminance) component from 3.3 and compute the 2-level 2-D wavelet coefficients of it by using Bi18/10 filter, $r \times c$ is the size of LL_2 .
- (3) We refer to [35]'s chaotic system called toral automorphisms as chaotic map to get high security watermark. For general applying our algorithms, we also can use scrambling techniques like shuffle to get high security watermark and to solve the issue that the toral automorphisms only suits to square images by transforming two-dimensional matrix to one-dimensional matrix. Map $Q_{num} = \lfloor LL_2 / q_1 \rfloor$ and K_1 as controlling parameter. Using equation (9) (10), we obtain the binary watermark $W(i, j) \in \{0, 1\}, 1 \leq i \leq r \quad 1 \leq j \leq c$.

$$A_r(k_1): \begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ Q_{num} + k_1 & Q_{num} + k_1 + 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \pmod{r} \quad (9)$$

$$W(i, j) = (x' + y') \pmod{2} \quad (10)$$

(4) We use K_2 as random seed to create two-dimensional pseudo-random array $location(i, j) \in \{1, 2, 3\}, 1 \leq i \leq r \quad 1 \leq j \leq c$ to determine the watermark embedding location corresponding to $\{LH_2, HL_2, HH_2\}$.

(5) The binary watermark is embedded into the visible watermarked image by using simple odd-even quantization. We define odd-even quantization function in formula (11) (12) (13) (14) (15). The formula performs quantization on $X(i, j)$ into odd-even region according the binary watermark W . q_2 is the quantization parameter.

$$y(i, j) = f(x(i, j), W, q_2) \quad x \in R \quad W \in \{0, 1\} \quad q_2 \in Z^+ \quad (11)$$

Note: (i, j) indicates the spatial location. X is the decomposed wavelet coefficients of the visible watermarked image.

$$I = \begin{cases} 0 & \lfloor x(i, j) / q_2 \rfloor \text{ is even} \\ 1 & \lfloor x(i, j) / q_2 \rfloor \text{ is odd} \end{cases} \quad (12)$$

Note: $\lfloor \cdot \rfloor$ denotes the floor function.

$y(i, j)$ is obtained as follows:

$$y(i, j) = \begin{cases} \lfloor x(i, j) / q_2 \rfloor \times q_2 + q_2 / 2 + x_r & \text{if } I = W \\ y' + x_r & \text{if } I \neq W \end{cases} \quad (13)$$

$$y' = \begin{cases} \lfloor x(i,j)/q_2 - 1 \rfloor \times q_2 + q_2/2 & \text{if} \\ x \in [\lfloor x(i,j)/q_2 \rfloor \times q_2, \lfloor x(i,j)/q_2 \rfloor \times q_2 + q_2/2] \\ \lfloor x(i,j)/q_2 + 1 \rfloor \times q_2 + q_2/2 & \text{if} \\ x \in [\lfloor x(i,j)/q_2 \rfloor \times q_2 + q_2/2, \lfloor x(i,j)/q_2 \rfloor \times q_2 + q_2] \end{cases} \quad (14)$$

$$x_r = \text{sgn}(x(i,j))(|x(i,j)| \bmod 2) \quad (15)$$

(6) Perform quantization on wavelet coefficients as follows pseudo code:

```

For i = 1 to r
  For j = 1 to c
    SWITCH location(i, j)
    CASE 1: HL2(i, j) = f(HL2(i, j), W(i, j), q2)
    CASE 2: LH2(i, j) = f(LH2(i, j), W(i, j), q2)
    CASE 3: HH2(i, j) = f(HH2(i, j), W(i, j), q2)

```

(7) Inverse transform the DWT coefficients of the Y component. The Y component with visible and semi-fragile watermark is converted in the color space domain from YCrCb to RGB.

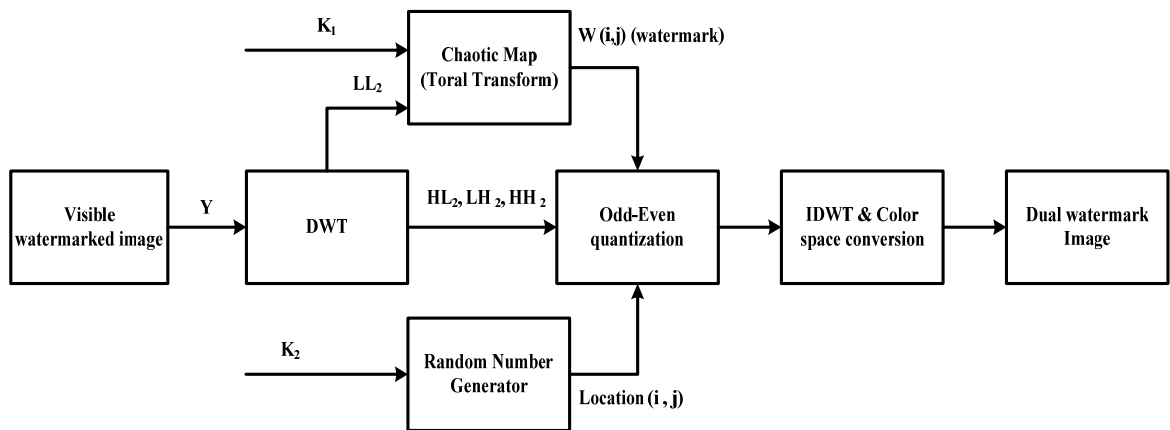


Fig. 8 The flow chart of the proposed semi-fragile watermark approach

Semi-Fragile watermark Authentication and Tamper Detection algorithm:

The Fig. 9 shows the flow chart of watermark detection scheme, which is similar to the part of semi-fragile watermark embedding. The tamper detection procedure as follows:

- (1) Select parameters: K_1 and K_2 are the private keys of the scheme. q_1 and q_2 are the quantization parameters. The value of K_1 , K_2 , q_1 and q_2 are the same in embedding and extraction processes.
- (2) The obtained visible watermarked image is converted in the color space domain from RGB to YCrCb.
- (3) Select the Y (Luminance) component and compute the 2-level 2-D wavelet coefficients of it, $r \times c$ is the size of LL_2 .
- (4) Use K_1 and K_2 to create two-dimensional pseudo-random arrays;
 $W'(i,j) \in \{0,1\}, 1 \leq i \leq r, 1 \leq j \leq c$ and $location(i,j) \in \{1,2,3\}, 1 \leq i \leq r, 1 \leq j \leq c$.
- (5) According to the $location(i,j)$, we find the sub-band and the quantized coefficient, defined as $u(i,j)$. The extract watermark may be obtained by the following formula (16):

$$W''(i,j) = (\lfloor (u(i,j) / q_2) \rfloor) \bmod 2 \quad (16)$$

- (6) Having obtained two watermarks W' and W'' , we define the tamper detection matrix as formula (17), If $W' = W''$, then $T=0$. It means the visible watermarked image was not tampered. Otherwise, the '1' element in the tamper detection matrix indicates the pixels that were tampered.

$$T = |W' - W''| \quad (17)$$

- (7) Since the algorithm is designed to be semi-fragile watermarking scheme which would want to be robust to mild modifications in all cases, it is inevitable that we can't detect all malicious attack in pixel-wise. However, for practical cases such as removal visible

watermark using neighbor pixels and image cropping which crops objects from a source and pastes them onto a target, the malicious attacks always be applied in a certain region in the watermarked image. That is to say, we assume tamper pixels are always continues. Therefore, for a certain tamper detection matrix element $T(i, j)$, if the number of tampered neighboring element for $T(i, j)$ is greater than a given threshold, we regard $T(i, j)$ as a tampered one. The summary of such post-processing operation of tamper detection matrix is shown as following formula (18):

$$T' = \begin{cases} 1 & , \quad \sum_{k=-L}^L \sum_{l=-L}^L T(i+k, j+l) > \beta \\ 0 & , \quad \sum_{k=-L}^L \sum_{l=-L}^L T(i+k, j+l) \leq \beta \end{cases} \quad (18)$$

Note: L as width of window, β as threshold.

- (8) According to the DWT decomposition of the watermarked image, the size of tamper detection matrix is $r \times c$, which is about $1/16$ of the watermarked image. Thus one element in the matrix indicates a corresponding 4×4 block in the watermarking image. Finally, we rescale the tamper detection matrix to have the same size of the watermarked image and obtain the tamper detection image.

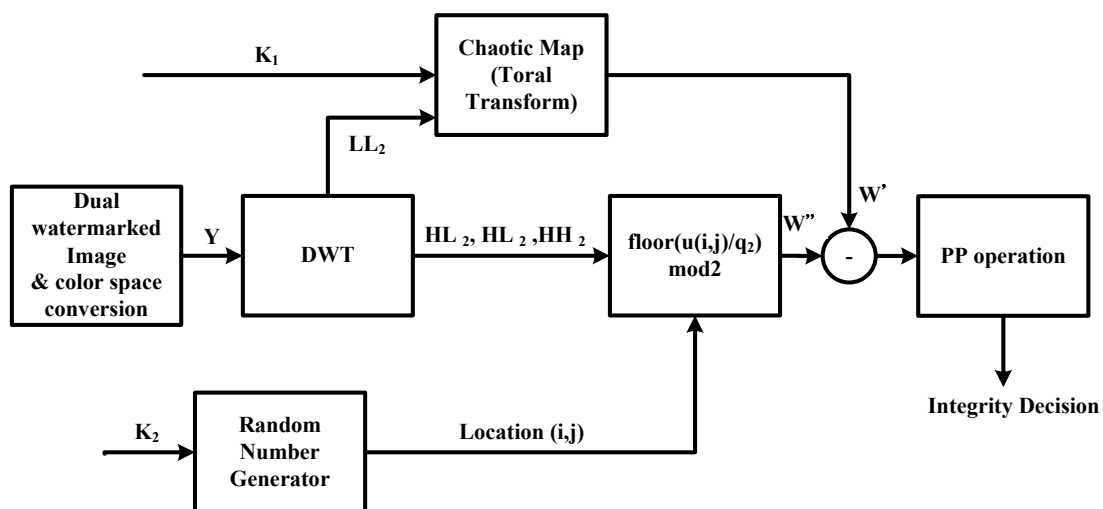


Fig. 9 The flow chart of authentication and tamper detection algorithm approach

IV. Experimental Results and Discussion

The proposed visible and semi-fragile watermarking algorithm has been implemented and intensively tested by using the commonly available color images from USC image database [36]. Because the evaluation standards for visible watermarking system are absent, we would compare our algorithm with previously proposed ones. To make the fair comparison with other visible watermarking considering HVS, the simulation of [9] is highly addressed here instead of the approaches from [4, 10-17]. Since the CSF based visible watermark technique from [9] has shown better performance than the methods from [16] and AiS Watermark Pictures Protector [37], we compared the results by [9] with the proposed approach and the performance of 512×512 colors images. In the Huang and Tang's method [9], they didn't describe the value of two thresholds used to classify the blocks of each subband, so we will implement their method by assuming the $T1=1$ and $T2=350$ to strong the energy of the watermark.

Two grayscale watermarks of logo image are embedded for illustration in Fig. 10 (a) NCTU LOGO (school logo) and Fig. 10 (b) IIM logo (department logo). The performance of 512x512 experimental images is tabulated in Fig. 11~18 for comparison purpose. Fig. 11~18 (a) show the original host images, these test images are named "Lena", "Baboon", "Lake", "Peppers". Fig. 11~18 (b) the results of the method in Huang and Tang's watermarking algorithm from [9] are compared with the proposed approach and the results are in Fig. 11~18 (c). The performance analysis can be categorized as following:

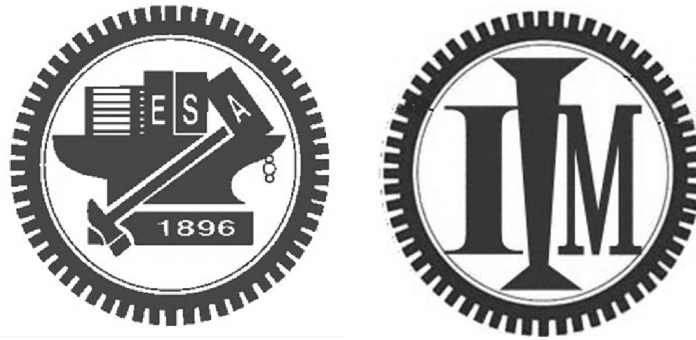


Fig. 10 Two watermark images : (a) NCTU logo (b) IIM logo



Fig. 11 (a) original Lena image (b) watermarked Lena image by the method in Huang and Tang (c) watermarked Lena image by the proposed algorithm



Fig. 12 (a) original Lena image (b) watermarked Lena image by the method in Huang and Tang (c) watermarked Lena image by the proposed algorithm

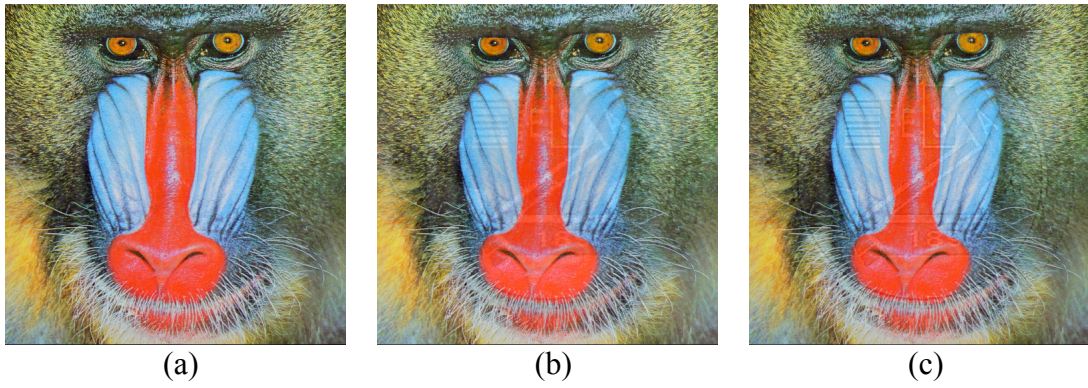


Fig. 13 (a) original Baboon image (b) watermarked Baboon image by the method in Huang and Tang (c) watermarked Baboon image by the proposed algorithm

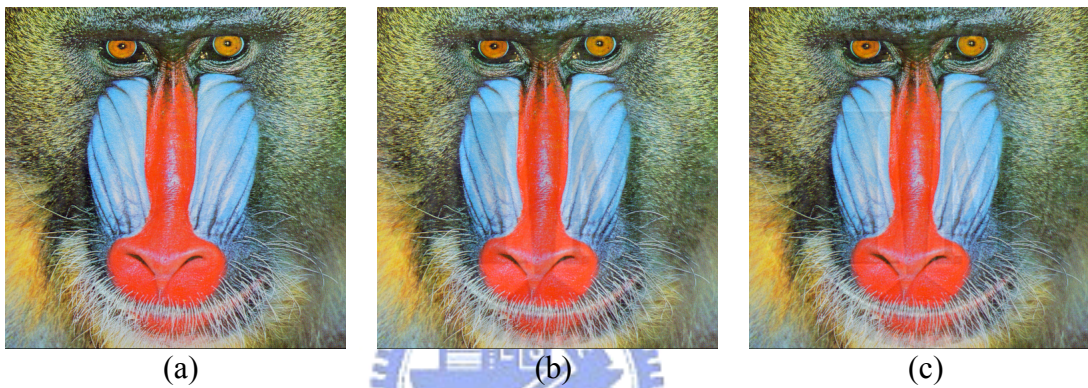


Fig. 14 (a) original Baboon image (b) watermarked Baboon image by the method in Huang and Tang (c) watermarked Baboon image by the proposed algorithm



Fig. 15 (a) original Lake image (b) watermarked Lake image by the method in Huang and Tang (c) watermarked Lake image by the proposed algorithm

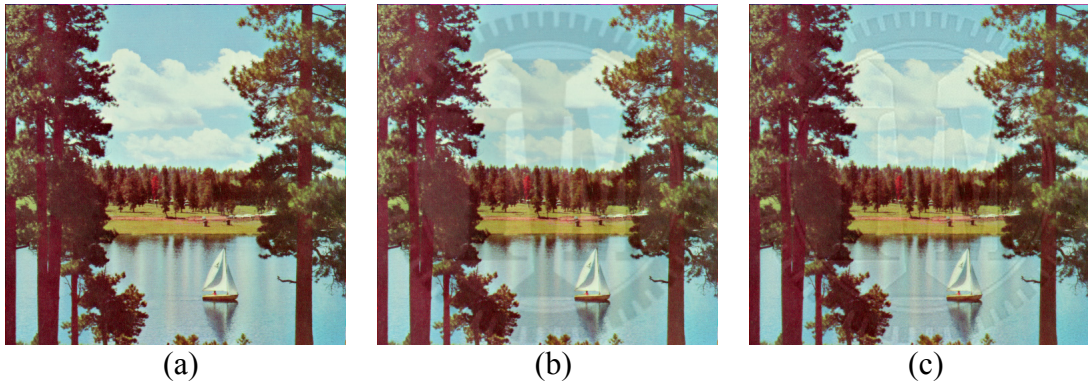


Fig. 16 (a) original Lake image (b) watermarked Lake image by the method in Huang and Tang (c) watermarked Lake image by the proposed algorithm

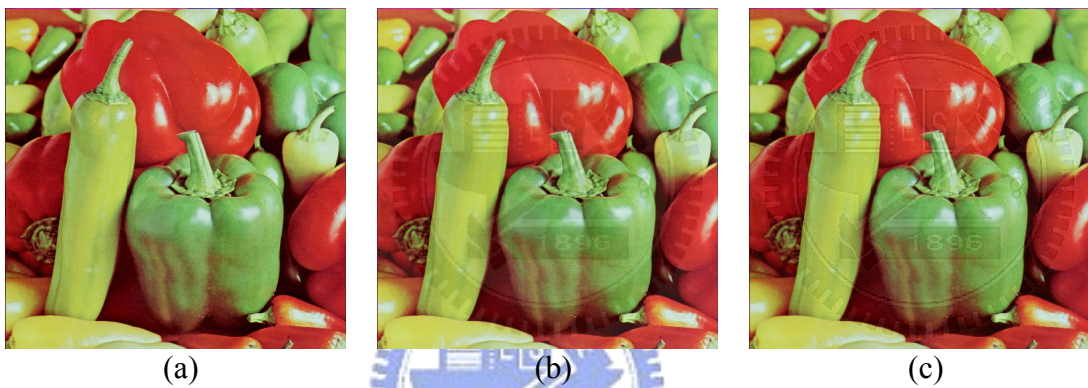


Fig. 17 (a) original Peppers image (b) watermarked Peppers image by the method in Huang and Tang (c) watermarked Peppers image by the proposed algorithm

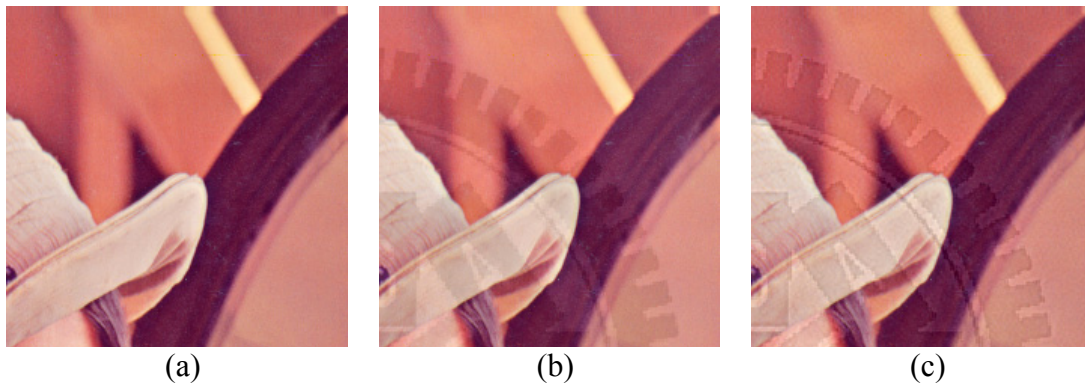


Fig. 18 (a) original Peppers image (b) watermarked Peppers image by the method in Huang and Tang (c) watermarked Peppers image by the proposed algorithm

4.1 Visual Effect

From Fig. 11 (b) (c) 、 Fig. 15 (b) (c) and Fig. 17 (b) (c), the proposed method has the closest luminance and chrominance maintenance compared with the original ones which are shown clearly from the photos even the difference is sometimes identified subjectively. The watermarked images by using [9] have more bright effect in the unmarked areas. On the other hand, translucence effect is one of requirements for an effective visible watermarking algorithm. The results from our proposed method have better translucence effect than Huang and Tang's method to make photos look more natural, because the watermarked images by using [9] affect the details of the host (original) image more, especially in Fig. 15 (b) (c) and Fig. 16 (b) (c).

To further compare the details from the watermarked images, Fig. 19 demonstrates some of close-ups for comparison. Fig 19 (a) are the close-ups from original image. Fig 19 (b) are the close-ups from the watermarked images by using [9]'s method. Fig 19 (c) are the close-ups from the watermarked images by using our proposed scheme. It is very clear that the watermark's edges and thin lines are blurred in Huang and Tang's method contrast to our results. However, the watermark patterns in our proposed method still have sharp edge and the logo watermark is evidently embedded. For the text pattern, the text of character *A* in our results is with sharper edge than the same character in results from Huang and Tang's method. In addition, the outlines in our results are clearer than those from Huang and Tang's method.



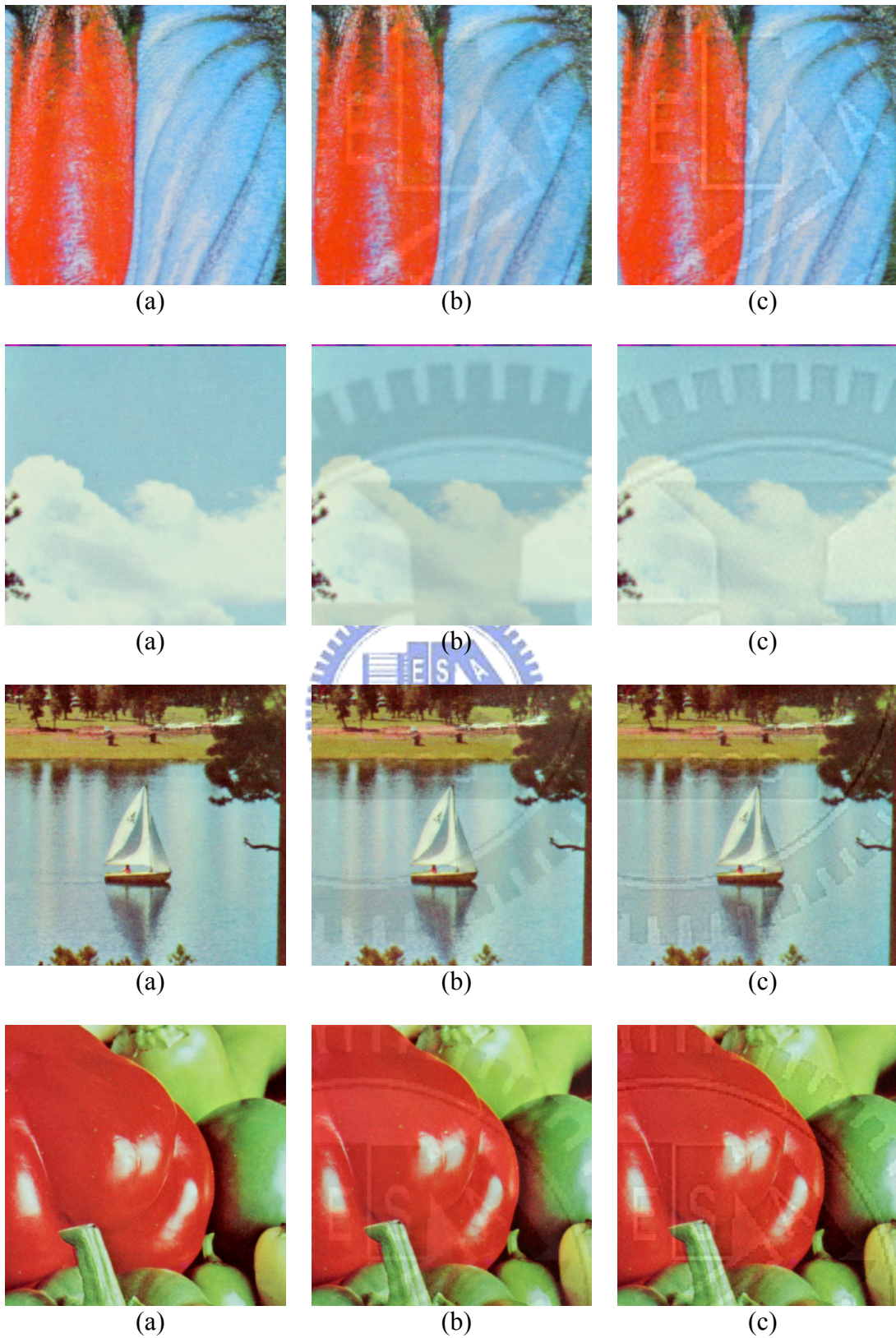


Fig. 19 The visual comparison of close-ups for images to figure 11 through 18 (a) close-ups of the original images (b) close-ups of the watermarked images by the method in Huang and Tang (c) close-ups of the watermarked images by the proposed algorithm

4.2 PSNR (Peak Signal-Noise Ratios)

To make a fair comparison with the method from [9], it is better to embed the same watermark for the same cover image. However, the watermark used in [9] is not available. We then embed two logo watermarks from Fig.10 to make the best effort for performance comparison. The tabulated results from TABLE 2 disclose that our watermarking scheme are with better statistical results and achieve higher PSNR values than the method in [9] where the PSNRs are generally below 30dB for different images. The low PSNRs have positive correlation with the degradation in image quality. This denotes the fidelity of images from our method is better than the Huang and Tang's method. In addition, the PSNR values of dual watermarked images are only 0.2~0.4 less than those of visible watermark only images. This means that our proposed multipurpose design could achieve as good as high image quality of visible watermarking but also with extra function of invisible watermarks.

Table 2 PSNR summary of watermarked color images

Image	Watermark	Huang and Tang's method 【T1=1, T2=350】	Proposed Approach	
			Visible watermark only	Dual watermarks
Lena	NCTU Logo	27.0 dB	31.5 dB	31.2 dB
Lena	IIM Logo	26.8 dB	32.7 dB	32.3 dB
Baboon	NCTU Logo	27.1 dB	30.2 db	29.9 dB
Baboon	IIM Logo	27.2 dB	31.0 dB	30.7 dB
lake	NCTU Logo	26.2 dB	30.7 dB	30.5 dB
lake	IIM Logo	26.1 dB	31.7 dB	31.3 dB
Peppers	NCTU Logo	26.9 dB	31.4 dB	31.1 dB
Peppers	IIM Logo	26.9 dB	32.5 dB	32.1 dB

4.3 JPEG 2000 Compression

We use StirMark software to test the robustness of the visible watermark and analyze the attacking results. We can clearly find the attacks from jpeg compression and median filter have ability to affect the structure of the visible watermark. In inverse, others attacks like rotation & noise are not able to influence the visible watermark. From above observations, we will list the results form jpeg compression and median filter as follows.

The robustness of the proposed dual watermark technique should be tested for comparison. For JPEG 2000 compression, software from [38] is adopted as the compression tool. The PSNR values before and after the jpeg 2000 compression are tabulated in TABLE 3. The compression ratio is 100:3 between the uncompressed image and compressed image. There are two columns of PSNR values for both methods labeled “after”. The pure “after” column means those PSNR values are compared between the compressed watermarked image and the original image. The after (wn) column means those PSNR values are compared between the compressed watermarked image and the watermarked image. From TABLE 3, we can find that the PSNR values are almost the same for both methods while the compressed watermarked images are compared with the watermarked images (after (wn) column). However, the PSNR values are higher while the compressed watermarked images are compared with the original images by the proposed approach than by the method of [9] (after column). Therefore, this statistic indicates that the image quality of watermarked image before and after compressed is higher by the proposed approach than the method of [9]. To further investigate the effect of compression, the visual difference can be illustrated by the close-up comparison. Fig. 20(a) show the close-ups of original images. From compression ratio of 100:3, Fig. 20(b) are the close-ups of watermarked images by Huang and Tang’s method. Fig. 20(c) are the close-ups of watermarked images by our proposed method. By comparing Fig. 30, the compressed images maintain the details of the logo pattern but the

characters E, S, A of watermarked images by our proposed method are more apparent than one of watermarked images by Huang and Tang's method. In addition, the stripes of logo pattern of watermarked baboon image are almost disappearing in Huang and Tang's method but still existing in our proposed method. This observation is consistent with the claim of our discussion in section II that the embedding factors in [9] emphasize more weights in the low frequency domain instead of the medium-to-high frequency domain while the high frequency components of the watermarked image easily suffer common image signal processing attacks like compression. Therefore, we can indicate that our proposed method is more robust than Huang and Tang's method by jpeg 2000 compression attack from above observation where the visibility of watermark is surely higher by the proposed approach.

Table 3 PSNR summary of watermarked color images before and after JPEG 2000

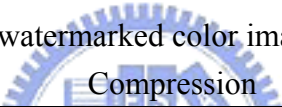


Image	Watermark	PSNR value (dB)					
		Method of [9]			Proposed method		
		Before	After	After (wn)	Before	After	After (wn)
Lena	NCTU	27.0	26.0	34.5	31.2	29.2	33.8
Lena	IIM	26.8	25.9	34.7	32.3	29.7	34.4
Baboon	NCTU	27.1	23.0	26.1	29.9	24.1	26.5
Baboon	IIM	27.2	23.0	26.1	30.7	24.2	26.6
lake	NCTU	26.2	24.2	30.2	30.5	26.9	30.1
lake	IIM	26.1	24.2	30.3	31.3	27.2	30.5
Peppers	NCTU	26.9	22.7	27.4	31.1	24.8	26.8
Peppers	IIM	26.9	22.8	27.3	32.1	25.1	26.9

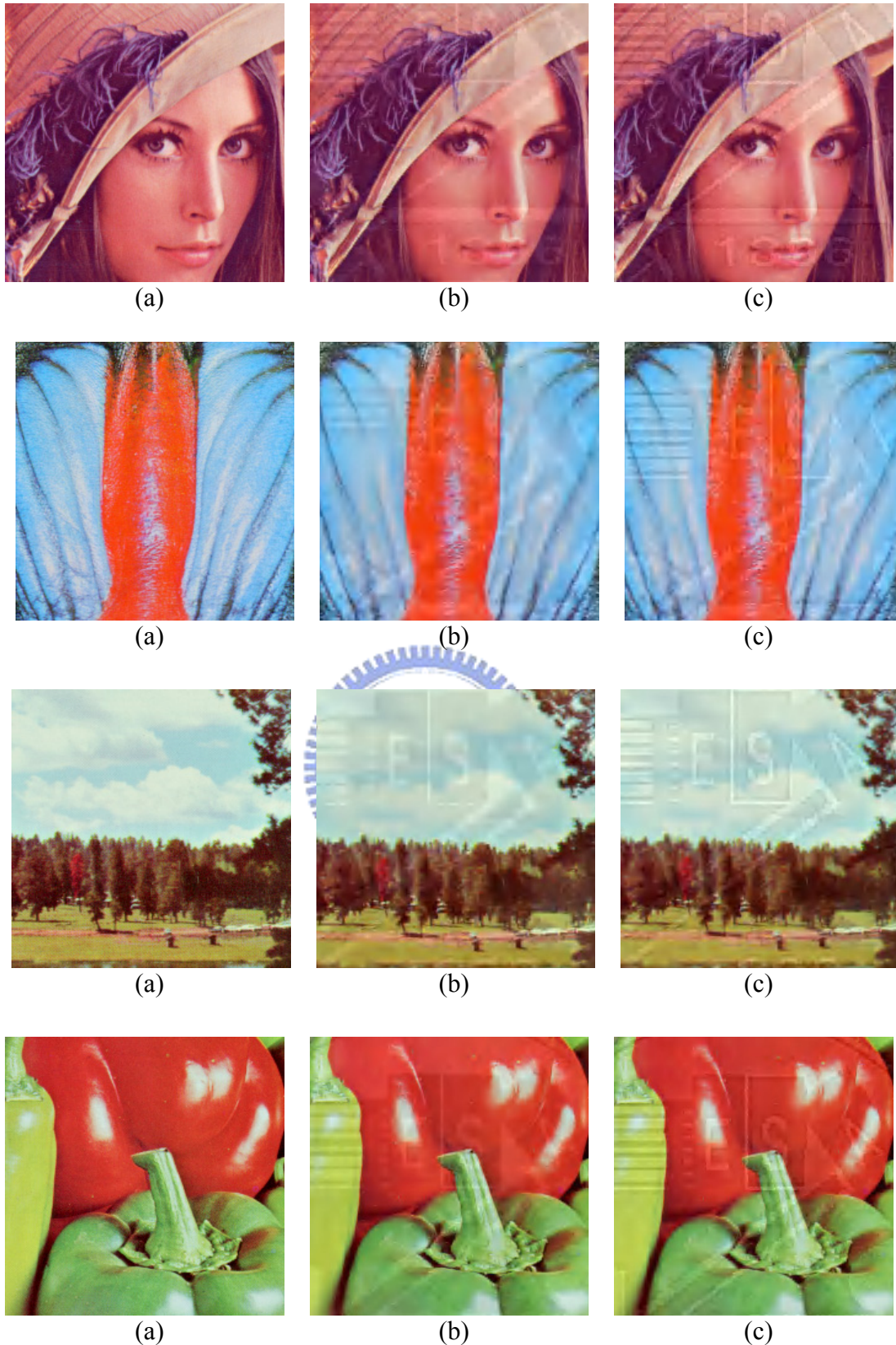


Fig. 20 The visual quality comparison of close-ups of watermarked image after jpeg 2000 compression ratio of 100:3 (a) original image (b) watermarked images by the Huang and Tang's method (c) watermarked image by the proposed algorithm

4.4 Median Filter

The robustness of Median filtering attack is also tested here and StirMark [39] software is adopted here for this attack. Since the results of 3×3 and 5×5 median filtering are similar to the illustration as shown in Fig. 11 ~ Fig. 18, a stronger attack as 7×7 median filtering is applied here for the comparison. The PSNR values before and after the median filtering are tabulated in TABLE 4. There are two columns of PSNR values for both methods labeled “after” and their meaning is the same as mentioned in the session of jpeg 2000 compression. From TABLE 4, we can find that the PSNR values are almost the same for both methods while the filtered watermarked images are compared with the watermarked images (after (wn) column). However, the PSNR values are higher while the filtered watermarked images are compared with the original images by the proposed approach than by the method of [9] (after column). Therefore, this statistic indicates that the image quality of watermarked image before and after filtered is higher by the proposed approach than the method of [9]. To further investigate the effect of median filtering, the visual difference can be illustrated by the close-up comparison. Fig. 21(a) are close-ups of original images. Fig. 21(b) are close-ups of 7×7 median filtering of watermarked image by the Huang and Tang’s method. Fig. 21(c) are close-ups of 7×7 median filtering of watermarked image by the proposed method. By comparing Fig. 21(b)-(c), the median filtered images became blurry but Fig. 21(c) has sharper contour than Fig. 21(b). It is apparent that the logo pattern (i.e. the characters of E, S, A, or the characters of 1896) is still evidently existed in Fig. 21(c) but is blurred and hard to be recognized in Fig. 21(b). Therefore, the proposed technique outperforms [9] by the median filtering attack from above observation where the visibility of watermark is surely higher by the proposed approach. Other attacks from [38] are also preformed and the experimental results are consistent with the above findings which indicate our visible watermarking scheme has better visual effect and high PSNR values than other schemes like [9]. In summary, an intensive comparison for

proposed technique has been illustrated above. Different attack and visual quality comparison is also illustrated. Therefore, we can conclude that the proposed method is more robust with better image quality than the algorithm in [9].

Table 4 PSNR summary of watermarked color images before and after Median Filter

Image	Watermark	PSNR value (dB)					
		Method of [9]			Proposed method		
		Before	After	After (wn)	Before	After	After (wn)
Lena	NCTU	27.0	21.2	24.7	31.2	23.1	24.4
Lena	IIM	26.8	21.3	24.7	32.3	23.2	24.7
Baboon	NCTU	27.1	17.7	19.4	29.9	18.5	19.9
Baboon	IIM	27.2	17.8	19.4	30.7	18.5	19.9
lake	NCTU	26.2	19.3	21.8	30.5	20.7	21.9
lake	IIM	26.1	19.4	21.9	31.3	20.8	22.1
Peppers	NCTU	26.9	18.4	20.8	31.1	19.8	20.6
Peppers	IIM	26.9	18.6	20.8	32.1	19.9	20.7

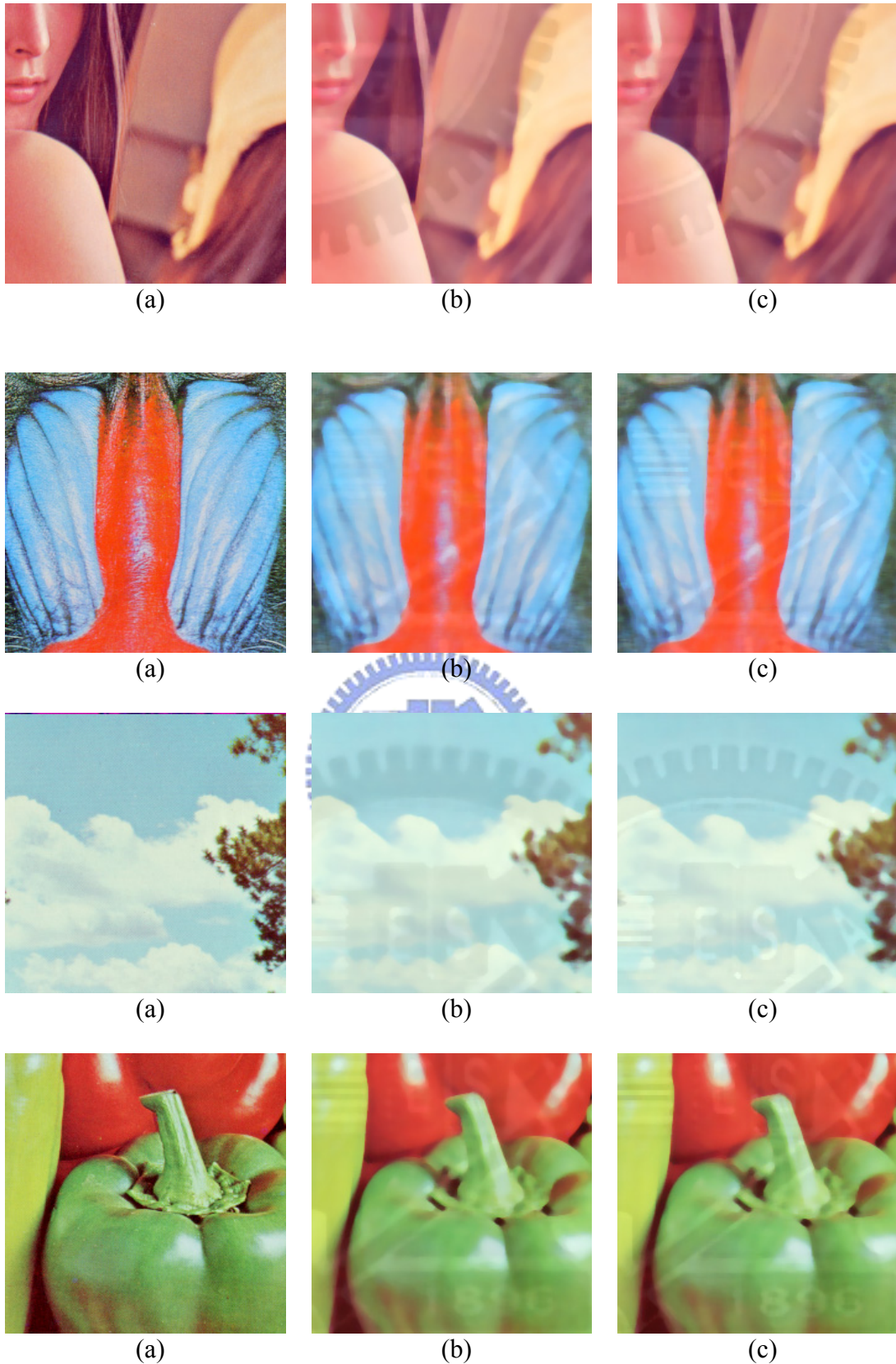


Fig. 21 The visual quality comparison of close-ups of 7x7 median filtering of watermarked image (a) original image (b) watermarked images by the Huang and Tang's method (c) watermarked image by the proposed algorithm

4.5 ICA (Independent component analysis) Image recovery Attack

Since the visible watermark is embedded with the images, it is not unusual that attacks would try any means to remove the watermark so they can use the images freely without any copyright concern. If the contour of an embedded visible watermark is completely removed or greatly distorted without introducing serious visual quality degradation, it is difficult for the content owner to claim the infringement by the illegal users. Even this situation existing, a good visible watermark scheme becomes the barrier for the attacks since expensive human labors are needed in order to remove the watermark itself.

Regarding the removal technique, the image recovery method [40] can remove visible watermarking patterns consisting of thin lines and a few human interventions of image-inpainting approach of [41] can deal with patterns of thick lines. However, the iterative process of image-inpainting is costly and time-consuming. Pei and Zeng [42] proposed another image recovery algorithm for removing visible watermarks which is simple, fast with less human intervention. The method mainly utilized independent component analysis (ICA), i.e. joint approximate diagonalization of eigenmatrices (JADE), second-order blind identification (SOBI), and FastICA to separate host images from watermarked and reference images. The algorithm included three phases: watermarked area segmentation, reference image generation, and image recovery. In their experiments, five different visible watermarking methods [4, 10-12, 13, 15] and three public domain images are tested. The experimental results showed that their algorithm can successfully removed the visible watermarks, and the algorithm itself is independent of both the adopted ICA approach and the visible watermarking method. Interested readers can refer [42] for detailed information.

In this paper, we propose a novel visible watermarking scheme and are also curious about the performance against the watermark removal attacks. Therefore, we have implemented the method of [42] and tested several public images used in [42] for comparison. Fig. 22 illustrates the recovered images of our implementation for images from [43, 44] and the results are consistent with the finding from [42] where the watermarks were completely removed. By applying the method of [42] to our proposed visible watermarking approach, Fig 33-35 illustrates the results of the watermark removal attack where the logo patterns slightly disappear but still exist and the contours are recognizable in Fig. 23 (b)(d), Fig. 24 (b)(d), Fig. 25 (b)(d), Fig. 26 (b)(d). Besides, the watermark removal scheme in [42] can remove the watermark by the method in [4, 10-12, 13, 15] but the proposed approach can resist such attack. We can conclude that the proposed visible scheme certainly outperforms the method in [4, 10-12, 13, 15].

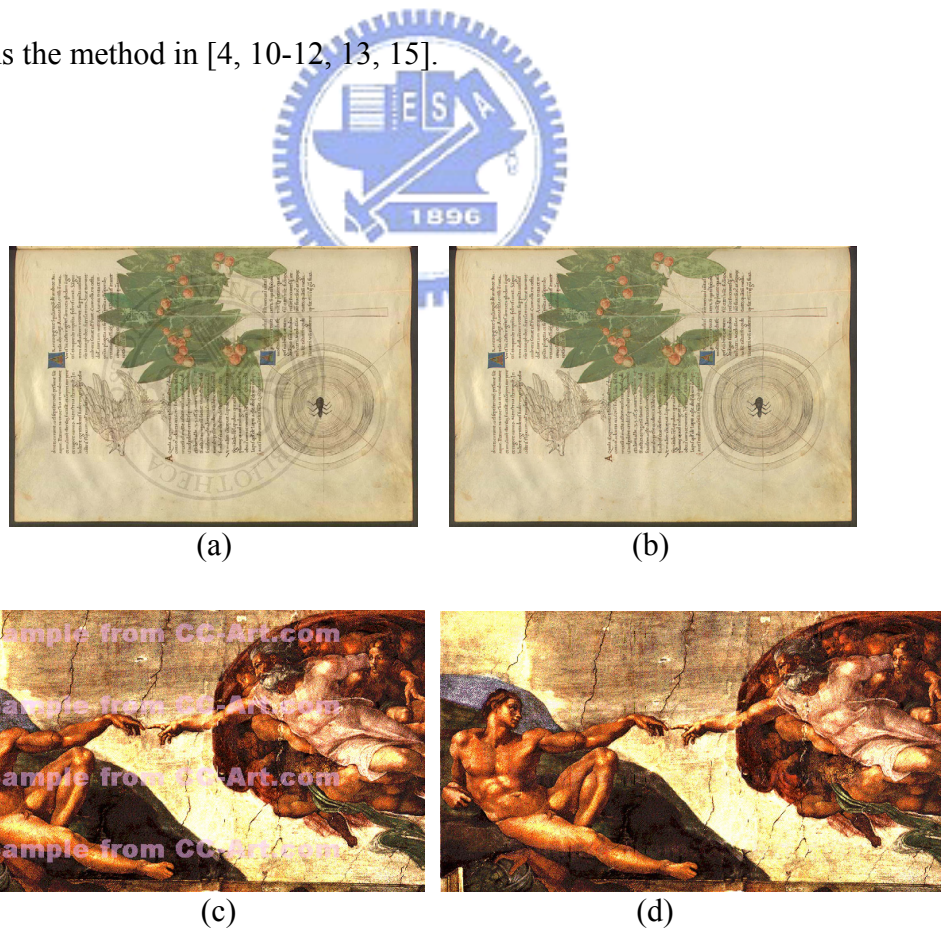


Fig. 22 Recovering the public domain image (a) watermarked image (b) recovered image (c) watermarked image (d) recovered image



Fig. 23 Recovering the watermarked images from our method (a) watermarked image with NCTU logo (b) recovered image from watermarked image with NCTU logo (c) watermarked image with IIM logo (d) recovered image from watermarked image with IIM logo

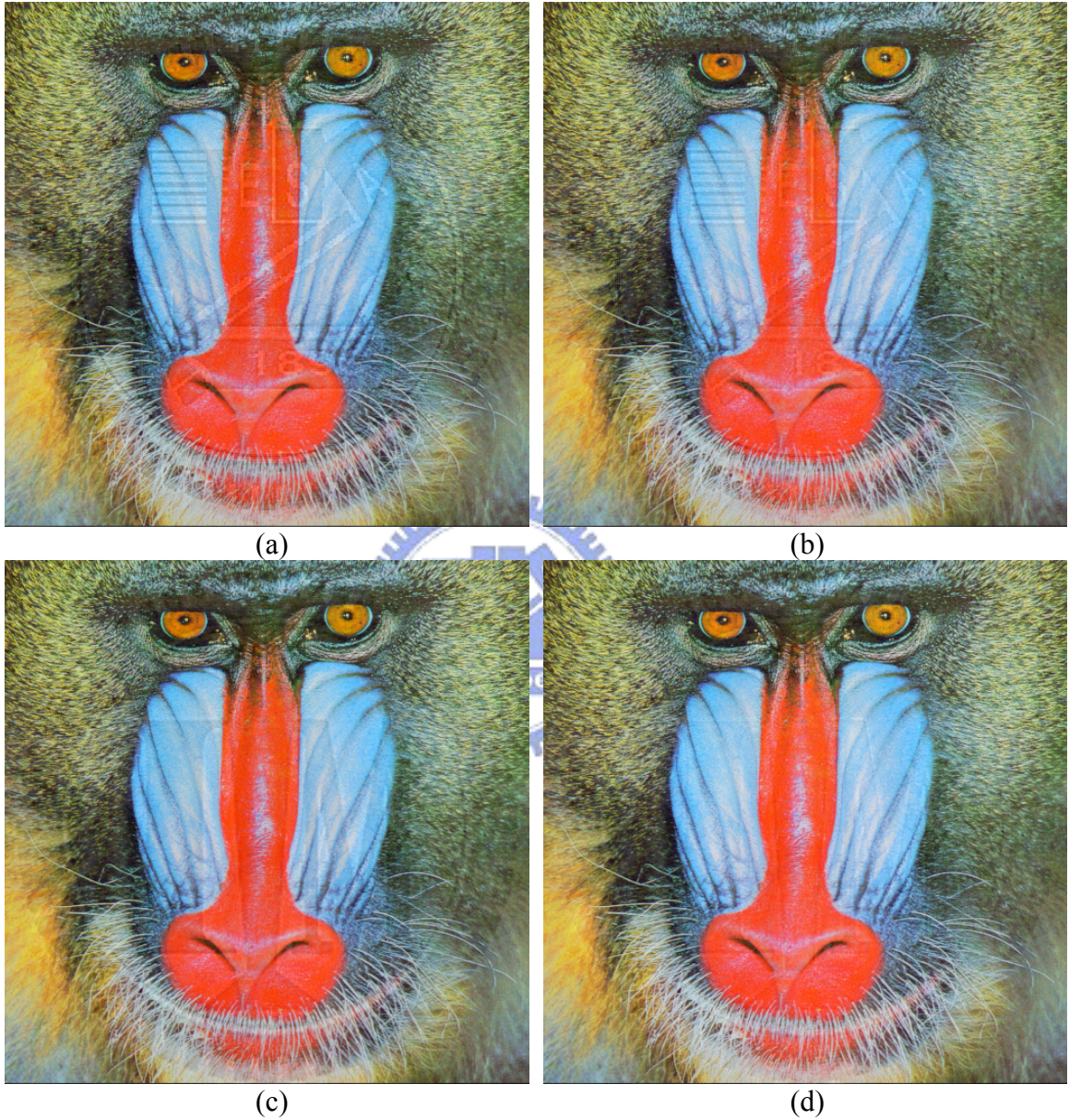


Fig. 24 Recovering the watermarked images from our method (a) watermarked image with NCTU logo (b) recovered image from watermarked image with NCTU logo (c) watermarked image with IIM logo (d) recovered image from watermarked image with IIM logo

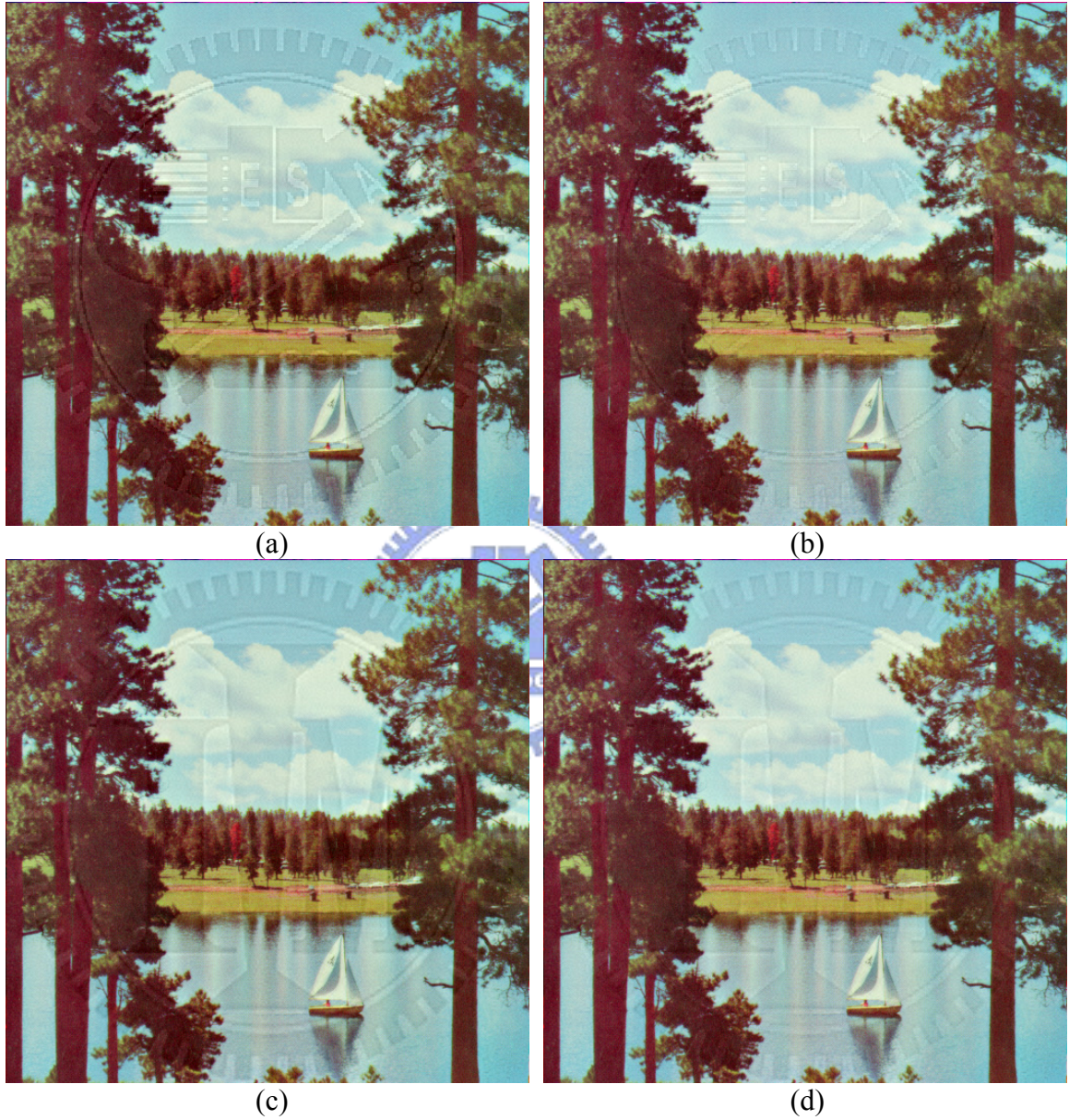


Fig. 25 Recovering the watermarked images from our method (a) watermarked image with NCTU logo (b) recovered image from watermarked image with NCTU logo (c) watermarked image with IIM logo (d) recovered image from watermarked image with IIM logo



Fig. 26 Recovering the watermarked images from our method (a) watermarked image with NCTU logo (b) recovered image from watermarked image with NCTU logo (c) watermarked image with IIM logo (d) recovered image from watermarked image with IIM logo

4.6 Tamper Detection

To evaluate the validity of the proposed image authentication algorithm and make up tampered images, we use Adobe Photoshop CS2 for implement of image processing operations. In our experiments, we let parameters $q_1=30$, $q_2=10$, $K_1=1234$, $K_2=1234$, $L=1$, $\beta=3$. Fig. 27~30 (a), (b), and (c) demonstrate the dual watermarked images (visible and semi-fragile watermark embedded), tampered images, and tampering detection images respectively. In Fig. 27 (b), one object (A .com logo) is inserted into the dual watermarked Lena image. In the shoulder part of the Lena image, we use neighboring pixels to remove the visible watermark. In Fig. 28 (b), one object (A .com logo) is inserted into the dual watermarked Baboon image. In the top right part of the watermark (logo) image, we use neighboring pixels to remove the visible watermark. In Fig. 29 (b), two objects (A .com logo and boat) are inserted into the dual watermarked Lake image. In the top part of the watermark (logo) image, we use neighboring pixels to remove the visible watermark. In Fig. 30 (b), three object (A .com logo and two Peppers) are inserted into the dual watermarked Peppers image. From the detection result of tampered images, the marked points indicate the tampered parts of watermarked image and these parts are located correctly.

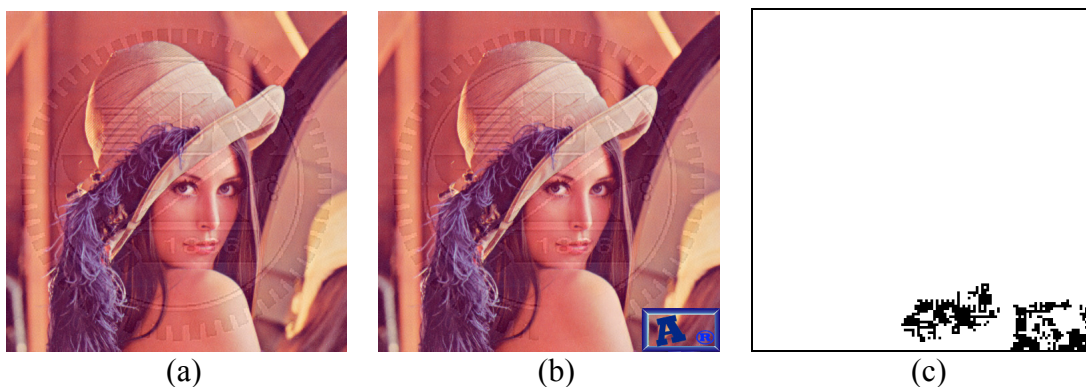


Fig. 27 (a) Result (watermarked) image (b) Tampered image (c) Tampering detection

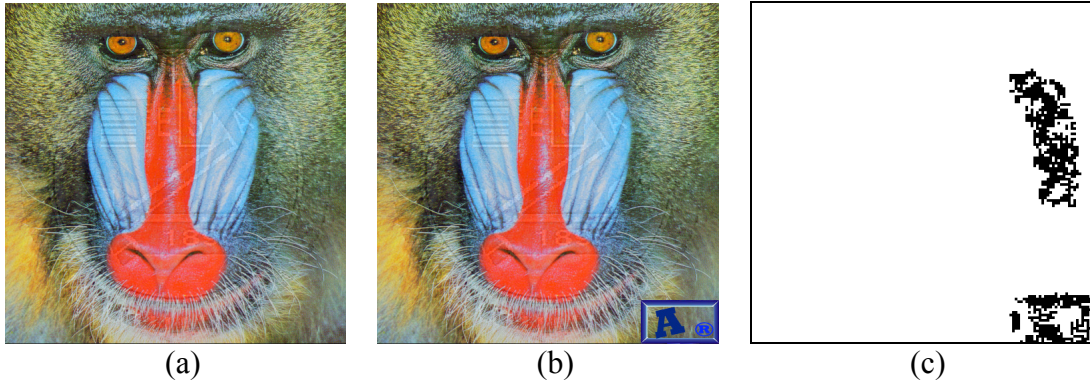


Fig. 28 (a) Result (watermarked) image (b) Tampered image (c) Tampering detection

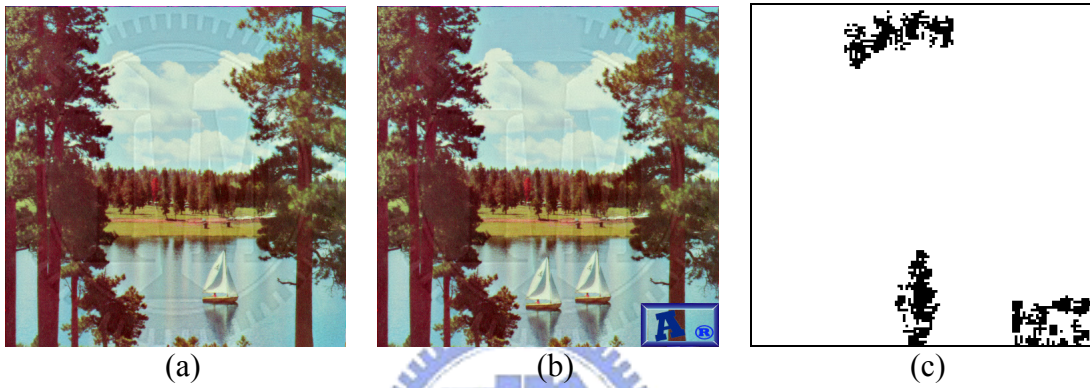


Fig. 29 (a) Result (watermarked) image (b) Tampered image (c) Tampering detection



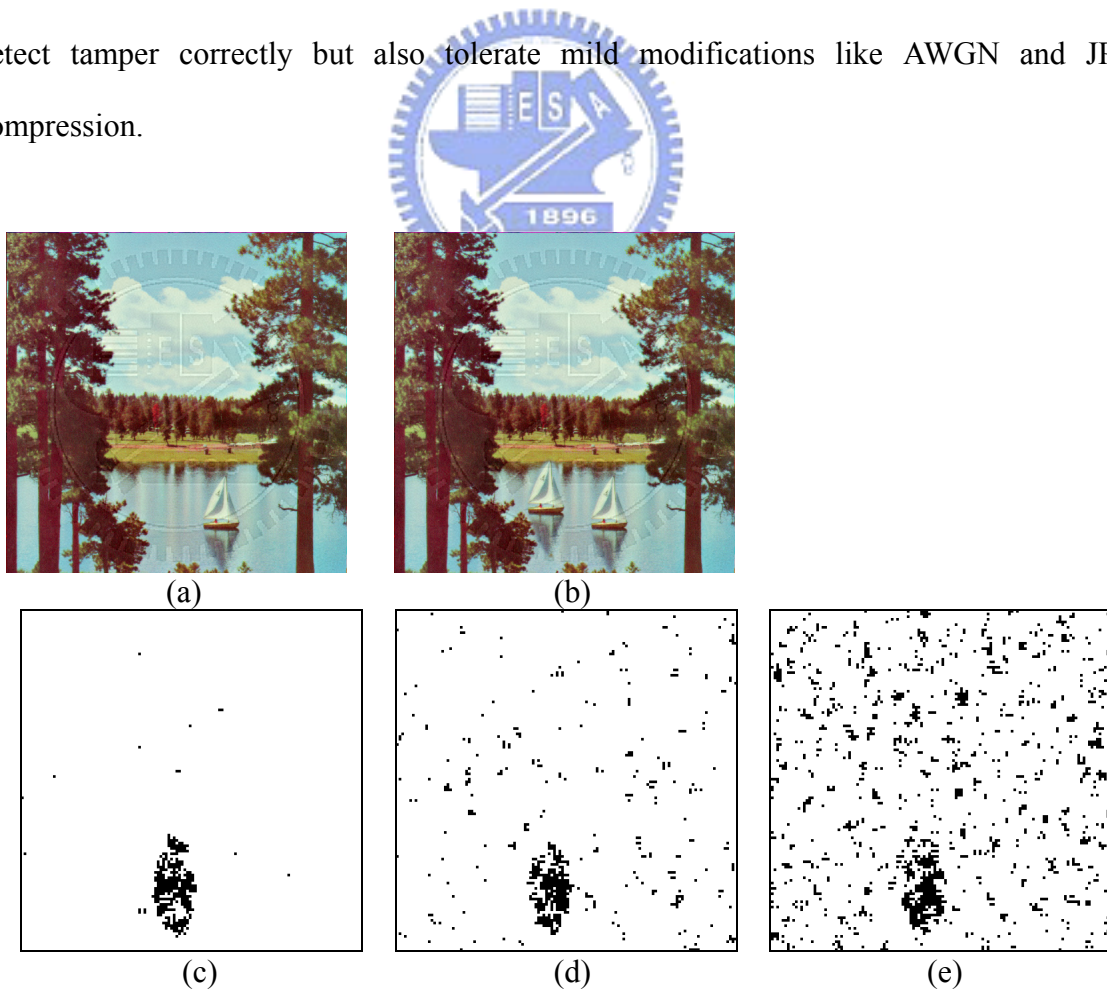
Fig. 30 (a) Result (watermarked) image (b) Tampered image (c) Tampering detection

For the combination of tampering operations and mild modifications, Fig. 31 and 32 show the tamper detection after AWGN with different σ^2 and JPEG compression with different quality factor (QF). Fig. 31 (a) shows the dual watermarked Lake image. Fig 31 (b), shows the tampered Lake image: one object (a boat) is inserted into the dual watermarked Lake image. From Fig 31 (c) (d) (e), we can see the detection result of tampered Lake image is located correctly after AWGN with different σ^2 . From Fig 32 (a) (b)

(c) (d), we can see the detection result of tampered Lake image is located correctly after JPEG compression with different quality factor (QF) setting.

From more serious attacks like watermark removal, we are also interested in the detection capability by the proposed approach. Fig. 33~36 demonstrates the tamper detection result. We can clearly see the tampered area are labeled and reflected the evidence of tampering.

Out of the above experiment results, we employ the normalized cross-correlation (NC) to evaluate the performance of watermark detection without post-processing (PP) operation. The value of NC is calculated as formula (16). Table 5~13 shows the NC value after AWGN with different σ^2 and JPEG compression with different quality factor (QF). From the results from Fig. 33~36 and Table 5~13, we can see the authentication scheme not only detect tamper correctly but also tolerate mild modifications like AWGN and JPEG compression.



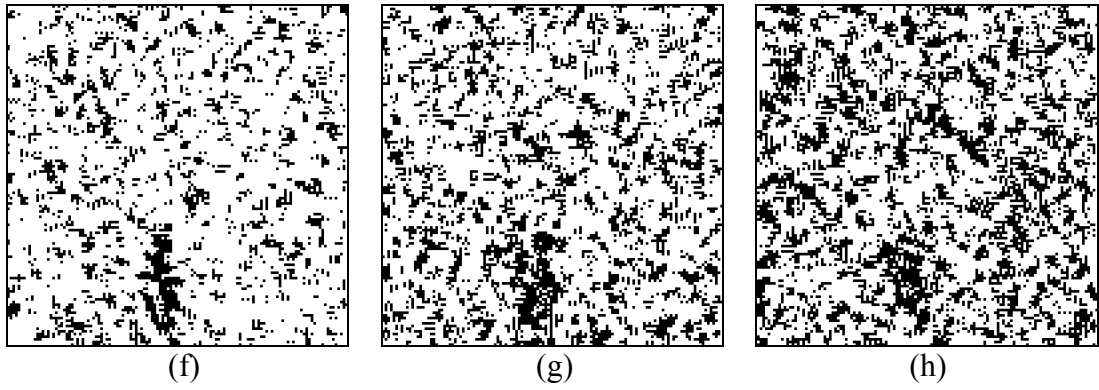


Fig. 31 Tamper detection for mixing tampering operations and AWGN (a) watermarked image (b) tampered image (c) $\sigma^2 = 6$ (d) $\sigma^2 = 12$ (e) $\sigma^2 = 18$ (f) $\sigma^2 = 24$ (g) $\sigma^2 = 30$ (h) $\sigma^2 = 36$.

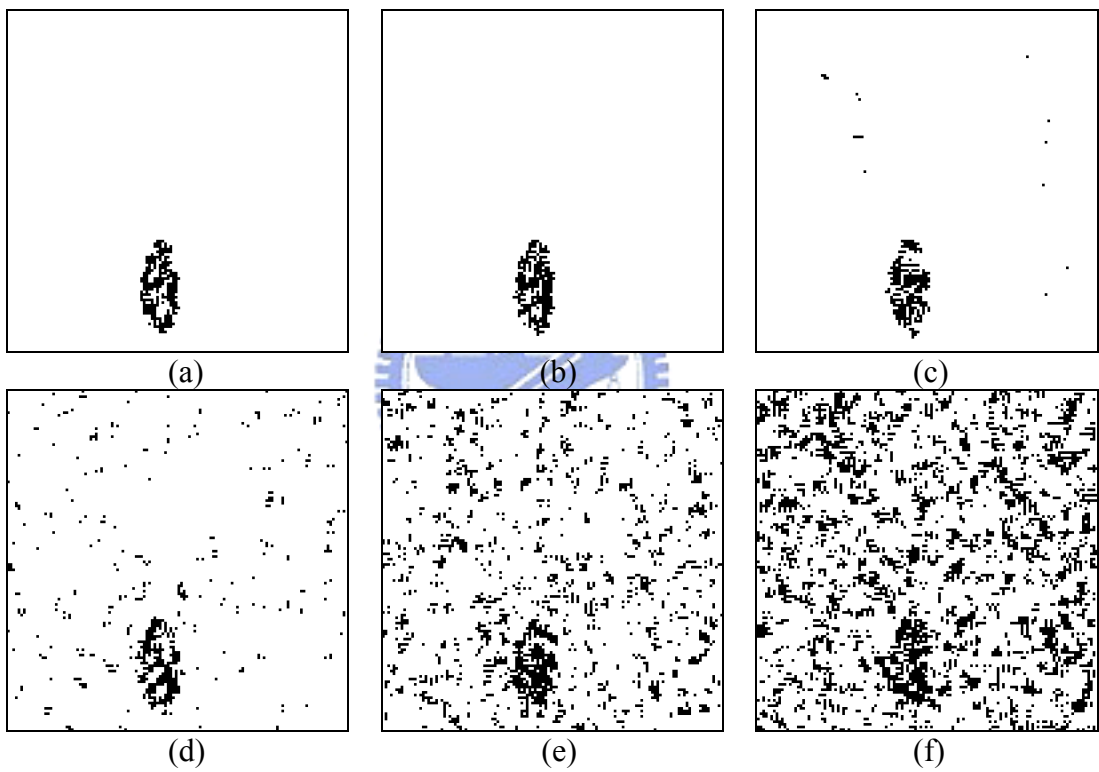


Fig. 32 Tamper detection for mixing tampering operations and JPEG compression (a) QF=100 (b) QF=90 (c) QF=80 (d) QF=70 (e) QF=60 (f) QF=50.



Fig. 33 (a) Dual watermarked image of Lena (b) Tampered dual watermarked image with watermark removal attack (c) Tampering Detection

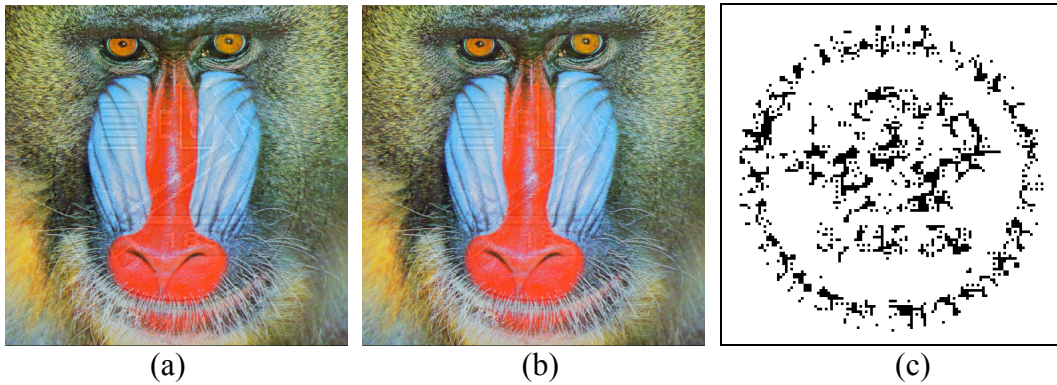


Fig. 34 (a) Dual watermarked image of Baboon (b) Tampered dual watermarked image with watermark removal attack (c) Tampering Detection



Fig. 35 (a) Dual watermarked image of Lake (b) Tampered dual watermarked image with watermark removal attack (c) Tampering Detection



Fig. 36 (a) Dual watermarked image of Peppers (b) Tampered dual watermarked image with watermark removal attack (c) Tampering Detection

$$NC = \frac{\sum_{i=1}^r \sum_{j=1}^c W'(i, j) W''(i, j)}{\sum_{i=1}^r \sum_{j=1}^c |W'(i, j)|^2} \quad (16)$$

Table 5 Lena (NCTU logo): Robustness against AWGN and JPEG compression.

Image	Lena (NCTU logo)					
AWGN: σ^2	6	12	18	24	30	36
NC	0.94	0.85	0.78	0.71	0.67	0.63
JPEG:QF	100	90	80	70	60	50
NC	0.99	0.99	0.93	0.86	0.76	0.69

Table 6 Lena (IIM logo): Robustness against AWGN and JPEG compression.

Image	Lena (IIM logo)					
AWGN: σ^2	6	12	18	24	30	36
NC	0.94	0.85	0.77	0.72	0.67	0.63
JPEG:QF	100	90	80	70	60	50
NC	0.99	0.99	0.94	0.86	0.77	0.69

Table 7 Baboon (NCTU logo): Robustness against AWGN and JPEG compression.

Image	Baboon (NCTU logo)					
AWGN: σ^2	6	12	18	24	30	36
NC	0.94	0.85	0.77	0.71	0.66	0.63
JPEG:QF	100	90	80	70	60	50
NC	0.99	0.98	0.92	0.82	0.72	0.64

Table 8 Baboon (IIM logo): Robustness against AWGN and JPEG compression.

Image	Baboon (IIM logo)					
AWGN: σ^2	6	12	18	24	30	36
NC	0.94	0.85	0.77	0.71	0.67	0.63
JPEG:QF	100	90	80	70	60	50
NC	0.99	0.98	0.92	0.82	0.72	0.65

Table 9 lake (NCTU logo): Robustness against AWGN and JPEG compression.

Image	lake (NCTU logo)					
AWGN: σ^2	6	12	18	24	30	36
NC	0.94	0.85	0.77	0.72	0.67	0.63
JPEG:QF	100	90	80	70	60	50

NC	0.99	0.98	0.93	0.85	0.75	0.67
----	------	------	------	------	------	------

Table 10 lake (IIM logo): Robustness against AWGN and JPEG compression.

Image	lake (IIM logo)					
AWGN: σ^2	6	12	18	24	30	36
NC	0.94	0.86	0.77	0.72	0.66	0.63
JPEG:QF	100	90	80	70	60	50
NC	0.99	0.98	0.93	0.85	0.76	0.68

Table 11 Peppers (NCTU logo): Robustness against AWGN and JPEG compression.

Image	Peppers (NCTU logo)					
AWGN: σ^2	6	12	18	24	30	36
NC	0.93	0.85	0.78	0.71	0.65	0.63
JPEG:QF	100	90	80	70	60	50
NC	0.99	0.98	0.93	0.85	0.76	0.68

Table 12 Peppers (IIM logo): Robustness against AWGN and JPEG compression.

Image	Peppers (IIM logo)					
AWGN: σ^2	6	12	18	24	30	36
NC	0.93	0.85	0.77	0.71	0.66	0.63
JPEG:QF	100	90	80	70	60	50
NC	0.99	0.98	0.93	0.86	0.77	0.70

In our dual watermarking algorithm, we apply Bi18/10 filter for semi-fragile watermark not Bi9/7 filter. Because we find Bi18/10 have better robustness than Bi9/7 filter from the experimental results. Fig. 37 (a) (b) (c) is the tamper detection after JPEG compression with different quality factor by using Bi18/10 filter. Fig. 37 (d) (e) (f) is the tamper detection after JPEG compression with different quality factor by using Bi9/7 filter. Fig. 38 (a) (b) (c) is the tamper detection after AWGN with different σ^2 by using Bi18/10 filter. Fig. 38 (d) (e) (f) is the tamper detection after AWGN with different σ^2 by using Bi9/7 filter. In advance, Table 14~15 shows the NC value from these filters after AWGN with different σ^2 and JPEG compression with different quality factor (QF). It is clear that semi-fragile watermark

algorithm by using Bi18/10 filter have more robust than using Bi9/7 filter.

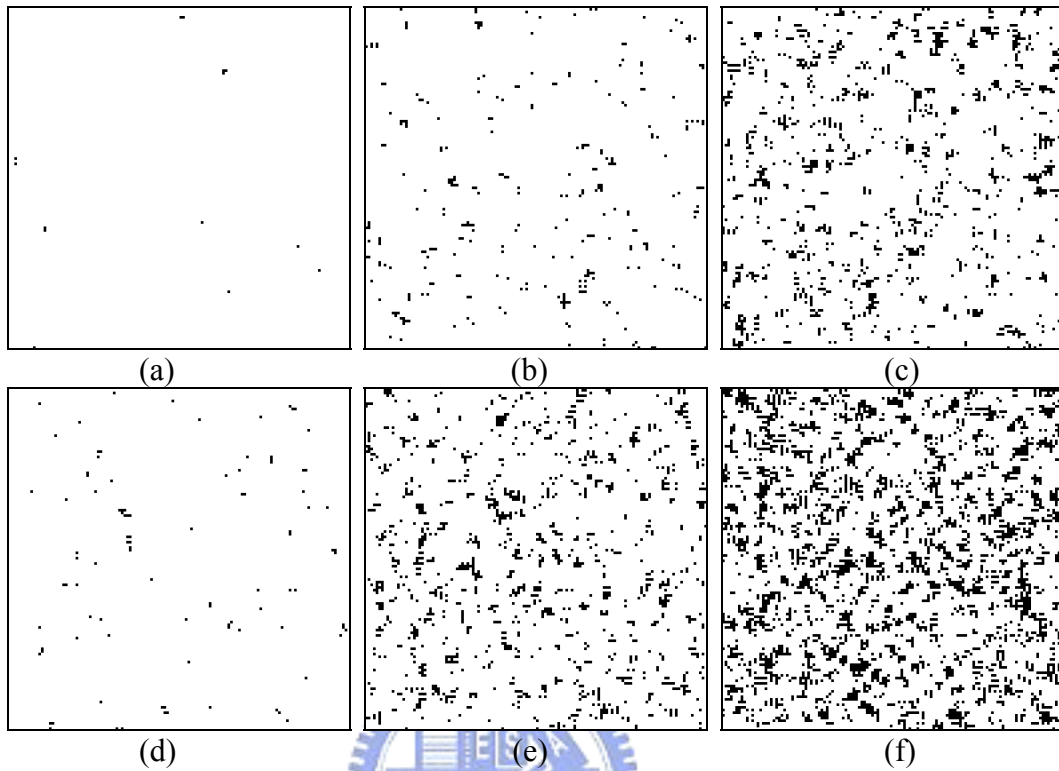
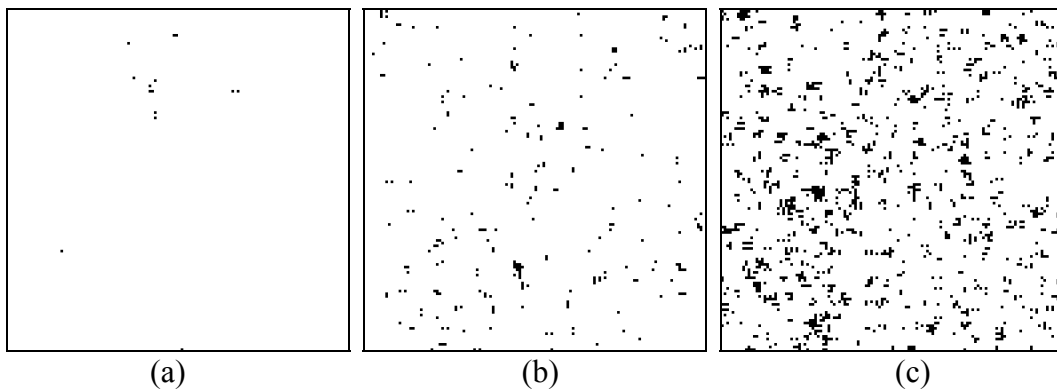


Fig. 37 Tamper Detection after JPEG compression using different filters (QF) (a) QF=80 by using Bi 18/10 Filter (b) QF=70 by using Bi 18/10 Filter (c) QF=60 by using Bi 18/10 Filter (d) QF=80 by using Bi 9/7 Filter (e) QF=70 by using Bi 9/7 Filter (f) QF=60 by using Bi 9/7 Filter



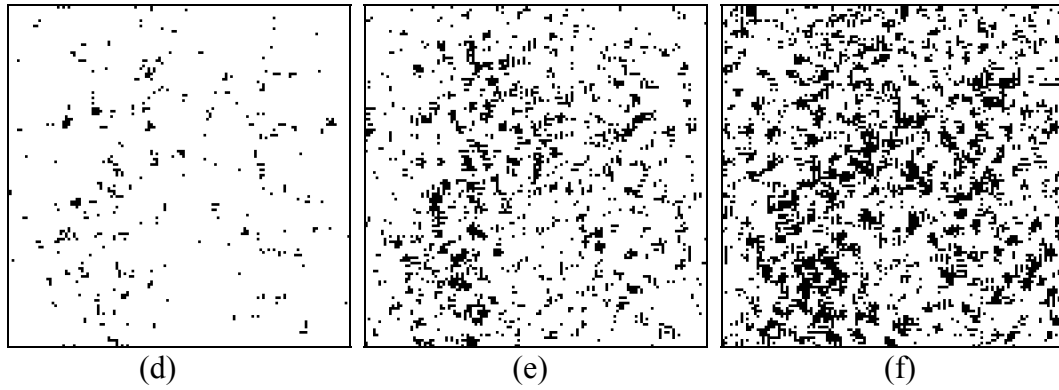


Fig. 38 Tamper Detection after AWGN using different filters (a) $\sigma^2 = 6$ by using Bi 18/10 Filter (b) $\sigma^2 = 12$ by using Bi 18/10 Filter (c) $\sigma^2 = 18$ by using Bi 18/10 Filter (d) $\sigma^2 = 6$ by using Bi 9/7 Filter (e) $\sigma^2 = 12$ by using Bi 9/7 Filter (f) $\sigma^2 = 18$ by using Bi 9/7 Filter

Table 13 Lena (NCTU logo): Robustness against AWGN and JPEG compression by using Bi18/10 Filter.

Image	Lena (NCTU logo)					
AWGN: σ^2	6	12	18	24	30	36
NC	0.94	0.85	0.78	0.71	0.67	0.63
JPEG:QF	100	90	80	70	60	50
NC	0.99	0.99	0.93	0.86	0.76	0.69

Table 14 Lena (NCTU logo): Robustness against AWGN and JPEG compression by using Bi9/7 Filter.

Image	Lena (NCTU logo)					
AWGN: σ^2	6	12	18	24	30	36
NC	0.90	0.77	0.68	0.62	0.59	0.56
JPEG:QF	100	90	80	70	60	50
NC	0.99	0.96	0.85	0.75	0.67	0.62

For general applying our algorithm, we use scrambling technique to generate binary watermark and embed it into rectangle image as semi-fragile watermark. Fig. 39 (a) shows the dual watermarked image of Lena and the size is 512×480. Fig. 39 (b) shows tampered dual watermarked image and the size is 512×480. We add one eye on the hat in the tampered image. From the detection result of tampered image, the marked points indicate the tampered parts of watermarked image and these parts are located correctly.

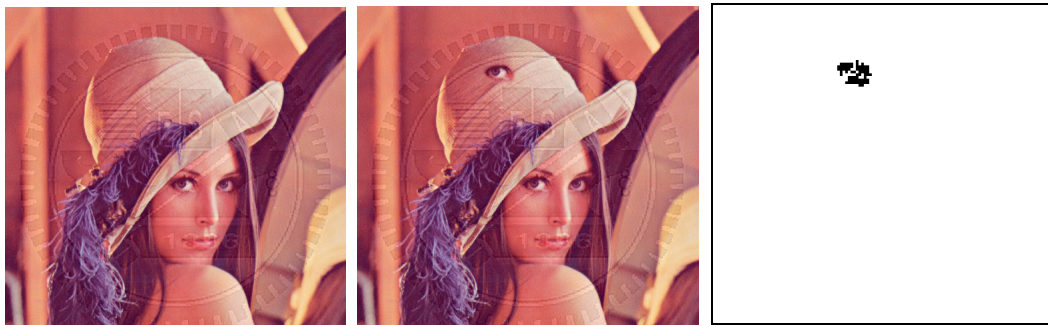


Fig. 39 (a) Dual watermarked image of Lena and the size is 512×480 (b) Tampered dual watermarked image and the size is 512×480 (c) Tampering Detection

After the intensive performance comparison, the results of different attacks, visual quality analyses and temper detection demonstrate that the proposed multipurpose color image watermarking by using dual watermarks with HVS method is more robust with better image quality. In summary, we are convinced that the proposed complete architecture is a superior scheme among the referred published techniques.

V. Conclusion and future work

A novel watermarking-based technique for copyright protection and authentication has been presented in this study. In copyright protection, we propose a new visible watermarking technique where the intensity of the watermark in different regions of the image depends on the underlying content of the image and human sensitivity to spatial frequencies. The collaboration of CSF and NVF for HVS models is leveraged with the noise reduction of the visibility thresholds for HVS in DWT domain. The perceptual weights is fine tuned for watermark embedding which results significant improvement over the watermarked images by CSF only based algorithms regarding the image quality, translucence and robustness of the watermarking. For authentication and verification of the integrity for the dual watermarked images, we applied a semi-fragile watermark algorithm which can detect and localize malicious attack effectively yet tolerate mild modifications such as JPEG compression and channel additive white Gaussian noise (AWGN). In addition, the experimental results demonstrate the proposed visible watermarking scheme has achieved high PSNR values with better visual fidelity and robustness to attacks than other schemes and the semi-fragile watermarking scheme has the capability to verify the integrity of the images.

In the future work, we hope to apply the proposed dual watermarking scheme to other multimedia contents like video and hope to find another better way to solve the security issue from visible watermark.


References

- [1] World Intellectual Property Organization (WIPO), <http://www.wipo.int/>.
- [2] I. J. Cox, et al., “Secure spread spectrum watermarking for multimedia”, IEEE Trans. on Image Proc., vol. 6, no. 12, pp. 1673-1687, Dec. 1997.
- [3] S.-J. Lee and S.-H. Jung, “A Survey of watermarking techniques”, IEEE Int’l Symposium on. Industrial Electronics, IEEE Press, pp.272-277, 2001.
- [4] G.W. Braudaway, K.A. Magerlein , and F.C. Mintzer, “Protecting publicly-available images with a visible image watermark”, Proc. Conf. Optical Security and Counterfeit Deterrence Techniques, SPIE, pp. 126-132, 1996.
- [5] C. S. Lu and H.Y. M. Liao, “Multipurpose watermarking for image authentication and protection”, IEEE Trans. on Image Proc., vol. 10, no. 10, pp. 1579-1592, Oct. 2001.
- [6] Queluz, M.P,” Authentication of digital images and video: Generic models and a new contribution”, Signal Process.: Image Comm. 16 (5), 461–475, 2001.
- [7] Chang C.C, Hu Y.S., Lu T.C., “A Watermarking-Based Image Ownership and Tampering Authentication Scheme”, Elsevier, Pattern Recognition Letter, 2005.
- [8] C. Fei, D. Kundur and R. Kwong, “Analysis and Design of Secure Watermark-based Authentication Systems”, IEEE Transactions on Information Forensics and Security, vol. 1, pp.43-55, March 2006.
- [9] B. B. Huang and S. X. Tang, “A contrast-sensitive visible watermarking scheme”, IEEE Multimedia, vol. 13, no. 2, pp. 60-66, April-June 2006.
- [10] J. Meng and S.-F. Chang, “Embedding visible video watermarks in the compressed domain,” in *Proc. ICIP*, vol. 1, pp. 474–477, Oct. 4–7 1998.
- [11] S. P. Mohanty, K. R. Ramakrishnan, and M. S. Kankanhalli, “A dual watermarking technique for image,” in Proc. 7th ACM Int. Multimedia Conf., vol. 2, pp. 49–51.,

Oct./Nov. 1999

- [12] P.-M. Chen, "A visible watermarking mechanism using a statistic approach," in *Proc. 5th Int. Conf. Signal Processing*, vol. 2, pp. 910–913, 2000.
- [13] M.S. Kankanhalli, R. Lil, and R. Ramakrishnan, "Adaptive Visible Watermarking of Images", *Proc. IEEE Int'l Conf. Multimedia Computing and Systems*, IEEE CS Press, pp. 68-73, 1999.
- [14] S.P. Mohanty, M.S. Kankanhalli, R. Ramakrishnan, "A DCT domain visible watermarking technique for image", in *Proc. IEEE Int. Conf Multimedia and Expo.*, vol. 20, pp. 1029-1032, Jul./Aug. 2000.
- [15] Y. Hu and S.Kwong, "Wavelet domain adaptive visiblewatermarking," *Electron. Lett.*, vol. 37, no. 20, pp. 1219–1220, Sep. 2001.
- [16] Y. Hu and S. Kwong, "An Image Fusion-Based Visible Watermarking Algorithm", *Proc. 2003 Int'l Symp. Circuits and Systems*, IEEE Press, pp. 25-28, 2003.
- [17] L. Yong et al., "Translucent Digital Watermark Based on Wavelets and Error-Correct Code", *Chinese J. of Computers*, vol. 27, no. 11, pp. 1533-1539, Nov. 2004.
- [18] A.P. Beegan, L.R. Iyer, and A.E. Bell, "Design and Evaluation of Perceptual Masks for Wavelet Image Compression", *Proc. 10th IEEE Digital Signal Processing Workshop*, IEEE CS Press, pp. 88-93, 2002.
- [19] D. Levický and P. Foriš, "Human Visual System Models in Digital Image Watermarking," *RADIOENGINEERING*, vol.13, no. 4, pp. 38-43, 2004.
- [20] A.B. Watson, G.Y. Yang, J.A. Solomon, J. Villasenor, "Visibility of wavelet quantization noise", *Image Processing, IEEE Transactions on*, vol.6, no.8, pp. 1164-1175, 1997.
- [21] Walton, S., "Information Authentication for a Slippery New Age", *Dr. Dobbs J.* 20 (4), pp. 18–26, 1995.
- [22] Schyndel, R.G., Tirkel, A.Z., Osborne, C.F., "A Digital Watermark", *Proceedings of*

- [23] Wolfgang, R.B., Delp, E.J., “A Watermark for Digital Images”, Proceedings of IEEE International Conference on Image Processing, Lausanne, Switzerland, vol. 3, pp. 219–222, 1996.
- [24] M.Hamad Hassan, and S.A.M Gilani, “A Semi-Fragile Signature based Scheme for Ownership Identification and Color Image”, TRANSACTIONS ON ENGINEERING, COMPUTING AND TECHNOLOGY VOLUME 13 MAY 2006.
- [25] Ö. Ekici, B. Sankur, B. Coşkun, U. Nazi and M. Akcay, “Comparative evaluation of semifragile watermarking algorithms”, Journal of Electronic Imaging, vol. 13 (1), pp. 209- 216, 2004.
- [26] D.Kundur and D. Hatzinakos, “Digital watermarking for telltale tamper proofing and authentication,” *Proc. IEEE*, vol. 87, no. 7, pp. 1167–1180, July. 1999.
- [27] H.P. Alexandre, K.W. Rabab, “Wavelet-based digital watermarking for image” , IEEE Canadian Conference on Electrical and Computer Engineering, vol. I, pp. 879-884, 2002.
- [28] J.Q. Hu, J.W. Huang, D.R. Huang, and Y.Q. Shi, “Image fragile watermarking based on fusion of multi-resolution tamper detection,” *Electron. Letter*, vol.38, no.24, pp.1512–1523, 2002.
- [29] Z.M. Lu, C.H. Liu, D.G. Xu, and S.H. Sun, “Semi-fragile image watermarking method based on index constrained vector quantization,” *Electron. Lett.*, vol.39, no.1, pp.35–36, 2003.
- [30] H. Yuan and X.P. Zhang, “A multiscale fragile watermarking based on the Gaussian mixture model in the wavelet domain,” *Proc. 2004 Int. Conf. on Acoustics, Speech and Signal Processing*, vol.3, pp.413–416, Montreal, QC, Canada, May 2004.
- [31] K. DING, C. HE, L.G. JIANG, and H.X. WANG, “Wavelet-Based Semi-Fragile

- Watermarking with Tamper Detection” , IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, E88-A(3), pp.787-790 , 2005.
- [32] Yiping Chu, Yin Zhang, Sanyuan Zhang, Xiuzi Ye, "Region of Interest Fragile Watermarking for Image Authentication," First International Multi-Symposiums on Computer and Computational Sciences-*imsccs*, pp. 726-731, Vol. 1 ,November 2006.
- [33] J. L. Mannos and D. J. Sakrison, “The effects of a visual fidelity criterion on the encoding of images”, IEEE Trans. on Info. Theory, vol. 20, no. 4, pp. 525-536, Jul. 1974.
- [34] S. Voloshynovskiy, et al., “A stochastic approach to content adaptive digital image watermarking”, in Proc. 3rd Int. Workshop Information Hiding, Dresden, Germany, pp. 211-236, Sep. 1999.
- [35] G. Voyatzis and I. Pitas, “Application of Toral Automorphisms in Image Watermarking ”, IEEE Int. Conf. on Image Processing, Vol. 2, pp 237-240, September 1996.
- [36] USC SIPI—The USC-SIPI Image Database

 [Online]:<http://sipi.usc.edu/services/database/Database.html>
- [37] AiS Watermark Pictures Protector:<http://www.watermarker.com>
- [38] JPEG 2000 compression,[Online]:<http://www.ece.uvic.ca/mdadams/hasper/~>
- [39] StirMark,[Online]:http://www.petitcolas.net/fabien/software/StirMarkBenchmark_4_0_129.zip
- [40] M. Bertalmio, V. Caselles, and C. Ballester, “Image inpainting”, presented at the *SIGGRAPH 2000*, Aug. 2000.
- [41] C.-H. Huang and J.-L. Wu, “Attacking visible watermarking”, IEEE Trans. Multimedia, vol. 6, no. 1, pp. 16-30, Feb. 2004.
- [42] S. C. Pei and Y. C. Zeng, “A Novel Image Recovery Algorithm for Visible Watermarked Image”, IEEE Trans on Information Forensics and Security, Vol. 1, Issue:4,

pp. 543-550, December 2006.

[43] [Online]:<http://www.dlib.org/dlib/december97/ibm/12lotspiech.html>

[44] [Online]:<http://www.biblepicturegallery.com/>

