A Novel Watermarking Scheme for Image Authentication in Social Networks

Thien Huynh-The
Dept. of Electrical and Electronics Engineering,
Hochiminh City University of Technology and Education
Hochiminh City, Vietnam
thethien2208@gmail.com

Oresti Banos
Dept. of Computer Engineering,
Kyung Hee University
Yongin-si, Gyeonggi-do, Korea
oresti@oslab.khu.ac.kr

Sungyoung Lee
Dept. of Computer Engineering,
Kyung Hee University
Yongin-si, Gyeonggi-do, Korea
sylee@oslab.khu.ac.kr

Yongik Yoon
Dept. of Multimedia Science,
Sookmyung Women's University
Youngsan-gu, Seoul, Korea
yiyoon@sookmyung.ac.kr

Thuong Le-Tien
Dept. of Electrical and Electronics Engineering,
Hochiminh City University of Technology
Hochiminh City, Vietnam
thuongle@hcmut.edu.vn

ABSTRACT

This paper presents a novel watermarking scheme for authentication of digital color images in social networks. The procedure consists of the embedding of a binary watermark image, containing the owner information, into the image to be authenticated. In order to minimize the artifacts in the host image the process is carried out in the wavelets domain. Concretely, the watermark embedding is performed in the HL4 and LH4 sub-band coefficients of the red, green and blue channels of the original image, based on an optimal channel selection quantization technique. To ensure a high robustness to tampering and malicious attacks a key-based pixel shuffling mechanism is further used. The reverse process is likewise identified for the extraction of the watermark from the authenticated image. Both embedding and extraction procedures are benchmarked on diverse color images and under the effects of different types of attacks, including geometric, non-geometric, and JPEG compression transformations. The proposed scheme proves to support imperceptible watermarking, while also showing a high resiliency to common image processing operations.

Categories and Subject Descriptors

I.4.0 [**General**]: Image processing software; D.4.6 [**Security and Protection**]: Authentication, Information flow controls; I.3 [**Special-Purpose and Application-based System**]: Signal processing systems

IMCOM '15, January 08-10, 2015, Bali, Indonesia
Copyright 2015 ACM 978-1-4503-3377-1/15/01
http://dx.doi.org/10.1145/2701126.2701237 ...$15.00.

General Terms

Algorithms, Designs, Measurement, Performance, Theory

Keywords

Digital Image Watermarking, Discrete Wavelet Transform, Coefficients Quantization, Optimal Color-Channel Selection

1. INTRODUCTION

Every second millions of images are generated and shared all around the world through different social network portals, websites and applications. This introduces important challenges in terms of transmission and storage, normally addressed by most content suppliers. However, security and privacy aspects are still major limitations to be overcome. People can easily upload images or other multimedia contents, which can be usually accessed and downloaded by others. In most cases, users do not retain the copyright of the uploaded images, and accordingly there is no way to certify the ownership of the digital content. As a consequence, personal images might be used for commercial or other purposes by third parties without legally requiring the user consent. To avoid this kind of situations, efficient and robust techniques are required for digital image copyright protection and authentication.

Although there exist diverse techniques for image authentication, watermarking techniques are amongst the most widely used. Watermarking systems consist of two parts: the embedding process, in charge of introducing the information of the ownership of the copyright, a.k.a, watermark, into the host image; and the extraction process, which allows the recovery of the hidden information from the watermarked image. Although digital watermarking systems may potentially build on powerful secure watermarks such as digital biometric signatures (e.g., fingerprints or eye retinas), these systems are subject to important limitations. On the one hand, the quality of the original image may significantly worsen after embedding [3, 15]. On the other hand, the watermarks may fail to be detected after slight modifications or common image transformations, such as, scaling, cropping, rotation, filtering, noise or compression [11, 12].

Watermarking systems are normally categorized based on the data used for the extraction process: non-blind watermarking models [9, 13], which require the original data for the extraction of the watermark; semi-blind watermarking models [2], which use one or more parts of the original content; and blind watermarking models [15, 8, 4, 7], which need no original data. The blind model is the most challenging type, although it provides the highest benefits in terms of security and lightness, since a private key is solely required for extracting the watermark.

In this paper, we propose a novel blind watermarking model for color images that develops on a robust wavelets quantization technique. During the embedding process, both LH and HL wavelets coefficients are grouped into wavelet blocks for each color channel after applying a 4-level discrete wavelet transformation (DWT). The bits of the binary watermark are securely shuffled and then encoded into the optimal channel wavelet blocks to minimize the perceptible differences between the original image and the watermarked image. In an inverse process, an adaptive threshold calculated through the Otsu method is used to categorize the recovered bits to obtain the watermark image. The remaining of this paper is organized as follows: Section 2 introduces the related work in the digital image watermarking domain. Section 3 describes the proposed watermarking scheme. Experimental results and their evaluation are presented in Section 4. Finally, conclusions and future work are outlined in Section 5.

2. RELATED WORK

Due to the limitations of integrating watermarks in the spatial domain, i.e., perceptible changes in the original image or fragility to image processing operations, most image watermarking techniques operate on a more robust transformed domain. Commonly used transformations are the Fourier transform [15], contourlet transform [7], curvelet transform [10] and wavelet transform [2, 3, 6, 8, 9]. For example, Wang et al. [15] introduced a robust blind color image watermarking based on the combination of Discrete Fourier Transform (DFT) and Least Squares Support Vector Machine (LS-SVM) to counteract the effects of color-based attacks and geometric distortions. However, the drawbacks of this scheme are the computational time required for the training of the LS-SVM model and the assessment of the pseudo-Zernike moments in the watermark decoding. A variation of the previous model, Quaternion Fourier Transform (QFT), is used by Tsui et al. [13]. Although this model proves to be robust against geometrical operations, it shows sensitive to hue-based processes. Hong et al. [10] used the Curvelet Transform to decompose the original image and code the watermark binary bits in the middle-frequency subbands. However, the computational cost of this approach limits its use in real-time applications.

Particularly popular has become the use of the wavelet transform due to its multiple uses in image processing. In [2], Bhatnagar et al. suggested a robust watermarking method using the Fractional Wavelet Packet Transform (FWPT) for decomposition. The embedding algorithm is implemented based on the modification of singular values of non-overlapping blocks of host images after segmentation in the wavelet domain. Hsieh et al. [6] combined Just-Noticeable-Distortion (JND) model and wavelet transform to embed a binary image into the color host image. The luminance channel in the YCbCr color space is chosen to hide the secret information as a solution to protect the visual quality of the output images. Also considering a binary image as a watermark, Run et al. [8] developed a blind watermarking scheme using a quantization technique based on Wavelet Tree Analysis (WTA). However, the usage of a constant threshold makes this procedure weak to image attacks. In an effort to improve the robustness under diverse image attacks, Song et al. [9] utilized Singular Value Decomposition (SVD) together with DWT in a dual-image system. This scheme applied dual watermarking mechanisms to embed parts of the watermark images into selected regions of the host images. More recently, Chou et al. [3] also showed that the strength of the embedded watermark signal can be controlled by measuring the perceptual redundancy inherent to each wavelet coefficient of each color channel.

More complex machine learning algorithms have also been used in image watermarking. For example, Fu et al. [4] used Support Vector Machine (SVM) to extract the watermark. Although the information can be successfully extracted, the robustness is limited under the effects of geometric attacks. Agarwal et al. [1] used a Genetic Algorithm - Back Propagation Network (GA-BPN) for embedding and extracting the watermark based on identified characteristics of the human visual system. The main limitations of this approach refer to both computational and time costs.

3. A NOVEL WATERMARKING SCHEME FOR IMAGE AUTHENTICATION

The proposed watermarking scheme consists of a set of steps for both watermark embedding and extraction processes (Fig. 1). These steps are described next.

3.1 Watermark Embedding Process

The embedding process consists in encoding the watermark information in a transformed version of the host image, which is then recovered back to its original domain. Given a color host image, the first step of the watermark embedding process consists in transforming this image into a more robust domain, here the wavelet domain. To that end, a DWT is applied to each channel of the host image, i.e., red (R), green (G) and blue (B). The choice of the level of decomposition strictly relates to the robustness and amount of information that can be actually embedded into the image. In fact, the higher the decomposition level is, the more robust the hidden information will be, but also the less information can be hidden. Moreover, the amount of information that can be embedded into a particular host image also depends on its size. It can be simply derived that for a n-DWT decomposition, given a host image of $P \times R$ pixels, the watermark payload, i.e., the maximum number of binary bits that can be hidden in the host image, would be $N = \frac{P \times R}{2^2 n}$. Accordingly, in this work we use a 4-DWT decomposition which is devised to provide a reasonable trade-off between robustness and payload. For this case, if an 512×512 host image is for example used, the watermark payload would be 1024 bits.

For each level of decomposition, four sub-bands are generated, respectively containing the approximation coefficients,

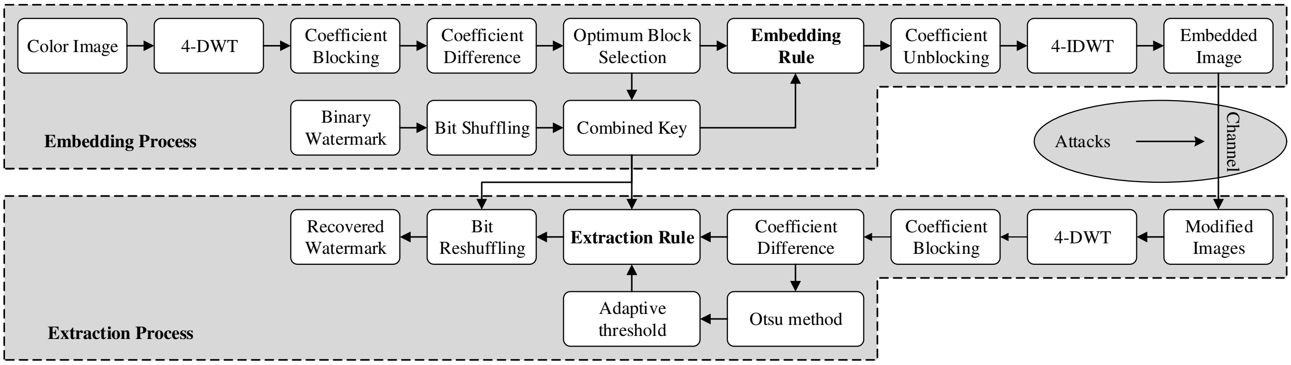


Figure 1: Flowchart of the proposed watermarking model.

LL, and detail coefficients, LH, HL and HH (horizontal, vertical, and diagonal). From these, only the two middle-frequency components, i.e., LH and HL, are used to effectively embed the watermark information, since LL coefficients are too much sensitive to noise and HH coefficients are easily eliminated during JPEG compression. Once both HL and LH coefficients are obtained, these are grouped as shown in Fig. 2. From here, the difference between LH and HL coefficients is computed for each channel as follows:

$$\Delta_{i,k} = \left| C_{LH_{i,k}} - C_{HL_{i,k}} \right| \tag{1}$$

where $C_{LH_{i,k}}$ and $C_{HL_{i,k}}$ represent the LH and HL coefficients of the i^{th} wavelet block from the k^{th} color channel.

In order to encode the information of the watermark into the LH and HL coefficients, a quantization technique is employed. Two quantization thresholds, y_1 and y_2 ($y_1 < y_2$), are respectively used to quantize the watermark bits, w_i. The quantization technique seeks to set $\Delta_{i,k}$ to y_1 if w_i is a 0-bit, and to y_2 or higher if w_i is a 1-bit. To improve the quality of the eventual watermarked image [8], $C_{LH_{i,k}}$ and $C_{HL_{i,k}}$ coefficients are first sorted in ascending order of difference. Accordingly, the coefficients with the smallest difference ($\Delta_{i,k} \downarrow$) will be used to code the 0-bits, while those with the greatest difference ($\Delta_{i,k} \uparrow$) will be used to code the 1-bits. We note in advance the sorted coefficient differences as $\Delta^S_{i,k}$. Then, given N_0 the number of 0-bits in the watermark, y_1 can be determined through averaging $\Delta^S_{i,k}$ across all channels for the first N_0 blocks:

$$y_1 = \frac{1}{N_0} \sum_{k=1}^{3} \sum_{i=1}^{N_0} \Delta^S_{i,k} \tag{2}$$

Being N_1 the number of 1-bits in the watermark, the value of y_2 can be calculated as follows:

$$y_2 = \frac{1}{3} \sum_{k=1}^{3} \Delta^S_{i=\lambda N_1,k} \tag{3}$$

where λ is the robustness factor representing the strength of the watermark on the host image. The higher the λ value, the higher the y_2 and vice versa. From these equations it can be clearly seen that the first N_0 sorted blocks are used for encoding the watermark 0-bits, while the remaining N_1 blocks are used for encoding the 1-bits, with $N = N_0 + N_1$ the total amount of bits in the watermark.

In order to increase the robustness and security of the embedding process, as well as to enrich the quality of the watermarked image, the quantization is not applied to all channels for all blocks. Rather than that, one specific channel is selected for each block during the encoding of the watermark bits. The selected channel, *k_opt*, is simply the one which minimizes the difference between $\Delta^S_{i,k}$ and y_1 for $w_i = 0$, and y_2 for $w_i = 1$:

$$k\_opt = \begin{cases} \arg\min\limits_{k} \left(\left| \Delta^S_{i,k} - y_1 \right| \right) & ; \forall w_i = 0 \\ \arg\min\limits_{k} \left(\left| \Delta^S_{i,k} - y_2 \right| \right) & ; \forall w_i = 1 \end{cases} \tag{4}$$

This process is part of the so-called optimal block selection.

Now that the quantization thresholds are computed and also the optimal blocks selected, the embedding rule to encode the watermark 0-bits and 1-bits can be simply described as follows:

- For $w_i = 0$ (0-bits):

$$\begin{array}{ll} C_{LH_{i,k\_opt}} \geq C_{HL_{i,k\_opt}} \rightarrow & C_{LH_{i,k\_opt}} = C_{LH_{i,k\_opt}} + \nabla^0_i \\ C_{LH_{i,k\_opt}} < C_{HL_{i,k\_opt}} \rightarrow & C_{HL_{i,k\_opt}} = C_{HL_{i,k\_opt}} + \nabla^0_i \end{array} \tag{5}$$

where $C_{LH_{i,k\_opt}}$ and $C_{HL_{i,k\_opt}}$ are the LH and HL coefficients of the i^{th} wavelet block ($\forall i = 1, ..., N_0$) from the *k_opt* channel. $\nabla^0_i = y_1 - \Delta^S_{i,k}$ represents the actual modification of the original coefficients required to encode the 0-bits.

- For $w_i = 1$ (1-bits):
  If $\Delta^S_{i,k} < y_2$

$$\begin{array}{ll} C_{LH_{i,k\_opt}} \geq C_{HL_{i,k\_opt}} \rightarrow & \begin{cases} C_{LH_{i,k\_opt}} = C_{LH_{i,k\_opt}} + \nabla^1_i \\ C_{HL_{i,k\_opt}} = C_{HL_{i,k\_opt}} - \nabla^1_i \end{cases} \\ C_{LH_{i,k\_opt}} < C_{HL_{i,k\_opt}} \rightarrow & \begin{cases} C_{LH_{i,k\_opt}} = C_{LH_{i,k\_opt}} - \nabla^1_i \\ C_{HL_{i,k\_opt}} = C_{HL_{i,k\_opt}} + \nabla^1_i \end{cases} \end{array} \tag{6}$$

with $\nabla^1_i = y_2 - \Delta^S_{i,k}$ the change that needs to be introduced in the original coefficients when encoding the 1-bits for the i^{th} block ($\forall i = N_0 + 1, ..., N$).

If $\Delta^S_{i,k} \geq y_2$

$$\begin{array}{l} C_{LH_{i,k\_opt}} = C_{LH_{i,k\_opt}} \\ C_{HL_{i,k\_opt}} = C_{HL_{i,k\_opt}} \end{array} \tag{7}$$

This quantization procedure can be directly applied to the original watermark. However, for security reasons, the watermark bits are first shuffled to encrypt the information. A key combining the information about the position of the watermark bits before shuffling, and the corresponding channel used for the codification of each pixel, is generated. Through this, we can ensure that only the owner of this key can recover the original watermark during the extraction process.

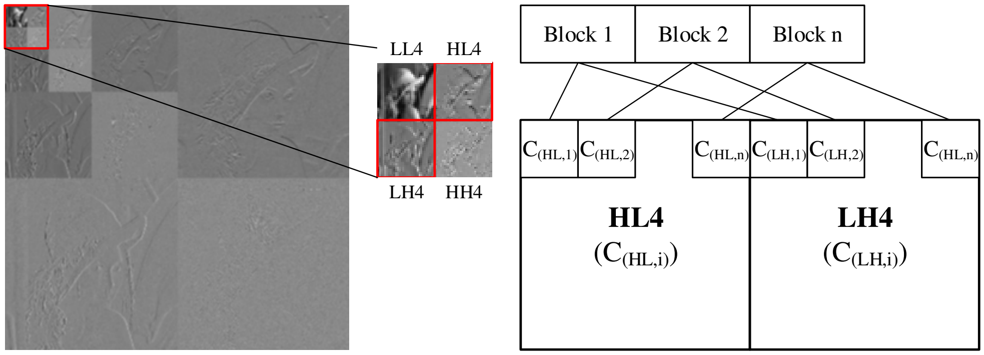


Figure 2: Decomposition and grouping of the 4-DWT LH and HL coefficients.

After encoding the watermark into the image, the modified coefficients are reconstructed into the original LH and HL sub-bands. Then, each color channel is recovered by using the Inverse Discrete Wavelet Transform (IDWT). At this point, the watermarked image is ready.

3.2 Watermark Extraction Process

A process very similar to the watermark embedding is used for extracting the watermark from the authenticated image. The watermarked image is 4-DWT decomposed to obtain its wavelet coefficients. Then, both LH and HL coefficients are grouped in blocks and the coefficient differences computed. From here, the blocks containing watermark information can be identified by using the combined key. For those particular blocks, the encoded information can be extracted from the coefficient differences. As described in the previous section, for $\Delta_{i,k} = y_1$ a 0-bit would be found, and a 1-bit for $\Delta_{i,k} \geq y_2$. Nevertheless, y_1 and y_2 are unknown to the extraction model. Therefore, an empirical threshold, y, must be determined based on the available information. This threshold, that must satisfy $y_1 < y < y_2$, may potentially vary from image to image, and also under the effects of image transformations. Thus, the authors propose the use of an adaptive threshold based on the Otsu method [5]. This method calculates the optimum threshold separating two classes or distributions so that their combined spread, i.e., intra-class variance, is minimal. In application to our case, the threshold would be computed as follows:

$$y = \arg\min_{\Delta} \left(\sigma_\omega^2 \left(\Delta\right)\right) \tag{8}$$

where $\sigma_\omega^2 \left(\Delta\right)$ represents the variance of the coefficients differences Δ. Fig. 3 shows some examples of the thresholds computed for diverse watermarked images under the effects of various transformations.

The watermark bits can be then simply extracted from the coefficient differences by comparing them to y:

$$w_i = \begin{cases} 1 & (\Delta_{i,k\_opt} \geq y) \\ 0 & otherwise \end{cases} \tag{9}$$

Finally, the recovered bit series need to be reshuffled to obtain the original binary watermark image, for which here again the key is used.

4. EXPERIMENTAL RESULTS AND EVALUATION

The efficacy of the watermarking scheme is measured by the imperceptibility of the inserted mark to human observers and the robustness of the mark to other imperceptible manipulations of the marked data. Imperceptibility and robustness are competing goals, because increasing robustness must mean more alteration to the original image, distortion which at some level may become perceptible. In this section, both imperceptibility after embedding and robustness after extraction are evaluated.

4.1 Experimental Setup

The proposed watermarking method is benchmarked on several color images from the publicly available USC-SIPI Image Database[1]. Eight widely used samples are considered (512 × 512 pixels, 8 bits/pixel/channel), namely Airplane, Girl, House, Lena, Mandrill, Peppers, Sailboat, and Splash. The watermark used for evaluation is a 16 × 64 binary image containing the information for authentication (Fig. 7.a). This image fulfills the maximum watermark payload for the considered host images (1024 bits).

4.2 Evaluation Metrics

For the watermark embedding process, the Color Peak Signal-To-Noise Ratio (CPSNR) and the Similarity Structure Index (SSIM) [14] metrics are used to measure the quality of the watermarked image. The CPSNR is calculated as follows:

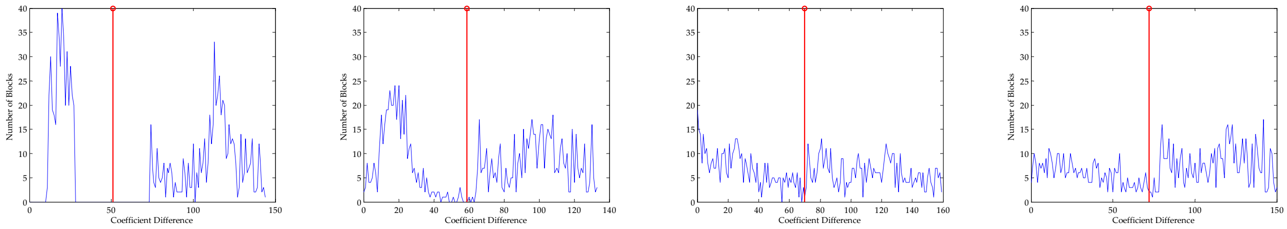
$$CPSNR = 10\log_{10}\left(255^2 \Bigg/ \frac{\sum\limits_{k=1}^{3}\sum\limits_{i=1}^{P}\sum\limits_{j=1}^{R}\left(O_k\left(i,j\right) - W_k\left(i,j\right)\right)^2}{3 \times P \times R}\right) \tag{10}$$

where P and R are the height and width of the original (O) and watermarked (W) image, and $O_k\left(i,j\right)$ and $W_k\left(i,j\right)$ the values of the $i^{th} - j^{th}$ pixels for each channel k. The SSIM value can be obtained as:

$$SSIM = \frac{1}{T}\sum\nolimits_{t=1}^{T} SSIM\_MAP\left(O_t, W_t\right) \tag{11}$$

where T is the number of local windows in the image. The $SSIM\_MAP$ function [14] is here defined as the product of the luminance, contrast and structural similarities between two windows extracted from the original and watermarked images.

[1] ftp://http://sipi.usc.edu/database/



(a) (b) (c) (d)

Figure 3: Determined Otsu thresholds under the effects of different types of attacks: (a).No attack, (b).Median filter (7×7), (c).Rotation $\left(0.25^0\right)$, (d).Gaussian noise $\left(\mu = 0, \sigma^2 = 0.05\right)$.

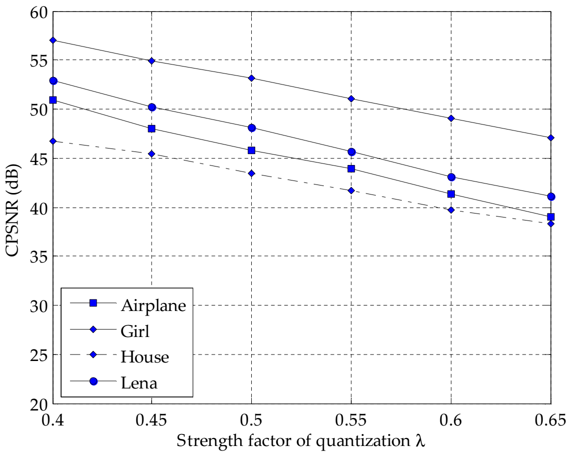


Figure 5: Quality of the watermarked images for different λ values.

For the extraction process, the Normalized Correlation (NC) value is used to estimate the quality of the extracted watermark with respect to the original one. The NC figure is computed as follows:

$$NC = \frac{1}{p \times r} \sum_{i=1}^{p} \sum_{j=1}^{r} w(i,j) \times w'(i,j) \tag{12}$$

where $p \times r$ is the size of the watermark, and $w(i,j)$ and $w'(i,j)$ are the values of the $i^{th} - j^{th}$ pixels of the original and extracted watermark. The value of $w(i,j)$ is set to 1 if the watermark bit for that position is 1, otherwise, it is set -1, and similarly for $w'(i,j)$. Therefore, the value of $w(i,j) \times w'(i,j)$ is either 1 or -1. If the number of correctly extracted bits exceeds the incorrect ones, the NC value will be positive; otherwise, it will be negative. At best, the value should converge to 1.

4.3 Image Quality after Embedment

This section analyzes the quality of the watermarked image for different values of the robustness factor λ. As it was described in Section 3.1, λ represents the strength of the watermark into the host image. For low λ values the watermarked robustness decreases, while its overall quality increases. The opposite is seen for high λ values. This phenomena can be empirically observed for some examples in Fig. 5.

Fig. 4 shows the qualitative results obtained after embedding a binary image in several host images for $\lambda = 0.5$. Visually, the embedded data is perceptually invisible to the human eye system. From the quantitative results, Table 1, it can be nevertheless observed the actual effect of λ. Through analyzing the tendencies of the CPSNR and SSIM metrics for all samples it can be effectively confirmed that the quality of the output image degrades as λ increases.

4.4 Watermark Robustness after Extraction

The robustness of the watermark after extracted from embedded images, subject to diverse attacks, is here analyzed. The attacks include geometric transformations like scaling (resize to 128×128 and then restore to 512×512), cropping (remove a quarter of the embedded image at the center and replace this portion with 0-bits), rotation (0.5^0), and Gaussian noise (mean=0, variance=0.05); non-geometric attacks like histogram equalization (for luminance channel), average filter, median filter, and Gaussian filter using a 7×7 mask for all of them; and JPEG compression with various grades of Quality Factor (QF). The classical Lena sample is used for illustrating these attacks in Fig. 6. The watermarks extracted from the attacked images are shown in Fig. 7, while the quantitative results are represented in Table 2. In general, the proposed watermarking scheme proves tolerant to common image processing operations, such as scaling, low-frequency filtering, and JPEG compression; however, the robustness to cropping and histogram equalization is not that high, as it could be expected. The process of spreading the watermark bits on the whole image during the embedding may explain the high sensitivity to croppings and rotations, whilst hue-based operations negatively affect the color channel-based embedding technique. Moreover, the robustness sometimes also depends on the structure of the image as it is the case for the Splash sample.

It is also aim of this work to evaluate the efficiency of the proposed method when using three selective color channels for the coefficient quantization instead of only one color channel [4] or luminance channel [6] as suggested in existing approaches. The comparison of the NC values obtained for the extracted watermark is shown in Table 3. Clearly, the proposed scheme, i.e., watermarking through the 3-channels, outperforms the others in most attack cases. When embedding the information into the luminance channel, the results are worst due to the error introduced during the conversion between RGB and YCbCr color spaces. Red and Green channels prove in general to be robust, while the Blue channel appears to be quite sensitive to the effects of JPEG com-

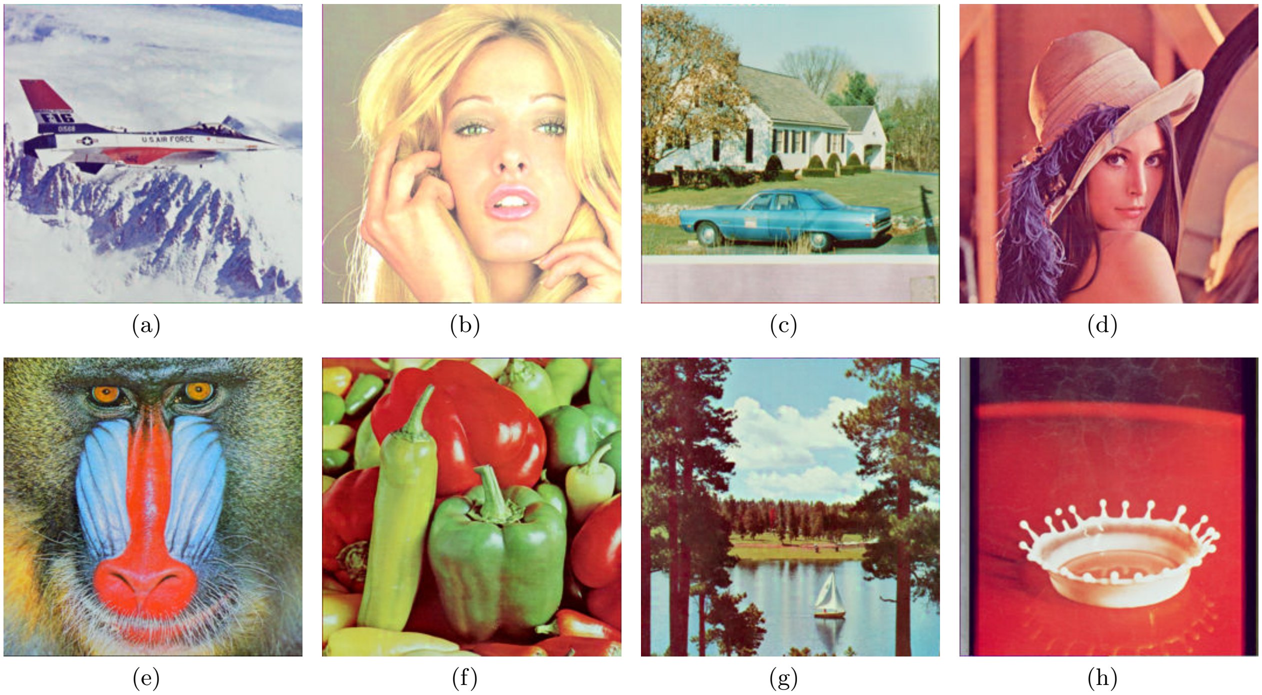

(a) (b) (c) (d)
(e) (f) (g) (h)

Figure 4: Output images after watermarking: (a).Airplane, (b).Girl, (c).House, (d).Lena, (e).Mandrill, (f).Peppers, (g).Sailboat, (h).Splash.

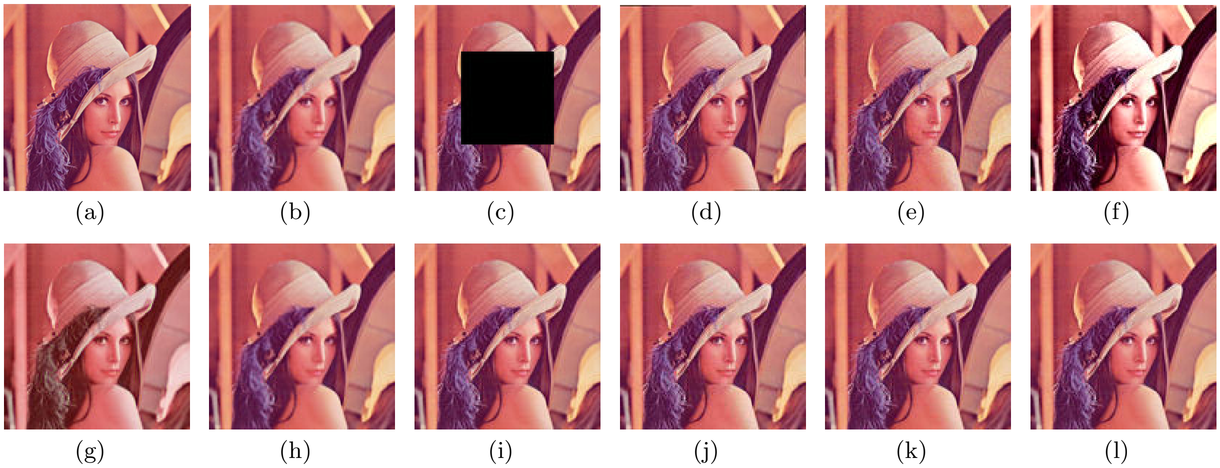
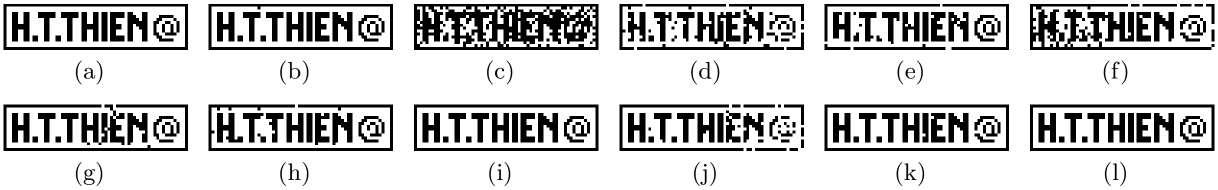

(a) (b) (c) (d) (e) (f)
(g) (h) (i) (j) (k) (l)

Figure 6: Watermarked image under (a).No attack; Geometric Attacks: (b).Scaling, (c).Cropping, (d).Rotation, (e).Gaussian noise; Non-geometric Attacks: (f).Histogram equalization, (g).Average filter, (h).Median filter, (i).Gaussian filter; JPEG Compression: (j).QF=20%, (k).QF=40%, (l).QF=60%.



(a) (b) (c) (d) (e) (f)
(g) (h) (i) (j) (k) (l)

Figure 7: Extracted watermark from an authenticated image subject to diverse attacks: (a).Original; Geometric Attacks: (b).Scaling, (c).Cropping, (d).Rotation, (e).Gaussian noise; Non-geometric Attacks: (f).Histogram equalization, (g).Average filter, (h).Median filter, (i).Gaussian filter; JPEG Compression: (j).QF=20%, (k).QF=40%, (l).QF=60%.

pression and Gaussian noise.

Table 4: Comparison of the proposed scheme and Niu's method (Lena sample)

Attacking	Niu [7]	Proposed
	40.71 dB	48.17 dB
Scaling	0.9454	0.998
Cropping 20%	0.7950	0.9121
Rotation 5^0	0.9394	0.5625
Gaussian noise (m=0,var=0.006)	0.9454	0.9883
Median filter (3 × 3)	0.9394	1.0000
Gaussian filter (3 × 3)	0.9374	1.0000
JPEG QF=30%	0.9200	0.9277
JPEG QF=40%	0.9332	0.9941
JPEG QF=70%	0.9358	1.0000

Finally, the authors compare the proposed scheme with one of the most prominent and robust watermarking techniques in this domain (Niu et al., [7]). Conversely to other approaches, Niu's technique focuses on the robustness to geometric distortions, proving a high resiliency to geometric attacks. The NC values obtained for the extracted watermark for both models are presented in Table 4. As it can be observed, the proposed scheme outperforms Niu's method in most cases, but for the rotation operation. This demonstrates here again the potential of our model.

5. CONCLUSIONS

In this work, we proposed a novel watermarking scheme for authentication of color images. The embedding process consists in encoding a binary image containing the watermark information into the middle sub-bands wavelet coefficients of the host image. An automatic optimal color channel selection procedure is defined to quantize the wavelet coefficients based on the watermark payload. This color channel selection is proved to be a key advantage of this model, since it improves the quality of the watermarked image, and also serves as a mechanism to increase the security and integrity of the watermark. The watermark is simply extracted by using an adaptive threshold approach based on the Otsu method, which is shown to be applicable in different cases of image attacks. From the experimental results, it can be concluded that the proposed method is capable of watermarking an image without introducing perceptible changes to the human vision. Likewise, the presented mechanism allows for a very robust recovery of the watermark even when the embedded image is subject to harsh image attacks. The main drawbacks of this method include high computational costs due to the processing of the three color channels and low robustness to some geometric operation, such as cropping and rotation. Next steps of this work aims at solving these shortcomings by investigating more efficient domain transformations.

6. ACKNOWLEDGMENTS

This research was partially funded by the Korean Ministry of Science, ICT & Future Planning (MSIP) as part of the ICT R&D Program 2014. This work was also supported by the Industrial Core Technology Development Program, funded by the Korean Ministry of Trade, Industry and Energy (MOTIE), under grant number #10049079.

7. REFERENCES

[1] C. Agarwal, A. Mishrab, and A. Sharma. Gray-scale image watermarking using ga-bpn hybrid network. *J. Vis. Commun. Image R.*, 24(7):1135–1146, Oct 2013.

[2] G. Bhatnagar, B. Raman, and Q. Wu. Robust watermarking using fractional wavelet packet transform. *IET Image Processing*, 6(4):386–397, Jun 2012.

[3] C.-H. Chou and K.-C. Liu. A perceptually tuned watermarking scheme for color images. *IEEE Transactions on Image Processing*, 19(11):2966–2982, Nov 2010.

[4] Y. Fu, R. Shen, and H. Lu. Watermarking scheme based on support vector machine for colour images. *Electronics Letters*, 40(16):986–987, Aug 2004.

[5] R. C. Gonzalez and R. E. Woods. Digital image processing. *3rd Edition, Prentice Hall*, 2007.

[6] S.-L. Hsieh, J.-J. Jian, I.-J. Tsai, and B.-Y. Huang. A color image watermarking scheme based on secret sharing and wavelet transform. *in Proc. on Systems, Man and Cybernetics*, pages 2143–2148, Oct 2007.

[7] P.-P. Niu, X.-Y. Wang, Y.-P. Yang, and M.-Y. Lu. A novel color image watermarking scheme in nonsampled contourlet-domain. *Expert Systems with Applications*, 38(3):2081–2098, Mar 2011.

[8] R.-S. Run, S.-J. Horng, W.-H. Lin, T.-W. Kao, P. Fan, and M. K. Khan. An efficient wavelet-tree-based watermarking method. *Expert Systems with Applications*, 38(12):14357–14366, Nov 2011.

[9] C. Song, S. Sudirman, and M. Merabti. A robust region-adaptive dual image watermarking technique. *J. Vis. Commun. Image R.*, 23(3):549–568, Apr 2012.

[10] H. Song and J. Gu. Curvelet based adaptive watermarking for images. *in Proc. on Computer Science and Network Technology*, pages 1101–1105, Dec 2012.

[11] P.-C. Su, Y.-C. Chang, and C.-Y. Wu. Geometrically resilient digital image watermarking by using interest point extraction and extended pilot signals. *IEEE Transactions on Information Forensics and Security*, 08(12):1897–1908, Dec 2013.

[12] T. N. Thanh, D. Taubman, V. V. Huynh, and T. Le-Tien. A novel technique for geometrically robust blind image watermarking extraction. *in Proc. on Advanced Technologies for Communication*, pages 101–105, Oct 2013.

[13] T. K. Tsui, , X.-P. Zhang, and D. Androutsos. Color image watermarking using multidimensional fourier transforms. *IEEE Transactions on Information Forensics and Security*, 3(1):16–28, Mar 2008.

[14] Z. Wang, A. C. Bvik, H. R. Sheikh, and E. Simoncelli. Image quality assessment: From error visibility to structural similarity. *IEEE Transactions on Image Processing*, 13(4):600–612, Apr 2004.

[15] W. Xiang-yang, W. Chun-peng, Y. Hong-yinga, and N. Pan-pan. A robust blind color image watermarking in quaternion fourier transform domain. *Journal of Systems and Software*, 86(2):255–277, Feb 2012.

Table 1: **Quality of the watermarked image for different values of λ**

Image	**CPSNR (dB)**					**SSIM**				
	0.4	0.45	0.5	0.55	0.6	0.4	0.45	0.5	0.55	0.6
Airplane	50.95	47.97	45.81	43.90	41.33	0.9972	0.9948	0.9920	0.9884	0.9812
Girl	57.01	54.95	53.13	51.01	49.12	0.9999	0.9999	0.9999	0.9998	0.9997
House	46.75	45.49	43.41	41.71	39.74	0.9977	0.9970	0.9955	0.9936	0.9904
Lena	52.88	50.20	48.17	45.69	43.07	0.9999	0.9998	0.9997	0.9995	0.9991
Mandrill	49.98	48.35	46.75	45.17	43.64	0.9996	0.9995	0.9992	0.9989	0.9984
Peppers	49.34	47.06	44.57	42.46	40.51	0.9998	0.9997	0.9994	0.9991	0.9986
Sailboat	48.45	46.03	43.73	41.33	39.54	0.9992	0.9987	0.9980	0.9967	0.9952
Splash	60.21	58.01	55.28	51.78	49.22	1.0000	0.9999	0.9999	0.9998	0.9996

Table 2: **NC values for the watermark extraction after various types of attacks and $\lambda = 0.5$**

Attack types	Airplane	Girl	House	Lena	Mandrill	Peppers	Sailboat	Splash
Without attacking	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000
Scaling	0.994	0.996	1.000	0.998	0.996	1.000	0.998	0.986
Cropping 25%	0.664	0.711	0.672	0.647	0.740	0.709	0.660	0.742
Rotation 0.5^0	0.813	0.850	0.830	0.893	0.734	0.877	0.838	0.846
Gaussian noise	0.945	0.789	0.982	0.945	0.938	0.971	0.986	0.617
Histogram equalization	0.619	0.748	0.742	0.863	0.787	0.799	0.885	0.627
Average filter 7 × 7	0.900	0.856	0.781	0.979	0.637	0.975	0.840	0.904
Median filter 7 × 7	0.922	0.924	0.961	0.969	0.889	0.981	0.959	0.904
Gaussian filter 7 × 7	1.000	1.000	1.000	1.000	1.000	1.000	1.000	1.000
JPEG QF=10%	0.738	0.679	0.707	0.686	0.453	0.828	0.848	0.557
JPEG QF=20%	0.914	0.842	0.951	0.928	0.832	0.951	0.963	0.623
JPEG QF=40%	0.984	0.963	0.998	0.994	0.957	1.000	0.996	0.856
JPEG QF=60%	1.000	0.986	1.000	1.000	0.994	1.000	1.000	0.961

Table 3: **NC values for the watermark extraction when embedding the information in different channels.**

Attack types	3-channel	Luminance	Red	Green	Blue
	(48.17 dB)	(39.24 dB)	(44.79 dB)	(43.74 dB)	(49.71 dB)
Without attacking	1.000	0.9277	1.000	1.000	1.000
Scaling	0.998	0.902	0.998	1.000	1.000
Cropping 25%	0.647	0.602	0.680	0.654	0.639
Rotation 0.25^0	0.893	0.781	0.869	0.906	0.867
Gaussian noise	0.945	0.836	0.938	0.981	0.826
Histogram equalization	0.863	0.809	0.865	0.885	0.869
Average filter 7 × 7	0.979	0.869	0.977	0.982	0.965
Median filter 7 × 7	0.969	0.902	0.981	0.984	0.969
Gaussian filter 7 × 7	1.000	0.924	1.000	1.000	1.000
JPEG QF=10%	0.686	0.760	0.678	0.887	0.561
JPEG QF=20%	0.928	0.885	0.887	0.992	0.727
JPEG QF=40%	0.994	0.908	0.988	1.000	0.834
JPEG QF=60%	1.000	0.932	1.000	1.000	0.973