A New Color Image Watermarking Technique Using Hybrid Domain

Ghazali Bin Sulong [1], Harith Hasan(Corresponding author) [2] , Ali Selamat[3] , Mohammed Ibrahim [4] and Saparudin [5]

[1,2,3,4] **Faculty of Computer Science and Information Systems**
University Technology Malaysia
81310, Skudai, Johor, Malaysia

[5] **Faculty of Computer Science University of Sriwijaya**
Fasilkom campus, Indralaya potentials. Ogan Ilir. Indonesia

Abstract

Many watermarking techniques have been used for copyright protection of digital images. A color image watermarking technique which is robust and resilient to many types of attack is proposed. This technique involves three stages, viz: preprocessing, embedding and extraction. RGB image is converted to YCbCr to ensure the best imperceptibility and robustness. In spatial domain, the best quadrant of host image is selected by applying canny edge detection to ensure that the selected quadrant contains the highest number of edges. In frequency domain, the low frequency sub-band which is exploited to embed the watermark image is selected by applying DWT. The watermarked image was exposed to six types of attacks. It is encouraging to observe that, using standard quality measurements, the technique proposed performs better than those suggested by Kong & Peng [10] and Al-Asmari [1].

Keywords: Hybrid image watermarking, Robustness, Imperceptibility, Canny Edge Detection, Discrete wavelet transform, watermarking attacks.

1. Introduction

Copyright protection has always been a problem for businesses which deal with image records (and also audio as well as video records) over the internet. Due to its wide access, internet facilitates transaction of picture contents stored in digital form. With the ever continuous development of downloading as well as copying and decrypting free application software, easy access to these digital picture contents would mean widespread plagiarisms and hence copyright protection of these digital materials will become increasingly challenging. Digital watermarking provides a way of protecting the rights of the owner of a file. Even if the file is copied and then changed with minor alterations and transformations, the owner can still prove it is his or her original file [7].

Watermarking can either be visible or invisible. Visible watermarking, normally displays special logo or stamp, is used as an identifier of the ownership of the content. In contrary, invisible watermarking is normally embedded in such a way that any alterations made to the pixel value can be detected and the original pixel value as well as the embedded watermark can be recovered with appropriate decoding mechanism. The majority of work done on watermarking recently uses frequency domain [12]. The frequency domain techniques are more popular than spatial domain techniques because working in this domain produces more robust and imperceptible watermarking [5]. Whether using spatial domain or frequency domain, the image is first converted to any of these respective domains before embedding the watermark. In spatial domain, the watermark image is embedded on the whole cover image pixels directly [2]. For cases where the image is not suitable for heavy modification, the modifications could be in the low order bit of chosen pixels [6]. In frequency domain, the methods used to handle watermarking are discrete cosine transform (DCT), discrete Fourier transform (DFT), and discrete wavelet transform (DWT). There are two types of attacks on watermarking; that is intentional or unintentional. Intentional attack refers to the process which tests the ability of the watermark to survive and is normally used to improve the watermarking scheme. Unintentional attack, on the other hand, refers to meta-programming which are intended to attack a watermark so as to ensure that the mark of ownership and originality of digital contents is either obliterated or unrecognizable. Examples of unintentional attacks are:

Geometric, Signal processing and Specialized Attack.

2. Background & Related Works

Many sophisticated software which can be used to download picture contents from the internet, quickly and with ease, are free; and are readily available. As a big percentage of these picture contents are intellectual properties, copyright protection has become a necessity. Watermarking which is a solution to this problem has been proposed by many researchers. Jianhong et al.

[9] proposed one such watermarking technique by using discrete wavelet transform (DWT) which utilised human visual system (HVS) to convert picture content to wavelet packets. Human visual system captures chroma of image because human eyes are less sensitive to chroma than brightness. Down sampling was performed before decomposition with DWT by reducing Cb (blue) and Cr (red) and by taking Y (luminance) which is more resistant to JPEG compression, than Cb and Cr. Ganic & Eskicioglu's [8] watermarking overcame unintentional attacks by decomposing the luminance component using 2 level DWT, and the binary watermark was embedded in the diagonal components of the DWT. Four host images of size 512 x 512 pixels were used in their experiments. Ganic & Eskicioglu's technique was able to overcome, to a degree, attacks by JPEG compression. However, this technique was not hardy against geometric attacks such as filtering, rescaling and gaussian blurring. Al-Asmari et al. [1] suggested using ownership verification application. Optimal pyramid transform (OPT), digital scrambling and rotation of watermark image were utilised in this method to increase security level. Al-Asmari's OPT employed multi-scale signal representation to produce error images which were, selectively or entirely chosen as input to the DWT. The watermark was embedded in the higher sub-bands coefficient. The watermarked image was then reconstructed using inverse discrete wavelet transform (IDWT). Color image with 512 x 512 pixels size was used for the experiment. This method entailed more involved computation due to the combined process of both OPT and DWT. It embedded watermark image in the green channel which is more sensitive to human eyes than the blue channel. Self-embedding watermarking was the solution proposed by Qiang and Hongbin [13] to minimize the effects of unintentional attacks. In this technique, a compressed original image was embedded on to itself as a watermark image. Three RGB channel components of the original image were extracted. DWT was applied on to each channel component. DWT output from each channel was multiplied by a fixed coefficient to produce the watermark information for that channel. For each channel, the watermark information was embedded on to its DWT output. For security purposes, each channel will have its own unique value of fixed coefficient. This method was proposed to improve recent self-embedding methods which had problems regarding robustness and imperceptibility. Kong and Peng [10] chose a watermarking method based on HSI color space with DWT. H, S and I represent hue, saturation, and intensity respectively. HSI color space is designed based on the human visual perception; hence, it is more efficient when used for interpreting and describing colors. In this method, each of the RGB components of an image was converted to its HIS constituent parts. These were then embedded on to the intensity of host image according to the HVS. DWT was applied using Haar filter to decompose cover image. This method however was found to be weak against Sharpening attack. Chavan et al. [3] indicated that digital color image watermarking could be carried out by embedding color watermark on to color host image. Experiments involving the proposed method were performed in the frequency domain by using a combination of DWT and DCT on the host image. Firstly DWT was applied on host image, and then DCT was applied on to the middle frequencies (LH and HL), sub-bands of DWT. The algorithm renders the watermarking to be adequately robust against some attacks like image compression (JPEG), image editing, cropping and salt & pepper noise. However, it is weak against Gaussian noise and geometric distortions.

Table2.1: Summary Of Related Work.

Year	Author	Result	Remark
2008	Jianhong et al.[9]	Good against JPEG Compression not good against some geometric Attacks	Embedding in diagonal component is not robust against rescaling, Gaussian noise, JPEG2000 compression, and Gaussian blur attacks[8].
2009	Al-Asmari et al.[1]	Good against Gaussian and Salt & Pepper noise. Not robust against JPEG compression at quality factors less than 50.	The method has expensive computation cost, embedding in green channel which is more sensitive to human eyes than blue channel
2010	Qiang and Hongbin. [13]	The robustness good in general but PSNR values are low.	The author doesn't coNCCern human visual system in proposed method which is important in watermarking systems
2010	Kong and Peng.[10]	Not robust against Rotation and PSNR low against Sharpening attack	The author applied one image in the experiments
2010	Chavan et al.[3]	PSNR very low for Gaussian and Cropping attack	Proposed scheme is not very robust against some attacks like Gaussian noise and geometric distortions

3. Methodology

The proposed method of color image watermarking technique covers three stages: Firstly, a RGB color image, which serves as a host is converted to YCbCr color space. This is done because the latter is more robust and has higher imperceptibility than the former. In addition, YCbCr consists of three components namely, luminance (Y), blue chrominance (Cb) and red chrominance Cr). In this study, Cb has been chosen for embedding purposes due to its less sensitivity to HVS. Next, Canny edge detection is applied on the Cb component to seek for the best quadrant that contains the most number of edges. The selected quadrant is then transformed into its frequency domain using DWT that produces LL, HL, LH, and HH sub-bands. Finally, LL is empirically chosen for the embedding to take place.

Secondly, prior to the embedding, a watermark is first prepared by splitting it into four equal parts: these pieces are then randomly embedded in the LL sub-band by using Equation (1) below. Once the process is completed, the embedded quadrant is inverted to its spatial domain using Inverse Wavelet Discrete Transform (IDWT), and is merged with the remaining three quadrants, which together they form an YCrCb image. The image is then converted into RGB color space which serves as the final watermarked image.

$$W' = (H + \alpha w) \qquad (1)$$

Where: W' = watermarked image, H = partitioned original image, w = Watermark, α = Scaling factor.

Finally, the extracting stage involves recovering the watermark from the watermarked image. The procedure is as follows: convert watermarked image from RGB to YCbCr color space, extract Cb component, partition extracted Cb component to four quadrants, apply Canny edge detection on all quadrants, then choose the best quadrant, apply DWT on the chosen quadrant, extract all four watermark pieces from LL sub-band using equation (2) and apply IDWT on selected quadrant, combine Cb quadrants and collect the watermark pieces, combine YCbCr components and finally convert the image from YCbCr to RGB color space.

$$w = (W' - H) / \alpha \qquad (2)$$

Where: W' = watermarked image, H = partitioned original image, w = Watermark image, α = Scaling factor, which is = 0.1.

Details algorithms for the above process are as follow:-

A. Watermarking embedding algorithms

```
Input: RGB host image & RGB watermark image.
Output: RGB watermarked image.
Step – 1 Convert RGB to YCbCr color space.
Step – 2 Extract Cb components.
Step – 3 Partition the image into four quadrants.
Step – 4 Apply Canny Edge Detection.
Step – 5 Select the best quadrant which has the most number of edges.
Step – 6 Apply DWT on the selected quadrant.
Step – 7 Select (LL) sub-band.
Step – 8 Partition the watermark into 4 parts; embed them using eq.(1).
Step – 9 Apply IDWT on the selected quadrant.
Step – 10 Merge all the quadrants.
Step – 11 Reconstruct YCbCr.
Step – 12 Convert YCbCr to RGB.
```

B. Watermarking extracting Algorithm

```
Input: RGB Watermarked Image.
Output: Watermark Image.
Step – 1 Convert RGB to YCbCr color space.
Step – 2 Extract Cb components.
Step – 3 Partition the image into four quadrants.
Step – 4 Apply Canny Edge Detection.
Step – 5 Select the best quadrant which has the most numbers of edges.
Step – 6 Apply DWT on quadrant.
Step – 7 Extract watermark pieces, eq.(2).
Step – 8 Combine watermark pieces.
```

4. RESULTS AND DISCUSSION

The proposed technique has been applied by using two standard 512 x 512 pixels host color images of Lena and Baboon, and by using 32 x 32 pixels watermark image. Peak Signal to Noise Ratio (PSNR) is used to measure the quality ratio between the signal of original host image and watermarked image to determine the quality before and after attack. The minimum value for PSNR should not be less than 30 for perceptual fidelity [4]. Human Visual System (HVS) was employed in the proposed technique to get maximum hiding level. Human eyes have different sensitivity degrees for different image areas because each part of the image has its own properties. To increase invisibility of watermark image, the busier area which contains more edges has been chosen for embedding (Tables 4.1 – 4.2 & Figures 4.1 – 4.2).

Image Quadrants	Number Of Edges
Q-1	666
Q-2	908
Q-3	1262
Q-4	1259

Table 4.1 : Number of detected edges in Lena image.

Image Quadrants	Number Of Edges
Q-1	1503
Q-2	810
Q-3	2158
Q-4	678

Table 4.2 : Number of detected edges in Baboon image.

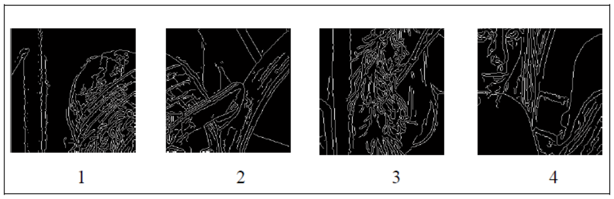

Figure 4.1: Partitioned Lena image with detected edges.

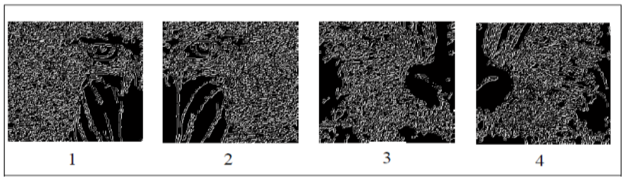

Figure 4.2 : Partitioned Baboon image with detected edges .

Correlation is used to measure the robustness by evaluating the difference between original watermark and extracted watermark which has been passed through the different types of attacks such as noise, geometric and filtering assaults. Figures 4.3 – 4.6 depict the performances of the proposed technique:

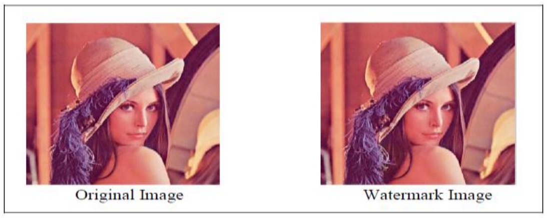

Figure 4.3 : Original and watermarked Lena.

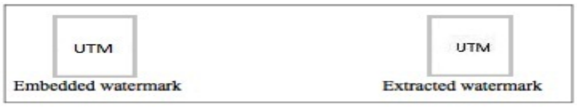

Figure 4.4 : Extracted watermark from Lena Image.

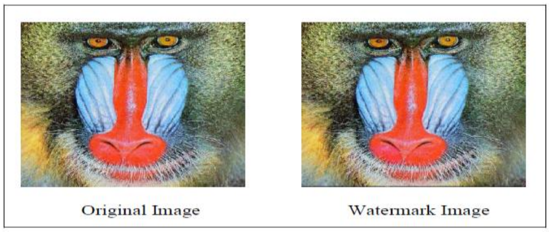

Figure 4.5 : Original and watermarked Baboon.

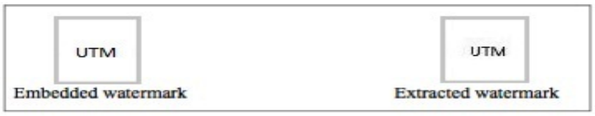

Figure 4.6 : Extracted watermark from Baboon Image.

4.1 Before attack results

The following table shows the result before attacks on both Lena and Baboon images respectively.

Image	PSNR	Correlation
Lena	48.70	0.9987
Baboon	47.39	0.9987

Table 4.3: Lena & Baboon images results Before Attacks

4.2 After attack results

When the attacks are Gaussian noise, Salt & Peppers, Sharpening, Median filter, Rotation and JPEG compression, the key measurements are as in Tables 4.4 – 4.9.

Ratio	0.01%		0.02%		0.03%	
Measurements	PSNR	NCC	PSNR	NCC	PSNR	NCC
Lena	20.17	0.9987	20.07	0.9972	19.87	0.9972
Baboon	20.20	0.9984	20.09	0.9818	19.90	0.9974

Table 4.4: Gaussian noise attack results.

Ratio	0.01%		0.02%		0.03%	
Measurements	PSNR	NCC	PSNR	NCC	PSNR	NCC
Lena	25.09	0.9931	22.20	0.9914	20.40	0.8663
Baboon	25.09	0.9987	22.06	0.9777	20.34	0.9557

Table 4.5 : Salt & Pepper noise attack results.

Measurements	Lena	Baboon
Correlation	0.8431	0.9987
PSNR	25.91	15.80

Table 4.6 : Sharpening attack results.

Measurements	Lena	Baboon
Correlation	0.9987	0.9987
PSNR	31.21	19.56

Table 4.7 : Median Filter attack results.

Ratio	1		2		3	
Measurements	PSNR	NCC	PSNR	NCC	PSNR	NCC
Lena	21.10	0.9987	18.20	0.9737	16.69	0.9987
Baboon	14.82	0.9987	14.22	0.9987	13.70	0.9987

Table 4.8 : Rotation attack results.

Ratio	10		30		60	
Measurements	PSNR	NCC	PSNR	NCC	PSNR	NCC
Lena	33.37	0.9987	38.38	0.9987	42.33	0.9987
Baboon	26.29	0.9987	34.02	0.9987	37.13	0.9987

Table 4.9 : JPEG Compression attack results.

Finally, when tested using Lena and Baboon images, PSNR was found to be larger than 45 which indicates that the proposed technique has a performance that is close to near optimum [4].NCC for Baboon images was found to be larger than 0.99 before any attack but produced a measured figure of not less than 0.95 after all the attacks (worst possible case).NCC for Lena images was 0.99 before any attack but registered a value of not less than 0.95 for all attacks except when assailed by Salt & Pepper (0.03%) attack and Sharpening attack.

4.3 Comparison

In the proposed technique, a watermark is embedded on to the cover image using discrete wavelet transform. According to Lubin et al, Megalingam et al, Qiang et al and Shi et al [11,14] the low frequency areas are more robust than high and middle frequency areas but more sensitive to the human visual system. These two properties are the principle behind the proposed technique. This technique optimally searches for the best quadrant for embedding on to the host image and chooses a blue channel to gain more invisibility (with reference to the human visual system). To gain robustness, it embeds the watermark in the low frequency sub-band (LL). This strategy helps the proposed technique have the advantage of invisibility and robustness while, at the same time, making the embedding process simple and easy to implement. It is hoped that ongoing research which will implement the use of DWT for embedding and extracting RGB images, will result in improved efficiency of the proposed technique. The proposed technique is compared to the system suggested by Kong and Peng [10] and to that proposed by Al-Asmari [1]. Comparison of key analytical quality measurements between the proposed technique to the system suggested by Kong and Peng are as in Tables 4.10 – 4.14. Comparison between the proposed technique to that proposed by Al-Asmari is displayed in Tables 4.15 – 4.16)

4.3.1 Comparative with Kong and Peng [10].

Measurements	Proposed Technique (Lena)	Kong & Peng,[10]
Correlation	0.9987	0.9242
PSNR	20.17	28.20

Table 4.10 : Gaussian noise with (0.01%) of density.

Measurements	Proposed Technique (Lena)	Kong & Peng,[10]
Correlation	0.9914	0.9018
PSNR	22.06	25.08

Table 4.11 : Salt & Pepper with (0.02%) of density.

Measurements	Proposed Technique (Lena)	Kong & Peng,[10]
Correlation	0.8431	0.8902
PSNR	25.91	18.34

Table 4.12 : Sharping attack result.

Measurements	Proposed Technique (Lena)	Kong & Peng,[10]
Correlation	0.9737	0.7933
PSNR	18.20	27.58

Table 4.13 : Rotation with (2°)degrees.

Measurements	Proposed Technique	Kong & Peng,[10]
Correlation	0.9987	0.8375
PSNR	35.32	30.32

Table 4.14 : JPEG Compression with (20%)of quality factor.

4.3.2 Comparative with Al - Asmari et al,[1].

Measurements	Proposed Technique	Al - Asmari et al,[1]
Correlation(Lena)	0.9987	0.90
Correlation(Baboon)	0.9984	0.98

Table 4.15: Gaussian noise attack results.

Measurements	Proposed Technique	Al - Asmari et al,[1]
Correlation(Lena)	0.9931	0.91
Correlation(Baboon)	0.9987	0.98

Table 4.16: Salt & Pepper noise attack results.

5. CONCLUSION

In this paper a new technique which improves watermarking applications is proposed. The new technique fulfills the three requirements which are important to watermarking, namely: imperceptibility, robustness and capacity. Current research work is focused on an investigation to see if it is advantageous to embed horizontal edges of watermark image on to the horizontal edge parts of cover image. Finding the best ratio between the high frequency and low frequency parts of the watermark image and sorting out which part is suitable for embedding on to the cover image for both high and low frequency bands, is a challenge.

References

[1] Al-Asmari, A. K. and Al-Enizi, F. A., A Pyramid-Based Watermarking Technique for Digital Color Images Copyright Protection, International Conference on Computing, Engineering and Information, (2009) 978-0-7695- 3538.

[2] Chaelynne M.W., Digital Watermarking, School of Computer and Information Sciences Nova Southeastern University, 2001.

[3] Chavan, S. Shah, R. Poojary, R. Jose, J. and George, G. A., Novel Robust Colour Watermarking Scheme for Color watermark images in Frequency Domain, International Conference on Advances in Recent Technologies in Communication and Computing, (2010) 978-0-7695-4.

[4] Chin, Chen. C. Yung. C. C. and Tzu, C. L, A Semi-blind Watermarking Based on Discrete Wavelet Transform, Proceedings of the 9th International Conference Information and Communications Security, Zheng zhou, China, (2007) 164-176.

[5] Cox, I. J. Miller, M. L. Bloom, J. A. Fridrich, J. and Kalker, T., digital watermarking and steganography, 2nd. Ed. morgan kaufmann publishers, 2008.

[6] El-Gayyar, M., Watermarking Techniques Spatial Domain Digital Rights Seminar, Ph.D. Thesis, Media Informatics University of Bonn Germany, 2006.

[7] Eric Cole. and Ronald D. Krutz, Hiding in Plain Sight: Steganography and the Art of Covert Communication, Wiley Publishing, Inc.,(2003) 86-87.

[8] Ganic, E. and Eskicioglu A. M., Robust DWT-SVD Domain Image Watermarking: Embedding Data in All Frequencies, Department of Computer and Information Science Department of Computer and Information Science, (2004) ACM 1-58113-854.

[9] Jianhong, S. Junsheng, L. and Zhiyong, L., An Improved Algorithm of Digital Watermarking Based on Wavelet Transform, World Congress on Computer Science and Information Engineering, (2009) 978-0-7695-3507-4/08.

[10] Kong, F. and Peng Y., Color Image Watermarking Algorithm Based On HSI Color Space, the 2nd International Conference on Industrial and Information Systems, 2010.

[11] Lubin, J. Bloom, J. A. and Cheng, H., Robust content-dependent high- fidelity watermark for tracking in digital cinema, In proceedings of The International Society for Optical Engineering, Security and watermarking of multimedia content 5th conference, Vol. 5020, 2003, pp. 536-545.

[12] Megalingam, R. K. Nair, M. M. Srikumar, R. Balasubramanian V. K. and Sarma V. S. V. A., Comparative Study on Performance of Novel, Robust Spatial Domain Digital Image Watermarking with DCT Based Watermarking, International Journal of Computer Theory and Engineering, 2(4) (2010) 8201.

[13] Qiang, S. and Hongbin, Z., Color Image Self-Embedding and Watermarking Based on DWT, International Conference on Measuring Technology and Mechatronics Automation, 2010.

[14] Shi, Y. Q., and Sun, H., Image and video compression for multimedia engineering Fundamentals, algorithms and standards, 1999.

First Author was born in May 21, 1958 Malaysia. He received his Ph.D. Computing 1989 University of Wales College of Cardiff (UWCC), Wales, U.K., M.Sc. Computing 1982 University of Wales College Cardiff (UCC), Wales, U.K., B.Sc. Statistic 1979 UKM, Malaysia. Currently he is a Professor in Image Processing.

Second Author (**Corresponding author**) was born in Aug, 20, 1980 Iraq. He received his **M.Sc.** Computer Science 2005 University of Al-Mustansiria, Baghdad .Iraq, **B.Sc.** Computer Science 2002 University of Al-Mustansiria, Baghdad .Iraq, Currently he is a Ph.D. student in University of Technology Malaysia (UTM),Johor, Malaysia . is a member of the IEEE and the IEEE Computer Society.

Third Author has received a B.Sc. (Hons.) in IT from Teesside University, U.K. and M.Sc. in Distributed Multimedia Interactive Systems from Lancaster University, U.K. in 1997 and 1998, respectively. He has received a Ph.D. degree from Osaka Prefecture University, Japan in 2003. Currently, he is an associate professor and IT Manager at the School of Graduate Studies (SPS), UTM and the head of Software Engineering Research Group (SERG), K-Economy Research Alliance, UTM. He is the editors of International Journal of Digital Content Technology and its Applications (JDCTA) and International Journal of Advancements in Computing Technology (IJACT).

Fourth Author has received a B.Sc.in computer science from Al-Mousel University, Mousel, Iraq. He received his M.Sc. in Computer Science from University of Technology Malaysia (UTM),Johor ,Malaysia in 2011.

Fifth Author has received a B.Sc. (Hons.) in Mathematics from Sriwijaya University 1993. and M.Sc. in Informatics ITB in 2000. He has received a Ph.D. degree from University of Technology Malaysia (UTM) in computer science in 2012.