A Dual watermarking technique for images with encryption

Ghassan Sabeeh Mahmood, Huang Dong Jun, Baidaa Abdulrahman Jaleel

Abstract— Digital watermarking is a technology to ensure and facilitate data authentication, security and copyright protection of digital media. In this paper, we employ a dual image watermarking and cryptography to achieve the requirements of robustness and security. In this method, the first watermark is encrypted by using a secret key and embedded it into the second watermark and then the result is embedded into the cover image. As well as we take some data from the cover image and add it to the second watermark to confirm the validity of the cover file and reliability of watermark. Also, we hide the secret key into the second watermark for more safety. Finally, experimental results reveal the effectiveness of the proposed method.

Index Terms— Watermarking, Least Significant Bit (LSB), Encryption, Decryption.

1 Introduction

THe explosive growth of digital multimedia techniques and the wide distribution of digital images over the Internet have made digital media easily available, however these media can be attacked and modified readily during transmission [1]. Digital watermarking techniques provide the solution to this problem [2]. Digital watermarking is a process to embed some information called watermark into different types of media called Cover [3]. The process of embedding information into another object can be called as watermarking. Watermarking is mainly used for copy protection and copyright-protection [4], [5]. For any watermarking technique to be valid, it must satisfy three important requirements: perceptual invisibility, robustness against various image processing attacks, as well as security [6].

Security and capacity of watermark data are very important issues to be taken into account. Watermarking is a research field of copyright protection and authentication of electronic documents and media. Most of the research is going on in this field, especially in the field of image watermarking. The reason might be that there are a lot of images are available on the Internet that needs to be protected [7]. The watermark pattern in the marked image can be either visible or invisible, the visible watermark is limited in many applications. It distorts the original image and is susceptible to attack through direct image processing [8]. Watermarks are sure to serve an important role in the future of intellectual property rights with the growing threat of piracy in the Internet and copyright infringement cases [4].

In this paper, we propose a dual digital watermarking technique for watermark embedding and extraction by using the least significant bit in a spatial domain to hide information in digital images. In this method, the first watermark is encrypted and embedded into the second watermark and this dual watermark (watermark embedded into another watermark) is finally embedded into the main cover image.

Our method can attain the security of the scheme due to the encryption of watermarks. It also increases the embedding capacity of a watermark due to the use of dual watermark.

The rest of this paper is organized as follows. Section 2 reviews the related works. While section 3 introduces the proposed method and the proposed algorithm in detail. Section 4 presents the experimental results. Concluding remarks are given in Section 5.

2. Related Works

This section describes the previous works which had been done on digital watermarking.

[9] Proposed an algorithm is based on Dual Intermediate Significant Bit (DISB) model. In this algorithm 2 keys (k1 and k2 such that k2>k1) are used in the process of embedding. The extracting process has been done after

- *Ghassan Sabeeh Mahmood is a master's degree student in school of information science and engineering in central south university, china - and lecturer in computer science in Diyala University, Iraq.*
- *Huang Dong Jun is a Professor in school of information science and engineering in central south university, china.*
- *Baidaa Abdulrahman Jaleel is a BSc graduate from Computer Science, Diyala University, Iraq.*

applying some types of attacks. This method concentrates on the greatest quality of the watermarked image.

[10] Proposed a method based on multiple watermarks in which two different watermarks are embedded at the same time in the intermediate significant bits of the host image pixels.

[5] Proposed a novel copyright protection scheme for digital images of any size based on visual cryptography and statistics. This is done by sampling distribution of means and visual cryptography to achieve the requirements of robustness and security. This method can register multiple secret images, without altering the host image and can identify the rightful ownership without resorting to the original image.

[11] proposed Comparative study of single watermarking to multiple watermarking over a color image. This study shows that multiple watermarks provide extra protection by embedding more than one watermark on the image.

[12] proposed watermarking based on the least significant bits (LSBs) of medical image, in which a set of data is embedded into a medical image. This method is used to check the integrity and confidentiality of medical information and to maintain confidentiality for patient and hospital data.

3. Proposed Method

In this paper, we propose a dual digital watermarking technique. "Dual digital watermark" is meant embed watermark into another watermark. In this method, the first watermark is encrypted (using XOR Algorithm, by generating a secret key) and then embed the encrypted watermark into the second watermark, finally the result is embed it into the main cover image, as well as we take some of the data from the cover image and embed it into the second watermark to test the validity of the cover file and reliability watermark. Also, we embed the secret key into the second watermark for more safety.

This method provides high security for watermarks because of the encryption of watermark. It also increases the embedding capacity of a watermark because of the use a dual watermark.

In this paper, we adopted the spatial domain by using the least significant bit to hide information in digital images.

3.1 Watermark Embedding Algorithm

The algorithm for hiding the dual watermark is as follows:

Input:

Watermark 1 – A binary image (the first watermark).

Watermark 2 – A grayscale image (the second watermark).

Cover Image – Color image to be watermarked.

K1 – key1: Used for encrypting Watermark1.

K2 – key2: Used for signature.

Output:

Watermarked2 – Final watermarked image.

Embedding Algorithm

1. Begin.

2. Read the first watermark image (Watermark1) and encrypt it by performing the XOR operation with the key1 (K1). The output of this step is called Encrypted1.

3. Read the second watermark image (Watermark2).

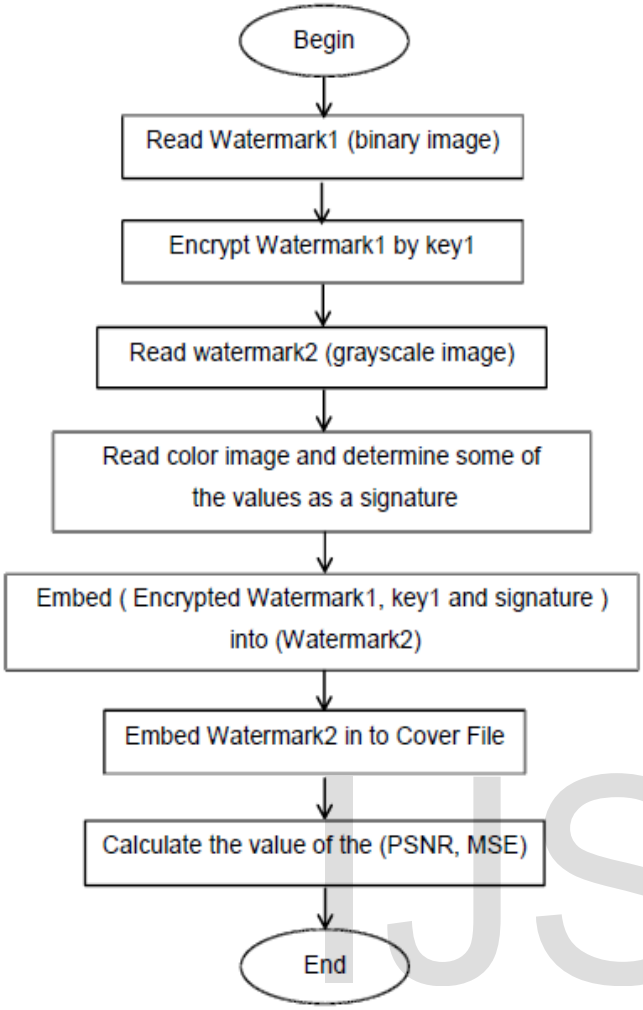
4. Read the cover image (color image) and take some of the data from it as a signature to test the validity of the cover file and the reliability watermark by key2 (K2).

5. Embed Encrypted1 and the keys $(K1, K2)$ into (Watermark2), Let output image be Watermarked1.

7. Embed Watermarked1 into the Cover Image. The output image is a final watermarked image (Watermarked2).

8. Calculate the value of Peak Signal To Noise Ratio (PSNR) and Mean Squared Error (MSE).

9. End.



Flowchart (1) the process of hiding dual watermark

3.2 Watermark Extraction Algorithm

The algorithm for extracting the dual watermark is as follows:

Input:

Watermarked2 –Is the received watermarked image.

K1 – key1: Used for decrypting recovered watermark from (watermark2).

K2 – key2: Used for signature.

Output:

Recovered2 – Watermark2 recovered from the received watermarked image.

Recovered1 – Watermark1 recovered from the watermark2.

Extraction Algorithm

1. Begin.

2. Read the Watermarked2 (received watermarked image) and apply a procedure to extract watermark2 from it, say the recovered image is Recovered2.

4. Extract (K1, K2) from Watermarked2.

5. Compare the values of the real signature with the values retrieved from the second watermark by the key2, if the values are equal that means the cover contains watermarks is correct.

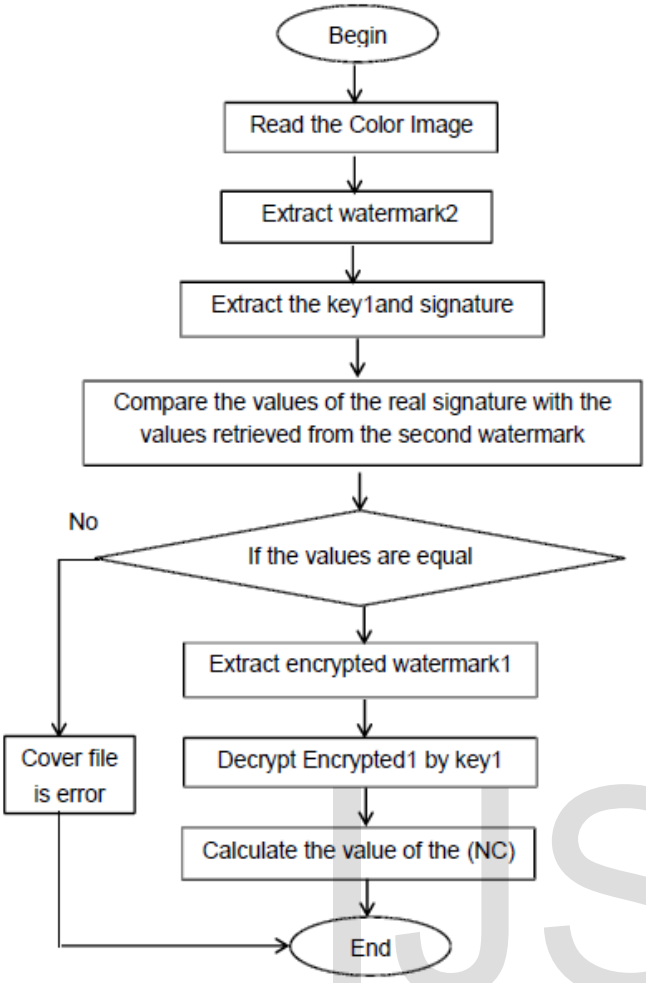
6. If the values are not equal that means the cover is incorrect, go to step (10).

7. Extract encrypted watermark1 from Recovered2. Image recovered is called Encrypted1.

8. Decrypt Encrypted1 using XOR with key (K1), output of this step is called Recovered1 (watermark1).

9. Calculate the value of the Normalization Correlation (NC).

10. End.



Flowchart (2) the process of extraction dual watermark

4. Experimental Results

In this paper, we adopted a number of measures (proposed by [13], [14] for the purpose of measuring the quality of images resulting from the algorithms which are:

1- Mean Squared Error (MSE) :

$$MSE = \frac{1}{M*N} * \sum_{ij}\left(sw(I,j) - s(I,j)\right)^2$$

2- Peak Signal To Noise Ratio (PSNR) :

$$PSNR = 20*\log 10\left(\frac{255}{\sqrt{\frac{1}{M*N}\sum_i\sum_j(sw(i,j)-s(i,j))^2}}\right)$$

The Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR) are the two error metrics used to compare image quality. This ratio is often used as a quality measurement between the original and a watermarked image. If one of the signals is an original signal of acceptable quality, and the other is a distorted version of it whose quality is being evaluated, then the MSE may also be regarded as a measure of signal quality.

3- Normalization Correlation (NC) :

$$NC = \sum_i sw(i) * s(i) / \sum_i (s(i))^2$$

Normalized Correlation is one of the metrics used to calculate the matching ratio by the following equation:

Where:

SW: Represents the values of array that contains the watermark.

S: The original array values.

M: Represents the number of rows.

N: Represents the number of columns.

We adopted the spatial domain by using the least significant bit to hide dual watermarks in digital images, table (1) shows the values of (MSE, PSNR), where the cover uses different types of images while the watermarks uses different sizes of images.

Example for the process of hiding and the extraction of dual watermark can be seen in Figure 1, Figure 2.

Type of Image			JPEG	BMP
Image Size 128x128	MSE	Gray image	0.0839	0.2068
		Color image	0.0879	0.0867
	PSNR	Gray image	58.8930	54.9743
		Color image	58.6894	58.7511
Image Size 256x256	MSE	Gray image	0.0838	0.2014
		Color image	0.0894	0.0895
	PSNR	Gray image	58.8980	55.0899
		Color image	58.6198	58.6102
Image Size 512x512	MSE	Gray image	0.0836	0.2493
		Color image	0.0891	0.0903
	PSNR	Gray image	58.9093	54.1639
		Color image	58.6330	58.5720

Table (1): shows the values of (MSE, PSNR)

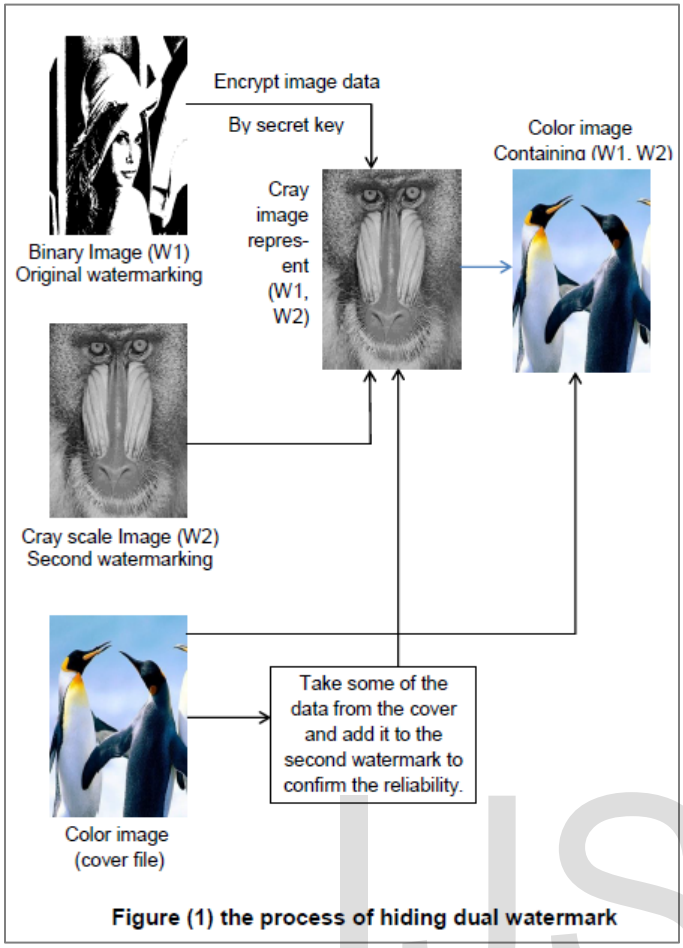


Figure (1) the process of hiding dual watermark

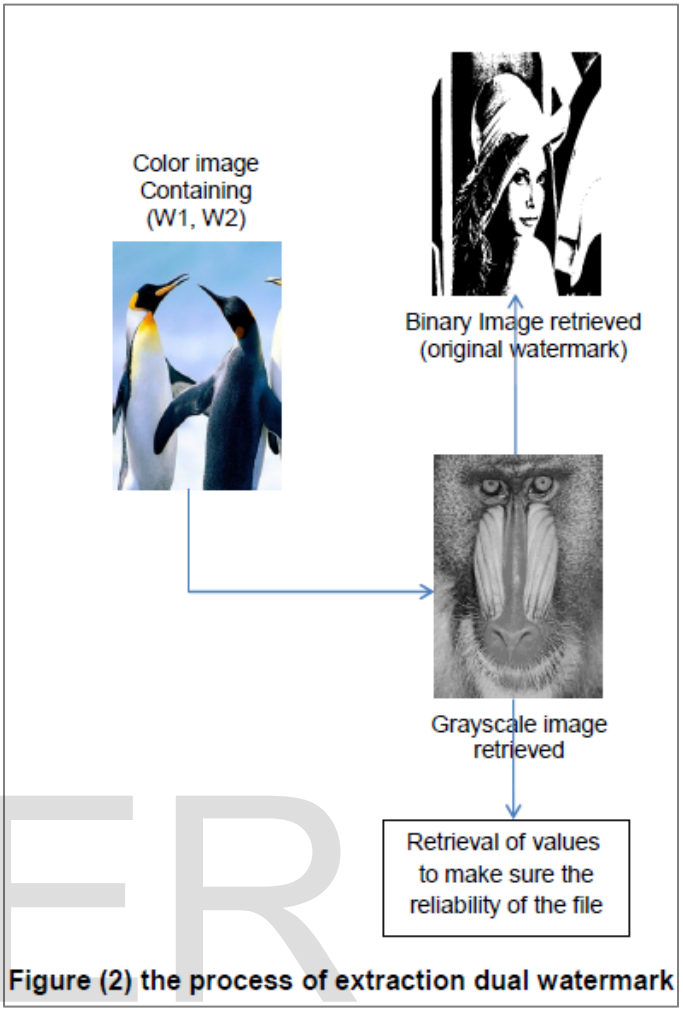


Figure (2) the process of extraction dual watermark

The above proposed method was executed using the Matlab R2012a software.

5. Conclusion and Future Work

In this paper, a new technique of digital watermarking is proposed in which a watermark is encrypted and embedded into another watermark and this combined watermark is embedded into the main image. This phenomenon of embedding one watermark into another is known as "Dual watermarking". By doing so, the level of security of the watermark increases (due to use of encryption and decryption technique) and the embedding capacity of the watermark is also enhanced (due to use of Dual watermarks).

The proposed algorithm has been applied on images of different sizes and more than one type where the values of the Normalization Correlation (NC) equal to the (1). The distortion unconsciously suggesting that the image recovered and the values of the signature were completely identical, and this shows the efficiency of the performance of the algorithm to hide the watermark.

So in the future, some other algorithms can be used or proposed for embedding of watermarks and encryption or decryption.

References:

[1] Chih-Hung Lin, Ching-Yu Yang, "Multipurpose Watermarking Based on Blind Vector Quantization (BVQ)", Journal of Information Hiding and Multimedia Signal Processing 2011 ISSN 2073-4212 Ubiquitous International Volume 2, Number 3, July 2011.

[2] Khaled Loukhaoukha, Jean-Yves Chouinard, and Mohamed Haj Taieb, "Optimal Image Watermarking Algorithm Based on LWT-SVD via Multi-objective Ant Colony Optimization", Journal of Information Hiding and Multimedia Signal Processing 2011 ISSN 2073-4212 Ubiquitous International Volume 2, Number 4, October 2011.

[3] B Surekha, Dr GN Swamy, "A Spatial Domain Public Image Watermarking", International Journal of Security and Its Applications Vol. 5 No. 1, January, 2011.

[4] R.Dhanalakshmi , K.Thaiyalnayaki " Dual Watermarking Scheme with Encryption ", (IJCSIS) International Journal of Computer Science and Information Security, Vol. 7, No. 1, 2010.

[5] Ching-Sheng Hsu, Young-Chang Hou, "Copyright protection scheme for digital images using visual cryptography and sampling methods", Optical Engineering 44 (7), 077003 (July 2005).

[6] Maha Sharkas, Dahlia ElShafie, and Nadder Hamdy, "A Dual Digital-Image Watermarking Technique", World Academy of Science, Engineering and Technology 5 2007.

[7] Preeti Gupta, "Cryptography based digital image watermarking algorithm to increase security of watermark data, International Journal of Scientific & Engineering Research", Volume 3, Issue 9, September 2012 ISSN 2229-5518.

[8] Ren-Junn Hwang," A Digital Image Copyright Protection Scheme Based on Visual Cryptography", Tamkang Journal of Science and Engineering, Vol. 3, No. 2, pp. 97-106 (2000).

[9] Ghassan N. Mohammed, Azman Yasin, and Akram M. Zeki, "Improvement of the Quality for Digital Image Watermarking Based on Dual ISB", International Conference on IT Convergence and Security, Dec. 2013.

[10] MIR Shahriar Emami, Ghazali Bin Sulong, and Salbiah Binti Seliman, "A Novel Multiple Semi-Blind Enhanced ISB Watermarking Algorithm Using Watermark BIT-Pattern Histogram for Copyright protection", International journal of Innovative computing information and control, volume 8, Number 3 (A), March 2012.

[11] Kiratpreet Singh Dhaliwal , Rajneet Kaur," Comparative study of single watermarking to multiple watermarking over a color image", International Journal of Latest Trends in Engineering and Technology (IJLTET), Vol. 2 Issue 2 March 2013.

[12] Mohamed Ali HAJJAJI, Abdellatif MTIBAA, and El-bey BOURENNANE, "A Watermarking of Medical Image: Method Based "LSB" ", Journal of Emerging Trends in Computing and Information Sciences, VOL. 2, NO. 12, December 2011.

[13] Deepshikha Chopra, Preeti Gupta, Gaur Sanjay B.C. and Anil Gupta," Lsb Based Digital Image Watermarking For Gray Scale Image", IOSR Journal of Computer Engineering (IOSRJCE)ISSN: 2278-0661, ISBN: 2278-8727 Volume 6, Issue 1 (Sep-Oct. *2012)*, *PP 36-41*.

[14] H. Seddik, M. Sayadi, F. Fnaiech, and M. Cheriet, (2007), "New multi-domains image watermarking method based on multi-water marks embedding and neural network segmentation, Applied mathematical sciences, vol. 1, no. 39, pp. 1927-1939.