IRAQI JOURNAL OF APPLIED PHYSICS
IJAP, Vol. 10, No. 3, July-September 2014, pp. 3-5

A Novel Secure Digital Watermark Generation from Public Share by Using Visual Cryptography and MAC Techniques

Bashar S. Mahdi
Alia K. Abdul Hassan

Department of Computer Science, University of Technology, Baghdad, Iraq

Digital image watermarking is a technique in which a secret watermark is embedded into the original image to make an assertion about the image ownership and discouraging unauthorized copying. In this paper, a novel watermark was generated from public share using proposed visual cryptography scheme with Message Authentication Code (MAC) which is applied into a secret image (logo binary image). The proposed work was applied to provide the copyright protection and authentication of a digital image. Experimental results demonstrated that the proposed scheme has maintained the original pixel expansion, achieved a reduction of the watermark size, and allowed high security, high capacity, good feasibility, imperceptibility and robustness against several types of attacks.

Keywords: Watermarking, DCT, MAC, Visual Cryptography, Hash function
Received: 5 November 2014; **Revised**: 5 December 2014; **Accepted**: 12 December 2014

1. Introduction

Visual cryptography is an approach used to decrypt secret images by using the human visual system without any cryptography computations [1]. Visual cryptography is a kind of secret sharing which shares a secret into a number of shares so that the cooperation of a predetermined group of shareholders reveals the secret whereas the secret reconstruction is impossible for any unauthorized set of the shareholders [2]. Visual cryptography uses the human visual system (HVS) to read the secret message from some interlaced shares, and can create different shares of binary images from the secret message. The extraction of any information about a secret message from individual created shares is very difficult. However, the secret message information can only be revealed when overlapping the created shares. The digital watermarking techniques are very useful to protect the digital media (text, image, video and audio) from unauthorized copying of data. We can introduce the digital image watermarking as a technique in which a secret watermark is embedded into the host image to make an assertion about the host image ownership and discouraging unauthorized copying [3]. The watermarking schemes are broadly classified into two main domains; spatial and the transform domains. In spatial domain, the watermark is embedded by directly modifying the intensity values of the cover image. The most popular technique is the Least Significant Bit (LSB) method. In transform domain, the watermark is embedded by modifying the frequency coefficients of the transformed image. The common methods are Fourier Transform (DFT), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT) [4]. There are, however, some drawbacks of generating secret sharing from the watermark image using visual cryptography techniques. One of these drawbacks is the pixel expansion which causes a duplication of the watermark size (influenced by the covered image size and its imperceptibility). The other drawback, when using standard and many proposed visual cryptography techniques, is the random selection of the share pattern without any security and authentication key. These drawbacks can be presumably resolved the proposed scheme of this paper. The work of reference [5] is the earliest method proposed to take the properties of VC and produce copy protection of the digital image. Other related works have depended on the idea of [5] as a base to propose other schemes [6] [7] [8] [9]. In the current work, a visual cryptography technique is proposed to generate image share by combining a cryptographic hash function and some fashion with a secret key; Message Authentication Code (MAC). It generates a novel invisible watermark from a visible logo image; usually protected from malicious attacks. The generated watermark is embedded inside the cover image with a reduced number of bits needed for representing the invisible watermark and providing more robustness and capacity for the embedding process. The invisible and blind watermarking technique employs the middle band coefficients to hide the generated watermark data and avoid any type of attacks like JPEG compression. In section 2, we describe the concept of Message Authenticated Code (MAC). Section 3 is

 ISSN (printed) 1813-2065, (online) 2309-1673 Printed in IRAQ

a review of Visual Cryptography. Section 4 explains the proposed method of watermark generation, insertion and detection schemes. Section 5 is dedicated to experiment and discuss the results. Finally, conclusions appear in Section 6.

2. Message Authenticated Code MAC

Hash Function (HF) is a one way technique that works on a varying length input O and a fixed-length hash digits output h= HF (O). While it is easy to calculate hash digits, it is difficult to compute O from (h) such that HF (O) = h, and it is also difficult to find another message O` such that HF (O) ≠ HF (O`). There are many types of hashing functions like (MD4, MD5, SHA0, SHA1, SHA2, and SHA3). SHA1 is a good option for (HF) [10]. A message authenticated code (MAC) is a technique which is used to generate a unique code for specific input by using one-way hash function that depends on a secret key(K) [11]. The equation of (MAC) which is used in the proposed system depends on SHA1 function:

$$HV(P,K) = HF(K+HF(P)) \quad (1)$$

where K is a secret key known only to the owner, P is a pixel position, (+) represents concatenation, HF represents the hash function SHA1. HV is the result of MAC. HV produces 160 bits, but selects only two bits; bit number 160 and bit number 100 from the hash value to represent the index of selected share from visual cryptography. All processes of the proposed work are described in section 4.

3. Review of Visual Cryptography

Visual Cryptography can provide the idea of the one-time pad as a perfect and powerful security; the mathematical operations are very simple for encryption and decryption of the image. The decryption or detection depends on the human visual system by overlapping the two encrypted images. The feature about visual cryptography is interesting to provide a perfectly secure [12]. The traditional techniques of visual Cryptography use two sharing images which contain random pixels as a one pad image. The retrieving of secret information from one of the images is impossible because the two sharing images are required to reveal the information. Figure (1a) illustrates the visual cryptography table with expanding and encoding one pixel into four pixels for two shares. These shares represent either diagonals or Horizontal or Vertical.

When a random image contains truly random pixels, it can be seen as a one – time pad system and will offer unbreakable encryption. The principle of the one-time pad is based on the use of one way hash function with a secret key to create a pair of black and white images. Each appears as a randomness of white and black pixels, and no information can be extracted from either image on its own. Unlike most cryptography, it is not merely very difficult to extract information. An implementation of the one-time image principle with true random numbers is perfectly secure and unbreakable.

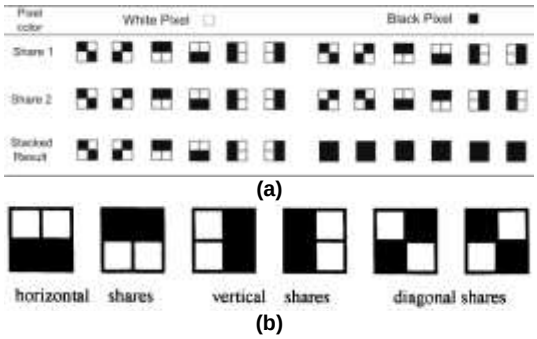


Fig. (1) (a) Visual cryptography sharing and stacking of pixels, and (b) Visual form for each pixel

4. The Proposed Methods

In this work, there are three significant phases: watermark generation, watermark embedding, and watermark extracting .the first and second phases illustrate below in the figure 2.

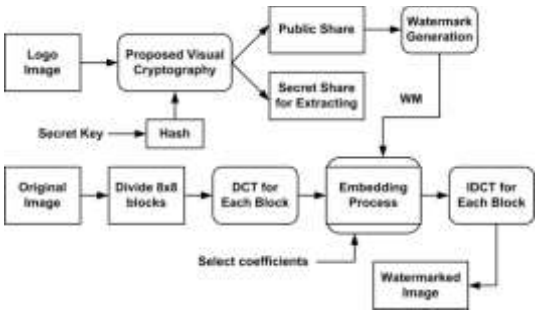


Fig. (2) Block diagram of the proposed watermarking embedding scheme

4.1 Proposed Visual Cryptography

The proposed technique for visual cryptography includes three components. These are:

I. Secret Encoding Table: regarded as a rule for encoding and decoding. It is used for creating the public and secret shares.

II. MAC based on hash function (MAC) is used for selecting the pattern from the Secret Encoding Table.

III. Visual cryptography processes are representation of the encryption (creating sharing images) and decryption (stacking image) processes.

The basic idea of the secret encoding table (table1) is to produce an encoding rule for sharing a single pixel (z) in a binary image (Z) for two shares (s_1) and (s_2). The pixel expansion was chosen as 4 in order to maintain the ratio of the secret image dimensions. There are four possible patterns for a (2 x 2) extended block; all pairs of two extended blocks (s_1, s_2) are for encoding a specific binary pixel (z). The proposed secret encoding table is shown in Table (1). The encoding suggested rules can be summarized as:-

 ISSN (printed) 1813-2065, (online) 2309-1673 Printed in IRAQ

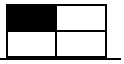
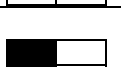
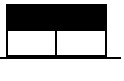
1- If (z) is white pixel, one of the first four rows of Table (1) will be chosen to encode (z) into (s_1) and (s_2) by using the indexing value from the third column.

2- If (z) is black, one of the last four rows in Table (1) will be chosen to encode (z) into (s_1) and (s_2) by using the indexing value from the third column.

3- The last column of Table (1) which represents the reconstructed pixel (s_1, s_2) may contain one, two and three black sub-pixels, and one, two and three white sub-pixels if (z) is white, or all four black sub-pixels when (z) is black.

For more security, there are eight possible patterns from which every block in a sharing image (the selection of the pattern for white or black pixel) performs by using Eq. (1) which uses the secret key (only known by the owner) and one way hashing function to produce 160 binary bits (only two specific bits are selected) to detect the pattern index from the rules in the table (1); so the secret image cannot be indented from a single share. From visual cryptography, two sharing images are produced; public share which is used for the watermarking generation and a secret share which is used for the watermarking extraction.

Table (1) The proposed visual secret sharing

Secret message (z)	Probability	Index	Share1 (s_1)	Share2 (s_2)	Stacked image (s_1,s_2)
White pixel	1/4	00			
	1/4	01			
	1/4	10			
	1/4	11			
Black Pixel	1/4	00			
	1/4	01			
	1/4	10			
	¼	11			

4.2 Watermark generation

The watermark pattern is generated from the content of the public share image by the following steps:

Procedure 1:
Input: logo image, secret key, secret encoding table (table 1).
Output: wm (watermark vector).
Step1: Apply visual cryptography onto logo secret image by using the rules of Table1.
Step2: Generate the public and secret shares from visual cryptography.
Step3: Use a public share image for watermark generation.
Step4: Divide the public share to 2x2 block.
Step5: Select the block for a black pixel by using visual cryptography rules and ignore the block that presents the white pixel by comparing with the rules of Table (1).
Step6: Compute the index of selected block from Table of rules.
Step7: Compute the watermark from concatenated the index of selected block from public share for black pixel
wm = wm + index /* (each index is two bits, + represent the concatenation) .
Step8: If not end of blocks, then go to step5 else go to step 9.
Step9: Represent the (wm) as binary vector used for embedding the process.
Step10: End.

Watermark is generated from only black pixel of logo image and by taking the index of pattern of (2×2) block of public share that is already selected by using Message Authentication Code Eq. (1). The white pixel is already the same in the public and secret shares; therefore, we ignore it, to reduce the redundancy that takes more size in the embedding. The generated watermark from the proposed generation is regarded as a secret after reducing its size to provide the highest robustness and capacity in watermarking algorithms. Figure (3) is a flowchart that explains the details.

4.3 Watermark embedding

The procedure of embedding watermark is illustrated in Fig. (2), and the details of embedding procedure 2 are explained in the following steps:
Procedure2:
Input: Original image, WM (watermark), coefficients position.
Output: X` (watermarked image)
Step1: Divide the original image into 8x8 blocks to produce (L) number of blocks

$$D(u,v)=\frac{2}{\sqrt{MN}}\alpha(u)\alpha(v)\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}f(m,n)\cos\left[\frac{(2m+1)u\pi}{2M}\right]\cos\left[\frac{(2n+1)v\pi}{2N}\right]$$
$$\text{where } \alpha(u)=\begin{cases}\sqrt{1/M} & \text{for } u=0\\ \sqrt{2/M} & \text{for } u=1,2,\ldots,M-1\end{cases}$$
$$\text{and } \alpha(v)=\begin{cases}\sqrt{1/N} & \text{for } v=0\\ \sqrt{2/N} & \text{for } v=1,2,\ldots,N-1\end{cases} \quad (2)$$

 ISSN (printed) 1813-2065, (online) 2309-1673 Printed in IRAQ

Step2: Perform DCT on each block and this can be obtained by using equation 2:
Step3: For i=1 to L /for each block of DCT blocks
Step4: Select the two middle DCT coefficients form 22 middle coefficients in a (8×8) block.
Step5: Take the (AV_i) average of 20 remaining middle Coefficients.
Step6: Embed the watermark bit in the two selected coefficients with embedding weight (α).
Step7: Depending on the generated watermark value (WM):

If $WM_i = 0$, then the two coefficients are modified by equation (3):

$$x'_i = x_i .(1-\alpha * w_i) \Rightarrow x'_i < AV_i \quad (3)$$

Step8: If $WM_i = 1$, then the two coefficients are modified by equation (4):

$$x'_i = x_i .(1+\alpha * w_i) \Rightarrow x'_i > AV_i \text{ ---------- } 4$$

Step9: Next i.
Step10: Produced the watermarked image X` by applying IDCT.
Step11: End.
where X represents the watermarked image, x is DCT coefficient, x` is the modified DCT coefficient, w_i is the watermark bit, WM is the watermark vector, i is the number of blocks, AV is the average value of 22 coefficients, L is the number of blocks, α is the embedding weight and IDCT is the inverse of the DCT transformation.

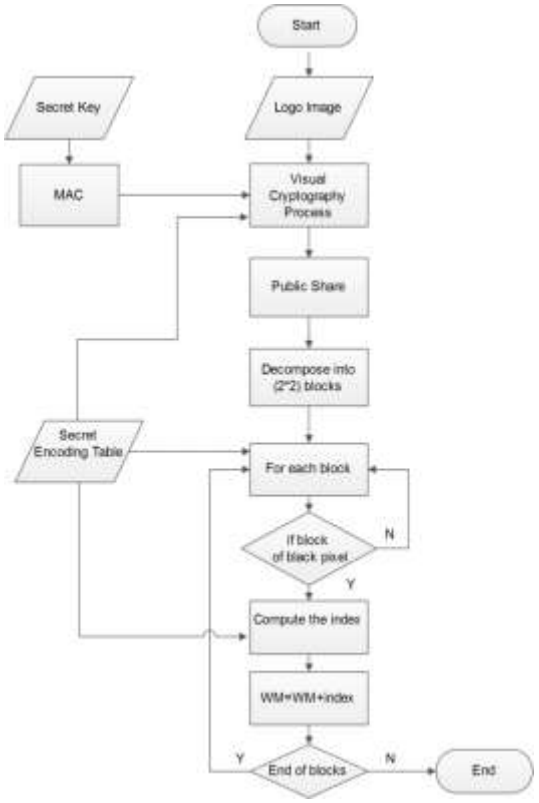


Fig. (3) Flowchart of the proposed watermark generation scheme

4.4 Watermark extraction

The embedded watermark can be extracted from the watermarked image by applying procedure 3 of extraction, see Fig. (4).

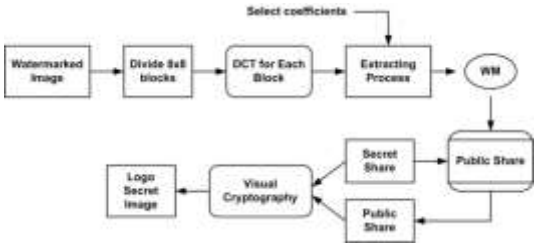


Fig. (4) Block diagram of the proposed watermarking extraction scheme

Procedure3:
Input: X` (watermarked image), secret encoding table (table1), secret share image
Output: Logo image
Step1: Divide the watermarked image into L of (8x8) blocks
Step 2: Apply the DCT for each block of watermarked
Step 3: Compute the average of twenty middle coefficients
Step 4: For i=1 to L /* for each block of DCT blocks
Step5: Depending on the average value (AV_i):
If (AV_i) is greater than one or two selected coefficients then W=0
If (AV_i) is less than one or two selected coefficients then W=1
Step 6: WM=WM+W /* + concatenate operation
Step7: Next i
Step8: Generate the blocks of public share as follows:

- Divide the secret share in to 2x2 blocks
- For each block

- Take 2 bits Sequential form WM vector
- If block is present from white pixel of table1 then Public share block = secret share block
else
Public share block = block represent from 2 bits of WM vector as index of black pixel of table1

Step9: Apply VC (proposed visual cryptography) to overlap the generated public share with secret share to obtain on the final watermark (logo image).
Step10: End.

where X` represents the watermarked image, W watermark bit, WM is the watermark vector, AV is the average value of 22 coefficients and L is a number of blocks.

5. Experimental Results

The proposed method was tested on an original 512 x 512 Lena's image shown in Fig. 8(a). The binary watermark (logo image) to be embedded is of

 ISSN (printed) 1813-2065, (online) 2309-1673 Printed in IRAQ

size 64x64 pixels as shown in Fig. (8b). MATLAB R2012b and visual basic were employed to generate MAC (hashing value for each pixel of the watermark image with the secret key and with its position) to select high security and high randomly pattern from VC table depending on the type of pixel (white or black) pixel. The proposed visual cryptography produces the public share, which is used to generate the watermark to be embedding into the original image and produce the secure share used in the detection phase. These two generated images look like one-time image (random image) and shown in Fig. (11) and Fig. (12). The watermark vector is generated from a public share image by selecting only blocks that represent the black pixel in the logo image. Generated watermark provides the high security and capacity. Security of watermark comes from using of public share image which is one time image. The capacity and robustness are coming from reducing the size of the generated watermark (number of bits) needed to embedding. This was done by modifying the mid band coefficients DCT in the original image.

5.1 discussion and analysis

Our purposed Technique is robust to different attacks like JPEG compression attack, Salt and Pepper attack and Gaussian Noise attack, which are shown in figures (5), (6), (9) and (10). By using the effectiveness measurement for the watermarked and the extracted images, the imperceptibility of the watermarked image is measured by the peak signal-to noise ratio (PSNR) in Eq. (6).

$$\mathrm{MSE} = \frac{\sum_{i=1}^{n}\sum_{j=1}^{m}(xij - x\sim ij\ ^2)}{NM} \qquad (5)$$

$$\mathrm{PSNR} = 10\log\left(\frac{255*255}{MSE}\right) \qquad (6)$$

where the I and j are the positions of pixel, and *m* and *n* are the image coordination

The measurement of the robustness is NC, defined in Eq. (7) and will be applied to the watermark image after extracted.

$$N_C = \frac{\sum_{i=0}^{M_1-1}\sum_{j=0}^{M_2-1} W(i,j)W^*(i,j)}{\sum_{i=0}^{M_1-1}\sum_{j=0}^{M_2-1}[W(i,j)]^2} \qquad (7)$$

where the i, j are the position of pixel, *m* and *n* are the watermark image coordination

JPEG compression is needed to reduce the information size of the image for transmission or archiving. Therefore, the robustness against this type of attack is very important. In Fig. (5), different values of quality factor were used for JPEG compression attack on the watermarked image which begins from 90%. This means that the visually of image (PSNR) is high with low compression. By decreasing the quality factor which ending with the value 10%, the visually of image is poor with high compression. If we apply the attack of the JPEG compression with 90% of quality factor, then the watermark can be survived and extracted, but if the small than 40% of quality factor is applied, then the watermark can only be identified. The (NC) values in Fig. (6) illustrate the extracted logo image after JPEG compression attacks.

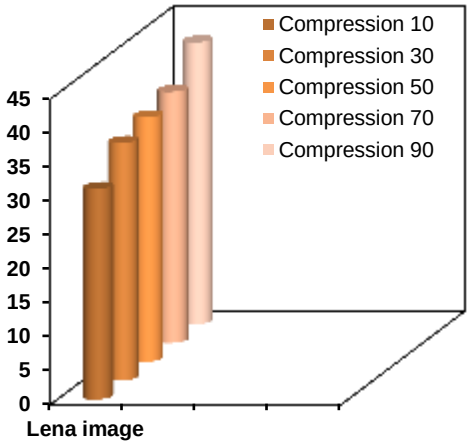


Fig. (5) PSNR results for different JPEG compression attack

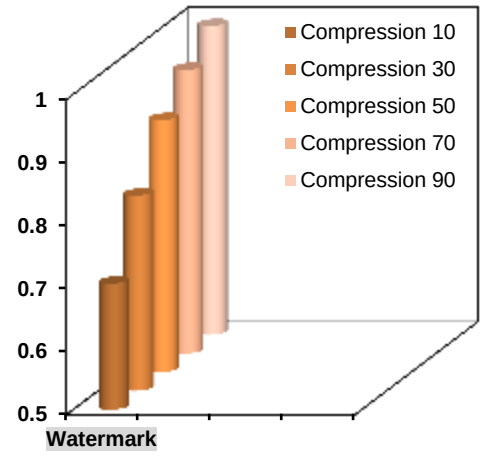


Fig. (6) NC results for different JPEG compression attack

Table (2) The NCC parameter value for watermarked image under attacks

Different attacks	NCC=
Low filter(4x4)	0.8214
Median (4x4) filter	0.7401
Gaussian filter 3x3	0.8982
Image sharpening	0.9140
Salt & pepper noise	0.9411

The robustness of the proposed watermarking embedding and extracted algorithm was tested after applying different attacks like (low pass filter, median pass filter, Gaussian filter, image sharpening and salt & pepper noise) on the watermarked image to measure the NC of each on. The results of our experiments are shown in the table (2).

The proposed work has many advantages, such as:

 ISSN (printed) 1813-2065, (online) 2309-1673 Printed in IRAQ

(1) Imperceptibility: The embedded generated watermark vector, after using embedding algorithm, does not damage the original image visually.

(2) Pixel expansion unchanged: The original image size didn't change; see figure 8.

(3) Robustness: The generated watermark vector is infeasible and difficult to remove from an attack.

(4) Watermark size reduced: The size of the generated watermark from VC public share was decreased.

(5) Feasibility: By using visual cryptography with one way hash function, it is imposable to reveal any information about the logo image without knowing the secret image (secret share.) At the same time, it is easy to implement and can be fast.

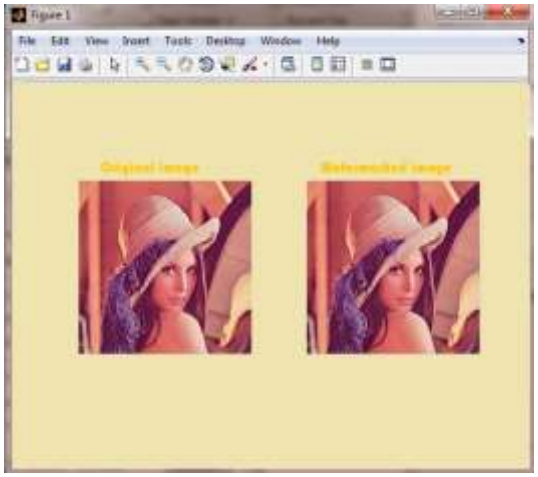


Fig. (7) Original image and watermarked image

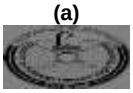
(a)

(b)

(c)

Fig. (8) (a) Watermarked image, (b) original watermark, (c)are the watermarking extraction without attacks NC=1

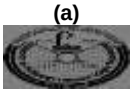
(a)



(b)

Fig. (9) (a) watermarked image, (b) the watermark extracting under attacks

(a)



(b)

Fig. (10) (a) watermarked Image, (b) watermark extracting under Salt & pepper noise attacks

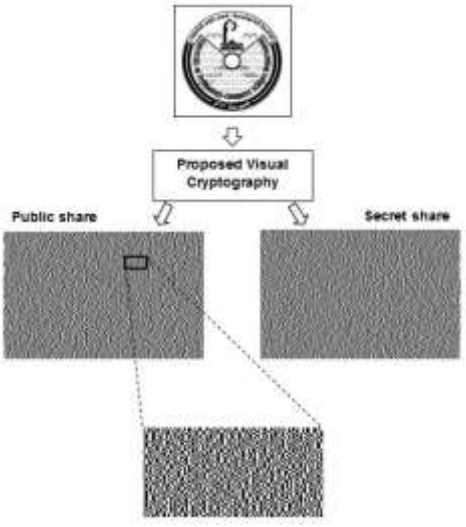


Fig. (11) Generation public share and secret share by proposed visual cryptography

 ISSN (printed) 1813-2065, (online) 2309-1673 Printed in IRAQ

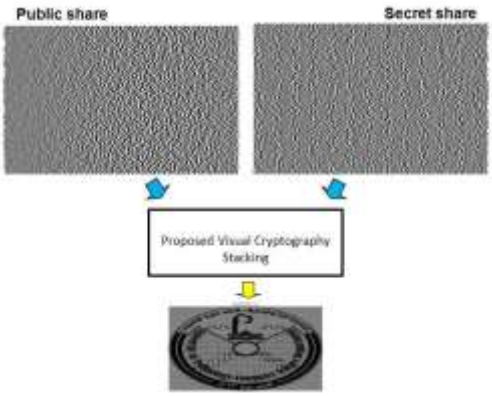
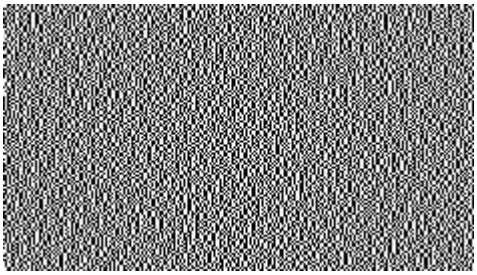


Fig. (12) Stacking image by using proposed visual cryptography

The test of Reliability: Our proposed work was tested by the reliability of evaluation. Different unauthorized keys, used in the extraction of the watermark from the watermarked image, were tried to examine any possibility of extracting the watermark with incorrect keys. Figure (13) shows an example of the retrieved watermark with the wrong key. The result reveals impossible extraction of the watermark (logo image) unless the correct secret key (secret share image) is used.



(a)

(b)

Fig. (13) (a) The extracted watermark with wrong key (b) the extracted watermark with correct key

6. Conclusions

In the current work, we could provide the highest security of watermarking algorithm on the digital image by using a public share from a proposed visual cryptography scheme and DCT transformation techniques. Novel watermark is generated to achieve a high robustness and capacity by reducing the size of generated watermark. We generated the one time image (secret image and public image) from the logo image by employing the MAC in the visual cryptography. Watermarking with middle band coefficients provided robustness against compression and active attacks and could avoid the malicious attacks by using the secret share image as an authentication tool. No change in the size of the original and watermarked images has resulted. The trade-off between the quality and robustness has been obtained. This work can be useful to provide the copyright protection and authentication of the digital image.

References

[1] M. Naor and A. Shamir, "Visual cryptography" Advance in Cryptology: Eurpocrypt'94, Lecture Notes In Computer Science, Springer Verlag, Germany, Vol. 950, pp. 1–12, 1995.
[2] A. Shamir, "How to Share a Secret", Communications of the ACM, vol. 22, 1996.
[3] J. Pan, H. Huang, L. Jain, "Intelligent Watermarking Techniques", World Scientific Publishing Co,2004.
[4] K. Katzenbeisser, F. Petitcolas, "Information Hiding Techniques for Steganography and Digital Watermarking", Artec House, 2000.
[5] C. Munesh, P.Shikha," A DWT Domain Visible Watermarking Techniques for Digital Images" International Conference on Electronics and Information Engineering ICEIE, V2, Pp-421-427, 2010.
[5] R. J. Hwang, "A digital copyright protection scheme based on visual cryptography," in Tamkang J. of Sci. and Eng., vol. 3,no. 3, pp. 97–106, 2000.
[6] A. Abusitta, "A visual cryptography based digital image copyright protection" in Journal of Information Security, vol. 3, pp. 96–104, 2012.
[7] S. Tai, C. Wang and C. Yu, "Repeating image watermarking technique by the visual cryptography," in IEICE Trans. Fundamentals, vol. E83-A, no. 8, pp. 1589–1598, August 2000.
[8] B. Surekha , G. Swamy, "Sensitive digital image watermarking for copyright protection," in International Journal of Network Security, vol. 15, no. 8, pp. 95–103, January 2013.
[9] M. Benyoussef, S. Mabtoul, M. El Marraki, D. Aboutajdine. "Blind Invisible Watermarking Technique in DT-CWT Domain using Visual Cryptography". ICIAP 2013, Part I, LNCS 8156, pp. 813–822, 2013.
[10] National Institute of Science and Technology, Information Processing Standard, "Secure Hash Standard", United States of America, FIPS 180-1,1993.
[11] W. Stalling, "Cryptography and Network Security Principles and Practice", 5th Edition, 2012.
[12] J. Weir, W. Yan, "Visual Cryptography and Its Applications", in Ventus Publishing, 2012.

 ISSN (printed) 1813-2065, (online) 2309-1673 Printed in IRAQ