

# HSV Image Watermarking Scheme Based on Visual Cryptography

Rawan I. Zaghloul, Enas F. Al-Rawashdeh

**Abstract**—In this paper a simple watermarking method for color images is proposed. The proposed method is based on watermark embedding for the histograms of the HSV planes using visual cryptography watermarking. The method has been proved to be robust for various image processing operations such as filtering, compression, additive noise, and various geometrical attacks such as rotation, scaling, cropping, flipping, and shearing.

**Keywords**— Histogram, HSV image, Visual Cryptography, Watermark.

## I. INTRODUCTION

THE growth of networked multimedia systems has magnified the need for image copyright protection. One approach used to address this problem is to watermark the image using visual cryptography. Visual cryptography is a concept introduced by Naor and Shamir in 1994 [1], which is a kind of cryptography that can be decoded directly by the human visual system without any special calculation for decryption.

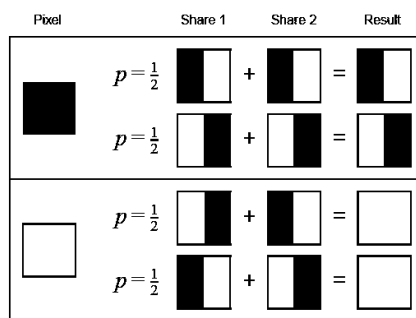


Fig.1 The basic scheme of visual cryptography

Naor and Shamir further describe the visual cryptography scheme as a visual secret sharing problem in which the secret message can be viewed as nothing more than a collection of black and white pixels as illustrated on fig. 1. Each pixel in the original image is represented by at least one subpixel in each of the  $n$  transparencies or shares generated. Each share is

comprised of collections of  $m$  black and white subpixels where each collection represents a particular original pixel. [1, 2, 3]

On 2000, R.J. Hwang proposed a watermark method based on visual cryptography, according to his Method, the owner should select an  $h \times n$  black/white image as the watermark. In the *embedding processes*, the owner should randomly select a number as his secret key,  $S$ , to embed the watermark into the image  $M$  that is a  $k \times l$  256 gray-leveled image. The owner embeds the watermark pattern  $W$  into the image  $M$  by generating the secret key,  $S$ , and the verification information,  $V$ , as the following steps:

- Select a random number  $S$  as the secret key of the image  $M$ .
- Use  $S$  as the seed to generate  $h \times n$  different random numbers over the interval  $[0, k \times l]$ . ( $R_i$  used to denote the  $i$ -th random number.)
- Assign the  $i$ -th pair ( $vi1$ ,  $vi2$ ) of the verification information  $V$  based on Table I.
- Assemble all the ( $vi1$ ,  $vi2$ ) pairs to construct the verification information  $V$ . [3]

TABLE I  
THE RULES TO ASSIGN THE VALUE OF VERIFICATION INFORMATION

$W_i$	Left most bit of the $R_i$ -th pixel of Image $M$	Assign ( $vi1$ , $vi2$ ), of $V$ is
0	1	(0,1)
0	0	(1,0)
1	1	(1,0)
1	0	(0,1)

In the *extraction process*, the notarial organization retrieves the verification information  $V$  and the watermark pattern  $W$ , which the owner has registered, and verifies the ownership of the image  $M'$  as follows:

- Use  $S$  as the seed to generate  $h \times n$  different random numbers over the interval  $[0, k \times l]$ . ( $R_i$  used to denote the  $i$ -th random number.)
- Assign the color of the  $i$ -th pixel of the watermark pattern  $W'$  based on Image  $M'$  as follows:
- Get the left-most bit,  $b$ , of the  $R_i$ -th pixel of Image  $M'$ , and, if  $b$  is "1", then assign  $fi=(1,0)$ ; otherwise,  $fi=(0,1)$ . If  $fi$  is equal to the  $i$ -th pair of  $V$  then assigns the color of the  $i$ -th pixel of  $W'$  to be white; otherwise, assign it to be black.
- If  $W'$  can be recognized as  $W$  through the human visual system, the notarial organization shall adjudge that the image  $M'$  is a copy of  $M$ . [3, 7]

Hwang's method has the following problems:

- It is applied over grayscale images only.
- At present most watermarking schemes perform poorly against geometrical attacks [8], and the robustness of this algorithm is also weak against some of geometrical attacks like rotation, scaling, shearing, and flipping.
- If we have an image  $F$  with some similarities with the original image  $M$ . The watermark pattern  $W$  may be restored successfully, although the image  $F$  is not the same as the image  $M$ . [7]

## II. THE PROPOSED METHOD

Our proposed method is based on extracting the features vector  $X'$  from the histograms of the HSV image. Fig.2 shows watermark *embedding process*, as explained in the following steps:

- Convert the host image from RGB color scheme to the HSV color scheme.
- Extract the  $H\_H$ ,  $H\_S$ , and  $H\_V$  vectors, which are the histograms of the hue, saturation, and the value planes respectively.
- Generate features vector  $X$ , which contains the largest values from  $H\_H$ ,  $H\_S$ , and  $H\_V$  respectively, i.e the values of  $X$  are determined as the values of  $H\_H$ ,  $H\_S$ , and  $H\_V$  which are greater than a threshold value (in our experimental results we assume threshold = 50 ). Make sure that the size of vector  $X$  is equals to or greater than the size of the watermark  $W$ .
- Then, apply Hwang's method for watermark embedding, over  $X$  vector to generate the verification vector  $V$ .
- Register  $V$  in the third party (notarial) organization.

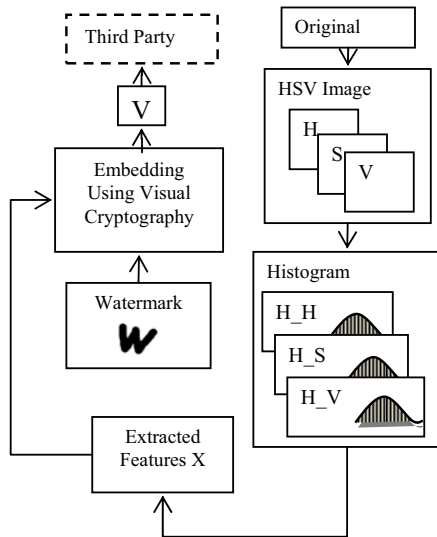


Fig.2 Embedding process of the proposed method

Fig.3 shows the *extraction process*, as illustrated in the following steps:

- Apply the first three steps of the embedding process over the watermarked image  $M'$ .

- Apply Hwang's method for watermark extraction which generates vector  $F'$ .
- The notarial organization determines  $W' = V \otimes F'$ , where  $\otimes$  denotes the *Exclusive OR* operation. So, If  $W'$  can be recognized as  $W$  through the human visual system, the notarial organization shall adjudge that image  $M'$  belongs to the owner.

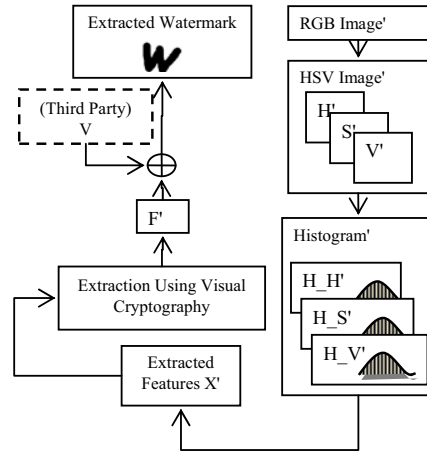


Fig.3 Extraction process of the proposed method

## III. EXPERIMENTAL RESULTS

In order to reveal the results of the proposed algorithm a color image *peppers.png* (256×256) is taken as the host image. The watermark image is a (32×32) binary bitmap. To measure distortion and similarity between the original watermark ( $W$ ) and the extracted watermark ( $W'$ ), the following quality metrics are used:

- Mean Square Error (MSE), as defined in (1),

$$MSE = \frac{1}{m \times n} \sum_{i=1}^m \sum_{j=1}^n (W_{ij} - W'_{ij})^2, \quad (1)$$

Where  $m \times n$  is the size of the watermark,  $W_{ij}$  is the watermark pixel in the  $i^{\text{th}}$  row and  $j^{\text{th}}$  column, and  $W'_{ij}$  is the  $W'$  in the  $i^{\text{th}}$  row and  $j^{\text{th}}$  column. [4]

- Peak Signal to Noise Ratio (PSNR), as defined in (2). [9]

$$PSNR = 10 \times \log \frac{255^2}{MSE} \quad (2)$$

- Correlation ( $Corr$ ), as defined in (3),

$$Corr = \frac{\sum_{i=1}^m \sum_{j=1}^n (W_{ij} - \bar{W})(W'_{ij} - \bar{W}')}{\sqrt{\left( \sum_{i=1}^m \sum_{j=1}^n (W_{ij} - \bar{W})^2 \right) \left( \sum_{i=1}^m \sum_{j=1}^n (W'_{ij} - \bar{W}')^2 \right)}} \quad (3)$$

Where  $\bar{W}$  and  $\bar{W}'$  are the mean for the original watermark and the extracted watermark respectively.[4]

Our method has been tested against two types of attacks. The first one is *signal processing* attacks, which concerns filtering, lossy compression, and noise addition. The other type is *geometrical attacks*, i.e cropping, scaling, shearing, and rotation [5, 6].

Fig.4 shows the host image, and the binary watermark image.



Fig.4 Host image and the watermark pattern

The robustness of the proposed algorithm is tested by applying particular operations on the watermarked image and then retrieving the watermark. Table II shows the results of watermark extraction after adding different types of noise to the watermarked image.

TABLE.II  
THE RESULTS OF NOISE ADDITION

Attack	MSE	PSNR	Corr	Extracted Watermark
Gaussian Noise [m=0 v= 0.01]	0.1308	56.96473	0.7045	
Gaussian Noise [m=0 v= 0.2]	0.2266	54.5782	0.5283	
Gaussian Noise [m=0.01 v= 0.01]	0.1338	56.86624	0.7014	
Gaussian Noise [m=0.01 v= 0.1]	0.1651	55.95333	0.6456	
Gaussian Noise [m=0.01 v=0.2]	0.2275	54.56099	0.5245	
Salt & Pepper [d=0.05]	0.0801	59.09448	0.8171	
Salt & Pepper [d=0.1]	0.1045	57.93964	0.7679	
Salt & Pepper [d=0.2]	0.1679	55.8803	0.6485	
Salt & Pepper [d=0.3]	0.1924	55.28875	0.6044	
Speckle Noise [v=0.04]	0.1397	56.67884	0.6869	
Speckle Noise [v=0.1]	0.1397	56.67884	0.6889	
Speckle Noise [v=0.2]	0.1406	56.65095	0.6886	
Speckle Noise [v=0.5]	0.1211	57.29936	0.7381	

As depicted in table II, the host image is affected by Gaussian noise with various values of mean ( $m$ ) and variance ( $v$ ). Then we have tested the host image by adding salt and pepper noise with different density values ( $d$ ). Also, the speckle noise is added to the host image with different variance values ( $v$ ).

The scheme shows 100% robustness against some attacks; such attacks are flipping, rotation ( $90^\circ$ ,  $180^\circ$ ,  $270^\circ$ ). Fig.5 Shows rotated watermarked images by  $30^\circ$  and  $60^\circ$  along with the extracted watermark.

Fig.6 shows the watermarked image cropped by a mask of size  $226 \times 226$ , and mask of size  $216 \times 216$  along with the extracted watermarks.

Fig.7 shows the sheared watermarked image and the extracted watermark.

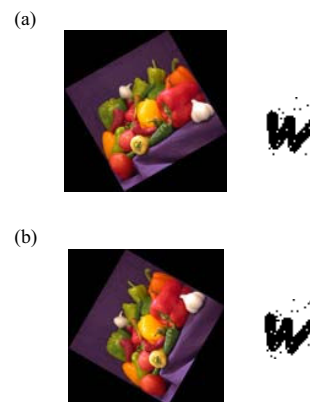


Fig.5 (a) watermarked image rotated  $30^\circ$  and its extracted watermark, (b) watermarked image rotated  $60^\circ$  and its extracted watermark from image



Fig.6 (a) Watermarked image cropped by  $226 \times 226$  mask along with its extracted watermark, (b) Watermarked image cropped by  $216 \times 216$  mask along with its extracted watermark



Fig.7 Watermarked image after shearing, and its extracted watermark

Table III lists the results of applying *Rotation*, *Cropping*, *Scaling*, and *Shearing* between the original watermark and the extracted one.

TABLE.III

THE RESULTS OF GEOMETRICAL ATTACKS			
Attack	MSE	PSNR	Corr
Rotation 30 degrees	0.0068	69.7828	0.9844
Rotation 60 degrees	0.0127	67.0944	0.9710
Crop square width=30	0.0840	58.8888	0.8086
Crop square width=40	0.1514	56.3295	0.6758
Shearing	0.0654	59.9727	0.8483
Scaling by factor of 2 to be 512×512	0.1162	57.4783	0.7348
Scaling by factor of 4 to be 1024×1024	0.1865	55.4235	0.5837

Table IV shows the performance of the proposed method after applying filtering process by Gaussian (with mean  $m=0.5$ ) and average filters using mask of size  $3 \times 3$ , and shows the results which are retrieved from JPEG compression with some quality levels  $Q$  of Photoshop7.0.

TABLE.IV








THE RESULTS OF OTHER SIGNAL PROCESSING ATTACKS				
Attack	MSE	PSNR	Corr	Extracted Watermark
Gaussian Filter $m=0.5$	0.0693	59.72179	0.8393	
Average Filter	0.0791	59.14741	0.8185	
Jpeg Compression Q=1 File size= 20,272 bytes	0.0918	58.5025	0.793	
Jpeg Compression Q=4 File size= 24,751 bytes	0.0947	58.3661	0.7882	
Jpeg Compression Q=6 File size=29,098 bytes	0.0947	58.3661	0.7882	
Jpeg Compression Q=9 File size=39,093 bytes	0.0947	58.3661	0.7871	
Jpeg Compression Q=12 File size=98,304 bytes	0.0781	59.2029	0.8209	

Fig.8 shows the extracted watermark from the host image after distortion, which result in a  $Corr = 0.74$ ,  $MSE=0.1201$ , and  $PSNR=57.33$ .

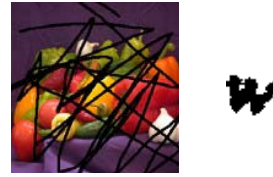


Fig.8 The distorted image along with the extracted watermark

#### IV. CONCLUSION

Watermarking is a good method to protect copyright ownership. In this paper, we propose a watermark method based on visual cryptography and we summarize the features of the proposed method as follows:

- The host image is color image (HSV scheme).
- The watermark pattern can't be retrieved from other similar image.
- The watermark is not embedded into the original image which leaves the watermark image equal to original image.
- The method has been proved to be robust against geometrical attacks like rotation, flipping, cropping, scaling, and shearing.
- The proposed method is robust against signal processing attacks like noise addition, filtering, and jpeg compression with good Corr values.

#### REFERENCES

- [1] N.Naor and A. Shamir, Visual Cryptography, Advances in Cryptology: Eurocrypt'94, Springer - Verlag, Berlin, pp 1-129 (1995).
- [2] L. Hawkes, A.Yasinsac and C. Cline, An Application of Visual Cryptography to Financial Documents; technical report TR001001, Florida State University (2000).
- [3] R. Hwang, A digital Image Copyright Protection Scheme Based on Visual Cryptography, Tambang Journal of science and Engineering, vol.3, No.2, pp. 97-106 (2000).
- [4] MathWorks, Image Processing Toolbox User's Guide 4.2.
- [5] S. Pereira, J. J. K. O Ruanaidh, F. Deguillaume, G. Csurka and T. Pun. Template based recovery of Fourier-based watermarks using log-polar and log-log maps, in IEEE Int. Conf. on Multimedia Computing and Systems, Florence, Italy, vol.1, pp.9870 (1999).
- [6] C. H. Lee and H. K. Lee. Improved autocorrelation function based watermarking with side information, SPIE, vol.14, No.1, ISSN 013012 (2005).
- [7] M. Hassan, and M. Khalili, Self Watermarking based on Visual Cryptography; PWASET, Budapest, Hungary, vol.8, No.31, pp. 159-162 (2005).
- [8] E. Chrysoschos, V. Fotopoulos, A. N. Skodras, and M. Xenos, Reversible Image Watermarking Based on Histogram Modification; 11th Panhellenic Conference on Informatics with international participation, Patras, Greece, vol. B, pp. 93-104 (2007).
- [9] B.Verma, S.Jain, D. Agarwal, and A.Phadikar, A New Color Image Watermarking Scheme; INFOCOMP, vol. 5, No.2, pp. 37-42 (2006).