International Journal of Innovative
Computing, Information and Control
Volume **13**, Number **5**, October **2017**

 ISSN 1349-4198
pp. 1709–1719

A SEMI-FRAGILE BLIND WATERMARKING SCHEME FOR COLOR IMAGES BASED ON VISUAL CRYPTOGRAPHY AND DISCRETE COSINE TRANSFORM

Xiaodan Jiang[1], Zheming Lu[2,*] and Xiajun Ding[1]

[1]College of Electrical and Information Engineering
Quzhou University
No. 78, North Jiuhua Ave., Quzhou 324000, P. R. China
16282409@qq.com

[2]School of Aeronautics and Astronautics
Zhejiang University
No. 38, Zheda Road, Hangzhou 310027, P. R. China
*Corresponding author: zheminglu@zju.edu.cn

Received March 2017; revised June 2017

Abstract. *This paper presents a semi-fragile blind watermarking scheme for color images based on Visual Cryptography (VC) and Discrete Cosine Transform (DCT). Firstly, the binary watermark image is separated into two shares, i.e., the public share and the private share, by using the VC technique. Then, the color host image is converted from the RGB color space into the HSV color space. Next, the DCT transform is performed on each* 8×8 *block in the V component of the host image. Finally, the public share is embedded into the DCT middle frequency coefficients. During the extraction process, the public share is first extracted, and then it is stacked over the private share to recover the original watermark. The experimental results show that the proposed scheme has good invisibility and good robustness to color transform, cropping and JPEG compression operations, but is vulnerable to Gaussian noise, Poisson noise, Speckle noise and Gaussian low-pass filtering attacks.*

Keywords: DCT transform, Visual cryptography, HSV, Semi-fragile watermark, Blind watermark

1. **Introduction.** With the development of multimedia technology and network technology, the use of digital multimedia has reached an unprecedented depth and breadth, and people enjoy the efficient and rapid dissemination of convenience. However, on the other hand, they face various threats, such as unauthorized copying and malicious tampering of digital data. As an important means of intellectual property protection, digital watermarking technology [1] has been paid more and more attention to.

Digital watermarking technology can be divided into two categories according to robustness: robust watermarking for copyright protection and fragile watermarking for content authentication [2,3]. Currently, most of the watermarking schemes are a way of embedding a certain amount of watermark information on the host image and then extracting the watermark information to perform discrimination or identification. Therefore, it is necessary to prevent others from interpreting the specific meaning of watermark. In the process of watermark embedding and extracting, we should pay attention to the security of watermark images, and we also demand the security of digital watermarking algorithms. Therefore, in order to further improve the security of digital watermarking, the researchers introduced the visual cryptography scheme (VCS) [4,5] into digital watermarking schemes. Several different shares are generated from the original watermark through

VCS, and then, the share is embedded into the host image. In the decryption, when a certain number of share images are stacked, the original watermark can be recovered, without operation, as long as the human visual system can identify. This operation not only increases the confidentiality and security of digital watermarking, but also does not increase the computational complexity.

In recent years, the combination of visual cryptography and digital watermarking technology appeared frequently [6-17]. On the one hand, the combined algorithm can be used in image copyright protection schemes [6-12]. Chang et al. [6] proposed an image copyright protection scheme of visual cryptography combined with DCT in 2002, but this algorithm does not really embed the watermark into the host image. Hsu and Hou [7] proposed combining the visual cryptography algorithm with sampling distribution, where the length of the binary watermark can be arbitrarily long. [10] proposed applying DWT to decomposing the cover image, and using the artificial bee colony algorithm to adaptively select feature blocks. Experimental results show that this scheme is robust. Recently, based on the combination of image geometric feature invariants and visual cryptography, a robust color image watermarking algorithm is proposed in [11]. On the other hand, some references combined visual cryptography and digital watermarking technology to be used in the field of credibility authentication [13-17]. Fang and Lin [13] proposed the VSC to hide some secret information, but without watermarking scheme. Li et al. [15] decomposed the host image into seven sub-bands by 2-level DWT and extracted the sub-band LL of the image in order to generate a feature image, then employed VCS to generate the secret image from the feature image to certify the authority. This scheme is robust against print-scan attacks, but it has the disadvantage that it is not a blind scheme that requires the host image during watermark extraction. A $(2, 2)$ extended visual cryptography scheme with meaningful shares is proposed in [16] in addition to the secret image, an additional watermark is also embedded to serve for authentication purpose, but it is suitable for grayscale images.

From the research references, we also noticed that there are more applications of the copyright protection than that of credibility authentication, therefore, in order to further enrich the research of credibility authentication and broaden the scope of application to watermarking technology. In this paper, we also do some useful exploration on the combination of visual cryptography and digital watermarking. The proposed scheme first applies visual cryptography to creating the public share and the private share from the binary watermark image. Then, the color host image is converted from the RGB space into the HSV color space, and the scheme performs the DCT transform on each 8×8 block in the V component image and embeds the public share into the DCT middle frequency coefficients. During the extraction process, the public share is first extracted and stacked on the private share to recover the original watermark. The experimental results show that the proposed watermarking scheme is semi-fragile, and can improve the security of the watermark image.

The structure of this paper is organized as follows. In Section 2, some basic concepts are briefly described. Then the corresponding watermarking scheme is described in Section 3. In Section 4, the experimental result and analysis are shown to prove the semi-fragility of our method. Finally, the conclusions are given in Section 5.

2. **Some Basic Concepts.**

There are two techniques relevant to the proposed semi-fragile blind watermarking scheme, namely the Visual Cryptography Scheme and the DCT transform. The VCS is utilized to construct share images. The DCT technique is used to acquire the features of a host image. These techniques are briefly described respectively as follows.

2.1. **Visual cryptography scheme.** In 1994, the visual cryptography [4] is a paradigm introduced by Naor and Shamir to encrypt a secret image into two or more random noise-like shares, human eyes cannot distinguish any information from a single share; however, when any k shares are stacked, the human eye can distinguish the secret image that does not need to have any knowledge of encryption and complex operations. Therefore, visual cryptography has become a new research hotspot in the field of information security.

In the conventional $\{2, 2\}$ visual cryptography scheme, Figure 1(a) illustrates its encryption and decryption strategies. Each secret pixel is encrypted into two 2×2 T_1 or T_2 blocks, each containing two white and two black pixels. When two shares are stacked, one white C^0 pixel contains two white pixels and two black pixels, while one black C^1 pixel contains four black pixels. It is clear that the size of each share is four times as large as that of the secret image.

Hence, the conventional $\{2, 2\}$ VCS increases a heavy load for the limited network bandwidth and the storage. Ito et al. [18] proposed a non-expansion VCS model which is based on a probabilistic principle. Figure 1(b) illustrates the encryption and decryption strategies of Ito et al.'s non-expansion VCS. The size of each share is equal to that of the secret image because there is no image size expansion. In Ito et al.'s model, each black pixel or white pixel in the secret image has two different encryption schemes. When encrypting a white C^0 (or black C^1) pixel, we randomly choose a column from C^0 (C^1), and assign them to the two share images in their corresponding positions [19]. In this paper, we choose the XOR operation based on the non-expansion VCS.

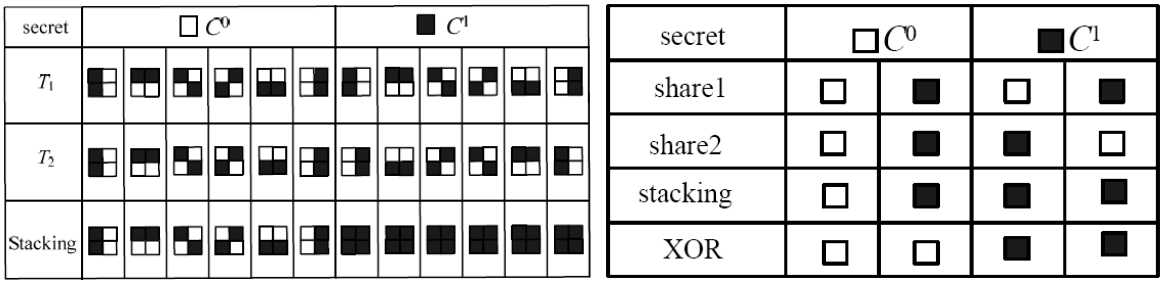


FIGURE 1. (a) Encryption and decryption strategies of the conventional $\{2, 2\}$ VCS; (b) encryption and decryption strategies of Ito et al.'s non-expansion VCS

2.2. **Discrete cosine transform.** DCT is a popular orthogonal transformation for image processing and signal processing [20,21], since it has the advantages of high compression ratio, low error rate, low computational complexity and being compatible with the international data compression standards JPEG and MPEG. Two-dimensional DCT and IDCT transforms can be defined as following two formulas:

$$F(u,v) = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1} C(u)C(v)f(i,j) \times \cos\left[\frac{\pi(2i+1)u}{2N}\right]\cos\left[\frac{\pi(2j+1)v}{2N}\right] \tag{1}$$

$$f(i,j) = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1} C(u)C(v)F(u,v) \times \cos\left[\frac{\pi(2i+1)u}{2N}\right]\cos\left[\frac{\pi(2j+1)v}{2N}\right] \tag{2}$$

where

$$C(u), C(v) = \begin{cases} \sqrt{1/N} & u, v = 0 \\ \sqrt{2/N} & u, v = 1, 2, \ldots, N-1 \end{cases} \tag{3}$$

where, u represents the horizontal frequency of cosine wave, v represents the vertical frequency of cosine wave. After the image signal is transformed by the two-dimensional DCT, the correlation among the image transform coefficients is reduced, and the energy of the data is concentrated in the low frequency coefficients on the left corner of the DCT matrix. When the image is reconstructed by the IDCT transform, the channel error and the quantization error are dispersed like random noises to each pixel in the image block without error accumulation. There are two main DCT transform based watermarking schemes, one is to perform the matrix DCT transform directly on the whole image $F(m, n)$ as a two-dimensional matrix, then embed the watermark information. Another method is to divide the image into small blocks and the DCT transform is performed on each block separately, and then embed the watermark information. The second kind of method is adopted in this paper.

3. **Proposed Scheme.** This section presents the proposed semi-fragile blind watermarking scheme. The scheme consists of two phases, i.e., watermark embedding and watermark extraction. An overview of the proposed scheme is shown in Figure 2. During watermark embedding, the watermark image is first divided into two shares, then the public share is embedded into the host image and the private share is given to the owner. In order to prove the legitimacy of the owner, the owner can stack the private share and the public share extracted from the host image to restore the binary watermark image. Based on the security of visual cryptography, we can ensure that the stolen embedded share does not reveal the original watermark information.

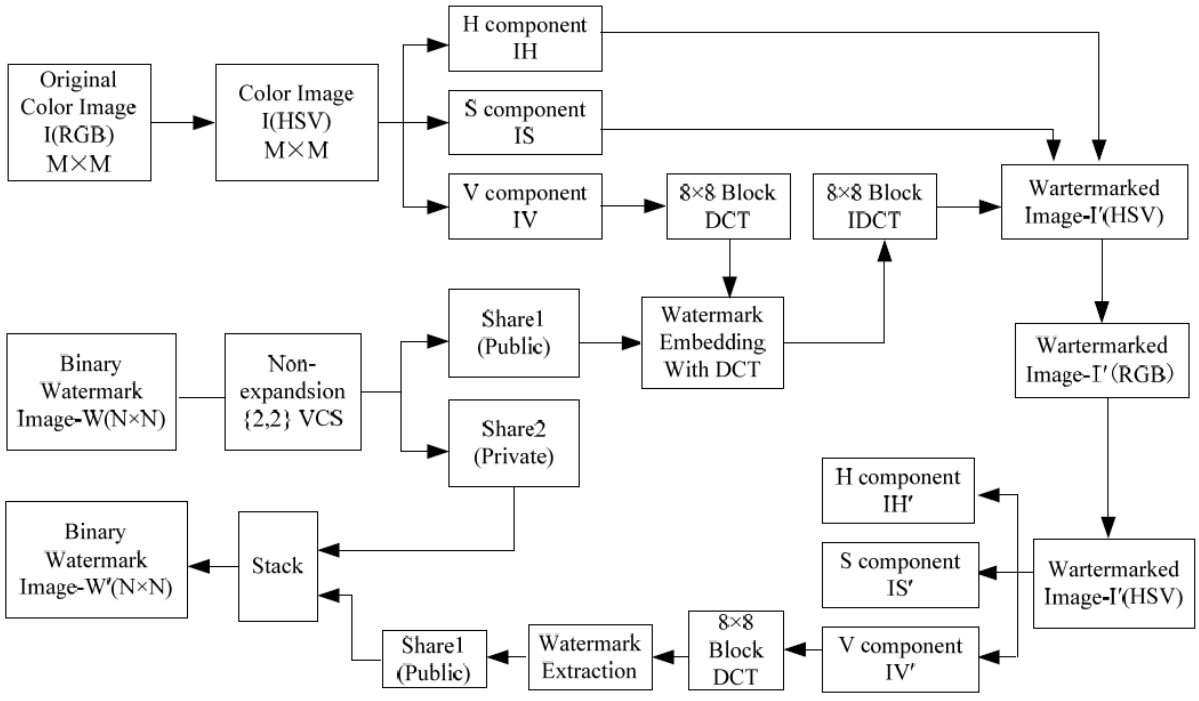


FIGURE 2. The proposed watermark embedding and extraction processes

3.1. **Pretreatment.** In color digital image processing, the RGB and HSV models are often used to establish the color space. The RGB space (R stands for red, G for green and B for blue) can cause any color perception on the electromagnetic spectrum, but the three-color component is highly correlated and is a non-uniform color space, so it is mainly used as a color space model for hardware devices. The HSV space is a color

space that is closer to the color perception of human eyes, its components are visually independent of each other, and the V component is independent of the color information of the pixel. According to the experiment results, it is shown that embedding the watermark information in the component V can guarantee the imperceptible characteristic of the digital watermark. The pretreatment steps are: (1) the color host images (RGB color space) are transformed into the HSV color space by using Equation (4); (2) separate the host image (HSV color space) into three components, H, S and V; (3) take the brightness component V as the watermark to be embedded.

$$\begin{cases} V = MAX(R,G,B) \\ S = \begin{cases} \dfrac{V - MIN(R,G,B)}{V} & \text{if } V \neq 0 \\ 0 & \text{otherwise} \end{cases} \\ H = \begin{cases} 60^\circ \times (G-B)/(V - MIN(R,G,B)) & \text{if } V = R \\ 120^\circ + 60^\circ \times (B-R)/(V - MIN(R,G,B)) & \text{if } V = G \\ 240^\circ + 60^\circ \times (R-G)/(V - MIN(R,G,B)) & \text{if } V = B \end{cases} \\ \text{if } H < 0 \text{ then } H = H + 360^\circ \end{cases} \tag{4}$$

where MAX is the maximum value in R, G, and B, and MIN is the minimum value of R, G, and B. The values of R, G and B fall into the interval $[0, 255]$; the value of H falls into the interval $[0, 360]$; the value of S falls into the interval $[0, 1]$; and the value of V falls into the interval $[0, 255]$.

3.2. **Watermark embedding process.** In this paper, the host image I is of size $M \times M$, and the binary watermark image W is of size $N \times N$, satisfying $N = M/8$. In order to improve the watermark extraction speed, we choose the non-expansion VCS, so the size of each share is $N \times N$ and $N = M/8$. The detailed embedding steps can be illustrated as follows.

Step 1: Pretreatment: the host image I is converted from the RGB color space to the HSV color space, then separate the HSV color space into three components: the H component image IH, the S component image IS and the V component image IV. The V component image is adopted to embed the watermark.

Step 2: Generate VC shares from the binary watermark image: the binary watermark image W is divided into two shares by using the non-expansion $\{2, 2\}$ VCS, the public share is embedded into the host image and the private share is given to the owner, and the public share is converted into a one-dimensional stored binary sequence $\{W_1, W_2, \ldots, W_{1024}\}$.

Step 3: DCT transformation: the host image I of size 512×512 is divided into 8×8 blocks, and the DCT transform is performed on each block. The block in the ith row and jth column is denoted as F_{ij} $(1 \leq i \leq 32,\ 1 \leq j \leq 32)$. In order to balance the imperceptibility of the watermark, this paper embeds the watermark into the low and middle frequency coefficients in the DCT block.

Step 4: Embedding watermark: the watermark information is embedded in the low frequency coefficient $F_{ij}(4, 4)$, and M_{ij} represents the average of its four adjacent coefficients. The embedding process can be illustrated as follows:

$$M_{ij} = mean\left(F_{ij}(4,3) + F_{ij}(4,5) + F_{ij}(3,4) + F_{ij}(5,4)\right) \quad (1 \leq i \leq 32, 1 \leq j \leq 32) \tag{5}$$

$$F'_{ij}(4,4) = \begin{cases} M_{ij} + key & \text{if } W_k = 1 \\ M_{ij} - key & \text{if } W_k = 0 \end{cases} \quad (1 \leq i \leq 32, 1 \leq j \leq 32, 1 \leq k \leq 1024) \tag{6}$$

where, the *key* denotes the embedding strength, the higher the key value is, the higher the robustness is, but the worse the watermark invisibility is. Through a large number of experiments, *key* is selected to be 10.

Step 5: Generate the watermarked image: the watermarked V component IV' is transformed by IDCT and merged with the original H component IH and S component IS into HSV image I' with the watermark, and finally converted to the RGB space, and thus the watermark embedding process is completed.

3.3. **Watermark extraction process.** In the watermark extraction process, firstly, we extract the public share from the watermarked image I', and then the public share is stacked with the private share to obtain the complete watermark image. The process is blind and does not require the participation of the original image. The detailed process is shown in Figure 2, and the specific steps can be described as follows.

Step 1: The watermarked image I' is converted from the RGB space to the HSV color space and is divided into three components, i.e., the H component image IH', the S component IS' and the V component IV'.

Step 2: The V component IV' of size 512×512 is divided into 8×8 blocks, and the DCT transform is performed for each block. Through comparing $F_{ij}(4,4)$ and $M_{ij} = \text{mean}\,(F_{ij}(4,3) + F_{ij}(4,5) + F_{ij}(3,4) + F_{ij}(5,4))$ extract each watermark bit. The extraction process satisfies the following equations:

$$W_k = \begin{cases} 1 & \text{if } F_{ij}(4,4) \geq M_{ij} \\ 0 & \text{if } F_{ij}(4,4) < M_{ij} \end{cases} \quad (1 \leq i \leq 32, 1 \leq j \leq 32, 1 \leq k \leq 1024) \tag{7}$$

Step 3: The extracted watermarking sequence is transformed into the two-dimensional public share, and the public share is stacked with the private share to obtain the complete watermark image; thus the watermark extraction and reconstruction are completed.

4. **Experimental Results.** In this section, the performance of the proposed semi-fragile blind watermark scheme is demonstrated. The robustness of the proposed scheme to various distortions are studied by a series of experiments on the color images. All the simulation experiments are conducted on VS2010 and OpenCV. Most of the color images in the experiment are selected from the database of the Computer Vision Group at the University of Granada [22], and six host images of size 256×256 are shown in Figure 3. The binary image of size 32×32 shown in Figure 4(a) is used as the watermark, Figure 4(b) shows the public share (embedded in the host image), Figure 4(c) shows the private image (owned by the owner), and Figure 4(d) shows the watermarked image. In our experiments, two objective parameters are used to evaluate the results.

(1) The Peak Signal to Noise Ratio (PSNR) is used to evaluate the visual quality of the attacked host color image. For a color image $f(x,y)$ of size $M \times M$ and its attacked version $f(x,y)$, the PSNR is defined as follows [23].

$$PSNR = 10 \log \left(\frac{255^2}{\frac{1}{3NM} \sum\limits_{c \in \{R,G,B\}} \sum\limits_{y=0}^{N-1} \sum\limits_{x=0}^{M-1} \left(f_c(x,y) - \tilde{f}_c(x,y) \right)^2} \right) \tag{8}$$

where the subscript c represents the three color components of the color image.

(a) Peppers (b) Barche (c) Baboon

(d) Lena (e) Barnfall (f) Apple

FIGURE 3. Examples of color host images

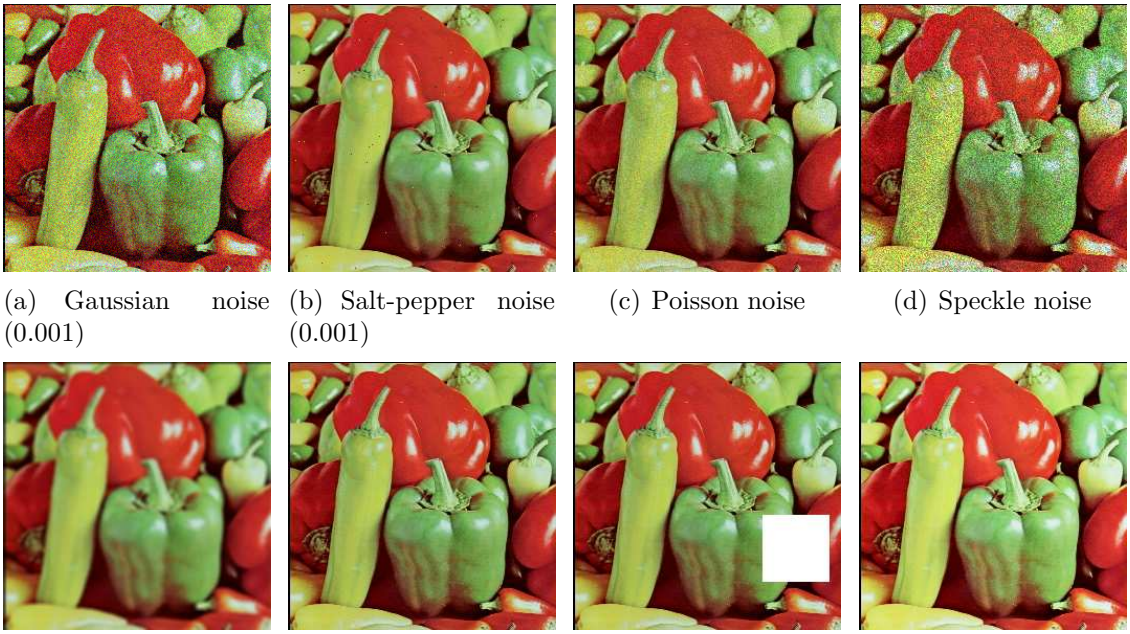
(a) Binary watermark image (b) Share 1 (public) (c) Share 2 (private) (d) Watermarked image

FIGURE 4. Example results of the proposed scheme

(2) Normalized Correlation (NC) is used as the objective quantitative measure to compare the original watermark and the extracted watermark. NC is defined as follows:

$$NC = \frac{\sum_{y=0}^{N-1}\sum_{x=0}^{M-1} f(x,y)\,\tilde{f}(x,y)}{\sum_{y=0}^{N-1}\sum_{x=0}^{M-1} f^2(x,y)} \tag{9}$$

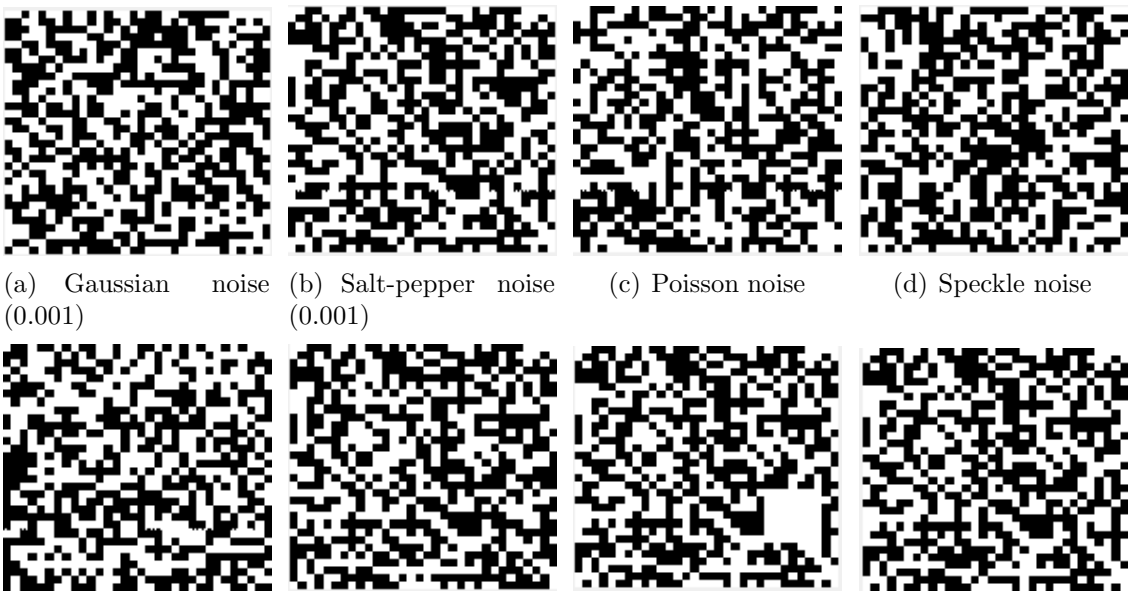
In order to verify the effectiveness and semi-fragility of the proposed scheme, several attack tests are carried out on the watermarked image including Gaussian noise, Salt and Pepper noise, Poisson noise, Speckle noise, Gaussian low-pass filtering, JPEG compression, Cropping, Brightness, etc. Figures 5-7 show the experimental results for the attacked "peppers" image.



(a) Gaussian noise (0.001) (b) Salt-pepper noise (0.001) (c) Poisson noise (d) Speckle noise

(e) Gaussian low-pass filtering (f) JPEG compression (80%) (g) Cropping (1/16) (h) Brightness (+30)

FIGURE 5. Examples of the attacked peppers image

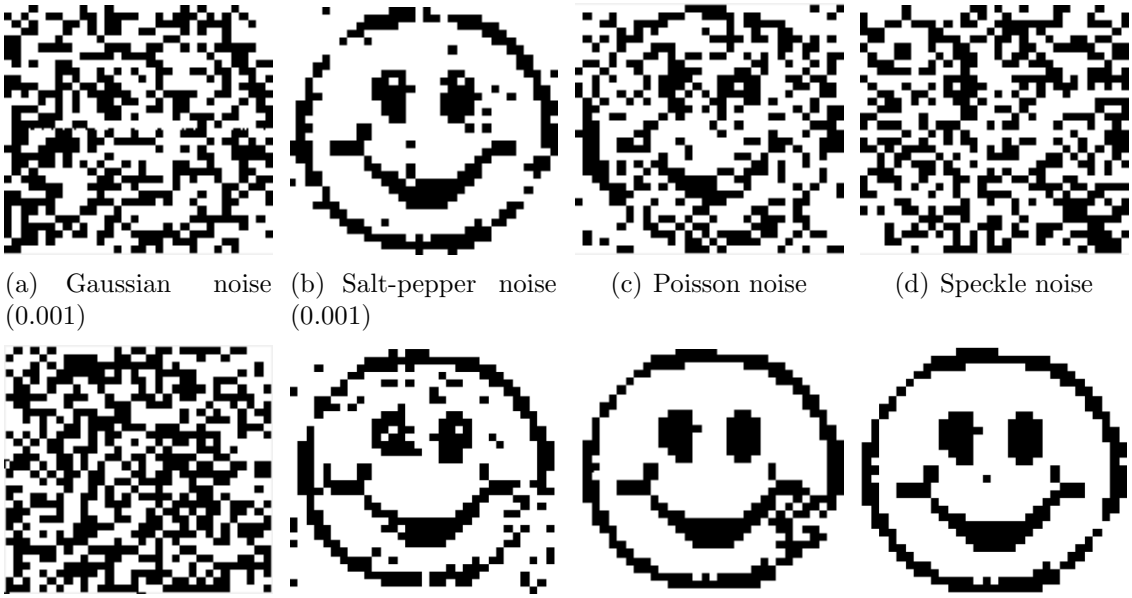


(a) Gaussian noise (0.001) (b) Salt-pepper noise (0.001) (c) Poisson noise (d) Speckle noise

(e) Gaussian low-pass filtering (f) JPEG compression (80%) (g) Cropping (1/16) (h) Brightness (+30)

FIGURE 6. Examples of extracted public share

According to the experimental results in Figure 7, we can see obviously that the proposed scheme is a semi-fragile scheme. It is robust to salt and pepper noise (0.001), JPEG compression (80%), cropping (1/16) and brightness (+30) and it is fragile to attacks such as Gaussian noise, Poisson noise, Speckle noise and Gaussian low-pass filtering. In addition, the scheme is sensitive to cropping. When the watermarked image is cropped as shown in Figure 5(g), the corresponding white area in Figure 6(g) indicates that the area



(a) Gaussian noise (0.001) (b) Salt-pepper noise (0.001) (c) Poisson noise (d) Speckle noise

(e) Gaussian low-pass filtering (f) JPEG compression (80%) (g) Cropping (1/16) (h) Brightness (+30)

FIGURE 7. Examples of stacked image

TABLE 1. Semi-fragility test results under various attacks for six host images

	Peppers		Barche		Baboon		Lena		Barnfall		Apple	
Attacks	PSNR	NC	PSNR	NC	PSNR	NC	PSNR	NC	PSNR	NC	PSNR	NC
Gaussian noise (0.001)	20.33	0.638	20.14	0.661	20.07	0.664	20.20	0.612	20.15	0.659	20.2	0.636
Gaussian noise (0.003)	20.32	0.603	20.15	0.699	20.08	0.677	20.20	0.642	20.12	0.645	20.21	0.634
Salt&pepper noise (0.01)	24.97	0.793	25.36	0.787	25.08	0.835	25.27	0.833	24.91	0.773	25.04	0.76
Salt-pepper noise (0.001)	34.49	0.968	34.65	0.975	34.44	0.993	34.42	0.976	33.56	0.961	34.44	0.963
Poisson noise	27.97	0.75	27.07	0.834	26.85	0.816	27.21	0.735	29.03	0.816	28.61	0.793
Speckle noise	19.95	0.611	18.6	0.7	18.82	0.674	19.21	0.58	22.76	0.698	21.56	0.643
Gaussian low-pass filtering	25.81	0.484	25.25	0.514	21.03	0.535	26.58	0.521	25.34	0.502	33.42	0.508
JPEG (80%)	38.19	0.923	38.05	0.99	33.05	0.941	36.21	0.888	35.25	0.982	41.41	0.901
JPEG (60%)	34.96	0.615	35.08	0.73	29.42	0.794	33.29	0.594	32.19	0.847	39.09	0.547
Cropping (1/16)	15.52	0.956	15.09	0.949	17.67	0.95	18.22	0.958	14.48	0.953	16.4	0.942
Cropping (1/8)	12.53	0.884	14.86	0.895	14.58	0.9	15.53	0.882	12.56	0.873	12.05	0.886
Brightness (+10)	30.51	1	28.83	1	29.21	1	29.89	1	32.84	1	32.24	1
Brightness (+30)	22.19	0.998	20.36	0.992	21.21	0.98	21.52	0.994	23.64	0.998	23.1	1
Brightness (−10)	30.82	1	29.4	1	29.4	1	30.09	1	33.33	1	32.58	1
Brightness (−30)	22.68	0.998	21.13	0.998	21.7	0.996	21.93	0.996	25.05	1	24.11	1

has been tampered. So the result shows the proposed scheme can locate the tampered region accurately. Table 1 summarizes the PSNR and NC values of the six watermarked images under various attacks.

Table 1 shows semi-fragility test results under various attacks; although the host images are different and PSNR and NC values have some fluctuations, the overall analysis and test results are consistent with Figure 7. In addition, we compare the features of the

TABLE 2. Comparison with other similar schemes

Scheme	Pixel expansion	No computation	Tamper detection	With authentication	Watermark extraction	Host image
[13]	Yes	Yes	–	Yes	–	Grayscale
[15]	Yes	Yes	Yes	Yes	No-blind	Grayscale
[16]	Yes	Yes	–	Yes	Stack	Grayscale
Proposed	No	Yes	Yes	Yes	Blind	Color image

proposed scheme with other similar schemes which are analyzed in the introduction, and the qualitative comparison of features are summarized in Table 2.

As can be seen from Table 2, the proposed scheme can simultaneously meet the following features: (1) no pixel expansion, (2) no computation in the decoder, (3) tamper detection, (4) authentication ability, (5) blind detection, and (6) color host images.

5. **Conclusions.** In this paper, a semi-fragile blind watermarking scheme based on Ito et al.'s non-extended visual cryptography model is proposed. The feature of this scheme is that the watermark information can be reconstructed from the shared image without any loss, and the experimental results show that it is robust to the salt and pepper noise (0.001), JPEG compression (80%), cropping (1/16) and brightness (+30), but it is fragile to attacks such as Gaussian noise, Poisson noise, Speckle noise, Gaussian low-pass filtering. This scheme is suitable for some applications that require accurate watermark information restoration and require semi-fragile blind watermarking. Future works will concentrate on the VCS based watermarking techniques for the application of electronic ticket security.

Acknowledgment. This work is partially supported by the Project for Science and Technology Project of Quzhou, China (NO. 2015Y005), the Project for Public Interest Research Project of Science and Technology Program of Zhejiang Province, China (NO. 2016C31097 and NO. 2015C33230), Quzhou 115 Talent Project (Quzhou Liaison Office [2012] 1), and the Natural Science Foundation of Zhejiang Province, China (No. LY15F020041). The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

REFERENCES

[1] B. M. Macq and J. J. Quisquater, Cryptology for digital TV broadcasting, *Proc. of the IEEE*, vol.83, no.6, pp.944-957, 1995.
[2] S. H. Sun, Z. M. Lu and X. M. Niu, *Digital Watermarking Techniques and Application*, Science Publishing Company, 2004.
[3] J. S. Pan, H. C. Huang and L. C. Jain, *Intelligent Watermarking Techniques*, World Scientific, 2004.
[4] M. Naor and A. Shamir, Visual cryptography, *Lecture Notes in Computer Science*, vol.950, no.9, pp.1-12, 1994.
[5] C. Vyas and M. Lunagaria, A review on methods for image authentication and visual cryptography in digital image watermarking, *IEEE International Conference on Computational Intelligence and Computing Research*, pp.1-6, 2015.
[6] C. C. Chang, J. Y. Hsiao and J. C. Yeh, A colour image copyright protection scheme based on visual cryptography and discrete cosine transform, *Image Science Journal*, vol.50, no.3, pp.133-140, 2002.
[7] C. S. Hsu and Y. C. Hou, Copyright protection scheme for digital images using visual cryptography and sampling methods, *Optical Engineering*, vol.44, no.44, 2005.
[8] N. S. Gavini and S. Borra, Lossless watermarking technique for copyright protection of high resolution images, *Region 10 Symposium*, pp.73-78, 2014.

[9] M. Benyoussef, S. Mabtoul, M. E. Marraki et al., Blind invisible watermarking technique in DT-CWT domain using visual cryptography, *The 17th Int. Conf. Image Analysis and Processing (ICIAP 2013), LNCS*, vol.8156, pp.813-822, 2013.

[10] Y. Chen, W. Yu, J. Feng et al., A visual cryptography copyright protection method based on artificial bee colony algorithm, *International Journal of Computer Applications in Technology*, vol.49, no.3/4, pp.297-305, 2014.

[11] Z. Shao, Y. Shang, R. Zeng et al., Robust watermarking scheme for color image based on quaternion-type moment invariants and visual cryptography, *Signal Processing Image Communication*, vol.48, pp.12-21, 2016.

[12] A. E. A. E. Hossaini, M. E. Aroussi, K. Jamali, S. Mbarki, M. Wahbi et al., A new robust blind copyright protection scheme based on visual cryptography and steerable pyramid, *International Journal of Network Security*, vol.18, no.2, pp.250-262, 2016.

[13] W. P. Fang and J. C. Lin, Visual cryptography with extra ability of hiding confidential data, *Journal of Electronic Imaging*, vol.15, no.2, pp.615-629, 2006.

[14] G. Wang, W. Yan and M. Kankanhalli, Content based authentication of visual cryptography, *Multimedia Tools & Applications*, pp.1-15, 2016.

[15] D. Li, Z. Liu and L. H. Cui, A zero-watermark scheme for identification photos based on QR code and visual cryptography, *International Journal of Security and Its Applications*, vol.10, no.1, pp.203-214, 2016.

[16] B. Yan, Y. F. Wang and L. Y. Song, Size-invariant extended visual cryptography with embedded watermark based on error diffusion, *Multimedia Tools and Applications*, vol.75, no.18, pp.11157-11180, 2016.

[17] Y. R. Wang, W. H. Lin and L. Yang, A lossless watermarking using visual cryptography authentication, *International Conference on Machine Learning and Cybernetics*, pp.1109-1113, 2013.

[18] R. Ito, H. Kuwakado and H. Tanka, Image size invariant visual cryptography, *IEICE Trans. Fundamentals*, vol.E82-A, no.10, pp.2172-2177, 1999.

[19] F. X. Yu and Z. M. Lu, A BTC-compressed domain information hiding method based on histogram modification and visual cryptography, *International Journal of Innovative Computing, Information and Control*, vol.12, no.2, pp.395-405, 2016.

[20] J. Xiao and Y. Wang, A robust digital watermarking algorithm based on multiple-level discrete cosine transform, *Chinese Journal of Computers*, vol.32, no.5, pp.1055-1560, 2009.

[21] L. Liu, Y. J. Zhou, B. Zhang et al., Digital watermarking method for QR code images based on DCT and SVD, *Infrared and Laser Engineering*, pp.304-311, 2013.

[22] *http://decsai.ugr.es/cvg/dbimagenes/*.

[23] K. Dabov, A. Foi and K. Egiazarian, Video denoising by sparse 3D transform-domain collaborative filtering, *IEEE Trans. Image Processing*, vol.16, no.8, pp.2080-2095, 2007.