Journal of Information Hiding and Multimedia Signal Processing ©2017 ISSN 2073-4212
Ubiquitous International Volume **8**, Number **3**, May **2017**

Homomorphic Visual Cryptography

Xin Liu[1,2], Shen Wang[1*], Xuehu Yan[3], Weizhe Zhang[1]

[1]Harbin Institute of Technology
Harbin, 150001, China
[2]Harbin University of Science and Technology
Harbin, 150080, China
[3]Hefei electronic engineering institute
230037 Hefei China
[*]Corresponding author: shen.wang@hit.edu.cn
liuxin@hrbust.edu.cn; publictiger@126.com wzzhang@hit.edu.cn

Received September, 2016; revised January, 2017

Abstract. *Recently, a novel visual cryptographic scheme named homomorphic visual cryptographic scheme (HVCS) was proposed. The HVCS inherits the good features of traditional VCS, loss-tolerant, simply reconstructed method, and so on. Meanwhile, the HVCS can support signal processing in the encrypted domain (SPED), e.g., homomorphic operations and authentication. The HVCS can be used to protect the user's privacy as well as improve the security in online internet applications. In this paper, the HVCS is illustrated in detail and more useful HVC operations was exploited. Both the theoretical analysis and simulation results demonstrate the effectiveness and security of the HVCS.*
Keywords: Visual cryptography, Homomorphic visual cryptography, Signal processing in the encrypted domain (SPED), Homomorphic encryption, Online internet service

1. **Introduction.** Nowadays, digital image can be easily obtained, transmitted and manipulated. Security of digital image protects the sensitive information from the malicious behavior during the transmission. An alternative method to ensure the confidentiality and high level security is cryptography. Cryptography deals with the techniques that transform the data between comprehensible and incomprehensible forms by encryption/decryption operations under the control of key(s). It provides the content confidentiality and access control. Even if one bit of the data is destroyed and the whole secret information isn't leaked, the data is not available in cryptography. Therefore, retrieving the original data without any distortion is a matter of importance in case of a certain amount of data is lost in transmission.

Visual secret sharing (VSS) [1, 2], also called visual cryptography (VC), encodes the secret image into different meaningless or meaningful shadows(shares), and distributes them to a group of participants [3, 4, 5]. The process of recovering the secret image is performed by superposing all or some of shadow images. Based on human visual system (HVS) we can easily get the secret image, however, less than the threshold coefficient (k) participants cannot reveal any information of the secret image.

Shamir [6] first proposed (k, n) threshold secret sharing scheme. Using Lagrange's interpolation, the secret image (may be other format data) can be perfectly reconstructed. Following Shamir's study, a lot of polynomial-based schemes [6, 7, 8] were proposed. The secret image can be recovered losslessly which is main advantage. However, Shamir's

polynomial-based schemes requires complicated computations, i.e., Lagrange interpolations, for decoding. The limitation makes it useless without computational device and unsuitable for light-weight devices, such as, mobile phone, smart TV and so on.

Naor and Shamir's scheme [2] suffers from pixel expansion and designing basic matrix. Most studies [3, 4, 5] try to reduce the pixel expansion. The probabilistic VSS (ProbVSS) [3, 4] has no pixel expansion, but it still suffers from designing basic matrix. Random grid (RG)-based VSS which could avoid using basic matrix and expanding pixel get more attention [5, 9, 10]. Then, lots of RG-based VSS focus on improving the visual quality [11, 12, 13]. In order to get the best visual quality of the recovered image, [14, 15, 16] research lossless recovery property of VCS. The lossless recovery can reconstruct the secret losslessly if the light-weight computation device is available.

At the same time, online applications, social networking, distributed processing and cloud computing have been rapidly developed. Which have raised important concerns about the security (privacy) of user-related content [17]. If the processor itself is untrusted [17], the data can not be protected by the traditional cryptographic technologies, for example, more and more data leakages. All the online service provider need personal information of users, the service providers may gain a lot about a user's privacy information, past behavior, preferences, and biometrics. In order to use the service, the user must trust the online service provider requiring his personal data. Nevertheless, the online service provider may be untrusted. Thus, the use of personal information in presentation and processing becomes more varied with more flexibility.

Particularly, advanced biometric techniques are increasingly employed to verify the identity of a person with digital photos [18, 19, 20], such as, face recognition/authentication. The surveillance cameras in public areas led to the high interest in face recognition technologies [17], aiming to automatically match the faces of people shown on surveillance images against a database of known suspects. If the face recognition process is performed or stored at untrusted or only a central cloud server, the widespread use of biometrics raises lots of privacy risks. The image of faces might be used in criminal and deceptive behavior.

Signal processing in the encrypted domain (SPED) technologies [21] are proposed to address the issue, such as homomorphic encryption [22, 23, 24] and authentication. The main motivator is to process the sensitive signals at potentially untrusted sites, minimally or leaking no information. However, homomorphic encryption and authentication are not loss-tolerant and require more complicated computations for decryption. The homomorphic encryption and VCS are effectively combined (Homomorphic VCS, HVCS) may be an alternative way to solve the problem, which will be introduced in detail in this paper. In HVCS, secret images are processed through the shares (encrypted domain) which shows the security of the HVCS. Based previous study [25], this paper introduces HVCS in detail and exploits the homomorphic property of traditional VC. The HVCS achieves the features of both homomorphic encryption and VSS. The contribution of this paper lies in: 1) the homomorphic property of traditional VC is exploited; 2) some operations of traditional VCS are proved or validated to support HVC operations. The traditional RG-based VCS as an example are exploited to support HVC operations in the proposed schemes. The proposed schemes have homomorphic property where the result of a specific signal processing operation performed on the secret image is equivalent to that of the decryption of the same (may be different) signal processing operation performed on the shares. Moreover, they allow the authentication to be carried out by utilizing the shadows instead of the original secret image. Simulation results show the effectiveness of the proposed schemes.

The rest of the paper is organized as follows. Section 2 introduces the preliminary techniques as the basis for our method. In Section 3, the proposed schemes are presented in detail. Section 4 is devoted to experimental results. Finally, Section 5 concludes this paper.

2. **Preliminaries.** In this section, we introduce some preliminaries and related works about RG-based VCS [5, 9] which are the basis for our method. In what follows, the binary secret image S sized of $M \times N$ is shared among n shadow images which are denoted as $SC_p(1 \leq p \leq n)$, while the recovered secret image S' is recovered from t $(2 \leq t \leq n, t \in \mathrm{Z}^+)$ shadow images by stacking or calculating. The symbols $\oplus$ and $\otimes$ denote the Boolean XOR and OR operations. In this paper, 0 is for white and 1 is for black.

For a certain pixel x in a binary image X with size of $M \times N$, i.e., $x = X(i,j)$, the pixel color is transparent or white (0), say $(x = 0)$, and the same for that pixel color is opaque or black(1). Besides, $(X = 0) = 1 - \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} X(i,j), 1 \leq i \leq M, 1 \leq j \leq N$.

The generation and recovery phases of one original (2, 2) RG-based VCS [5] are described below.

Generation:

Step 1: Randomly generate 1 RG SC_1 .

Step 2: Compute SC_2 using Eq.(1).

Recovery:

$S' = SC_1 \otimes SC_2$ using Eq.(2). If a certain secret pixel of $S(i,j)$, simply denoted as s, is 1, the recovery result $SC_1 \otimes SC_2 = 1$ is always black. If s is 0, the recovery result $SC_1 \otimes SC_2 = SC_1(i,j) \otimes SC_1(i,j)$ has half chance to be black or white since SC_1 are generated randomly.

$$SC_2(i,j) = \begin{cases} SC_1(i,j) & if\ S(i,j) = 0 \\ \overline{SC_1(i,j)} & if\ S(i,j) = 1 \end{cases} \tag{1}$$

$$S'(i,j) = SC_1(i,j) \otimes SC_2(i,j) = \begin{cases} SC_1(i,j) \otimes \overline{SC_1(i,j)} & if\ S(i,j) = 0 \\ SC_1(i,j) \otimes \overline{SC_1(i,j)} = 1 & if\ S(i,j) = 1 \end{cases} \tag{2}$$

3. **Homomorphic visual cryptography.** In this section, the definition of the HVCS will be given and some HVC operations and their analyses are given in detail.

3.1. **Definition of HVCS.** All the participants are denoted as $\mathcal{P} = \{1, 2, \cdots n\}$. The original binary secret image S is shared among n $(2 \leq n, n \in Z^+)$ shadow images $SC_1, SC_2, \cdots SC_n$ by generation function E, that is $(SC_1, SC_2, \cdots SC_n) = E(S)$; while the recovered secret image is recovered from t $(1 \leq t \leq n, t \in Z^+)$ shadow images by recovery function D, that is $S' = D(SC_{i_1}, SC_{i_2}, \cdots SC_{i_t})$, where $(i_1, i_2, \cdots, i_t)$ is the subsequence of $(1, 2, \cdots, n)$ and $t = 1$ means $SC_i = S$ or $S' = S$.

According to the recent study [25], the definition of HVCS is introduced as follows.

Definition 1 (HVCS): A VCS is a HVCS if there exist $f_1()$ and $f_2()$ satisfying one of the following two conditions:

1) For one secret image. $f_1(S') = D(f_2(SC_{i_1}, SC_{i_2}, \cdots SC_{i_t}))$.

2) For two secret images.

$f_1(S_1', S_2') = D(f_2(S_1C_{i_1}, S_1C_{i_2}, \cdots S_1C_{i_t}, S_2C_{i_1}, S_2C_{i_2}, \cdots S_2C_{i_t}))$.

where, $f_1()$ and $f_2()$ denote two operations which are also called HVC operations in VCS. Two original recovered secret image ${S_1}'$ and ${S_2}'$ without operations corresponding to the original two secret image S_1 and S_2, respectively.

The above two conditions imply:

1. The result of the operation $f_1()$ on the original revealed secret image S' is the same as that of the decryption of the operation $f_2()$ on the corresponding random shares.
2. The result of the operation $f_1()$ on the two original revealed secret images ${S_1}'$ and ${S_2}'$ is the same as that of the decryption of the operation $f_2()$ on the corresponding random shares.

Based on definition 1, a HVCS is a VCS with HVC operation. The above definition can be extended to share more than two secret images based on repeatedly applying definition 1.

It is noting that the HVCS belongs to partial homomorphic encryption [24] from the non-strict sense, since we only perform one operation on encrypted data (shares) in HVCS.

3.2. **HVC operations for single secret image.** In traditional VCS, the secret image is encrypted pixel by pixel, thus pixel-based operations belong to HVC operations. Some HVC operations for singel secret image are stated as follows.

1. Cutting operation: removing part of S' or shares.
2. Darkening operation: making S' or shares become darker.
3. Brightening operation: making S' or shares lighter or brighter.
   Based on the result of darkening or brightening operation, we can approximate the result of noise operation.
4. Rotation operation: a transformation in which the coordinate axes are rotated by a fixed angle about the origin.
5. Scaling operation: enlarging the size of S' or shares.
6. Permutation operation: changing the arrangement of pixels in S' or shares. Based on the HVC permutation operation, the permutation encryption of the original secret image can be performed on the ciphertext shares instead of the plaintext secret image. In addition, after the secret image is encrypted by the HVC permutation operation, the contrast also can be computed in the encrypted domain rather than the plaintext domain.

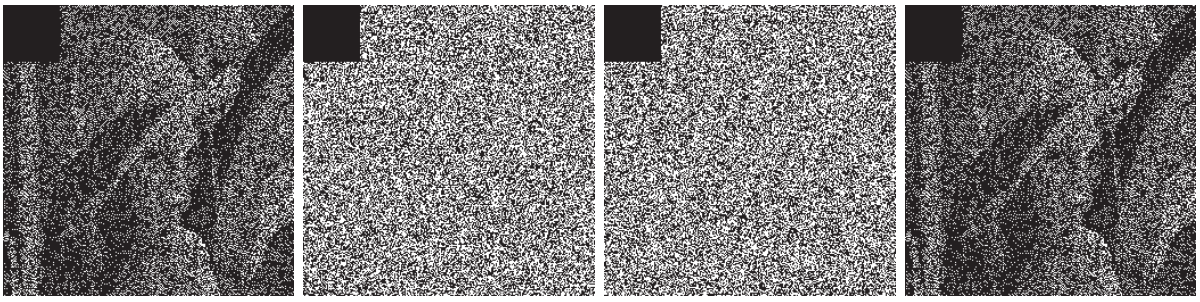
The above HVC operations are also suitable for (k, n) threshold VCS. For case (k, n), the secret recovery is based on superposing ($\otimes$) or HVS when directly stacking k or more shares. Besides, if less than k shares are stacked, the original secret image information will not be revealed.

3.3. **HVC operation for multiple images.** HVC operation for multiple secret images is suitable for the application scenario that multiple secret images should be protected. In the following, the two secret images as an example to illustrate the HVC operation. Firstly, the XOR operation is a HVC operation will be proven when both two secret images need protection. Where both $f_1()$ and $f_2()$ denote the XOR operation. Then some other HVC operations such as AND operation for two secret images are proved when only one secret image S_1 needs protection.

In fact, Eq.(1) is equal to

$$sc_2 = sc_1 \oplus s \ or \ s = sc_1 \oplus sc_2 \tag{3}$$

since if $s = 0$, we have $sc_2 = sc_1$
else $s = 1$, $sc_2 = \overline{sc_1}$



(a) (b) (c) (d)

FIGURE 1. Simulation result of HVC cutting operation for single secret image. (a) The original recovered secret image S' performed the HVC operation; (b) − (c) two shares SC_1 and SC_2 performed the HVC operation; (d) stacking result by (b) and (c).

The same equation can be extended to $s = sc_1 \oplus sc_2 \oplus \cdots \oplus sc_k$ and the VCS can be extended to (k, k) RG-based VCS.

Based on the above discussions, when XOR operation is applied for two secret images S_1 and S_2, we have:

$$\begin{aligned} S_1 &= S_1C_1 \oplus S_1C_2 \oplus \cdots \oplus S_1C_k \\ S_2 &= S_2C_1 \oplus S_2C_2 \oplus \cdots \oplus S_2C_k \end{aligned} \tag{4}$$

Thus,

$$S_1 \oplus S_2 = (S_1C_1 \oplus S_2C_1) \oplus (S_1C_2 \oplus S_2C_2) \oplus \cdots \oplus (S_1C_k \oplus S_2C_k) \tag{5}$$

Hence, the XOR operation is a HVC operation based on definition 1 for two secret images S_1 and S_2, where the recovery function $D()$ indicates XOR operation. The feature can be applied for authentication in encrypted domain, which can improve the security. An $(2, 2)$ application diagram is illustrated in Fig. 2. The template is generated into two random shares in the enrollment step. The two shares are stored in two different databases respectively.

For authentication, the input template is generated into two shares by the $(2, 2)$ RG-based VCS. Based on the proposed HVC operation, the authentication can be achieved by the shares instead of the original secret image. Thus, the original secret image and the template are protected in a degree.

Both enrolled secret image and the verified secret image are protected through above HVC operation. If only the enrolled secret image needs protection, i.e., the verified secret image might be plaintext. This situation can be handled by two cases. Case 1: based on XOR operation; Case 2 based on AND(&) operation.

Case 1: based on XOR operation.

$$S_2 \oplus S_1 = S_2 \oplus (S_1C_1 \oplus S_1C_2) = (S_2 \oplus S_1C_1) \oplus S_1C_2 \tag{6}$$

For the (k, k) RG-based VCS,

$$S_2 \oplus S_1 = S_2 \oplus (S_1C_1 \oplus S_1C_2 \oplus \cdots \oplus S_1C_k) = (S_2 \oplus S_1C_1 \oplus \cdots \oplus S_1C_{k-1}) \oplus S_1C_k \tag{7}$$

Thus, it is proved theoretically that XOR operation is a HVC operation when only one secret image needs protection.

Case 2: based on & operation.

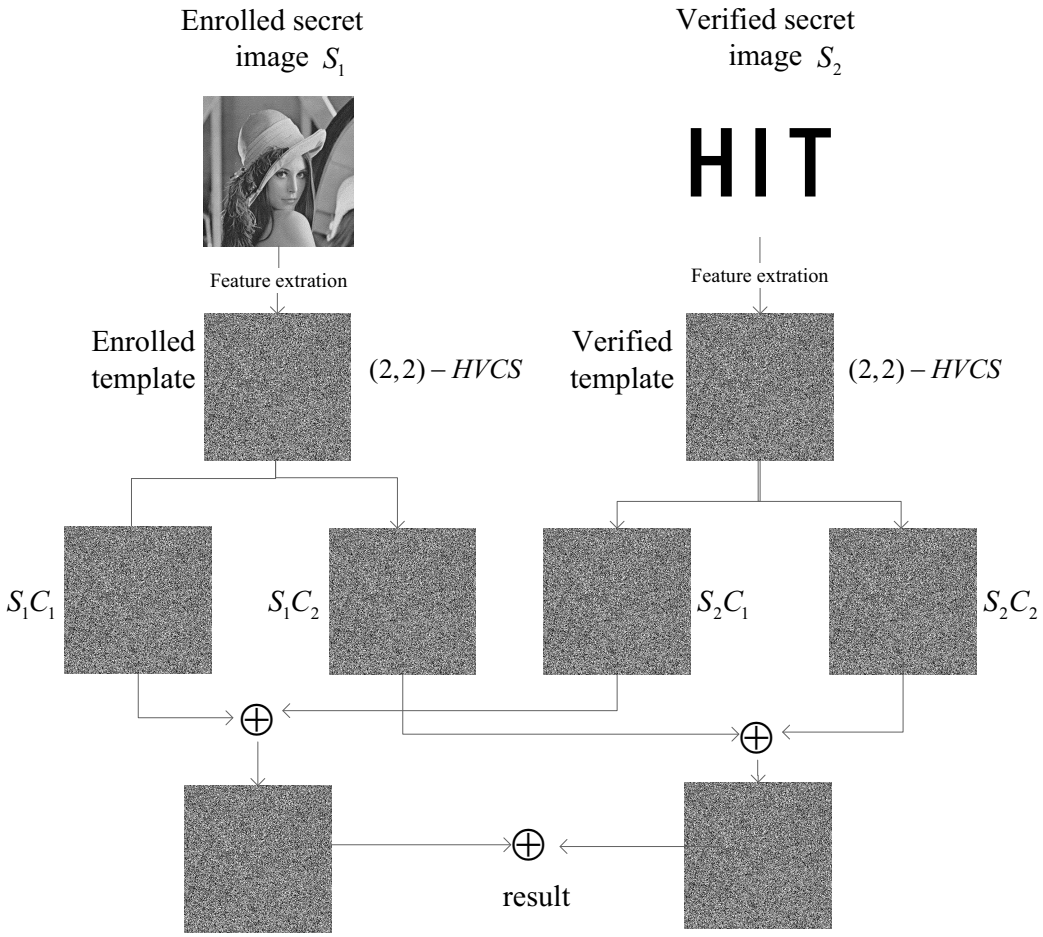


FIGURE 2. An application diagram of the proposed HVC operation for two secret images

$$S_2\&S_1 = S_2\&\left(S_1C_1 \oplus S_1C_2\right) = \left(S_2\&S_1C_1\right) \oplus \left(S_2\&S_1C_2\right) \tag{8}$$

For the (k, k) RG-based VCS,

$$S_2\&S_1 = S_2\&\left(S_1C_1 \oplus S_1C_2\right) = \left(S_2\&S_1C_1\right) \oplus \left(S_2\&S_1C_2\right) \oplus \cdots \oplus \left(S_2\&S_1C_k\right) \tag{9}$$

Hence, & operation also is a HVC operation when only one secret image needs protection. Here, both $f_1()$ and $f_2()$ denote the & operation and the recovery function $D()$ indicates XOR operation.

Further, both $f_1()$ and $f_2()$ denote the & operation and the recovery function $D()$ indicates $\otimes$ operation, which also can be proved to be a HVC operation according to the following equation:

$$S_2\&\left(S_1C_1 \otimes S_1C_2\right) = \left(S_2\&S_1C_1\right) \otimes \left(S_2\&S_1C_2\right) \tag{10}$$

For the (k, k) RG-based VCS,

$$S_2\&\left(S_1C_1 \otimes S_1C_2\right) = \left(S_2\&S_1C_1\right) \otimes \left(S_2\&S_1C_2\right) \otimes \cdots \otimes \left(S_2\&S_1C_k\right) \tag{11}$$

Herein, it should be noted that we should exclude the cheaters for security in the above applications.

In summary, the features of the proposed HVCS for biometrics privacy protection lie in:

1. The template is generated into two shares which are stored in two different databases respectively, and the separately share reveals nothing about the template. Which more security than that they are stored in only one central database. In addition, the approach can be extended to generate k shares.
2. The proposed HVCSs with no pixel expansion, which could reduce the storage and transmission bandwidth. In addition, the VCS with meaningful shares [26] can be applied in the proposed schemes, because it can increase the efficiency of management and security.
3. Without reconstructing the original secret template authentication can be achieved by the shares, which can decrease the risk of template leakage.
4. The recognition or authentication can be realized without preserving and showing an ID card which is main advantage of biometrics. The same user can generate different shares for each validation.
5. No encryption key is used in the HVCSs.

3.4. **Extension for grayscale/color images.** The proposed schemes can be extended to share grayscale/color images [1, 27]. To share a grayscale image, halftone technologies such as error diffusion [27] are applied to convert the grayscale image into a binary image, then the proposed schemes could be applied. In order to share a high-resolution grayscale image, two methods may be used, please refer to [1].

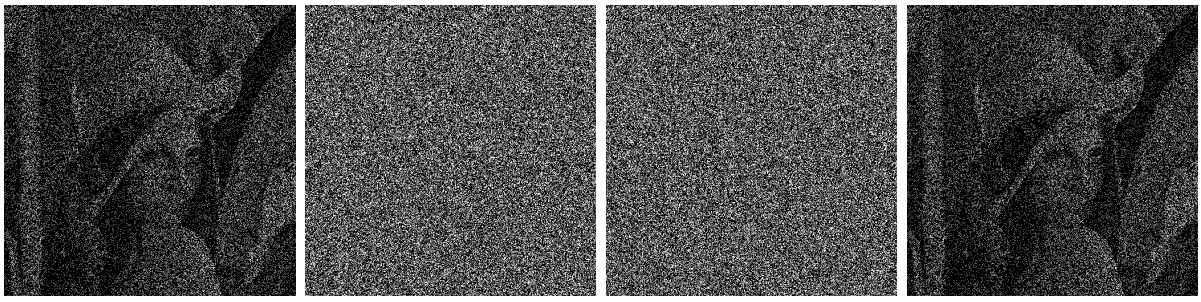
For sharing a color image, color decomposition and color composition are applied. A color image can be described by color model, such as CMY (cyan–magenta–yellow) model. CMY is a subtractive color model which displays a color by reflecting light from a surface of an object. The color secret image is decomposed into three color components first. Then our methods for grayscale images can be applied.

4. **Experimental results.** In this section, based on traditional RG-based $(2, 2)$ VCS [5], we perform the experiments to evaluate the effectiveness of the proposed schemes. In the experiment we only focus on binary secret images since the binary secret image is the basic object in VCS. In addition, some comparisons and discussions are provided.

Fig. 1 presents simulation result of HVC cutting operation for singel secret image. 1 (a) is the original recovered secret image S' performed the HVC operation. Fig. 1 (b) − Fig. 1 (c) are the shares performed the HVC operation. The stacking result by the two shares is illustrated in Fig. 1 (d), which reconstructs the secret performed the HVC operation. The experiment also proves that cutting operation is a HVC operation for single secret image.

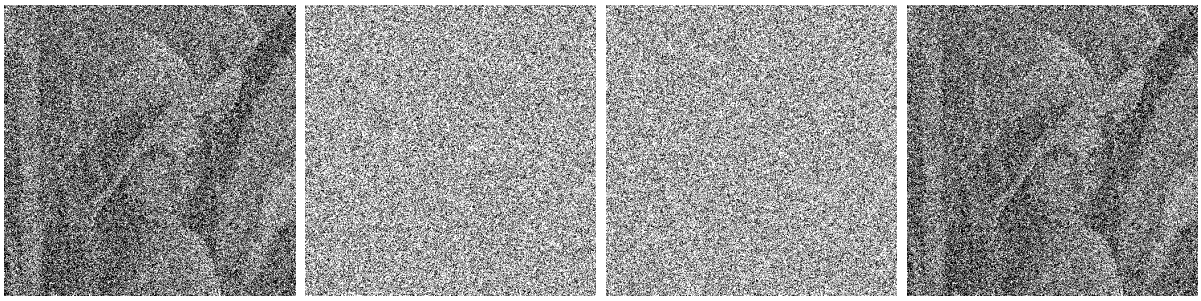
Simulation results of some HVC operations for one secret image are exhibited in Fig. 3, Fig. 4, Fig. 5, Fig. 6 and Fig. 7 corresponding to darkening operation, brightening operation, rotation operation, scaling operation and permutation operation, respectively. The same results as cutting operation can be obtained for these HVC operations. In the experiment for permutation operation, i.e., Fig. 7, we use Arnold permutation with $T = 100$ iterations, and its process is shown in Eq. (12), where (i', j') is the position after permutation corresponding to the original position (i, j). For an image with size of $M \times N$ one can choose M or N in the Arnold permutation, here we use M. The permutation can also be implemented by other methods, such as: chaotic standard map and Baker map encryption.

$$\begin{bmatrix} i' \\ j' \end{bmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}^T \begin{bmatrix} i \\ j \end{bmatrix} (\text{mod } M) \tag{12}$$



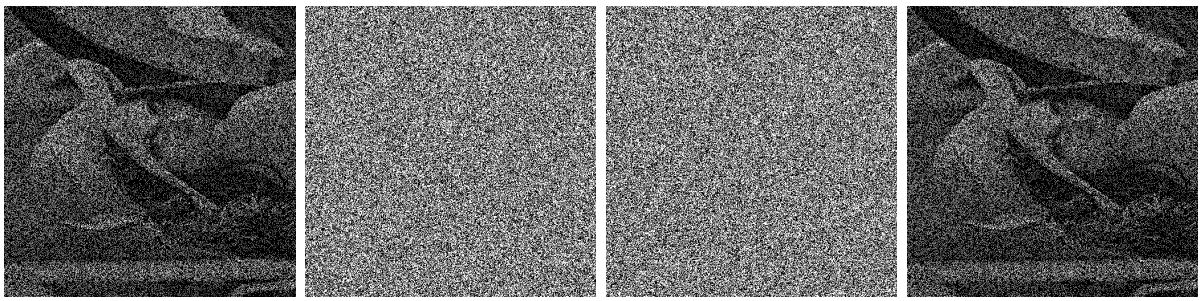
(a) (b) (c) (d)

FIGURE 3. Simulation result of HVC darkening operation for one secret image with darkening degree 30%. (a) The original recovered secret image S' performed the HVC operation; (b) − (c) two shares SC_1 and SC_2 performed the HVC operation; (d) stacking result by (b) and (c).



(a) (b) (c) (d)

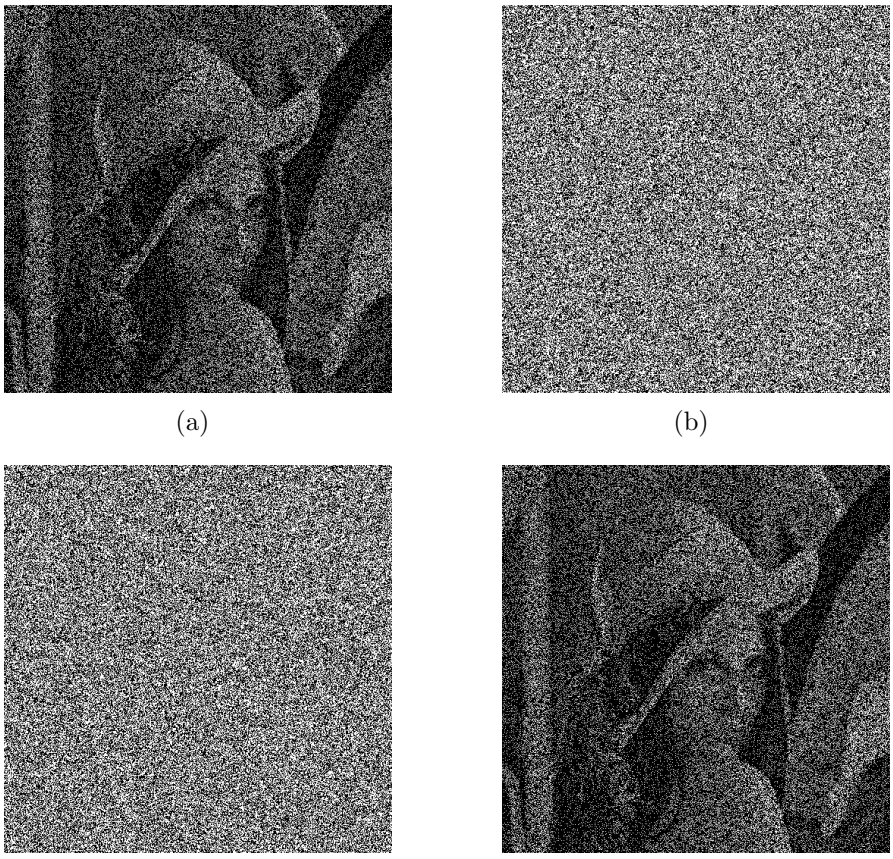
FIGURE 4. Simulation result of HVC brightening operation for one secret image with brightening degree 30%. (a) The original recovered secret image S' performed the HVC operation; (b) − (c) two shares SC_1 and SC_2 performed the HVC operation; (d) stacking result by (b) and (c).



(a) (b) (c) (d)

FIGURE 5. Simulation result of HVC rotation operation for one secret image with rotation angle 90. (a) The original recovered secret image S' performed the HVC operation; (b) − (c) two shares SC_1 and SC_2 performed the HVC operation; (d) stacking result by (b) and (c).

Fig. 8 demonstrates the simulation result of HVC XOR operation for two secret images. Fig. 8 (a) is the secret image S_1 and Fig. 8 (b) and Fig. 8 (c) show the corresponding two shares. Fig. 8 (d) is the secret image S_2 and Fig. 8 (e) and Fig. 8 (f) show the



(a) (b)

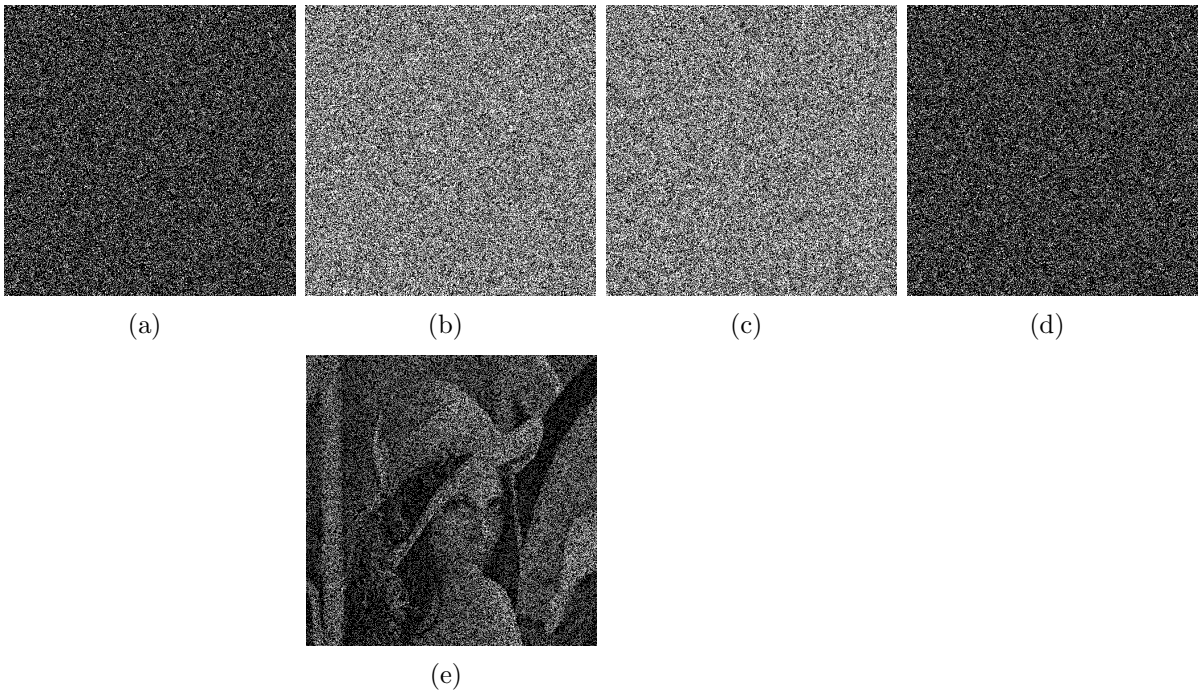
(c) (d)

FIGURE 6. Simulation result of HVC scaling operation for one secret image with scaling factor 2. (a) The original recovered secret image S' performed the HVC operation; (b) − (c) two shares SC_1 and SC_2 performed the HVC operation; (d) stacking result by (b) and (c).

corresponding two shares. Fig. 8 (g) indicates HVC XOR operation result of (a) and (d), and HVC XOR operation result of (b) and (e) is given in Fig. 8 (h). Fig. 8(i) shows HVC XOR operation result of (c) and (f), and Fig. 8(j) presents XOR result by (h) and (i). Through the experiment, we can see Fig. 8 (j) is same as Fig. 8 (g). Thus, XOR operation achieves homomorphic feature and XOR operation is a HVC operation for two secret images.

Fig. 9, Fig. 10 and Fig. 11 present simulation results of other HVC operations for two secret images when only one secret image S_1 needs protection. The same results as the above HVC XOR operation can be obtained for these HVC operations.

5. **Conclusion.** The novel homomorphic visual cryptographic scheme has some good features, such as loss-tolerant, simply reconstructed method and homomorphic feature. The result of a HVC operation performed on the secret image is equivalent to that of the decryption of the same HVC operation performed on the shares. The HVCS can be used for authentication and recognition, which can protect the privacy in online internet applications. This paper illustrates the HVCS more detail and exploit more useful HVC operations. Both the theoretical analysis and simulation results demonstrate the effectiveness and security of the HVCS. The HVCS may be used for more other applications.



(a) (b) (c) (d)

(e)

FIGURE 7. Simulation result of HVC permutation operation for one secret image. (a) The original recovered secret image S' after permutation; (b) – (c) two shares SC_1 and SC_2 after permutation; (d) stacking result by (b) and (c); (e) the decryption result from (d).

Acknowledgement. The authors would like to thank the anonymous reviewers for their valuable discussions and comments. This work is supported by the National Natural Science Foundation of China (Grant Number: 61471141, 61361166006, 61301099, 61472108, 61672186, 61501148,), the National Key Research and Development Program of China (Grant Number: 2016YFB0800801), Key Technology Program of Shenzhen, China, (No. JSGG20160427185010977) and Basic Research Project of Shenzhen, China (Grant Number:JCYJ20150513517065 61).

REFERENCES

[1] X. Yan, S. Wang, A. A. A. El-Latif, and X. Niu.: A novel perceptual secret sharing scheme *Springer Transactions on Data Hiding and Multimedia Security (DHMS)*, pp. 68-90, 2013.

[2] M. Naor, A. Shamir, Visual cryptography. In: *Advances in CryptologyEUROCRYPT'94 Lecture Notes in Computer Science, Workshop on the Theory and Application of Cryptographic Techniques,* May 9C12, pp. 1-12. Springer, Springer, Perugia, Italy (1995)

[3] C.N. Yang, New visual secret sharing schemes using probabilistic method. *Pattern Recognit. Lett.* vol. 25, no. 4, pp. 481-494, 2004

[4] S.Cimato, R. De Prisco, , De Santis, A.: Probabilistic visual cryptography schemes. *The Computer Journal* , vol. 49, no. 1, pp. 97-107, 2006.

[5] O. Kafri, E. Keren, : Encryption of pictures and shapes by random grids. *Optics Letters* , vol. 12, no. 6, pp. 377-379, 1987.

[6] A. Shamir, How to share a secret, C*ommunications of the ACM, vol.* 22, no. 11, 1979. 612–613.

[7] C.-C. Thien, J.-C. Lin, Secret image sharing, *Computers & Graphics* , vol.26 , no. 5 pp. 765–770, 2002.

[8] C.-N. Yang, C.-B. Ciou, Image secret sharing method with two-decoding-options: Lossless recovery and previewing capability, Image and Vision Computing 28 (12) (2010) 1600–1610.

[9] Liu, F., Wu, C., Qian, L., et al.: Improving the visual quality of size invariant visual cryptography scheme. Journal of Visual Communication and Image Representation , vol. 23, no. 2), 331–342 (2012)

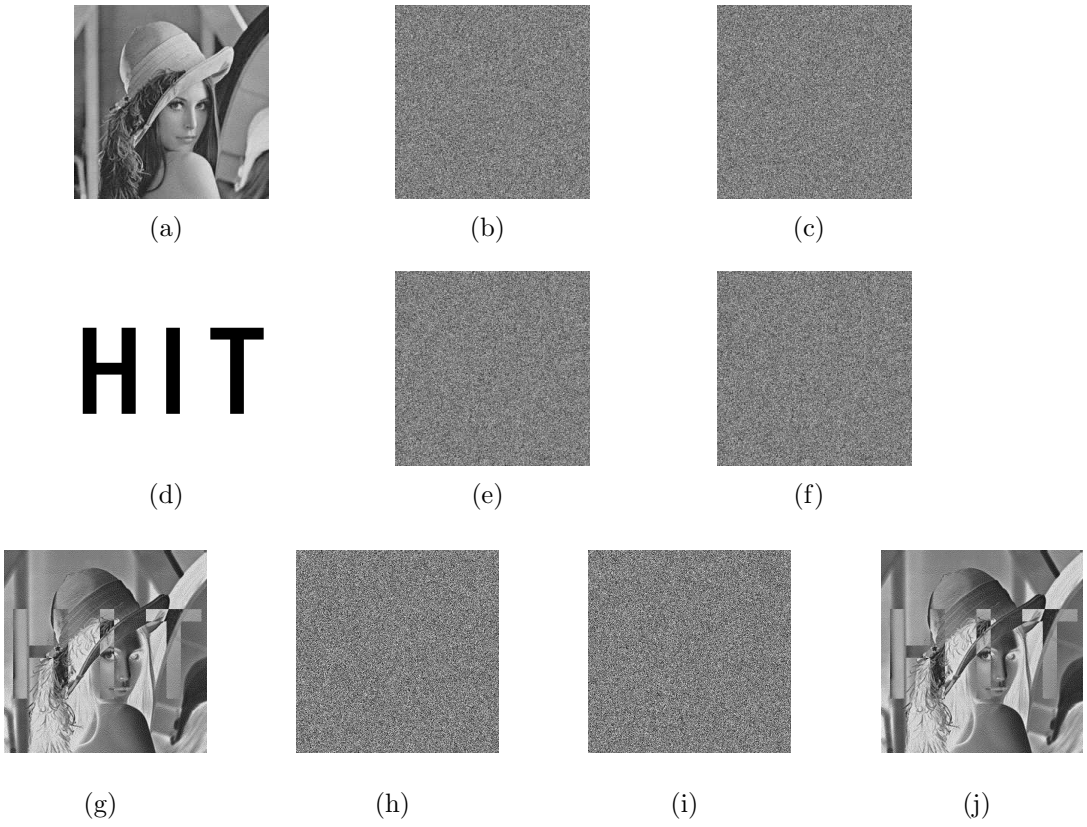


FIGURE 8. Simulation result of HVC XOR operation for two secret images. (a) The original secret image S_1; (b) − (c) two shares S_1C_1 and S_1C_2; (d) The original secret image S_2; (e) − (f) two shares S_2C_1 and S_2C_2; (g) HVC XOR operation result of (a) and (d); (h) HVC XOR operation result of (b) and (e); (i) HVC XOR operation result of (c) and (f); (j) XOR result by (h) and (i).

[10] Yan, X., Wang, S., Niu, X.: Threshold construction from specific cases in visual cryptography without the pixel expansion. Signal Processing , vol. 105, pp. 389-398 (2014)
[11] Chen, T.H., Tsao, K.H.: Image encryption by (n,n) random grids. In: Proceedings of 18th Information Security Conference, Hualien (2008)
[12] Wu, X., Sun, W.: Improving the visual quality of random grid-based visual secret sharing. Signal Processing , vol. 93, no. 5), pp. 977-995 (2013)
[13] X. Yan, X. Liu, Yang, C.N.: An enhanced threshold visual secret sharing based on random grids. Journal of Real-Time Image Processing , pp. 1-13 (2015)
[14] Chen, G., Wang, C., Yan, X., Li, P.: Progressive Visual Secret Sharing with Multiple Decryptions and Unexpanded Shares. Digital-Forensics and Watermarking - 13th International Workshop (IWDW), Taiwan (2014)
[15] Wu, X., Sun,W.: Random grid-based visual secret sharing with abilities of OR and XOR decryptions. JVis Commun Image R , vol. 37, pp. 48C62, (2013)
[16] Liu, X., Wang, S., Sang, J., et al.: A novel mapping-based lossless recovery algorithm for VSS. Journal of Real-Time Image Processing, 1-10, (2016)
[17] R. L. Lagendijk, Z. Erkin, M. Barni, Encrypted signal processing for privacy protection: Conveying the utility of homomorphic encryption and multiparty computation, Signal Processing Magazine, IEEE 30 (1) (2013) pp. 82-105.
[18] Y. S. Rao, Y. Sukonkina, C. Bhagwati, U. K. Singh, Fingerprint based authentication application using visual cryptography methods (improved id card), in: TENCON 2008-2008 IEEE Region 10 Conference, IEEE, 2008, pp. 1–5.

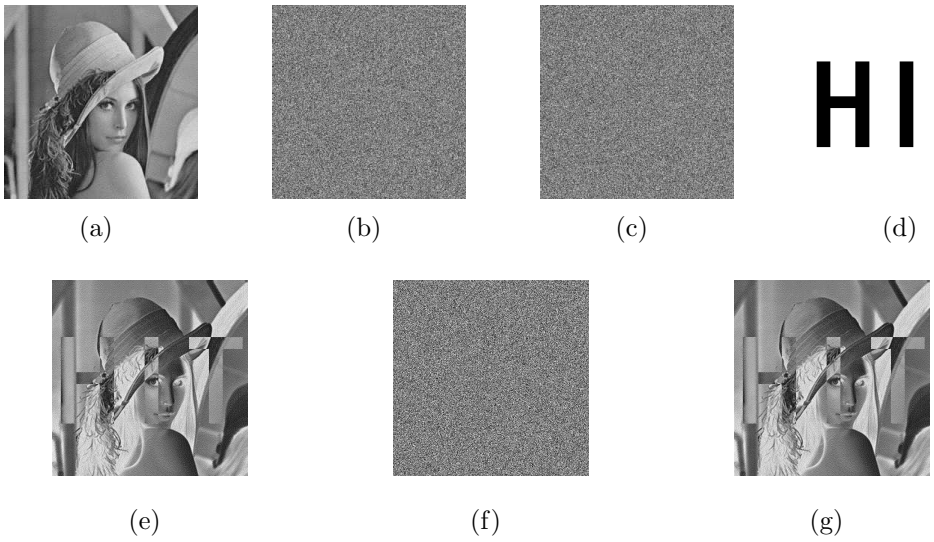


FIGURE 9. Simulation result of HVC XOR operation for two secret images when only one secret image S_1 needs protection, where both $f_1()$ and $f_2()$ denote the XOR operation and recovery function $D()$ indicates XOR operation. (a) The original secret image S_1; (b) − (c) two shares S_1C_1 and S_1C_2; (d) The original secret image S_2; (e) XOR operation result of (a) and (d); (f) XOR operation result of (d) and (b); (g) XOR operation result of (f) and (c).

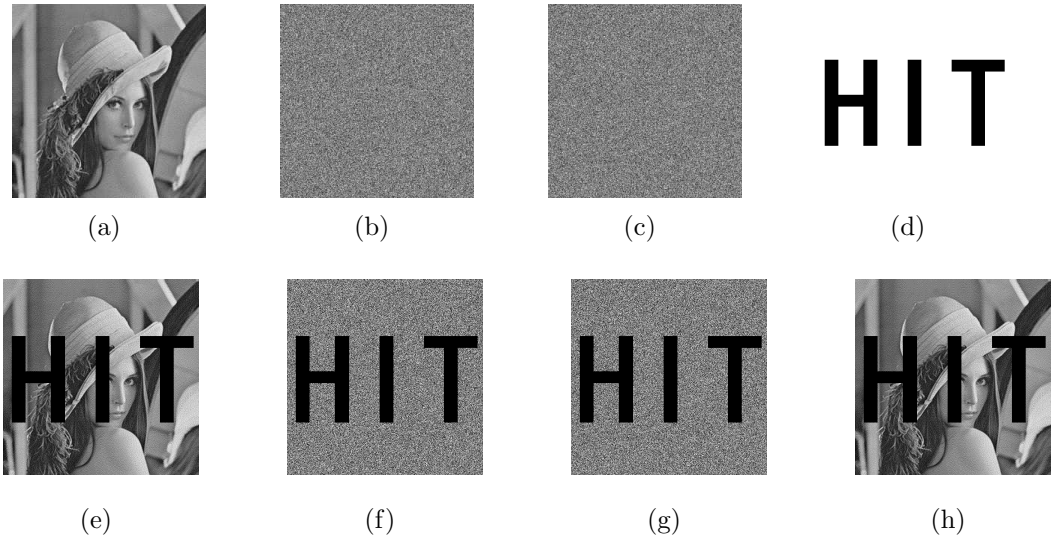


FIGURE 10. Simulation result of HVC XOR operation for two secret images when only one secret image S_1 needs protection, where both $f_1()$ and $f_2()$ denote the & operation and recovery function $D()$ indicates XOR operation. (a) The original secret image S_1; (b) − (c) two shares S_1C_1 and S_1C_2; (d) The original secret image S_2; (e) & operation result of (a) and (d); (f) & operation result of (d) and (b); (g) & operation result of (d) and (c); (h) XOR result by (f) and (g).

[19] P. Revenkar, A. Anjum, W. Gandhare, Secure iris authentication using visual cryptography, arXiv preprint arXiv:1004.1748.

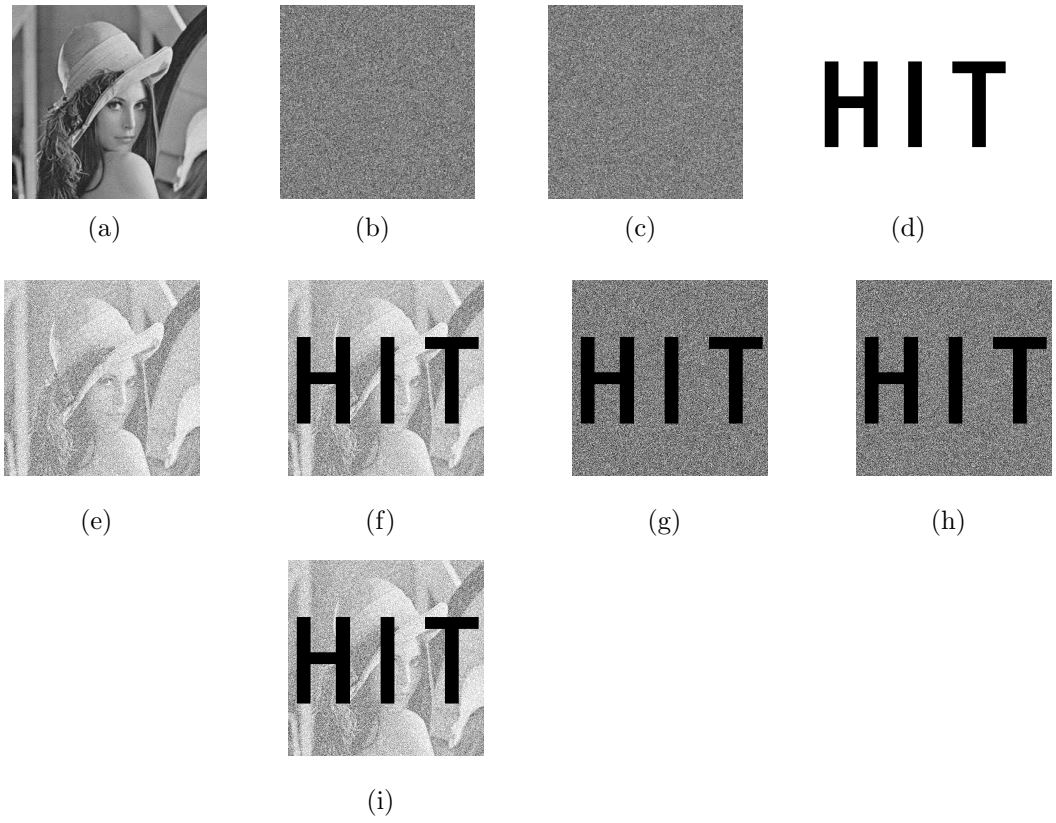


FIGURE 11. Simulation result of HVC XOR operation for two secret images when only one secret image S_1 needs protection, where both $f_1()$ and $f_2()$ denote the & operation and recovery function $D()$ indicates OR operation. (a) The original secret image S_1; (b) − (c) two shares S_1C_1 and S_1C_2; (d) The original secret image S_2; (e) OR operation result of (b) and (c); (f) & operation result of (d) and (e); (g) & operation result of (d) and (b); (h) & operation result of (d) and (c); (i) OR result by (g) and (h).

[20] A. Ross, A. Othman, Visual cryptography for biometric privacy, IEEE transactions on information forensics and security 6 (1) (2011) pp. 70–81.
[21] M. Barni, T. Kalker, S. Katzenbeisser, Inspiring new research in the field of signal processing in the encrypted domain [from the guest editors], Signal Processing Magazine, IEEE 30 (2) (2013) pp. 16–16.
[22] L. Li, A. A. Abd El-Latif, X. Niu, Elliptic curve elgamal based homomorphic image encryption scheme for sharing secret images, Signal Processing 92 (4) (2012) 1069–1078.
[23] Z. Erkin, A. Piva, S. Katzenbeisser, R. L. Lagendijk, J. Shokrollahi, G. Neven, M. Barni, Protection and retrieval of encrypted multimedia content: When cryptography meets signal processing, EURASIP Journal on Information Security 2007.
[24] N. Smart, F. Vercauteren, Fully homomorphic simd operations, Designs, Codes and Cryptography 71 (1) (2014) pp. 57–81.
[25] Yan, Xuehu, et al. "Exploiting the Homomorphic Property of Visual Cryptography." International Journal of Digital Crime and Forensics (IJDCF) 9.2 (2017), pp. 45-56.
[26] C.-N. Yang, Y.-Y. Yang, New extended visual cryptography schemes with clearer shadow images, Information Sciences 271 (2014), pp. 246–263.
[27] X. Wu, W. Sun, Improving the visual quality of random grid-based visual secret sharing, Signal Processing 93 (5) (2013), pp. 977–995.