Journal of Information Hiding and Multimedia Signal Processing ©2014 ISSN 2073-4212
Ubiquitous International Volume **5**, Number **1**, January **2014**

Visual Cryptography for Gray-scale Images Using Bit-level

D. Taghaddos, A. Latif
Electrical and Computer Engineering Department
Yazd University
Yazd, Iran
taghaddos@stu.yazd.ac.ir, alatif@yazd.ac.ir

Received May, 2013; revised September, 2013

Abstract. *Cryptographic schemes are presented for communication to fulfill the need for security. Visual cryptography is an image cryptographic scheme in which a secret image is encrypted into two separate share images. Each share individually reveals no information about the secret, but when shares are superposed the secret is revealed. Almost all of the previous presented variants of VC are designed for binary images that are not qualified for most applications. In this paper, a new variant of visual cryptography for gray-scale images is presented. We use bit-level decomposition to extract binary bit planes from a gray-scale image. Then the bit planes are encrypted and recomposed back as two gray-scale shares. The secret image is revealed when two gray-scale shares are superposed. Experimental results show that the quality of the revealed secret is satisfactory.*
Keywords: Visual cryptography, Bit-level decomposition, Gray-scale image, Visual secret sharing.

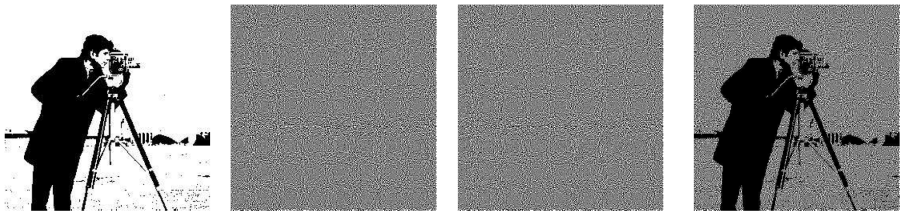
1. **Introduction.** One of the reasons of secure communication is widespread of open access computer networks such as Internet. Digital images are one of the most important data that is transferred over these networks. Some important solutions of secure communication for data images such as secret key cryptography, watermarking, secret sharing schemes, etc. are presented [6, 7, 8]. Image encryption is applied to secure the communication with digital images. Traditional image encryption schemes encrypt the image based on mathematical algorithms using some keys. Image decryption without the keys is impossible and image data cannot be retrieved correctly. One of the disadvantages of image encryption schemes is that the decryption process requires computing devices.

Focusing on this matter, Naor and Shamir proposed a new cryptographic scheme for binary images called Visual Cryptography (VC) [1]. Contrary to traditional encryption schemes, VC does not have any keys. Visual ryptography is applied to encrypt a binary image into two separate binary images called shares that are apparently random, and reveal no information about the original image. Shares are generated based on the original image pixels values; and Human Visual System (HVS) is the decryption device.

To achieve this, encrypted images are generated block by block corresponding to each pixel in the original image. Table 1 illustrates an example of blocks that are used in share images. If the pixel in original image is white, both blocks placed in encrypted images are the same, as well as if the pixel is black, blocks values are adverse. Blocks for both black and white pixels are shown in table 1. Superposing shares results a fully black pixel

Secret pixel	White	Black
Share 1		
Share 2		
Stacking result		

TABLE 1. Blocks used in shares and stacking results



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

FIGURE 1. Binary visual cryptography
(a) Cameraman binary image ; (b) Share 1; (c) Share 2; (d) Retrieved image;

block for each black pixel in the original image; and a pixel block with black sub-pixels for each white pixel.

Using transparency specification and HVS ability, original image is revealed if the encrypted images are superposed correctly. Since there are six different blocks for each pixel in a share which are randomly chosen, decryption with a single share is impossible, taking $6^{m\times n}$ states ($m \times n$ is size of the original image) for a brute force attack to decrypt the secret from a single share. This method is perfectly secure; however, it only works with binary images. Figure 1 is an example of visual cryptography.

Using HVS, this method requires no computation in decryption phase. Naor and Shamir also proposed a method to share an image for N participants that require at least K participants to reveal the original image. This method is called (K,N)-VC [1]. Visual cryptography has attracted many researchers because of this great idea of using HVS instead of computer in decryption phase. Some applications of visual cryptography are visual voting, visual authentication and private key cryptosystems [1].

In addition to binary VC, useful VC schemes for gray-scale images were presented. They used different halftone techniques to convert the gray-scale image into a binary image, and then used visual cryptography to encrypt the new binary image. Main focus in these methods is on novelty of halftone technique implementation or visual cryptography block models. Even though the HVS is not able to differentiate the intensity of pixels one by one, it is a disadvantage that in these methods the revealed image is not continuous tone [2, 3, 5].

Pixels in continuous tone gray-scale images have 256 gray values. In Computer Display Systems (CDS) values start from zero as a black pixel to 255 as a white pixel. Therefore, each pixel in gray-scale image can be evaluated by an eight-bit integer. Each bit in pixels gray value is called a bit level and each binary image representing a bit level is a bit plane. Dividing a gray-scale image into these bit planes and working on each plane separately is called bit level decomposition. Another method based on bit-level decomposition for secret image sharing is also presented [4]. In this paper, we have presented a new visual cryptographic scheme for gray-scale images using bit level decomposition. Our method

does not change the contents of original image in the encryption phase. Also it is simple to implement and has an acceptable quality for the revealed secret.

Rest of this paper is organized as follows. In the next section the proposed method for gray-scale VC is described. In section 3 the experimental results are illustrated and finally the conclusion is presented in section 4.

2. **Proposed Method.**

To encrypt a gray-scale image into two gray-scale shares, the original image is decomposed into eight bit planes. Each bit plane is encrypted using binary VC. All the encrypted shares of the bit planes are recomposed and two gray-scale shares are created. Superposing gray-scale shares reveals the secret.

Algorithm 1 The proposed method algorithm

```
Read original image A with size m × n
VCB ← All blocks used in visual cryptography
Create two 2m × 2n integer matrix S1 and S2
for i = 1 to m do
    for j = 1 to n do
        for b = 1 to 8 do
            B ← a randomly chosen 2 × 2 block from VCB
            Bc ← 2 × 2 block complementary to B
            if A(i, j)b = 1 then
                S1b(2i − 1, 2j − 1) ← B(1, 1)
                S1b(2i − 1, 2j) ← B(1, 2)
                S1b(2i, 2j − 1) ← B(2, 1)
                S1b(2i, 2j) ← B(2, 2)
                S2b(2i − 1, 2j − 1) ← B(1, 1)
                S2b(2i − 1, 2j) ← B(1, 2)
                S2b(2i, 2j − 1) ← B(2, 1)
                S2b(2i, 2j) ← B(2, 2)
            else
                S1b(2i − 1, 2j − 1) ← B(1, 1)
                S1b(2i − 1, 2j) ← B(1, 2)
                S1b(2i, 2j − 1) ← B(2, 1)
                S1b(2i, 2j) ← B(2, 2)
                S2b(2i − 1, 2j − 1) ← Bc(1, 1)
                S2b(2i − 1, 2j) ← Bc(1, 2)
                S2b(2i, 2j − 1) ← Bc(2, 1)
                S2b(2i, 2j) ← Bc(2, 2)
            end if
        end for
    end for
end for
```

The algorithm 1 depicts our proposed method precisely. In this algorithm, the original image with size $m \times n$ is completely scanned. Two gray-scale shares S_1 and S_2 are defined with size $2_m \times 2_n$. Then each bit b in values of $(2i-1, 2j-1) - (2i, 2j)$ pixels in S_1 and S_2 is assigned, corresponding to bit b in value of pixel (i, j) in the original image.

The following description is an example of proposed algorithm, executed on a 2×2 image. Let A be an arbitrary image with intensity values of (62, 147, 11, 83), respectively.

$$A = \begin{pmatrix} 62 & 147 \\ 11 & 93 \end{pmatrix} = \begin{pmatrix} 00111110 & 10010011 \\ 00001011 & 01010011 \end{pmatrix}$$

Matrices A_1-A_8 are bit planes of A. A_1 represents the least and A_8 is the most significant bit plane.

$$A_1 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, A_2 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, A_3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, A_4 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$
$$, A_5 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, A_6 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, A_7 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, A_8 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

Each of A's bit planes can be encrypted using binary VC that results a set of eight binary matrix pairs. Matrices $E_{1,1} - E_{1,8}$ and $E_{2,1} - E_{2,8}$ are encrypted matrix pairs corresponding to A's bit planes. For example the block $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ is randomly chosen for $A_1(1, 1)$ (the first bit in A_1) to be placed into $\begin{pmatrix} E_{1,1}(1,1) = 1 & E_{1,1}(1,2) = 1 \\ E_{1,1}(2,1) = 0 & E_{1,1}(2,2) = 0 \end{pmatrix}$ and its complementary is placed into $\begin{pmatrix} E_{2,1}(1,1) = 0 & E_{2,1}(1,2) = 0 \\ E_{2,1}(2,1) = 1 & E_{2,1}(2,2) = 1 \end{pmatrix}$, because the value of $A_1(1, 1)$ is zero which represents a black pixel. The same process is applied to fill the values of all $E_{1,1} - E_{1,8}$ and $E_{2,1} - E_{2,8}$ matrices.

$$E_{1,1} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}, E_{2,1} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$
$$E_{1,2} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}, E_{2,2} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$
$$E_{1,3} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}, E_{2,3} = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix}$$
$$E_{1,4} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, E_{2,4} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$
$$E_{1,5} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}, E_{2,5} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$
$$E_{1,6} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}, E_{2,6} = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$
$$E_{1,7} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}, E_{2,7} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}$$

$$E_{1,8} = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, E_{2,8} = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

In printing process, printed black pixels get a value of one; because there is ink to absorb the light and printed white pixels have a value of zero. HVS performs binary OR operation on two shares; because on superposition, if the pixel is black at least in one share, the light is absorbed and HVS sees the result as black; and only if both of the pixels are white, it is appeared as white. This representation is performed reversely in CDS. As for black pixels, light is not projected (0 value) and for white pixels, light is projected (1 value). Therefore to simulate HVS superposition on a CDS, the OR operation that is done by HVS should be replaced by AND operation in the CDS.

Superposing $E_{1,k}$ and $E_{2,k}$ results R_k (k is the index of bit plane) as the AND operation is applied to them. Each 2×2 sub-matrix in R_k represents the original value in A_k. Recomposing these matrices, as they were decomposed, results matrix R as a representation of matrix A in retrieval phase.

$$R_1 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}, R_2 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}, R_3 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

$$, R_4 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, R_5 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}, R_6 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$, R_7 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}, R_8 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

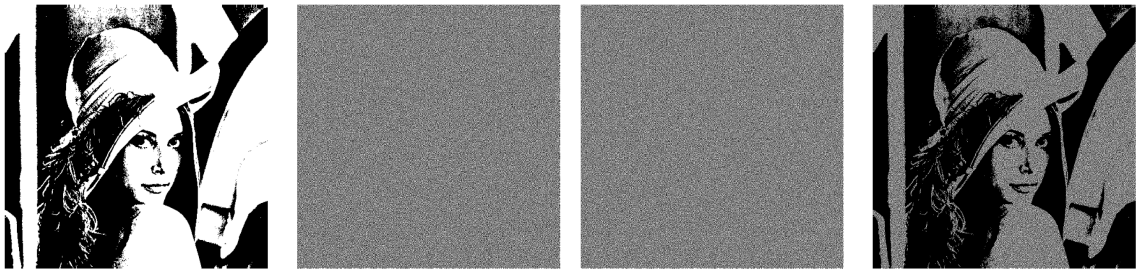
Recomposing $R_1 V R_8$ leads to integer matrix R. A binary representation of matrix R and integer results are as following:

$$R = \begin{pmatrix} \begin{pmatrix} 00100010 & 00010000 \\ 00101110 & 00011100 \end{pmatrix} & \begin{pmatrix} 00000010 & 10000000 \\ 10010001 & 00010011 \end{pmatrix} \\ \begin{pmatrix} 00001001 & 00001010 \\ 00000010 & 00000001 \end{pmatrix} & \begin{pmatrix} 00001000 & 01000000 \\ 0010101 & 01011101 \end{pmatrix} \end{pmatrix}$$

$$= \begin{pmatrix} \begin{pmatrix} 34 & 16 \\ 46 & 28 \end{pmatrix} & \begin{pmatrix} 2 & 128 \\ 145 & 19 \end{pmatrix} \\ \begin{pmatrix} 9 & 10 \\ 2 & 1 \end{pmatrix} & \begin{pmatrix} 8 & 64 \\ 21 & 93 \end{pmatrix} \end{pmatrix}$$

Figure 2 illustrates a bit plane encrypted in two shares and the retrieved result. Figure 2(a) is one of the bit planes in Lena image. Figures 2(b), 2(c) are the encrypted binary share images generated by VC. Figure 2(d) is the result of superposing those encrypted bit planes.

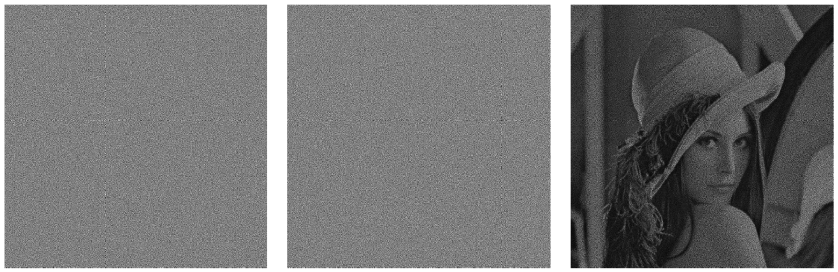
3. **Experimental Results.** In this section, some gray-scale images are used to evaluate the performance of our proposed method. These images are used because they contain different gray values and sufficient image details. Figures 3(a) and 3(b) are gray-scale



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

FIGURE 2. Binary VC on an original bit plane after decomposition
(a) 8th bit plane of Lena image; (b) Share 1; (c) Share 2; (d) Retrieved image;

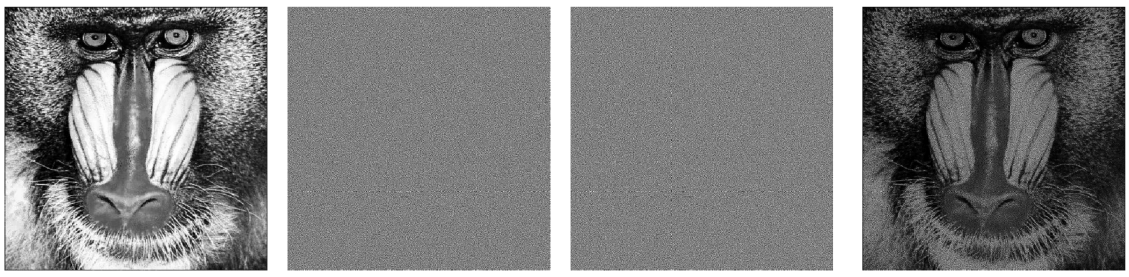
shares generated by the proposed method. Each single share leaks no information about the original image; but when they are superposed figure 3(c) is the result and the original Lena image is visible.



(a) (b) (c)

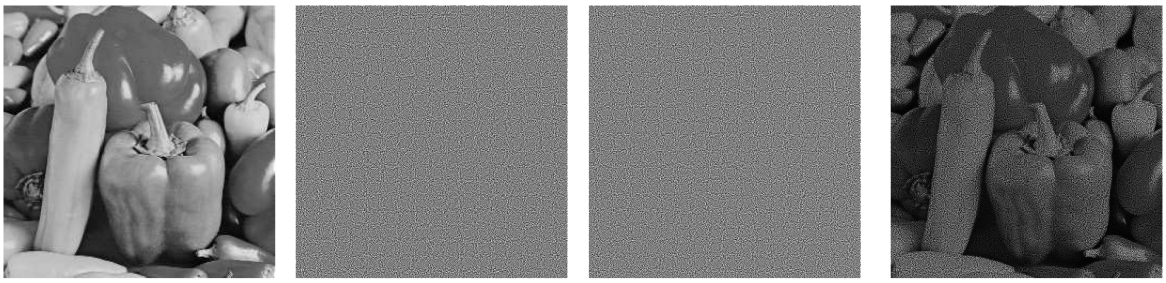
FIGURE 3. Result of proposed scheme
(a) Gray-scale share 1; (b) Gray-scale share 2; (c) Retrieved gray-scale image;

The pixel expansion in the proposed method is four, which means that the generated shares are twice the size of the original image. Figure 4(a) is the original image. Figure 4(d) is the retrieved image that is figure 4(b) and figure 4(c) superposition result. As it is shown, the details in figure 4(a) are recognizable in figure 4(d). Quality improvement methods can also be combined with the proposed method to be used as a secret image sharing scheme [9]. Figures 5, 6 and 7 are examples and proofs of proposed method security.



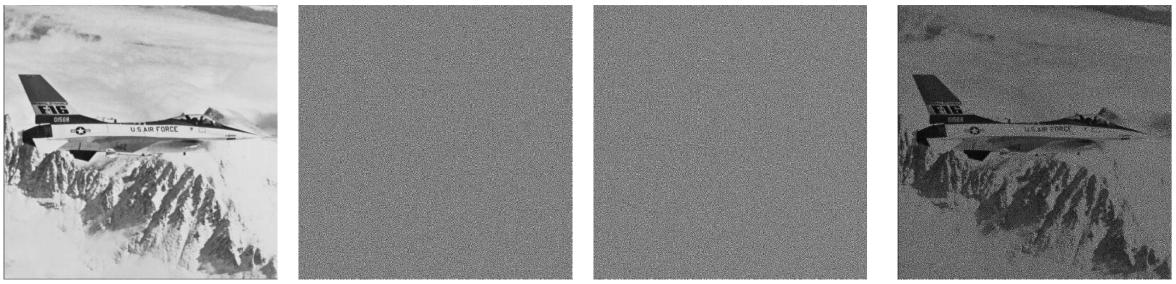
(a) (b) (c) (d)

FIGURE 4. Result of proposed scheme
(a) Baboon gray-scale image ; (b) Share 1; (c) Share 2; (d) Retrieved image;



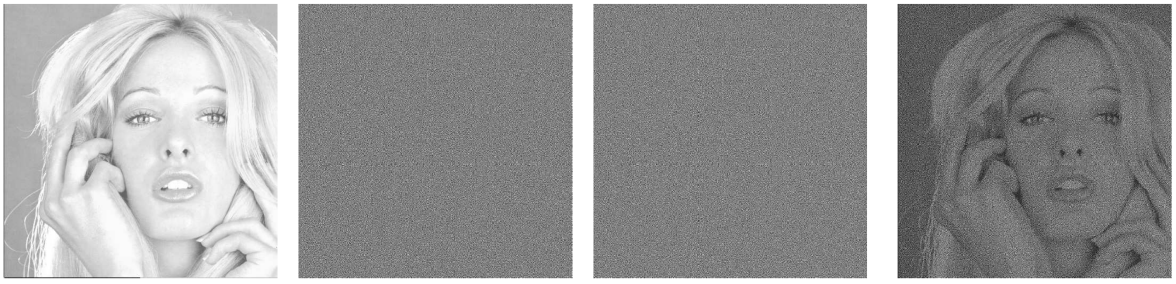
(a) (b) (c) (d)

FIGURE 5. Result of proposed scheme
(a) Pepper gray-scale image ; (b) Share 1; (c) Share 2; (d) Retrieved image;



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

FIGURE 6. Result of proposed scheme
(a) Airplane gray-scale image ; (b) Share 1; (c) Share 2; (d) Retrieved image;



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

FIGURE 7. Result of proposed scheme
(a) Tiffany gray-scale image ; (b) Share 1; (c) Share 2; (d) Retrieved image;

4. **Conclusions.** Visual cryptography is a very useful technique in secure communication as it uses no computing devices in the decryption phase; and it becomes more useful when extended to gray-scale images. We have presented a new variant of VC for gray-scale images using bit-level decomposition. In contrast to previous methods, our proposed method does not need the change of the original image to binary (with halftone techniques) and it is easy to understand and implement. Also, decryption with a single share needs $8 \times 2^{2m \times 2n}$ images to find the secret with a single share; so the security of the proposed method is guaranteed because each single share leaks no information about the original image.

Acknowledgement. The authors gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

REFERENCES

[1] M. Naor, and A. Shamir, Visual cryptography, *Proc. of Advances in Cryptology - EUROCRYPT*, LNCS 950, Springer, pp. 1-12, 1995.

[2] C. C. Lin, and W. H. Tsai, Visual cryptography for gray-level images by dithering techniques, *Journal of Pattern Recognition Letters*, vol. 24. no. 1-3, pp. 349-358, 2003.

[3] Y. C. Hou, Visual cryptography for color images, *Journal of Pattern Recognitions*, vol. 36, no. 7, pp. 1619-1629, 2003.

[4] R. Lukac, and K. N. Plataniotis, Bit-level based secret sharing for image encryption, *Journal of Pattern Recognitions*, vol. 38, no. 5, pp. 767-772, 2005.

[5] C. Blundo, A. D. Santis, and M. Naor, Visual cryptography for grey level images, *Journal of Information Processing Letters*, vol. 75, no. 6, pp. 255-259, 2000.

[6] B. Li, J. H. He, J. W. Huang, and Y. Q. Shi, A survey on image steganography and steganalysis, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 2, no. 2, pp. 142-172, 2006.

[7] Z. H. Wang, C. C. Chang, H. N. Tu, and M. C. Li, Sharing a secret image in binary images with verification, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 2, no. 1, pp. 78-90, 2008.

[8] A. Latif, and A. R. Naghsh-Nilchi, Digital image watermarking based on parameters amelioration of parametric slant-hadamart transform using genetic algorithm, *International Journal of Innovative Computing, Information and Control*, vol. 8, no. 2, pp. 1205-1220, 2012.

[9] F. Liu, T. Guo, C. K. Wu, and L. Qian, Improving the visual quality of size invariant visual cryptography scheme, *Journal of Visual Communication and Image Representation*, vol. 23, no. 2, pp. 331-342, 2012.