Journal of Software Engineering and Applications, 2017, 10, 1-10
http://www.scirp.org/journal/jsea
ISSN Online: 1945-3124
ISSN Print: 1945-3116

A Secure Visual Cryptography Scheme Using Private Key with Invariant Share Sizes

Rola I. Al-Khalid[1], Randa A. Al-Dallah[2], Aseel M. Al-Anani[1], Raghad M. Barham[2], Salam I. Hajir[2]

[1]Department of Computer Information Systems, King Abdullah II School for Information Technology, The University of Jordan, Amman, Jordan
[2]Department of Computer and Networks Engineering, Faculty of Engineering Technology, Al-Balqa' Applied University, Amman, Jordan
Email: r.khaild@ju.edu.jo, randa.dallah@bau.edu.jo, a.anani@ju.edu.jo, raghadbarham1994@yahoo.com, salamhajir@yahoo.com

How to cite this paper: Al-Khalid, R.I., Al-Dallah, R.A., Al-Anani, A.M., Barham, R.M. and Hajir, S.I. (2017) A Secure Visual Cryptography Scheme Using Private Key with Invariant Share Sizes. *Journal of Software Engineering and Applications*, **10**, 1-10.
http://dx.doi.org/10.4236/jsea.2017.101001

Received: December 14, 2016
Accepted: January 16, 2017
Published: January 19, 2017

Abstract

Visual cryptography (VC) is one of the best techniques used to secure information. It uses the human vision to decrypt the encrypted images without any cryptographic computations. The basic concept of visual cryptography is splitting the secret image into shares such that when the shares are stacked, the secret image is revealed. In this paper we proposed a method that is based on the concept of visual cryptography for color images and without any pixel expansion which requires less space. The proposed method is used to encrypt halftone color images by generating two shares, random and key shares which are the same size as the secret color image. The two shares are generated based on a private key. At the receiving side, the secret color image is revealed by stacking the two shares and exploiting the human vision system. In this paper, we produce an enhanced form of the proposed method by modifying the encryption technique used to generate the random and the key shares. Experimental results have shown that the proposed and the enhanced methods suggest an efficient way to encrypt a secret color image with better level of security, less storage space, less time of computation and with a better value of PSNR.

Keywords

Visual Cryptography (VC), Halftone Color Images, Pixel Expansion, PSNR, Private Key

1. Introduction

The rapid development in computer technology and the internet and the need to

transfer data from one place to another requires finding a way to secure data transmission. Secure methods are needed to guard data against hacking or attacks. An attempt to find a secure method that guarantees data protection has become a challenge for many researchers in this field. Pioneering innovation in securing and encrypting secret data against hacking are Naor and Shamir [1]. In 1994, they proposed a visual cryptography scheme, which can decode concealed images without any complex cryptographic computations. Their basic model was used for black and white images where it generates n transparencies of the original secret image. Stacking only k (or more) of the n transparencies can reveal the original secret image. This model suffers from pixel expansion, where the size of the recovered secret image is not the same as the size of the original one. Many VC techniques have been proposed to recover black and white images and color images [2]-[10]. Moreover, several studies employ both cryptography and steganography to provide a high level of security for data transmission [11] [12] [13]. Askari, Heys and Moloney in [14], proposed an extended VC scheme for processing halftone images, where the size of the share images and the recovered image is the same as the original secret image. The scheme improved the quality of the share images and the recovered secret image. They first presented a method based on a block-wise approach called *simple block replacement* (*SBR*) for preprocessing the halftone image. The method is easy to implement but the resulting secret image is darker than the original image. Therefore, they proposed the *balance block replacement* (*BBR*) method in order to keep the local ratio of black to white pixels in the processed image close to the local ratio of the black to white pixels in the original halftone image thus improve the quality of the resulting image. Amin and Lijina in [15], applied dithering to the block replacement method called *balance block replacement* (*BBR*) in order to improve the quality of both the shared images and the recovered secret image. In [16], Fersna and Athira proposed an encryption technique without pixel expansion for color images. The technique gradually recovers the secret image.

As more and more shares are stacked the secret cover image can be revealed progressively. In their paper they combined progressive visual cryptography technique with digital watermarking scheme to generate meaningful shares providing higher security. Xiaoyo *et al.* proposed a visual cryptography technique which supports color images without pixel expansion, original image without preprocessing, k-out-of-n threshold setting as well as supporting a tunable number of color levels in the secret sharing process [17].

In this paper, we proposed a visual cryptography method for color images and without any pixel expansion compared to [1]. The proposed method is used to encrypt halftone color images. The secret color image is revealed without any complex computation, thus minimizing the preprocessing time which other papers suffer from [14] [15] [16].

Our proposed method is used to encrypt halftone color images by generating two shares, random and key shares, which are the same size as the secret color

image. The two shares are generated based on a private key. At the receiving side, the secret color image is revealed by stacking the two shares and exploiting the human vision system. The proposed method keeps the secret color image with a better level of security and quality as much as possible. Also time and storage space needed are minimized.

This paper is organized a follows. Section 2 presents our proposed and enhanced methods, section 3 reports and discusses some experimental results. Finally, conclusions appear in section 4.

2. The Proposed Method

The proposed method suggested a way to encrypt a secret color image based on VC system. The secret color image is encoded into meaningless share images. Individual share images do not give any information about the original secret image. The contents of the secret image can only be revealed by stacking all the share images. The resulted share images are the same size as the original secret image without pixels expansion.

The proposed method involves two stages; encryption and decryption:

2.1. The Encryption Stage

Step 1: The creation of the halftone image.

The original secret image is half toned into a binary image using a dithering technique.

Step 2: The halftone image is split into three layers Red, Green and Blue (*ImgR*, *ImgB*, and *ImgG*)

Step 3: The generation of one layer of the Random share (the *Mask*)

The size of the *Mask* generated is the same as the size of the secret image.

To generate the random share (*Mask*), a private key, which both the sending and receiving sides know, is used.

We consider the share as a set of rows and columns. The pixels in the even rows take a random value (either 0 or 1). The odd rows are filled with the complement value of the pixels in the even rows directly above it. If the pixel in the even row is black (white) then the pixel in the odd row beneath it will be white (black) see Figure 1. The *Mask* will be used to generate the key share in Step 4.

Step 4: The generation of the key share (*share* 2)

The Key share is consisted of three layers Red, Green and Blue (called *share*2*R*, *share*2*G* and *share*2*B*). The layers of the key share are constructed using the random share (*Mask*) and the layers of the half toned image. Each layer of the key share will be constructed as follows:

Each layer of the half toned image is partitioned into non-overlapping blocks of size 2 × 1 pixels. *Key Share* layers will be generated block by block using the half toned image and the random share. Starting from the top left block and moving left to right and top to bottom in raster format, the pixel at the top of each half toned block is checked. If the pixel in the half toned block is black then the corresponding block of *Key Share* will be filled by complementing the values

of the two pixels in the corresponding block of the random share (*Mask*). On the other hand, if the pixel in the half toned block is white then the corresponding block of *Key Share* will be filled with the same values of the corresponding block of the random share (*Mask*), see Figure 2. The resulting layers (*share* 2*R*, *share* 2*G* and *share* 2*B*) are combined to form the key share (share 2). The key share is the same size as the secret image without pixel expansion so it does not require more storage space. Processing blocks of size 2 × 1 pixels in the steps of the encryption stage reduces the time of computation by half. The encryption algorithm that shows the steps of encrypting the colored secret image is shown in Figure 3.

The encryption procedure of the colored secret image is illustrated in Figure 4.

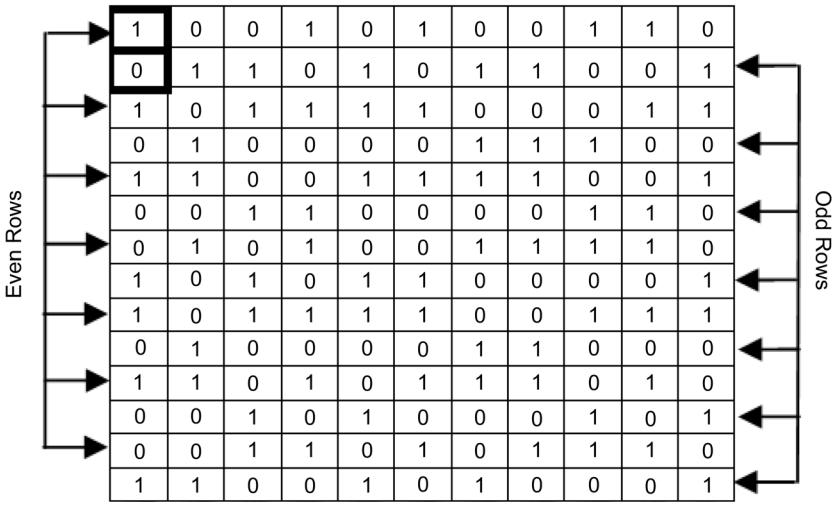

Figure 1. The generation of the Mask share.

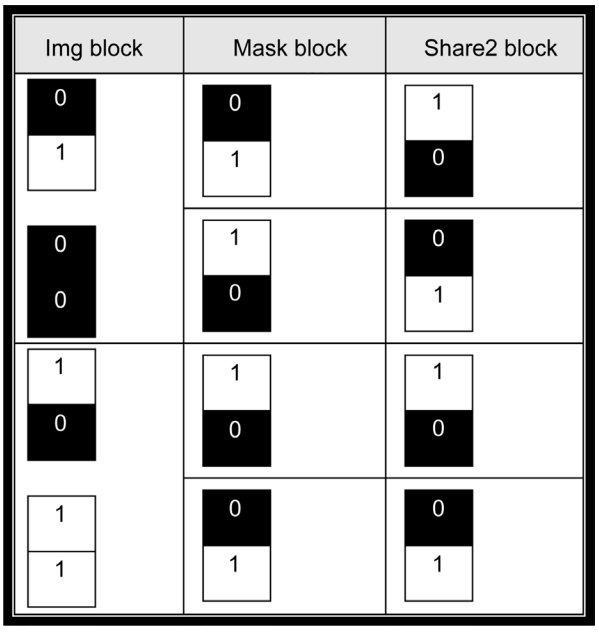

Figure 2. Share 2 block according to the corresponding Image block.

Input: Colored Secret Image (*Image*) of size $N \times M$ a Private Key K1
Output: Key share of size $N \times M$
Steps:

1. Halftone the colored secret image (*Image*) using a dithering technique (*Img*).
2. Split (*Img*) into three layers R,G, and B, where:

$$Image \xrightarrow{Halftoning} img \xrightarrow{Split} [ImgR \quad ImgG \quad ImgB]$$

3. Generate one layer Random share (*mask* share) with the same size as the secret image (see Figure 1 and Figure 2).
   $\forall (2\times 1) block \in mask$, do the following:
   According to the private key $K1$, generate randomly a value either 0 or 1 and store it in the first pixel in the mask block ($Mask_{ij}$). The other pixel ($Mask_{i+1,j}$) is filled with the complement value of the first pixel ($Mask_{ij}$). This step will make the mask a half black-and-white block.
   The values for each block will be:

$$Mask_{2x1} = \left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\}$$

4. Generate a key share (share 2) according to the following steps:
   For all halftone image layers of the secret image (*ImgR*, *ImgG*, *ImgB*) do the following:
   a) $\forall\ 2\times 1 block\ (ImgR_{ij}, ImgR_{i+1\,j}) \in ImgR$, do the following:
   According to the value of first pixel in each block ($ImgR_{ij}$):
   i) If $ImgR_{ij} = 0$, set the complement of the corresponding mask block values to the corresponding position of *Share* 2*R* block ($Share\,2R_{ij}$, $Share\,2R_{i+1,j}$)
   ii) If $ImgR_{ij} = 1$, set the same values of the corresponding mask block to the corresponding position of *Share* 2*R* block ($Share\,2R_{ij}$, $Share\,2R_{i+1,j}$)
   b) Repeat step (a) for *ImgG* and *ImgB*, then store the outcomes in *Share* 2*G* and *Share* 2*B* respectively.

Figure 3. The encryption algorithm of the colored secret image.

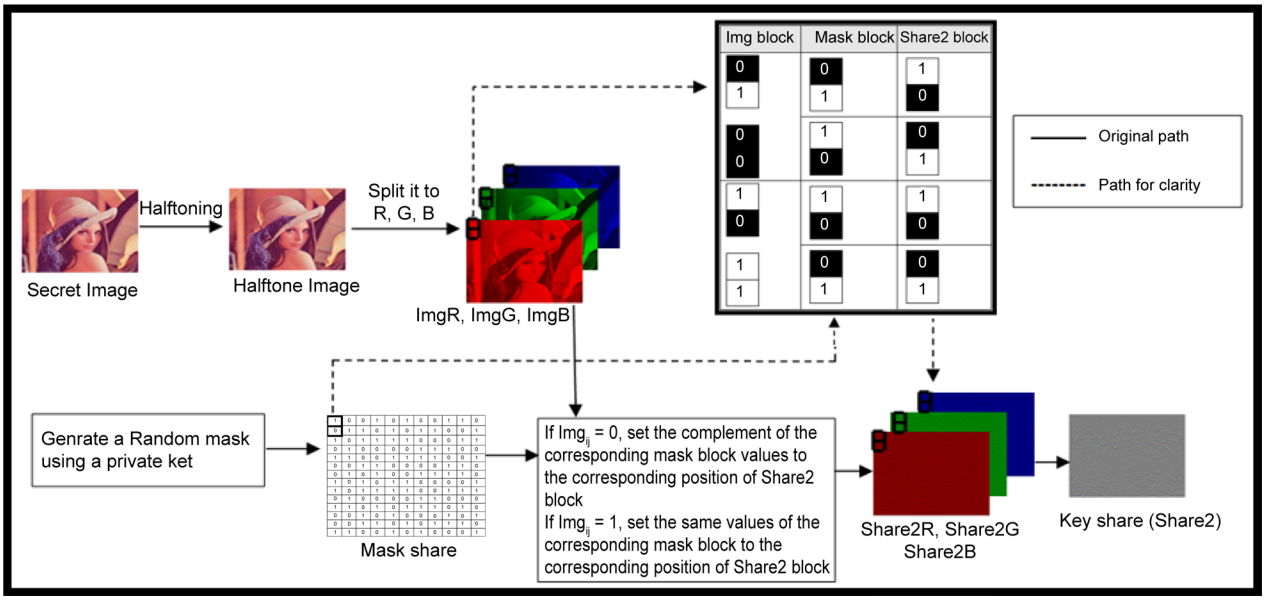

Figure 4. The encryption procedure of the colored secret image.

In order to improve the value of PSNR and to increase the level of accuracy and security, we enhanced step 4 of the encryption stage in the proposed method (see Figure 5 and Figure 6).

2.2. The Decryption Stage

To reveal the original secret image, the key share (*Share* 2) is decomposed into three layers (*Share* 2*R*, *Share* 2*G* and *Share* 2*B*). Each layer is stacked with the

4. Generate a key share (share 2) according to the following steps:
   For all halftone image layers of the secret image (ImgR, ImgG, ImgB) do the following:
   $\forall\ 2\times 1\ block\ (ImgR_{ij}, ImgR_{i+1\,j}) \in ImgR$, do the following:
   According to the value of the two pixels in each block ($ImgR_{ij}$):
   I. If $ImgR_{ij} = 0$ and $ImgR_{i+1j} = 0$, set the complement of the corresponding mask block values to the corresponding position of Share2R block (Share $2R_{ij}$, Share $2R_{i+1\,j}$)
   II. If $ImgR_{ij} = 1$ and $ImgR_{i+1j} = 1$, set the same values of the corresponding mask block to the corresponding position of Share2R block (Share $2R_{ij}$, Share $2R_{i+1\,j}$)
   III. If $ImgR_{ij} = 1$ and $ImgR_{i+1j} = 0$ or If $ImgR_{ij} = 0$ and $ImgR_{i+1j} = 1$, set the same values of the halftone image to the corresponding position of Share 2R block(Share $2R_{ij}$, Share $2R_{i+1\,j}$) and to the mask block ($mask_{ij}$, $mask_{i+1\,j}$).
   Repeat step (a) for ImgG and ImgB, then store the outcomes in Share 2G and Share 2B respectively.

Figure 5. The enhanced encryption algorithm of the colored secret image.

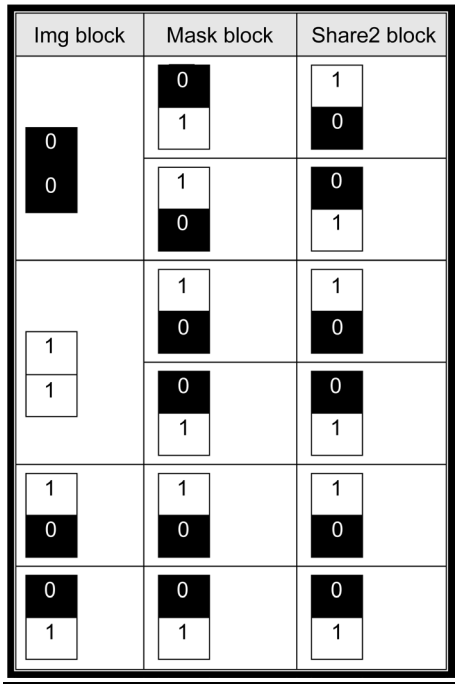

Figure 6. Share 2 block according to the corresponding Image block.

mask then the resulted layers are combined to reveal the original secret image with the same size (see Figure 7). Secret information is retrieved using the human visual system and without the need of any complex computation. The decryption algorithm of the colored secret image is shown in Figure 8.

3. Experimental Results

The proposed method and its enhanced form have been applied to a wide range of images of different sizes. PSNR values were calculated for both methods and compared to the results of using the traditional visual cryptography scheme. As shown in Table 1, we found that there is no apparent difference between the PSNR values of VC and the proposed method, whereas the enhanced form of the proposed method shows a significant improvement. From Table 1, taking Leena image as an example, the PSNR value of the VC method is 30.1. While the PSNR

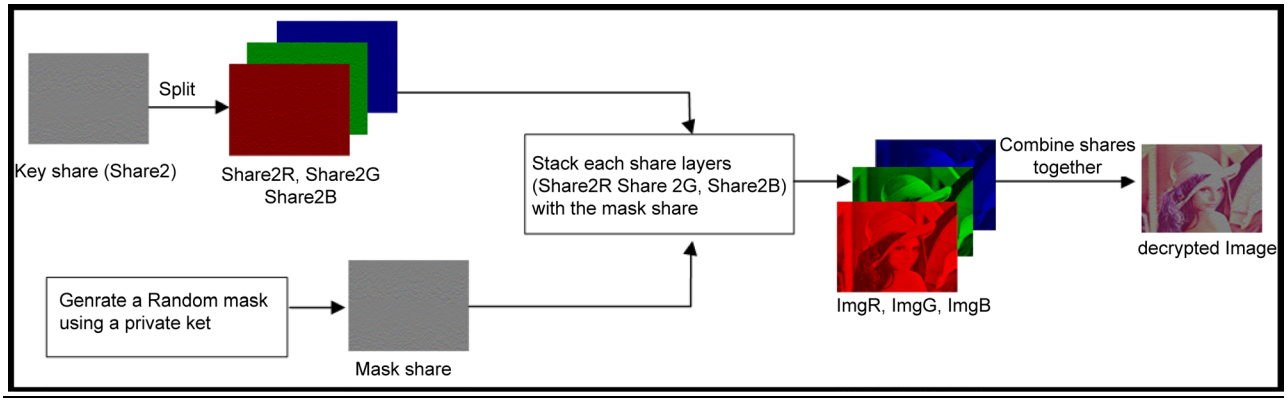

Figure 7. The decryption procedure of the colored secret image.

Input: Key share (Share2) of size $N \times M$, a Private Key K1
Output: Colored Secret Image of size $N \times M$
Steps:
1. Split the key share (*share*2) into RGB Layers (*Share*2*R Share*2*G*, *Share*2*B*)
$share2 \xrightarrow{split} [share2R \quad share2G \quad share2B]$
2. Generate a Random share (*mask*) using the same private key k1 as discussed in the encryption algorithm.
3. Stack each layer of *Share*2 (*Share*2*R Share*2*G*, *Share*2*B*) with the mask.
4. Combine the resulted layers together to retrieve the secret colored image.

Figure 8. The decryption algorithm of the colored secret image.

Table 1. PSNR values for different sample images.

Image / PSNR	VC Method	Proposed Method	Enhanced Method
Barbra (576 × 720)	31.182	29.83	36.9
Lena (300 × 300)	30.1	28.93	34.17
Airplane (256 × 256)	28.54	27.86	30.31
Peppers (128 × 128)	30.68	29.52	34.76
Baboon (300 × 266)	30.17	28.94	34.75
Ward (300 × 400)	32.46	31.13	38.04
Pollen (500 × 500)	30.6	29.55	34.1
Lena Black and white image (300 × 300)	30.5	30.4	30.8

value of the proposed method is 28.93, which very close. The enhanced form on the other hand gives a better result which is 34.17. The results in the last row of the table for the black and white Leena image the PSNR values or the VC, proposed and enhanced methods are 30.5, 30.4 and 30.8 respectively. This proves that the results of the enhanced method are also better. This also can be seen for the Baboon and Word images where the enhanced method gives PSNR values of 34.75 and 38.04 respectively. These results can be justified in that there are four different cases of the two pixels in the 2 × 1 image blocks (see Figure 6). The cases where the two pixels in the image block are complement of each other, share 2 blocks in the encryption step will be set with the same values of the corresponding blocks in the original image. On the other hand, if the two pixels

taken from the original image are the same, then share 2 blocks will be set randomly according to the mask block. As we can see 50% of the cases after decrypting the encrypted image blocks remain the same as the original without any distortion. Furthermore, unlike VC, our methods encrypt the secret image without pixel expansion thus creating an encrypted secret image having the same size as the original (see Figure 9). The techniques we used also reduce the time of computation by half compared to VC because in the key share generation step, blocks of size 2 × 1 pixels are being processed in the encryption stage. A sample set of host images with different sizes is shown in Figure 10.

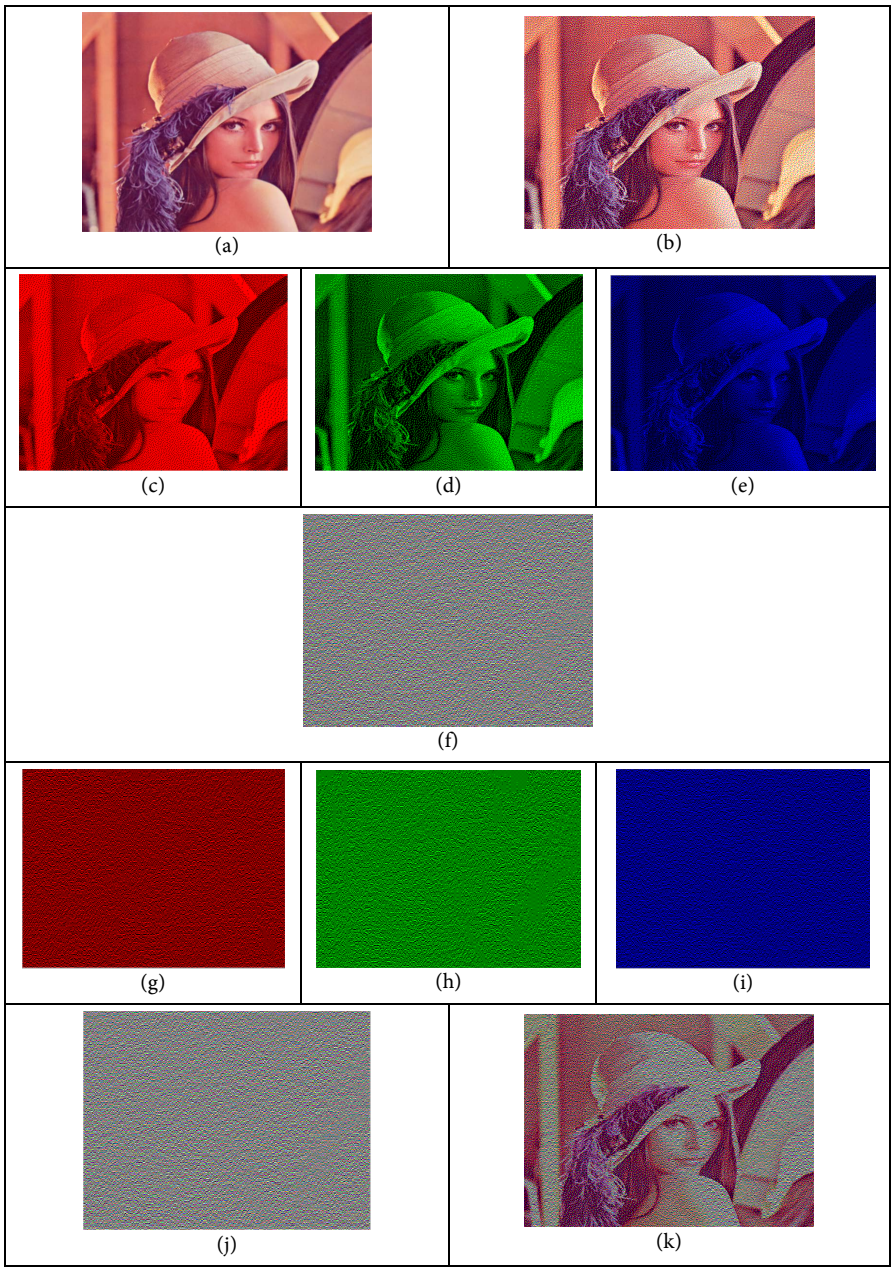

Figure 9. An example of the proposed method for 24 color levels. (a) Color secret image. (b) Dither color image. (c) ImgR. (d) ImgG. (e) ImgB. (f) Mask share. (g) ShareR. (h) ShareG. (i) ShareB. (j) Share 2. (k) Decrypted Image.

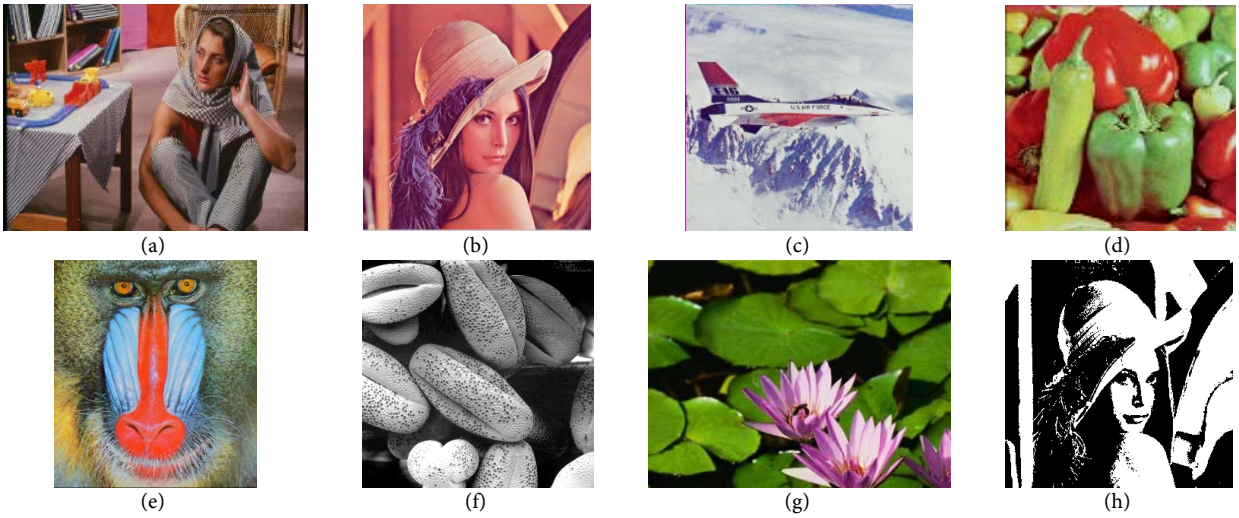

Figure 10. Sample test images. (a) Barbra of size (400 × 300). (b) Lena of size (300 × 300). (c) Airplane of size (256 × 256). (d) Pepper of size (128 × 128). (e) Baboon of size (576 × 720). (f) Pollen of size (500 × 500). (g) Lilies of size (300 × 400). (h) Black & white Lena of size (300 × 300).

We use the halftone Lena image and the random share to generate the key share. Figure 9 shows that no information can be revealed from the two shares, the resultant decrypted image has the same size as the original color secret image and the image quality is maintained.

4. Conclusion

Visual cryptography is an encryption technique that has the advantage of using the human vision to decrypt the encrypted images without any cryptographic computations. On the other hand VC has suffered from pixel expansion. In this paper, the proposed and the enhanced methods overcome this by suggesting a new way of encryption without pixel expansion. Our methods require less space storage and less time for computation during the encryption process. The secret image is encrypted by splitting it into two shares, a random share and a key share. The key share is generated using the halftone image and the random share, and is then sent to the receiving side. The random share, on the other hand, is generated at both the sending and receiving sides using a private key. The secret color image is revealed by stacking the two shares and exploiting the human vision system. The proposed and the enhanced methods offer a good PSNR values compared to VC. As a future work, we will enhance our methods to encrypt halftone color images by generating meaningful shares as well as applying our methods in applications that require high level of security.

References

[1] Naor, M. and Shamir, A. (1995) Visual Cryptography. In: De Santis, A., Eds., *Advances in Cryptology—EUROCRYPT*'94. EUROCRYPT 1994. Lecture Notes in Computer Science, Vol. 950. Springer, Berlin, Heidelberg. https://doi.org/10.1007/bfb0053419

[2] Tekade, R., Kharat, R., Magade, V., Shaikh, M. and Mendhe, P. (2016) E-Voting

System Using Visual Cryptography & Homomorphic Encryption. *International Journal of Advanced Research in Computer and Communication Engineering* (*IJARCCE*), 1.

[3] Poonkuzhali1, S.M. and Therasa, M. (2015) Data Hiding Using Visual Cryptography For Secure Transmission. *International Journal of Advanced Research in Computer and Communication Engineering* (*IJARCCE*), **4**, 4.

[4] Das, K., Sen, A. and Bandyopadhyay, S.K. (2016) A New Visual Cryptography Scheme For Color Image Using Sliding Puzzle Technique. *International Journal of Information Research and Review* (*IJIRR*), **3**, 2238-2241.

[5] Reddy, M.S. and Mohan, S.M. (2014) Visual Cryptography scheme for Secret image retrieval. *International Journal of Computer Science and Network Security* (*IJCSNS*), **14**, 6.

[6] Hou. Y.-C. (2003) Visual Cryptography for Color Images. *Pattern Recognition*, Elsevier, **36**, 1619-1629. https://doi.org/10.1016/S0031-3203(02)00258-3

[7] Kumar, M.S., Shilpa, A. and Vijayalakshm, J.R. (2016) A survey on Visual Cryptography Techniques. *International Journal of Application or Innovation in Engineering & Management* (*IJAIEM*), **5**, 100-112.

[8] Dua, R. and Singh, N. (2016) Secured Visual Cryptography Scheme Using Meaningful Shares. *International Journal of Innovative Research in Computer and Communication Engineering*, **4**, 5342-5347.

[9] Mahadik, V., Sangale, R., Murame, P. and Ahir, D. (2014) Technique for Halftone Images without Pixel Expansion Using an Extended Visual Cryptography Scheme. *International Journal of Engineering Research and Reviews*, **2**, 56-60.

[10] Sankar, D. and Asoke, N. (2016) A Secure Approach for Data Hiding using Visual Cryptography. *International Journal of Innovative Research in Computer and Communication Engineering*, **4**, 10274-10282. https://doi.org/10.15680/IJIRCCE.2016.0406004

[11] Saraireh, S. (2013) A Secure Data Communication System Using Cryptography and Steganography. *International Journal of Computer Networks & Communications* (*IJCNC*), **5**, 3.

[12] Al-Anani, A.M., Abdallah, M.H., Al-Dallah, R.A. and Al-Khalid, R.I. (2008) Multimedia Multilevel Hiding Technique. *European Journal of Scientific Research*, **24**, 1.

[13] Al-Khalid, R., Al-Dallah, R. and Abdallah, M. (2011) Efficient Techniques for Multimedia Information Hiding Using Color Visual Cryptography. *Dirasat*: *Pure Sciences*, **38**, 100-112.

[14] Askari, N., Heys, H.M. and Moloney, C.R. (2013) An extended Visual Cryptography Scheme without Pixel Expansion for Halftone Images. *IEEE Canadian Conference on Electrical and Computer Engineering* (*CCECE*), **6**, 33-38. https://doi.org/10.1109/ccece.2013.6567726

[15] Shereen, A. and Lijina, S. (2016) An Extended Visual Cryptography Scheme Without Pixel Expansion Using Dithering. *International Journal of Advanced Research in Computer and Communication Engineering*, **5**, 1.

[16] Fersna, S. and Athira, V. (2015) Progressive visual cryptography scheme without pixel expansion for color images. *International Journal of Advanced Research in Computer and Communication Engineering*, **4**, 6.

[17] Wu, X.Y., Wong, D.S. and Li, Q. (2009) Threshold Visual Cryptography Scheme for Color Images with No Pixel Expansion. ISCSCT '09, 26-28, 310-315.