Extended Visual Secret Sharing with Cover Images Using Halftoning

Abhishek Mishra and Ashutosh Gupta

Abstract An extended visual cryptography scheme (EVCS) is a category of visual cryptography scheme (VCS) in which secret image is encoded into multiple shares of meaningful images. It has two additional images which are covering shares by the end of the encoding process. These meaningful shares are created by different approaches. The purpose of cover images (meaningful images) is to hide the secret image under it. In this paper, we propose an extended visual cryptography scheme with cover images using halftoning method. The halftoning method we designed for conversion of gray level image into binary image is based on dithering. The obtained halftoned image is transformed into multiple shares that are distributed to the participants. These shares are finally covered with some cover images to obtain meaningful shares. The experimental results and analysis show that the proposed scheme has satisfactory results.

Keywords Extended visual cryptography · Halftoning · Cover images · Security

1 Introduction

There is huge increase in transmission of data over network for instant access or distribution of data. As data are available in many forms that include text, image, audio, and video, images are one of the important data items. Today, researchers use visual cryptography schemes for distribution of secret images in the form of share (or shadow) images. The concept of secret sharing was first introduced by Naor and Shamir [1] and it is one of the active research areas in information security. There are a variety of ways through which information can be secure

Abhishek Mishra (✉)
IFTM University, Moradabad, India
e-mail: abhimishra2@gmail.com

Ashutosh Gupta
MJP Rohilkhand University, Bareilly, India
e-mail: ashutosh3333@gmail.com

S.C. Satapathy et al. (eds.), *Proceedings of the International Congress on Information and Communication Technology*, Advances in Intelligent Systems and Computing 438, DOI 10.1007/978-981-10-0767-5_10

including image hiding, watermarking, key exchange, authentication etc. However, these methods have a drawback that secret image is concealed in a single information carrier. If this concealed information is lost, there is no way to retrieve it.

Such problem can be overcome by visual secret sharing (VCS) scheme introduced by Naor and Shamir [1–3]. The scheme splits a secret image into multiple parts, also called share or shadow images and distributes each share among the number of participants. A subset of participants can only reveal the secret image by stacking the shares in some predefined order.

An extended visual cryptography scheme (EVCS) is a type of VCS in which secret image is encoded into multiple shares of meaningful images. These meaningful shares are created by different approaches. The purpose of cover images (meaningful images) is to hide the secret image under it. It is also a practical fact that secret images are not always in the form of monochrome. They may be in the form of color or gray level images. The same explanation also holds for cover images. This necessitates that there should be some transformation mechanism that converts the color or gray level images into monochrome images. The most common transformation to convert color or gray level image into binary image is halftoning. In this paper, we propose a visual cryptography scheme with cover images using halftoning method. The halftoning method we designed for conversion of gray level image into binary image is based on dithering. The rest of the paper is organized as follows: Sect. 2 explains the basics of extended VCS and common halftoning techniques. In Sect. 3, we describe our proposed EVCS scheme followed by experimental results in Sect. 4. Finally, Sect. 5 concludes the work.

2 Background and Related Work

Ateniese et al. [4] first proposed the concept of extended visual cryptography scheme (EVCS), which is a special category of VCS where secret image is encoded into multiple meaningful shares. An extended VCS requires more inputs compared to traditional VCS and these additional inputs are also images that work as cover shares (or images) after completion of the encoding process.

In the first step, the shares of a secret image are generated in the usual way by applying a VCS scheme. The first step is common for all varieties of images. Many visual cryptography schemes have been developed in the recent past [5–9]. The next task is how these generated shares are embedded or hidden within the chosen meaningful (cover) images. This requires a suitable method so that pixels from the secret shares remain distinct over the chosen cover image. The input image may be monochrome or grayscale or colored in nature. The same argument is also applied for chosen cover images. In this case, it is essential to convert the secret image into a monochrome image as the traditional or newly proposed secret sharing scheme [10, 11] relies on binary images before these shares are hidden within meaningful shares.

The conversion of secret image into binary image is performed through halftoning. Halftone visual cryptography (HVC) proposed by Wang et al. [12] adds digital halftoning techniques to extend the area of visual cryptography. The figure shows the dithering matrix of the gray-levels 0–9 to obtain proper halftoned patterns. Specifically, in VSS schemes, meaningful visual information can be used to encode a secret image into halftone shares. Halftoning is a method that simulates the grayscale of pixels by utilizing the density of printed dots. The human visual system can record only the overall intensity and integrate the fine detail in an image viewed from a distance. The denser the dot, the darker the image; in contrast, the sparser the dots, the lighter the image. Thus, one can use either black or white colors to simulate a continuous tone such that continuous-tone image can be changed to binary image.

For example, Fig. 1a shows a gray-level image that is transformed into a binary image [13] shown in Fig. 1b with black and white dots using halftoning. However, Fig. 1b is a binary image, and the human visual system can still perceive the gray level changes as it is a gray level image. Mostly, the visual cryptographic methods are designed for binary images, so the halftoning method is used to convert a gray-level image into a binary image. Thus, one can use the Naor and Shamir (2, 2)-threshold VSS scheme to encrypt Fig. 3b. The result is shown in Fig. 3c, which demonstrates the applicability and feasibility of using halftoning to construct a VSS scheme for gray-level images. The above arguments prove that halftoning techniques are useful preprocessing steps in visual cryptography to convert grayscale images to binary images. Since, halftoning reduces the quality of an image when applied on grayscale image and further degradation in image quality is due to VSS schemes, thus the overall effect is moderate degradation in image quality. This becomes an important parameter in a visual cryptography scheme along with some other issues as image expansion [14] and conciliation of the security of the scheme [15].

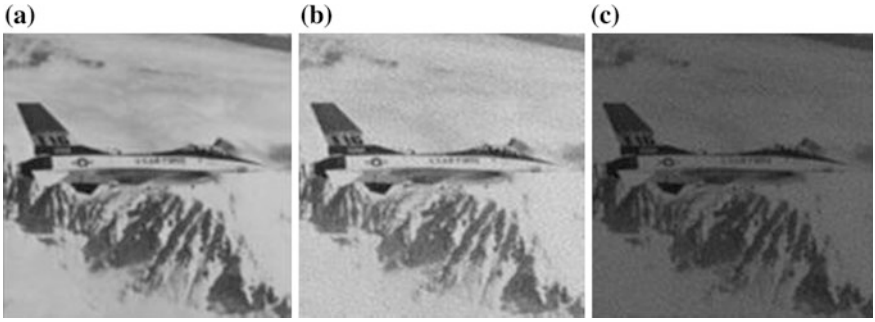

Fig. 1 Halftoning (512 × 512 pixels). **a** A continuous-tone image. **b** A halftone image. **c** The stacked image (1024 × 1024)

3 Proposed Scheme

In this section, we propose a halftoning method and visual secret sharing where shares are generated in some meaningful form. The meaningful shares are generated by hiding the secret shares through some cover images.

3.1 Halftone an Image

This section describes a halftone method where gray-level image is converted into a binary image. The method used for halftone conversion is ordered dithering. Let I and P be an $m \times m$ gray level and corresponding halftoned binary image respectively. Let $M(m, m)$ be the random image consisting of $L = 16$ gray levels. The mapping of $I(i, j)$ to $P(i, j)$ is done by normalizing the gray level value of $I(i, j)$ and $M(i, j)$. The proposed halftoned algorithm computes and compares the normalized value of $I(i, j)$ with $M(i, j)$. If normalized value of $I(i, j)$ is greater than or equal to normalized value of $M(i, j)$, then pixel value of halftone image is set to 1, otherwise 0. The algorithm for converting grayscale image to halftoned image is shown in Fig. 2.

3.2 Share Generation

This section presents the method for generating the shares from the halftone image P obtained from algorithm 1 with some meaningful image (also called cover image) taken as inputs. Next are the n random binary matrices M_k where $1 \leq k \leq n$ is generated. The n intermediate matrices I_k are generated by applying XOR operation according to the following rule:

Algorithm 1: Algorithm for constructing Halftone image

Pre-condition: A gray scale images I and M of size N x N and L=16
Post-condition: Halftone image P.

```
for i = 1 to N
    for j = 1 to N
        if I(i, j)/256 ≥ M(i, j)/L
            P(i, j)= 1;
        else
            P(i, j) =0;
        endif
    end for
end for
```

Fig. 2 Algorithm for halftone image

1. If $P(i, j) = 0$ (i.e., black pixel), then $I_k = M_n \oplus M_k$. (a) If values of both M_n and M_k are 0 or 1 respectively, then $I_k = 0$. (b) If values of M_n and M_k are either 0 or 1, then $I_k = 1$. This implies that there is 50 % probability that black pixel passes as it is to the I_k.
2. If $P(i, j) = 1$ (i.e., white pixel), then $I_k = \overline{M_n}$. This also implies that there is 50 % probability that white pixel passes as it is to the I_k.

Thus, it makes some kind of confusion about the nature of the original pixel with the compromise in contrast value. Hence, some distortion is introduced in the intermediate matrices. The n shares for n participant from the intermediate matrices are generated using a cover image C according to the following rule:

for $k = 1$–n

$S_k = C \ \oplus I_k$

endfor

Algorithm 2: Algorithm for (2, n) Extended VSS

// Distribution Phase
Pre-condition: Halftoned Image P; A Gray scale Cover Image: C
Post-condition: Two shares p_1 and p_2.
(1) Generate n random binary matrices M_1, M_2,.., M_n
(2) //Generate intermediate matrices according to the following rule
for i = 1 to N
 for j = 1 to N
  if P(i, j) == 0 // black pixel
  for k = 1 to n
  $I_k(i, j) = M_n(i, j) \oplus M_k(i, j)$
  endfor
  else
  for k = 1 to n
  $I_k(i, j) = \overline{M_n(i, j)}$
  end for
  endif
 end for
end for
(3)// Generate shares according to the rule
 for k = 1 to n
 $S_k = C \oplus I_k$
 end for
(4)//Distribute cover images and shares
A single share is consist of pair (C, S_i).
The shares $(C, S_i) \mid 1 \leq i \leq n$ is distributed to n participants.

// Reconstruction Phase
INPUT: Any two shares (C, S_i) and (C, S_i), where $i \neq j$.
OUTPUT: Secret image R.
(1) $I_i = C \oplus S_i$
(2) $I_j = C \oplus S_j$
(3) $R = \overline{I_i \oplus I_j}$

Fig. 3 Algorithm for share generation and revealing phase

Since cover image is a grayscale image, the XORing of C with corresponding I_k has very little effect as XORing only effects the LSB of cover image. This operation generates a single share. The process is repeated n times to generate n shares. Finally, a single share with doublet (C, S_i) is distributed to participant p_i. During revealing phase, any two participants p_i and p_j perform the operation on their shares $(C \oplus S_i)$ and $(C \oplus S_j)$, respectively, to yield intermediate matrices where $1 \leq i, j \leq n$ and $i \neq j$. Finally, any two distinct participants perform the XNOR operation to reveal the secret. Algorithm 2 for generating and revealing the secret image is shown in Fig. 3.

4 Experimental Results and Analysis

This section illustrates the results of an experiment conducted on a grayscale image of Leena (512 × 512) with a cover image of woman.tif (512 × 512) shown in Fig. 4a, b. The first step is to transform the grayscale image into an approximate binary image; we used the algorithm discussed in Sect. 3.1. The converted image of size 512 × 512 pixels is shown in Fig. 4c. Algorithm 2 applied on halftone image

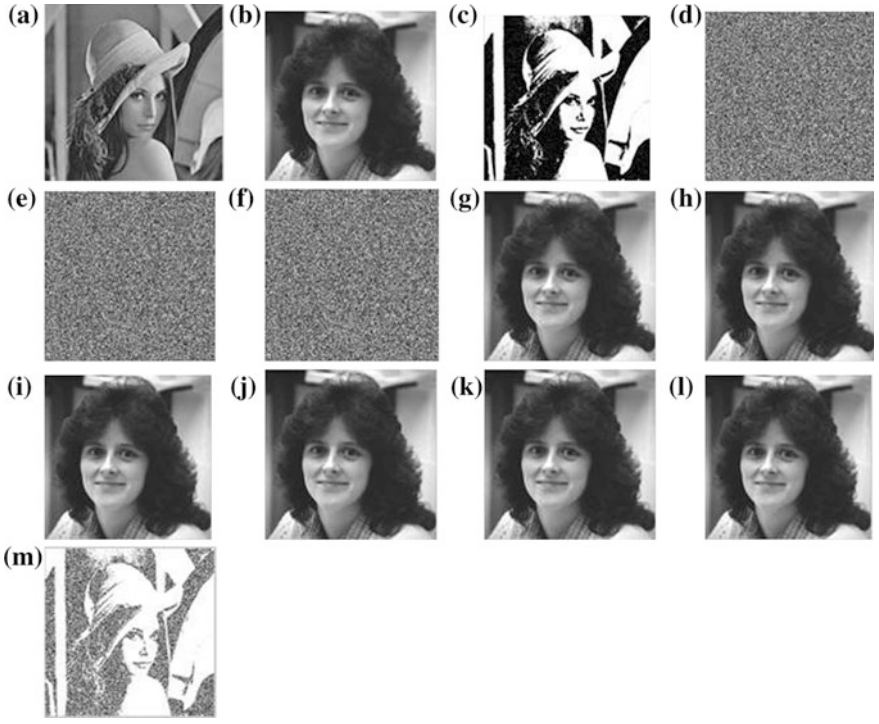

Fig. 4 Result of halftoning and share generation. **a** Secret image. **b** Cover image: C. **c** Halftone image. **d** Intermediate image: I1. **e** Intermediate image: I2. **f** Intermediate image: I3. **g** Share 1: S1. **h** Share 2: S2. **i** Share 3: S3. **j** Participant 1: (C, S1), **k** Participant 2: (C, S2). **l** Participant 3: (C, S3). **m** Revealed image

produces images shown in part d–l of Fig. 4. The intermediate images shown in part d–f are temporary images. These images with the cover image produces shares shown in part g–i. The participants receive a doublet consisting of a cover image and a single share S_i. Once a share S_i is distributed, it cannot be distributed again. At reconstruction, the secret image is obtained by performing XNOR operation. The reconstructed image is shown in Fig. 4m. The experimental results show that our proposed scheme has the following observations:

1. Since encoding and decoding is done on pixels without expanding them, there is no pixel expansion ($m = 1$).
2. The quality of the shadow images are meaningful. This feature is introduced with the help of cover image.
3. The halftoning method explained in Sect. 3 is used to transform the gray level image into a monochrome image. During the probabilistic share generation, the probabilities of sending black-and-white pixels are nearly 50 %. This introduces noise in the secret image which is hidden by some cover image. Thus, when the secret is revealed it mainly suffers due to low PSNR and MSE. The PSNR and MSE values between original secret image and revealed secret image for Fig. 4 are 5.7081 and 17,469. The resulting high value of mean square error is due to both halftoning and share generation phase.
4. As security issue is concerned, it is hard to visualize any difference between individual shares of a participant doublet. However, C and S_i look the same and even though participant p_i makes XOR operation between its components C and S_i, he will never get any information behind the image. To gain complete knowledge of secret image, participation of another participant is mandatory. This makes the scheme more robust and ensures meaningful image.

5 Conclusion

This paper explains the scheme that hides the randomness appeared in the shares by introducing some meaningful information. Visualizing the meaningful information still keeps the actual secret data safe. Such a scheme is known as extended visual cryptography (EVC). This paper introduces an extended cryptography scheme with cover images. The preprocessing of the image is done with the help of the proposed halftoning scheme. The obtained halftoned image is transformed into multiple shares that are distributed to the participants. These shares are finally covered with some cover images to obtain meaningful shares. The experimental results and analysis shows that the proposed scheme has satisfactory results in terms of pixel expansion and security. However, there is scope to develop some improved algorithms that result in low mean square error that arises due to both halftoning and share generation phase.

References

1. Shamir, A.: How to share a secret. Commun. ACM 22(11) (nov 1979) 612–613.
2. Naor, M., Shamir, A.: Visual cryptography, Springer-Verlag (1995) 1–12.
3. Naor, Shamir: Visual cryptographyii: Improving the contrast via the cover base. In: Security Protocols Workshop. Volume 1189. (1996) 197–202.
4. G. Ateniese, C. Blundo, A.D.S., Stinson, D.: Extended capabilities for visual cryp-tography. Theoretical Computer Science 250 (2001) 143–161.
5. Rossand, A., Othman, A.A.: Visual cryptography for biometric privacy. IEEE Transactions on Information Forensic and security 6(1) (2011) 70–81.
6. N. Askari, C.M., Heys, H.: A novel visual secret sharing schemewithout image size expansion. In: IEEE Canadian Conference on Electrical and Computer Engineering (CCECE). (2012) 1–4.
7. N. Askari, H.H., Moloney, C.: An extended visual cryptography scheme without pixel expansion for halftone images. IEEE Canadian Conference of Electrical and Computer Engineering (CCECE) 6(1) (2013) 33–38.
8. Wu, C., Chen, L.: A Study on Visual Cryptography. PhD thesis, Institute of Com-puter and Information Science, National Chiao Tung University, Taiwan (1998).
9. Sharma, S., Priyadarshni, P.: Analysis and design of secure and contrast enhanced secret sharing scheme using progressive visual cryptography. International Journal of Science and Research (IJSR) 3(8) (August 2014) 1181–1186.
10. C. Priyanka, T.V.R., Somashekar, T.: Analysis of secret sharing and review on extended visual cryptography scheme. academia.edu 1(10) (2012) 43–51.
11. D. S. Tsai, T.C., Horng, G.: On generating meaningful shares in visual secret sharing scheme. Imag. Sci. J. 56 (2008) 49–55.
12. Wang, Z., Arce, G.R., Di Crescenzo, G.: Halftone visual cryptography via error di usion. Trans. Info. For. Sec. 4(3) (September 2009) 383–396.
13. Floyd, R.W., Steinberg, L.: An adaptive algorithm for spatial gray scale. In: Society for Information Display. Volume 17. (1976) 75–77.
14. Weir, J., Yan, W.: A comprehensive study of visual cryptography. T. Data Hiding and Multimedia Security 5 (2010) 70–105.
15. Nakajima, M., Yamaguchi, Y.: Extended visual cryptography for natural images. In: in Proceeedings of WSCG. (2002) 303–310.