Extended Visual Cryptography Scheme for Multi-secret Sharing

L. Siva Reddy and Munaga V.N.K. Prasad

Abstract This paper proposes a novel user-friendly visual cryptography scheme for multiple secret sharing. We have generated meaningful shares for multiple secret images using cover images. These meaningful shares are shared among participants. All the shares are required to recover secret images that are shared. The proposed scheme uses Boolean-based operations for generating meaningful shares and recovering all secret images that are used. The proposed scheme achieved lossless recovery of multiple secrets and overcomes the problem of management of meaningless shares.

Keywords Visual cryptography · User-friendly visual cryptography scheme · Multiple secret sharing · Extended visual cryptography scheme · Meaningful shares

1 Introduction

Secret sharing scheme was initially proposed by Blakely and Shamir in 1979 [1, 2, 3]. In general this secret sharing scheme is also called (k,n) secret sharing. In this scheme secret information is divided into n shares and distributed among n participants and it is an encryption operation. At least k participants are needed to recover original secret information and it is a decryption operation. Participants less than k cannot recover secret information. Naor and Shamir proposed (k,n) visual cryp-

L. Siva Reddy (✉) · M.V.N.K. Prasad
Institute for Development and Research in Banking Technology, Hyderabad, India
e-mail: sivareddy09503@gmail.com

M.V.N.K. Prasad
e-mail: mvnkprasad@idrbt.ac.in

L. Siva Reddy
School of Computer and Information Sciences, University of Hyderabad,
Hyderabad, India

A. Nagar et al. (eds.), *Proceedings of 3rd International Conference on Advanced Computing, Networking and Informatics*, Smart Innovation,
Systems and Technologies 44, DOI 10.1007/978-81-322-2529-4_26

tography scheme (VCS) to encode secret which is in the image form [4]. In this scheme computational devices are used to encrypt secret image into n shares. Decryption can be done by human visual system after stacking k shares. This scheme is useful if there are no computational devices for decryption. Random-grid based VCS is proposed by Kafri et al. and Shyu [5, 6] to overcome the drawback of pixel expansion of conventional scheme. In this scheme each share acts as random grid.

Multiple Visual Cryptography Secret (MVCS) sharing scheme was proposed to encrypt multiple secrets at a time. Wu and Chen [7] proposed (2,2) MVCS to encrypt two secrets into two square shares SH1 and SH2. The first secret S1 is recovered by stacking two shares SH1 and SH2. The second secret image S2 is recovered by stacking share SH1 with 90° rotated share SH2 [7]. The rotation angle can be of q × 90 where $1 \leq q \leq 3$. Wu and Chang [8] proposed multi-secret sharing scheme by encrypting secrets in the form of circular shares. Generation of secret S2 can be done by stacking share SH1 with 360° multiple rotated share SH2. In this scheme the limitation of 90, 180, 270° rotation is removed. Shyu et al. [9] proposed MVCS for more than two secrets using two circular shares with different rotation on one of shares. Feng et al. [10] proposed another MVCS scheme for sharing multiple secrets. In this scheme two circular ring shares R1 and R2 are used to encrypt multiple secrets. Some of the other authors who work on multiple secret sharing are Shyu et al. [11], Chang et al. [12], Wu et al. [13].

All the above mentioned schemes for MVCS have many drawbacks. One of the main drawbacks is lack of visual quality of the recovered secret image. The second drawback is distortion of the recovered image from the original image (pixel expansion). These schemes didn't prepare meaningful shares for users. These meaningful shares are mainly used for identification and management by users and to avoid suspicion of attackers who may focus on meaningless shares.

The disadvantages of meaningless shares can be minimized by using extended visual cryptography scheme (EVCS). It is also called as user-friendly visual cryptography scheme. The EVCS generates meaningful shares by stacking cover images onto meaningless shares. By using EVCS dealers can identify each share easily. Ateniese et al. proposed (k,k)-threshold EVCS which generates meaningful shares using binary images [14]. In this sheme k meaningful shares are generated and all are needed to recover secret image. Fang [15] proposed EVCS for conventional VC with a progressive decryption effect. Here progressive decryption effect means quality of secret image gets improved when number of shares is increased in overlapping. Chen et al. [16] proposed EVCS for random-grid-based techniques. Random-grid based techniques are pixel expansion less schemes. Wang et al. developed an EVCS using matrix extension algorithm which generates random matrix shares instead of meaningless shares [17]. Here shares are matrices which have pixel values of secret image.

Chen and Wu proposed an (n,n) secure Boolean-based multi-secret sharing scheme [18]. In this scheme n shares are generated using n secret images. This scheme mainly uses Boolean-based operations like XOR and bitwise circular shift operation. N shares are required to recover n secrets. Chen and Wu scheme [18] uses random image R in order to randomize the original secret images. It is generated by using two functions XOR operation and bitwise shift operation. This scheme for MVCS faces some drawbacks. The first drawback is generation of meaningless shares in which dealers feel difficulty to manage those shares. The second drawback is to use minimum number of secrets (4 or more) for sharing in order to ensure relative security. If we use two secrets for share generation then shares may have secret information as they are generated using XOR calculation.

This paper proposes extended visual cryptography scheme for multiple secret sharing that develops meaningful shares from multiple secrets and cover images. The proposed scheme uses Boolean-based operations for generating meaningful shares using cover images. Lossless recovery of multiple secrets is achieved using proposed scheme. The proposed scheme is free from pixel expansion. The experimental results of the proposed work shows that MVCS sharing scheme gets improved with meaningful shares.

The organization of this paper is as follows. Proposed scheme is discussed in Sect. 2. Sections 2.1 and 2.2 explains proposed scheme share generation and its recovery, respectively. Section 2.3 discusses on proposed scheme. Section 3 shows experimental results and comparison with related work. Section 4 completes the proposed scheme with conclusion.

2 Proposed Scheme

This section explains proposed work of extended visual cryptography scheme for multi-secret sharing. This scheme generates meaningful shares using multiple secrets and cover images. Boolean based operations are mainly used in this scheme. Lossless recovery of multiple secrets is achieved using the proposed work. Sections 2.1 and 2.2 explains about share generation and secret recovery of the proposed scheme. Section 2.3 discusses on proposed scheme.

2.1 Share Generation

This section explains how to generate meaningful shares using multiple secret images and cover images. The proposed scheme for share generation uses random image generation function which was proposed by Chen and Wu [18]. This random image generating function mainly involves two functions F_1 and F_2. Function F_1 uses XOR operation and function F_2 uses bitwise circular shift operation. The algorithm for share generation is as follows:

1. Let I_1, I_2, …, I_n are n multiple secret images that are used as input for share generation.

2. Now random image R_1 is generated using secret images I_1, I_2, …, I_n as follows:

$$\begin{aligned} R_1 &= F_1(F_2(I_1, I_2, \ldots, I_n)); \\ \text{where } F_2 &= I_1 \oplus I_2 \oplus \ldots \oplus I_n; \\ F_1 &= \text{bitwise circular shift of } F_2. \end{aligned}$$

3. Meaningless images M_1, M_2, …, M_n, are generated using XOR operation of given multiple secret images with random image R_1 respectively.
4. Now meaningful shares S_1, S_2, …, S_k are generated from meaningless images and n cover images C_1, C_2, …, C_n using Boolean OR and Boolean AND operations as follows:

$$\begin{aligned} S_1 &= M_1 \otimes C_1 \\ S_2 &= M_1 \odot C_1 \\ S_3 &= C_1 \\ S_4 &= M_2 \otimes C_2 \\ S_5 &= M_2 \odot C_2 \\ S_6 &= C_2 \\ &\vdots \\ S_{k-2} &= M_n \otimes C_n \\ S_{k-1} &= M_n \odot C_n \\ S_n &= C_n \end{aligned}$$

where $1 \le k \le 3 \times n$

5. Finally k meaningful shares are generated for the given multiple secret images.

Figure 1 shows share generation phase of the proposed scheme. In this phase n multiple secret images $I_1, I_2, \ldots, I_n$ are used. A random image is generated from these secret images using random image generation function. Then N meaningless images M_1, M_2, …, M_n are generated by applying XOR operation on the secret images and random image. Finally, K meaningful shares S_1, S_2, …, S_k are developed by performing Boolean operations AND, OR between meaningless images and cover images.

2.2 Secret Images Recovery Procedure

The recovery procedure uses k meaningful share images from share generation as an input for recovering original secret images. Boolean XOR operation is used on these shares to generate n meaningless shares. Random image R_1 is generated from these meaningless share images using random image generating function. Finally n secret images are recovered by applying Boolean XOR operation between random image and meaningless shares. The algorithm for secret images recovery is as follows:

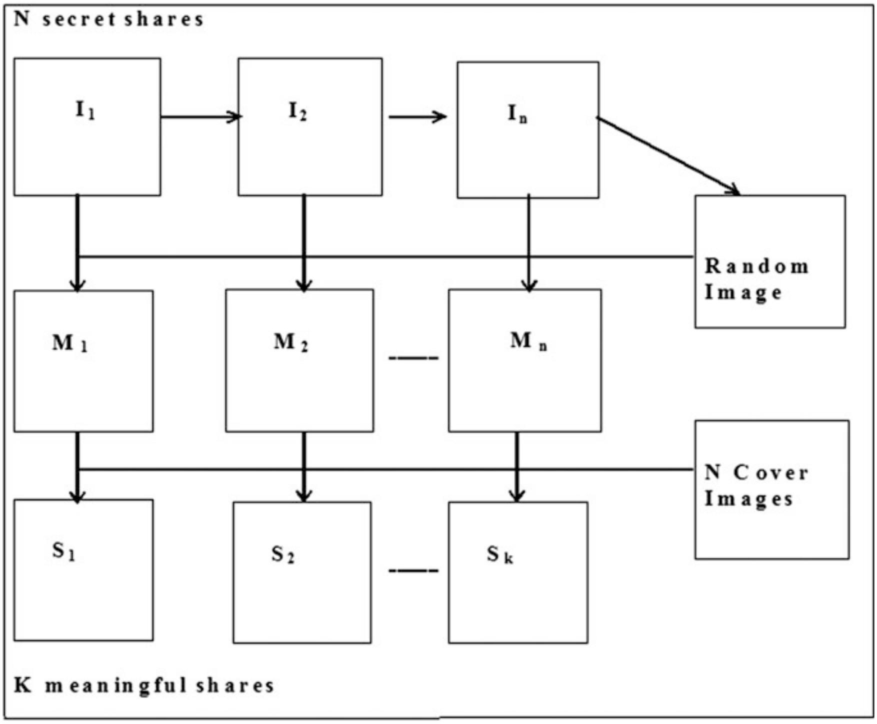

Fig. 1 N meaningful share images generation from n secret images

1. Recover meaningless shares $M_1, M_2, \cdots, M_n$ from k meaningful shares as follows:

$$\begin{aligned} M_1 &= S_1 \oplus S_2 \oplus S_3; \\ M_2 &= S_4 \oplus S_5 \oplus S_6; \\ &\vdots \\ M_n &= S_{k-2} \oplus S_{k-1} \oplus S_k; \end{aligned}$$

   where 1 ≤ k ≤ 3 × n
2. Random image R_1 is generated using meaningful shares.
3. Finally, n secret images $I_1, I_2, \cdots, I_n$ are generated as follows:

$$\begin{aligned} I_1 &= M_1 \oplus R_1; \\ I_2 &= M_2 \oplus R_1; \\ &\vdots \\ I_n &= M_n \oplus R_1; \end{aligned}$$

2.3 Discussion on Proposed Scheme

The proposed scheme develops (k,k) multi-secret sharing with user-friendly visual cryptography. It generates k shares for multiple secrets (2 or more). K shares are needed to recover all secret images. It doesn't require code book for generating meaningful shares. These meaningful shares are generated using simple Boolean operations. So this scheme requires less CPU computation time. Moreover the proposed scheme achieved lossless recovery of multiple secret images. The two drawbacks of Chen and Wu [18] scheme can be overcome by using the proposed method for multi-secret sharing. The developed scheme generates meaningful shares and it can encrypt 2 or more secrets in a more secure manner.

3 Experimental Results

This section discusses about the proposed method experimental results and its comparison with related work. We used Matlab R2010a on a computer with Windows 7 operating system, Intel core I3 processor and 4 GB RAM for implementing the proposed work.

3.1 Results with 2 Secrets

Figure 2 shows experimental results of the proposed work. Here we took two secret images: Pepper, Barbara and two cover images: Lena, Cameraman. All these images are of 512 × 512 size. Figure 2e–j shows the meaningful shares generated by applying proposed work share generation operation. Figure 2k, l shows recovered secret images generated by applying secret recovery procedure. Lossless recovery of the secret images is achieved with meaningful shares.

Peak Signal-to-Noise Ratio (PSNR) is the accuracy measure for the image quality of generated shares. Table 1 shows PSNR values between share images and original images. In general, PSNR value of any image to be visible is more than 30 dB. The proposed work achieved PSNR value of the recovered images approaches to infinite which means that lossless recovery of secret images. Meaningful shares generated by the proposed scheme have PSNR values more than 50 dB. So the generated shares can be easily managed by the dealer as they are visible to human visual system. In this way proposed method works as extended visual cryptography scheme for multiple secret sharing.

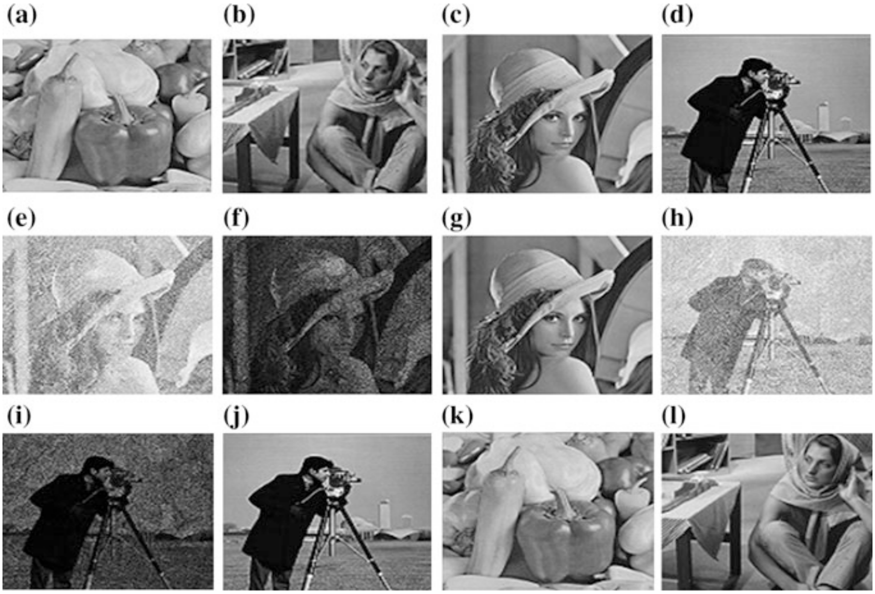

Fig. 2 Two secret images (**a**, **b**), two cover images (**c**, **d**), six meaningful shares (**e**–**j**), recovered images (**k**, **l**)

Table 1 PSNR values between share images and original images

Image	PSNR value
Share 1 versus cover image 1	57.6077
Share 2 versus cover image 1	57.8255
Share 3 versus cover image 1	Infinite
Share 4 versus cover image 2	56.9659
Share 5 versus cover image 2	57.8235
Share 6 versus cover image 2	Infinite
Recovered image 1 versus secret image 1	Infinite
Recovered image 2 versus secret image 2	Infinite

3.2 *Comparison of the Proposed Method with Related Schemes*

This section explains the comparison between the proposed work and the related schemes. Comparison is made in different areas like: share shape, shareable secrets, quality of share, recovery type, and pixel expansion. Share shape indicates type of generated share like square, rectangle, and circle. Shareable secrets mean number of secrets that can be shareable by using the scheme. Quality of share explains about generated share visual quality. Recovery type indicates that how secret images are recovered for the scheme. Pixel expansion explains about distortion of recovered image from the original image.

Table 2 Comparison between related works and the proposed method

Proposed method	Share shape	Shareable secrets	Share quality	Type of recovery	Pixel expansion
Wu and Chang [8]	Circle	2	Meaningless	Recognizable	Yes
Shyu et al. [9]	Circle	n	Meaningless	Recognizable	Yes
Feng et al. [10]	Square	n	Meaningless	Recognizable	Yes
Chen and Wu [19]	Square	n − 1	Meaningless	lossless	No
Shyu and Chen [20]	Square or rectangle	2 or 4 or 8	Meaningless	Recognizable	Yes
Chen and Wu [18]	Square	n	Meaningless	Lossless	No
Proposed scheme	Square	n	Meaningful	Lossless	No

Table 2 indicates how proposed scheme achieved better sharing for multiple secret images. It generates square shape share images which are mainly used in image processing. It can share multiple secrets without distortion which is not possible for schemes of [8–10, 19, 20]. The most important property of the proposed method is meaningful share generation which is impossible for all other schemes. Lossless recovery of all the secrets is only possible with the proposed scheme and Chen and Wu [18] scheme. From all the comparisons we found that the proposed work is better useful scheme for multiple secret sharing.

4 Conclusion

In this paper we proposed a novel algorithm for meaningful share generation of multiple secret sharing scheme. The experimental results show that proposed scheme is a better suitable scheme for multi-secret sharing than previous approaches. It also indicates that lossless recovery of multiple secrets is achieved with our scheme. As the scheme requires only Boolean based operations it is computationally costless scheme. There are many advantages applicable for the proposed work. The first one is generating meaningful shares which enable dealers to manage the shares effectively. The second one is its distortion free recovery of multiple secrets. The third one is its ability to share many secrets. The main contribution of our proposed work is applying extended visual cryptography scheme or user-friendly cryptography for the multi-secret sharing schemes with lossless recovery of secrets.

References

1. Blakely, G.R.: Safeguarding cryptography keys. Proc. Nat. Comput. Conf. **48**, 313–317 (1979)
2. Shamir, A.: How to share a secret. Commun. ACM **22**, 612–613 (1979)
3. Cimato, S., Yang, C.-N.: Visual cryptography and secret image sharing. In: Digital Imaging and Computer Vision Series (2012)

4. Naor, M., Shamir, A.: Visual cryptography, In: Proceedings of Advances in Cryptology, pp. 1–12 (1995)
5. Kafri, O., Keren, E.: Encryption of pictures and shapes by random grids. Opt. Lett. **12**, 377–379 (1987)
6. Shyu, S.: Image encryption by random grids. Pattern Recogn. **40**, 1014–1031 (2007)
7. Wu, C.C., Chen, L.H.: A study on visual cryptography. Master Thesis, Institute of Computer and Information Sciences, National Chaio Tung University, Taiwan (1998)
8. Wu, H.C., Chang, C.C.: Sharing visual multi-secret using circle shares. Comput. Stan. Interfaces **28**, 123–135 (2005)
9. Shyu, S.J., Huang, S.Y., Lee, Y.K., Wang, R.Z.: Sharing multiple secrets in visual cryptography. Pattern Recogn. **40**(12), 3633–3651 (2007)
10. Feng, J.B., Wu, H.C., Tsai, C.S., Chang, Y.F., Chu, Y.P.: Visual secret sharing for multiple secrets. Pattern Recogn. **41**, 3572–3581 (2008)
11. Shyu, S.J., Huang, S.Y., Lee, Y.K., Wang, R.Z.Chen: Sharing multiple secrets in visual cryptography. Pattern Recogn. **40**, 3633–3651 (2007)
12. Chang, C.-C., Tu, N.T., Le, H.D.: Lossless and unlimited multi-image sharing based on Chinese remainder theorem and Lagrange interpolation. Sig. Process. **99**, 159–170 (2014)
13. Wu, H.C., Chang, C.C.: Sharing visual multi-secrets using circle shares. Comput. Stand. Interfaces **28**, 123–135 (2005)
14. Ateniese, G., Blundo, C., Santis, A.D., Stinson, D.R.: Extended capabilities for visual cryptography. Theoret. Comput. Sci. **250**, 143–161 (2001)
15. Fang, W.P.: Friendly progressive visual secret sharing. Pattern Recogn. **41**, 1410–1414 (2008)
16. Chen, T.H., Lee, Y.S.: Yet another friendly progressive visual secret sharing scheme. In: Proceedings of 5th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 353–356 (2009)
17. Wang, D., Yi, F., Li, X.: On general construction for extended visual cryptography schemes. Pattern Recogn. **42**, 3071–3082 (2009)
18. Chen, T.H., Wu, C.S.: Efficient multi secret image sharing based on Boolean operations. J. Syst. Softw. **92**, 107–114 (2014)
19. Chen, T.H., Wu, C.S.: Efficient multi-secret image sharing based on Boolean operations. Sig. Process. **91**, 90–97 (2011)
20. Shyu, S.J., Chen, K.: Visual multiple secret sharing based upon turning and flipping. Inf. Sci. **181**, 3246–3266 (2011)