International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:2682
Vol.4,No.7, July 2015 DOI:10.15693/ijaist/2015.v4i7.111-117

Random Grid based Extended Visual Cryptography Schemes using OR and XOR Decryption

Sruthy K Joseph
PG Student/ Department of CSE
ASIET, MG University, Kerala,

Ramesh R
Asst. Prof / Department of CSE
ASIET, MG University, Kerala

***Abstract*—Visual cryptography (VC) is a paradigm of cryptography which prevents a secret from being modified or destructed by using the notions of perfect cipher and can be easily decoded by the human visual system. It doesn't require any complex cryptographic computations. This visual secret sharing scheme is developed by Moni Naor and Adi Shamir in 1994. In this scheme an image is divided into n shares, so that only someone with all k (k<n) shares can decode the secret, while k-1 shares will not reveal any information about the original secret image. But these initial schemes of visual cryptography suffer from many drawbacks such as: pixel expansion, share management difficulty, etc. So this paper discusses three visual cryptography schemes: OR-based (n, n) VCS, XOR-based (n, n) VCS and extended (n, n) VCS; using random grids. Since RG is used here all the three schemes were designed without pixel expansion. (n, n) extended VCS offers better share management without pixel expansion. This method also removes the restriction of using one cover images for all generated shares. The proposed (n, n) extended VCS provide meaningful share images with improved security and visual quality.**

Index terms - Meaningful share, random grid, visual quality, visual cryptography, OR, XOR, pixel expansion

I. INTRODUCTION

To ensure fundamental data security requirements such as confidentiality, integrity, availability during data transmission over the Internet, conventional cryptography schemes were used in previous decades. It uses a secret key and complex mathematical computation to convert plain text into meaningless (cipher) text. Major disadvantage of cryptography is that a computer is required for the both process of encryption and decryption, resulting in wastage of computational resources and CPU execution time. Cryptography can be used only for the secure transmission of textual data but it cannot be used when the data to be secured is an image (picture or handwritten documents). For this a new visual secret sharing (VSS) scheme called visual cryptography (VC) was developed to protect sensitive images from rapacious behavior. It is initially proposed by Naor and Shamir [1] in 1994.Visual cryptography is a powerful visual secret sharing scheme in which a secret image is distributed among some (say *n*) participants by dividing the secret image into two or more noise-like shares (or shadow images). When the shares on transparencies are stacked (superimposed) together, the original secret image will be revealed without any mechanical devices like a computer. Decryption can be done using the Human Visual System (HVS).

In the (*k, n*) threshold VSS scheme, a secret image is shared by generating *n* noise-like share images. Superimposing any *k (where* $k \leq n$*)* or more share images together, the secret image will get revealed using human visual system. On the other hand, if *k* - 1 participants attempt to reconstruct the secret, they will fail and the secret will never be revealed.VC is a simple mechanism for decrypting/ decoding the secret image with perfect security when computer resources are not available. Various schemes of visual cryptography were briefly discussed in [15].

This paper provides some visual cryptography schemes that can generate non-expanded (size invariant) share images. However, most of the available VC schemes perform pixel expansion method to decompose the secret image and so the generated share images become larger than the original secret image. The major drawback caused due to this enlargement is that it leads to the wastage of storage space, network bandwidth (unnecessary wastage of network resources while transmitting the share images) and distorts the image quality. So our method utilizes random grid method which can construct share images without pixel expansion.

II. RELATED WORK

The process of visual cryptography proposed by Naor and Shamir [1] discusses a technique for encrypting a binary secret image into *n* shares (printed on transparencies), where each pixel is expanded *m* times. Each participant will get a share image but the secret image cannot be revealed with any one share. Any n participants can compute the original secret when any *k* (or more) of them are stacked together. No group of *k-1* (or fewer) participants can compute the original secret.
Figure 1 shows the basic workflow of visual cryptography schemes. The secret image cannot be seen from one transparency, but when *k* or more transparencies are stacked together the image will begin to emerge as the contrast between the black and white pixels becomes sufficient that the human eye will be able to recognize the secret image. Neither computational devices nor cryptographic knowledge are required for the decryption process. This approach is called *(k, n)*-threshold Visual Secret Sharing (VSS).
Initially the binary secret image is encoded (i.e. shares are generated) and during decoding the k or n shares are stacked together (according to the *(k, n)* or *(n, n)* scheme discussed

later) to reveal the secret image. The secret image will get visible to the human visual system.

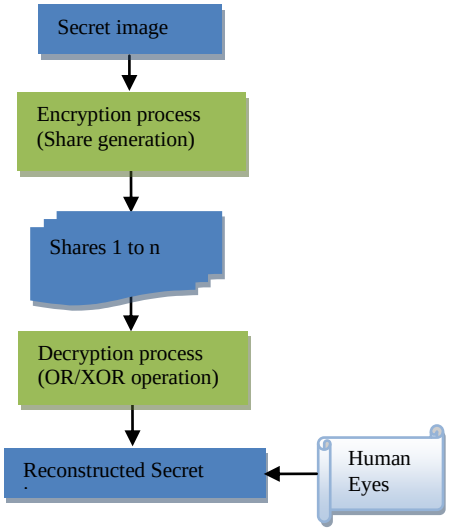


Figure 1. Basic flowchart of Visual Cryptography

In the *(k, n)* visual cryptography scheme, two collections of *(n* x *m)* Boolean matrices (Basis matrices), C0 and C_1 are used. To share a white (black) pixel, the dealer randomly selects one row of the Boolean matrix C_0 (C_1) and assigns it to the corresponding share image. The gray level and contrast of the m sub-pixels in each of the n share images is defined by the chosen row (of the Boolean matrix).

$$C_0 = \begin{bmatrix} 1 & 0 & 0 & . & . & 0 \\ 1 & 0 & 0 & . & . & 0 \\ . & . & . & . & . & . \\ 1 & 0 & 0 & . & . & 0 \end{bmatrix} \quad C_1 = \begin{bmatrix} 1 & 0 & 0 & . & . & 0 \\ 0 & 1 & 0 & . & . & 0 \\ . & . & . & . & . & . \\ 1 & 0 & 0 & . & . & 1 \end{bmatrix}$$

The major drawbacks of visual cryptography include pixel expansion, loss of contrast, and share management difficulty (due to random or noise-like share images).

(2, 2) Visual Cryptography Scheme (VCS)

The secret image is divided into two (*n*) share images so that the secret can be revealed only if both the shares are stacked together. The Boolean matrices to be dispatched can be designed as follows:

$$S_0 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \quad S_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

To encode the white secret pixel, one row from S_0 is selected and dispatched towards each share. The value 1 and 0 indicates the black and white pixels respectively. Two pixels from the first row are distributed to the first share and the remaining two pixels in the second row to the second share.

A. Traditional Visual Cryptography

A secret is something which is kept from the

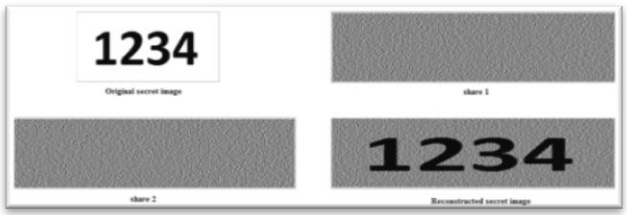
Secret pixel	Share 1	Share 2	Stacked pixel (OR operation)
■	■□ / □■	□■ / ■□	■■ / ■■
□	■□ / □■	■□ / □■	■□ / ■■

knowledge of any but the initiated or privileged. Secret sharing defines a method by which a secret is distributed among a group of participants, whereby each participant is allocated a piece of the secret. This piece of the secret is known as a *share*. The secret can only be reconstructed when a sufficient number of shares are combined together. While these shares are separate, no information about the secret can be accessed. That is, the shares are completely useless while they are separated.

Within a secret sharing scheme, the secret is divided into a number of shares and distributed among n persons. When any *k* or more of these persons (where k ≤ n) bring their shares together, the secret can be recovered. However, if *k - 1* persons attempt to reconstruct the secret, they will fail. Due to this threshold scheme, we typically refer to such a secret sharing system as a *(k, n)*-threshold scheme or k-out-of-n secret sharing, where n is the number of Total Participant and k is the number of Qualified Participant The basic model for visual sharing of the k out of n secret image is such that;

- Any *n* participants can compute the original message if any *k* (or more) of them are stacked together.
- No group of *k-1* (or fewer) participants cannot compute the original message.

In *k out of n* visual cryptography scheme, a digital image is divided into n number of shares by some cryptographic computations. In the decryption process only *k* or more number of shares can reveal the original information and so less than *k* number of shares can not reveal the original information. *A (k, n)* VSS scheme is a method by which the shared image (printed text, handwritten notes, pictures, etc.) is visible by k or more participants by stacking their transparencies with the help of an overhead projector. To share a white pixel, the dealer randomly chooses one of the matrices in C_0 and to share a black pixel, the dealer randomly chooses one of the matrices in C_1. The chosen matrix defines the colour of the *m* sub-pixels in each one of the *n* transparencies. The major drawback is the pixel expansion and low contrast of the reconstructed secret image.



B. Extended Visual Cryptography

Extended Visual Cryptography (EVC) takes the idea of visual cryptography further by creating shares which are meaningful to anyone who views them. This helps to alleviate suspicion that any encryption has taken place and also presents visually pleasing shares which incorporate all the previously mentioned features of VC. It allows the construction of visual secret sharing schemes within which the shares are meaningful as opposed to having random noise on the shares. After the sets of shares are superimposed, this meaningful information disappears and the secret is recovered. Meaningful shares avoid attention of hacker considering the security issues over the communication channels. EVCS can also be viewed as a method of steganography. One scenario of the applications of EVCS is to evade the custom inspections, because the shares of EVCS are meaningful images, hence there are fewer chances for the shares to be suspected and detected. In case of EVCS, shares were simply generated by replacing the white and black sub-pixels in a traditional VCS share with transparent pixels and pixels from the cover images, respectively. This scheme provides meaningful share images but endure pixel expansion problem.

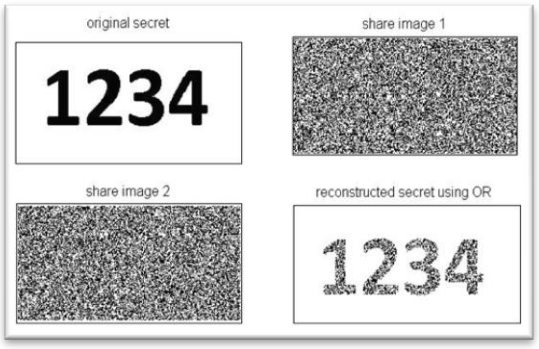
Generally all extended VC schemes show some meaningful content on its shares (same or different content), but a scheme is said to be absolute when all the shares show different content over it.

C. Halftone Visual Cryptography

The halftoning technique can be applied to both colour and gray-scale images. Halftoning simulates a continuous tone through the use of dots, varying either in size or in spacing. In general halftone visual cryptography framework, a secret binary image is encrypted into high-quality halftone images or halftone shares. It applies the rich theory of blue noise halftoning to the construction mechanism used in traditional VC to produce halftone shares, while the security properties are still maintained. The same contrast is obtained over the whole decoded image. The halftone shares bear significant visual information to the viewers, such as buildings, landscapes, etc. The visual quality attained by the new method is significantly better than that attained by extended VC or any other available VC method known to date. Halftone VC is built upon the basis matrices and collections available in conventional VC. This scheme is better than EVC in terms of contrast of the recovered secret but both the shares and the reconstructed secret suffer from pixel expansion.

D. Random Grids based Visual Cryptography

Random grid (RG) is a method to implement visual cryptography (VC) without pixel expansion. RG is defined as a transparency comprising a two-dimensional array of pixels, where each pixel can be fully transparent (white) or totally opaque (black), and the choice between the alternatives is made by a coin-flip procedure. Half of the pixels in a RG are white, and the remaining pixels are black. Encoding an image by random grids was introduced initially in 1987 by Kafri and Keren. A binary secret image is encoded into two noise-like transparencies with the same size of the original secret image, and stacking of the two transparencies reveals the content of the secret. Comparing RGs with basis matrices, one of the major advantages is that the size of generated transparencies is unexpanded. The RG scheme is similar to the probabilistic model of the VC scheme, but the RG scheme is not based on the basis matrices.

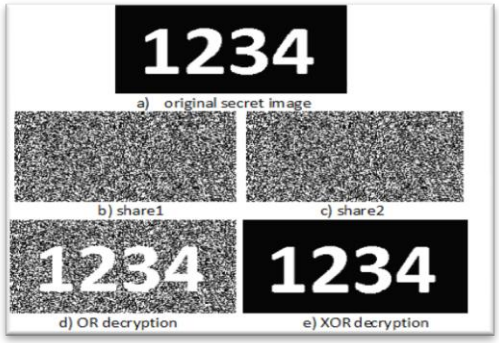


E. User-friendly Visual Secret sharing scheme

Chen and Tsao [5] proposed a novel random grid based visual secret sharing scheme that has been skillfully designed to produce meaningful (user-friendly) share images without pixel expansion. It explains a procedure with different light transmissions based on the share images and the logo image (cover image) used to make the shares user-friendly. To implement meaningfulness, this scheme adjusts the respective contrasts of some areas of the two generated random grids G_1 and G_2 based on the cover image.

F. OR and XOR Visual Cryptography

A (k, n) visual cryptographic scheme encrypts a secret image into n share images (printed on transparencies) distributed among n participants. When any k participants stack their shares on an overhead projector (OR operation), the secret image can be visually discovered by a human visual system without the aid of computers (computation). But the monotone property of OR operation reduces the visual quality of reconstructed secret image for OR-based VCS. Generally all the conventional visual cryptography schemes (VCS) uses OR operation for stacking operations and so it is also called OR-based VCS. But it offers a poor visual quality image during decoding (stacking). Major advantage of XOR-based VCS (XVCS), is that it uses XOR operation for decoding those results to enhance the contrast.



III. METHODOLOGY

Visual cryptography is paradigm of cryptography which allows visual information (e.g. images, printed text and handwritten notes) to be encrypted in such a way that its decryption can be done by the human eye, without the aid of computers. It avoids the need of complex mathematical computations during decryption and the secret image can be reconstructed using stacking (OR operation). There are diverse visual cryptography schemes based on the factors such as pixel expansion, contrast, security, meaningless or meaningful shares, type of secret image (either binary or color) and the number of secret images encrypted (single or multiple secret) etc. This paper mainly discusses two visual cryptography schemes: *OR-based VC* and *XOR-based VC*; and also steps to improve these schemes into *extended OR-based (n, n) VC* and *extended XOR-based (n, n) VC*

R1	R2	R1⊗ R2
0	0	0
0	1	1
1	0	1
1	1	1

R1	R2	R1 ⊕ R2
0	0	0
0	1	1
1	0	1
1	1	0

$\oplus$ represents bitwise-XOR operation and $\otimes$ represents bitwise-OR operation.

There are mainly three schemes to generate size invariant shares: probabilistic VC, random grid based VC and multi-pixel encoding. Here we are using random grid based method to construct shares. In (2, 2) RG based VC, the binary secret image is encrypted in such a way that, the first share RG_1 is generated randomly. And the second share RG_2 is generated according to the binary secret image, S and the first share (RG_1) as follows:

Secret pixel, S(i,j)	RG_1	RG_2	Stacked result, S′(i,j)
■	■□	□■	■■
□	■□	■□	■□

The stacked secret image, S′, will be recovered with 50% contrast when bitwise-OR operation is used for decryption. Perfect recovery can be obtained when bitwise-XOR operation is used for decryption. This scheme generates meaningless (random or noise-like) share images without pixel expansion. In case of *(n, n)* scheme, the shares are produced in the same way as that of *(2, 2)* scheme.

Algorithm1: (2, 2) RG based VC

Input: A binary secret image S.

Output: Two random grids R_1 and R_2

1. Generate a random grid R_1 randomly,

   where R_1 (i, j) ϵ {0, 1} [R_1 =rand (0.5);]

2. For each secret pixel S (i, j),

$$R_2(i,j) = \begin{cases} R_1(i,j), \text{ if } S(i,j) = 0 \\ R_1(i,j)', \text{ otherwise} \end{cases}$$

3. Output: R_1 and R_2

This algorithm will generate two non-expanded share images and the decryption process can be either OR / XOR operation. If OR operation is used for decryption process, then the reconstructed secret will be of 50% contrast and is enough for efficient viewing using Human Visual System. And if XOR operation is used then it offers perfect reconstruction of the secret image without any distortion.

Algorithm2: OR-based (n, n) VCS

Input: A binary secret image S of *m x n* size.

Output: A set of *'n'* random grids R_1, R_2, R_3, R_4… R_n

1. Initialize *'n'* random grids with ½ probability.
2. For each secret pixel S(i,j), $1 \le i \le m$ and $1 \le j \le n$
3. Set x_1 as R_1
4. For k: 2 to n-1

$x_k = f(R_k, a_{k-1})$

5. $R_n = f(S, a_{n-1})$
6. Output: R_1, R_2, R_3, R_4… R_n.

where s ϵ S, r ϵ R and function f(s, r1) is:

$f(s, r_1) = r_2$, i.e., s=if s=0, $r_2=r_1$ else s=1 then $r_2=r_1$.

Both algorithms 1 and 2 will generate size invariant share images for a binary secret image S. The decryption process is simply stacking (OR) operation. These schemes produce meaningless share images without the need of codebook.

The algorithm2 can be diagrammatically represented in the figure 2:

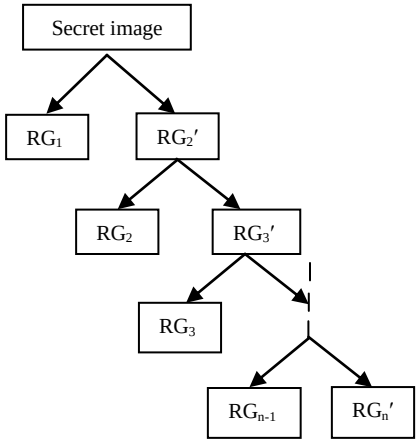


Figure 2. Random grid based Visual Cryptography

Algorithm3: XOR-based (n, n) VCS

Input: A binary secret image S of *m x n* size.
Output: A set of *'n'* random grids R_1, R_2, R_3, R_4… R_n

1. Initialize *'n'* random grids with ½ probability.
2. For k: 2 to n-1
   rr = rr $\oplus$ r_k
3. Generate n^{th} random grid R_n as
   i. If S(i, j) = 0
      rr =0 then $r_n = 0$
      rr = 1 then $r_n = 1$
   ii. else S(i, j) = 1
      rr = 0, then $r_n = 1$
      rr = 1, then $r_n = 0$
4. Output: R_1, R_2, R_3, R_4… R_n.

The decryption process of algorithm3 is by using XOR operation. The binary secret, S will be reconstructed exactly without any distortion or pixel expansion.

Extended (n, n) VCS

Extended VC will generate the meaningful share images and so it alleviates encryption and makes share management easier. The meaningless (random) shares can be generated by any of the above two algorithm (2 or 3). To make shares meaningful, n different cover images can be used. Set a variable α, values must be between 0.5 and 1. Generate n cover image pixels with α probability. Replace original random grid pixels with cover images to show an illusion of cover image on it.

Algorithm4: Extended (n, n) RG based VCS

Input: A binary secret image S of *m x n* size and 'n' cover images, CI_k, $1 \le k \le n$

Output: A set of *'n'* random grids R_1, R_2, R_3, R_4… R_n

1. Generate 'n' share images either using algorithm 2 or algorithm 3.
2. Set $\alpha : 0.5 \le \alpha \le 1$
3. Generate α % of pixels from cover images, CI_k
4. If all the generated pixels are white, randomly choose one pixel and set it as black pixel.
5. Replace the generated cover images pixels with the random shares to make them meaningful.
6. Use either OR / XOR operation for decryption according to the algorithm used in step 1.

The parameter α can be varied between 0.5 and 1. When α is near to 0.5 the decoded secret is much clearer and the share images will be of less quality, whereas α closer to 1 then the shares will have higher contrast and the decoded secret will be of poor quality.

Encryption process of the proposed extended (n, n) RG based VCS

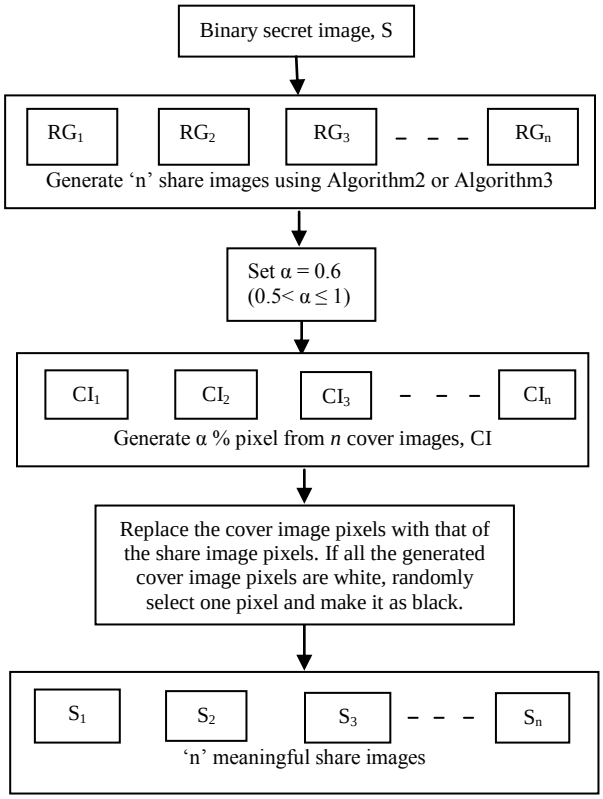
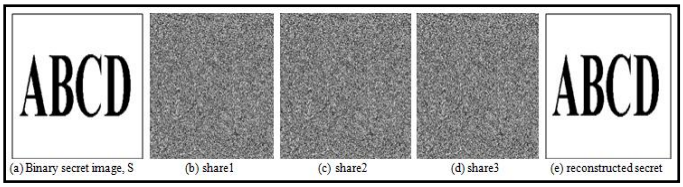


Figure 3. Proposed Extended (n, n) Visual Cryptography Scheme

In the above figure 3, RG_1 RG_2, RG_3 … RG_n are random shares generated by either algorithm 2 or algorithm 3. CI_1, CI_2, CI3… CI_n are *n* different cover images that make *n* share images meaningful (each share with different content).

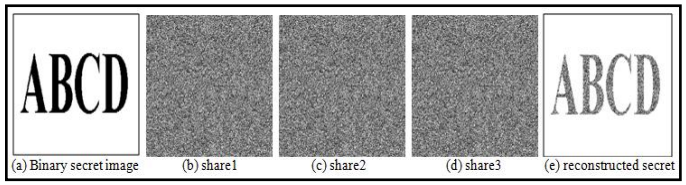
IV. EXPERIMENTAL RESULTS

For XOR-based (n, n) VCS, the contrast of the decoded secret image will be 100%.i.e.; perfect secret reconstruction is possible using this algorithm. The following figure shows an example of XOR-based (3, 3) VCS:



In this algorithm, larger value of *n* doesn't depend on the quality of the decrypted secret. The only disadvantage is that the shares generated are meaningless (random or noise-like) shares.

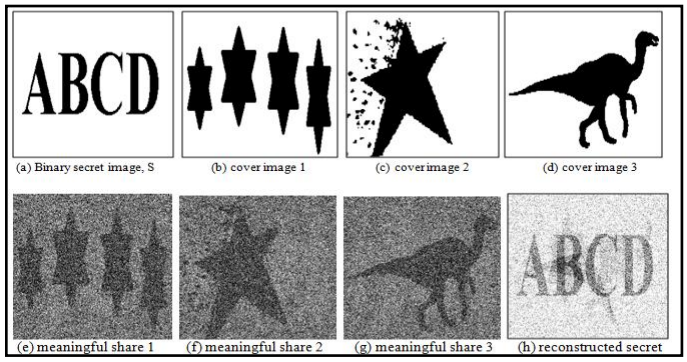
For OR-based (n, n) VCS, the contrast of the decoded secret image is of better quality. In this case as long as *n* increases, the quality of the decrypted secret will be of poor quality. The following figure shows an example of OR-based (3, 3) VCS:



The algorithm 4 generates meaningful shares with good contrast. All these shares are size invariant and the decoded secret image will be of good quality as compared to all the previous extended VCS [3], [13] and halftone VCS [5]. These schemes were having many drawbacks such as: pixel expansion problem, poor quality of the decoded secret etc. From the following two output figures, we can see that algorithm3 gives more improved result that algorithm2 when used as its initial step (step1).

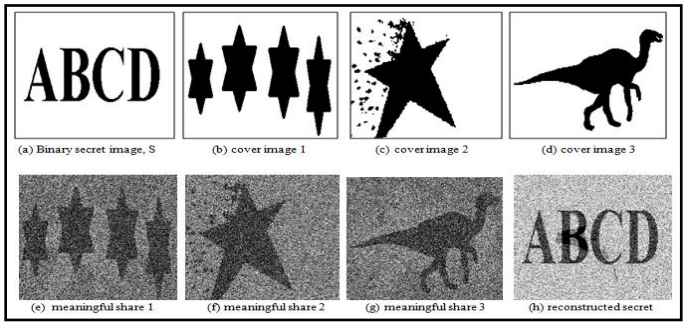
OR-based (n, n) VCS need not require any extra hardware (such as computers) to decode the secret and it can be done by simply stacking all the shares together.

The following figure shows the output of agorithm4 (using algorithm 2 in step1):



The above shares are generated using OR-based (3, 3) VCS with parameter $\alpha = 0.6$. Cover images1, 2 and 3 are the three different cover images used to make the shares meaningful with a different content. Since random grid method is used during share generation both the share images and the decoded secret image is of same size as that of the original secret. To improve the quality of the share images choose α closer to 1. But it leads to poor quality decoded secret with less contrast. Using algorithm3, exact recovery of the secret is possible but it creates only random shares which make share management difficult. So to make the shares meaningful, algorithm4 takes different cover images and takes a proportion of the cover image to replace it with random shares generated using algorithm3. The value of α must be between 0.5 and 1. For high quality of the decoded secret, choose α closer to 1 and for high quality share images, choose values closer to 0.5.When α is closer towards 0.5, the contrast of the decoded secret image increases but share images will be of less quality, and the contrast of share image become better with larger values of α.

The following figure shows the output of agorithm4 (using algorithm 3 in step1):



Comparison of the proposed scheme and some related schemes.

Scheme	Pixel expansion	Codebook design	Meaningful shares	Share scheme	Different cover image	Decryption
Multiple random grids[11]	no	no	no	(n, n)	no	OR (stacking)
Extended Visual Cryptography [13]	yes	yes	yes	GAS	yes	OR
Halftone Visual Cryptography[5]	yes	yes	yes	GAS	yes	OR (improved contrast than [13])
User-friendly [3]	no	no	yes	(2, 2)	no (yes for extension)	OR
Generalized Random Grid [16]	no	no	yes	(n, n)	no	XOR
Random-Grid based VCS [12]	no	no (yes for user-friendly)	yes	(2, 2)	yes	OR
k out of k EVCS [14]	no	no	yes	(n, n)	yes	OR
Ours	no	no	yes	(n, n)	yes	OR/XOR

V. PERFORMANCE EVALUATION

There are various parameters used to evaluate the performance of a visual cryptography scheme.

A. Pixel expansion

Pixel expansion m refers to the number of sub-pixels in the generated shares that represents a pixel of the original secret image. It represents the loss in resolution from the original secret image to the shared one.

B. Contrast

Contrast is the relative difference in weight between combined shares that come from a white pixel and a black pixel in the

original image. Contrast of the recovered secret image must be adjusted so that it is visible to the human eye.

C. Security

Security is satisfied when each share individually discloses no information of the original image and the original image cannot be reconstructed with shares fewer than n in (n, n) scheme.

D. Accuracy

Accuracy is measured to be the quality of the reconstructed secret image and evaluated by peak signal-to-noise ratio (PSNR). Mean Squared Error (MSE) can also be used for evaluating the accuracy of reconstructed image

VI. CONCLUSION

Visual cryptography offers perfect security for all the digitally transmitted secret images. It is a cryptographic technique which can encrypt visual information, such as images and text; and can decrypt the secret without a computer (stack operation). This paper discusses some visual cryptography schemes and commonly used performance evaluation parameters. Since random grid method is used, all the above schemes produce share images without pixel expansion. OR-based VCS can be decrypted without any extra hardware, whereas XOR-based VCS needs special device to do XOR operation. XOR based (n, n) VCS provide perfect reconstruction of the secret, but the shares generated are meaningless. Extended (n, n) RG based VCS were used to generate meaningful shares, by using *n* different cover images. So this paper proposes an extended VCS that have many advantages like: no pixel expansion, better contrast and meaningful shares. The proposed method can be used either with OR decryption or XOR decryption. The output of XOR-based (n, n) VCS will provide better result than OR-based (n, n) VCS.

REFERENCES

[1]. Moni Naor and Adi Shamir, "Visual cryptography". In Proceedings of Advances in Cryptology, EUROCRYPT 94, Lecture Notes in Computer Science, 1995, (950):pp. 1-12.
[2]. . G. Ateniese, C. Blundo, A. DeSantis, and D. R. Stinson, "Visual cryptography for general access structures", Proc.ICAL96, Springer, Berlin, 1996, pp.416-428.
[3]. T. Chen and K. Tsao, "User-friendly random-grid-based visual secret sharing", IEEE Trans. Circuits Syst. Video Technol., vol. 21, no. 11, pp. 1693_1703, Nov. 2011.
[4]. P. Tuyls, H. Hollmann, J. Lint, and L. Tolhuizen, "XOR-based visual cryptography schemes", Designs, Codes, Cryptography, vol. 37, no. 1, pp. 169_186, 2005.
[5]. Z. Zhou, G.R. Arce, and G. Di Crescenzo, "Halftone Visual Cryptography", *IEEE Transactions on Image Processing*, vol. 15, no. 8, pp. 2441-2451, 2006
[6]. http://bookboon.com/en/visual-cryptography-and-its-applications-ebook
[7]. R. Ito, H. Kuwakado, H. Tanaka, "Image size invariant visual cryptography", IEICETrans. Fundam. Electron. Commun. Comput. E82-A (10)(1999)2172–2177.
[8]. R.-Z. Wang, "Region incrementing visual cryptography," *IEEE Signal Process. Lett.*, vol. 16, no. 8, pp. 659–662, Aug. 2009.
[9]. S. Cimato1, R. De Prisco∗ and A. De Santis, "Probabilistic Visual Cryptography Schemes", *The Computer Journal*, December 1, 2005
[10]. Shyong Jian Shyu, "Image encryption by multiple random grids", *Pattern Recognition, 42 (2009) 1582 – 1596.*
[11]. Young-Chang Hou, Shih-Chieh Wei, and Chia-Yin Lin, "Random-Grid based Visual Cryptography Schemes", *IEEE Transactions on Circuits and Systems for Video Technology, VOL. 24, NO. 5, May 2014.*
[12]. *Teng Guo, Feng Liu, ChuanKun Wu, "k out of k extended visual cryptography by random grids", Signal Processing 94 (2014) 90–101.*
[13]. *Kai-Hui Lee and Pei-Ling Chiu, "An Extended Visual Cryptography for General Access Structures", IEEE Transactions on Information Forensics and Security, vol. 7, NO. 1, February 2012.*
[14]. *Sruthy K Joseph, Ramesh R, "Diverse Visual Cryptography Schemes: A Glimpse", International Journal of Engineering Research & Technology (IJERT), vol. 4 Issue 07, July-2015.*
[15]. *Xiaotian Wu and Wei Sun, "Generalized Random Grid and Its Applications in Visual Cryptography", IEEE Transactions On Information Forensics And Security, vol. 8, NO. 9, September 2013.*

Authors Profile

Sruthy K Joseph received **B Tech.** degree in Computer Science & Engineering from Mangalam College of Engineering, Kottayam, M.G University, Kerala, India, in 2011. Currently doing **M.Tech.** in computer science and engineering in Adi Shankara Institute of Engineering and Technology, Kalady, MG University, Kerala, India. Her research interest includes security, visual cryptography, image processing and cloud computing.

Ramesh R received **B.Tech** Degree from Mahatma Gandhi University in 2010 and **M.Tech** in computer science and engineering from M.G.University. Currently working as Assistant professor at Adi Shankara Institute of Enginerring & Technology. His research interest includes big data processing and network security.