JCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol. 9, Issue.5, May 2021 E-ISSN: 2347-2693

Mutated Random grid Approach to Share Secret Image into Visually Pleasing Shares

Jasvant Kumar[1*], Suresh Prasad Kannojia[2]

[1]Department of Computer Science and Engineering, BN College of Engineering and Technology, BKT, Sitapur Road, Lucknow, India
[2]Department of Computer Science, University of Lucknow, Lucknow, India

Corresponding Author: er.jaswantsingh786@gmail.com, Tel.: +919140738670

DOI: https://doi.org/10.26438/ijcse/v9i5.16 | Available online at: www.ijcseonline.org

Received: 06/May/2021, Accepted: 17/May/2021, Published: 31/May/2021

Abstract— Visual cryptography is a technique to diffuse and disguise a secret image into a 2D pattern of black and white pixels, called shares. Individual or any k-1 shares have no clue about the secret image, but any k shares out of n, can decode the secret image. These meaningless shares are subject to suspect for the intruders. Stacking of shares reconstructs the secret image populated with noisy pixels. In addition to these traditional visual cryptography suffer with pixel alignment problem. To resolve these problems this paper proposes a (2, 2) mutated random grid approach to share a secret image into visually pleasing shares. The solution to the problem is based on assignment of instances of random two dimensional matrix of binary numbers and its XOR operation with respective pixels with auxiliary gray image. It requires lightweight computing device to decode the secret image. Comparative analysis of the experimental results with that of existing fundamental approaches shows that proposed approach performs better.

Keywords—Visually Pleasing Shares, Mutated Random grids, XOR, Visual Secret Sharing, Light weight Computation, Pixel Expansion, Contrast-loss

I. INTRODUCTION

Visual cryptography, a visual secret sharing technique used to secure image data. It takes digital secret image as input and process it using the code-book to make n share images as output. These n share images are assigned to n members of a group of participants. Individual or any less than k members from a group of participants have no clue about input secret image. At a later time whenever required any k, $2 \leq k \leq n$ or more members of the group can reveal the secret image by stacking their share images printed on transparencies.

Unlike, traditional cryptography, visual cryptography is free from dependency on key, as secret key in a symmetric encryption or a pair of key in an asymmetric encryption. In addition to these confidentiality achieved through executing simple algorithms. Due to various advantageous features wide studies on visual cryptography and its associated properties such as its application to different type (Binary, Gray etc.) of secret images, reduction of noise pixels of the shares, multiple secret sharing, contrast improvement of the reconstructed secret image, reduction of pixel expansion etc. are conducted using the pioneer work done by Noar [1]. Constructions of visual cryptography for general access structures are given in [2,3]. Extended Visual cryptography [4,5] proposed with the objective of meaningful appearance of shares, so that users can identify and manage them easily. Halftone visual cryptography [6,7] proposed with the intention to apply visual cryptography to gray and color secret image. Bounds on optimal contrast, are proposed in [8, 9]. Probabilistic visual cryptography [10, 11, 12] and random grid visual cryptography secret sharing schemes absolve pixel expansion very well. Random grid visual secret sharing (RGVSS) is a kind of visual secret sharing techniques which do not need a code - book to encrypt the digital image and no pixel expansion in the random grids. Principle of the random grid method proposed by Kafri and Keren [13]. Random grids are created by flipping the coin for each and every pixel of the input image. When both the random grids are superimposed (OR operation), input image can be revealed by the human visual system due to differences in light transmitted by the random grids. This method is so called (2, 2) random grid visual cryptography. The Major advantage of random grid visual cryptography is that expansion free shares are generated without using implicit or explicit code-book. Application of random grid for grayscale and color images augmented by Shyu[14,15]. Shyu first converted gray scale secret image into halftone image, after that basic algorithm are adopted for the encryption purpose. Generalized random grid visual cryptography proposed in [16,17].

Chen, et al. [18] proposes (2, n) and (n, n) methods to encrypt the input image by random grids. Random grid-based visual secret sharing with OR and XOR decoding methods investigated by Wu and Sun [19]. All above discussed schemes are not user friendly because of meaningless shares. The Quality of reconstructed secret image still a major issue for the researchers. To improve the quality of reconstructed secret image XOR-based visual secret sharing investigated by Tuyls et. al.[20]. Wu, et al. [21] adopted exclusive-OR operation in random grids for creating meaningful shares. Visual secret sharing with user-friendly random grids given by Chen and Tao[22]. User friendly random grid visual secret sharing for general access structures proposed by Pang et al.[23]. Construction for progressive visual cryptography defined by S.B. Bhagate,[24]. Progressive approach for QR code in association with visual cryptography studied by Komal S. [25]. Shares produced by these random grid secret sharing schemes are populated with noisy pixels therefore subject to suspect for intruders. To void the problem of suspect by intruders, this paper proposes mutated random grid approach to share secret image into visually pleasing shares.

In this paper, Section II gives a brief review of existing approaches. The proposed approach described in Section III. Experimental results are shown in Section IV and the conclusion is made in Section V.

II. Related Work

To fulfill the intended objective of visual secret sharing three basic approaches are developed, which are deterministic, random grids and probabilistic approach, which are briefly described in the sub-sections A, B and C respectively.

A. Deterministic Approach

In this approach of visual cryptography, the secret image shared among n shares, distributed to n participant. Whenever required, secret can be exposed using any k ≤ n shares of participants.

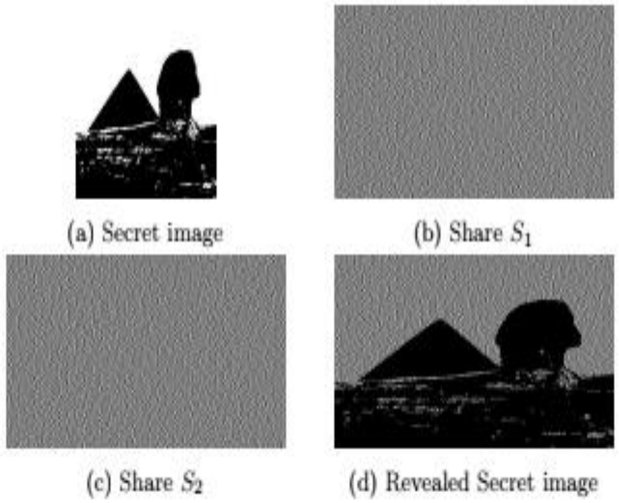


Fig. 1: Results of (2, 2) Deterministic approach (a) Secret image (b) Share S1 (c) Share S2 (d) Revealed Secret image

Here, Threshold k plays an important role, any one or any combination of k−1 shares have no clue about the secret image. For illustration, experimental results for the special case of (k, n) threshold visual cryptography where k = n = 2 are given in the Fig. 1. Here, due to pixel expansion (m=2) shares and revealed secret image are double in size to secret image. So that revealed secret image distorted in shape. It is also visible that revealed secret image populated with noise pixels. Using this approach only 50%, pixels are reconstructed correctly.

B. Random grids Approach

By default, this approach is free of pixel expansion as well as requirement of code book to encrypt the pixels of secret image.

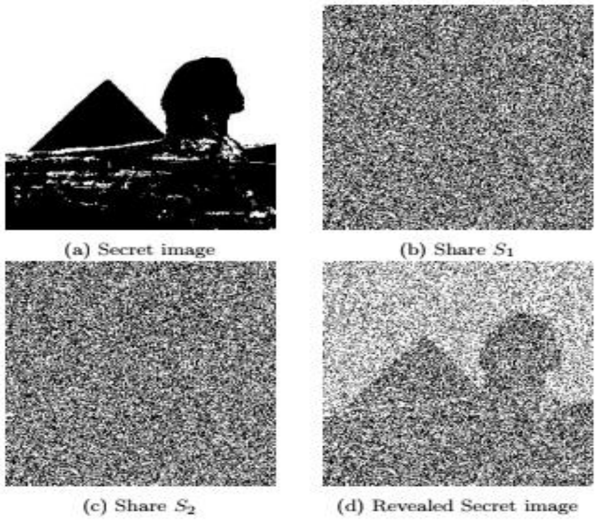


Fig. 2: Results of (2, 2) Random grids approach (a) Secret image (b) Share S1 (c) Share S2 (d) Revealed Secret image

It is first proposed and pioneered by Kafri and Keren in 1987. Using one of the three algorithms introduced in [2], a binary picture or shape is encrypted in two random grids for which experimental results are shown in Fig. 2. Here, only 25% pixels are revealed correctly.

C. Probabilistic Approach

Unlike the deterministic approach, probabilistic approach uses pixel operation instead of sub pixel operation.

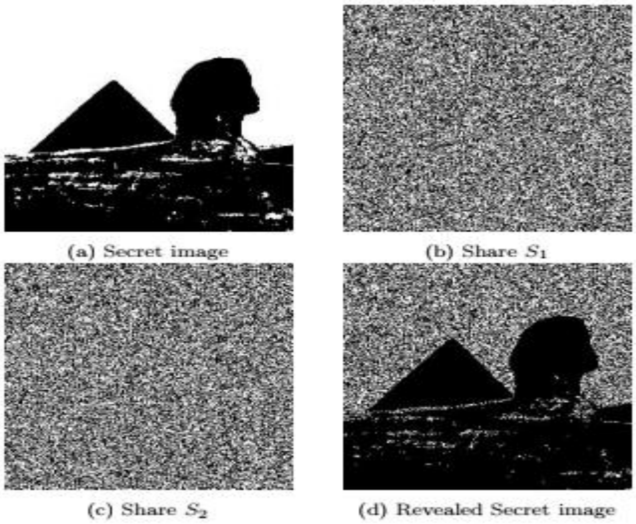


Fig. 3: Results of the (2, 2) Probabilistic approach (a) Shared secret (b) Share S1 (c) Share S2 (d) Revealed Secret image

It means probabilistic approach generates unexpanded shares and reveals a secret image of the same size as of an original secret image. Experimental results for the (2, 2) Probabilistic visual secret sharing scheme is shown in Fig. 3. Herein, it is clear that in recovered image, there are about 50% white pixels in white and 50% black pixels in the white area, and 100% black pixels in black area.

III. METHODOLOGY

The proposed approach encrypts the binary or halftone secret image with the help of auxiliary gray scale images into visually pleasing shares. Selected auxiliary gray image is used to make visually pleasing shares. Using this approach a secret sharing scheme called as 2-out-of-2 secret sharing scheme with visually pleasing shares is developed, which contributes in the literature with the following features:

- Generates visually pleasing shares
- Generates unexpanded shares
- Requires no codebook
- Reconstructs unexpanded secret image
- Reconstructs white pixels perfectly

The idea of the proposed scheme is depicted through block diagram shown in Fig 4, for which step-wise procedure is given through ALGORITHM 1, detailed description is given here. Let S is a secret image to be diffused and disguised into the shares S_1 and S_2 with the help of auxiliary grey image C. To encrypt pixel $S(i,j)$, $1 \le i \le M$, $1 \le j \le N$, of the secret image, first of all initialize the shares S_1 and S_2 with the random binary patterns of the size $M \times N$. After that, consider the colour of the pixel $S(i,j)$. If it is white(0), perform XOR-operation between the $C(i,j)$ and $S_1(i,j)$, $C(i,j)$ and $S_2(i,j)$ then assign resultant values to $S_1(i,j)$ and $S_2(i,j)$ as $S_1(i,j) \leftarrow C(i,j) \oplus S_1(i,j)$ and $S_2(i,j) \leftarrow C(i,j) \oplus S_2(i,j)$ respectively. If colour of the pixel $S(i,j)$ is black(1), choose a random number r from 1 and 2. Depending on the value of r, encryption of the pixel $S(i,j)$ is carried out as follows. If $r == 2$, swap the values of the pixels $S_1(i,j)$ and $S_2(i,j)$ after that perform XOR-operation between $C(i,j)$ and 1, $C(i,j)$ and 0 and assign values to $S_1(i,J)$ and $S_2(i,j)$ as $S_1(i,j) \leftarrow C(i,j) \oplus 1$ and $S_2(i,j) \leftarrow C(i,j) \oplus 0$ respectively. If $r == 1$, perform XOR-operation between $C(i,j)$ and 0, $C(i,j)$and 1 and assign values to $S_1(i,J)$ and $S_2(i,j)$ as $S_1(i,j) \leftarrow C(i,j) \oplus 0$ and $S_2(i,j) \leftarrow C(i,j) \oplus 1$ respectively. After encryption of every pixel of the secret image we obtain the shares S_1 and S_2. Secret image can be revealed by performing XOR operation between share S_1 and S_2.

Input: Binary or halftone secret image S and auxiliary grey scale image C

Ensure:
:
Secret image is binary or halftone image
Auxiliary image is grey scale image
Size of auxiliary image is same as that of secret image

```
Find the number of rows $M$ and columns $N$ of the secret image
$S_1 \leftarrow$ randi([0 1], M, N)
$S_2 \leftarrow$ randi([0 1], M, N)
for $i = 1$ to $M$ do
    for $j = 1$ to $N$ do
        if S(i,j)==0 then
            $S_1(i,j) \leftarrow bitxor(C(i,j)S_1(i,j))$    . bitxor is a MATLAB function to perform XOR-operation
            $S_2(i,j) \leftarrow bitxor(C(i,j)S_2(i,j))$
        end if
    end for
end for
for i=1 to M do
    for j=1 to N do
        r ← randi([1, 2])
        if r==2 then
            $S_1(i,j) \leftarrow S_2(i,j)$
            $S_2(i,j) \leftarrow S_1(i,j)$
            if S(i,j)==1 then
                $S_1(i,j) \leftarrow bitxor(C(i,j),1)$
                $S_2(i,j) \leftarrow bitxor(C(i,j),0)$
            end if
        else
            if S(i,j)==1 then
                $S_1(i,j) \leftarrow bitxor(C(i,j),0)$
                $S_2(i,j) \leftarrow bitxor(C(i,j),1)$
            end if
        end if
    end for
end for
Output: Shares $S_1$ and $S_2$
```

ALGORITHM 1: ALGORITHM FOR THE PROPOSED SCHEME

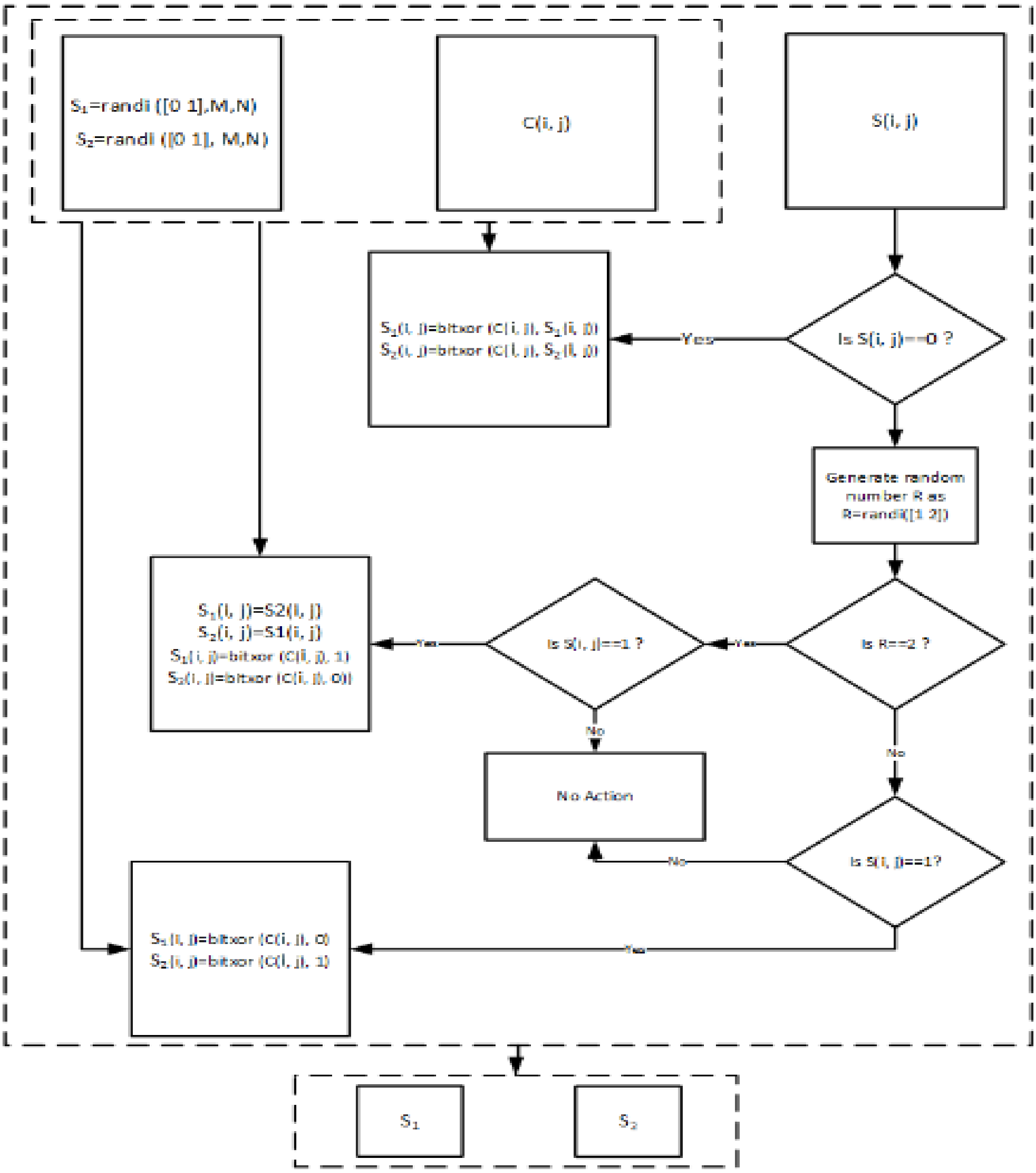

S_1=randi ([0 1],M,N)
S_2=randi ([0 1], M,N)
C(i, j)
S(i, j)
S_1(i, j)=bitxor (C(i, j), S_1(i, j))
S_2(i, j)=bitxor (C(i, j), S_2(i, j))
Yes
Is S(i, j)==0 ?
Generate random number R as R=randi([1 2])
S_1(i, j)=S2(i, j)
S_2(i, j)=S1(i, j)
S_1(i, j)=bitxor (C(i, j), 1)
S_2(i, j)=bitxor (C(i, j), 0))
Yes
Is S(i, j)==1 ?
Yes
Is R==2 ?
No
No Action
No
No
Is S(i, j)==1?
S_1(i, j)=bitxor (C(i, j), 0)
S_2(i, j)=bitxor (C(i, j), 1)
Yes
S_1
S_2

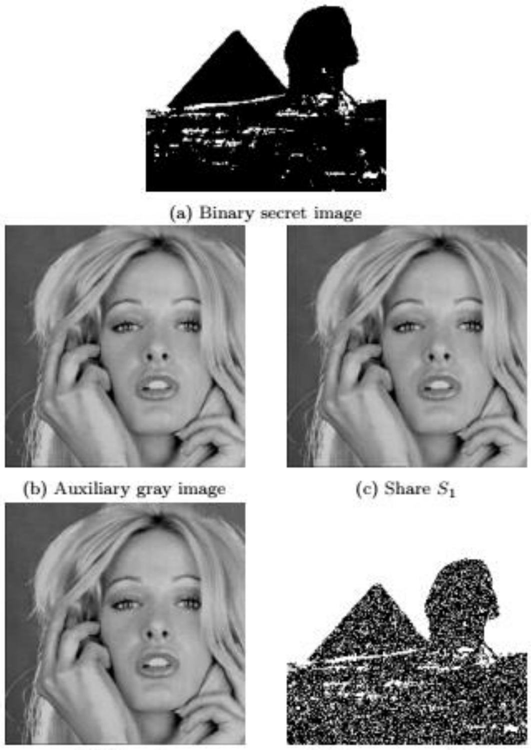
Fig. 4 Block diagram of the proposed scheme

VI. Experimental Results and Discussion

To ensure the feasibility of the proposed scheme experiment is carried out using an image processing tool provided by MATLAB, experimental results are shown in Section 4.1 followed by the performance analysis in Section 4.2.

4.1 *Feasibility*

Image INRIA.jpg from the INRIA Holidays dataset is selected as the source image. It is first converted into single bit monochrome image. This converted image is called as secret image, and is shown in Fig. 5a. Auxiliary gray scale image is shown in Fig. 5b. Fig. 5c and 2d are shares. Figure 2e is reconstructed secret image. From experimental results it is obvious that shares are similar to the auxiliary gray images and are visually pleasing and meaningful. Here it is clear that proposed scheme is feasible.



(a) Binary secret image

(b) Auxiliary gray image

(c) Share S_1

(d) Share S_2

(e) Reconstructed image

Fig. 5: Experimental results for proposed approach: (a) Secret image (b) Auxiliary gray image (c) Share *S*1 (d) Share *S*2 (e) Reconstructed secret image ($S1 \oplus S2$)

4.2 Performance analysis

To evaluate the performance of proposed scheme analysis and comparison of the experimental results with existing basic approaches is given in Table 1. Herein, **DA, RgA** and **PrA** are abbreviations for **D**eterministic **A**pproach, **R**andom **g**rid **A**pproach and **Pr**obabilistic **A**pproach respectively. Deterministic approach requires pixel expansion $m \geq 2$ to encrypt single bit pixel of the monochrome secret image. Therefore, this approach generates shares *m* times larger than the original secret image. It means deterministic approach suffers from pixel expansion. Black pixels of the revealed secret image are completely black while white pixels are partially black and white due to which revealed image explores more black pixels in comparison to the original secret image. Overall, deterministic approach reveals 50% pixels correctly. Random grids approach based on the average light transmission through individual grids. Every pixel of the random grid is either black or white with 50% probability. Therefore, average light transmission of the Random grid S_1 is denoted as

$$T(S_1) = \frac{1}{2} = 50\% \tag{1}$$

Average light transmission of random grid S_2 is denoted as

$$T(S_2) = \frac{1}{2} = 50\% \tag{2}$$

Therefore, average light transmission of superimposition of *S*1 and *S*2 is given by

$$T(S_1 \otimes S_2) = \frac{1}{4} = 25\% \tag{3}$$

Because light transmission is possible only when, corresponding pixels of both grids are white.

In probabilistic approach, frequency of white pixels in the revealed secret image plays a major role. Frequency of white pixels in black and white areas of the revealed secret image is used by the human visual system to decide the colour (black or white) in the revealed secret image. Experimental results are given to Fig. 3 show that 100% black pixels in the black area, whereas 50% black and 50% white pixels in the white area.

For the proposed approach, experimental results given in Fig. 5 show that white pixels of revealed secret image are 100% white whereas in black area pixels 50% black pixels. It generates visually pleasing shares. Overall, from Table 1 it is clear that the proposed scheme reveals 100% white pixels and 50% black pixels in addition to these, generates visually pleasing shares.

V. CONCLUSION

Table 1 Comparison with Existing Fundamental approaches

Approach	Codebook	Decoding	Secret	m	Meaningful shares	Visually pleasing shares	Revealed black pixel	Revealed white pixels
DA	No	OR	Binary	2	No	No	100%	50%
R_gA	No	OR	Binary	1	No	No	25%	25%
P_rA	No	OR	Binary	1	No	No	100%	50%
Proposed	No	XOR	Binary	1	Yes	Yes	50%	100%

Traditional visual cryptography suffers with noisy pixels as well as pixel alignment at the time of revealing the secret. The meaningless shares are subject of suspect by unauthorised users. These problems are resolved by Mutated random grid approach to share a secret image into visually pleasing shares. Proposed approach makes use of auxiliary grey image and patterns of binary pixels to make shares visually pleasing. In addition to these proposed approach is based on XOR operation which resolves the problem of pixel alignment. Comparison with the existing visual secret sharing approaches and experimental results show that, it generates unexpanded, visually pleasing shares without codebook requirement and reveals secret image with increased image quality. Therefore, the proposed approach is well suited for situations to be suspected by the intruders.

REFERENCES

[1] M., Naor, and A. Shamir, “Visual cryptography”, In Workshop on the Theory and Applicationof of Cryptographic Techniques Springer, Berlin, Heidelberg, **pp. 1-12, 1994**

[2] Ateniese G, Blundo C, De Santis A, Stinson DR,”Visual cryptography for general access structures”, Information and Computation. Vol.**129**, Issue.**2**, pp.**86-106**, **1996 Sep 15**

[3] Liu F, Wu C, Lin X., “Step construction of visual cryptography schemes”, IEEE Transactionson Information Forensics and Security, Vol.**5**, Issue.**1**, pp.**27-38, 2010**

[4] Ateniese G, Blundo C, De Santis A, Stinson DR, “Extended capabilities for visual cryptography”, Theoretical Computer Science, Vol.**250**.Issue.**1**, pp.**143-161**, **2001 Jan 6**

[5] Lee KH, Chiu PL., “An extended visual cryptography algorithm for general access structures”, ieee transactions on information forensics and security, Vol.**7**, Issue.**1**, pp.**219-229, 2012**

[6] Zhou Z, Arce GR, Di Crescenzo G., “Halftone visual cryptography. IEEE transactions onimage processing”, Vol.**15, Issue.8**, pp.**2441-2453, 2006 Aug**

[7] Wang Z, Arce GR, Di Crescenzo G., “Halftone visual cryptography via error diffusion”, IEEEtransactions on information forensics and security, Vol.**4**, Issue.**3**, pp.**383-396, 2009 Sep**

[8] Hofmeister T, Krause M, Simon HU., “Contrast-optimal k out of n secret sharing schemes invisual cryptography”,. Theoretical Computer Science, Vol.**240, Issue.2**, pp.**471-485**, **2000 Jun 17**

[9] Krause M, Simon HU., “Determining the optimal contrast for secret sharing schemes invisual cryptography”, Combinatorics, Probability and Computing, Vol.**12,** Issue.**3**, pp.**285-299**, **2003 May**

[10] Ito R, Kuwakado H, Tanaka H., “Image size invariant visual cryptography”, IEICE transactions on fundamentals of electronics, communications and computer sciences, Vol.**82**, Issue.**10**, pp.**2172-2177**, **1999 Oct 25**

[11] Cimato S, De Prisco R, De Santis A., “Probabilistic visual cryptography schemes”, TheComputer Journal, Vol.**49,** Issue..**1**, pp.**97-107**, **2005 Dec 1**

[12] Yang, Ching-Nung., “New visual secret sharing schemes using probabilistic method.” Pattern Recognition Letters, Vol.**25**, Issue.4, pp.**481-494**, **2004**

[13] Kafri, O., and Keren, E. “Encryption of pictures and shapes by random grids”, Optics letters, Vol.**12**, Issue.**6**, pp.**377-379, 1987**

[14] Shyu, S. J., “Image encryption by random grids”, *Pattern Recognition*, Vol.**40,** Issue.**3**, pp.**1014-1031**, **2007**

[15] Shyu, S. J., “Image encryption by multiple random grids”, *Pattern Recognition*, Vol.**42,** Issue.**7**, pp.**1582-1596**, **2009**

[16] Wu X, Sun W., “Generalized random grid and its applications in visual cryptography”, IEEE Transactions on Information Forensics and Security, Vol.**8**, Issue.**9**, pp.**1541-1553, 2013 Sep**

[17] Wu, X., and Sun, W., “Random grid-based visual secret sharing for general access structures with cheat-preventing ability”, *Journal of Systems and Software*, Vol.**85,** Issue.**5**, pp.**1119-1134**, **2012**

[18] Chen, T. H., and Tsao, K. H., “Visual secret sharing by random grids revisited. *Pattern Recognition*, Vol.**42,** Issue.**9**, pp.**2203-2217**, **2009**

[19] Wu, X., and Sun, W., “Random grid-based visual secret sharing with abilities of OR and XOR decryptions”, *Journal of Visual Communication and Image Representation*, Vol.**24,** Issue.**1**, pp.**48-62**, **2013**

[20] Tuyls, P., Hollmann, H. D., Van Lint, J. H., and Tolhuizen, L. M. G. M., “XOR-based visual cryptography schemes. Designs, Codes and Cryptography”, Vol.**37**, Issue.**1**, pp.**169-186, 2005**

[21] Wu X, Sun W., “Improving the visual quality of random grid-based visual secret sharing”, Signal Processing., Vol.**93**, Issue.**5**, pp.**977-995**, **2013 May 31**

[22] Wu, X., Ou, D., Dai, L., and Sun, W., “Xor-based meaningful visual secret sharing by generalized random grids”, In Proceedings of the first ACM workshop on Information hiding and multimedia security, pp. **181-190**, **2013**

[23] Pang L, Miao D, Lian C., “Userfriendly randomgridbased visual secret sharing for generalaccess structures” Security and Communication Networks, Vol.**9**, Issue.**10**, pp.**966-976**, **2016 Jul 10**

[24] S.B. Bhagate, P.J. Kulkarni, "Construction of Basis Matrices for (k, n) and Progressive Visual Cryptography Schemes", International Journal of Computer Sciences and Engineering, Vol.**06**, Special Issue.**01**, pp.**43-47**, **2018**

[25] Komal S. Patil, Suhas B. Bhagate, "*Progressive Visual Secret Sharing Scheme for QR Code Message*", International Journal of Computer Sciences and Engineering, Vol.7, Issue.6, pp.882-887, 2019.

AUTHORS PROFILE

Jasvant Kumar has received his B.Tech in Computer Science and Engineering from the Uttar Pradesh Technical University, Lucknow in 2005, after that he has completed his M.Tech in Computer has completed his M.Tech in Computer Science and Engineering from the Integral University, Lucknow in 2014. He has completed his Ph.D from the University of Lucknow, Lucknow, India with visual cryptography as an area of research. His current research interest includes image security using visual secret sharing schemes, digital watermarking and pattern recognition. Currently, He has published 7 research papers in national and international journal/conferences. He is currently working as Assistant Professor at BN College of Engineering and Technology, BKT, Sitapur Road, Lucknow.

Suresh Prasad Kannojia is working as an Assistant Professor in the Department of Computer Science, University of Lucknow, Lucknow, since 2005. He has completed his Ph.D in 2013 from the University of Lucknow, Lucknow. His current area of research interest includes pattern recognition, image security, software quality, system security/reliability, data warehousing and data mining, Soft computing. He has also organized three national conferences and one national research scholars meet. He has published 15 research papers in national and international journal/conferences.