International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-2, July 2019

Verifiable Essential Secret Image Sharing with Multiple Decryptions

Mainejar Yadav, Ranvijay

Abstract: ***We know that the essential secret image sharing (ESIS) scheme differs from traditional visual secret sharing with respect to the essentiality of the shares. In ESIS, to reconstruct the secret image, threshold number of the shares are required which includes all the essential shares. All the shares are very sensitive because it carries the secret information. Hence, reliability and authenticity of the shares before the decoding of the secret image are required which prevents a participant from intentionally or unintentionally to provide invalid shares. Proposed method is a novel verifiable essential secret image sharing (VESIS) with multiple decryption. Multiple decryption means that the decoding and verification process is done by human visual system as well as by EX-ORing the shares. Apart from this, proposed scheme also eliminates unnecessary encryption constraints of VSS like pixel expansion, explicit codebook and the number of the participants and it is also required simple computation and O(k) complexity for the decoding process.***

Index Terms: Collusion Attack, Cheating Prevention, Essential Secret Image Sharing, Random grids.

I. INTRODUCTION

In traditional Visual Secret Sharing all the shares have an equal significance, but few participants require more privileged with respect to their rank in some applications. Consequently, a few shadows or shares of participants might be more important than others. In this type of VSS, we have generated n shares of secret image which are further divided into the t essential shares and (n-t) non-essential shares. During the process of decoding, for any revelation of secret, it is mandatory to have minimum k number of shares along with at least t essential shares.

For instance, a gathering comprising of 2 officers and eight fighters does rocket propelling, which is controlled by a secret dispatch word. This secret key is encoded into ten shares and circulated among these individuals (members). As we know that the main problem is to dispatch the rocket, so the dispatchment of the rocket needs positive support of 6 individuals (i.e. k =6) having agreement of 2 officers (i.e. t=2). There is a sum of 10 individuals (i.e. n =10) including 2 essential members (t =2) and 8 non-essential members. In this manner, this situation relates to 2(6, 10)- essential VSS or essential secret image sharing (ESIS) scheme.

Revised Manuscript Received on 30 July 2019.
***** Correspondence Author
Mainejar Yadav, CSED, MNNIT ALLAHABAD, Prayagraj, India.
Ranvijay, CSED, MNNIT ALLAHABAD, Prayagraj, India.

Li et al. [7], who proposed the (t, k, n) essential SIS scheme for this type of application. In their method, where all n shares or shadows are characterized into t number of essential shadows and (n-t) number of non-essential shadows. The (t, k, n) scheme needs k shares or shadows, including t essential shares, while reconstructing the secret image or picture. The decoding strategy for this scheme depends on the Lagrange interpolations. Hence, during the reconstruction of the secret image, it requires complicated computations along with the known request of shares. Further, C-N Yang et al. [8] proposed an essential secret image sharing approach which reduced the communication cost by minimizing the share size. But different sizes of shares are the culprit of the security vulnerability. Intruder can be easily identified the important participants on the basis of different sizes of the shares. This scheme also used the Lagrange interpolations in the decoding process.

Proposed VESIS approach is a fusion of Essential Secret Image Sharing (ESIS) and Verifiable Visual Secret Sharing (VVSS) approaches with their main basic feature of secret decryption with threshold number of shares which includes all the essential shares and collusion attack prevention for shares respectively. It also eliminates some other constraints like pixel expansion, complex computation explicit codebook and restriction on the number of participants. Pixel expansion m is the number of sub-pixels required corresponding to encrypt a single secret pixel. The value of m is 1 in the proposed scheme which reduces the storage space and communication overhead. The decoding process is done by using two different (OR and XOR) operators which are very simple and having less computation cost compared to other techniques used by existing ESIS approaches like Langerage [7] Interpolation and Birkhoff Interpolation. The storage space overhead and searching overhead at sender and receiver side will increase due to the explicit codebook and the limitation of the number of the participants restrict the number of application areas of VSS. All the shares either essential or non-essential are very sensible objects because it carries the secret information, so it is a very important process to verify their authenticity before decryption of the secret.

Proposed approach eliminates all the above issues by the following features-

1. Unexpanded shares
2. No need of codebook
3. Generalized scheme like t(k,n)*, where 1<=t<=k<=n and n>=3
4. Each shares contain its own authentication information

5. Multiple decryption options are available at receiver end e.g. decryption of the secret is done by either OR operator or XOR operator.

The rest part of the paper is organized as follows- section 2 describes the proposed method. Experimental results and analysis are discussed in section 3, and conclusion is given in the section 4.

II. PROPOSED VERIFIBLE ESSENTIAL SECRET IMAGE SHARING (VESIS) APPROACH

The proposed verifiable essential secret image sharing (VESIS) has three parts, in first part, share generation has been discussed, verification of the shares is done in next part and in third part, I have discussed how to reconstruct the secret image.

A. Share Generation (Encryption process):

Encryption technique is outlined in figure 2. The detailed description of the encoding is given in Algorithm 1. Encoding process is done in two steps, in first step, five tag or labeled pictures are taken as input to generate the temporary shares which are used as input for the second step. To encode the tag images, different folding of lines is used which is shown in figure 1. The information about folding of lines has secret from participants, which ensures the secrecy of tag images. These tag images are verified at the time of share verification at receiver end, which prevents from the cheating. The input of the second step of share generation is temporary generated shares along with secret image and the output is n number of tagged shares where t number of essential and (n-t) number of non-essential shares which are distributed among the participants.

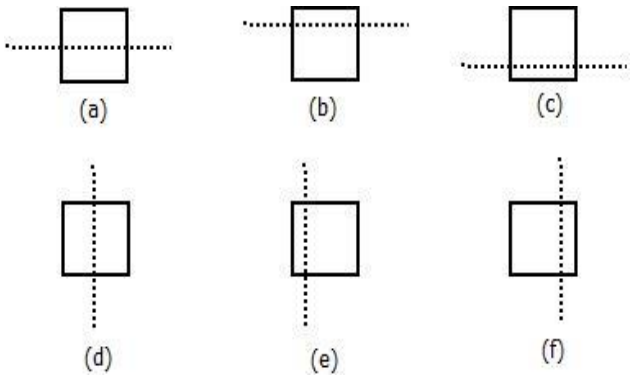

Fig. 1: Different Folding-Up Lines Used In Share Construction. (A) Horizontal Folding-Up Line In The Middle Of The Shares, (B) Horizontal Folding-Up Line In The Upper Part Of The Shares, (C) Horizontal Folding-Up Line In The Bottom Part Of The Shares, (D) Vertical Folding-Up Line In The Middle Of The Shares, (E) Vertical Folding-Up Line In The Left Part Of The Shares, (F) Vertical Folding-Up Line In The Right Part Of The Shares.

Proposed method does not consider the following cases: t=0, t=k and t=n. For t=0, it discards the essentiality aspect and t=n implies that all shares are essential shares. Therefore, for t=0 the t(k,n)* VESIS method is reduced as threshold secret image sharing (SIS) scheme. Also, proposed method does not consider the case t=k where other non-essential shares are not required for the recovery of the secret image.

Assume Q_g, E_g and NE_g indicate the group of all shares, group of essential shares and group of non-essential shares respectively, where $Q_g=E_g \cup NE_g$ and $E_g \cap NE_g=\Phi$ A qualified subset of shares P_s should satisfy two conditions-
(i) Essentiality condition: $|P_s \backslash NES| \geq t$
(ii) Threshold condition: $|P_s| \geq k$
where $P_s \backslash NES$ denotes the essential shares in qualified subset.

Example 1:
1(3, 4)* VESIS: This scheme has total four participants, where one participant (having the essential share) is essential and three participants (having the non-essential share) are non-essential. The threshold number of these participants (participants share) is three i.e. at least three shares are required for revealing the secret image which will include all the essential participants (participants share). Here, we consider share1 as essential share and share2, share3 and share4 as the non-essential shares, i.e. E_g=share1 and NE_g=share2, share3 and share4. According to this example, the qualified set (QFS) includes share123, share124 and share134 while the other combinations formed by shares 1, 2, 3, 4 belong to the forbidden set (FOS), i.e. QFS={(123), (124), (134)}. If we will use only forbidden set of shares then revelation of secret information is not possible.

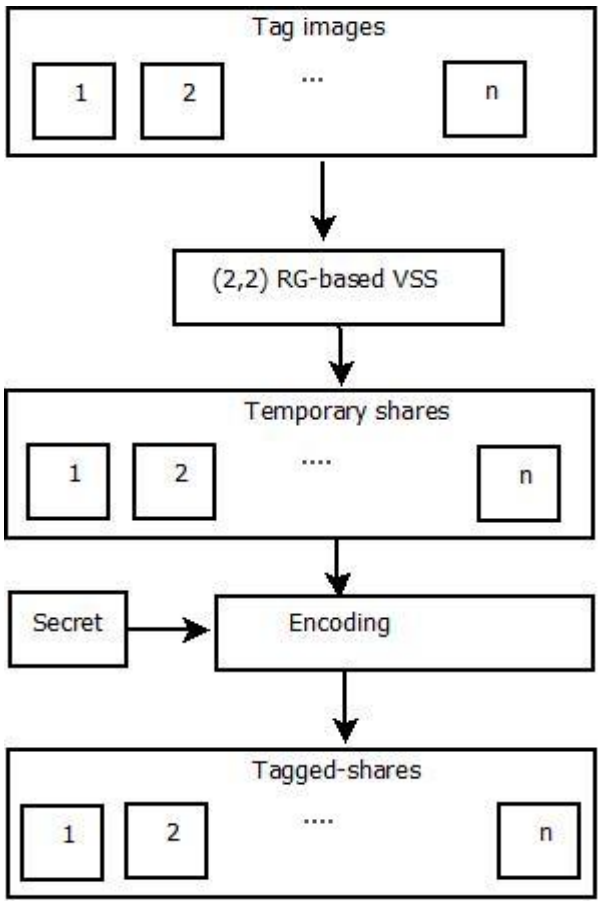

Fig. 2 Share Construction Process In The Proposed Method

B. Share Verification

At the receiver end, before reconstructing the secret image, share verification process is done, in this process each share is authenticated to reveal the embedded tag image by folding up share at correct position. If the tag image is shown correctly, it means that the produced share is genuine otherwise it is forge or tempered shares. The verification algorithm is given in algorithm 2.

Algorithm 1: Algorithm for share generation

Input: A binary secret image S with P x Q pixels and n tag images T_{g1} to T_{gn} with P x Q/2 pixels.
Output: n tagged share images R_1 to R_n with P x Q pixels
Step1: Construct n interim shares from the n tag images by
$[R_x(i,j), R_x(i,Q-j+1)]$=random grid[(2,2), $T_x(i,j)$]
where random grid method is implemented by (k, n) RG-based VC, (2,2) [17] is the desired threshold, $1 \le i \le P$, $1 \le j \le Q/2$, $1 \le x \le n$
Step2: Modify the n interim shares R_1 to R_n to form n tagged-shares by Step 3.
Step3: Suppose k, t and d_0 denote the threshold number of shares, essential number of shares and set of essential shares, respectively.

```
[P Q]=size(S);
d0= [(n+1)-1, (n+1)-2,....,(n+1)-t];
For i = 1 to P
   For j = 1 to Q
          key=randperm(n-t,k-t);
          d1=union(key,d0);
          idx = randperm(length(d1));
          d2 = d1(idx);
          temp=S(i,j);
          temp1=S(i,Q-j+1);
               For y = 1 to k-1
                   temp=xor(R(i,j,d2(y)),temp);
                   temp1=xor(R(i,Q-j+1,d2(y)),temp1);
               end
          R(i,j,d2(k))=temp;
          R(i,Q-j+1,d2(k))=temp1;
     end
end
```

Algorithm 2: Algorithm for Share Verification

Input: n tagged share images R_1 to R_n with P x Q pixels
Output: n tag images T_{g1} to T_{gn} with P x Q/2 pixels

```
Step1:    tag=zeros(P,Q/2);
Step2:    For y=1 to n      do
              For i = 1 to P    do
                   For j = 1 to Q/2    do
                        tag(i,j)=or(R(i,j,y),R(i,Q-j+1,y));
                   end
              end
         end
```

After successfully share verification, the reconstruction of the secret image is start, the decryption process given in next section.

C. Decryption process

In the decoding process, the secret image is constructed by simply stacking of the threshold number (k) of the shares which include all the essential shares, further; XORing of the shares will enhance the contrast of the reconstructed secret image. The detailed of the decryption process is shown in algorithm 3.

Algorithm 3: Algorithm for Decryption

Input: n tagged share images R_1 to R_n with P x Q pixels
Output: Reconstructed secret image S' = {S'(i,j) | S'(i,j) ϵ [0,1], $1 \le i \le P$, $1 \le j \le Q$}
Step1: select t essential shares (ES_{g1} to ES_{gt}) and randomly select (k-t) non- essential shares (NE_{g1} to $NE_{g(k-t)}$) from n tagged share images R_1 to R_n
Step2:

```
For i=1 to P      do
     For i=1 to Q      do
S'(i,j)=OR(ES_g1(i,j).....ES_gt(i,j), NE_g1(i,j).....NE_g(k-t)(i,j))
     End
End
```

III. EXPERIMENTAL RESULTS AND ANALYSIS

To check the feasibility and effectiveness, I have performed the different simulations on the different set of images. The size of the taken image in the simulation is 512 x 512. Figure 3 shows the reconstructed tag images with good visual quality which are clearly visualize and ensures the authenticity of the shares i.e. shares are genuine or not. This figure shows the original tag images and reconstructed tag images by using OR and XOR operators.

In this simulation, take a 3(4, 5)* VESIS as an example scenario. The figures 4 and 5, show the reconstructed image where OR and XOR operators are used in the decryption process respectively. In this example, 3 shares are essential and 2 shares are non-essential. Reconstruction of the secret image is possible if and only if the essentiality and threshold conditions are satisfied. On the basis of these conditions, make two sets of shares, one qualified set and another forbidden set. Only qualified set shares will be able to reconstruct the secret information. Figure 4 (a) shows the secret image, this secret image is encrypted in the random shares shown in (b) to (f) and reconstructed secret image by qualified set of shares is shown in the (n) to (p). Figure 5 (a) shows the secret image, this secret image is encoded in the random shares, shown in (b) to (f), and reconstructed secret image by qualified set of shares is shown in the (g) to (n). The simulation results show that the proposed scheme ensures the threshold and essentiality conditions.

Example 2: 3(4, 5)* VESIS scheme, it has total five participants, where three participants (having the essential share) are essential and two participants (having the non-essential share) are non-essential. The threshold number of these participants (participants share) is 4 i.e. at least four shares are required for revealing the secret image which would include all the essential participants (participants share).

Here, we have considered share1, share2 and share5 as the essential shares and share3, share4 as the non-essential shares. According to this example, the qualified set includes {(share1, share2, share3, share5), (share1, share2, share3, share5)} while the other combinations are formed by shares 1, 2, 3, 4, 5 belong to the forbidden set.

Fig. 3 (a)-(e) Original tag images, (f)-(j) recovered tag images by using OR operator, (k)-(o) recovered tag images by using XOR operator

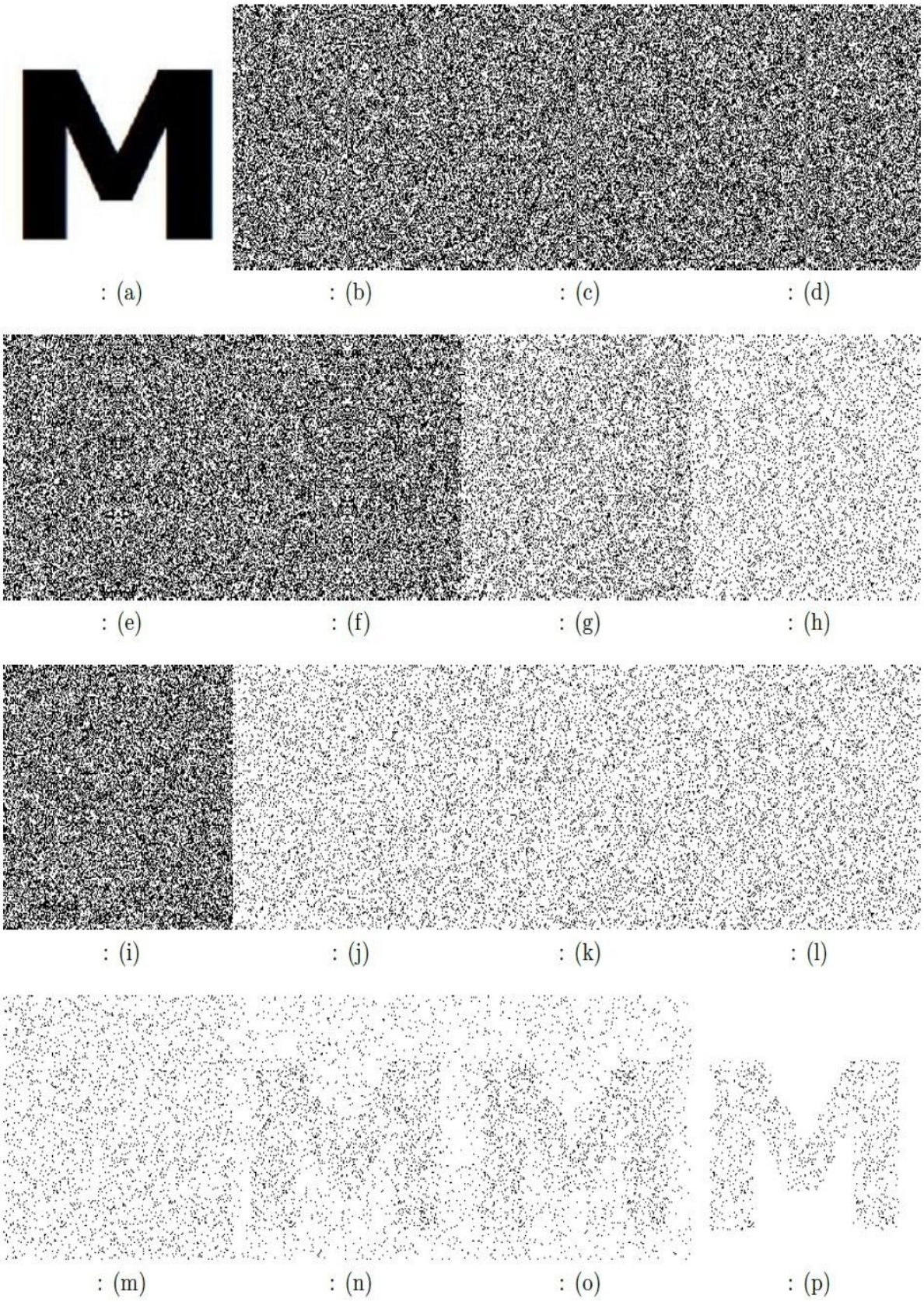

Fig. 4: An example of 3(4, 5)* VSS based on OR operator, (a) Original secret image, (b) to (f) Share1 to Share5, (g) to (m) recovered secret images by using forbidden set of shares and (n)-(p) reconstructed secret image by using qualified set of shares.

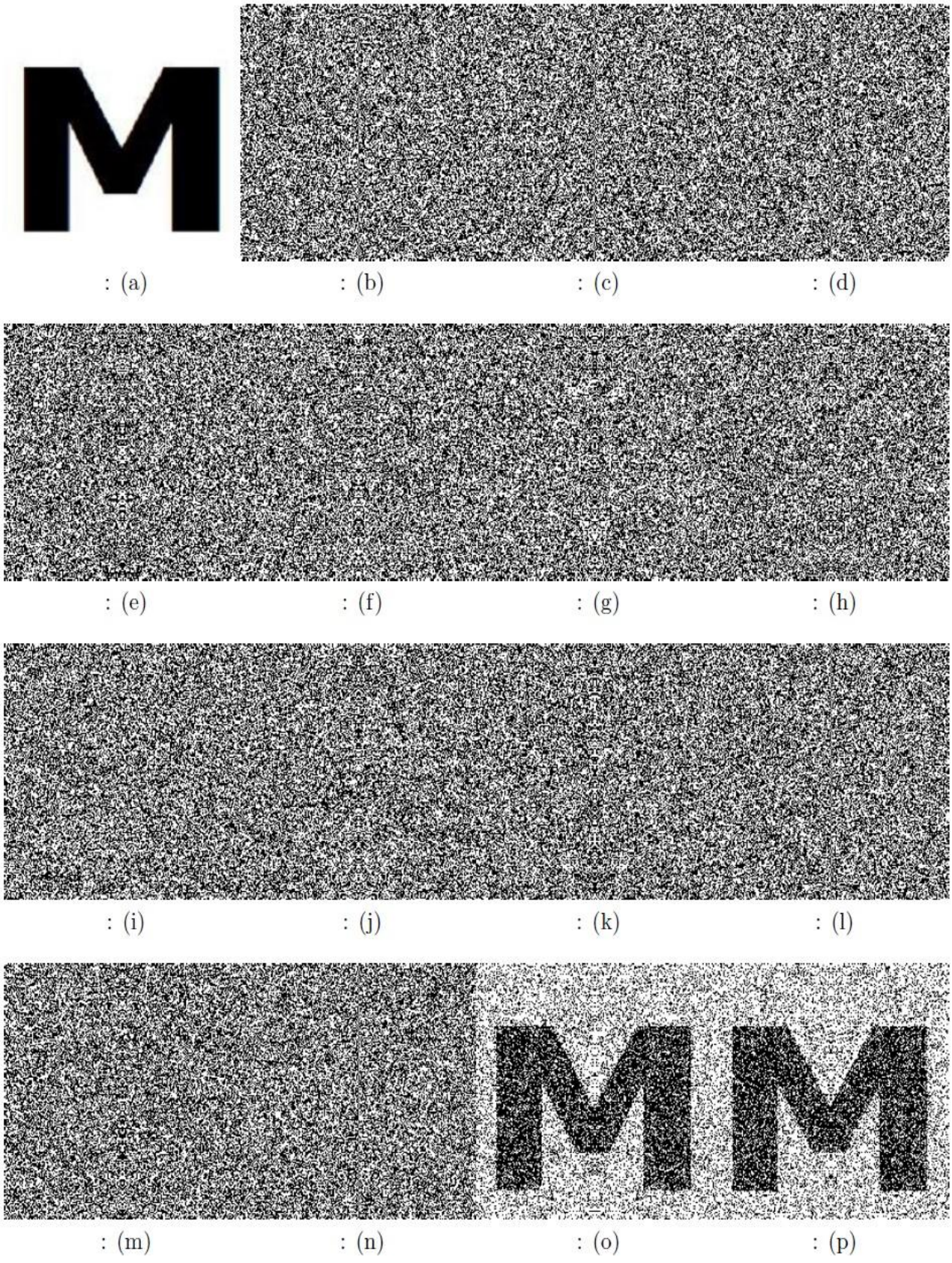

Fig. 5: An example of 3(4, 5)* VSS based on XOR operator, (a) Original secret image, (b) to (f) Share1 to Share5, (g) to (n) recovered secret images by using forbidden set of shares and (o)-(p) reconstructed secret image by using qualified set of shares.

The proposed method has the following features-

Pixel expansion and distortion free: Because the generated share and original secret image having equal size, therefore it is distortion free and pixel expansion is 1. This feature helps to protect the identity of the essential participants, which is the issue in [7] and [8].

Simple and low-cost computation: The proposed method uses OR and Exclusive-OR based operation in encoding and decoding of the secret image while other schemes use Lagrange and Birkhop Interpolation. The decoding complexity of proposed scheme is constant i.e. O(1) and O(K) with respect to the OR and XOR operators used in the decoding process.

Secure: The generated shares (Essential and Non-Essential share) have the random nature i.e. the intruder is unable to disclose any information regarding to secret image from a single share. Further, it is also validated by the correlation coefficient and also protects from the cheating activity by using the verification of shares.

Codebook: In this model, codebook is not required.

A. Visual performance:

Table I shows the experimental results of the proposed method through objective evaluation parameters. It shows the visual quality of the recovered secret image and labeled or tag images.

B. Ability of cheating prevention:

Proposed approach has cheating prevention ability. To verify this ability, by simulating an example scenario 1(3,4)* VESIS scheme has been discussed. The simulated results are shown in figure 6, where (a) shows the secret image and (b) to (e) show the tag images which are used for share verification. By using the encryption algorithm 1, we have generated the four labeled shares which are shown in (f) to (i). The corresponding recovered tag images are outlined in Figure 6 (m) to (p). Successfully recovered tag images ensure the authenticity of the shares. After verification of the shares, secret image is recovered by using decryption algorithm. The reconstructed secret image is shown in figure 6 (j), (k) and (l). Suppose 1st and 4th participants are intended to do harm and the shares exhibited in Figure 6 (f) and (i) are holed by them. According to the Y. Lee et. al. [3], the collusion cheating attack process is performed on this 1(3,4) scenario. The simulated result is shown in the figure 7 where (a) demonstrates the fake secret picture and (b) shows the created fake share.

Participant 2 and 3 are cheated by participants 1 and 4, this is done by reconstructing the fake secret image by using qualified set of shares where cheaters give the fake share in place of his/her genuine share. The reconstructed fake secret image is shown in figure 7 (c) and (d). To prevent this tricking action, the dealer must fold up the shares of qualified set prior to secret image recovery for the verification of the shares. In the verification, if the tag image is recovered successfully by the shares then the shares are genuine otherwise fake. The folded up result of the fake share is shown in Figure 7(e), which does not show the label or tag image, which means that fake share is not able to reconstruct the tag image and dealer takes the decision that this share is fake and this share should not include in the decoding process. The test result shows that the proposed strategy has the capability of cheat prevention.

C. Security Analysis:

The security of the proposed method is assessed by utilizing correlation test; Correlation test is used to know the perplexity and dissemination of the proposed method. This test has been broadly utilized as a part of image encryption [1] and SIS [4]. The correlation coefficient of each pair pixels is calculated by-

$$C_{xy} = \frac{cov(x,y)}{\sqrt{D(x)D(y)}} \quad (7)$$

where x and y are the values of two neighboring pixels in an image. Further, cov(x,y) and D(x) are calculated as follows:

$$cov(x,y) = \frac{\sum_{i=1}^{PQ}(xi-E(x))(yi-E(y))}{PQ} \quad (8)$$

$$D(x) = \frac{\sum_{i=1}^{PQ}(xi-E(x))2}{PQ} \quad (9)$$

$$E(x) = \frac{\sum_{i=1}^{PQ} xi}{PQ} \quad (10)$$

We haphazardly select 4000 pairs of pixels in the test picture, where test pictures are secret image, generated shares and reconstructed secret image by using forbidden set of shares.

Here we take an example scenario of the proposed scheme is 2(4,5)* VESIS. We calculate the correlation coefficient in four ways, between two vertically neighboring pixels (CC_V), two horizontally adjacent pixels (CC_H), two principal diagonal adjacent pixels (CC_D) and two anti-diagonal adjacent pixels (CC_{AD}).The experimental results are shown in table II, where Pixels in the generated shares (share1, share2, share3, share4 and share5) and reconstructed secret image by using forbidden set of shares are in frail correlation, i.e. the secret image can't be reconstructed by without satisfied the threshold (insufficient shares) and essentiality conditions.

Table I: Objective evaluation measures of the proposed VESIS scheme

Parameter	Standard	Secret	Tag1	Tag2	Tag3	Tag4	Tag5
BCR	1	0.59	0.90	0.56	0.46	0.36	0.60
BER	0	49	9.9	43.1	53	0.64	0.40
FM	1	0.32	0.92	0.88	0.34	0.35	0.88
NRM	0	0.50	0.09	0.43	0.53	0.64	0.40
Precision	1	0.93	0.99	0.99	0.88	0.82	0.98
RECALL	1	0.20	0.85	0.80	0.21	0.22	0.80
Specificity	1	0.85	0.96	0.32	0.72	0.49	0.40

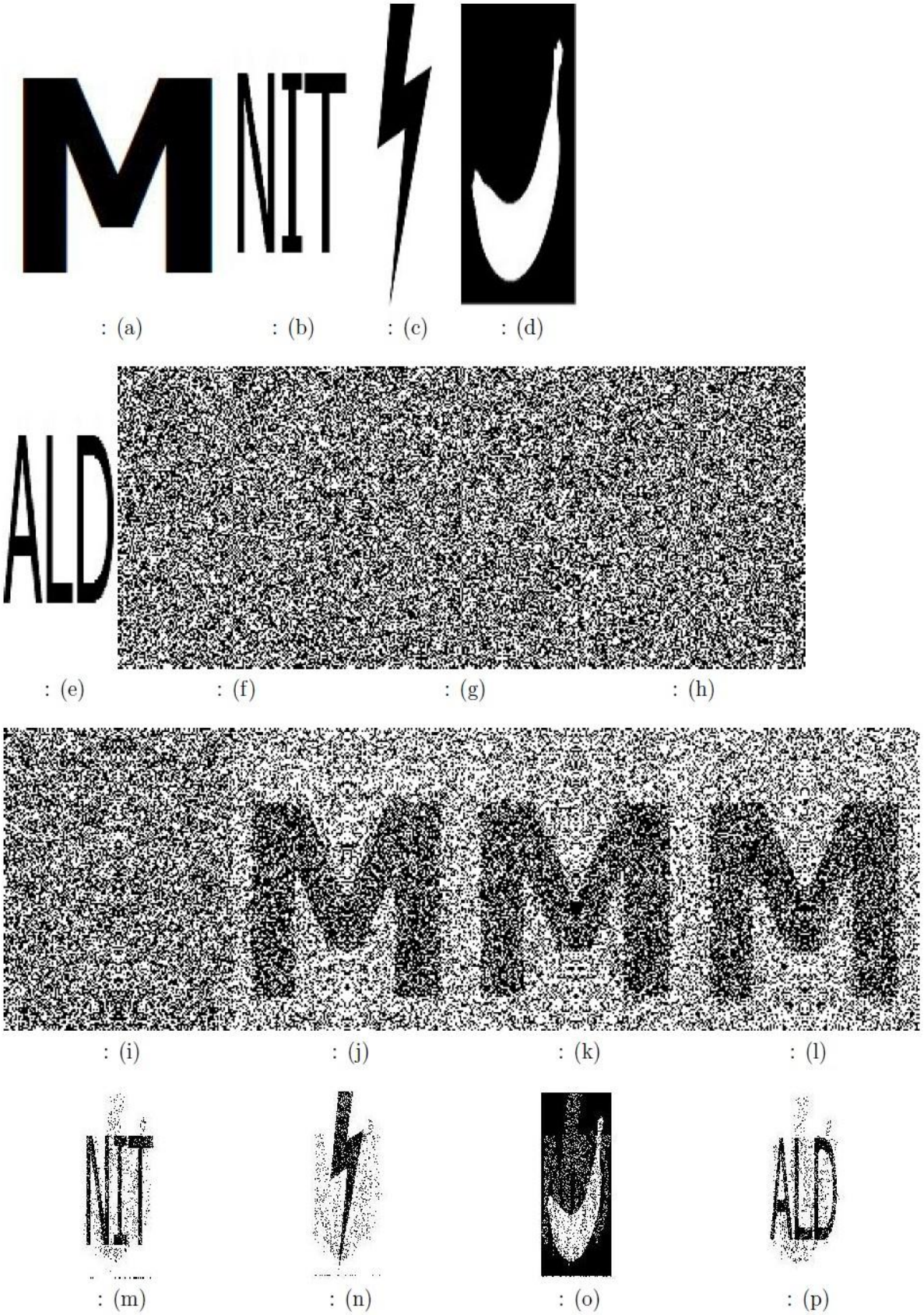

Fig. 6: An example of 1(3, 4)* VSS based on XOR operator, (a) Original secret image, (b) to (e) Original tag images, (f) to (i) Share1 to Share4, (j) to (l) recovered secret images by using qualified set of shares and (m) to (p) reconstructed tag images

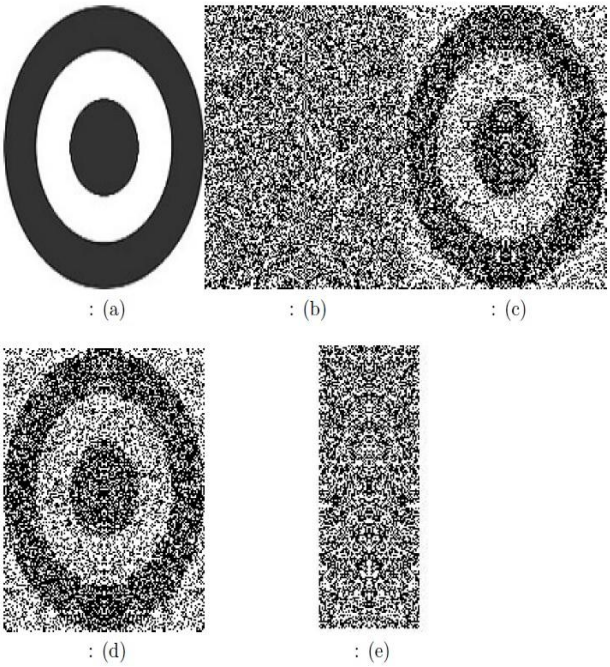

Fig. 7: The collusive cheating attack on the proposed method (a) Fake secret image, (b) Fake share, (c) and (d) XORed result by the one fake share and two genuine shares, (e) recovered tag image by fake share.

Table II: Correlation coefficients of neighboring pixels for the original secret image, shares and XOR-ed shares in the 3(4, 5)* experiment.

Images	CC_H	CC_V	CC_D	CC_{AD}
Original secret image	0.974	0.983	0.954	0.956
Share1	0.020	0.013	0.013	-0.018
Share2	-0.038	-0.003	0.025	-0.010
Share3	0.013	0.032	0.002	-0.005
Share4	0.010	-0.003	0.012	0.001
Share5	0.048	-0.024	-0.010	0.020
Share12	-0.002	-0.023	0.012	0.027
Share13	-0.017	-0.002	-0.004	0.041
Share123	0.004	0.008	-0.015	-0.014
Share124	0.036	-0.014	0.011	0.009
Share125	-0.024	-0.011	0.011	0.009
Share145	0.011	0.004	0.001	0.024
Share345	-0.010	-0.014	-0.022	0.015
Share1234	0.005	-0.011	-0.001	0.015
Share1245	-0.024	-0.031	-0.004	0.024

TABLE III. Characteristics Compared Between The Proposed Scheme And Important Literatures

Scheme Features	Thien and Lin [9]	Huang [10]	D. Ou [11]	Tsai [12]	Proposed scheme
Type of VSS	SIS	PROGRESSIVE SIS	SIS	ESIS	ESIS
Privilege of share	Equal	Equal	Equal	Different	Different
Share verification	No	No	No	No	Yes
Decryption complexity	O(2kn)	O(2kn+2n)	O(n)	$O(2k^2)$	O(k)

D. Features comparison:

Comparative analysis of the proposed strategy and existing VSS schemes have been composed in Table III. Here, the comparative analysis on the different subjective parameter has been tabulated.

IV. CONCLUSION AND FUTURE SCOPE

In this paper, we have proposed a RG-based VESIS scheme which have the capability of significant prevention of collusive cheating attack because it has the share verification facility. In the proposed scheme, algorithm for share generation is used at sender side and algorithm for share verification and reconstruction of secret image is used at receiver side. Proposed scheme eliminates basic security constraints of visual secret sharing like explicit codebook requirement, pixel expansion in the share, restriction on the number of participants and complex computation for encoding and decoding process. To reconstruct the secret image, stacking of the shares as well as by XORing the shares is done. The visual quality of the reconstructed secret image, by using the XOR operator is better than OR operator. The theoretical and experimental results have shown the effectiveness and usefulness of the proposed scheme. More enhancement of the visual quality of the recovered secret/tag image will be taken up as future research work.

REFERENCES

1. X. Liao, S. Lai, Q. Zhou, "A novel image encryption algorithm based on self adaptive Wave transmission", in: Signal Processing 90, 2010, pp. 2714--2722.
2. S. Shyu, "Image encryption by random rids", in: Pattern Recognit, 40(3), 2007, pp.1014--1031.
3. Y.Lee,T.Chen, "Insight in to collusion attacks in random-grid-based visual secret sharing", in: SignalProcess.92(3), 2012, pp. 727--736.
4. X. Wu,W.Sun, "Random grid-based visual secret sharing with abilities of OR and XOR decryptions", in: J.Vis.Commun.ImageRepre- sent., 24(1), 2013, pp. 48--62.
5. R. Wang,S.Hsu, "Tagged visual cryptography", in: IEEE Signal Process. Lett. 18(11), 2011, pp. 627--630.
6. G. Horng,T.Chen,D.-S.Tsai, "Cheating in visual cryptography", in: Design. Code. Cryptogr.38(2), 2006, pp. 219--236.
7. Li, P., Yang, C.N., Wu, C.C., Kong, Q., Ma, Y., "Essential secret image sharing scheme with different importance of shadows", in: Journal of Visual Communication and Image Representation, 24(7), 2013, pp. 1106--1114.
8. C.N. Yang, P. Li, C.C. Wu, S.R. Cai, "Reducing shadow size in essential secret image sharing by conjunctive hierarchical approach", in: Signal Process. Image Communication 31, 2015, pp. 1--9.

9. C.C. Thien, J.C. Lin, "Secret image sharing", in: Comput. Graph. 26, 2002, pp.765--770.
10. K.H. Hung , Y.J. Chang, J.C. Lin, "Progressive sharing of an image", in: Optical Engineering,Vol. 47, 2008.
11. D. Ou, W. Sun and X. Wu, "Non expansible XOR based visual cryptography scheme with meaningful shares", in: Signal Processing, 2015, pp. 604--621.
12. C.C. Chen and Y.H. Tsai, "An Expansible Essential Secret Image Sharing Structure", in: Journal of Information Hiding and Multimedia Signal Processing,Vol. 7, 2016, pp. 135--144.

AUTHORS PROFILE

Mainejar Yadav received B.Tech degree from UPTU Lucknow, M.Tech degree from MNNIT, Allahabad and presently pursuing Ph.D. from MNNIT, Allahabad. He is Assistant Professor of Computer Science and Engineering Department in RAJKIYA ENGINEERING COLLEGE Sonbhadra, Utter Pradesh. His areas of interests include Visual Cryptography, Digital Watermarking and Network Security.

Ranvijay received M.Tech and Ph.D. Degree from MNNIT Allahabad. He is Assistant Professor of Computer Science and Engineering Department in MNNIT Allahabad, Prayagraj, Utter Pradesh. His contributions in various international and national Journals. His area of interests includes Visual Cryptography, Network Security and Real time system.