IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727
PP 01-05
www.iosrjournals.org

Multiple share images using random grids and XOR-Based visual cryptography

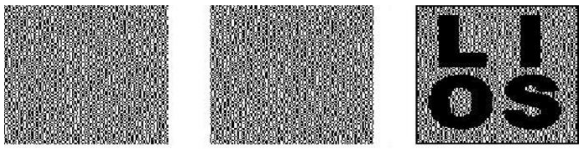
Miss A. A. Naphade, Dr.R.N.khobaragade,Dr.V.M.Thakare
naphadeanjali8@gmail.com,SGBAU,Amravati,
rnkhobragade@gmail.com,SGBAU,Amravati
vilthakare@yahoo.com ,SGBAU,Amravati

Abstract: *Visual Cryptography is a special type of secret sharing deterministic and random grid visual cryptography The XOR – based visual cryptography (VC) is a possible methodology to work out on the poor visual quality without darkening the background. This paper focus on some technique as , Extended visual cryptography scheme (EVCS) for general assess structures, RG-based visual secret scheme (VSS), Adaptive region incrementing XOR- based VC ,Compared relation in deterministic and random visual cryptography and XOR based visual cryptography. The new scheme propose for multiple share image using XOR and random grids is proposed which will encrypt and decrypt algorithm by secrete images recovered quality improvement*
Keyword: *Visual secret sharing, visual cryptography, meaningful share, XOR visual quality*

I. INTRODUCTION:

Visual cryptography (VC), which was proposed by Naor and Shamir [1] allows the encryption of secret information in the image form the concept of secret sharing, number of a secret image can be encrypted as different share images printed on transparencies. Visual cryptography is a special type of secret Sharing. Two models are independent to each other's deterministic visual cryptography and random grid visual cryptography.Visual secret sharing (VSS) secret which is also called visual cryptography (VC), is a technique of cryptography which avoids a secret from being modified or destructed by using the notions of perfect cipher and human visual system.XOR-based visual cryptography is methodology to solve the reduced visual quality problem without darken background in VC .The properties such as good resolution, high security and height contrast are managed. This methodsinvolveto confidential threshold schemes.It solves the pixel expansionproblem.The result is implementing by image secure with cover image and stacking two secure images find low contrast image recovered .

This paper, discusses methods, Extended visual cryptography scheme (EVCS) for general assess structures(GAS), Meaningful visual secrete sharing (VSS), Adaptive region incrementing XOR- based , VC , XOR based visual cryptography (XVCS) Compared relation in deterministic and random visual cryptography improving method XOR –based extended visual cryptography moreover superior visual quality.



(a) (b) (c)

fig :Traditional VSC.

II. BACKGROUND:

The study visual cryptography scheme (VCS) is an encryption method that operate the human visual system in recovered a secret image.extended visual cryptography scheme (EVCS) for GAS and this method approach the a two-phased encryption algorithm contained two stage intermediate shares meaningless appearance and no pixel expansion second stage cover images. presentation of the plannedoptimization model by comparing with the previous VC outcome for GASs. [1]

Meaningful visual secrete sharing (VSS) , the method improving in contrast of images.RG-based VSS scheme without pixel expansion, But recovered secret image with low visual quality expose due to the stacking process. The noise-like look further raise the chance of doubt on secret image communication moreover impose complexity for managing the shares.[2]XOR –based Visual Cryptography (XVCS) this scheme is more efficient than OR –based schemes .there drawbacks is the more complexity in this techniques [3].

adaptive region incrementing XOR- based VC that implement approach compared relation in deterministic and random visual cryptography XOR based visual cryptography which uses XOR operation for decoding, enhance the contrast.It capable of easily decode the secret image by stacking operation, or we may select the complex operation (XOR) to enhance the contrast of reconstructed image. [4] Compared relation in deterministic and random visual cryptography that research approach compares in two cryptography techniques . Strong relation between two models . This able to improve several schemes and provide many upper bounds for the random grid model .[5]

Section I Introduction. **Section II** discusses Background. **Section III** discusses previous work. **Section IV** discusses existing methodologies. **Section V** discusses attributes and parameters and how these are affected on images. **Section VI** proposed method and outcome result possible. Finally **section VII**Conclusion of this paper.

III. PREVIOUS WORK DONE:

In research literature , it improving security and decreasing pixel expansion efficiency increasing to covered images[1][2][3][4][5]. In this recent methods,extended visual cryptography (EVCS) which adds the meaningful cover images in each shares . Itsolves the problem dealer identify each shares.[1] .The pixel expansion problem is most common the VSS schemes. A novel encryption algorithm of EVCS for GAS to handle with the pixel expansion problem. that method is related to binary secrete and covered image Without computational device during decryption phase.[2] The encryption process can be divided into two phases. The first stage is algorithm for optimization techniques for a specified access structure, constructs like as noise-like shares and pixel-expansion-free and second stage added cover image using stamping algorithm.[3]RG-based VSSis a new branch of VSS system thatbetter visual qualitythan adoptingXOR operation to decryptthe secret. Worthless appearance of the share some increasesthe chance of doubt on secret communication and impose impenetrability for organization the shares.A (*n; n*) XOR-based VSS is constructedAlgorithm. . Generalized RG-based VSS for (*n; n*) case.Input area binary secret image *S* with $M \times N$ pixels, images get outputs a *N*shares *R*1*; ・ ・ ・;Rn*.] [4].

Close relation between the random grid model and the deterministic model. Improve many upper bounds for the random grid model the other cases gap between the contrast of known schemes and the upper bound.XOR –based VSS , new XVCS. Our main input is to prove the basis matrices in (*k, n*)-OVCS also convince the contrast and security conditions of (*k, n*)-XVCS. Meantime, the contrast is $2(k-1)$ times enhanced by XOR operation.This method exploits the capabilities for xor based vc. [5] Two XOR based VC algorithm ,namely XOR based VCis complexion strategy and adaptive region incrementing XOR-based VC it designing flexible sharing strategy become feasible.

IV. EXISTING METHODOLOGIES:

Extended visual cryptography (EVCS) which adds the meaningful cover images in each shares . There are different methodologies that are implemented for extended visual cryptography i.eextended visual cryptography scheme (EVCS) for general assess structures, Meaningful visual secrete sharing (vss), adaptive region incrementing XOR- based vccompared relation in deterministic and random visual cryptography and XOR based visual cryptography.

Extended visual cryptography scheme (EVCS) for general assess structures:

method is related to binary secrete and covered image Without computational device during decryption phase. The encryption process can be divided into two phases. The first stage is algorithm for optimization techniques for a specified access structure, constructs like as noise-like shares pixel-expansion-free and second stage added cover image using stamping algorithm

Meaningful VSS:

where the average light transmission of a share becomes adjustable. Further, a (*n; n*) XOR-based meaningful VSS are derived, wheremeaningfulshares are generated .it transmission the black and white transmission.

Compared relation in deterministic and random visual cryptography: There is a close relation between the random grid model and the deterministic model. The secret image consists of black and white1 pixels .m is apixel expansion parameter each pixel of the secret image is expanded into *m* pixels .

XOR –based VCS (XVCS) : The stacking operation in VCS is OR operation .the origin matrices in (*k, n*)-OVCS also convince the contrast and security conditions of (*k, n*)-XVCS easily decode the secret image by stacking operation . A close relation between the random grid model and The stacking operation in VCS is OR operation adactive region incrementing in XOR operation.

Adaptive region incrementing XOR- based vc: The two methods an OVCS is also a XVCS and vice versa the contrast of XVCS is 2(*k*-1) images greater than OVCS can easily decode the secret image by stacking operation, or we may choose the complex operation (XOR) to enhance the contrast of reconstructed image

V. ANALYSIS AND DISCUSSION

The performance of the proposed encryption algorithm for EVCS in terms of the contras recovered secret images. Contrast values are upper bound of the recovered image. VC schemes can be customized into form their extended VC schemes without redesigning codebooks.It shown that deterministic and random grid visual cryptography are strictly related. As a consequence many results known for the deterministic model can be used in the random grid model and viceversa. The other cases there is still a gap between the contrast of known schemes and the upper bound. For the case of $k = 2$, the schemes match the upper bound only for $n = 2$, 3. To improve several schemes and to provide many upper bounds for the random grid model and by exploiting some results known for the random grid model.XOR-based meaningful VSS is derived by synthesizing two (*n;n*) generalized RG-based VSS schemes with different values of *u*,*v*. Shares with meaningful contents are constructed, and superior visual quality of both the share and recovered secret image is obtained by the proposed method. OVCS is also a XVCS and vice versa the contrast of XVCS is 2(*k*-1) images greater than OVCS can easily decode the secret image by stacking operation, or we may choose the complex operation (XOR) to enhance the contrast of reconstructed image.

The concept of adaptive security level is reconstructed in accordance with qualified set instead of the quantity of stacked shares .the adaptive region incrementing XOR –based VC .designing flexible sharing strategy becomes Feasible. Pixel explanation problem is solved.

	Methods				
Attributes	EVCS for GAS	Meaningful visual secrete sharing	adaptive region XOR- based vc	RG-based (vss)	XOR based visual cryptography
Pixel expansion	NO	yes	no	no	yes
Code book expansion	Yes	no	no	no	yes
Decryption	XOR	stack	XOR	stack	XOR
Perfect recovered	yes	yes	yes	no	no
Type of VC	()K,n	(k,n)	GAS	(k,n)	(k,n)

Advantage and disadvantage of the methods are

Methods	Advantage	Disadvantage
EVCS for GAS	to design a sophisticated codebook	addresses the pixel problem
Meaningful visual secrete sharing	superior visual quality	recovered secret image with low visual quality reveals
Adaptive region XOR-based VC.	security and pixel nonexpanding	It is use only black and white image
XOR Based visual cryptography	Enhance the contrast**.**	tediously increasing property of the threshold condition.

VI. PRAPOSED METHOD:

The proposed scheme makes use of the encryption strategy using Random grid multiple, visual image secrete sharing (VSS) shame using XOR –based. It is better than OR based scheme . In the images forming in clusters and cluster are converting in the small pixel , Whereas two consecutive pixels frothe same secret image form a block the proposed method builds the pixel block via allowing for pixels from more than one secret. It proposed method in two phases secret image sharing and recover the secret images. Grid computing using in scheme for providing security and Cipher grid functions using for key added function and using to mod function for calclulation.$\oplus$ is the bit-wise XOR operation and R israndam.

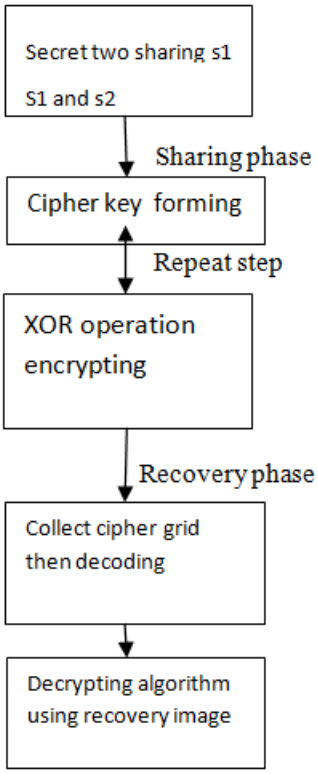
Given two secret images S1 and S2, size is 256 ×256 the pixel blocks are constructed by fetching pixel P1 from the first secret image S1 and pixel P2 from another secret image S2. Note that the pixels are accessed from the same position. i.e P1 = S1 (I , j) and P2 =S2 (I , j). I1 and I2 are intermediate image.

- *Sharing phase:*

Step1: Given two secrets S1 and S2, each of size
M × N,Where, P1 and P2 are pixel of secret image S1 and S2 , P1 = S1(I , j) and P2 = S2(I , j).
Construct i^{th}, pixel block P (i) = $\begin{bmatrix} p1 \\ p2 \end{bmatrix}$
Step 2: The first layer of encryption using random grid will encode the block P(i) into the cipher block C(i) as
C (I , 1) = (K11P1 + K12 P2) mod 256,
C (I , 2) = (K21P1 + K22 P2) mod 256.
Step 3: Repeat step-2 for all successive blocks and construct the intermediate shares I1 and I2,
where , I1 (i) = C (i, 1) and I 2 (i) = C(i , 2).
Step 4: Generate a random grid R of the same size as that of S1 and S2.
Step 5: A second layer of encryption is performed through the random grid using XOR operation as follows:
E 1 (i) = I1 (i) ⊕R(i)
E2 (i) = I2 (i)⊕R (i)
Step 6: Distribute E1 and E2 as the share images.

- *Recovery images phase:*

Step 7: Collect the cipher grids E1 and E2.
1. Collect the cipher grids E1 and E2.
2. Apply random grid process again on E1 and E2 to obtain the intermediate images I1 and I2 .
I (i) = E1(i) ⊕ R(i)
I2 (i) = E2(i) ⊕R(i)
Step 8: Further, Hill cipher decryption is carried out on the pixel block constructed from I1 and I2 to obtain the i pixel block P (i).
Step 9: Restore the pixels from each block from the corresponding positions in S1 and S2.Then recovered the image.
The figare showing the implementation of the .XOR –based using random grid .It providing the more security .



Implementing the propose technique in nine steps, it recovered enhance image with reduce transition risk.

VII. OUTCOME POSSIBLE RESULT

The results of the proposed algorithm is implemented on the gray scale images of size 256 ×256 .n-Secret Sharing algorithm. The original secretsimage S1and S2. Hill cipher encrypts S1 and S2 into intermediate

images I1 and I2 After applying a second layer of encryption using XOR, the images I1 and I2 turn into final shares E1 and E2. During recovery, first theprofile of the secrets is obtained through XOR. Further, Hill encryption with inverse of key recovers both secrets S1 and S2. The profile of the secret images after hill encryption gives less clue of the original secrets and retrieved secrets using XOR operation.

VIII. CONCLUSION

Paper suggests a method formulti-secret sharing using XOR –BASED and random grids. Securitiesflaws observed in the method proposed in have been eliminated in the case of multiple secrets. Given secrets were encrypted into cipher and then the random grid in the second layer provides additional security. It is observed that security is improved recovery when multiple images are encrypted using Hill cipher as the cipher grids do not reveal any information about the original secrets. It recover image without darkening background and lossless data with more security.

IX. FUTURE SCOP:

From Observation, the scope and planned to be studied in future work, the propose method are more suitable for implementing in visual cryptography is more efficient and provided the more security. It provided security the multiple images in GAS.

REFERANCES

[1]. Kai-Hui Lee and Pei-Ling Chiu, "An Extended Visual Cryptography Algorithm for General Access Structures" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 1, FEBRUARY 2012.

[2]. Xiaotian Wu and DuanhaoOu "XOR-Based Meaningful Visual Secret Sharing Generalized Random Grids," ACM 978-1-4503-2081-8/13/06 .

[3]. Ching-Nung Yang,and Dao-Shun Wang "Property Analysis of XOR-Based VisualCryptography" IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 24, NO. 2, FEBRUARY 2014

[4]. Xiaotian Wu and Wai sun "Extended Capabalities for XOR-Based Visual cryptography" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 10,0CTOBER 2014

[5]. Roberto De Prisco and Alfredo De Santis "On the Relation of Random Grid and Deterministic Visual Cryptography" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 4, APRIL 2014