ISSN: 0975-766X
CODEN: IJPTFI
Available Online through *Research Article*
www.ijptonline.com

GENERATING VISUAL CRYPTOGRAPHIC SHARES BY SEGMENTATION TECHNIQUE

Kaushik Roy*, MCA Scholar, Brindha K, Assistant Prof.(Sr.)
SITE, VIT University, Chennai.
Email: kroy.compsc@gmail.com

Received on: 20-07-2017 *Accepted on: 25-08-2017*

A. Abstract

In past recent years, the concern of storing personal information in computer system has been increased a lot and at the same time the security issue also has become more important than previous. Visual cryptography is one of mostly used cryptographic model for encrypting the biometric information, like-finger print, retina image etc. Visual cryptography segment the information or secret image into one or more number of shares and one time secured digital transmission is done through it, whereas the original image is reusable. The goal of this paper is to discuss the exiting visual cryptographic models, their comparative comparison with respect to various parameters.

Keywords: Visual Cryptography, Single secret Shares, Multiple secret shares.

B. Introduction

Visual cryptography is a method where we hide the information into more than one images by segmenting them in such a way that the information can be retrieved again with human visual system, without help of any mathematical computation. In this technique we segment the original image into n modified images (known as shares) such that every pixel would have n black and white subdivided sub-pixels.[1] Basically in a simplest method if there are two shares, one contains random pixels selected and other one contains the secret data. Again, when these two shares are super imposed then it shows the information that washidden in one of those two. Now how the first share chooses the random noisy pixel that depends on sub mathematical interpretation. That means selection of random sub-pixels from a block of pixels is not actually random. The generated pattern is a random one but the selection process should be in a manner such that the human visual system can identify the changes over the plain when the two shares are super imposed. The best and advantageous part in this that the individual shares do not have the information retrieval effectiveness because of their

random pixel selection pattern. One can easily get the information if he had the all shares, even it does not matter whether he is aware of cryptography or not and at the same time not required of mathematical computation to get that. The visual cryptography plan is utilized for encrypting the data. Visual cryptography is a strategy's one of encryption which is utilized to shroud the data in a picture; decryption should be possible by human visual framework. By utilizing just this sort of cryptography, nobody is capable reuse the information. The picture which we can recoup after decryption won't be same as unique picture so it can't be reused. There are number of visual cryptography plans in presence. Some of them are portrayed underneath:

1. Binary Image
2. Gray Images
3. Color Images

C. Literature Review

C.1.Binary Image:

This type of image has only two type of pixels-black and white, typically they are represented by 0 and 1 respectively in a digital computer system.

C.1.1. Single Secret Sharing Image:

The simplest type of visual cryptography where the secret image is divided into exactly two halves or shares. This idea was introduced by Naor and Shamir [2] where from a binary Image P, one pixel p is segmented into two shares, called S1 and S2 (Table 1)[8].Now if the pixel p is white then it chooses any one of the first two rows randomly and again if it is black it chooses any one of last two rows randomly to encrypt the S1 and S2. That means mathematically there is possibility to occur any one of those encoding scheme whether the p is black or white. Now when the S1 and S2 are stacked together again we get black if p was black or we get one half black other half white when the p was white (Right most column of Table1). Our visual system recognizes the black and white pixels in this manner when they are stacked upon one another.

In most of the real life cases to keep the aspect ratio of a pixel p, it is segmented into 4(2X2) sub-pixels (Table 2)[8]. In that cases for every pixel p, there is six possibilities from which system can choose any one of them randomly. When the pixel p is white, it chooses any one of the first six rows and if p is black than anyone of the last six rows. So when the S1

and S2 shares are stacked upon one another, the resultant image would be black if p was black and two of the sub-pixels are white and other two are black when the p was white.

To shroud a binary image into two meaningful shares Chin-Chen Chang et al [3] recommended spatial-domain image hiding plans. These two secret shares are inserted into two gray level spread images. To unravel the hidden messages, embedding images can be superimposed. Balancing the performance between pixel expansion and contrast Liguo Fang [4] recommend a (2, n) plan based on combination. Limit visual secret sharing plans blended XOR and OR operation with reversing and based on binary linear blunder correcting code was proposed by Xiao-Qing and Tan [5].

The problem with this technique is that at a time we could hide only one secret message within two shares. That means if we want to hide a large message we have to use a huge number of shares.

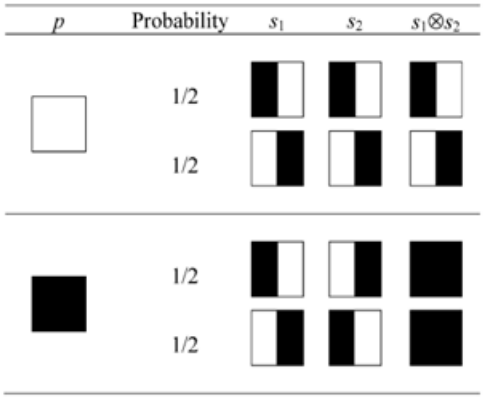

Table 1: Binary pixel p into two shares s1 and s2

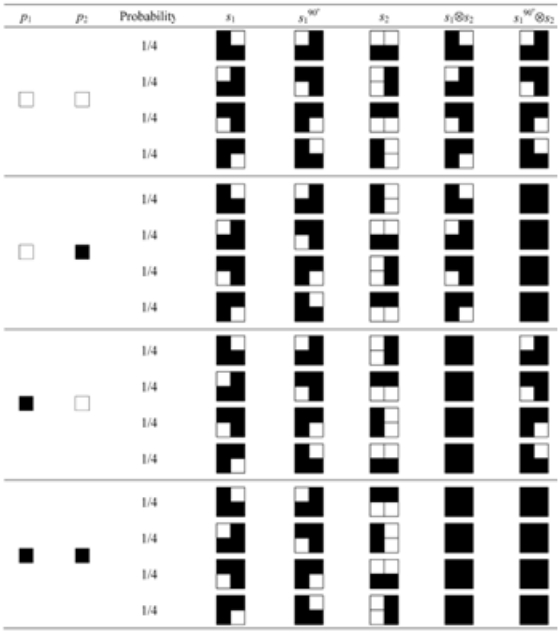

Table 3: Wu and Chen's visual cryptographic model with two-secret

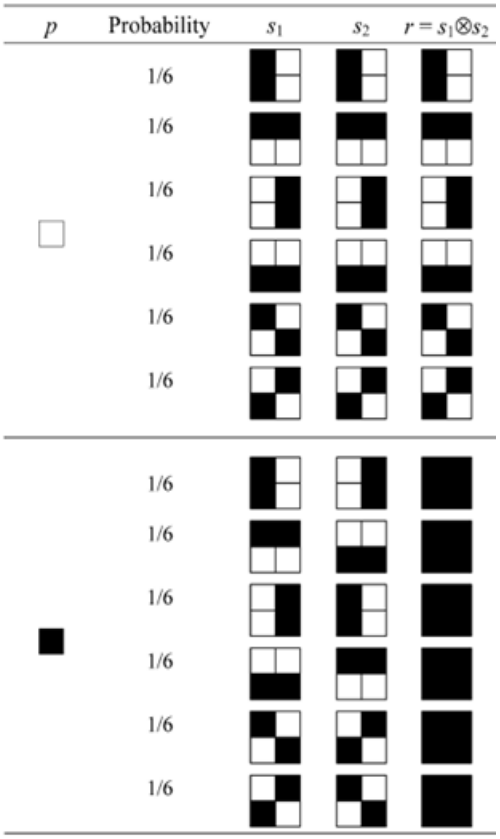

Table 2: Binary pixel p expansion of 4 into s1 and s2

C.1.2.Multiple Secret Sharing Image:

Wu and Chen [6] were first specialists to introduce the visual cryptography plans to share two secret pictures in two shares. He concealed two secret parallel pictures into two random shares, that is A and B, such that the first secret can be seen by stacking the two shares, indicated by A⊗ B, and the second secret can be acquired by first pivoting A Θ against clockwise. They outlined the pivot point Θ to be 90◦. On the other hand, it is anything but difficult to acquire that Θ can be 180◦ or 270◦. To beat the point limitation of Wu and Chen's plan [6].Wu and Chang [7] likewise refined the thought of Wu and Chen [6] by encoding shares to be circles so that the confinements to the pivoting edges (Θ = 90◦, 180◦ or 270◦).

If there is a NXN two images, called P1 and P2, which are segmented into two shares S1 and S2 and stacking together S1 and S2 reveals P1 where as to get the P2 we have to stack $S1^{90^o}$and S2. The only restriction is that the size of P1 and P2 should be same. A pair of pixels p1 and p2 from P1 and P2 images respectively are called *corresponding pixels*[6] when p1*(i,j)* and p2*(u,v)* position in the respective images are exactly same row-wise*(i=u)* as well as column-wise*(j=v).*In Table3 for each pair of corresponding pixels, p1 and p2 they are represented in sub-pixels extended block of S1 and S2 ; at the same time $S1^{90^o}$is the counter clockwise rotation of S1 with 90º.

For an example assume two images P1 and P2 with 12X12 pixels and their shares S1 and S2 would have 48X48 sub-pixels (12X4).They first decay S1 into four triangle-like territories with an equivalent size as appeared inFig. 1(a)[6][8]. The greater part of the four zones are made out of an equivalent measure of augmented squares (2 × 2 pixels each) which are filed as appeared in Fig. 1(b) where every triangle-like zone contains 36 pieces. Let piece j in region k be indicated as b^k_j for 1≤k≤4 and 1≤j ≤36. The developed pieces in range I, b^1_j, are arbitrarily chosen out of those in Fig. 1(c). Every piece, say b^t_j , in zone II, III, IV is allotted to be the same as b^1_j in territory I, that is,b^t_j= b^1_j for t = 2, 3, 4 and 1≤j ≤36.

Give us a chance to pay consideration on the four pixels at the upper right, topleft,base left and base right corners in arrangement (counterclockwise)in P1 and P2. Accept that those pixels in P1 (P2) are □, □, ■, ■ (□, ■, □, ■) as appeared in Fig. 2(a) (Fig. 2(b)). Expect that relating piece b^1_{26} at S1 is arbitrarily decided as▟, then as specified b^t_{26} is ▟ for 2≤t≤4 (see Fig. 2(c)). The aforementioned pixels in P1 and P2 constitute four arrangements of relating pixels: (□, □), (□, ■), (■, □) and (■, ■). Since b^k_{26} in S1 is for 1≤k≤4, as per Table3 the four pieces b^1_{26}, b^2_{26}, b^3_{26} and b^4_{26}, in S2 concerning the four arrangements of the comparing pixels are▟, ▙, ▜ and▛, individually (see the second, sixth, tenth and

fourteenth lines in section s2 of Table 3). Fig. 2(d) outlines the encoding consequence of S2. As expected, the four corners in the aforementioned request in S1⊗S2 uncover □, □, ■, ■ separately (see Fig. 2(e)) to our visual framework. At the point when S1 is turned as $S_1^{90^o}$ as showed in Fig. 2(f), where all squares are as $S_1^{90^o}$, the four relating corners in $S_1^{90^\circ}$ ⊗S2 recoup □, ■, □, ■ separately (see Fig.3(g)). It is not difficult to observe that by encoding all pixels in S1 furthermore, S2 as for the relating pixels in P1 and P2 as indicated by Table 3, P1 and P2 can be recouped by S1 ⊗ S2 furthermore, $S_1^{90^\circ}$⊗S2.

S.J. Shyu, S.Y. Hunang, Y.K. Lee,R. Wang and Kun Chen [8] proposed to hide multiple secret messages in visual cryptography with only two shares. According to them there are three secret pictures to be shared i.e. x = 3. So we have P1, P2 and P3 the three binary secret images with the same size u×v. Now p1, p2 and p3 are the corresponding pixels in P1, P2 and P3, individually. Let A and and B are the two circular shares to complete this visual cryptography. Their goal was to reveal P1 on A ⊗ B , then P2 on A^{120° ⊗ B and then P3 on A^{240° ⊗ B. As there were three secrets, the circular shares A and B decomposed into three (x = 3) *chord-areas*[8]. A circle have 360º as a whole, and if we want to segment it three chord areas each of them would have 120º (360º/3). Using this geometrical interpretation they hid three secret messages with every rotational angle of 120º. They again segmented each chord area into an arrangement of 2 ×3 (2 ×x) chord pieces. Let the number of 2 ×3 blocks in every chord area be β. Let a^k_j and b^k_j indicate region j of chord k in A and B, separately, $1 \le j \le \beta$ and $1 \le k \le 3$ (=x). The chords are ordered clockwise and the partitioned obstructs in A and B are ordered as appeared in Figs. 3(a) and (b), respectively. It can be considered as a^k_j and b^k_j are corresponding blocks in A and B.

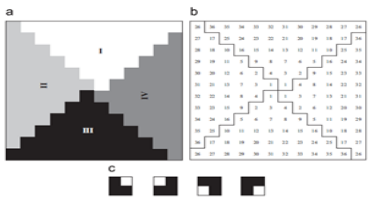

Fig 1: Wu and Chen's model (a) For triangular region (b) Each triangles are numbered (c) Blocks are assigned likewise.

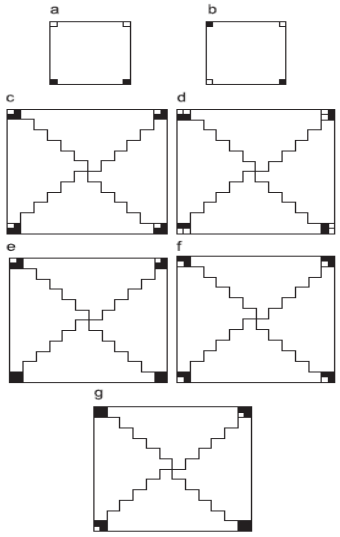

Fig. 2: Wu and Chen model (a) P1 (b) P2 (c) S1 (d) S2 (e) S1 ⊗ S2 (f) $S_1^{90^\circ}$ (g) $S_1^{90^\circ}$ ⊗S2

So in their proposed method they showed that the number of chord areas and blocks depend on how many secret messages we want to hide inside the shares. According to the number of messages the rotational angle reduces for every single secret message (Fig. 4). Suppose we want to hide four message (x=4) then the rotational angle will be 90º (360º/4). From mathematically point of view it looks like we could embed 360 messages in two shares likewise, per one degree of rotational angel. But this is not actually possible as human visual system also has some limitations. So after 30º-40º rotational angle reduction, human eyes faces difficulties to distinguish the hidden messages.

Fang [9] proposed reversible visual cryptography plan. In this plan two secret images which are encoded into two shares; one secret image shows up with simply stacking two shares and the other secret image shows up with stack two shares subsequent to turning around one of them. Jen-Bang Feng [10] added to a visual secret sharing plan for concealing numerous secret images into two shares. This plan breaks down the secret pixels and the comparing share squares to develop a stacking relationship chart. In this the vertices signify the share pieces and the edges indicate two squares stacked together at the sought unscrambling point. By utilizing this diagram and the pre-characterized visual example set, two shares are created. To give more haphazardness to producing the shares Mustafa Ulutas [11] exhorted secret sharing plan in light of the turn of shares. In this plan shares are of rectangular shape and they are made in a completely irregular way. Stacking of the two shares reproduces the first secret. Turning the first share by 90° counterclockwise and stacking it with the second share recreates the second secret.

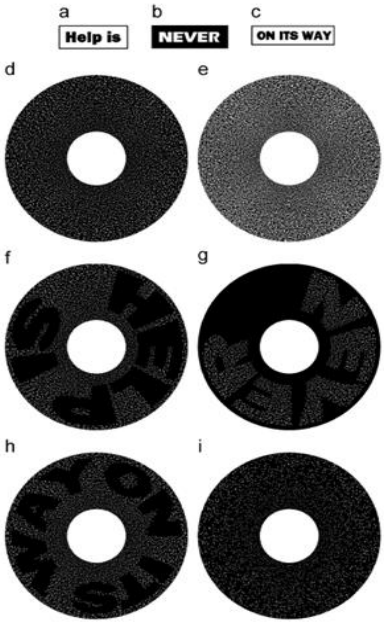

Fig. 4: Example of three 3-secret sharing (a)P1 (b)P2 (c)P3 (d)A (e)B (f) A ⊗ B (g) $A^{120°}$ ⊗ B (h) $A^{240°}$ ⊗ B (i) $A^{85°}$ ⊗ B

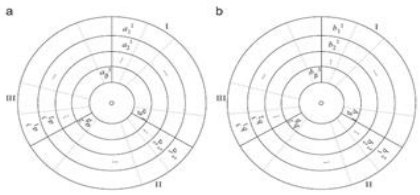

Fig. 3: A and B are segmented into some co-centric chords and further divided in blocks: (a) A, (b) B

Jonathan Weir [12] recommended sharing various secrets utilizing visual cryptography. An master key is produced for all the secret images; correspondingly, secret images are shared utilizing the master key and different shares are gotten. This sort of plan permits separating a secret into K number of shares. At that point the secret can be open from any N number of Shares among K. The significant issue connected with this plan is that the client needs to keep up numerous shares which may come about into loss of shares. Likewise more number of shares means more memory utilization. The utilization of this plan is generally found with managing banking system. In the shared accounts, three shares are made. One is held with bank's server, second is given to the one client for the shared service and third share is conveyed to the second client. Consequently both clients have the capacity to get to the record [13].

C.2.Gray Image:

Gray scale image is a digital image format which stores the intensity value of each pixel. Now the intensity values represents different shades of black and white. That means the range of the intensity value represents from weakest black intensity to the strongest white intensity, with near about continuous value of gray. In visual cryptography gray scale image is not too popular to use, as it has near about continuous intensity value.

In their paper Zhi-hui Wang, Chin-Chen Chang, Huynh Ngoc Tu[14], they proposed a novel method to embed the watermarking and its verification. The proposed system permits a n×n watermark image to be installed into a n×n secret image to develop two shadows and after that to be utilized to check the exactness of the reproduced image. But it was proposed for binary image mainly.

C.3.Color Image:

Color image represent real life colors. In a digital computer system a color image can be represented by different color models-like RGB, YCbCr, HSV etc.

C.3.1. Single Secret Sharing Image:

First color visual cryptography was proposed by Verheul and Van Tilborg[15].Their proposed method was called c-color method. In this method every pixel was sub-divided into n sub pixels and each of the sub pixels were again sub divided in c color regions. In each of those sub pixels only one color region was colored by a single color and rest of them were pure black. Now which sub-pixel would be chosen for which color that was dependent on how two shares would stack upon one another. The pixel expansion n=cX3, c is the number of different colors.

Chang and Tsai [16] proposed a scheme of hiding one secret color image into two color images of same size of the secret image. They generated color index table according to which the secret image was being segmented and then those segmentations were embedded into two color images. But the most critical issue was it requires some additional significant amount of space to embed that color index table into those two images.

Initially in color visual cryptographic model after embedding the secret image into multiple images disturbed the signal and noise ratio. Later R. Youmaran[17] proposed an improved model where a color image can be embedded into multiple color images without disturbing the signal to noise ratio, which actually used to produce the similar quality image as original. Later S.J. Shyu[18] developed more efficient model to reduce pixel expansion. In this new model the pixel expansion was$\log_2 c * m$ where m was the pixel expansion of the used binary technique.

Gopi et. al[19] proposed a new color image cryptographic model where one binary image was used as encryption and decryption. The secret color image used to decompose into three monochromatic images based on color model YCbCr and later they were converted into binary images. Finally they are encrypted by the master binary key image and lastly all of them were XOR-ed together to get the final share. In decryption the binary images were inversed half toned and combined them together.

C.3.2. Multiple Secret Sharing Image:

Tzung-Her Chen [20] expected a multi-secrets visual cryptography which was reached out from conventional visual secret sharing. The arrangement of conventional visual secret picture sharing executed to produce offer pictures macro block by macro block in a manner that different duplicates secret pictures were transformed into just two share pictures and unravel every one of the secrets one by one by stacking two of share pictures in a method for shifting. This plan can be utilized for binary, gray and color secret pictures with pixel extension of 4.

C.4. Segment Cryptography:

Segment display is a type of displaying decimal numerals. . There are diverse sorts of segment displays. Some of them are as 7-Segment Display, 9-Segment Display, 14-Segment Display, 16-Segment Display.

7 Segment display is the most well-known and simple of all segment display. 7 portion shows, as its name shows, is a made out of seven components. These seven components are joined to produce representations of the Arabic numerals.

The seven segments are kept as a rectangle of two vertical segments on every side with one horizontal portion on the top, base, moreover, the seventh fragment cuts up the rectangle on a horizontal plane. [28]

D. Comparative Study

Various parameters are considered by the researchers to develop visual cryptography models. But to evaluate them two major parameters were recommended by Naor and Shamir[2] and those are pixel expansion(m) and contrast α. Pixel expansion means the number of sub pixels in a share that represents a single pixel of the original image. It signifies the loss of resolution from original image to a share image. Contrast means the difference in weight of white pixels and black pixels from the original image to the combined n share images together.

Sr.No	Researchers	Pixel Expansion	Image Format	Genera-ted Shares
1	Naor and Shamir[2]	4	Binary	Random
2	Chin-Chen Chang[3]	4	Binary	Pattern-wise
3	Liguo Fang[4]	2	Binary	Random
4	Xiao-qing Ta[5]	1	Binary	Random
5	E. Verheuland [15]	C*3	Binary	Random
6	C. Chang, C.Tsai[16]	529	Color	Random
7	Chin-Chen Chang[3]	9	Gray	Pattern-wise
8	R. Youmaran[17]	9	Color	Patter-wise
9	S.J. Shyu[18]	$\log_2 c * m$	Color	Random
10	F. Liu[21]	1	Color	Random

Table 4: Single Secret Sharing Algorithms.

Sr.No	Reserachers	No of Secret Images	Pixel Expansion	Image Format	Genera-ted Shares
1	Wu and Chen[6]	2	4	Binary	Random
2	H-C. Hsu[22]	2	4	Binary	Random
3	Wu and Chang[7]	2	4	Binary	Random
4	S.J. Shyu[8]	n>=2	2n	Binary	Random
5	W.P. Fang[9]	2	9	Binary	Random
6	Mustafa Ulutas[11]	2	4	Binary	Random
7	Tzung-Her Chen[20]	n>=2	4	Binary	Random
8	Jonathan Weir[12]	n	4	Binary, Gray, Color	Random

Table 5: Multiple Secret Sharing Algorithms.

E. Proposed Model

This proposed method is based on the segmentation based visual cryptography method. Till now segmentation based visual cryptography is only available for the numeric digits. So this technique is being used for banking passwords, amount transfers exchanges and the key transfers in several cryptographic techniques.

This method represents the alphabets also through segmentation based visual cryptography. In this technique each alphabet is represented by an 11X9 matrix, like a pixel wise repetition about which pixels should be turned on and which are not to represent that specific alphabet. For the time being all the alphabets are represented in upper case letters, but they can also be represented in lower case. Please see from page no. 03 and 05 to understand their representation.

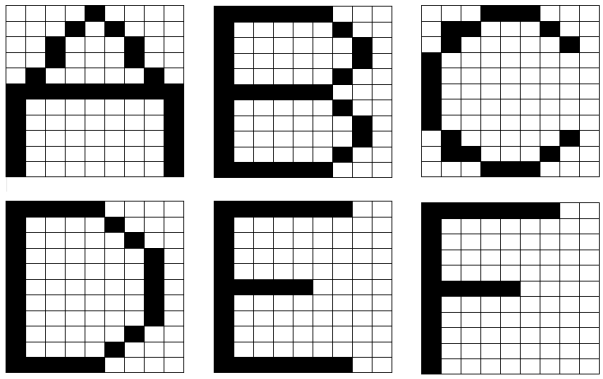

Fig 5: Sample Representation of alphabets.

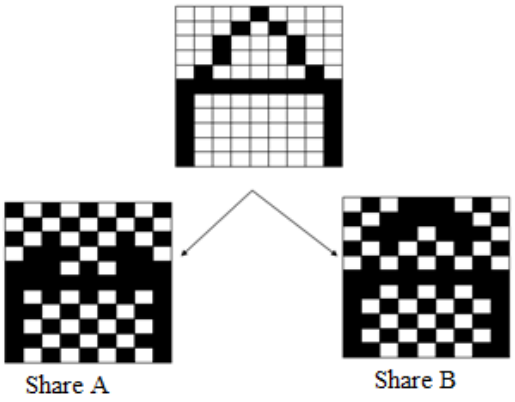

Fig 6: Share-wise Encryption.

The encryption algorithm is as following.

1. Read the current character from the message.

   Ex- If the message is 'HELLO', for the first iteration the current character will be 'H'

2. Now identify the valid pixels on an 11X9 matrix for the current character
3. Take two shares, called 'A' and 'B'

   3.1. In both of the shares put those valid pixels as black

4. Now take share 'A'

   4.1. Put black in alternative cells starting from (0, 0) location.

   4.2. In the next row start with alternative white pixel i.e. put (1, 0) pixel as white and (1, 1) as black, like chessboard.

   4.3. Continue this till the whole 11X9 matrix share not being populated.

5. Now take share 'B'

   5.1. Put white in alternative cells starting from (0, 0) location.

   5.2. In the next row start with alternative black pixel i.e. put (1, 0) pixel as black and (1, 1) as white, like chess board.

   5.3. Continue this till the whole 11X9 matrix share not being populated

6. Repeat from step one for next character until all it ends

The above encryption model takes care about the two things: 1) All the valid pixels in both shares will be black. 2) All the invalid pixels will be white and black alternatively in two shares. For example if in share 'A' the *(i,j)* pixel is black then in 'B' the *(i,j)* pixel will be white. Because of these two fundamental law the resultant image of 'A' and 'B' always show the valid pixels in a dark black pixels and other invalid pixels will be faded, like ash color.

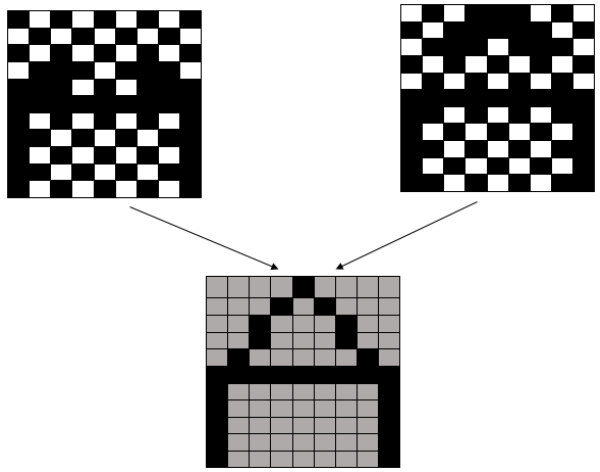

Fig 7: Decryption from two shares.

This one is an efficient method because it didn't need any additional complex computation to find out which pixel should be black or white on which share. We can directly start coloring the pixels on the shares alternatively though an iterative loop. The only problem is to store the valid pixels for each character and mapping them on a matrix of 11X9. These leads little bit additional memory complexity which balances the model in computational complexity/ timecomplexity than other existing methods.

F. Application of Visual Cryptography

Visual cryptography permits effective secret sharing between various trusted gatherings.In the visual cryptography gives a capable method by which one secret can be appropriated into two or more shares. The shares are xeroxed onto transparencies and after that superimposed precisely together; in unique secret can be found without PC support. Some authors [23] described it as a good copyright protection method. The single secret share method is mostly used for remote voting system for authentication purpose.

The significance of using biometrics to build up individual credibility and to identify shams is developing sector in the present situation of worldwide. It is very useful to secure biometric information, like- face identification, iris, gait, fingerprint and voice. Newton [24] and Gross [25] presented a face de-recognizable computation that minimized the

possibilities of performing programmed face acknowledgment while safeguarding points of interest of the face, for example, expression, sexual orientation, and age. Bitouk [26] proposed a face inter-changing method which ensured the character of a face picture via naturally substituting it with substitutions taken from a vast library of open source of face pictures. The advantage of Visual Cryptography is that it is purely based on the human visual system which actually helps to deploy a lot of interesting utilizations in private and public sector. The disadvantage of this is that as it uses very short length of messages, encryption of public key is quite easy by a cryptanalyst.

G. Conclusion

This review paper covers most of the visual cryptographic model from its beginning to till date. All the popular and well secured methods, proposed so far, have been discussed in this paper with proper description and details. It is also taken care about the comprehensive discussion of pros and cons of those methods and they are also evaluated on the basis of different parameters. This paper also has discussed their respective area of uses. This study is exceptionally valuable to comprehend distinctive plan of visual cryptography procedures actualize in the biometric applications and their execution is assessed on four criteria: number of secret pictures, pixel extension, picture organization and sort of share created.

References:

1. Hegde C ,Manu S, Shenoy P D, Venugopal, K. R., Patnaik L. ”*Secured Authentication using Image Processing and Visual Cryptography for Banking Applications,*” in Proceedings of 16 Th IEEE International Conference on Advanced Computing and Communications, ADCOM 2008,2008, pp. 65-72.
2. M. Naor, A. Shamir, “*Visual cryptography*”, in: A. De Santis (Ed.), Advances in Cryptology: Eurpocrypt’94, Lecture Notes in Computer Science, vol. 950, 1995, pp. 1–12.
3. Chin-Chen Chang, Jun-Chou Chuang, Pei-YuLin, Sharing A Secret Two-Tone Image In Two Gray-Level Images”, Proceedings of the 11th International Conferenceon Paralleland Distributed Systems (ICPADS'05), 2005.
4. Liguo Fang, Bin Yu, “Research On Pixel Expansion Of (2,n) Visual Thres hold Scheme”, 1st International Symposiumon Pervasive Computing and Applications, pp.856-860, IEEE.
5. Xiao-qing Tan, “Two Kinds Of Ideal Contrast Visual Cryptography Schemes”, International Conference on Signal Processing Systems, pp. 450-453, 2009.

6. C.C. Wu, L.H. Chen, "*A Study On Visual Cryptography*", Master Thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, R.O.C., 1998.
7. H.-C. Wu, C.-C. Chang, "*Sharing Visual Multi-Secrets Using Circle Shares*", Comput. Stand. Interfaces 134 (28), pp. 123–135, (2005).
8. S.J. Shyu, S.Y. Hunang, Y.K. Lee, R. Wang and Kun Chen , "*Sharing multiple secrets in visual cryptography*", The Journal of The Pattern Recognition Society, Published by Elsevier 2007. Pp. 3633-3651
9. Wen-Pinn Fang, "*Visual Cryptography In Reversible Style*", IEEE Proceedingon the Third International Conference on ntelligent Information Hidingand Multimedia Signal Processing (IIHMSP2007, Kaohsiung, Taiwan, R.O.C,2007.
10. Jen-Bang Feng, Hsien-Chu Wu, Chwei-Shyong Tsai, Ya-Fen Chang, Yen-Ping Chu, "*Visual Secret Sharing For Multiple Secrets*", Pattern Recognition 41, pp.3572–3581, 2008.
11. Mustafa Ulutas, Rıfat Yazıcı, Vasif V.Nabiyev, Güzin Ulutas, (2,2)- "*Secret Sharing Scheme With Improved Share Randomness*",978-1-4244-2881- 6/08,IEEE,2008.
12. Jonathan Weir, WeiQi Yan, "*Sharing Multiple SecretsUsing Visual Cryptography*", 978-1-4244-3828-0/09, IEEE, pp 509-512, 2009.
13. Che Lee, Wen Tsai, " *Authentication of Binary Images in PNG Format Based on a Secret Sharing Technique*," in Proceedings of IEEE International Conference on System and Engineering, Taipei, July 2010, pp. 506-510.
14. Zhi-hui Wang, Chin-Chen Chang, Huynh Ngoc Tu, *"Sharing a Secret Image in Binary Images with Verification"* Journal of Information Hiding and Multimedia Signal Processing Volume 2, Number 1, January 2011
15. E. Verheuland H. V. Tilborg, "Constructions *And Properties Of K Out Of N Visual Secret Sharing Schemes. "*Designs, Codes and Cryptography, 11(2), pp.179–196, 1997.
16. C.Chang, C. Tsai, and T. Chen."*A New Scheme For Sharing Secret Color Images"* In Computer Network", Proceedings of International Conference on Parallel and Distributed Systems, pp. 21–27,July 2000.
17. R.Youmaran, A. Adler, A.Miri, "*An Improved Visual Cryptography Scheme for Secret Hiding*", 23rd Biennial Symposium on Communications, pp. 340-343, 2006. Acquisition and Modeling, pp. 340-344, 2008.
18. S.J. Shyu, "*Efficient Visual Secret Sharing Scheme For Color Images*", Pattern Recognition 39(5) ,pp. 866–880, 2006.

19. Gopi Krishnan S and Loganathan D, "*Color Image Cryptography Scheme Based on Visual Cryptography*", Proceedings of 2011 International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN 2011)
20. Tzung-Her Chen, Kai-Hsiang Tsao, and Kuo-Chen Wei, "*Multiple-Image Encryption By Rotating Random Grids*", Eighth International Conference on Intelligent Systems Design and Applications, pp. 252-256 , 2008.
21. F. Liu, C.K. Wu X.J. Lin, "*Colour Visual Cryptography Schemes*", IET Information Security, vol. 2,No. 4, pp 151-165, 2008.
22. H.-C.Hsu, T.-S. Chen,Y.-H.Lin, "*The Ring Shadow Image Technology Of Visual Cryptography By Applying Diverse Rotating Angles To Hide The Secret Sharing*", in Proceedings of the 2004 IEEE International Conferenceon Networking, Sensing & Control, Taipei, Taiwan, pp.996–1001, March2004.
23. Shen Ying, "*Visual Cryptography based Multiparty Copyright Protect Scheme*", 978-1-4244-5848-6/10/ ©2010 IEEE.
24. E. M. Newton, L. Sweeney, and B. Malin, "*Preserving privacy by de-identifying face images*,"IEEE Trans. Knowl. Data Eng., vol. 17,no. 2, pp. 232–243, Feb. 2005.
25. R. Gross, L. Sweeney, F. De la Torre, and S. Baker, "*Model-based face de-identification*," inIEEE Workshop on Privacy Research in Vision, Los Alamitos, CA, 2006.
26. D. Bitouk, N. Kumar, S. Dhillon, P. Belhumeur, and S. K. Nayar, "*Face swapping: Automatically replacing faces in photographs*," ACM Trans. Graph., vol. 27, no. 3, pp. 1–8, 2008.
27. Sonal Wange, "*A Visual Cryptography to Secure biometric Database:A Review",* International Journal of Advanced Research in Computer Science and Software Engineering, Vol 3, Issue 11, Nov 2013. pp-1540-1547
28. F.W.Wood: Illuminated Announcement and Display Signal. US Patent 974943, 1908.

Corresponding Author:

Kaushik Roy*,

Email: kroy.compsc@gmail.com