ISSN:2320-0790

compusoft
An International Journal of Advanced Computer Technology

Survey of Multiple Information Hiding Techniques using Visual Cryptography

Bijoy Chhetri[1], Sandeep Gurung[2], M.K.Ghose[3]
[1]Department of Computer Science and Engineering, Sikkim Manipal Institute of Technology
[2]Associate Professor, Department of Computer Science and Engineering, Sikkim Manipal Institute of Technology
[3]Dean Academics, Sikkim Manipal Institute of Technology

Abstract: Information now a day's seems to have become abundant and the secure transmission and visualization of it has been a challenge. The major security concerns are of Authentication, Confidentiality and Data Integrity. In regard to this, the various security methodologies have been introduced and Cryptography is one of the schemes where the information is transferred in the disguise form and only authentic user can reveal the exact information. Various Cryptographic techniques has played a very vital role in this regard, among which Visual Cryptographic System(VCS) is one of such kind where the secret data (image, text etc) is encoded into multiple images and decoded using Human Visual System(HVS) without having to tedious calculations and sound knowledge of Cryptography. VC is one of such methodology where the secret information is bifurcated into many disguise images and on super imposing these images, the original secret information is revealed, using Human Visual System(HVS) unlike the traditional cryptography where lot of complex mathematical and time consuming calculation are to be performed. In this paper study of various VC techniques has been done based on number of shares, number of secret messages and types of shares in the cases of Grayscale Image.

Keywords: Visual Cryptography, Secret Sharing Scheme, Random Grids, Pixel expansion, Multiple information Hiding.

I. INTRODUCTION

The explosive growth of information and the security related factors are of growing concern and our dependence on it has become a vital part of our livelihood. Apart from the business enterprises and community holding the larger share, the social, personal, science & geographical information etc are also too abundant across the globe leading to the ubiquitous computing and transmission over the nodes in the web. Many attempts have been made in order to ensure secure access, transmission and confidentially in the data such that the intruder do not make use of weak link over the communication network.

In order to facilitate Authentication, Confidentiality and Integrity of the data that flows across the globe, various Cryptographic techniques have ensured security at the extreme limits.

Cryptography is the art and science of protecting information from undesirable individuals by converting it into a disguised form which is non-recognizable by its attackers while stored and transmitted. Cryptography mainly is the scrambling of the content of data, such as text, image, audio, video to make the data unreadable, during transmission or storage which is termed as Encryption. The reverse of the data encryption is known as Decryption which will reveal the original information. The main goal of cryptography is to keep data secured from unauthorized persons.

Visual cryptography is one of such cryptographic scheme which employs secret sharing methods, that uses human eyes to decrypt the secret message. The dependence of Security solution on the Key distribution policy of public and private key exchange schemes has been eased by using secret sharing schemes where the secret message is shared as (k:n) components during the encryption and upon decryption the minimal of k shares are superimposed to generate the secret message. Any black-and-white visual cryptography scheme can be described using two n x m Boolean matrices S0 and S1, called basis matrices, to describe the sub pixels in the shares. The basis matrix S0 is used if the pixel in the original image is white, and the basis matrix S1 is used if the pixel in the original image is black. The use of the basis matrices S0 and S1 can have small memory requirements (it keeps only the basis matrices S0 and S1), and it is efficient because it only generates a permutation of the columns of S0 or S1 while generating the secret shares.

During the year 1994, Noar & Shamir [10], introduced Visual Cryptography where encryption is done with the secret image after dividing and converting each of the pixel into multiple (n) forms and printed on the transparencies upon receiving all (n) or some (k<n) transparency, the decryption is done by superimposing the images to reveal secret by human eyes avoiding mathematical computation and within limited resources and without a secret key. The various models have been proposed with various other ground of attention including size invariant, single to multiple secret sharing, monochrome, gray scale and color images.

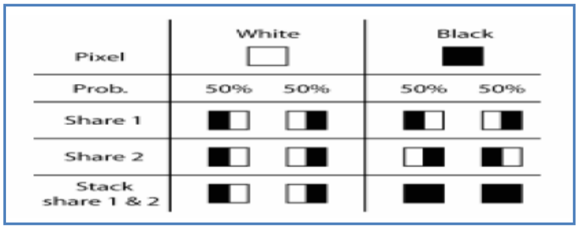
II. Variations on Visual Cryptography

A secret sharing scheme in VC permits a secret to be shared among a set of n participants in such a way that in (n:n) threshold scheme only qualified sets of all n shares can recover the secret whereas in case of (k:n) threshold scheme secret key cannot be reconstructed from the knowledge of fewer than k shares. On the recovery of the image the size of final image varies according to the methodology of share generations used. In such case , the size of share always increase to some extent in case of traditional VC system with Pixel expansion whereas in case of non expansion of pixels the size of recovered image is same as the size of original secret image.

A. Pixel Expansion

Pixel expansion theory implies that the decrypted image gets expanded to the form of n, where n is no of shares, the original image is encrypted into different secret images. All the conventional Visual Cryptography needed the image expansion with the generation of code book. The contrast and the aspect ratio are also the primary factor that affects the performance of this category of algorithms. Due to the increase of size, it can lead to the difficulty in carrying these shares and consumes more storage space and network bandwidth.

Naor and Shamir[10] first proposed pixel expansion based (n:n) threshold VSS scheme, with initial (2,2) share to generate 2 shares based on the encoding of binary pixel into two different images. In case of (2, 2) Scheme the sub-pixels can be arranged as follows in Figure.1.



Pixel	White □		Black ■	
Prob.	50%	50%	50%	50%
Share 1	■□	□■	■□	□■
Share 2	■□	□■	□■	■□
Stack share 1 & 2	■□	□■	■■	■■

Figure-1 Sub-pixels for black pixel in (2,2) scheme [10]

In Figure 2, the implementation and results of (2, 2)-VC Scheme which displays the secret image, the two shares that are generated and the recovery of the secret after overlapping share one and share two, where the final image is larger than the original image.

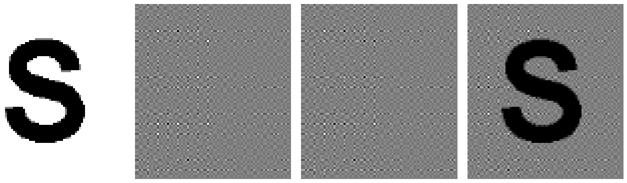


Figure.2 Result of (2,2) VC scheme with Pixel Expansion

From the above observation it is quite evident that at least three drawbacks of traditional VC as follows

1) Codebook design: - VC-based VSS always needs a codebook to support encoding. The codebook is not easily generated and maintained.
2) Pixel expansion:-The designated codebook significantly increases the data size and decreases transmission.
3) Shape distortion: - As in Figure 2.the shape of recovered image becomes wider than that of the original.

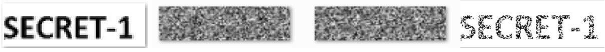
B. Without Pixel Expansion

Unlike the conventional VC where each pixel is probabilistic selection of different expansion code from the code book, the non-pixel expansion method incorporate the methodologies which reveals the secret image from the shares that are of same size. Many schemes have been proposed to solve the problem of pixel expansion.

In order to reduce the pixel expansion of VCS, various size Invariant Visual Cryptography Schemes has been developed. The pixel encoding is constructed for the (k, n)-VCS by using two collection of column vectors, C0 and C1, which are transformed from basic matrices of the conventional (k, n)-VCS. Suppose the basis matrix contains n x m entries, C1 (C0) will contain (m n) x1 columns vectors. To share a black (white) pixel one of the column vectors in C1 (C0) is randomly chosen and then distributes ith entry in the column vector to ith share. In this fashion, each secret pixel within a secret image is encrypted in only one pixel in each constituent share. Thus, image size of shared and stacked images is same as the secret image.

There are various other Multi Level Encoding and Block level encoding techniques to explore the size invariant VCS. The aspect ratio which is the proportional relationship between width and height of the images, in case of invariant secret sharing scheme dramatically reduces the number of extra sub pixels needed in order to construct the secret, thus results in smaller shares, closer to the size of the original secret while also maintaining the aspect ratio, thus avoiding distortion when reconstructing the secret.

In 1987, Kafri and Keren[15] proposed Random Grid (RG) based VC scheme, in which three algorithms were designed to encrypt a binary secret image. As in the example secret image "SECRET-1" with the size of h×w and generated two random grids rGrid1 and rGrid2, whose size is the same as that of original image. The stacked result rGrid1$\oplus$rGrid2 is recognized as the shape or information as that of original image as shown in Figure 3.



Secret Image (188X56) Shares (188X56) Recovered Image (188X56)

Figure.3 Random Grid based VCS

A random grid is regarded as a transparency with a two-dimensional array of pixels. Each pixel is either transparent or opaque. Each pixel is chosen by a random procedure in which there is no relationship among the pixels. According to random probability, the number of transparent pixels is probabilistically equal to that of the opaque pixels in the random grid, also called the cipher-grid. Number of opaque pixels where O denotes opaque , the probP(O)= ½. Similarly, Number of transparent pixels where Tp denotes transparent probP(Tp) = ½; Therefore , average light transmission of a random grid is also ½.

If we assume 'R' to be the random grid then: T(R) = ½ and for a certain pixel 'r' in random grid R the probability of r to be transparent is equal to that of r being opaque.

Therefore P (r=0) = P(r=1) = ½; where 0 denotes opaque and 1 denotes transparent. Probability of light transmission of random pixel 'r' in random grid 'R': T(r) = ½; Superimposing of two random grids pixel by pixel is denoted by the generalised OR operation"$\otimes$"such that T (R$\otimes$R) = t(r $\otimes$r) = ½ for each pixel r in grid R.

The idea proposed with three different algorithms for Random Grid Visual Sharing Scheme (RGVSS) for encrypting binary images by random grids with the following parameters.

```
Algorithm 1:-
Input: A binary secret image
S = {S(i, j) |S(i, j) = 0 or 1, 0 6 i < w,0 6 j < h}
Output: Two cipher-grids
Gk = {Gk(i, j) |Gk(i, j) = 0 or 1, 0 < i < w,0 < j < h},
        where k = ''1'' or ''2''
Step-1:- For (i and j, 0 < i < w and 0 < j < h)//,
        generate a random grid G1 and T(G1) = ½
G1 (i, j) = Random_pixel(0,1)

Step-2:- For (i and j, 0 < i < w and 0 < j < h),
2.1 if(S(i, j) == 0)
2.2 G2(i, j) = G1(i, j); else
2.3 G2(i, j) = G1 ' (i, j); // G1 ' (i, j);represents ''the bit-inverse of G1 (i, j)

Step-3:- Output (G1,G2)
```

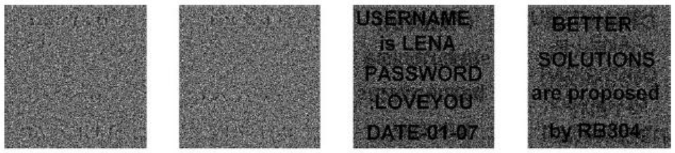
Algorithm 2:-
Encryption of binary image using random grids by inserting random pixel for second random grid for black pixel in original image.

Algorithm 3:-
Encryption same as Algorithm 2 except substitution of pixel takes place for white pixel.

III. MULTIPLE INFORMATION HIDING

The major drawback with traditional VC is that the share are unable to embed more than one secret image and also the share generated with this occur large amount of space compared to the original image which in turn spoil the quality of the revealed image.

The multiple secret sharing problem was initially solved by sharing secrets within two sets of shares S1 and S2. The first secret is revealed when S1 and S2 are superimposed. The second becomes available when S1 is rotated at some predefined angle and superimposed on S2. Since the shares are Rectangular in nature thus restricting the angles required for revealing the secrets as (90◦, 180◦ or 270◦) and the fact that this scheme can only share, at most, two secrets. Multiple secret sharing was developed further by designing circular shares so that the limitations of the angle would no longer raise any such issue . The secrets can be revealed when S1 is superimposed on S2 and rotated clockwise or anticlockwise by a certain angle between 0◦ and 360◦.



(a) S_1 (b) S_2 (c) Stacked result (d) Stacked result by rotating the S_2 with 180°

Figure.4. The share image and stack results [7]

The concept of recursive hiding of secrets in visual cryptography was also proposed by many researchers. This provides a method of hiding secrets recursively in the shares of threshold schemes, which permits an efficient utilization of data. In recursive hiding of secrets, several additional messages can be hidden in one of the shares of the original secret image thereby making reduced network load while information transmission. The basic idea behind recursive threshold Visual Cryptography is information hiding of smaller secrets in shares of larger secrets with secret sizes doubling at every step, and thereby increasing the information, every bit of share conveys to (n-1)/n bit of secret which is sufficient to reveal the secrets on superimposing.

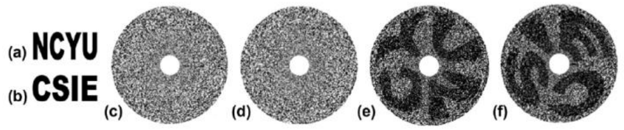


Figure.5. (a) and (b) Original secret images,(c) and (d) generated circular cipher-grids, (e)and(f) recovered secrets.[15]

IV. Analysis of various multiple information hiding techniques

Various parameters are recommended by researchers to evaluate the performance of visual cryptography scheme. Naor and Shamir [10] suggested two main parameters: pixel expansion E and contrast α. Pixel expansion E refers to the number of sub pixels in the generated shares that represents a pixel of the original input image. It represents the loss in resolution from the original picture to the shared one whereas contrast α is the relative difference in weight between combined shares that come from a white pixel and a black pixel in the original image.

Accuracy is considered to be the quality of the reconstructed secret image and evaluated by peak signal-to-noise ratio (PSNR) measure and computational complexity concerns the total number of operators required both to generate the set of n shares and to restructure the original secret image.

Jen.Beng Feng et al.[7] proposed a system of 2 out 2 scheme of extended visual sharing scheme where the stacking rule and the relationship between the pixels of each secret must be indicated. The graph of bipartite in nature is constructed with corresponding share block and forming a graph K(m,m). Each share block is filled by m visual pattern. The share blocks are generated after testing the various visual patterns, which reveals meaningful stacking result with white or black pixel and ineffective visual pattern as well, which always causes the black blocks. The random permutation for every block is performed to break up the regular pixel distribution. Here the expansion size is the ratio of the share image size over the original secret image size, smaller the number means the better performance. The contrast, which is the difference between the revealed black and white pixel, which is in the order of 1/3m where m is no of secret images as shown in the Figure 4.

Multiple Secret sharing without pixel expansion is the work done by Tsung Leigh Lin et al.[17] which is inspired by the concept of sharing multiple secret into meaningless share images. The system has function H(.) which is the Hamming weight of the shares. For the block of pixels in the binary image, the corresponding matrix made to count the number of black pixels as Nb and sum of digits in the corresponding matrix as H (F(m,n)) where (m,n) is mth block of n pixels. In this scheme, there is a process of dividing of each block into nxn size and separating each block into two separate non-intersecting sets. After divide and separating (DS), the sticking process (SP) is performed. Where two shares are combined to generate secret share, the other shares are generated with the rotation of certain angle. Finally, the camouflaging process is done in order to ensure that every block has equal density of the black pixel.

Sandeep Gurung et al.[12] have proposed a hybrid mix of recursive hiding with the circular Random Grid secret sharing scheme. Usage of Random Grid here makes any pixel to behave either of black or white with the average light transmission is ½. The idea of recursive hiding is to allow one to encrypt multiple images efficiently. This scheme uses the random grid generation algorithm proposed by Kafri and Keren. The multiple secret images are hidden one after another after concatenating either horizontally or vertically by making the resultant grid same as the size of the next secret to be hidden. The circular grid is generated to represent the final decrypted image after conversion of the rectangular grid into circular representation .In this scheme the size of secret images has to be in the increasing order, which at one point becomes a bottleneck of the scheme.

Tzung Her Chen et al.[15] proposed a scheme for multi image encryption by using Circular random Grid as shown in the Figure.5. The scheme uses the algorithm proposed by Kafri and Keren to generate the random secret share and with the approach of combing the random grids with fixed angle segmentation generating the two cipher grids of circular nature. Multiple secrets are randomly pricked which are encoded into two circular cipher Grids. By gradually rotating the two grids at a fixed angle 360/m degree multiple secret are reconstructed. Under this scheme, the various secret images are read as a ID matrix, along with the circular Random grid being read sector wise, rotate sector pixel block wise at (k x 360/m) when k is random value. The sector pixel of circular grid and a pixel of secret image will yield another circular cipher grid. On deciphering the two circular grids are super imposed and the clock wise rotation of 360/m will recover other secret images.

The other scheme proposed by Joy Jo Ying et al.[8] is also inspired by Encryption model proposed by Kafri and Keren using random grids. In this work, the random grids are shifted horizontally in order to embed multiple secret images.

In other work of Jeanne Chen et al. [6] the multiple secret data is embedded on the cipher grids which are circular in nature based on the circular shadow image and fixed angle and fixed angle segmentation. In this work the circular gird is generated with black circle and white circle with radius r >o, to generated, the pixels are segmented sector wise with the increasing angular degree till 360. The secret image, represented as the matrix is read and embedded with circular representation by permuting the original pixels generating the cipher Grids.

In special type of the circular visual cryptography for multiple secret hiding, by H. C. Hsu et al.[4], the concentric circular rings are used. The multiple secrets are hidden by relating the share through an angle off to the other. With segmentation of circular share by 1, the 360 segments are gradually filled in by the secret images, so that each secret message is at some angle distance away. By rotating and flipping the circular shares, multiple numbers of secrets could be hidden. The entire summary of all the above comparison is projected in the Table I.

Table I. Comparison of different Methodologies for Multiple information Hiding

Author and Work done	Method Used	No & type of Shares	Con	Share Capacity	Scope of Improvement
H-C Hsu, et-al “Special type of circular visual cryptography for multiple secret hiding”	Pixel Expansion using code book	2, C	Good	4	• Pixel expansion is a bottleneck. • Requires the management of pixel distribution list which is often cumbersome.
Tzung-Her Chen , Kuang-Che Li “Multi-image encryption by circular random grids”	Random Grids	2,C	Low	2	• The number of secrets information is restricted to two. • Visibility problem with less contrast
Tsung Leih Lin, Kai Hui Lee “Novel Visual Secret Sharing scheme for Multiple Secrets without pixel expansion”	Special coding of the pixel with non intersectiong subset	2,R	Good	2	• Only two secrets is shared • The management of each pixel while creating the subsets is considered to be tough job
Jen Bang Feng, Hsein Chu Wu “Visual Secret sharing for Multiple Secrets”	Random Grids	2,R	Low	4	• Rigid Rotatory Angles of 90,180,270. • Uses pixel expansion.
Joy Jo Yi Chang, Justie Su Tzu Juan “Two Secret Sharing Scheme by Shifting Random Grids”	Random Grids	2, R	Good	2	• The number of secrets hidden is limited to two. • Exploiting various directional shifts would increase the efficiency as the idea uses only horizontal shifting
Sandeep Gurung, ,et al. “Multiple Image Encryption using Random Circular Grids and Recursive Image	Recursive Hiding using Random Grids	2, C	Good	3	• Hiding of multiple Image within the same share. • Size of share increases as the number of

Hiding”					iteration is increased
Jeanne Chen et al., “New visual cryptography system based on circular shadow image and fixed angle segmentation”	Pixel Expansion using (2,2) code book	2,C	Good	3	• Pixel expansion • Use of code book • Implementing it using the Random Grids would be efficient to generate more number of Secrets.
Legends used:- Con- Contrast, C-Circular, R-Rectangular					

V. CONCLUSION

The study reveals that there are various techniques proposed by various authors that have various merits and demerits of their own. Further there is a wider scope of implementing the Visual Cryptography in more generalized manner and also improvised by enabling the shares to hold as many information as possible. Further a mechanism can be worked out to have authentication of each share by the Master share to cover up the Confidentiality and Integrity of data with validation and authentication.

REFERENCES

[1] Aarti Pushpendra K Rajput, Multiple Secret Sharing Scheme with Gray-Level Mixing using EVCS, Special Issue of International Journal of Computer Applications (0975 – 8887) on Issues and Challenges in Networking, Intelligence and Computing Technologies – ICNICT 2012, November 2012.

[2] Cheng Chi Lee, Hong Hao Chen A new Visual Cryptography with multilevel encoding Elsevier on Visual Language and Computing Vol 25(2014) pg 243-250.

[3]Cheng Guo,Chin-Chen Chang, Chuan Qin, Multi-Threshold Visual Secret Sharing, Advances in information Sciences and Service Sciences(AISS),Volume4, Number4, March 2012.

[4]H-C Hsu, J Chen, T-S Chen and Y-H Lin Special type of circular visual cryptography for Multiple secret hiding, The Imaging Science Journal Vol 55, pg 175-179.

[5] Hsien-Chu Wu,, Chin-Chen Chang Sharing visual multi-secrets using circle shares ,Computer Standards & Interfaces 28 (2005) 123–135

[6] Jeanne Chen , Tung-Shou Chen , Hwa-Ching Hsu , Hsiao-Wen Chen ,New visual cryptography system based on circular Shadow Image and fixed angle segmentation, Journal of Electronic Imaging 14(3), 033018 (1-5) (Jul–Sep 2005).

[7] Jen Beng Feng, Hesien Chu Wu, Chwei Shyong Tsai, Visual Secret Sharing for multiple secrets Elsevier on Pattern Recognition 41(2008) pg 3572-3581.

[8] Joy Jo Ying and Justice Su Tzu Juan, Two secret sharing scheme by Shifting Random Grids, Workshop procedding on Combinatorial Mathematics and computation, National Chi Nan University, Taiwan.

[9] K.H.Lee, P.L.Chiu, Extended visual Cryptography, IEEE proceeding on Information Forensic and Security Vol-7 No.1 Taiwan.

[10] M. Naor, A. Shamir, Visual cryptography, in: Proceedings of Advances in Cryptology: Eurocrypt94, Lecture Notes in Computer Science, vol. 950, 1995,pg. 1–12.

[11] Saman Salehi, M.A. Balafar,Visual multi secret sharing by cylindrical random grid , Ensivier journal of information security and applications Vol 19 (2 0 1 4) pg 245-255.

[12] Sandeep Gurung, Gaurav Ojha, M.K Ghose,Multiple Image Encryption using Random Circular Grids and Recursive Image Hiding, IJCA vol 86 no 10 Jan 2014.

[13] Sandeep Katta, Recursive Hiding Scheme , Okhlama State University.

[14]Shang-Kuan Chen,A Visual Cryptography based system for sharing multiple secret images, Proceedings of the 7th WSEAS Int. Conf. on Signal Processing, Computational Geometry & Artificial Vision, Athens, Greece, August 24-26, 2007.

[15]Tzung .Her. Chen, K C Li , Multi image Encryption by circular random grids, Information Science 189-2012 , pg 255-265.

[16]T.H. Chen, K.H. Tsao, K.C. Wei, Multiple-image encryption by rotating random grids, in: Proceedings of the 8th International Conference on Intelligent System Design and Applications (ISDA’2008), Kaohsiung, Taiwan, 2008.

[17] Tsung Leih Lin, Kai Hui Lee Novel Visual Secret Sharing scheme for Multiple Secrets without pixel expansion ,Elsevier on Expert system with application 37(2012) pg 7858-7869.