Visual Cryptography Schemes for Secret Image Sharing using GAS Algorithm

Bharanivendhan N
Department of computer science
Dhanalakshmi College of Engineering
Chennai, India

Amitha T, Ph. D
Department of computer science
Dhanalakshmi College of Engineering
Chennai, India

ABSTRACT
Visual Cryptography Schemes (VCS) is a method of image encryption used to hide the secret information in images. In the traditional VCS, the secret image is encrypted into n number of shares randomly and distributed to the n number of participates. The secret image can be recovered simply by stacking the shares without any complex computation involved. However previous approach suffers a security, pixel expansion and noise problem. The proposed system consists of two phases. At the sender side, the input secret image generates the four meaningless shares based on GAS algorithm is done in the first phase. In the second phase, the cover images are added in each shares directly by using stamping algorithm and distributed the embedded images to the participants. At the receiver side, the embedded images can be processed to extract the covering images from the generated shares and the secret images can be retrieved by overlapping the shares in the correct order. The password authentication is also provided at both the sender and receiver side. The proposed system provides high security, increase in the number of shares and reduce the pixel expansion problem and high resolution to visualize the secret image.

Keywords
Visual cryptography schemes (VCS); GAS algorithm; stamping algorithm; pixel expansion.

1. INTRODUCTION
Recently, the transmission of data through network is increasing rapidly, which provides instant access or distribution of digital data. Visual cryptography is the technique using in the latest technology to transmit the secret information in images i.e., called secret image. Secret image sharing is the important subject in the field of communication technology, information security and production. However security can be introduced in many ways like transmitting password, image hiding, watermarking technique, authentication and identification. But the drawback of these methods is that the secret images can be protected in single information carrier. If it lost once, the information carrier is either damaged or destroyed.

To overcome this problem, VCS secret sharing scheme was introduced by Naor and shamir[1], the secret image is split up into number of shares and transmit to the number of participants. A visual secret sharing scheme is a technique used to encrypt the secret image by splitting the shares into several piece and distribute it into the corresponding participants. A set of qualified participants can be able to retrieve the secret image by overlapping the shares in correct order. A traditional VCS takes the secret image as input and number of shares as output, it satisfies two conditions 1) secret images can be recover by any qualified subset of shares; 2) any forbidden subset of shares cannot gain any information about the secret image. For example, In traditional (k,n)-VCS, the secret image is revealed if k of n shares are known. Any number of n shares less than k is not sufficient to reveal secret image where, k is the number of participants and n is the number of shares.

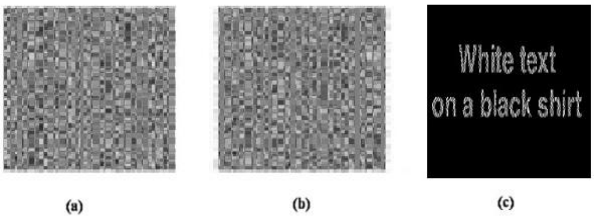

Figure 1: Example of traditional (2, 2)-VCS with image size 128x128.

Secret image is split up into two shares, share (a) and share (b) as shown in figure 1. The shares are distributed to two participants and neither the single participant cannot gain any information about the secret image.

2. BACKGROUND AND RELATED
2.1 Visual Authentication and Identification
M. Naor and B. Pinkas describe the visual authentication and visual identification methods [2], which are the methods for human users based on visual cryptography. These methods are very natural and easy to use and can be implemented using very common "low tech" technology. The advantages of this system are that the physical requirements are linear in the size of the message and logarithmic in the fault probability p. Each scheme defines what capabilities the human participant should have in order for the scheme to be secure. In some cases these capabilities are quantified and the other complexity measures are connected to the parameters of this quantification. The assumptions made about human capabilities can be verified through experiments. When these assumptions are verified the protocol is completely proved to be secure. The drawback of this method describes about the visual authentication methods which are applicable for any kind of visual data: numerical, textual or graphical. These methods are one-time methods that can be used for only a single authentication.

2.2 Visual Cryptography Scheme
Blundo et al [3] analyzes the (k, n)-threshold VCS in which the reconstruction of black pixels is perfect. It provided a construction for (k, n)-threshold VCS for any value of n and k with $2 \leq k \leq n$. Such a scheme improves on the ones given with respect to the pixel expansion. For any $n \geq 3$, a complete characterization of maximal-contrast $(n - 1, n)$-threshold VCS

in canonical form having parameter $h \geq 1$ and minimum pixel expansion. The advantage includes a construction for a maximal-contrast c-color (2, n)-threshold VCS, when $c > n$. Such a construction is optimal with respect to the pixel expansion. And the relations between the number of colors that have in any c-color (k, n)-threshold VCS their pixel expansion and the values k and n. Finally, the two constructions for c-color (n, n)-threshold VCS, one for n even and one for n odd. Such constructions improve to the pixel expansion. The main drawback of this system is that the pixel problem is not solved.

2.3 Meaningful Shares in Visual Secret Sharing Scheme

Tsai et al [6] describes the k-out-of-n visual secret sharing scheme (VSSS) propose a binary secret image, is encoded into n shares called transparencies. Each share consists of black and white pixels, in the form of noise and has size larger than that of the secret image. The binary secret image can be decoded by using the visual system through superimposing any k of n transparencies without performing any cryptographic computation. To overcome the above problem, this system takes three pictures as an input and generates two images which correspond to two of the three input pictures. The third picture is reconstructed by printing the two output images onto transparencies and stacking them together. While the previous researches basically handle only binary images, but this establishes the extended visual cryptography scheme suitable for natural images. Advantage is to extend the schemes and encoded n shares as meaningful. Disadvantage of this technique is in practice, meaningless shares, however, might invite the adversary attention and to manage numerous increasing transparencies belonging to different secrets is also a problem.

2.4 EVCS by Using Halftone Visual Cryptography

Wang et al. have discussed Halftone visual cryptography (HVC) [5] enlarges the area of visual cryptography by the addition of digital halftoning techniques. The proper halftoned patterns of the dithering matrix of the gray-levels 0…9 is as shown in the figure 2. In particular, in visual secret sharing schemes, a secret image can be encoded into halftone shares taking meaningful visual information. Error diffusion has low complexity and provides halftone shares with good image quality. A reconstructed secret image, obtained by stacking qualified shares together, does not suffer from cross interference of share images. To overcome this problem, three methods are developed to make the reconstructed image immune to the interference from the share images. The first method employs a complementary halftone image pair. The second method deliberately introduces homogeneously distributed black pixels into each share, which has the advantage that complementary image pairs are not needed. The third method exploits the fact that the half toning of the grayscale images alone may generate a sufficient number of black pixels to satisfy the contrast condition of image decoding. The Half toning process for each pixel is done using the Algorithm1. A black pixel is deliberately introduced only when a sufficient number of black pixels have not yet been produced. Thus, complementary shares are also not required. With fewer constraints on error diffusion, the third method has the potential to obtain shares showing natural images with fine details.

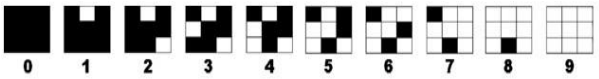

Figure 2: Halftoned patterns of the dithering matrix of the gray-levels 0…9

Algorithm 1: The Half toning Process for Each Pixel

INPUT : The c X d dithering matrix D and a pixel x with gray-level g in input image I
OUTPUT : The halftone pattern at the position of the pixel x
METHOD : Step 1: For i=0 to c-1 do
Step 2: For j=0 to d-1 do
Step 3: If $g \leq D_{ij}$ then print a black pixel at position (i,j);
Step 4: Else print a white pixel at position (i,j);

The drawback in method 2 is that the requirement of a complementary pair is removed and all the shares are generated to carry the natural images. It is clear that in method 2, the quality index is more correlated to {k, n} in the VC scheme. Under the same VC scheme, if the HVC expansion is also the same, lower image quality is achieved in method 2 than in method 1.

2.5 Embedded Visual Cryptography Schemes

The Proposed EVCS developed by Feng Liu and Chuankun Wu [10] is a kind of secret sharing scheme which allows the encoding of a secret image into shares distributed to participants. The EVCS is for the (2, 2) access structure, and the scheme may have security issues when relaxing the constraint of the dynamic range. In addition, EVCS is only for threshold access structure. The Embedded EVCS can be applied on general access structure and is always unconditionally secure which is inherited from the corresponding VCS. The Embedded EVCS is flexible in the sense that there exist two trade-offs between the share pixel expansion and the visual quality of the shares and between the secret image pixel expansion and the visual quality of the shares. The disadvantage includes in physical properties such as contrast, pixel expansion, and color were extensively studied by researchers worldwide. The applications of EVCS is to avoid the custom inspections, because the shares of EVCS are meaningful images and (2, 2) hence there are fewer chances for the shares to be suspected and detected. Pixel problem still exists. The secret image is also not fully protected.

3. THE PROPOSED SCHEME

The architecture design describes the overall flow of the system and it is very much important to develop the project by the developers. It explains all the main process such as generate shares, embedding process and extraction process along with its sub process in blocks. The architectural diagram is shown in figure 3.

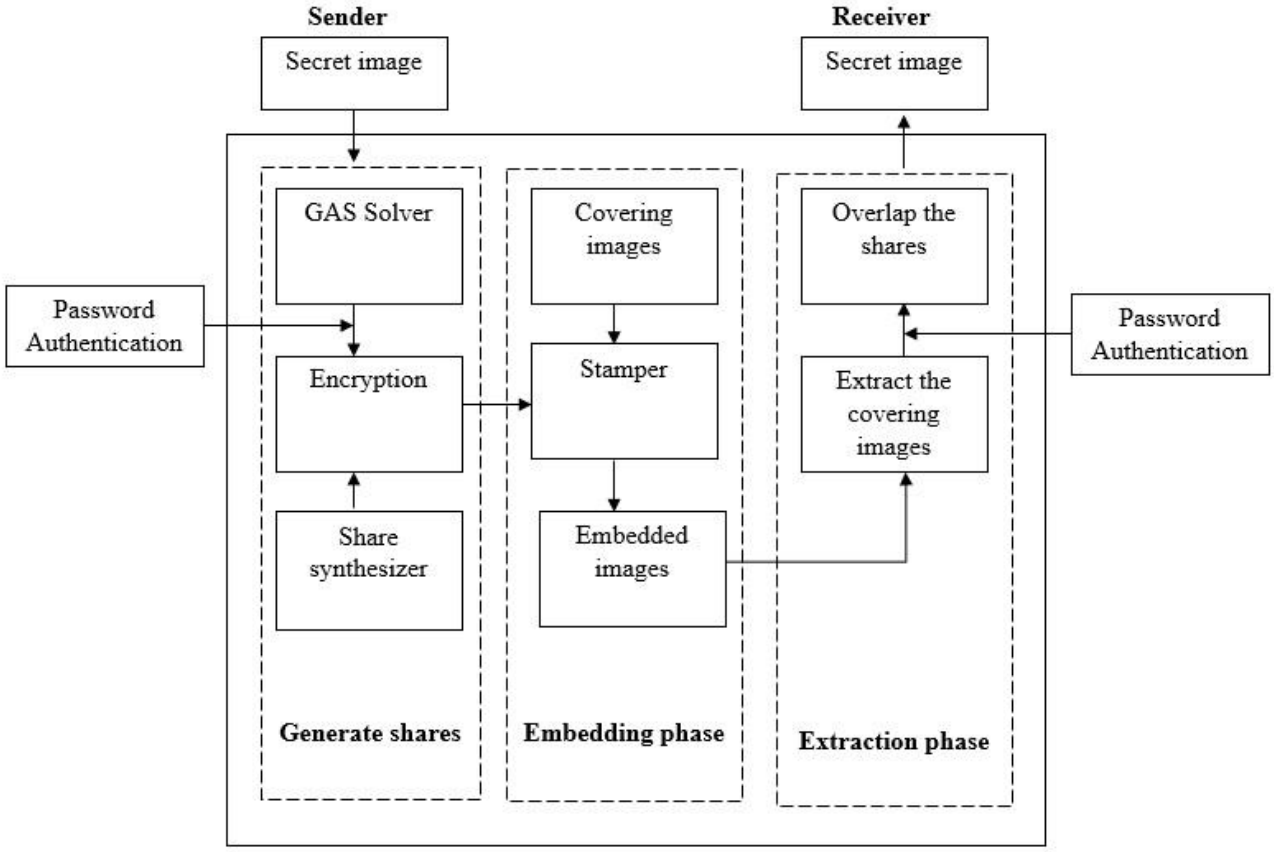

Figure 3: Architectural diagram

In general, three main processes are implemented in this system. At the sender side, the preprocessed secret image can be encrypted by using the GAS solver algorithm. This image can be protected by using the password authentication. The share synthesizer splits the image into the number of shares as per the number of participants can be done in the generate shares phase. At the embedding phase, the shares can be stamped with the covering images. The embedded images are now ready to send it to the receiver. At the receiver side, the shares can be extracted from the covering images. Thus by overlapping the shares in an order with the correct password verification, the secret image can be retrieved at the extraction phase.

4. EXPERIMENTAL RESULTS

In this section, the experimental results for each phase using the algorithm can be illustrated and the screen shots for the output retrieved can also be produced.

4.1 Generation of Shares

The algorithm starts to find a solution for the given GAS by the procedure access structure () with an initial set of participants and number of participants in Steps 1 and 2. In each iteration of Steps 3, the algorithm proceeds to find a minimum n' by decreasing or increasing the value of n' by 1 where n is the number of shares and n' is the number of participants. If a solution is found (i.e., C← C_{best} denotes the best-found energy function in the last iteration), the algorithm stops while n'← n'-1 or it decreases the value of n' by 1 and proceeds to the next iteration with the lower n'. On the contrary, if a solution is not found, the algorithm stops while n'< n or it increases the value of n' by 1 and proceeds to the next iteration while n'>n. At the end of the procedure, the algorithm outputs a minimum n' and a construction set C as the optimal solution of the problem. If no solution can be found for a given access structure, the solution procedure will be terminated while n'=n'_{max}, where n'_{max} is a given parameter that prevents Algorithm 2 from falling into an infinite loop. The output of the algorithm produces the qualified shares from where the secret image is hidden in it.

Algorithm 2: SA-based algorithm for GAS solver

INPUT : Set of participants P= $\{i_1, i_2, \ldots, i_n\}$ and an access structure (T_{Qual}, T_{Forb})
OUTPUT : Constructed qualified shares $\{S_1, S_2, \ldots, S_n\}$
METHOD :
STEP 1: Sender set the number of participants P= $\{i_1, i_2, \ldots, i_n\}$.
STEP 2: The qualified and forbidden set has to be declared.
STEP 3: The secret image is splitted into the number of shares as mentioned.
If n'=n_{max} then Stop and Output "No solution found"
Else
C ← C_{best}
Until n'←n'-1
STEP 4: Until the number of shares 'n', the share synthesizer generates the shares
STEP 5: The generated share is sent to the embedding process

After getting the secret image, share synthesizer generates the number of shares as per the number of participants and the

password authentication is used for the security concerns as shown in figure 4. Then, the protected shares are sent it to the embedding process.

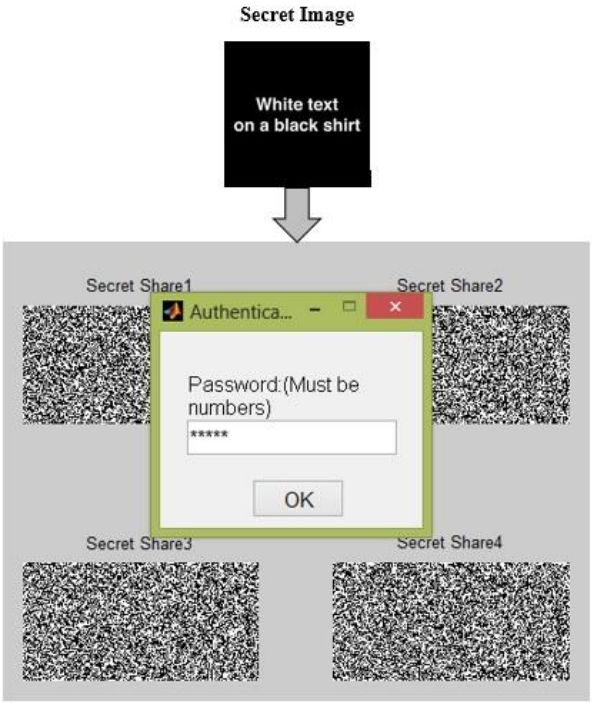

Figure 4: Generating the Shares with Authentication

4.2 The Embedding Process

The Embedding process involves embedding the binary image with the covering shares. For that, the covering shares can be divided into the blocks which contain the sub pixels each. Embedding is nothing but the pixels in the embedding positions are replaced by the sub pixels of the share matrix. The input for the embedding process is the covering shares constructed to the corresponding VCS with the covering images required.

Algorithm 3: Stamping Algorithm

INPUT : Shares and covering images
OUTPUT : Embedded image
METHOD: Procedure Stamping (shares, cover images)
STEP 1: Calculate the collection of pixel colors for shares, cover images and secret image in coordinate (x,y)
STEP 2: Calculate required amount of cover pixels in shares in black and white region of the secret image
STEP 3: Calculate the amount of black pixels overlapped at coordinate (x,y)
STEP 4: Set the indicator for coordinate to 0 i.e.., available for stamping cover pixel.
STEP 5: Add cover pixels on selected coordinates (x,y) of shares. The black pixels will be added on candidate coordinate (x,y) of share that has a white pixel on it.
STEP 6: Repeat from step 3 to step 5 until all require cover pixels are stamped on shares

In step 1 to 3, the required parameters used in this algorithm is to be calculated. In step 4, the indicator for an image is to be set to 0. The next step involves adding the cover pixels on to the shares. The stamped embedded image is to be obtained as an output as shown in the figure 5.

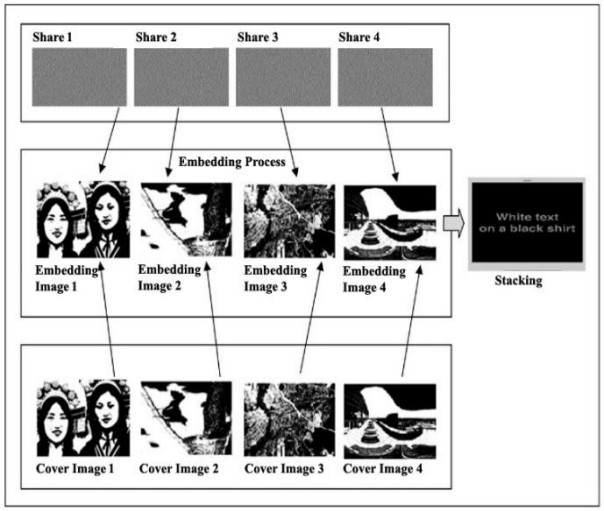

Figure 5: Embedding Process

Select the cover images to embed the generated shares with the cover images. Now, the shares are turned into meaningful shares. The generated shares are chosen to embed the covering images with the shares. And then it is transmitted to the receiver side. The output of this process would be the embedded shares which are more secure and tough to find and hack by the hackers.

4.3 Recover Images Figures and Tables

Extract the embedded cover images and secret shares. By stacking the shares in the correct order will get an original secret image is done using the algorithm 4. At the receiver side they stack the shares by using the logical or operation and extract an original secret image. The beauty of such a scheme is that a set of qualified participants is able to recover the secret image.

Algorithm 4: Extraction Process

INPUT : Embedded images
OUTPUT : Secret image
METHOD:
STEP 1: Extract the covering images and the shares from the stamped images
STEP 2: Overlap the shares in the appropriate order with authenticated password
STEP 3: The exact secret image can be obtained at the receiver side.
STEP 4: If the order changes or fetching an unauthenticated password leads to retrieve a forbidden image.

The embedded images are stored in the Embedded Images folder. It is used while the extraction operation is performed. At receiver side, the covering images are extracted from the embedded images after accepting the correct password as shown in the figure 6. The extracted shares extracted from the embedded images and stored in the extracted images folder.

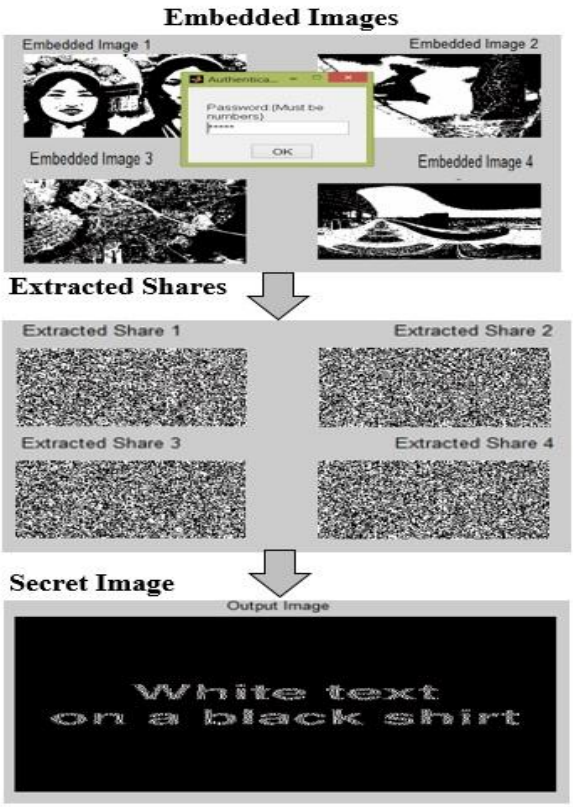

Figure 6: Extraction Process

5. DISCUSSION AND ANALYSIS

In this section, the existing EVCS is compared with the proposed GAS algorithm. The values related to the images are tabulated in the table 1, which describes a image memory size and dimensions of an images. The five secret images are analyzed in this section. In EVCS, the two shares are split up and stacked to retrieve an original secret image. But by using the GAS algorithm, the secret image can be split up into four shares and the secret image can be retrieved with high resolution. The graph shows the variance in between the EVCS and GAS algorithm. Higher the memory size leads to high resolution. The most important property of visual cryptography is that, the decryption of the secret images requires neither the knowledge of cryptography nor complex computation.

Table 1: Comparison between existing and proposed system

Secret Image Name	Memory Size		Dimension
	EVCS (Existing)	GAS (Proposed)	
Bwimg1	0.866KB	4.11KB	344X147
Bwimg2	0.934KB	6.87KB	478X147
Bwimg3	3.77KB	8.91KB	568X177
Colimg1	4.08KB	14.7KB	720X140
Colimg2	33.2KB	45.3KB	1000X369

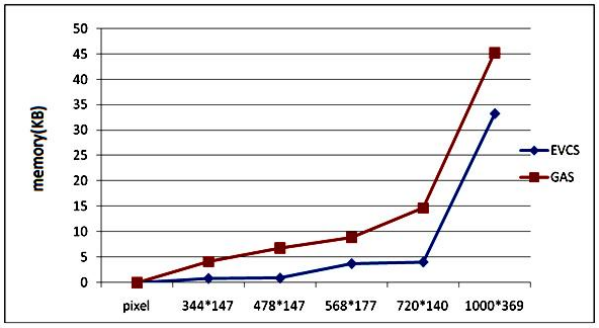

Figure 7: Representation of EVCS with GAS

By comparing the values of Embedded Visual cryptography Schemes (EVCS) with General Access Structures (GAS), it is realized that the values of original image resolution is comparatively higher after using the GAS algorithm cryptography schemes as shown in table 1. The graphical representation gives the higher curve in GAS shows the higher resolution can be shown in the figure 7. This can also increases the security and the number of shares produced.

6. CONCLUSION AND FUTURE WORK

Visual Cryptography Scheme (VCS) is an encryption method that uses the GAS (General Access Structures) algorithm. The pixel expansion problem is comparatively reduced than the existing system by increasing the number of shares. It also makes high resolution of an image with good visual quality. A secret sharing scheme is a technique to share a secret among a group of participants. The share synthesizer generates the number of shares as per the number of participants. The shares are embedded with the covering images using stamping algorithm, to make the secret image more protective. At the receiver side, the secret image can be retrieved by stacking the shares in the correct order. The password authentication on both the sender and receiver side adds more security to the system. The hackers cannot find the secret image since all the images are covered using meaningless shares. It compares image quality and memory size using EVCS and GAS algorithm.

The future work involves the more number of shares and to implement the secret color images and share the multiple secret images by using various methods.

7. REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," in Proc. EUROCRYPT' 94, Berlin, Germany, 1995, vol. 950, pp. 1–12, Springer-Verlag, LNCS.

[2] M. Naor and B. Pinkas, "Visual authentication and identification," Springer-Verlag LNCS, vol. 1294, pp. 322–336, 1997.

[3] C. Blundo, A. De Bonis, and A. De Santis, "Improved schemes for visual cryptography," Designs, Codes and Cryptography, vol. 24, pp. 255–278, 2001.

[4] Z. Zhou, G. R. Arce, and G. Di Crescenzo, "Halftone visual cryptography," IEEE Trans. Image Process., vol. 15, no. 8, pp. 2441–2453, Aug. 2006.

[5] Z. M. Wang, G. R. Arce, and G.Di Crescenzo, "Halftone visual cryptography via error diffusion," IEEE Trans. Inf. Forensics Security, vol.4, no. 3, pp. 383–396, Sep. 2009.

[6] D. S. Tsai, T. Chenc, and G. Horng, "On generating meaningful shares in visual secret sharing scheme," Imag. Sci. J., vol. 56, pp. 49-55, 2008.

[7] M.Amarnath Reddy, P.Shanthi Bala, G.Aghila, "Comparison of Visual Cryptographic Schemes," IJEST, vol. 3 no. 5, pp. 4145-4150, 2011

[8] Guzin Ulutas, Mustafa Ulutas, Vasif Nabiyev, "Distortion free geometry based secret image sharing" Procedia Computer Science, vol 3, pp. 721–726, 2011

[9] Mrs. Bhandare Shital, Mr. Jhade Manoj and Mrs. Jadhav Angarika," An improved approach for Extended Visual Cryptography Scheme for Colour Images", IJCA, no.2, pp.1-4, 2011

[10] Feng Liu and Chuankun Wu, "Embedded Extended Visual Cryptography Schemes," IEEE, vol. 6, no. 2, pp. 307-322, 2011.

[11] Xiaotian Wu and Wei Sun, "Random grid-based visual secret sharing for general access structures with cheat-preventing ability," The Journal of Systems and Software 85, pp. 1119– 1134, 2012

[12] Cheng Guo, Chin-Chen Chang, Chuan Qin, "A hierarchical threshold secret image sharing," Pattern Recognition Letters, vol 3, pp. 83–91, 2012

[13] Kai-Hui Lee and Pei-Ling Chiu,"An Extended Visual Cryptography Algorithm For General Access Structures," IEEE , vol. 7, no. 1, pp. 219-229, Feb 2012.

[14] Lonarkar S.G And Pande K.P,"Embedded Extended Visual Cryptography Schemes For Different Patterns" IJCS, vol 2, Issue 1, pp.14-17, March 2012

[15] B.Sreenivas Rao, Chindam Sambasiva Rao, P Divya, SM Riyazoddin, "Analysis of Secret Sharing & Review on Extended Visual Cryptography Scheme", IJETTCS, vol 1, Issue 1, pp.90-95, June 2012.

[16] Shyong Jiang Shyu, "Visual Cryptography of Random Grids for General Access Strctures", IEEE, vol. 23. no. 3, March 2013