Varied Visual Cryptographic Techniques

Anushree Suklabaidya
Department of Computer Science
Birla Institute of Technology, Mesra
Ranchi, India
anushree.suklabaidya@gmail.com

G. Sahoo
Department of Information Technology
Birla Institute of Technology, Mesra
Ranchi, India
gsahoo@bitmesra.ac.in

ABSTRACT: ***The need for security in information technology is felt more when e-commerce, e-transactions, e-mail, e-banking, e-data processing boomed. With these becoming very common in everybody's life, information security became very important and essential. Cryptographic techniques are used to secure information but require complex mathematical understanding and calculations. Visual Cryptography on the other hand eliminates the use of complex mathematics in the decryption process. Hence Visual Cryptography is suitable for most situations where the participants have little knowledge of cryptography and the calculations related to cryptography.***

Keywords*: Visual Secret Sharing Scheme, Shares, Visual Cryptography, secrets, subpixel, superimpose***.**

I. INTRODUCTION

Since the use of the Internet is very common these days and hence the exchange of important data is growing, the security of the exchange of data is of major concern. To deal with the problem of exchanging secret information, Naor and Shamir [1] came up with a technique known as Visual Cryptography. Visual Cryptography is a secret sharing scheme which can be used to share secrets among participants who do not have the knowledge of complex mathematics. Any written printed text, pictures etc. can be encrypted using Visual Cryptography and the decryption is done based on the human visual sensibility. The secret is segregated into n parts in the encryption process, each known as 'shares'. The required numbers of shares are then superimposed in a correct alignment to reveal the secret in the decryption process. The advantage of using Visual Cryptography over traditional cryptographic techniques is that the former requires no complex mathematical ability for the decryption of the secret message.

The remaining part of this paper is organized as follows: Section II consists of a description of different cryptographic techniques, section III consists of a comparison among the different techniques and section IV concludes the paper.

II. DIFFERENT VISUAL CRYPTOGRAPHIC TECHNIQUES

Different visual cryptographic techniques came into use after Naor and Shamir [1] came up with the idea of sharing a secret using Visual Cryptography. There are schemes that shares only one secret and schemes that shares multiple secrets. Some of such schemes are discussed below:

A. SINGLE SECRET SHARING SCHEMES:

i. NAOR AND SHAMIR:

Naor and Shamir [1] were the first to introduce Visual Cryptography. According to them Visual Cryptography can take any of the following forms:

- (k, n) Visual Secret Sharing Scheme
- (n, n) Visual Secret Sharing Scheme

In (k, n) Visual Secret Sharing Scheme a secret message is divided into n shares so that the original message is visible if any k (or more) of the shares are stacked one upon the other. But the shares will not reveal any information regarding the secret message if fewer than k shares are stacked.

In (n, n) Visual Secret Sharing Scheme all the shares are stacked together so that the original secret shared is revealed.

Their model assumed that the secret message consists of a collection if black and white pixels. Each pixel is divided into two subpixels according to the following table in Figure 1:

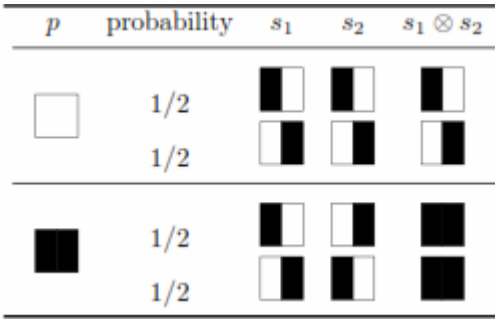


Figure 1: Creation of shares using two subpixels per secret pixel.

The inferred structure is described as an n×m Boolean matrix S = [s_{ij}] where s_{ij}= 1 iff the j^{th} subpixel in the i^{th} share is black, else s_{ij}=0 iff j^{th} subpixel in the i^{th} share is white. When the shares are stacked together the black pixel of the resulting structure is the Boolean "OR" of the rows $i_1, i_2, \ldots\ldots, i_r$ in S. It is seen that using two subpixels per pixel can be used for (*k*, *n*) Visual Secret Sharing Scheme but it distorts the aspect ratio in the resulting image. So, Naor and Shamir recommended using four subpixels per pixels instead of two, which will keep the aspect ratio of the original image intact. The creation of shares using four subpixels per pixel is shown in the Figure 2:

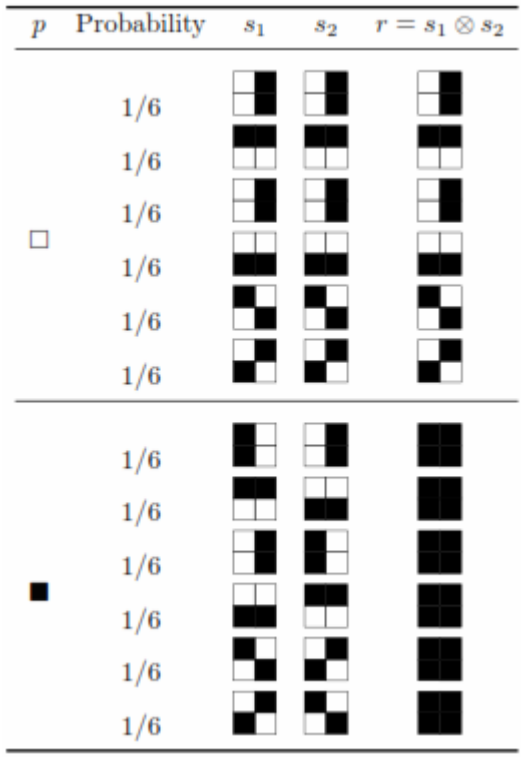


Figure 2: Creation of shares using four subpixels per secret pixel.

ii. VISUAL CRYPTOGRPAHY FOR GENERAL ACCESS STRUCTURES:

Ateniese et al. [2] developed general access structures for Visual Cryptography. General access structures are developed to outdo the weak security condition of the basic Visual Cryptography model. They have described the set of Qualified subsets as Γ_{Qual} and the set of Forbidden subsets as Γ_{Forb} on n participants P = {1, 2, ..., n}. The participants in Γ_{Qual} can decrypt the secret message whereas the participants in Γ_{Forb} cannot. (Γ_{Qual}, Γ_{Forb}) is called the access structure. The set of all subsets of P is denoted by 2^P. Then,

$\Gamma_{Qual.} \subseteq 2^P$ and $\Gamma_{Forb.} \subseteq 2^P$ and $\Gamma_{Qual} \cap \Gamma_{Forb} = \varphi$

Γ_{Qual} is called monotone increasing iff suppose we have a subset $X \in \Gamma_{Qual}$ then if the participants of X can decrypt the secret message, a superset of X viz., Y should also be able to decrypt the secret message.

Γ_{Forb} is called monotone decreasing iff suppose a subset $X \in \Gamma_{Forb}$ cannot decrypt the secret message then a subset Y of X should also be unable to decrypt the secret message.

An access structure is called strong access structure iff Γ_{Qual} is monotone increasing, Γ_{Forb} is monotone decreasing and $\Gamma_{Qual} \cup \Gamma_{Forb} = 2^P$.

iii. EXTENDED VISUAL SECRET SHARING SCHEME:

The basic Visual Cryptographic shares are random patterns that carry no meaning when observed individually. Hence it raises a suspicion that it may be a part of some kind of encryption and hence may lead to the detection of the secret hidden. To overcome this suspicion several extended Visual Cryptographic schemes have been proposed. Droste [3], Ateniese et al. [2] and Wang et al. [4] proposed different Extended Visual Cryptographic Schemes that were constructed by manipulating the share matrices. Nakajima et al. [5] developed Extended Visual Cryptographic Scheme for natural images. Tsai et al. [6] proposed an Extended Visual Cryptographic Scheme in which its shares were constructed simply by replacing the white pixels by transparent pixels and replacing the black pixels by the pixels from the cover image.

iv. HALFTONE VISUAL CRYPTOGRAPHY:

The halftone Visual Cryptography proposed by Zhou et al. [7] is based on the model of general access structures developed by Ateniese et al. [2]. It is built upon the basis matrices and matrices C_0 and C_1 representing the white and black secret pixel respectively. In halftone Visual Cryptography a secret binary pixel p is encoded into an array of $Q_1 \times Q_2$ subpixels in each of the n shares. This array of $Q_1 \times Q_2$ subpixels is known as the halftone cell. The pixel expansion of this scheme is Q_1Q_2. Generally a

square halftone cell where $Q_1=Q_2$ gives an undistorted reconstructed image.

v. VISUAL CRYPTOGRAPHY FOR GRAYLEVEL IMAGE:

Visual Cryptography was used for binary images before Choulin et al. [8] came up with a Visual Cryptographic scheme applicable for real time based scenario. Their proposed scheme was designed for graylevel images using dithering techniques. They did not use a gray pixel directly in the shares rather used dithering techniques to convert the graylevel images into the approximate binary images. Then they used the existing Visual Cryptographic schemes for binary images to encrypt the secret into the shares. The shares for (3, 3) Visual Secret Sharing Scheme and the decoded image are shown in Figure 3.

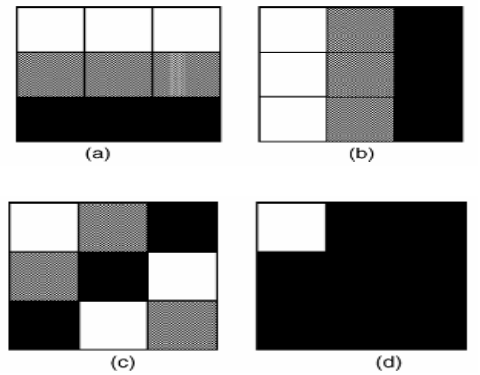


Figure 3: Shares and decoded image for a (3, 3) Visual Secret Sharing Scheme (a) share 1 (b) share 2 (c) share 3 (d) decoded image with gray-level 0.

vi. COLORED VISUAL CRYPTOGRAPHIC SCHEME:

Since binary image is not more practical and since the Visual Cryptographic schemes based on the binary images reflect poor quality of the reconstructed image, traditional Visual Cryptographic schemes cannot be used for encrypting color images. Liu et al. [9] proposed a colored Visual Cryptographic scheme for encrypting color images into several shares. Their approaches are mentioned below:

- The first approach is to print the colors contained in the secret image directly onto the shares as was is done in the basic Visual Cryptographic model. This reduces the quality of the decrypted color image since the pixel expansion is large.
- The second approach uses the three color channels (red, green, blue or cyan, magenta, yellow). The colored image is converted to black and white image based on those three colored channels. Then traditional Visual Cryptographic schemes are applied on the converted image to encrypt it into shares. This approach uses halftoning that degrades the quality of the decrypted image even though the pixel expansion is decreased.
- The third approach carries out bitwise encryption based on the binary representation of the colored pixels of the secret image. The decrypted image is of better quality than the other approaches.

vii. PROGRESSIVE VISUAL CRYPTOGRAPHY:

The loss of contrast in the traditional Visual Cryptographic techniques degrades the quality of the decrypted secret image. Again the digital halftoning techniques used in traditional Visual Cryptography is of lossy nature and do not produce the original image after decryption. It produces a degraded image after decryption. Yan et al. [10] proposed a method wherein the grayscale and colored images are first transformed into monochrome images without the loss of any information. A much better reconstructed image is produced using their proposed technique with the existing Visual Cryptographic Techniques.

B. MULTIPLE SECRET SHARING SCHEMES:

Traditional Visual Secret Sharing schemes are used to share only one secret using several or minimum two shares. So, different researchers viz., Wu and Chen [11], Wu and Chang [12], Hsu et al. [13], Feng et al. [14], Shyu et al. [15] and Maged Hamada Ibrahim [16] came up with different methods to share several secrets in two shares or more.

i. WU AND CHEN'S VISUAL CRYPTOGRAPHIC SCHEME:

Wu and Chen [11] proposed a scheme to share two secrets using two shares. They used the rotation of the shares to different angles and then superimposing both to get the secret message. Their approach is as follows:

- Firstly, the secret messages are converted into two binary images.
- The first share is divided into four equal parts called areas. These areas contain equal number of any of the six patterns shown in Figure 4. The first area takes up patterns randomly and the other areas assign similar patterns corresponding to the position of the pattern in the first area.

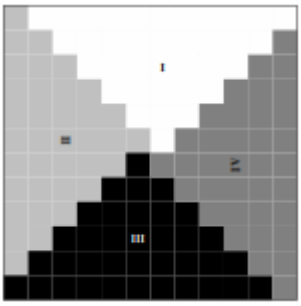


Figure 4: Division of a share into areas.

- To construct the second share they used the pattern corresponding to that in the first share and the table shown in Figure 5.
- In the decryption process, the first share is revealed by normally superimposing both the shares and the second secret is revealed by rotating the first share 90° counter clockwise and superimposing it on the second share.

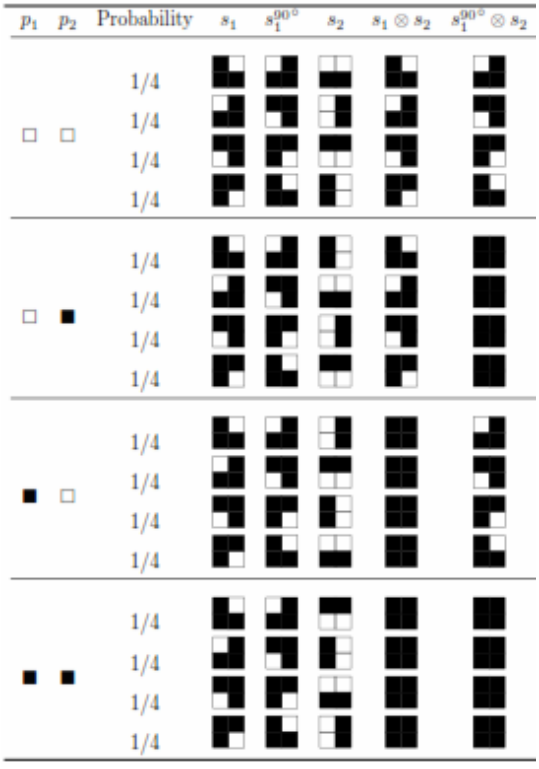


Figure 5: Wu and Chen's [12] Visual Secret Sharing Scheme.

ii. WU AND CHANG'S VISUAL CRYPTOGRAPHY:

The idea proposed by Wu and Chen [11] had a disadvantage of restricted rotation angles to 90°, 180° or 270°. Wu and Chang [12] overcame the restriction of angles by considering circular share. This made the rotation angle other than 90°, 180° or 270° feasible. Assuming an angle arbitrarily and two secret images S_1 and S_2, their proposed idea makes the circular shares A and B such that superimposing A and B will give S_1 and superimposing $A^{-\Theta}$ and B will produce S_2 where $0^o<\Theta<360^o$. They divided the circle into $360^o/\Theta$ areas and each area contains equal number of sector blocks. The sector blocks are selected from the patterns shown in Figure 6.

Figure 6: Patterns used for the sector blocks

The first share is divided into $360^o/\Theta$ areas. All the shares contain equal number of sector blocks. The first area is assigned with the random selection of sector blocks. The other areas are assigned with sector blocks according to the relation cited below:
Suppose a_j^1 is the j^{th} sector block of area 1 and a_j^2 is the j^{th} sector block of area 2 then the assignment of the sector block will be:

$$a_j^2 = \text{next}(a_j^1)$$

iii. RING SHADOW IMAGE TECHNOLOGY:

Another approach to overcome the rotation angle restriction of Wu and Chen [11] was proposed by Hsu et al. [13]. Their approach rolls the shares in the form of rings because it is easy to rotate at any arbitrary angle. The encryption and decryption of both the secrets are shown in the Figure 7, Figure 8 and Figure 9.

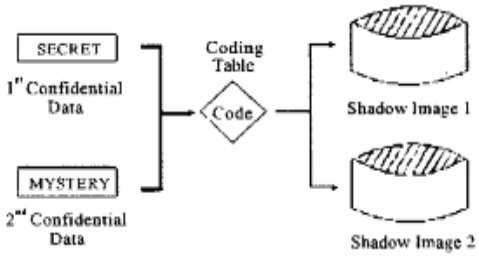


Figure 7: The encryption process

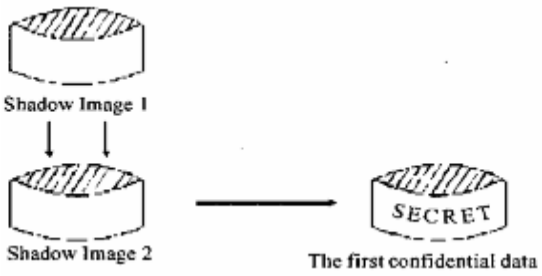


Figure 8: The decryption Process for the first secret.

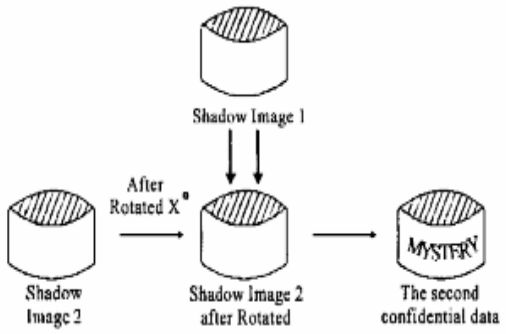


Figure 9: The decryption process for the second secret.

Suppose X is a factor of 360°. So, stacking the block at an angle (i×X)° of the first share and the block at an angle (i×X)° of the second share gives us the first secret. Stacking the block at an angle ((i+1)×X)° of the first share and the block at an angle (i×X)° of the second share will give us the second secret. According to the stacking relations, the rows are divided into different sets like for the first set, the encryption is done at angles 0°, X°, 2X°, . . . , (360°-X). For the next set the encryption will be done at positions right next to those in the first set.

iv. FENG ET. AL.'S SCHEME:

Feng et al. [14] proposed a scheme to share m secrets in two shares. These secrets are revealed at m aliquot angles. In their scheme the different sets formed according to the stacking relations are done for block in the first set at the angles:

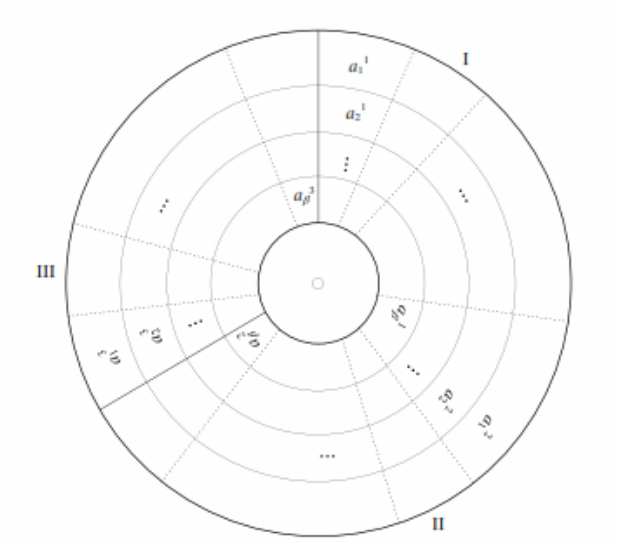
$0^o,\ 360^o/m,\ 360^o/m \times 2, \ldots., 360^o/m \times (m-1)$

These angles are used to form a graph. The vertices in this graph represent the share blocks in the positions and the edges represent the relation between the two blocks when they are stacked at some angles.

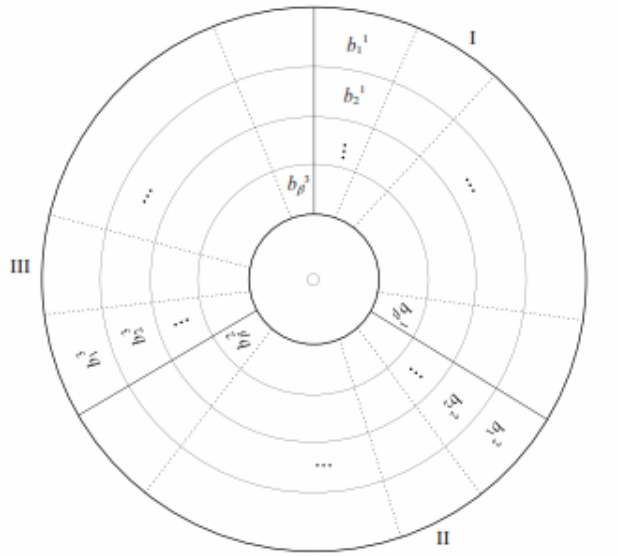
v. SHYU ET. AL.'S VISUAL CRYPTOGRAPHIC SCHEME:

The scheme proposed by Shyu et al. [14] shares S secrets (S≥2) using two shares. It considers circular shares into as many chord areas as the number of secrets. The angles to which each chord areas extend are given by $360^o/x$. Each chord area is divided into 2×x chord blocks. The chord areas are indexed clockwise. Suppose we consider x=3, then the 2×3 elementary blocks are shown in Figure 10. The chord areas are shown in Figure 11.

Figure 10: The elementary block considered in Shyu et al.'s scheme



(a)



(b)

Figure 11: decomposition of the shares into 2×3 chord areas (a) for the first share (b) for the second share

These elementary blocks contain only one white subpixel and five black subpixels each. They used permutation of the subpixels within the elementary blocks to ensure randomness in the shares. They represented the set of three blocks (a_j^1, a_j^2, a_j^3) as the related blocks of the three chords in the first share. Then the assignment of the other blocks in the chord of the first share is done as the permutation of the related block used. The angle of rotation will be $360^o/3=120^o$ as x=3(assumed).

While encoding the second share they divided the secrets viz., P_1, P_2, P_3 of size h×w evenly into β=h×(w/3) strips. Let $(P_i)_j^k$ denote the j^{th} pixel of the strip k in P_i and (P_1, P_2, P_3)$_j^k$ =($(P_1)_j^k$, ($P_2)_j^k$, $(P_3)_j^k$) be the j^{th} corresponding pixels of the strip k for (P_1, P_2, P_3). Then each block in the second share is assigned based on the related block (a_j^1, a_j^2, a_j^3) and the corresponding pixels (P_1, P_2, P_3)j^k in (P_1, P_2, P_3) according to the table in Figure 12.

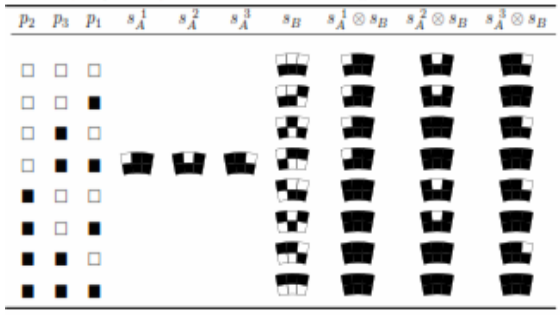


Figure 12: The overlapping of shares

vi. MAGED HAMADA IBRAHIM'S VISUAL CRYPTOGRAPHY:

Maged Hamada Ibrahim [16] proposed a scheme where he used traditional (*k*, *n*) Visual Secret Sharing Scheme or (*k*, *k*) Visual Secret Sharing Scheme to share *k* secrets. His scheme does not carry any extra overheads or pixel expansion than the existing Visual Secret Sharing Scheme used. The secrets are revealed by correctly sliding the shares to the right or left or upward or downward or even diagonal by one column. He used the shifting of the shares towards right to demonstrate his method. The proposed approach has a constraint on the size of the secret shared. If the first secret SI_o is of size *cr* pixels then the other secrets SI_j (1≤j≤k-1) should be of the size *(c-1)r* pixels. Each secret pixel is encoded using two subpixels and the shares are formed. The generalization algorithm is given below:

- Divide the n shares into g=$\lceil n/(k-1) \rceil$ groups. Each group contain at most k-1 shares. This ensures the "Orientation Uniqueness".
- Every share is marked with its group number and its number within the group. Let g_i be the number of the shares in group i.
- SI_o of size *cr* pixels is visible when any k or more shares are stacked together.
- Shares of group i are shifted to the right by i-1 columns will give SI_1.
- SI_q (2≤q≤k-1) of size *(c-gq)r* is revealed when shares q, . . ., g_i in each group in addition to all the shares in the group above them are shifted i-1 more columns to the right without undoing any previous shifts.
- If q≥g_i continue shifting share g_i.

III. COMPARISON

The table given in Figure 13 shows the comparison of some of the techniques discussed in this paper. The values that are being compared are the number of shares, type of image used, pixel expansion while constructing the shares, type of the shares that are formed.

Schemes	Number of secrets	Image type	Pixel expansion	Share type
Naor and Shamir [1]	1	Binary	4	Random
Droste [4]	1	Binary	4	Meaningful
Nakajima et al. [6]	1	Grayscale	m	Meaningful
Zhou et al. [8]	1	Binary	Q_1Q_2 (Q_1 ×Q_2 is the size of the shares)	Meaningful
Liu et al. [10]	1	Color	1	Random
Wu and Chen[12]	2	Binary	4	Random
Wu and Chang [13]	2	Binary	4	Random
Hsu et al. [14]	2	Binary	4	Random
Shyu et al. [15]	n (n≥2)	Binary	2n	Random
Feng et al. [16]	n (n≥2)	Binary	3n	Random
Maged Hamada Ibrahim[17]	n	Binary	2	Random

Figure 13 : Comparison table

IV. CONCLUSION

This paper provides an idea about the different Visual Cryptographic Schemes. Naor and Shamir [1] came up with this beautiful technique. The purpose of this technique is basically sharing secrets and ensuring authentication. It shares secrets among participants which are then visually decrypted. Hence it is also called Visual Secret Sharing Scheme. It can also be used during an authentication process along with the biometric authentication to make sure that the person desiring to gain information or get access to something important is authorized. Counting its advantages, Visual Cryptography stands as a suitable technique to share secrets with persons who are not aware of complex cryptographic computations.

REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," in *Proc. Eurocrypt'94*LNCS 950. 1995, pp. 1–12.

[2] G. Ateniese, C. Blundo, A. De Santis and D. R. Stinson, Visual cryptography for general access structures, *Inform. Computation*, Vol. 129, No. 2 (1996) pp. 86–106.

[3] G. Ateniese, C. Blundo, A. Santis, and D. Stinson, "Extended capabilities for visual cryptography," *ACM Theoretical Computer Science*, vol. 250, pp. 143–161, 2001.

[4] Stefan Droste, "New results on visual cryptography,"*CRYPTO '96 Springer-Verlag LNCS*, vol. 1109, pp. 401-415, 1996.

[5] D.S.Wang, F.Yi andX.B.Li,"On general construction for extended visual cryptography schemes," *Pattern Recognit.*, vol. 42, pp.3071–3082, 2009.

[6] M. Nakajima and Y. Yamaguchi, "Extended visual cryptography for natural images," in *Proc. WSCG Conf. 2002*, 2002, pp. 303–412.

[7] 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.

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

[9] C. C. Lin and W. H. Tsai, "Visual cryptography for gray-level images by dithering techniques," *Pattern Recognit. Lett.*, vol. 24, nos. 1–3, pp.349–358, Jan. 2003.

[10] F. Liu, C. K. Wu, and X. J. Lin, "Color visual cryptography schemes, "*IET Inf. Security*, vol. 2, no. 4, pp. 151–165, 2008.

[11] Jin, D., Yan, W. and Kankanhalli, M.S, "Progressive color visual cryptography", *Journal of Electron. Imaging (JIE/SPIE)*, vol.14 issue 3.

[12] L.H. Chen, C.C. Wu, "A Study on Visual Cryptography", Master thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, R.O.C., 1998.

[13] H. C. Wu and C. C. Chang, "Sharing visual multi-secrets using circle shares," *Comput. Standards Interfaces*, vol. 28, no. 1, pp. 123–135, Jul.2005.

[14] H.-C. Hsu, T.-S. Chen, and Y.-H. Lin, "The ringed shadow image technology of visual cryptography by applying diverse rotating angles to hide the secret sharing," Networking, Sensing and Control, vol. 2, pp. 996 – 1001, 2004.

[15] S. J. Shyu, S. Y. Huang, Y. K. Lee, R. Z. Wang, and K. Chen, "Sharing multiple secrets in visual cryptography," *Pattern Recognit.*., vol. 40, no.12, pp. 3633–3651, Dec. 2007.

[16] J. B. Feng, H. C. Wu, C. S, Tsai, Y. F. Chang, and Y. P. Chu, "Visual secret sharing for multiple secrets," *Pattern Recognit.*, vol. 41, no. 12, pp. 3572–3581, Dec. 2008.

[17] Maged Hamada Ibrahim, "New Capabilities of Visual Cryptography", *International Journal of Computer Science Issues(IJCSI), vol. 9,Issue 5, No. 1,pp. 225-231, September 2012.*

AUTHOR'S PROFILE

Anushree Suklabaidya received her B.E from Rural Engineering College, Bhalki affiliated to Visvesvaraya Technological University, Belgaum. She is currently pursuing her M.Tech from Birla Institute of Technology, Mesra. Her research interest includes information security, network security, image processing and pattern recognition.

G. Sahoo received his MSc in Mathematics from Utkal University in the year 1980 and PhD in the Area of Computational Mathematics from Indian Institute of Technology, Kharagpur in the year 1987. He has been associated with Birla Institute of Technology, Mesra, Ranchi, India since 1988, and currently, he is working as a Professor and Head in the Department of Information Technology. His research interest includes theoretical computer science, parallel and distributed computing, cloud computing, evolutionary computing, information security, image processing and pattern recognition.