

An Antiquity to the contemporary of Secret Sharing Scheme

Ms. K. CHITRA,
Research Scholar,
Department of Banking Technology,
School of Management, Pondicherry University,
Pondicherry -605014.
Email: chitrakrishnamoorthy07@gmail.com

Dr. V. PRASANNA VENKATESAN
Professor,
Department of Banking Technology,
School of Management, Pondicherry University,
Pondicherry -605014.
Email: prasanna_v@yahoo.com

Abstract: Secret Sharing (SS) scheme divides a secret image into shadow images (referred to as shares) in a way that requires the shadows in a certain privileged coalition for the secret reconstruction. However, the secret image cannot be revealed if they are not combined in a prescribed way. In this paper, the evolution of the traditional secret sharing scheme to the contemporary of secret sharing scheme has been presented based on its technology adoption. The basic comparison between the traditional secret sharing scheme and Visual cryptography is presented. The image-based share generation process has been explained in the context of pixel sharing patterns and its process. The reconstruction image is obtained by the XOR /OR Boolean operation. The threshold-based share generation schemes are explained mathematically and the comparative analysis of these schemes also presented.

Keywords: secret sharing, secret splitting, Visual cryptography, sharing scheme

1.Introduction

In early 1990's there was a tremendous growth in World Wide Web (WWW) which led to fling the multimedia content communication via a digital network. The delegacy of media in digital form alleviates its access. Multimedia is one such form it is the integration of various forms of media such as audio, video, image, text, software and animation, etc. Digital image is one of the most commonly used format globally. The enormous growth of digital image communication increases the need of image security. Digital image must be protected based on their sensitivity and confidentiality like bank documents, legal document, etc., which requires high security. In the current scenario, the data transmission is available online in the form of digital image. The digital image gives transparency to the user as well as the system, so there is a possibility of attacks made on the digital image. In order to

resolve the issues in data transmission using digital images cryptographic technique is required to secure the confidential information.

Cryptographic techniques are applied to uphold the confidential information for a safe and secure transfer of information. Most commonly used cryptographic techniques are Data Encryption (DE) (Horst Feistel, 1973), Secret Sharing (SS) Scheme (G. R. Blackely and A. Shamir, 1979), Private Information Retrieval (PIR) (Chor et al., 1998) and Homomorphic Encryption (HE) (Gentry, 2009). With the help of these techniques, the confidential information is protected while the data is being outsourced in the distributed storage system.

Among these techniques Private Information Retrieval and Homomorphic Encryption offer privacy but both of these techniques have some hitches like huge computational cost and latency (Kantarcigen and Clifton, 2005). Data Encryption technique lacks data security because this technique is still vulnerable to data loss, theft, and damage. Secret Sharing (SS) Scheme provides better data security and maintains the confidentiality as compared with other cryptography techniques.

Moreover, the SS scheme has low storage and computational costs. A Secret Sharing scheme is a vital technique for data outsourcing in a distributed file system which protects the information against data loss, damage, leakage, and destruction. The review of this paper presents the evolution of secret sharing scheme to the contemporary along with some essential points of secret sharing scheme.

2. Evolution of Secret Sharing Scheme in Visual Cryptography

The Secret Sharing (SS) scheme is a cryptographic technique, that access the sharing scheme based on cryptographic protocols. This cryptographic sharing protocols helps to protect the confidential information which was shared among the members. The SS scheme is a sharing protocol which maintains the increased level of security to the confidential information. All the members in the sharing scheme are allocated with a piece of data called 'share'. The secret image can be reconstructed by combining the sufficient number of shares together. The process responsible for share generation is called the 'dealer' and share reconstruction is called 'combiner'.

The SS scheme was independently introduced by Adi Shamir and George Blakley in 1979 (Adi Shamir, 1979; George Blakley, 1979). In their sharing scheme, Shamir demonstrates two types of shareholders: 'qualified' and 'forbidden'. The qualified shareholders are responsible for combining 't' shares among 'n' shares to reconstruct the secret. The forbidden shareholders have dummy shares that don't create the secret. Generally, Shamir's sharing scheme provides perfect secrecy for the secret during the reconstruction of shares.

The Blackley sharing scheme does the same sharing process but it fails to ensure secrecy about the secret. This happens due to the regeneration of partial information about the secret while recreating the shares. To ensure perfect secrecy in Blackley's scheme, it requires additional modification which was addressed by Ito in 1987 (Ito et al., 1987). They introduced (n, n) secret sharing scheme in general access structure. As compared to the earlier sharing scheme, this scheme brings the sharing process in matrix form and it gives a perfect structure for each generated share. Moreover, the earlier sharing scheme was based on polynomials and their intersection created more alignment problem as well as space insufficiency during computation.

In order to prevail against the space insufficiency, Moni Naor and Adi Shamir introduced another sharing scheme called ' $(2, 2)$ sharing scheme'. This sharing scheme creates a concept called 'Visual Cryptography' (Moni Naor and Adi Shamir, 1994). In visual cryptography (VC) shares are generated based on contrast level of the pixel. While this scheme fails in obtaining the contrast level when more number of share are shared and combined together. To overcome this problem ' $(2, n)$ sharing scheme' was introduced (C. Blundo et al., 1994). Even though improvement was made in the sharing scheme, it lagged to provide the perfect contrast proposition which was addressed by (Hofmeister et al., 2000). Hofmeister improved the contrast level and he tried to provide the perfect reconstructed image with perfect contrast.

All of the above mentioned authors focused mainly on the share generation, perfect reconstruction of shares and enhancement of contrast. These techniques were lacking the dimension of providing security to secret. This problem was addressed by (Tsai et al., 2001). He introduced the digital watermarking technique to the visual cryptographic concept (Praveena, A et al., 2016) to ensure the authenticity of the authorised person shares. Due to the new technology adoption, the combination of these two techniques faced alignment problem while reconstructing the shares to view the secret. To nullify the alignment problem in sharing scheme 'Boolean Operation' based share reconstruction process was introduced by (S. S. Lee et al., 2002). Hence, 'OR' based share reconstruction scheme was adopted by (Luckac Plataniotis et al., 2005) and 'XOR' based share reconstruction scheme was adopted by (Yang et al., 2006).

Spatial domain embedding process in digital watermarking techniques was introduced in visual cryptographic technique by (Surekha and Swamy, 2011). This concept ensured more security with less computation cost. The secret sharing schemes were distributed to cloud system so that they can distribute data to multiple servers. The sharing scheme in cloud is resistant to system failures caused by Natural disasters (or) Human error (K. Brindha and N. Jeyanthi, 2015) (Vinothkanna et al 2019). Initially, the SS scheme was distributed to cloud system to use secret sharing for health data in multi-provider clouds (Smys.S., et al 2019).

Later, these combination scheme was spread into sensor networks which was addressed by (Tapasi Bhattacharjee et al., 2018 and 2019). At present, the visual cryptographic technique is spread into

‘Augmented Reality’ (Ruofel Du et al., 2019) (Koresh, et al., 2019) which provides 3D effects and the communications are made virtually.

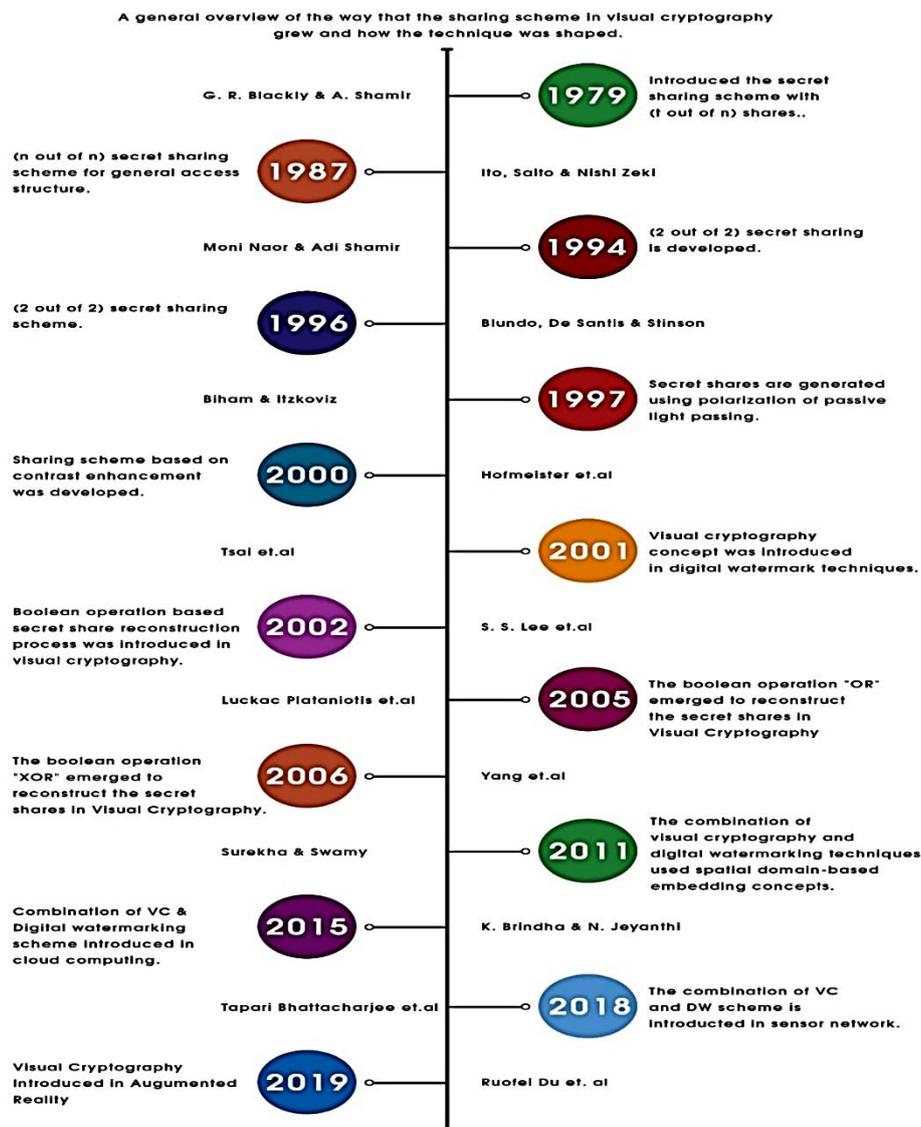


Figure 1. Timeline for secret sharing scheme in visual cryptography

This timeline Figure 1 shows secret sharing scheme from the antiquity to the contemporary. Based on this sharing scheme, many researchers contributed their concepts according to their needs and necessity.

3. Distinguish Between Secret Sharing Scheme and Visual Cryptography

For the past three decades the secret sharing scheme has improved tremendously for providing better image security. Adi shamir (Adi shamir, 1979) introduced SS scheme in the form of physical document to hide the information using transparent sheets. Later, Adi Shamir and Moni Naor improved the SS scheme for better security (Adi Shamir and Moni Naor, 1994). Due to the advancement in technology and adoption of electronic devices, the visual cryptography technique emerged to protect the digital information. The basic difference between the traditional secret sharing scheme and visual cryptography is shown in the comparison Table 1. Most of the major differences were addressed by (Stelvio Cimato and Ching-Nung Yang, 2012) which are mentioned in the tabular column.

Table 1 Comparison between Traditional Secret Sharing Scheme and Visual Cryptography

Traditional Secret Sharing Scheme	Visual Cryptography
The lesser amount of secret is embedded	It encrypts a huge amount of secret information
Codebook is required	Polynomial based sharing scheme in visual cryptography requires codebook.
Facing alignment problem while decrypting the secrets	Boolean operation-based decryption nullifies the alignment problem
The generation of shares is based on the threshold level	The generation of shares is based on binary values
Secret sharing scheme is derived from cryptographic concepts	Visual cryptography is derived from the secret sharing scheme
Cost of computing is high for transmitting and storing the information	Cost of computing is low while transmitting and storing the information.
The problem arises in a secret sharing scheme is Space-efficient, robustness, contrast, etc.	Contrast problem only arises in this scheme
Does the sharing process for text messages	Does the sharing process for images, later it spread into all multimedia contents.

4. Image-Based Share Generation Process

The image-based share generation process is called Visual Cryptography (Adi Shamir and Moni Naor, 1994). Visual Cryptography (VC) is a type of visual secret sharing scheme, which involves splitting of secret information into shares and the shares can be decrypted by imbricating the shares visually without computer assistance. The secret may be of any form in the digital world like audio, video, text, image, graphics, etc.

The shares are generated based on patterns. This pattern based sharing scheme was introduced by (Adi Shamir and Moni Naor, 1994) to obtain a better contrast level. Three types of sharing patterns were used in VC viz., Horizontal shares, Vertical shares, and Diagonal shares which are shown in the Figure 2. In horizontal sharing pattern, the information pixel is available either in the upper or lower half of the horizontal scale of the pixel. In the same way, the vertical sharing pattern also contains the information pixel either in left or right half of the pixel.

In diagonal sharing pattern, the information pixel is splits alternatively which provide better security as compared to other pixel sharing pattern schemes (C. C. Thien et al., 2004; C. Blundo et al., 2003; C. N. Yang and T. S. Chen, 2007 and 2008). Hence, most of the researchers in this field chose the diagonal sharing pattern for their research. The main advantage of using the diagonal pattern is that it doesn't give any clue to the hacker. Even though it is difficult to find the information contained in visual cryptography, horizontal and vertical information content is easy to identify the secret because it has information clue in sharing halves which reveals some truth about the secret as well as shares.

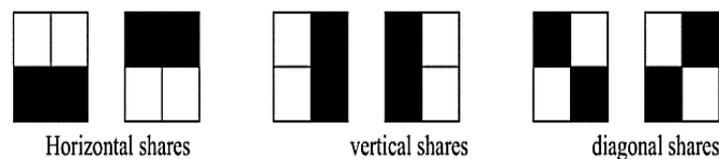


Figure 2 Moni Naor and Shamir's Sharing Patterns

In visual cryptography, the share generation and reconstruction process are carried out based on pixel color. If the selected pixel from the message block is white, then the user has to select any one of the sharing patterns from the visual cryptographic codebook. If the selected pixel from the message block is black, then the user has to select the complementary pair of patterns from the visual cryptographic codebook (Tzung-Her Chen et al., 2009). The Figure 3 shows various forms of share out patterns used in message blocks based on pixel colors.

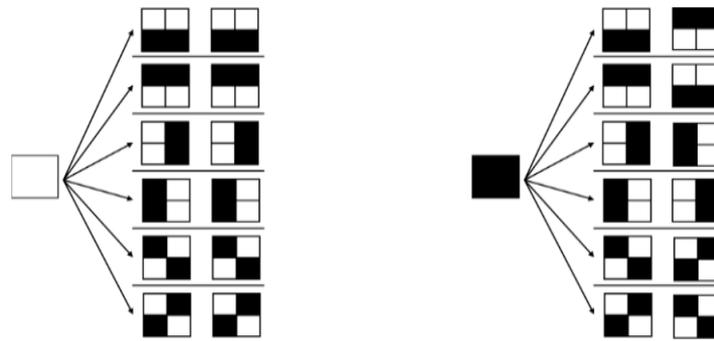


Figure 3 Wu and Chen's (2, 2) visual cryptographic schemes patterns

Based on the sharing patterns and the pixel share out schemes the secret image has been splitted which generates shares and these shares are overlapped using Boolean operation which reveals the secret image. The working process of the visual cryptographic concept is given as follows.

Assume letter 'M' as the secret image as shown in Figure 4. This secret image is taken for share generation using (2, 2) secret sharing scheme. According to this scheme, the user has to present both of his two shares to reveal the secret. Now move on to the share generation phase. The original image is divided into a number of blocks and that block is divided into number of pixels. The share generator randomly picks up any one of the pixels, for example, consider the topmost left corner pixel of an image. The considered pixel color is black color.

Based on the visual cryptographic rule, consider the black color as the binary value 1 i.e., the pixel value is '1'. Based on the share generation pattern chosen by the user, assume that the authorized person chooses a diagonal pattern. The diagonal pixel share generation pattern is applied which is clearly shown in the Figure 4. In the same way, all the pixel values are processed and this processed pixel generates the shares. This process takes place until all the pixels are decomposed.

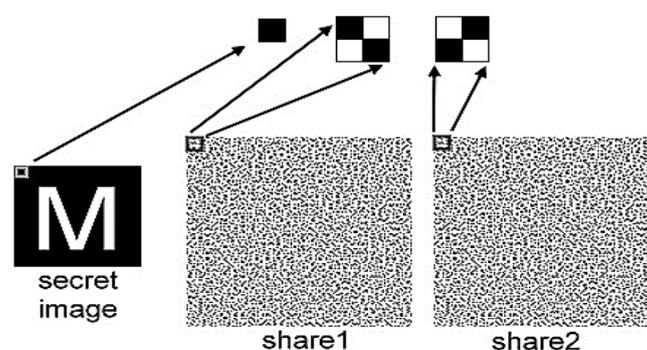


Figure 4 The working principle of Visual Cryptography

The secret information is reconstructed using Boolean operation, this operation reveals the secret by performing bit by bit Boolean operation while considering all the shares. The Boolean reconstruction of pixel using OR and XOR operation are shown in the Table 2. As compared to both the Boolean operation scheme XOR operation provides better contrast values than OR operation which was proved and demonstrated by the researcher (Punitha et al., 2010; Surekha and Swamy, 2011; Genm – dal park et al., 2014; Surekha et al., 2014; Neil buckely et al., 2015).

Table 2 Reconstruction of Pixels using OR and XOR Boolean operation

Secret Image	Shares	OR	XOR
White pixel (0)	$\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$
Black pixel (1)	$\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$

5. Threshold Based Share Generation Schemes in Visual Cryptography

A predefined sub-collection of shares which contains the whole secret in some form is called an *Allowed coalition*. Allowed coalition is also referred in the literature by other names too, such as authentic collection, qualified collection or authorized set. This technique follows a procedure which allows only a qualified collection of the subgroup is able to reconstruct the secret. The qualified collection was accomplished by ‘t’ number of subgroups or more than ‘t’ (for threshold). Such a subgroup is called (t, n) threshold scheme, ‘t’ and ‘n’ is called as the threshold level.

Threshold-based sharing scheme was initially propounded by Adi Shamir and Moni Naor (Adi Shamir and Moni Naor, 1994). Later many researchers came into existence and created many threshold based sharing schemes. This section mainly focuses on the most commonly used threshold-based sharing scheme, which is explained clearly with mathematical notations. The secret sharing scheme based on threshold level has been categorized into four forms. The chronological order of threshold based sharing schemes are shown in the Figure 5.

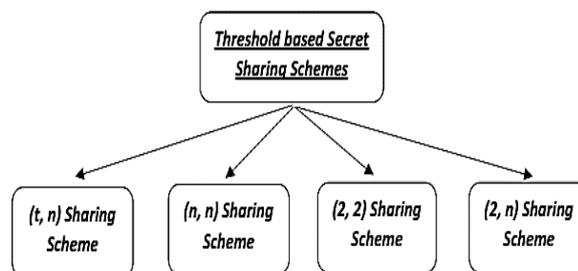


Figure 5 Threshold-based Sharing Schemes as per chronological order

5.1. (t, n) threshold sharing scheme

This secret sharing scheme dispenses a secret amid ‘n’ participants in such a way that only ‘t’ number of participants’ shares will reconstruct the secret, but any (t-1) or fewer participants do not gain any information about the secret.

Sharing schemes are usually set up by a reliable expert who works out all the available shares and dispersed amid the participants via communication channels. The reliable expert who fathom the scheme is called a “dealer”. The members grip their shares until some of them choose to puddle their shares and reconstruct the original secret information.

The retrieval of the secret is done by combining the shares from reliable experts. Assume, that the letter K having secrets from the set belongs to S.

Let S_i be the set from which the dealer pulls for the participants ρ_i , $i= 1, 2, \dots, n$. the set of entire participants $P = \{ \rho_1, \rho_2, \dots, \rho_n \}$. A (t, n) is the assortment of two algorithms they are:

- i. Dealer
 - ii. Combiner
- i. Dealer**

$$D: K \rightarrow S_1 \times S_2 \times \dots \times S_n$$

In dealer, assign shares to each and every members who are responsible for clandestine $k \in K$ and the share $s_i \in S_i$ is communicated through a safe network to every participant ρ_i who are all involved in the sharing process. If the entire shared sets S_i are identical then just say that $S_i \in S$.

- ii. Combiner**

$$C: S_{i_1} \times S_{i_2} \times \dots \times S_{i_j} \rightarrow K$$

In combiner, it proceeds a random collection of shares and tries to figure out the original secret information. Combiner recuperates the secret fruitfully only when all shares are combined together will generates the value which is greater or equal to t ($j \geq t$). If the condition stated above statement is true, then the share will not assign to anyone. Similarly, the information about the secret will not reveal by anyone and the secret will be retained.

(2, n) sharing scheme is similar to (t, n) sharing the difference in this scheme is, ‘t’ number of shares is required to reconstruct the secret for (t, n) scheme. But in (2, n) scheme it requires only 2 shares to reconstruct the secret among the ‘n’ number of shares and the remaining process are same as in the (t, n) sharing scheme.



5.2 (n, n) threshold sharing scheme

Let us consider the integer ‘K’ be given secret, the dealer has to select modulus ‘p’ can be any integer that integer must be greater than the integer ‘K’ which decides the security factors. If the dealer randomly selects (t-1) elements from the set $S = \{S_1, S_2, S_3, \dots, S_{t-1}\}$ then it belongs to Z_p . The equation for the share S_t is given as,

$$S_t = K - \sum_{i=1}^{t-1} S_i \pmod{p}$$

The shares are dispersed safely to the participants from the set $P = \{\rho_1, \rho_2, \dots, \rho_t\}$. At the time of reconstruction, all the secret shares are required to reconstruct the information which is given as,

$$K = \sum_{i=1}^t S_i \pmod{p}$$

For any (t-1) or less number of shares doesn't reveal any approximate information about the secret K.

(2, 2) sharing scheme is similar to (n, n) sharing. The difference is instead of taking ‘n’ number of shares for both the dealer and combiner, only two number of shares are required to generate this scheme and the remaining process are remains same as (n, n) sharing scheme.

6. Comparative Analysis of Threshold-Based Sharing Scheme

The conceptual view of threshold-based sharing scheme is discussed in the previous section. In this section, the comparative analysis of threshold-based sharing scheme as per their chronological order is discussed in Table 2.3. The major differences are addressed by (Stelvio Cimato and Ching-Nung Yang, 2012; Jonathan Weir and Weiqi yan, 2012; B. Mahalakshmi and C. C. Christiyana, 2014) which is mentioned in the Table 3.

Table 3 Threshold-based sharing scheme comparison

Sharing Scheme	Contrast Level		Pixel Expansion	Security	Remarks
	XOR	OR			

(t, n)	high	low	2:1	Moderate	Need more memory space but it provides a higher quality of the reconstructed image
(n, n)	high	moderate	2:1	High	Managing shares is difficult which increases the time complexity.
(2, n)	high	low	1:2	Moderate	Provide optimal contrast level.
(2, 2)	High	moderate	1:1	High	Absolutely secure and no share image leaks any secret information of the original image.

Table 3 compares the major problems faced by the sharing scheme while data transmissions such as contrast level, pixel expansion, and security. Among the compared schemes, (2, 2) sharing scheme provides better security, less pixel expansion, and the XOR-based share reconstruction creates a higher level of contrast.

7. Discussion

A general overview of the way the sharing scheme in visual cryptography grew and how the technique has shaped are discussed elaborately. The major difference between the traditional secret sharing scheme and visual cryptography is highlighted in the Table 1.

The general working process of image based share generation and reconstruction process is explained. A threshold based visual cryptography sharing scheme hierarchy is developed as per the chronological order, and its characteristics like contrast level, pixel expansion and security are comparatively analyzed.

The problems faced by threshold based share generation process are comparatively analyzed and its problems are highlighted.

8. Conclusion

The evolution of a secret sharing scheme is presented in the form of a timeline. In order to get a better understanding of the secret sharing scheme, the working principles of sharing scheme, sharing patterns

are derived from the literature and it is presented. The overview of the secret sharing scheme is carried out in various ways.

References

- [1] Feiste H. (1973) SCIENTIFIC. Sci Am a Div Nat Am Inc.; 228(5):15-23.
- [2] Bhattacharjee T, Maity SP, Islam SR (2018). Hierarchical secret image sharing scheme in compressed sensing. *Signal Process Image Communication*; 61(October 2017):21-32. Doi:10.1016/j.image.2017.10.012
- [3] Bhattacharjee T, Rout RK, Maity SP (2017). Affine Boolean classification in secret image sharing for progressive quality access control. *Journal Information Security Applications*; 33:16-29. Doi:10.1016/j.jisa.2017.01.001
- [4] BLAKLEY GR (2019). Safeguarding cryptographic keys. 313-318. Doi:10.1109/mark.1979.8817296
- [5] Blömer J. (2011), How to share a secret. *Algorithms Unplug*, 159-168. Doi: 10.1007/978-3-642-15328-0_17
- [6] Blundo C, Santis A De, Gargano L, Salerno U. (2014), Secret Sharing Schemes with Veto Capabilities.
- [7] Brindha K, Jeyanthi N. (2015), secured document sharing using visual cryptography in cloud data storage. *Cybernetic Information Technology*. 15(4):111-123. Doi: 10.1515/cait-2015-0058
- [8] Buckley N, Nagar AK, Arumugam S. (2015), On real-valued visual cryptographic basis matrices. *Journal of Universal Computer Science*; 21(12):1536-1562.
- [9] Chen T, Chang C, Wu C, Lou D. (2009), On the security of a copyright protection scheme based on visual cryptography. *Computational Standard Interfaces*; 31:1-5. Doi:10.1016/j.csi.2007.09.001
- [10] Chor B, Goldwasser S, Baruccl A. (1985), Verifiable Secret Sh ~ Iring and Acclieving Silnllll ~ Illeity in the Presence of Falllts; (1):383-395. Doi:10.1109/SFCS.1985.64
- [11] Christiyana CC. (2014), A Secure Authentication Method for Grayscale Document Images; 2(March).
- [12] De Santis A, Ferrara AL, Masucci B. (2017), Visual cryptography schemes with reversing, *Visual Cryptography Secret Image Sharing*; 51(6):255-279. Doi: 10.1201/b11068
- [13] Du R, Li D, Varshney A. (2019), Geollery: A mixed reality social media platform. *Conference Human Factors Computational System - Proc.* ;(1):1-2. doi:10.1145/3290605.3300915
- [14] Gentry C. (2009), Fully Homomorphic Encryption Using Ideal Lattices. *Proceeding Annual ACM Symp Theory Computer*: 169-178. Doi:10.1145/1536414.1536440
- [15] Hofmeister T, Krause M, Simon HU. (1997), Contrast-optimal k out of n secret sharing schemes in visual cryptography. *Lecturer Notes Computer Science (including Subser Lecturer Notes Artificial Intelligent Lecturer Notes Bioinformatics)*; 1276:176-185.
- [16] Ito M, Saito A, Nishizeki T. (1989), Secret sharing scheme realizing general access structure. *Electron Communication Japan (Part III Fundamental Electron Sci.)*; 72(9):56-64. Doi:10.1002/ecjc.4430720906
- [17] Lee SS, Na JC, Sohn SW, Park C, Seo DH, Kim SJ. (2002), Visual cryptography based on an interferometric encryption technique. *ETRI J.*; 24(5):373-380. Doi:10.4218/etrij.02.0102.0505

- [18] Lukac R, Plataniotis KN (2005). Bit-level based secret sharing for image encryption. *Pattern Recognition*; 38(5):767-772. Doi:10.1016/j.patcog.2004.11.010
- [19] Park G, Kim D. (2014), Lossless Codebook-Based Digital Watermarking Scheme with Authentication. Doi:10.1109/ITNG.2014.43
- [20] Punitha S, Thompson S, Siva Rama Lingam N. (2010), Binary watermarking technique based on visual cryptography. *IEEE International Conference Communication Control Computer Technology ICCCT 2010*. : 232-235. Doi:10.1109/ICCCCT.2010.5670557
- [21] Qing S, Hideki I, Wang G. (2014), *LNCS 4861 - Information and Communications Security*. 2007; May. Doi: 10.1007/978-3-642-34129-8
- [22] Surekha B, Swamy GN. (2011), A Spatial domain public image watermarking. *International Journal Security its Applications*; 5(1):1-12.
- [23] Surekha B, Swamy GN, Rao KS, Kumar AR. (2016), A Watermarking Technique based on Visual Cryptography.
- [24] Tsai CS, Chag CC, Chen TS. (2002), Sharing multiple secrets in digital images. *Journal System Software*; 64(2):163-170. Doi: 10.1016/S0164-1212(02)00034-1.
- [25] Weir J, Yan WQ. (2009), Image hatching for visual cryptography. *IMVIP 2009 - 2009 International Mach Visual Image Processing Conference*; 8(September):59-64. Doi:10.1109/IMVIP.2009.18
- [26] Wu YS, Thien CC, Lin JC. (2004), Sharing and hiding secret images with size constraint. *Pattern Recognition*; 37(7):1377-1385. Doi:10.1016/j.patcog.2004.01.002
- [27] Yang CN, Chen TS. (2007), Extended visual secret sharing schemes: Improving the shadow image quality. *International Journal Pattern Recognition Artificial Intelligence*; 21(5):879-898. Doi: 10.1142/S0218001407005740
- [28] Naor M, Shamir A. (1994), Visual Cryptography. *IEEE Explore*.
- [29] Koresh, Mr H. James Deva. "Computer vision based traffic sign sensing for smart transport." *Journal of Innovative Image Processing (JIIP)* 1, no. 01 (2019): 11-19.
- [30] Lukac R, Stanco F, Battiato S, Gallo G, Lezoray O, Grady L. (2012), Digital Imaging and Computer Vision Series Digital Imaging for Cultural Heritage Preservation: Analysis, Restoration, and Reconstruction of Ancient Artworks, *Image Processing and Analysis with Graphs: Theory and Practice*.
- [31] Vinothkanna, Mr R. "A secure steganography creation algorithm for multiple file formats." *Journal of Innovative Image Processing (JIIP)* 1, no. 01 (2019): 20-30.
- [32] Praveena, A., and S. Smys. "Efficient cryptographic approach for data security in wireless sensor networks using MES VU." In *2016 10th international conference on intelligent systems and control (ISCO)*, pp. 1-6. IEEE, 2016
- [33] Smys, S. "Energy-aware security routing protocol for wsn in big-data applications." *Journal of ISMAC* 1, no. 01 (2019): 38-55.