

## coding and zigzag scanning

Yelisela Rajesh<sup>1</sup>, Dr.Guruprakash.CD<sup>2</sup>,B.Sarath Chandra<sup>3</sup>

<sup>1</sup> Research scholar, Dept. of CSE, Visvesvaraya Technological University, Belagavi.

<sup>2</sup> Professor, Dept. of CSE, SSIT, Maralur, Kunigul road, Karnataka.

<sup>3</sup> Assistant Professor, Dept. of CSE, PSCMR College of Engineering & Tech, Vijayawada, AP

Emails: <sup>1</sup>rajeshrajiv1324@gmail.com; <sup>2</sup>cdguruprakash@gmail.com; <sup>3</sup>sarathit862@gmail.com

**Abstract**— Recently, the transmission of data through network is increasing rapidly, which provides instant access or distribution of digital data. Secret information 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. Many secure and confidential data items like military maps and commercial identifications are sent over the internet. While using secret documents (images, text etc.) for sending over the network, the security issue is to be taken into consideration, since there is a chance of stealing the secret information by the hackers due to weak link in the public network. In order to deal with the security issue of secret information, we are in need of an appropriate secure algorithm by which we can secure our data over the internet. With the help of Visual Cryptography, the system visual information can be securely sent over the internet.

**Keywords:** Visual cryptography, Security, Watermarking

### I. INTRODUCTION

It is the art of sending and receiving encrypted messages that can be decrypted only by the sender or the receiver. Encryption and decryption are accomplished by using mathematical algorithms in such a way that no one but the intended recipient can decrypt and read the message. VCS secret sharing scheme was introduced by Naor and Shamir [8], 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. The major feature of their scheme is that the secret image can be decrypted simply by the human visual system without having to resort to any complex computation [9,10]. Main feature of visual

cryptography scheme (VCS) is that it does not need mathematical computation to get the original secret [11,12]. During the past decade, Visual Secret Sharing (VSS) has attracted the attention of many researchers. Some of the literature has been related to the construction of a visual secret scheme [13, 14]. Based on the concept of sharing

binary secret images, researchers have extended the visual secret sharing scheme to suit the sharing of gray secret images [15, 16, 17, 18] and color secret images [19, 20, 21, 22].

There have been numerous cases of including in secret information sharing and Detection. Secret sharing techniques belong to the larger area of information hiding that includes watermarking [23, 24]. Recursive hiding of secrets is proposed in [25, 26, 27-29]. The idea involved is recursive hiding of smaller secrets in shares of larger secrets with secret sizes increasing at every step. While the scheme presented in [25] is a non-threshold scheme, schemes in [26, 27-29] are threshold schemes. Similarly, in color visual cryptography the shares generated is colorful. The visual secret sharing binary secret is explained in [30]. In terms of the number of share secret images, the literature has been solely concerned with sharing only one secret image. However, it would be useful to be able to share more than one secret image simultaneously. Clearly, it would be worthwhile to develop a visual secret sharing scheme for multiple secrets.

### II. LITERATURE SURVEY

Various secret sharing techniques have been proposed in the literature using visual cryptography and their explanations are listed in this section. Peng Li et al. [1] have explained the Sharing more information in gray visual cryptography scheme. Visual cryptography scheme (VCS) shares a binary secret image into several binary shadows and the secret image can be visually revealed by stacking qualified shadows without computation. From the point of view of sharing secret information, VCS was not efficiency because of the large size expansion and low visual quality. Here, they explained a general gray visual cryptography scheme, which was share more information, called Sharing More Information Gray Visual Cryptography Scheme (SMIGVCS). All the shadow pixels of VCS embed additional information to generate gray shadows of SMIGVCS, and the embedded information comes from the shadows of a polynomial-based secret sharing scheme (PSSS). In the revealing process, a vague secret image is visually decoded by stacking qualified shadows, and more information was revealed by computation.

Moreover, Yu-Chi Chen *et al.* [2] have analyzed the definition of cheating prevention and presented a

authentication based cheating prevention scheme. This scheme was constructed with Naor-Shamir's VC scheme. They developed an authentication based cheating prevention scheme which was constructed with Naor-Shamir's 2-out-of-n visual cryptography. The proposed scheme adopted the black patterns especially inserted into the verified stacking result. It was also proven to prevent cheating in practice. The number of the black patterns was used to check whether a share transparency was fake or not. Finally, the proposed scheme is more efficient and effective to prevent cheating than previous schemes.

Additionally, Sanjay Rawat *et al.* [3] have presented a robust copyright protection scheme based on fractional Fourier transform (FrFT) and visual cryptography (VC). Unlike the traditional schemes, in our scheme, the original image was not modified by embedding the watermark into the original image. They used the visual secret sharing scheme to construct two shares, namely, master share and ownership share. Features of the original image were extracted using SVD, and were used to generate the master share. Ownership share was generated with the help of secret image (watermark) and the master share, using VC technique. The two shares separately give no information about the secret image, but for ownership identification, the secret image was revealed by stacking the master share and the ownership share. In order to achieve the robustness and security, the properties of VC, FrFT and SVD were used in their scheme. The experimental results showed that the developed scheme was strong enough to resist various signal processing operations.

In [4], Duanhao Ou *et al.* have explained the Non-expandable XOR-based visual cryptography scheme with meaningful shares. XOR-based visual cryptography (VC), a brand-new type of VC, was suitable for solving the low image quality and alignment problems in VC system. However, meaningless share and pixel expansion remain to be continuing challenges in existing XOR-based VC. To fix those mentioned defects, XOR-based VC with meaningful shares was introduced here. A basic algorithm implemented by a simple image matrix for constructing a  $(n,n)$  XOR-based VC was first explained. In the following stage, a  $(n,n)$  XOR-based VC with meaningful shares was investigated by adopting the basic algorithm, where the meaningful share was directly generated without extra process. Extensive experimental results were demonstrated, exhibiting the effectiveness and advantages of the method. Further, sufficient theoretical proofs were provided for illustrating the correctness of the proposed XOR-based VC.

Likewise, Jung-San Lee *et al.* [5] have explained the Preserving user-friendly shadow and high-contrast quality for multiple visual secret sharing techniques. Traditional secret sharing scheme that encrypts secret image based on mathematical calculation to construct shadows often requires the complicated computation to extract the secret. Later on, conventional visual cryptography scheme was developed to

deal with the perplexed calculation in encryption and extraction of previous schemes. The stack-to-see technique was used easily to reveal the secret by human visual system, which was shorten computation time. However, the expansion of image size and the noise-liked shares of previous schemes lead to the difficulty in transmission and storage. Here, uses a pre-defined codebook to encode two secret images into two meaningful transparencies without pixel expansion. According to the turning mechanism, two secret images were embedded into two shares simultaneously. The decryption process allows the user to get two secrets via turning and stacking.

Moreover, M. Jenila Vincent and E. Angeline Helena [6] have explained the Securing Multiple Color Secrets Using Visual Cryptography. Visual secret sharing was an encryption methodology that allows retrieving the secret image where the secret image was cryptographically encoded into shares. The  $(n,n)$  visual secret sharing scheme proposed by Naor and Shamir was used to encrypt the secret image into  $n$  shares and by stacking the shares together, the secret was retrieved back. Color visual cryptography deals with color images as secret, where the color secrets are embedded into  $n$  shares. In this paper, they explained a  $(2,2)$  color visual secret sharing scheme for multiple color secrets based on Wu and Chen's code book. An experimental result was shown that the methodology retrieves multiple color secrets by stacking under various rotation angles.

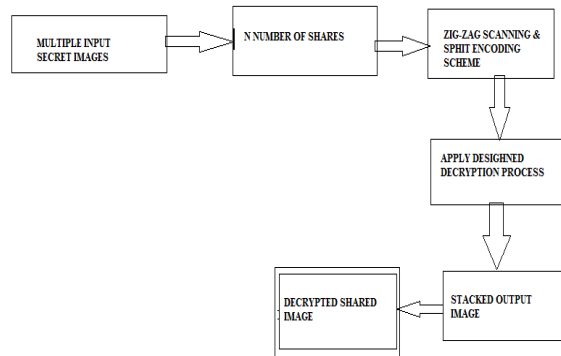
### III. PROPOSED METHODOLOGY

#### A. Objective Formulation-

The primary objective of my research is to design and develop an algorithm for visual cryptography with the incorporation of fraudulent detection of wrongly shared images. Accordingly, the problem is formulated as follows: Two input secret data should be revealed after sharing it with multiple persons with the criteria of detection of the fraudulent share if it happens at the stacking end.

Based on the objective formulated, an algorithm will be developed for visual cryptography along with the detection of fraudulent shares. At first, multiple input secret images will be divided into  $n$  number of shares. Then,  $n$  shares will be given to the encoding algorithm, and which will be done by making use, zigzag scanning, and SPIHT encoding scheme. Once we obtain the multiple shares through the proposed encoding procedure, the stacked output image will be obtained using the designed decryption process that will produce the decrypted share image. Finally, multiple visual secret images will be obtained from decrypted share image. The implementation will be done using MATLAB and the performance of the proposed system will be analyzed with the existing system. Proposed scheme yields Experimental

results which is feasible and efficient. Proposed scheme is more efficient and effective to prevent cheating than previous schemes.



- Step-1: Multiple Input secret images of form JPEG.  
 Step-2: Make 'N' number of shares of images.  
 Step-3: Apply Zig-Zag scanning and SPHIT encoding Scheme.  
 Step-4: Apply designed decryption process for the output produced from step-3.  
 Step-5: Create stacked output image.  
 Step-6: output will be in decrypted shared image.

#### IV. CONCLUSION & FUTURE WORK

My research is to design and develop an algorithm for visual cryptography with the incorporation of fraudulent detection of wrongly shared images. An algorithm will be developed for visual cryptography along with the detection of fraudulent shares. The implementation part will be done using MATLAB and the performance of the proposed system will be analyzed with the existing system.

#### REFERENCES

- [1] Peng Li, Ching-Nung Yang, Qian Kong, Yanpeng Ma and Zheng Liu, "Sharing more information in gray visual cryptography scheme", Journal of Visual Communication and Image Representation, Vol. 24, no. 8, pp. 1380-1393, 2013.
- [2] Yu-Chi Chen, Du-Shiau Tsai, Gwoboa Horng "A new authentication based cheating prevention scheme in Naor-Shamir's visual cryptography", J. Vis. Commun. Image R., Vol.23, pp.1225-1233, 2012.
- [3] Sanjay Rawat, Balasubramanian Raman, "A blind watermarking algorithm based on fractional Fourier transform and visual cryptography", Signal Processing, Vol.92, pp.1480-1491, 2012.
- [4] Duanhao Ou, Wei Sun and Xiaotian Wu, "Non-expandable XOR-based visual cryptography scheme with meaningful shares", Signal Processing, vol.108, pp. 604-621, 2015.
- [5] Jung-San Lee, Chin-Chen Chang, Ngoc-Tu Huynh and Hsin-Yi Tsai, "Preserving user-friendly shadow and high-contrast quality for multiple visual secret sharing technique", Digital Signal Processing, Vol. 40, pp.131-139, 2015.
- [6] M. Jenila Vincent and E. Angeline Helena, "Securing Multiple Color Secrets Using Visual Cryptography", Procedia Engineering, Vol. 38, pp.806-812, 2012
- [7] Bharanivendhan N and Amitha T, "Visual Cryptography Schemes for Secret Image Sharing using GAS Algorithm", International Journal of Computer Applications, Vol. 92 – No.8, 2014
- [8] M. Naor and A. Shamir, "Visual cryptography," in Proc. EUROCRYPT'94, Berlin, Germany, 1995, vol. 950, pp. 1-12, 1995.
- [9] G. Ateniese, C. Blundo, A. De Santis and D. R. Stinson, "Visual cryptography for general access structures," Information and Computation, Vol. 129, pp. 86-106, 1996
- [10] C. Blundo and A. De Santis, "Visual cryptography schemes with perfect reconstruction of black pixels", Computer Graphics, Vol. 22, No. 4, pp. 449-455, 1998
- [11] Wu C., Chen L., "A study on visual cryptography," Master's thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, R.O.C., 1998
- [12] Naor M., Shamir A., "Visual cryptography, Advances in Cryptology" EUROCRYPT '94. Lecture Notes in Computer Science, vol.950, pp. 1-12, 1995.
- [13] hen, Y. F., Chan, Y. K., Huang, C. C., Tsai, M. H., & Chu, Y. P., "A multiple-level visual secret-sharing scheme without image size expansion," Information Sciences, Vol.177, pp.4696-4710, 2007.
- [14] Yang, C. N., "New visual secret sharing schemes using probabilistic method," Pattern Recognition Letters, Vol.25, pp.481-494, 2004
- [15] Wang, D., Zhang, L., Ma, N., & Li, X., "Two secret sharing schemes based on Boolean operations," Pattern Recognition, Vol.40, pp.2776-2785, 2007.
- [16] Iwamoto, M., & Yamamoto, H., "The optimal n-out-of-n visual secret sharing scheme for gray-scale images," IEICE Transaction Fundamentals, vol.10, pp.2238-2247, 2003.
- [17] Wang, D., Zhang, L., Ma, N., & Li, X., "Two secret sharing schemes based on Boolean operations. Pattern Recognition, Vol.40, pp.2776-2785, 2007.
- [18] Yang, C. N., & Chen, T. S., "New size-reduced visual secret sharing schemes with half reduction of shadow size," IEICE Transaction Fundamentals, E89-A(2), pp.620-625, 2006.
- [19] Chang, C.C., Lin, C.C., Le, T.H.N., & Le, H.B., "A new probabilistic visual secret sharing scheme for color images", Intelligent information hiding and multimedia signal processing. In IHMSP '08 international conference on August 15-17, pp. 1305-1308, 2008.
- [20] Hou, Y. C. (2003), "Visual cryptography for color images," Pattern Recognition, Vol.36, pp.1619-1629.
- [21] Shyu, S. J., "Efficient visual secret sharing scheme for color images," Pattern Recognition, Vol.39, pp.866-880, 2006
- [22] Yang, C. N., & Chen, T. S., "Colored visual cryptography scheme based on additive color mixing," Pattern Recognition, Vol.41, pp.3114-3129, 2008.
- [23] Kafri, O and Keren, E. "Encryption of pictures and shapes by random grids," Optics Letters, No.12: pp.377-379, 1987.
- [24] Naor, M. and Shamir, A. "Visual cryptography," Advances in Cryptography-Eurocrypt, 950: pp.1-12, 1995.
- [25] Gnanaguruparan, M. and Kak, "Recursive Hiding of Secrets in Visual Cryptography", Cryptologia, vol 26, pp. 68-76, 2002.
- [26] Parakh, A. and Kak, "A Recursive Threshold Visual Cryptography Scheme", Cryptology ePrint Archive, Report 2008/535.
- [27] Parakh, A. and Kak, S. 2010. A Tree Based Recursive Information Hiding Scheme. To appear in proceedings of IEEE ICC 2010 – Communication and Information System Security Symposium („ICC'10 CISS"), May 23-27, Cape Town, South Africa.
- [28] Parakh, A. and Kak, S. Recursive Secret Sharing for Distributed Storage and Information Hiding, Advanced Networks and Telecommunication Systems (ANTS), IEEE 3rd International Symposium on, pp. 1-3, 14.

