A Survey On Visual Secret Sharing Scheme

Sameer. N. Rajput[1], Krunal J. Panchal[2]

[1]*Research Scholar, Information & Technology Department, L.J. Institute of Engineering & Technology, Gujarat, India*
[2] *Assistant Professor, Information & Technology Department, L.J. Institute of Engineering & Technology, Gujarat, India*

ABSTRACT

Visual secret sharing scheme is mostly used for secret communication technique. visual secret sharing technique Used for secret sharing that encrypt a secret image into many shares These share are encoded or are transparencies and stored into digital form. There are various criteria which decide the performance of visual secret sharing scheme like type and number of shares pixel expansion, security accuracy, computational complexity, share generated is meaningful or meaningless, type and numbers of secret images encrypted by the scheme. These share are reveal the secret image to supposed to be printed on transparences and after stacking them to each other. This paper focus and analyze of different visual secret sharing technique with respect to application and pros and cons of technique is also present.

Keywords :- *Visual secret sharing, meaningless shares, meaningful shares*

---

1. INTRODUCTION:

Visual secret sharing scheme is important technique for image security. Visual secret sharing schemes, encrypt the visual secret into share and distribute or transfer over any secure or unsecure communication channel. The secret image reconstructed without any decryption algorithm use. The superimposed shares generates the secret that can be recognized by the humans visual system.

A visual secret sharing scheme divide the secret into n shares, and using these share the secret can be decrypted, but no information can be revealed using n-1 shares. The generated shares are printed in the transparency for visibility and the original secret can be reconstructed by overlapping the shares without any complex computation.

Noar and Shamir [1] proposed vss scheme where the original image reconstructed without any decryption algorithm use or any additional computation. This is a perfect scheme with easy computations. it is also extended to visual images for k out of n scheme, where the dealer divide and distributes the transparency to all the n users; and the secret can be reveal by stacking any k shares. By stacking (k-1) share no information can be retrieve about it.

Daoshun wang,feng yi and xiaobo li [2] presented a new idea for processing grey and color images without any pixel expansion. K or more share generate the image but no information details can be reveal by stacking less number of shares than k. Even disqualified shares along with good shares also does not retrieve the secret.

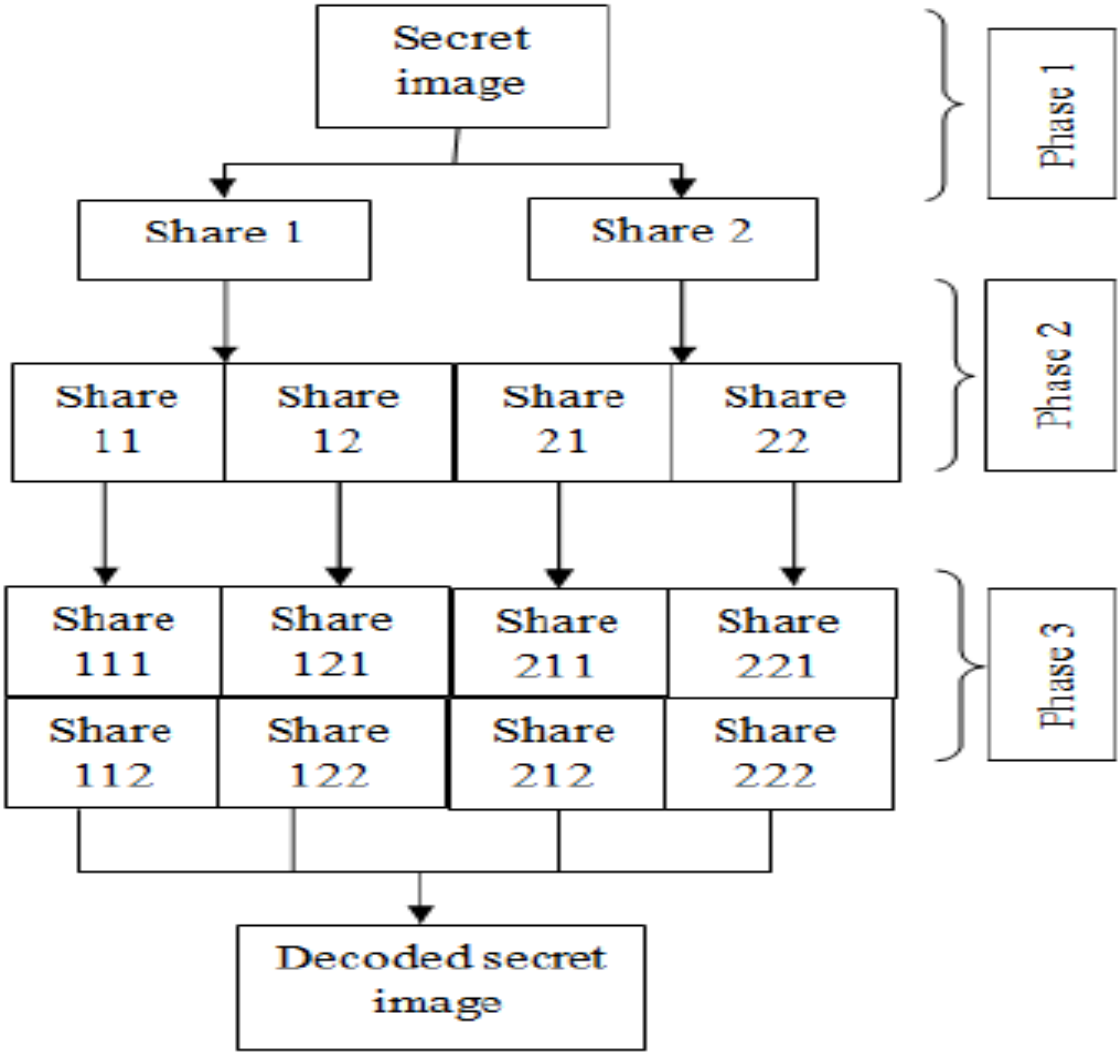

Fig. 1 Hierarchical Visual Cryptography Scheme [5]

Young-chang hou and zen-yu quan [3] proposed that the secret image can be construct by using less of k or more number of shares, but secret image are not retrieved with lesser than k shares. Similarly, progressive visual secret sharing construct the secret image step by step where superimposing more share gives original results. If minimum number than less number of shares are staked then only the outline of the secret image could be obtained. As the number of shares increases, the detail of constructed secret image information also increases progressively.

2. LITERATURE REVIEW:

2.1 An Efficient Tagged Visual Cryptography for Color Images

- In [4] R.M.Shiny,P.Jayalakshmi,A.Rajakrishnammal,T.Sivaprabha Abirami paper, In this paper proposes a tagged visual cryptography for color images, where the secret image is divided into two base shares based on the traditional visual secret sharing scheme. The generated base shares are stamped with the tag pattern using the probabilistic visual secret sharing scheme to obtain the tagged shares. One of the main advantage of

using tag patterns is providing the participants with augmented information to identify the relevant shares among the numerous shares. During retrieve the tag patterns are obtained by folding up the individual tagged shares. Superimposing the shares outcome in the secret color image which retains its original size thus ensuring no pixel expansion.

2.2 Hierarchical Visual Cryptography for Grayscale Image

- In [5] Trupti Patel, Rohit Srivastava Paper, In this paper we are applying Hierarchical Visual Cryptography Scheme on gray image instead of binary image. So, generated shares are gray share, not binary shares that are generated by the binary image. Here we are using the new proposed gray share generation algorithm for generation of n number of shares. Here original image is encrypted in to n number of levels so security of original image is more improved. At decryption side all n shares must have to participate to reveal the original secret. Decrypted image has same size and better visual quality then original secret image.

2.3 A (2,2) Secret Sharing Scheme for Visual Cryptography without Pixel Expansion

- In [6] Mahmoud E. Hodeish, Dr. V. T. Humbe, Secret sharing scheme a method by which a secret image can be distributed between a number of participants, whereby each participant is collected a piece of the secret. This piece of the secret is known as a share. The original secret image can be only be generated when a required minimum number of shares are combined together. In this paper, a *(2,2)* VCS has been proposed, where two adjacent pixels are taken together as the one time input for generation of shares. The simulation shows that after comparing the proposed method with conventional VCS, the proposed method has non-distortion (with respect to Aspect Ratio and Pixel Expansion) and the visual quality of reconstructed image is better (with respect to PSNR)..

2.3 Visual Cryptography using Image Pixel Transparency with Cover Image

- In [7] Dipesh Shrestha, Sanjeeb Prasad Panday, Transparencies of pixels of the shares can be used to reveal the secret image. The pixels of shares can be generated randomly or the cover image can be used to generate the first share. The encrypted shares generated using cover image seem to be visually less similar to those generated without using cover image. Also, on the basis of image similarity between shares and original image, further encryption of encrypted shares can be performed. Comparison of the outcomes when cover image is used and when not used to generate shares, shows that the latter is more sensitive to the transparency factor (alpha) than the former encouraging the use of properly selected cover image for visual cryptography using pixel transparency.

2.5 An Optimal (k,n)Visual Secret Sharing Scheme for Information Security

- In [9] Mahmoud E. Hodeisha, Linas Bukauskasb,Vikas T. Humbe, based on the concept of Visual Secret Sharing (VSS) scheme proposed by Naor and Shamir in 1994, many of schemes have been proposed to protect the security of binary image. Yet, the problems of pixel expansion, extensive codebook designs, and lossy recovery are still unsolved. The current paper attempts to propose a new (k,n) scheme to refute the pixel expansion based on codebook and transpose of matrices. This scheme will offer promising solutions for the security condition, computation complexity, storage requirement, fast network transmission, and reconstructing the secret image accurately without any distortion..

2.6 A Novel Visual Cryptographic Scheme For Improved Binary Image Quality

- In [8] . Arya K.,Rakhee BAIJU, Sreenarayan N. M, Lakshmi M, Nimisha Mohan, Visual secret scheme is an encryption method which shares secret information divided into n shares and decrypted into original image without any cryptographic algorithm or technique. Existing visual secret sharing scheme does not provide good visual quality reconstructed image. Hence a novel visual cryptography is introduced along with additional post processing technique which provide good quality recovered image. Experimental results on this technique show that recovered image has competitive visual quality compared with input binary image.

3. COMPARATIVE TABLE:

Table -1: Comparative Table

Paper Title	Methods/Techniques	Advantages	Disadvantages
An Efficient Tagged Visual Cryptography for Color Images	Halftoning Process using Floyd and Steinberg	advantage of using tag patterns is providing the participants with augmented information to identify the relevant shares among the numerous shares	the the quality gets reduced
Hierarchical Visual Cryptography for Grayscale Image	1 gray share generation algorithm 2 Hierarchical Visual Cryptography Scheme	the visual quality is improved and size of original secret image and decrypted image is same	Work On Grey Scale Images Only
A (2,2) Secret Sharing Scheme for Visual Cryptography without Pixel Expansion	1 Share generation 2 A random column-permutation	1To consume less battery power for increasing life time of the power continuation 2 To reduce the computational complexity	
Visual Cryptography using Image Pixel Transparency with Cover Image	Image transparency	increases the efficiency in terms of share image size and quality of regenerated image	it is sensitive to transparency factor (alpha) chosen
An Optimal (k,n)Visual Secret Sharing Scheme for Information Security	codebook matrics	solve the problem of pixel expansion and the lossy of recovered image	

A Novel Visual Cryptographic Scheme For Improved Binary Image Quality	novel visual Cryptography	improves the quality of reconstructed binary image.	pixel expansion problem not solve

4. CONCLUSION:

Among various advantages of Visual Cryptography Schemes is the property that VCS decoding relies purely on human visual system, which leads to a lot of interesting applications in private and public sectors of our society. Visual Cryptography is used with short messages, therefore giving the cryptanalyst little to work with.
It can be used with other data hiding techniques to provide better security.

5. REFERENCES:

[1]. M. Naor and A. Shamir,"Visual cryptography, "Advances in Cryptography: EUROCRYPT'94, LNCS" , vol. 950, pp. 1–12, 1995

[2]. Daoshun Wang,Feng Yi and Xiaobo li, "Probabilistic visual secret sharing schemes for grey scale images and color images,2011",Information Sciences181(2011)

[3]. Young-Chang Hou and Zen-Yu Quan, "Progressive Visual Cryptography",J.Electron.Imag(2011).

[4] R.M.Shiny,P.Jayalakshmi,A.Rajakrishnammal,T.Sivaprabha AbiramiR"An Efficient Tagged Visual Cryptography for Color Images" 2016 IEEE International Conference on Computational Intelligence and Computing Research.

[5]Trupti Patel, Rohit Srivastava "Hierarchical Visual Cryptography for Grayscale Image" 2016 Online International Conference on Green Engineering and Technologies (IC-GET).

[6]. Mahmoud E. Hodeish, Dr. V. T. Humbe "A (2,2) Secret Sharing Scheme for Visual Cryptography without Pixel Expansion "International Conference on Electrical, Electronics, Signals, Communication and Optimization (EESCO) – 2015.

[7]. Dipesh Shrestha, Sanjeeb Prasad Panday "Visual Cryptography using Image Pixel Transparency with Cover Image" 2015 9th International Conference on Software, Knowledge, Information Management and Applications (SKIMA).

[8]. ARYA K.,RAKHEE BAIJU, SREENARAYANAN N. M, LAKSHMI M, NIMISHA MOHAN , SOUMYA M. K, ASWATHY A.S, RESHMI K.C. "A Novel Visual Cryptographic Scheme For Improved Binary Image Quality" International Conference On Information Communication And Embedded System(ICICES 2016).

[9] Mahmoud E. Hodeisha, Linas Bukauskasb,Vikas T. Humbe "An Optimal (k, n)Visual Secret Sharing Scheme for Information Security" 6th International Conference On Advances In Computing & Communications, ICACC 2016, 6-8 September 2016, Cochin, India.