ISSN:0975-9646

# Watermarked LTVC Scheme

Aswathy. S
*M.Tech Student, Department of Computer Science and Engineering*
*Sarabhai Institute of Science and Technology*
*Vellanad, Trivandrum, Kerala, India*

***Abstract***— **Security has gained a lot of importance as information technology is widely used. The main issue in visual cryptography is quality of reconstructed image. This problem is overcome by using "Watermarked LTVC scheme". In this method the quality of reconstructed image is higher, compare with conventional visual cryptographic scheme. The secret image is converted into shares, that means black and white pixel images. Each share is embedded to different carrier images. Invisible watermarking method is used for embedding carrier image and shares. For security, the invisible watermarked shares are then encrypted, AES modified encryption method is used. The encrypted shares are send to other participants. At the receiver end receiving the shares and decrypt the shares, then combining these shares together reveal the secret. The quality of rejoined shares and original secret shares are almost same. The loss of image quality is less compared to other visual cryptographic schemes.**

***Keywords***— **LTVC: Lossless Tagged Visual Cryptography; Embedding; Watermarking; Shares; AES modified encryption.**

## I. INTRODUCTION

Cryptography refers to the study of mathematical techniques and related aspects of Information security like data confidentiality, data Integrity, and of data authentication. Visual cryptography was originally invented and pioneered by Moni Naor and Adi Shamir in 1994 [3] at the Euro crypt conference. Visual cryptography is ''a new type of cryptographic scheme, which can decode concealed images without any cryptographic computation". As the name suggests, visual cryptography is related to the human visual system. Visual cryptography is regularly used for image encryption. The text data is converted to image format and use that textual data as image. Encryption starts with the use of secret sharing concepts where the secret image is split into shares which are noise-like and secure. These images are then transmitted or distributed over an entrusted communication channel. Recognition of a secret message from overlapping shares and the secret image is decrypted without additional computations or cryptography knowledge. Visual cryptography schemes are characterized by two parameters: the expansion corresponding to the number of sub pixels contained in each share and the contrast, which measures the "difference" between black and white pixels in the reconstructed image. Combined the shares together reveal the information. Minimum two shares are needed for revealing the secret image. The shares are treated as black and white pixel; (n, n) matrix is used for representing black and white pixel. White is represented as "0" and black pixel is represented as "1". Fig. 1 illustrates a computer simulation result of a basic (2, 2) VC sharing example, where panel (a) is the secret image with text "VC," and panels (b) and (c) are the two generated shares. Each share consists of noisy black dots, and is two times the size of the original image. The result of superimposing the two shares is shown in panel (d), on which the secret text "VC" is revealed and can be recognized using naked eye. The performance of a VC scheme is usually characterized in terms of the pixel expansion and the contrast. Pixel expansion is the number of pixels in a share used to encode a pixel of the secret image, and contrast represents the luminance difference between the area of black pixels and the area of white pixels in the stacked image.

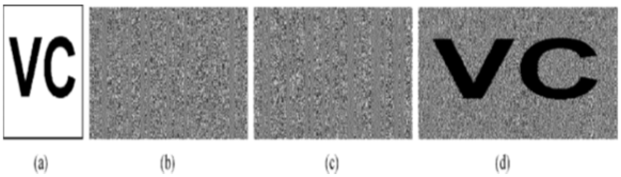

Fig. 1. Computer simulation of a (2, 2) VC scheme. (a) Secret image. (b) Share1. (c) Share 2. (d) The superimposing result of the two shares.

In the fig 1 the decoded image quality is less compared to the original secret image this problem can be overcome by using "watermarked LTVC scheme". The lossless TVC (LTVC) scheme which hides multiple secret images without affecting the quality of the original secret image. As a result, the decoder can rebuild exactly the identical secret image as that of conventional VC. In other words, the shares are losslessly modified to hide the tag images. The shares are watermarked first, an improved image watermarking invisible LSB embedding method, then the embedded image is encrypted by using AES modified encryption method. Using this encryption the security of share is increased.

### *A.* Secret Sharing

A secret is something which is kept from the knowledge of any but the initiated or privileged. Secret sharing defines a method by which a secret can be distributed between a group of participants, whereby each participant is allocated a piece of the secret. This piece of the secret is known as a share. The secret can only be reconstructed when a sufficient number of shares are combined together. While these shares are separate, no information about the secret can be accessed. That is, the shares are completely useless while they are separated.Within a secret sharing scheme, the secret is divided into a number of shares and distributed among n persons. When any k or more of these persons (where k ≤ n) bring their shares together, the secret can be recovered. However, if k - 1 persons attempt to reconstruct the secret, they will fail.

### *B*. Image Sharing

Image sharing is a subset of secret sharing because it acts as a special approach to the general secret sharing problem. The secrets in this case are concealed images. Each secret is treated as a number; this allows a specific encoding scheme supplied for each source of the secrets. Without the problem of inverse conversions, the digits may not be interpreted correctly to represent the true meaning of the secret.

Image sharing defines a scheme which is identical to that of general secret sharing. In (k, n) image sharing, the image that carries the secret is split up into n pieces (known as shares) and the decryption is totally unsuccessful unless at least k pieces are collected and superimposed. When the k shares are stacked together, the human eyes do the decryption. This allows anyone to use the system without any knowledge of cryptography and without performing any computations whatsoever. This is another advantage of visual cryptography over the other popular conditionally secure cryptography schemes. The mechanism is very secure and very easily implemented. An electronic secret can be shared directly; alternatively the secrets can be printed out onto transparencies and superimposed, revealing the secret.

## II. RELATED WORKS

Ran –Zan Wang and Shuo-Fang Hsu, proposed a method for implementing visual cryptography (VC) in which an additional tag is attached to each generated share. The proposed ,tagged visual cryptography (TVC)[2] scheme works like a traditional VC scheme does, where the original image is encoded in shares in such a way that the secret can be revealed by superimposing any or more shares, but knowledge of less than shares gets no secret information. A notable characteristic of TVC is that an extra tag can be revealed by folding up each share, which provides users with supplementary information such as augmented message or distinguishable patterns to identify the shares. The tagging property can easily be applied to any reported VC scheme to endow the generated shares with more capabilities. A common characteristic of both traditional VC and extended VC schemes is that a single share carries no useful information to users. In this letter, a method to endow VC schemes with the ability of displaying tag patterns by folding up a single share is proposed. The tagging property enriches new functions to the target shares. For example, it can display fake message to establish a cheating mechanism to unauthorized inspectors, or the tag pattern can exhibit unique symbol associated with each sharing instance, and provide a user-friendly environment for users to distinguish among and manage to the numerous shares. The proposed method is simple and can easily be applied to any reported VC schemes.

Visual secret sharing for multiple secrets[5].Conventional visual secret sharing schemes are designed for a single secret image so it is inefficient to generate numerous share images for multiple secret images simultaneously. Therefore, a novel visual secret sharing scheme for multiple secret images is proposed in this scheme. In the proposed encryption process, a stacking relationship graph of secret pixels and share blocks is generated to indicate the encryption functions, and a set of visual patterns is defined to produce two share images according to this graph. Based on the stacking properties of these patterns, the secret images can be obtained from the two share images at aliquot stacking angles. In this scheme makes the number of secret images not restricted and further extends it to be general. As a result, the proposed scheme enhances visual secret sharing schemes' ability for multiple secrets. In visual cryptography mainly images are handled, shares are embedded with another carrier images.

The visual cryptography scheme (VCS) is a secure method that encrypts a secret image by breaking it into shares. A distinctive property of VCS is that one can visually decode the secret image by superimposing shares without additional computation .The method presents an approach for embedding visual cryptography generated image shares in the host images to provide authentication for the VC shares and makes these secret shares invisible by embedding them into host images. The secret shares generated from VC encryption are watermarked into some host images using digital watermarking. Digital watermarking is used for providing the double security of image shares. The share is embedded into the host image in frequency domain using Discrete Cosine Transform (DCT). In frequency domain, the obtained marked image must be less distorted when compared to the original image. Thus secret shares are not available for any alteration by the adversaries who try to create fake shares. Every pixel of the binary Visual cryptography share is invisibly embedded into the individual block of the host image. The process of watermark extraction necessitates only the watermarked image and it does not require the original host image.

The scheme provides more secure and meaningful secret shares that are robust against a number of attacks like blurring, sharpening, motion blurring etc. There are various innovative ideas and extensions exist for the basic visual cryptographic model. In the existing VC schemes no security is provided to the secret shares and adversaries can alter its bit sequences to create fake shares. And in the proposed scheme, the vulnerability of these binary secret shares is overcome by hiding them invisibly into some host images. During the decryption phase, the secret shares are extracted from their cover images without needing any of the cover image characteristics because the watermark extraction technique is blind. The overlapping of these shares reveals the secret. The decoded secret image quality is improved.bIn recent works, the data will embedded to secret shares and send embedded data images to other participants. The other related work is decoded image quality is increased and the security of share is improved by using watermarking methods.

## III. PROPOSED SYSTEM

A lossless tagged visual cryptography scheme is one of the most efficient multi-secret visual cryptography (MVC) schemes, the tagged visual cryptography (TVC) is capable of hiding tag images into randomly selected shares. The encoding processes of TVC and other MVC schemes bring distortion to shares, which definitely lowers the visual quality of the decoded secret image. To overcome this lower quality problem new method is proposed, an extended TVC scheme, named as lossless TVC (LTVC). [1] Specifically, *lossless* means that the proposed LTVC scheme encodes the tag image without affecting the rebuilt secret image, i.e., the decoded secret image of LTVC has the same visual quality with that of the conventional VC scheme. Moreover, the probabilistic LTVC (P -LTVC) to solve the potential security problem of LTVC. In this thesis work the lossless tagged visual cryptography is applied in watermarking of compressed images.

Wang and Hsu proposed a tagged VC (TVC) [2] scheme in which more secret images can be revealed by the folding up operation. Specifically, when fold up a share along its midline, an additional secret image is visually presented. Obviously, the folding up operation is easier for participants. However, both MVC and TVC scheme have a problem that they inevitably bring distortion to the shares of conventional VC. Consequently, the secret image disclosed by stacking the shares in MVC or TVC has lower quality than that of Naor and Shamir's conventional VC.

To deal with this problem, a new method proposes a lossless TVC (LTVC) scheme which hides multiple secret images without affecting the quality of the original secret image. As a result, the decoder can rebuild exactly the identical secret image as that of conventional VC. In other words, the shares are losslessly modified to hide the tag images. This losslessy tagged shares are embedded with a carrier image, LSB embedding is used the watermarked shares are encrypted next and send the shares to other users. AES modified encryption is used. AES to ensure improving the encryption performance; mainly for images characterized by reduced entropy. The implementation of both techniques has been realized for experimental purposes.

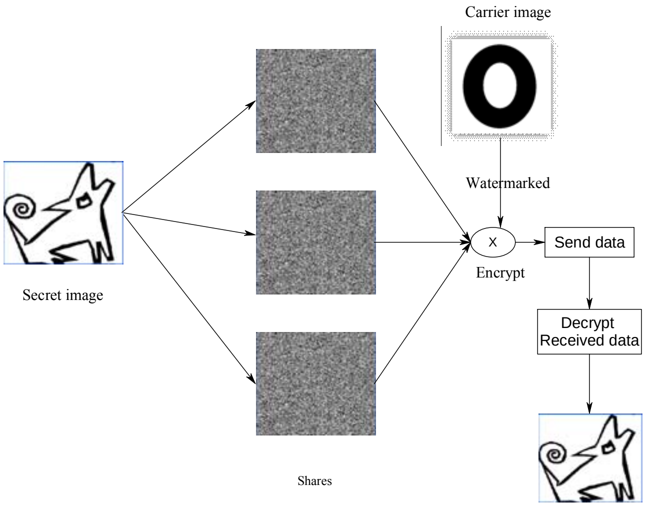

Fig 3.1System Architectural Diagram Representation

In this fig 3.1 the secret image is divided into shares and each share is embedded with a carrier image and the watermarked image is encrypted, then the image send to other participants. Then decrypt the image and reveal the information about the secret.

### *A.* Image Preprocessing

Select image from different source, then the image will be categorized. The data will be image or text, the text data converted into image format and then processed. The width and height of image is checked and resize the image if the size of image exceeds the system required image size. In visual cryptography the images are handled like black and white pixels. The selected images are categorized into two types carrier image and secret image. The images are first histogram based classifies and then the images are converted into black and white pixel using gray scale conversion. In image processing and photography, a color histogram is a representation of the distribution of colors in an image. For digital images, a color histogram represents the number of pixels that have colors in each of a fixed list of color ranges that span the image's color space, the set of all possible colors.

The color histogram can be built for any kind of color space, although the term is more often used for three-dimensional spaces like RGB or HSV. For monochromatic images, the term intensity histogram may be used instead. For multi-spectral images, where each pixel is represented by an arbitrary number of measurements (for example, beyond the three measurements in RGB), the color histogram is N-dimensional, with N being the number of measurements taken. Each measurement has its own wavelength range of the light spectrum, some of which may be outside the visible spectrum. If the set of possible color values is sufficiently small, each of those colors may be placed on a range by itself; then the histogram is merely the count of pixels that have each possible color.

### *B.* Share Construction

In this proposed scheme the secret image is divided into shares. The original image is divided into different shares such that each pixel in the original image is replaced with a non-overlapping block of two subpixels. Anyone who holds only one share will not be able to reveal any information about the secret. To decode the image, each of these shares is xeroxed onto a transparency. Stacking both these transparencies will permit visual recovery of the secret. In this module the secret image is selected and the white pixels in the image will be removed first and then each black pixels in the image is replaced to different shares. The shares will be stacked together then reveal the secret. For more security embedding the shares with a carrier image.

### *C.* Embedding Data

The carrier image is embedded with shares invisible watermarking ,LSB embedding is used. Least Significant Bit (LSB) embedding is a simple strategy to implement steganography. Like all steganographic methods, it embeds the data into the cover so that it cannot be detected by a casual observer. The technique works by replacing some of the information in a given pixel with information from the data in the image. While it is possible to embed data into an image on any bit-plane, LSB embedding is performed on the least significant bit(s). This minimizes the variation in colors that the embedding creates. For example, embedding into the least significant bit changes the color value by one. Embedding into the second bit-plane can change the color value by 2. If embedding is performed on the least significant two pixels, the result is that a color in the cover can be any of four colors after embedding. Steganography avoids introducing as much variation as possible, to minimize the likelihood of detection. In a LSB embedding, always lose some information from the cover image. This is an effect of embedding directly into a pixel. To do this we must discard some of the cover's information and replace it with information from the data to hide. LSB algorithms have a choice about how they embed that data to hide. They can embed losslessly, preserving all information about the data, or the data may be generalized so that it takes up less space. The embedded data will encrypted for more security, AES modified Encryption is used. Then the encrypted data is send.

### *D.* Extracting Data

At the receiver side the share will be received. The secret data is extracting from the embedded image. The decryption process for extracting carrier image and secret image is done, then reveal the secret. Extract the image from each document D.

## I V. CONCLUSION

Visual cryptography (VC) is a process where a secret image is encrypted into shares which refuse to divulge information about the original secret image. The secret image can be recovered simply by stacking the shares together. In conventional VC at the decoding time the quality of original image will be reduced. This problem is overcome by using A lossless tagged visual cryptography scheme, which is one of the most efficient multisecret visual cryptography (MVC) schemes. Specifically, *lossless* means that the proposed LTVC scheme encodes the tag image without affecting the rebuilt secret image. Security of sahares improved by using LSB embedding and AES encryption methods.

## ACKNOWLEDGEMENT

This work was supported in part by the Department of Computer Science & Engineering, SIST, Trivandrum. I would like to show my gratitude to Dr. C G Sukumaran Nair (HOD), Associate Professor, Ms. Sudha SK and Associate Professor, Mrs. Renji S, for their valuable guidance.

## REFERENCES

[1] A Lossless tagged visual cryptography scheme ,Xiang Wang, *Member ,IEEE,* Qingqi Pei, ,*Member ,IEEE,* and Hui Li

[2] R.-Z. Wang and S.-F. Hsu, "Tagged visual cryptography," *IEEE Signal Process. Lett.*, vol. 18, no. 11, pp. 627–630, 2011

[3] M. Naor and A. Shamir, "Visual cryptography," in *Advances in Cryp-tology–EUROCRYPT 1994, ser. Lecture Notes in Computer Science*, A. De Santis, Ed. Berlin/Heidelberg, Germany: Springer, 1995, vol. 950, pp. 1–12.

[4] Y. C. Hou, "Visual cryptography for color images," *Patt. .Recognit.*, vol. 36, no. 7, pp. 1619–1629, 2003.

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

[6] S.-J. Shyu and K. Chen, "Visual multiple secret sharing based upon turning and flipping," *Inf. Sci.*, vol. 181, no. 15, pp. 3246–3266, Aug. 2011.

[7] Jagdeep Verma, Dr.Vineeta Khemchandani," A Visual Cryptographic Technique to Secure Image Shares"*International Journal of Engineering Research and Applications* (IJERA) Vol. 2, Issue 1,Jan-Feb 2012, pp.1121-1125.

[8] Y.Bani, Dr.B.Majhi and R.S.Mangrulkar, 2008. A Novel Approach for Visual Cryptography Using a Watermarking Technique. *In Proceedings of 2nd National Conference, IndiaCom 2008.* Computing for national development, February 08-09, New Delhi.

[9] G.R. Blakley, Safeguarding cryptographic keys, in: Proceedings of the National Computer Conference, vol. 48, NJ, USA, 1979, pp. 313–317

[10] Anandhi and S.Satthiyaraj,"Embedded Visual Cryptography Schemes for Secret Images", *IJCSNS International Journal of Computer Science and Network Security,* VOL.12 No.12, December 2012

[11] Mr. Rohith S,Mr. Vinay G/ A NovelTwo Stage Binary Image Security System Using (2,2) Visual Cryptography Scheme./*International Journal Of Computational Engineering Research* /ISSN: 2250–3005.