ISSN 2319 – 7595
Volume 8, No.2, March - April 2019
International Journal of Information Systems and Computer Sciences
Available Online at http://warse.org/IJISCS/static/pdf/file/ijiscs17822019.pdf
https://doi.org/10.30534/ijiscs/2019/17822019

# Visual Cryptography: An Encryption Method To Encrypt Multiple Images Using Shares

**Sheeba Ann Thomas[1]Rincy Roy Oommen[2]Smita C Thomas[3]**
1sheebaannthomas@gmail.com 2rincyroy@gmail.com 3smitacthomas@gmail.com
[123]Department of computer science and engineering
[123]Mount Zioncollege of engineering, Kadamanitta, Pathanamthitta, India

**ABSTRACT**

Cryptography is the main pillars of information security. By the arrival of internet, its usage and usefulness has exploded. Cryptography means storing and transmitting data in a form that only targeted people can read and process. It is also an effective way of protecting sensitive data that is stored on media devices or transmitted over an unsecured network communication channel by encrypting it into an unreadable format. Visual cryptography is a cryptographic technique used to encodes a black and white secret image into n shadow image called shares and these shares are distributed among n participants and only qualified subset of participants can visually recover the secret image. DCT is used in the proposed system. It has two encryption methods: lossy encryption and lossless encryption. Lossless encryption is more appropriate because it preserves every single detail in the image.It reduces the transmission risk problem and the quality of image is retained.

**Key words :** Cryptography, Visual Secret Sharing, Embedding, Visual Cryptology.

## 1.INTRODUCTION

Visual Cryptography is a cryptographic technique used to protect the image. An image was broken up into n shares so that, someone with all the n shares could decrypt the image, while any n-1 shares revealed no information about the original image. Each share was printed on separate transparencies and decryption was performed by overlapping the shares. When all the n shares were overlaid, the original image would appear. Secret Sharing defines a method by which a secret can be distributed between a group of participants whereby, each participant is allocates a piece of secret. This piece of secret is known as shares.

A secret is something which is kept from the knowledge of any but the initiated or privileged. 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 $k \leq n$) bring their shares together, the secret can be recovered. However, if k - 1 persons attempt to reconstruct the secret, they will fail. 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.

## 2.LITERATURE SURVEY

VCS is a method of encryption. It is used to hide the secret information in images.In traditional VCS, the images are encrypted into n number of shares. These shares are distributed among n number of participants. The secret image can be recovered simply by stacking the shares without any complex computation. Previous approach a security, pixel expansion and noise problem. In thisproposed system, it has two phases, it has a sender side and receiver side. At sender, the input secret image generates for meaningless shares based on GAS algorithm. In second phase, the cover images are added in each share directly by using stamping algorithm. Then, distribute the embedded images to participants. At the receiver side, the embedded images can be processed to extract the cover images from shares [1]. The secret image can be retrieved

by overlapping the shares in correct order. Password authentication is provided by sender and receiver. It has high security and increase the shares count and reduce the problem of pixel expansion. The transmission of data through this network get increased day by day. Secret sharing is an important technology in the field of communication. However, security can be improved by using password, hiding image, water marking etc., But it has some disadvantages that is the secret image can be protected in single information carrier, if it is lost, then the information carrier is destroyed. To overcome this, VCS was introduced and the secret is split into n number of shares and transmit to n number of participants. The traditional VCS takes secret image as input and shares as output. It must satisfy two conditions. It has a qualified subset and forbidden subset. The secret image can be recovered by using qualified subset of shares and the forbidden subset does not reveals any secret information [2]. Now-a-days, the growth of the technology get increased. So that security of visual information during its transaction also be increased. Internet is the media used for communication like transmitting pictures, audios, videos etc., It also include military secrets, commercial and information about individuals. In this technique, visual cryptography, a secret image is encrypted into n number of shares which is very difficult to retrieve the original image. Chaotic-Pseudo-Random number generation and Zig-Zag scan pattern method is used. This method reduce the degradation of the resultant image and it is proposed by an extension from gray to color image. To improve security pixel index method is used. In this paper, shares are generated by using pixel reversal and pseudo random technique [3]. Multipixel encoding is an emerging method in visual cryptography. It can encode more than one pixel for each encoding run. The encoding length is invariable and very small for each run so that the encoding efficiency is verylow. A novel multipixel encoding called pixel block aware encoding is proposed in this paper. It scans each secret image by zig-zag and perceives a pixel block which contains many pixels. A pixel block consists of consecutive pixel which is of same type during scanning. The proposed system helps to improve the encoding efficiency over single pixel encoding and multipixel encoding[4].

Visual Secret Sharing Schemes hide a Secret image in shares that appear noise like picture or noiseless picture.VSS schemes suffer from a transmission risk problem while sharing shares contains Secret Images. To address this problem, we proposed a natural-image-based VSS scheme (NVSS scheme) that shares secret images via various carrier media to protect the secret and the participants during the transmission phase. This Process involves sharing a secret image over arbitrary selected natural images (called natural shares) and one noise-like share. The natural shares can be photos or hand-painted pictures in digital form or in printed form. The noise-like share is generated based on these natural shares and the secret image. The unaltered natural shares are diverse, thus greatly reducing the transmission risk problem. We also propose possible ways to hide the noise like share to reduce the transmission risk problem for the share. Experimental results indicate that the proposed approach is an excellent solution for solving the transmission riskproblem for the VSS schemes [5]. Visual cryptography scheme is a cryptographic technique which allows visual information to be encrypted into several shares in such a way that the decryption can be performed by the human visual system, without the aid of computers. Random grid is a methodology to construct visual secret sharing (vss) scheme without pixel expansion in which an RG scheme takes an input image and transforms it into multiple cipher-grids that provide no information on the original image and the resulting decrypted image retains the size of the original image. Intent of this paper is on comparative study of visual cryptography and Random grid cryptography on the basis of analysis and correctness of simple VC schemes and RG schemes, improving contrast of the reconstructed image using various algorithms and multiple-image encryption using rotating angles [6].

## 3.EXISTING SYSTEM

The main aim of the existing system is to maximize the range of access control of VSS schemes. Access control is the selective restriction that is to maximize the restrictions to access a resource. The main steps are a) formulation of access structure for a single secret which is generalized to multiple secrets. Group of parties that are granted access is called qualifies subset. In set theoretic form they are called qualified set. A set of all such qualified et is called access structure, b) a sufficient condition is to be satisfy: more general and can generate VSS scheme with strictly better contrast and pixel expansion, straight forward implementation. In the existing system color images can be converted into gray scale image and then the gray scale image is converted into n number of shares. To improve the security the images are embedded into another images. It provides two shares one is black and other is white. When these two shares are superimposed the original image get revealed. 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 $k \leq n$) bring their shares together, the secret can be recovered. The share division is shown in Figure1.

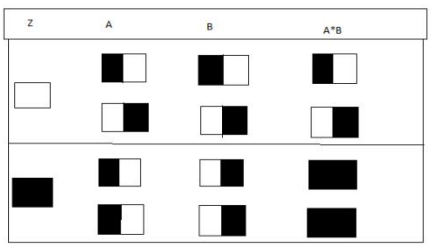


**Figure 1:** Share division

## 4.PROPOSED SYSTEM

Security has gained a lot of importance as information technology is widely used. 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 MoniNaor and Adi Shamir in 1994 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. DCT express a fine sequence of data points in terms of a sum of cosine function oscillating at different frequencies. DCTs are important to numerical applications in science and engineering from lossy compression of audio and images. Cryptography is a discipline of using codes to encrypt data into an unreadable format that only the targeted recipient can decrypt and encrypt. Encryption methods are divided into two categories: lossy and lossless.

In lossy encryption method, the decrypted image details are vulnerable to distortion. Lossless encryption methods are more relevant when marginal distortion is not tolerable. In this proposed algorithm , the image is transformed into frequency domain, where low and high frequency are processed in a way that guarantees a secure, reliable and unbreakable form. In this proposed VCS , DCT is used. It consist of lossy encryption and lossless encryption. The image encryption steps is shown in Figure2. The algorithm is designed to shuffle and reverse the sign of each frequency in the transformed block before the image blocks are transformed block to pixel domain. The result shows a total change in the encrypted image pixel values concealing the image details.

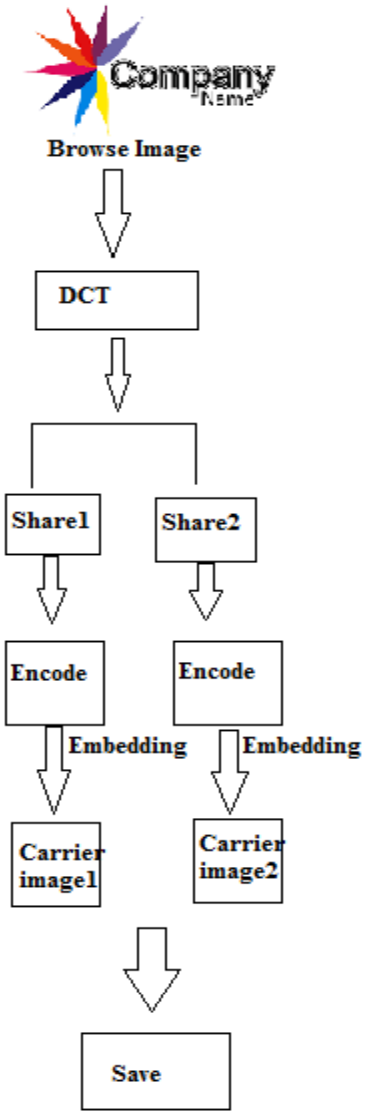


**Figure 2:** Image encryption

The decryption algorithm reverses the encryption steps as shown in figure 3and return the image to its original form without any loss in the pixel values. In the first step, the secret image is taken as input and image is compressed by using DCT. On this compressed image, encryption is performed by VC, it means shares are generated and these shares are transmitted over the network. At the receiver end, these shares are initially decrypted by XOR and decompression is performed by inverse DCT and finally our secret is revealed. Secret image is compressed by using DCT.

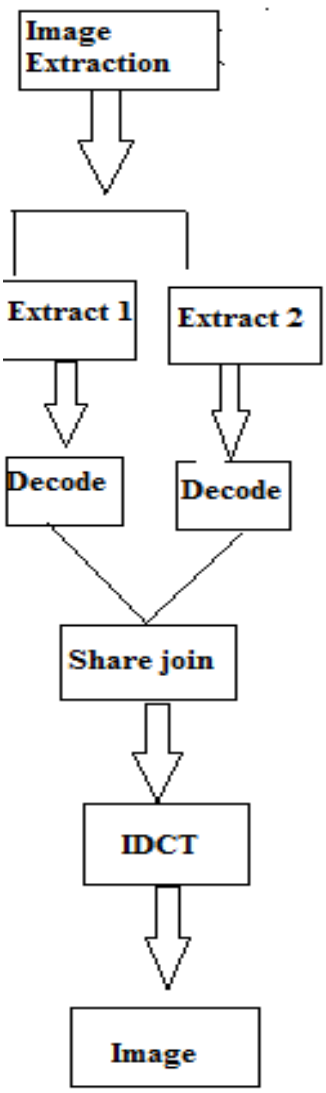


**Figure 3:** Image decryption

DCT converts the information contained in the blocks (8*8) of pixel from spatial domain to frequency domain. Here, the original image is divided into 8 by 8 blocks and 2-D DCT is computed for each block. The purpose of dividing the image into blocks is to reduce the number of calculations.

**5.MODULES**

The proposed system consists of 6 modules

1.Image Preprocessing

2.DCT Calculation

3.Share management

4.Share encryption/Share decryption

5.Share embedding

6. Inverse DCT calculation

***Image Preprocessing***: In this module first 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.

***DCT calculation***: In this module the image is broken into 8 x 8 blocks of pixels. Working from left to right, top to bottom, DCT is applied to each block. A discrete cosine transforms (DCT) expresses a finite sequence of data points in terms of a sum of cosine functions oscillating at different frequencies.

***Share Management*:** 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 sub pixels. Anyone who holds only one share will not be able to reveal any information about the secret.

***Share Encryption/Decryption*:** The most proposed approach for the image encryption/decryption is RC4 stream cipher. The reason, RC4 stream cipher is speedy encrypt image, less resources used, less time and implementation complexity. Basically, RC4 algorithm is the two stages process, KSA (Key scheduling Algorithm) and PRGA (Pseudo Random Generator algorithm).

***Share Embedding***:The method used for share embedding is LSB, it is the lowest bit in a sequence of binary number. The LSB based embedding is used to insert the secret data into the least significant bits of the pixel values in a cover image.

***For Encryption***:

Step 1. Read the cover image in which the secret data to be hidden.

Step 2. Read the secret data and convert in binary form.

Step 3. Compute the LSB of each pixels of cover image.

Step 4. Replace least significant bit (LSB) of cover image with each bit of secret data/image one by one.

Step 5. Write output image

***For Decryption*:**

Step 1. Readthe image.

Step 2. ComputeLSB of each pixel from the image.

Step3. Retrieve bits and convert each 8 bit into corresponding character

***Inverse DCT calculation:*** In this module the reverse calculation of DCT is applied to reconstruct the secret image. Here the size of image is compared to be large than the original secret image but quality is very high.

## 6.CONCLUSION

The proposed lossless visual cryptography scheme reconstructed image has high image quality (same as original secret image). However, other cryptography systems in general produce images that are susceptible to distortion and degradation of quality. Therefore, substantial lossless method is achieved at the expense of quality.

## ACKNOWLEDGEMENT

We would like to thank, first and foremost, Almighty God, without his support this work would not have been possible. We would also like to thank all the faculty members of Mount Zion college of engineering, for their immense support.

## REFERENCES

[1] MoniNaor and Adi Shamir, “Visual cryptography” .In Proceedings of the *advances in cryptology– Eurocrypt, 1-12*,1995.
https://doi.org/10.1007/BFb0053419
[2] Lin Kezheng, Fan Bo, Zhao Hong, “visual cryptographic scheme with high image quality”. In Proceedings of *the International Conference on Computational Intelligence and Security, 366-370,IEEE*,2008.
https://doi.org/10.1109/CIS.2008.106
[3] Wen-Pinn Fang “Non-expansion visual secret sharing in reversible style”. *IJCSNS International Journal of Computer Science and Network Security*,,February 2009.
[4] Xiao-qing Tan, “Two kinds of ideal contrast visual cryptography schemes”. In Proceedings of the *International Conference on Signal Processing Systems, 450-453*, 2009.
https://doi.org/10.1109/ICSPS.2009.119
[5]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.
[6]B.Padhmavati, P.Nirmal Kumar, M.A.Dorai Rangaswamy, 2010. A Novel Scheme for Mutual Authentication and Cheating Prevention in Visual Cryptography Using Image Processing. Proceedings of Int. Conf. on Advances in Computer Science 2010, DOI: 02, ACS.2010.01.264, ACEEE.