IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

# A Survey of Visual Cryptographic Method for Secure Data Transmission

**Dr. D. Devakumari MCA., M.Phil., PhD.[1], K. Geetha[2]**

Assistant Professor, Department of Computer Science, Government Arts College, Coimbatore, Tamil Nadu[1]

Student, Department of Computer Science, Government Arts College, Coimbatore, Tamil Nadu[2]

**Abstract:** Transmission of data between the users in the network is an important aspect of today, user of the network wants to share their information between other users of secured data transmission. They were many mode of transaction o data were done, but secured level of data transaction is an important aspect what everyone wants. Secret data transmission is still major problem in network. Embedding the secret information is an upgrading technology for sharing secret data, embedding process cryptography method plays a key role. Effective embedding of secret data by using visual cryptography helps a lot for secret data transmission. This paper provides the survey of various cryptographic methods and its effectiveness for secure transmission over network.

**Keywords**: Network, Data Transmission, Security, Visual Cryptography and Secure Data.

## I. INTRODUCTION

Visual Cryptography is a special encryption technique to hide information in images in such a way that it can be decrypted by the human vision if the correct key image is used. Visual Cryptography uses two transparent images. One image contains random pixels and the other image contains the secret information. It is impossible to retrieve the secret information from one of the images. Both transparent images and layers are required to reveal the information. Visual cryptography is a very secure and distinctive way to protect secrets [1]. Unlike traditional cryptographic schemes, visual cryptography uses human eyes to decrypt the secret without any complex decryption algorithms and the aid of computers. Usually, the decryption of the secret image consists of printing more than k shares onto transparences and superimposing these transparences on the whole; subsequently, applicants can recognize the get bettered secret from the stacked image with their observes. Visual cryptography which make available a very powerful method by which one top secret can be allocated into two or more pieces known as shares [2]. The top secret whose text Format subject matter to encryption using substitution cipher and the consequential encrypted text were embedded into the image. When the shares on transparencies are place over accurately mutually the original secret can be determined without computer contribution. Visual cryptography scheme is a secret sharing of secret image shares which involves dividing the secret image into number of shares and a certain number of shares are sent over the network. The decryption process involves stacking of the shares to get the secret image. The main advantage of visual cryptography scheme is that a number of qualified shares are able to recover the secret image without any cryptographic knowledge, calculation and computation devices [3].

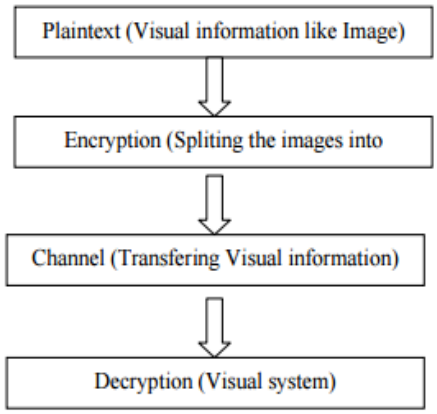


Figure 1: Mechanism of Visual Cryptography

Visual Cryptography is a special technique which is used to send the images securely over the network. The decryption process includes combining the shares to obtain the secret image. Secret image and original share images as inputs, and

outputs shares that satisfy the following conditions, first any required set of shares can recover the secret image, second any forbidden or mismatch set of shares cannot obtain any information of the secret image other than the size of the secret image. Image steganography, Symmetric encryption and visual cryptography algorithms are applied to enhance overall security of image transaction from one system to another. Data security has become a most important issue in data communication especially in the field of Computer Network.

The data can have many forms such as text, image, and sound etc. There are many cryptosystems exists to protect data; out of those Visual Cryptography (VC) is a popular technique to protect image based data. It splits the secret image into shares in encryption process and the original image can be retrieved by stacking the required number of shares at the time of decryption. Steganography is another method of cryptosystem used to protect data. It hides the secret inside another data [4, 5]. It makes the secret invisible to users. But in the rapid expansion of cryptanalysis and steganalysis, data is still very insecure in some state of affairs. Hence, to provide a strong security mechanism a hybrid approach using the feature of VC and steganography techniques is wise to adopt. This paper studies the visual cryptography scheme, for data security especially for image based data transmission.

## II. LITERATURE REVIEW

Kalyan Das [6] Visual cryptography is a method for protecting image-based secrets that has a computation-free decoding process. In this paper we propose a new color visual cryptography scheme. In visual cryptography the decipher can be performed by human visual system (HVS) without any complex process, providing high security. Our proposed method suggested a way to encrypt a color image using symmetric key encryption procedure. The proposed method is applied on several images and showed good result without any distortion. The algorithm proposed by this scheme reduces a considerable time for encryption and decryption in a much easier way and ensures the lossless transmissions of images.

P.S.Revenkar [7]Visual cryptography scheme is a cryptographic technique which allows visual information (e.g. printed text, handwritten notes, and picture) to be encrypted in such a way that the decryption can be performed by the human visual system, without the aid of computers. There are various measures on which performance of visual cryptography scheme depends, such as pixel expansion, contrast, security, accuracy, computational complexity, share generated is meaningful or meaningless, type of secret images( either binary or color) and number of secret images(either single or multiple) encrypted by the scheme. Intent of this paper is on study and performance analysis of the visual cryptography schemes on the basis of pixel expansion, number of secret images, image format and type of shares generated. In this paper various visual cryptography schemes are studied and their performance is evaluated on four criteria: number of secret images, pixel expansion, image format and type of share generated. For avoiding attention of hackers while transmitting the confidential messages are suitable selections.

D. Madhav VC [8], EVCS and Color EVCS are the three techniques used for Visual Cryptography Schemes. Visual Cryptography Scheme (VCS) is one of the techniques used to encrypt the image by dividing the original image into transparencies called Shares. A set of qualified participants is able to recover the secret image. An Extended Visual Cryptography Scheme (EVCS) is a kind of VCS which consists of embedded random shares realized by embedding shares into covering shares. Color Visual Cryptography (VC) encrypts a color secret image into n color halftone image shares. Different methods for VC have different algorithms to provide cryptography for images. This paper describes the trade-off between the image quality and the security is discussed by comparing these VC schemes. The shares generated in VC, EEVC and Color EVC schemes are meaningful transparency shares, and the stack of qualified subset of shares will recover the secret image quality without the aid of computers. Each method follows their own approaches for encryption and decryption processes to provide security and image quality. The results of this paper are based on the observations on the implementation of all the three VC techniques. Security and perceived image quality are better in Color EVCS when compared to Gray level VCS and Embedded Extended VCS.

Praveen Kumar [9] Visual cryptography technique encrypts pictorial information in such a way that their decryption can be done by human visual system. Security has become an important issue as communication is driving the world now. Cryptography is the science of making ciphers to provide data confidentiality, data security, entity authentication, but this is not only the way of providing information security, but one of the techniques. Visual cryptography can be applied for copy right for images, access control based user images identification, visual authentication through any kind images like normal or digital. Visual cryptography provides information security which user simple algorithm unlike computationally complex cryptographic algorithms This technique allows visual information (pictures, text, etc) to be encrypted in a way so that their decryption can be done by the human eye, without any complex computations. This technique encrypts a secret image into shares such a way that that stacking required number of shares reveals the secret image. Shares are visually presented in transparencies.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

In this paper we provide a thorough analysis of the various visual cryptography (VC) techniques and related security research work done in VC.

Z. Zhou and et al [10] explained Halftone visual cryptography and says that some of disadvantage in basic visual cryptography. The some important things are: The position of secret information pixel. The secret information pixels depend upon on black and white distribution to halftone images. • The changing of pixels position during the operation, chances of loss maximum shape of the image explained direct binary search for visual cryptography and explain about pixels distribution, The selection of secret pixel should be randomly or homogeneously distributed

R.Yadagiri Rao et al [11] effective and secure protection of sensitive information is the primary concerned in Communication systems or network storage systems. Never the less, it is also important for any information process to ensure data is not being tampered with. Encryption methods are one of the popular approaches to ensure the integrity and confidentiality of the protected information.

However one of the critical vulnerabilities of encryption techniques is protecting the information from being exposed. To address these reliability problems, especially for large information content items such as secret images (satellite photos or medical images), an image secret sharing schemes (SSS) is a good alternative to remedy these types of vulnerabilities. With the rapid advancement of network technology, multimedia information is transmitted over the Internet conveniently. While using secret images, security issues should be taken into consideration because hackers may utilize weak link over communication network to steal information that they want. To deal with the security problems of secret images, various image secret sharing schemes have been developed

## III. VISUAL CRYPTOGRAPHY

A Visual cryptography is a cryptographic scheme used to encrypt image based data such as handwritten notes, signature, pictures, diagrams etc. and decryption can achieve directly by human visual system, without the computation of computers. In VC Scheme the secret data splits into two or many shares, each of which individually cannot provide any information about the secret data. The secret data can be only retrieved when the desired numbers of shares are superimposed with one another. During decryption the shares are needed to be printed out in a transparency sheets/papers and needs to stack all or desired number of transparencies with each other that reveals the secret information [12].

Therefore, it does not require any complex calculation as like other traditional cryptography schemes.

### a. How it works?

Each pixel of the images is divided into smaller blocks. There are always the same number white (transparent) and black blocks. If a pixel is divided into two parts, there are one white and one black block. If the pixel is divided into four equal parts, there are two white and two black blocks.

### b. Visual Cryptography Transmission

The easiest way to implement Visual Cryptography is to print the two layers onto a transparent sheet. When the random image contains truly random pixels it can be seen as a one-time pad system and will offer unbreakable encryption. In the overlay animation you can observe the two layers sliding over each other until they are correctly aligned and the hidden information appears. For analyzing this, you can copy the example layers 1 and 2, and print them onto a transparent sheet or thin paper. Always use a program that displays the black and white pixels correctly and set the printer so that all pixels are printed accurate (no diffusion or photo enhancing etc) [13]. You can also copy and past them on each other in a drawing program like paint and see the result immediately, but make sure to select transparent drawing and align both layers exactly over each other.

### c. Encoding and Decoding

During the encoding procedure, our new scheme takes in two coding tables, cover coding table (CCT) and the secret coding table (SCT), respectively. CCT is to help with the encoding of the extracted cover image, and SCT is to help process the extracted secret image. SCT in our new scheme works the same way as Table. In the encoding procedure, the proposed scheme uses CCT to encode EA and EB, while ES is encoded by the SCT. In CCT, as shown in Table, the first row represents various color pixels in EA and the first column stands for various color pixels in EA. The intersections of the rows and the columns are the output blocks with the left side of the block belonging to Share 1 and the right side of the block belonging to Share 2. SCT, has the same definition as it does. Each pixel from the extracted image is expanded to one 2×2 block. The expanded block is placed in one of the 2×4 block patterns. By this way, the extracted image can produce a 2N×2N share.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

## IV. NETWORK SECURITY USING VISUAL CRYPTOGRAPHY TECHNIQUE

**a. The RSA Algorithm**

This is a public key encryption algorithm developed by Ron Rivest, Adi Shamir and Len Adlemen in 1977.The RSA algorithm is the most popular and proven asymmetric key cryptographic algorithm. The RSA algorithm is based on the mathematical fact that it is easy to find and multiply large prime numbers together, but it is extremely difficult to factor their product. The private and public keys in the RSA are based on very large (made up of 100 or more digits) prime numbers [14]. The algorithm itself is quite simple (unlike the symmetric key cryptographic algorithms). However, the real challenge in the case of RSA is the selection and generation of the public and private keys. To deal with the security problems of secret images, various image secret sharing schemes have been developed which gave rise to new technologies in the area of Image Cryptography using RSA algorithm which would require less computation and less storage.

**b. Least significant bit (LSB) method**

LSB is the lowest bit in a sequence of binary number. Say, if bits of binary number are 10101001, the least significant bit is far right 1 [6]. The LSB based Steganography is used to insert the secret data into the least significant bits of the pixel values in a cover image. For example, to insert a bit of secret information say 01010001 in a 8th bit of some or all the bytes of a cover image is as follows:

*Pixel of Cover image:*

(10101111 11101001 10101000)
(10100111 01011000 11101001)
(11011000 10000111 01011001)

*After change the LSB:*

(10101110 11101001 10101000)
(10100111 01011000 11101000)
(11011000 10000111 01011001)

Here, secret bits 01010001 are embedded into first eight bytes of the cover image and only three bits are changed. This minimal changes are not noticed by the human visual system, hence the LSB insertion is very easy to implement and most popular method in Steganography technique. This method add multiple layers of security it is always a good practice to use Cryptography and Steganography together [15]. By combining, the data encryption can be done by a software and then embed the cipher text in an image or any other media with the help of stego key. The combination of these two methods will enhance the security of the data embedded. This combined chemistry of steganography and cryptography will satisfy the requirements such as capacity, security and robustness for secure data transmission over an open channel. Concentrate to make review of combine data hiding techniques useable for security of data.

**c. Transform Domain Techniques**

In transform domain technique, embedding of secret information in a cover image is done by altering the DCT (Discrete Cosine Transform) coefficients. It splits the image into parts of differing importance. It transforms a signal/image from the spatial domain to the frequency domain. It split the image into high, middle and low frequency components. This technique hides secret information in the significant areas in the cover image that makes them robust against compression, cropping and other network attacks. One could have a secret image with confidential data which could be split up into various encrypted shares [16]. Finally when such encrypted shares are reassembled or decrypted to redesign the genuine image it is possible for one to have an exposed image which yet consists of confidential data. Such types of algorithms cannot persist without possessing appropriate characteristics in the visual cryptography procedure. The ground for this is that if the rebuilding method or even the encoding method changes the data exists in the image, then the system would accordingly change the encrypted information which makes the system feasible for extracting the encrypted data from the exposed image.

## V. CONCLUSION

Network plays an important role for transferring the data or information from one party to another. Transferring the data faces the security problem, while transferring the data may leak or loss due to the third party of the intruder in the network. For secret data transmission is still major problem in network. Embedding the data for secret information is an

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

upgrading technology for sharing secret data, many techniques were proposed by many authors using cryptography, stegnography, etc, which provide some drawbacks. From our analyses paper provides the survey of various cryptographic methods and its effectiveness for secure transmission over network through visual cryptography method which provides more secure of data transmission over the network.

## REFERENCES

[1] "A New Visual Cryptography Scheme for Color Images", B.SaiChandana ,S.Anuradha, International Journal of Engineering Science and TechnologyVol. 2(6), 2010, 1997-2000
[2] "A Three Way Visual Cryptography& its Application in biometric Security : A Review", Mr. Praveen Chouksey,
[3] Mr.Reetesh.Rai, www.ijraset.com Volume 3 Issue V, May 2015, IC Value: 13.98 ISSN: 2321-9653 "New Visual Cryptography Algorithm ForColored Image", Sozan Abdulla,
[4] Sathiamoorthy Manoharan, an empirical analysis of rs steganalysis, proceedings of the third international conference on internet monitoring and protection, ieee computer society washington, 2008.
[5] Y.C. Hou, C.Y. Chang, and F. Lin, "Visual cryptography for color images based on color decomposition," in Proc. of 5th Conference on Information Management, Taipei, Nov 1999, pp.584–591.
[6] Kalyan Das, "A New Visual Cryptography Scheme for Color Image Using Sliding Puzzle Technique".
[7] P.S.Revenkar, "Survey of Visual Cryptography Schemes".
[8] D. Madhav, "A Survey on Perceived Visual Quality and Secured Visual Cryptography Schemes".
[9] Praveen Kumar, "A Survey on Visual Cryptographic Schemes and their Comparative Analysis",
[10] Z. Zhou, G. R Arce, and G. Di Crescenzo, "Halftone Visual Cryptography," in Proc. of IEEE International Conference on Image Processing, Barcelona, Spain,Sept 2003, vol. 1, pp. 521–52
[11] R.Yadagiri Rao SECURE VISUAL CRYPTOGRAPHY
[12] RiteshD.Yelane, Dr.Nitiket. N. Mhala, Prof. B. J. ,"Chilke,Security Approach by Using Visual Cryptographic Technique
[13] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems". Communication of the ACM, pp. 120-126, 1978.
[14] Manika Sharma, Rekha Saraswat, "Secure Visual Cryptography Technique for Color Images Using RSA Algorithm", International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 10, April 2013.
[15] R. Chandramouli, Nasir Menon, Analysis of LSB Based Image Steganography techniques, IEEE-2001.
[16] Akshatha M M, Lokesh B and Nuthan A C, "Visual Cryptographic Technique for Enhancing the Security of Image Transaction", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 5, May 2014.