

# New Algorithm for user Friendly Encryption

Shyni T S

M.Tech Scholar, Department of ECE  
LBS Institute of Technology for Women  
Thiruvananthapuram, India

Anusree L

Assistant Professor, Department of ECE  
LBS Institute of Technology for Women  
Thiruvananthapuram, India

**Abstract**— This paper proposes a new algorithm for encrypting secret data to be communicated over internet. This method combines the advantage of normal encryption and visual cryptography. The secret image is encrypted using a new encryption algorithm producing multiple encrypted images. Images are same as the cover images thus become easy to handle. Then meaningful images are embedded on each share using embedding algorithm. At the receiver side after de embedding these meaningful encrypted images are decoded to form the secret image back. This method can be used for multiple meaningful encrypted images with perfect reconstruction of secret image.

**Keywords**—Cryptography; encryption; image embedding; shares.

## I. INTRODUCTION

During last decade, the use of computers in daily life has tremendously increased. Users deal with data not only in the form of text but also as audio, video etc. In recent years communication of multimedia content over internet have become very popular. However secret data communicated this way are vulnerable to unauthorized access. The data can be accessed by unauthorized user both during storage and transmission. A secure way to communicate secret image and video over internet is very necessary.

To ensure the security of secret data communicated over internet we generally use encryption. When secret data are communicated over internet, the eavesdroppers may duplicate the data. But encrypting the data will improve the security of data. Even if unauthorized user duplicates the information it will not be in readable form. To get the information content, decryption has to be done. Thus cryptography helps to send information between participants in such a way that prevents others from reading it. Also encrypting the data using a key will improve the security of data.

The application of encryption comes in communication of medical images. To reduce the cost of transferring nowadays medical data are sent over internet to laboratories and doctor's office. In order to ensure the privacy of patient data encryption is effectively used.

While the secret data is communicated over the channel there is a possibility that the data is modified by an unauthorized user. Thus at the receiver side user will not receive the secret which was actually sent. The modification occurred to secret data will cause severe problems in the case of communicating medical data and other important data. To ensure that the secret is not modified during communication we use watermarking.

Watermarking is technique used to ensure the authenticity of secret data and to verify the identity of its owner. Depending upon the use fragile or robust watermarking is added to data. In order to ensure the integrity of data communicated a fragile watermarking is added. When an unauthorized user modifies the watermarked image the watermarking gets altered. Thus the receiver will get to know that the secret data has undergone modification. But when watermarking is to show the copy right information a robust watermarking is added.

Nowadays the security of secret data communicated over internet has become an issue with great importance. Eavesdroppers use advanced techniques to decrypt the data. The security of data is not ensured by using conventional cryptographic methods. Thus in order to secure the secrecy of communication a new encryption algorithm incorporating some advantages of visual cryptography is proposed here.

This paper is structured as follows. Section II discusses basic concept of cryptography and concept of visual cryptography is explained in section III. Proposed method is explained in section IV and the experimental result of this method is given in section V. Finally conclusion is given in section VI.

## II. CRYPTOGRAPHY

Cryptography is the process of storing and transmitting data in noise like form such that, no information can be read directly from it and then transforming that information back to original form. Cryptography consists of two stages, encryption and decryption. The process of converting a secret data to noise like form using a key is called encryption. The reverse process of converting the encrypted data to original form is called decryption. The original intelligible message is called plain text. Transformed noise like message is called cipher text.

In general encryption standards a secret key is used for encryption. It the critical information used by cipher known only to sender and receiver. A secret key is used for encrypting the data and the same key is required for decrypting. If the key is lost the user will not be able to decrypt the image. Thus security of cryptographic system lies in how safely the key is kept. If an unauthorized user has the key he can easily access the secret data.

The conventional cryptographic schemes like block cipher and stream cipher algorithms are generally very complex. Also if the encryption key is lost the user can not decrypt the data back to original form. Thus for processing large amount of secret data a simple and secure encryption algorithm is required.

### III. VISUAL CRYPTOGRAPHY

Visual cryptography is an advanced method for ensuring security of data during transmission. The main difference between cryptography and visual cryptography is that visual cryptography does not have a decryption algorithm. The decryption is done visually. The secret image is converted to multiple noise like images called shares. At the receiver side overlapping these shares the secret image is revealed. Thus the user does not require any key for decryption.

The basic visual cryptographic scheme was first proposed by Naor and Shamir. In visual cryptography the secret image is divided into multiple shares where each share does not convey any information on its own. At the receiver side on overlapping these shares the original secret image is recovered. In  $(k,n)$  visual cryptographic scheme, where  $k < n$  the image is divided into  $n$  number of shares and for reconstruction only  $k$  shares are required. No information will be revealed when  $k-1$  images are stacked.















The main disadvantage of basic visual cryptography scheme is pixel expansion in stack image. Multiple pixels are used in shares for representing one pixel in secret image. Thus sizes of shares are larger than the secret image. Low contrast of stack image is another problem in this method. This results from the fact that white pixels in secret image can be represented in stack image only by using combination of black and white pixels. Thus contrast of stack image decreased to 50%.

The concept of basic  $(2,2)$  visual cryptography proposed by Naor and Shamir is shown in table I. To represent each pixel in secret image, two pixels are used in each share. For generating black pixel on stacking, share1 and share2 will have opposite combination of black white pixels. On stacking these shares two black pixels are obtained. On the other hand for generating white pixel in stack image both share 1 and share 2 use same combination of black and white pixels. On stacking these two shares one black pixel and one white pixel is generated.

Thus perfect reconstruction of white pixel is not possible. The white pixel in stack image will have only 50% contrast compared to original image. This method is not preferred much as it suffers from pixel expansion problem. Corresponding to each pixel on secret image, the stack image will have two pixels. Hence size of stack image is twice that of secret image. To overcome the low contrast and pixel expansion problem later new methods were proposed.

R. Ito, H. Kuwakado, and H. Tanaka [7] and C N Yang [4] used concept of probability to generate shares without pixel expansion. But due to random nature of probability, shares have low visual quality. Karfi and Keren [5] proposed random grid visual secret sharing scheme for generating non-expanded shares. To avoid share management problem Chen and Tsao [2] developed user friendly random grid visual secret sharing scheme which generates meaningful shares without pixel expansion. But this method can only generate stack image with low contrast.

TABLE I. CONCEPT OF  $(2,2)$  VISUAL CRYPTOGRAPHY SCHEME

Pixel		
Probability	50%    50%	50%    50%
Share 1	 	 
Share 2	 	 
Stack image	 	 

### IV. PROPOSED METHOD

A new method for secure communication of information is proposed here. This method includes advantages of both visual cryptography and normal encryption. In normal encryption methods a single image is obtained after encryption. Also the encrypted image will be in noise like form. This will lead to image management problem. To overcome this we introduce new encryption algorithm which include some advantages of visual cryptography.

In visual cryptography the secret image is divided into multiple meaningless noise like shares. On stacking these shares the secret image is revealed. Thus the secret can be accessed only if all owners of shares desires. Also in order to make the share management easy nowadays meaningful shares are generated. By using advanced visual cryptographic techniques shares which are same as the cover images are generated.

This idea of meaningful multiple share generation is used in the new encryption method. To encrypt a secret image using this algorithm two cover images are used. Using this new encryption algorithm the secret image is converted to two encrypted images. Each of these images is same as the cover images used. Thus meaningful multiple share generation is achieved.

In order to make this method more secure an additional image embedding algorithm is used. When images are embedded on each encrypted image the pixel values get changed. Thus even if an unauthorized user gets the share the pixel combination used for encryption is not revealed. Hence decryption of share is not possible. Thus the method becomes doubly secure. At the receiver side the embedded image is first de-embedded before the share is sent to decryption.

#### A. Encryption method

Four pixel values X, Y, Z, W are used to encrypt the secret image. First each pixel location of secret image is checked to find whether it is black or white. For black secret image pixels pixel values X, Y are used to encrypt and for white secret image pixel Z, W values are used. For a black pixel in secret image the corresponding location of covers are checked. If a cover pixel is black its value is modified as X and if it is white it is modified as Y.

Same way if secret image pixel is white the same process is done on covers using pixel values Z, W. The process is repeated for each pixel in secret image such that all pixel values in cover images are modified with one of the values X, Y, Z, W. The modified cover images will be same as before. According to number of users among which the secret is shared the number of encrypted image can be increased.

### B. Decryption

In order to decrypt the secret image back any one of the shares is required. Decoding is done by examining the pixel values in cover image. Whenever the pixel value is X or Y corresponding location of the secret image is taken as black. When the cover image pixel value is Z or W the corresponding location in secret image is taken as white.

### C. Encryption algorithm

**INPUT:** An  $H \times H$  secret image I, two  $H \times H$  cover images C1 and C2.

**Step 1** Read the pixel color of  $I(i, j)$ ,  $C1(i, j)$  and  $C2(i, j)$  and identify the combination

**Step 2** When secret image is black, black pixels in corresponding location of covers are modified to X and white pixels as Y. when secret image is white, black pixels in corresponding location of covers are modified to Z and white pixels as W.

**Step 3** Repeat steps 1 and 2 for all the pixels of I. Thus S1 and S2 are obtained.

**Step 4** Each share is embedded using an image embedding algorithm.

**OUTPUT:** Two  $H \times H$  meaningful share images S1 and S2

### D. Decryption algorithm

**INPUT:** Two  $H \times H$  meaningful share images S1 or S2

**Step 1** De embed each share S1 and S2 using de embedding algorithm.

**Step 2** Read the pixel value of  $S1(i, j)$  or  $S2(i, j)$

**Step 3** When share pixel is X or Y secret image pixel is taken as black and if share pixel is Z or W secret image pixel is taken as white.

**Step 4** Repeat steps 1 and 2 for all the pixels of share.

**OUTPUT:**  $H \times H$  decoded image.

This method has some advantages compared to conventional cryptographic schemes. First of the algorithm used for encryption is simple and cost effective. A secret image can be converted to multiple encrypted images which are different from one another. Thus single secret can be shared among multiple user and each of them can access secret without permission of others. This method is very useful in applications with multiple users.

## V. EXPERIMENTAL RESULTS

The experiments are performed in personal computer of 4GB memory on WINDOS 7. The platform used for development is MATLAB R2014a. The images used for experiment is shown in figure.

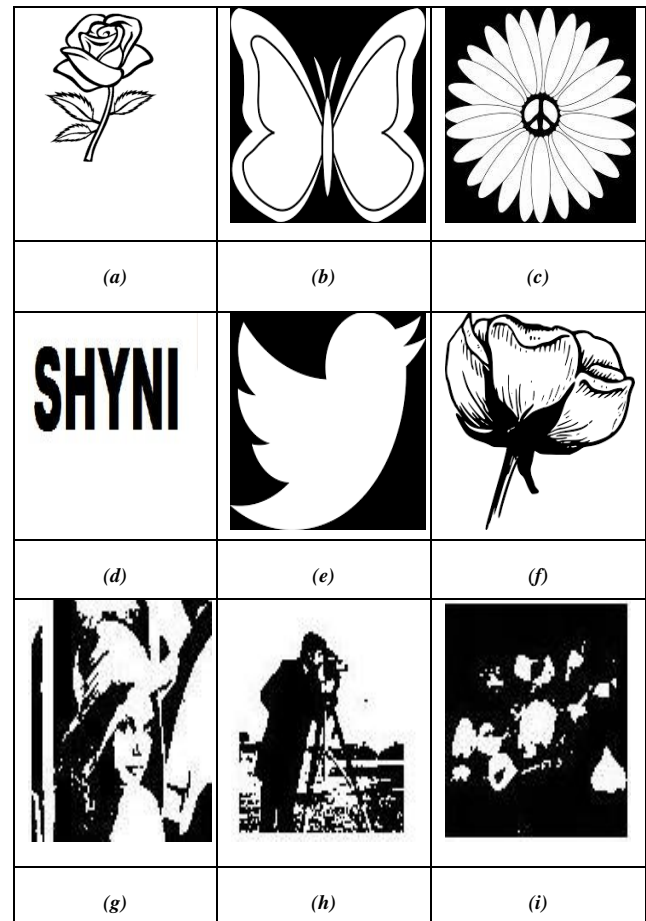


Figure 1 (a)- (f) Experimental images (a)- secret image (b) cover 1 (c) cover 2 (d) secret image (e) cover 1 (f) cover 2 (g) secret image (h) cover 1 (i) cover 2

### A. Experiment 1

#### Encrypting secret to multiple meaningful

The experimental results of new encryption algorithm are shown in figure.2 The results shows that the secret image is recovered perfectly. The encrypted images are same as the cover images used. The number of encrypted images can be increased based on the number of users among which secret is shared.

Embedding images on each encrypted images will improve the security of this system. As the pixel values in each share are changed even if an unauthorized user gets the share the pixel combination used for encryption is not revealed. Thus the security of this encryption method is doubled.

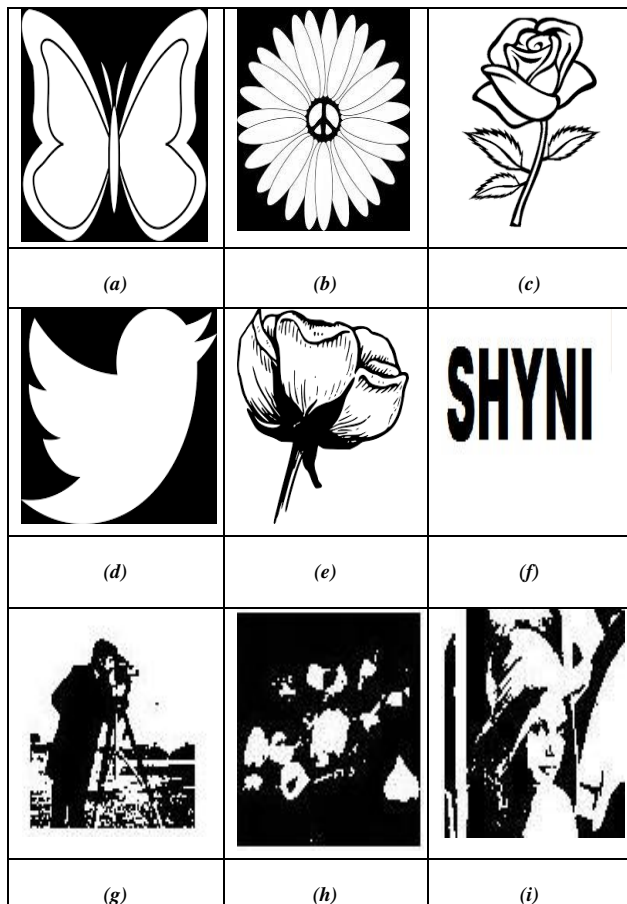


Figure 2 (a)- (f) Experimental images (a)- share 1 (b) share 2 (c) secret image  
(d) share 1 (e) share 2 (f) secret image  
(g) share 1 (h) share 2 (i) ) secret image.

## VI. CONCLUSION

A new data encryption method for secret communication is developed here. This method includes the advantages of both encryption and visual cryptography. This secure encryption scheme can be used in application in which access to secret is distributed among multiple users. This system can be used to generate multiple meaningful encrypted images which have wider applications.

## REFERENCES

- [1] Young-Chang Hou, Shih-Chieh Wei, and Chia-Yin Lin "Random-Grid-Based Visual Cryptography Schemes", IEEE transactions on circuits and systems for video technology, vol. 24, no. 5, may 2014
- [2] T. H. Chen and K. H. Tsao, "User-friendly random-grid-based visual secret sharing," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 21, no. 11, pp. 1693–1703, Nov. 2011.
- [3] T. H. Chen and K. H. Tsao, "Visual secret sharing by random grids revisited," *Pattern Recognit.*, vol. 42, no. 9, pp. 2203–2217, 2009.
- [4] C. N. Yang, "New visual secret sharing schemes using probabilistic method," *Pattern Recognit. Lett.*, vol. 25, no. 4, pp. 481–494, 2004
- [5] O. Kafri and E. Keren, "Encryption of pictures and shapes by random grids," *Opt. Lett.*, vol. 12, no. 6, pp. 377–379, Jun. 1987
- [6] M. Naor and A. Shamir, "Visual cryptography," in *Proc. Adv. Cryptology-EUROCRYPT'94*, LNCS 950, 1995, pp. 1–12
- [7] R. Ito, H. Kuwakado, and H. Tanaka, "Image size invariant visual cryptography," *IEICE Trans. Fund. Electron., Commun. Comput. Sci.*, vol. E82-A, no. 10, pp. 2172–2177, 1999.