IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 5, Ver. VI (Sep. - Oct. 2016), PP 19-23
www.iosrjournals.org

Providing High Security and Recovering Good Quality Image using Visual Cryptographic Technique

Prasanna Kumar H R[1], Niranjan N Chiplunkar[2]
[1]*Research Scholar, NMAMIT, Nitte, India*
[2]*Principal, NMAMIT, Nitte, India*

Abstract: *Security is an important factor, since many digital images are transmitted through internet, which contains secret information. Symmetric and Asymmetric methods are two types of cryptographic techniques used to encrypt and decrypt the confidential data. Conventional encryption technique is one of the methods used to transmit secret image which has a drawback of maintaining the secret key. Image splitting is another technique used, in which secret image is divided into different share images. Individual share does not reveal any information about the secret. Qualified set of shares are used to decrypt and get back the original image. Quality of the recovered image and security are the two major issues of this technique. In this paper, we proposed the cryptographic technique which uses three steps for encryption. Encryption process creates two shares, which are like random noise. Shares are transmitted to receiver and shares are decrypted separately and combine both the shares to obtain the original secret image. Proposed method increases the security level and the quality of decrypted image is same as that of original secret image.*
Keywords: *Decryption, Encryption, Visual Cryptography*

I. Introduction

In the current scenario, rapid development in the field of Information Technology, security has become more or less major issue. To transmit confidential data, internet has become the primary source. Transferring data securely is the major challenge. The technique or method is used for protecting confidential data is Cryptography. Due to hackers and other eavesdroppers on the internet, while transferring secret data, security issues are very much essential. Number of users is increasing day by day and they use simple text, photos, and videos as secret information. The network security becoming more and more important as the number of secret data being exchanged on the internet become increases. People may put images or videos online, which may contain some secret or private information. Cryptography technique is used to converting a secret message into cipher text which is in unreadable form. Cryptography is the mathematical technique, which provides information security.

The two operations performed widely in any cryptographic algorithm are encryption and decryption. Encryption is a process of converting original plaintext into unreadable format known as cipher text. Decryption process is used to get back the original secret information from cipher text. In a symmetric key method, single key is used for both encryption as well as decryption. Symmetric method is also referred to as single key or secret key method. In an asymmetric method, two different but logically related keys are used for encryption and decryption. In asymmetric method, the secret key is shared privately by sender and receiver. Each user should have two keys, a private and public in asymmetric method. The sender encrypts the message using receiver's public key and the receiver uses his private key to decrypt the secret data.

Symmetric algorithms are less complex and which executes faster as compared to asymmetric algorithm. But symmetric method needs to share the key securely. Asymmetric algorithm is slower than symmetric method and eliminates the need of sharing the private key securely.

Asymmetric method algorithm is more secure than symmetric method algorithm. Many algorithms have been developed for securing the information. But some of these algorithms are vulnerable to the attacks by the attackers. To provide security for images and videos, hiding the secret data using visual secret sharing scheme has been proposed. To maintain the confidentiality of images, two approaches being adopted. The first approach is similar to conventional technique, which contain an algorithm and a key to encrypt the image. The three major issues of this method are high computation, key management and weak security. The strength of this method is that the quality of recovered image is same as original secret image. The second method has the technique of splitting a secret image into multiple noises like images called shares, such that each individual share does not reveal any information about the secret. Here the set of qualified shares are used to decrypt and to get the original secret image. There is no key management in this approach, since the key is not used. The main issue of this method is that the quality of the recovered image is not same as that of original image.

II. Visual Cryptography

Visual cryptography method was proposed by Naor and Shamir [1], for the binary images. This method is used to provide a secure and reliable for transmit binary image, color image, text and gray images. In basic visual cryptography method, secret message is encrypted into two shares such that no individual share can reveal any secret, but two shares are printed on transparent sheet, to reveal the secret image. In this method, decryption takes place by human visual system without any complex computation.There are four schemes in Visual cryptography method: In (2, 2) scheme, encrypts the secret imager into two shares and both shares are required to reveal the original image. In (2, n) scheme, create n shares and if super imposing any two shares gives the original secret image. Here n represents the number of participants involved in the secure communication. In (n, n) scheme, creates n shares and secret image can be revealed only when all n shares are stacked. In this method any of the n-1 shares does not reveal any information about the secret. In (k, n) method, encrypt the message into n shares and group of k shares should overlaid to obtain the original image, where k is less than n and any k-1 of shares does not reveal any information about the secret. The basic method of visual cryptography is simple to implement and execute. The decryption method does not require any computation; it requires only a human visual system. Computation cost of visual cryptography is less and, we can send secret image through FAX or e-mail.

III. Related Work

Various techniques have been proposed by many researchers as an improvement to basic visual cryptography method. Zhi Zhou et al [2] proposed general framework of halftone visual cryptography. In this method visual quality of the halftone share is better. A verifiable visual cryptography is proposed by Bin Yu [3], in which verification share and corresponding verification image for each participant is added. F. Liu et al [4] discussed about various color visual cryptography scheme. In this method, pixel expansion is small and proposed method considers the color darkening phenomenon when stacking the pixels with the same color. This method does not need the halftone process while maintaining small pixel expansion.

Debasish Jena et al [5] proposed a method in which, generate the shares using basic visual cryptography method and then embed the shares into cover image, so that the shares will be more secure and meaningful.

Region incrementing visual cryptography is proposed by Ran-Zan Wang [6], which enables the dealers to specify the content of a secret image to multiple regions, where each region has its own secrecy property. John Blesswin et al [7] discussed various approaches like visual cryptography for general access structures, visual cryptography for gray scale images, Recursive threshold visual cryptography, Extended visual cryptography for natural images, Halftone visual cryptography, Visual cryptography for color images, Progressive visual cryptography and Regional incrementing visual cryptography.

Jaya et al [8] proposed a new method, which uses the technique of visual cryptography to improve the security level of existing schemes. The proposed method is fairly simple and produces image with good quality. Author compared various visual cryptography scheme based on the parameters like pixel expansion, contrast, computational complexity, number of colors supported, quality of reconstructed image, security of the method and generation of meaningful shares.

Nitty Sarah Alex et al [9] discussed about visual secret sharing based on halftone visual cryptography. Author applied various techniques of error diffusion to improve the image quality of the halftone shares. Young-Chang Hou et al [10] presented a novel scheme of progressive visual secret sharing scheme with unexpanded pixels. Himanshu Sharma et al [11] proposed a new algorithm to enhance the security in visual cryptography. Author proposed a cover image share embedded security algorithm to produce the meaningful shares from the secret image. J. K Mandal et al [12] proposed a novel (2, m+1) visual cryptography technique, where m is the number of secret image, has been encrypted based on a randomly generated master as a common share for all secrets which is decoded with any of the shares in conjunction with the master share out of m+1 generated shares.

Inkoo Kang et al [13] discussed about color visual cryptography scheme, which encrypts a color secret image into n color halftone shares. John Blesswin et al [14] discussed about the important parameter of visual cryptography like pixel expansion and contrast. The author suggested that the researchers should focus on two issues like good quality of the reconstructed image and increasing security with minimum pixel expansion. In this paper, author discussed about recursive threshold visual cryptography, extended visual cryptography for natural images, visual cryptography for gray scale images, Halftone visual cryptography and error diffusion technique. In this paper, proposed a novel self verifying secret sharing scheme for both gray and color images.

Divya A et al [15] constructed (n, n) visual cryptography scheme which has OR and XOR operations used for share creation and stacking process, which proves better in contrast and pixel expansion. Proposed method used additional matrix to increase the secrecy of the message in XOR operation. Feng Liu et al [16] proposed a construction of extended visual cryptography scheme, which is realized by embedding random

shares into meaningful covering shares. Proposed Extended visual cryptography scheme deal with gray scale input image, has a smaller pixel expansion is always unconditionally secure.

New color visual cryptography scheme based on the modified visual cryptography is proposed by Xiao-Yi Liu et al [17]. This method avoids the pixel expansion problem and makes it possible to recover secret images without any distortion. Gyan Singh Yadav et al [18] presented a novel visual cryptography scheme based on the substitution cipher and random grid. The scheme is secure and decryption is lossless.

Mizuho NAKAJIMA et al [19] proposed a method which constructs the image by stacking some meaningful images together. Here the method takes three pictures as an input and generates two images which corresponds to two of three input pictures. The third picture is reconstructed by printing the two output images onto transparencies and stacking them together.

IV. Proposed work

To maintain the confidentiality of images, two different approaches are used. In the first approach, image encryption can be done using algorithm and key. This method is same as conventional method for encryption. In the second approach, image is divided into different noise like shares such that any individual share does not reveal any information about the secret. Only the qualified set of shares can be used for decryption process.

In this paper, new cryptographic method is proposed to overcome the limitations of two approaches. The main advantages of proposed method are good quality of the recovered image and no key management. In the proposed method, original secret image is encrypted to get two shares and each share contains some part of the secret image. After decrypting each share and then combining the same, we will get original image.

To create shares, initially filtering the combined RGB components into R, G and B as three individual components. Dividing the R, G, B components into x parts or shares is the next step. According to [20] [21], the process uses random function to shuffle the RGB pixels to create the shares. In the technique specified in [20], to retrieve the secret code random share of all the participants would be required. But in the proposed method, the system uses some predefined location to shuffle the RGB pixels. Proposed method gives better quality image along with increased security level.

V. Result and Discussion

The original secret image is encrypted using three steps and two shares are generated. The trusted people decrypt these two shares without any loss in the data. The decrypted shares are combined together in order to get original secret image.

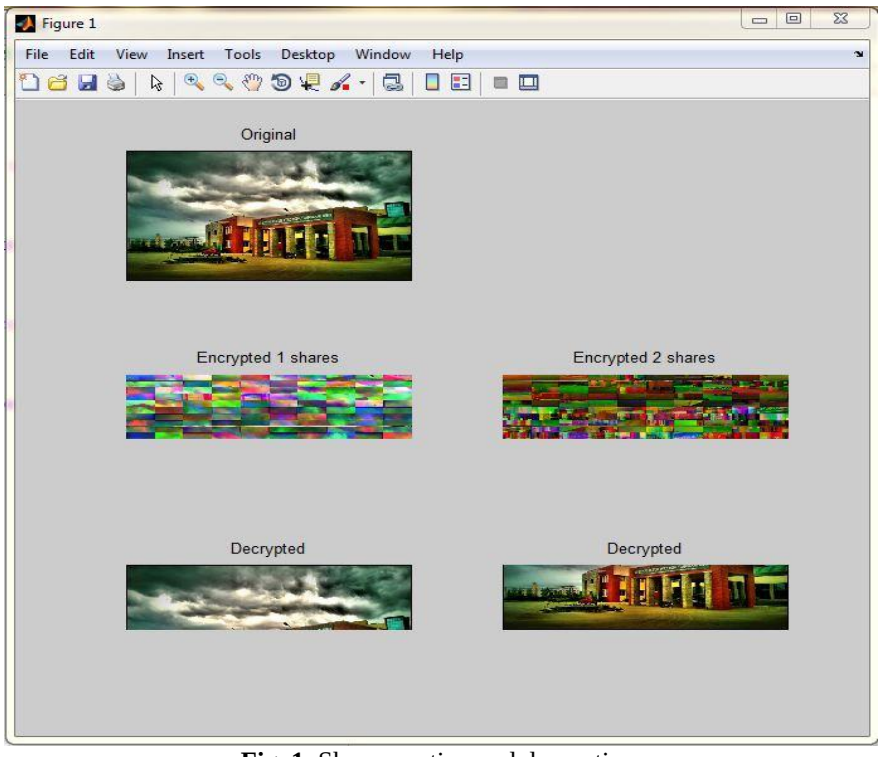

Fig. 1. Share creation and decryption

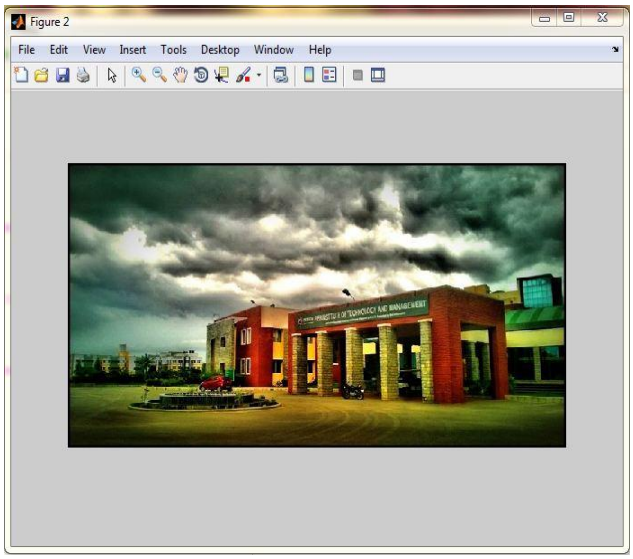

Fig.2. Recovered image after combining two shares

The histogram of an image is a graph showing the number of pixels in an image at each different intensity value found in that image. The result shows that no intensity loss at whole process. We observed that there is no distortion for the given image after retrieving process.

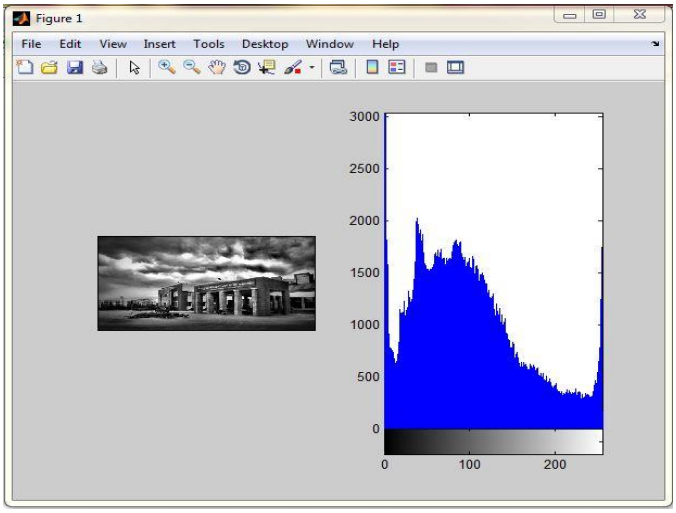

Fig. 3. Histogram of the input secret image

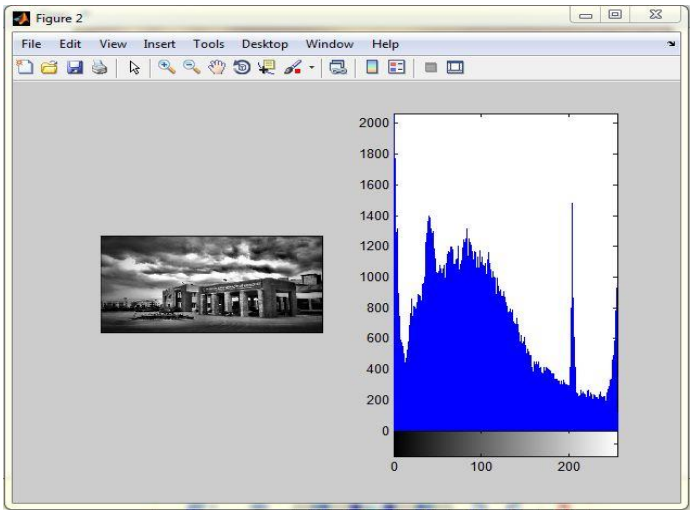

Fig. 4. Histogram of the recovered image

VI. Conclusion

In this paper different visual cryptographic techniques proposed by researchers are discussed. We proposed a new cryptographic technique for secure transfer of secret image. To overcome the disadvantage of conventional method for image encryption like key management and to overcome the drawback of image splitting technique like quality of the recovered image, a new cryptographic technique has been proposed in this paper. Original secret image is encrypted into two share images; each share image does not reveal any information about the secret. At the receiver side, decrypt two shares and combine to get the original secret image. The result shows that the quality of the recovered image is same as original image. The proposed method increased the level of security, which is essential to avoid from hackers. In the encryption process three steps are used to create shares and shares need to be decrypt and combine at the receiver side.

References

[1]. M. Naor and A. Shamir, "Visual Cryptography", Proceedings of Euro Crypt 1994
[2]. Zhi Zhou, Gonzalo R. Arce, Giovanni Di Crescenzo, "Halftone Visual Cryptography", IEEE Transaction on Image Processing, Vol. 15, No.8, August 2006
[3]. Bin Yu, Liguo Fang, XiaohuiXu, " A Verifiable Visual cryptography scheme", International Conference on Computational Intelligence and Security", 2008, pp. 347-350
[4]. Debasish Jena, Sanjay Kumar Jena, "A Novel Visual Cryptography Scheme", International Conference on Advanced Computer Control, IEEE 2008
[5]. Ran-Zan Wang, " Region Incrementing Visual Cryptography"., IEEE Signal Processing letters, Vol. 16, No. 8, August 2009
[6]. John Blesswin, Rema, Jenifer Joselin, "Effective Recovery Technique for Halftone Images in Visual Cryptography", IEEE 2010
[7]. Jaya, Siddharth Malik, AbhinavAggarwal, Anjali Sardana, "Novel Authentication System Using Visual Cryptography", 2011 World Congress on Information and Communication Technologies, pp: 1181-1186
[8]. Nitty Sarah Alex, L. JaniAnbarasi, "Enhanced Image Secret Sharing via Error Diffusion in Halftone Visual Cryptography", IEEE 2011, pp: 393-397
[9]. Young-Chang Hou and Zen-Yu Quan, "Progressive Visual Cryptography with Unexpected Shares", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 21, No.11, November 2011
[10]. Himanshu Sharma, Neeraj Kumar, Govind Kumar Jha, " Enhancement of Security in Visual Cryptography System Using Cover Image Share Embedded Security algorithm", International Conference on Computer and Communication Technology, 2011
[11]. J. K Mandal, SubhankarGhatak, "A Novel Technique for Secret Communication through Optimal Shares Using Visual Cryptography", International Symposium on Electronic System Design", 2011
[12]. Inkoo Kang, Gonzalo R Arce, Heung-Kyu Lee, " Color Extended Visual Cryptography using error Diffusion", IEEE Transaction on Image processing, Vol. 20, No. 1, 2011
[13]. John Blesswin, Rema, Jenifer Joselin, "Recovering Secret Image in Visual Cryptography", IEEE 2011
[14]. Divya A, K. Ramalakshmi, "Maintaining the Secrecy in Visual Cryptography Schemes", IEEE 2011
[15]. Feng Liu, Chuankun Wu, " Embedded Extended Visual Cryptography Schemes", IEEE Transactions on Information Forensics and security, Vol.6, No. 2, 2011
[16]. Xiao-Yi Liu, Ming-Song Chen and Ya-Li Zhang, "A New Color Visual Cryptography Scheme with Perfect Contrast", 8th International Conference on Communications and Networking in China, 2013, pp. 449-454
[17]. Gyan Singh Yadav, AparajitaOjha, " A Novel Visual cryptography Scheme Based on Substitution Cipher", Proceedings of the 2013 IEEE Second International conference on Image Information processing, 2013
[18]. Mizuho NAKAJIMA and Yashi YAMAGUCHI, "Extended Visual Cryptography for Natural Images"
[19]. Shylaja L.N, JayanthJeemarahalli, Shwethad.A, "Image encryption Without Using Key", AEIJST, 2014, Vol. 2, Issue 6
[20]. Siddharth Malik and Anjali Sardana, "A keyless Approach To Image Encryption", International Conference on Communication Systems and Network Topologies, 2012