International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Enhanced Security Providing using Visual Cryptography

Ketan Raju Kundiya[1], Ram B. Joshi[2]

Department of Computer Engineering, MMCOE Pune, Maharashtra, India

Abstract: ***A visual cryptography scheme (VCS) 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. Simple Visual Cryptographic technique is not secure. Because simple visual cryptography scheme only deals with creation of secret share and just combined it at receiver side. In the proposed system we apply visual cryptography technique. The image is to be transferred on the network (also known as secret image) is first compressed and then hidden by cover image using LSB technique. To enhance security, additional security measures are applied further to get encrypted image using symmetric key algorithm. The shares are generated from the encrypted image using RNS (Residual Number System) algorithm. Next share stacking procedure is applied using CRT (Chinese Remainder Theorem) algorithm to get final encrypted image at receiver side. Further, decryption of final encrypted image is done by using same algorithm which is used for encryption purpose. By applying this technique security and quality of image is improved and pixel expansion problem will get reduced.***

Keywords*:* Visual Cryptography, Visual Secret Share, Share Stacking, Security.

1. Introduction

Visual Cryptography is a special technique which is used to send the images securely over the network. Simple Visual Cryptographic technique is not secure. In traditional cryptographic technique involves dividing the secret image into shares for encryption purpose and some of these shares sent over the network, no extra security parameters added. The decryption process includes combining the shares to obtain the secret image.

This paper consists of a novel approach to how to securely image transfer over network. 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. Detail of overall working of proposed system shown in proposed system section.

A. Motivation

Many works in this area have been done and several algorithms have been developed. In 1994 Naor and Shamir proposed VCS which is a simple and secure method that allows sharing of secret without the need of any cryptographic computations. To encode the image, original image is split into n modified versions referred as shares. Decoding can be done by simply stacking subset s of those n shares.

Recently so many researches in the field of visual cryptography have been done and so many scholars are working to improve VCS.

Existing systems motivates the work can be done to improve the security of image for send over the network as well as secure sharing of key over the network. There is scope to automate the process of encryption for saving time and improve the quality of shares. Work can be done to improve quality of decrypted image at receiver side. Pixel expansion is problem in various existing systems. Work can be done in pixel expansion problem. Some technique can be made to improve the quality of resultant image and also to reduce the power consumption.

2. Literature Review

Shamir proposed [7] the first secret sharing scheme in 1979 designed to encode a secret data set into n shares and distribute them to n participants, where any k or more of the shares can be collected to recover the secret data, but any k - 1 or fewer of them will gain no information about it. After the scheme was proposed, many related topics have been studied. Feng Liu and Chuankun Wu proposed [1] about Embedded visual cryptography schemes. In this paper they have given an insight of how improve the visual cryptography by meaningful shares. Reduce the black ratio which enhances the visual quality of shares. It overcomes the drawbacks of traditional VCS i.e. Proposed VCS supports gray scale images. Smaller pixel expansion is used so pixel expansion is problem in this proposed system.

N. Askari, H.M. Heys and C. R. Mononey proposed [2] about an extended visual cryptography scheme without pixel expansion for halftone images. In this paper they propose a method for processing halftone images that improves the quality of the share images and eliminate the problem of pixel expansion. This paper proposed system does not provide the high level of security to image shares.

In the above system the sender takes a secret image and encodes into shares. After encoding this shares are sent to participants. The receiver collects the shares and stack to get decoded secret image. Here no verification is done so easy cheating is done. Manika Sharma and Rekha Saraswat

proposed [3] about Secure visual cryptography technique for color images using RSA algorithm. In this paper they are using cryptographic technique for color images i.e. color error diffusion with XOR operation. The shares are developed using random numbers and the key generated for decryption process is sent securely over network using RSA algorithm. This paper proposed system required improvement in the secure sharing of the key over the network.

Rajan Kumar, Prasanna Kumar, Sudeepa KB and Ganesh Aithal proposed [4] about improved security system using symmetric encryption and visual cryptography. In this paper introduced visual cryptographic technique applicable for both Bitmap Color and Grayscale images. This method uses the concept of Residual Number System (RNS) based on Chinese Remainder Theorem (CRT) for share creation and share stacking of a given image. The key is generated using a pseudo random number generator and Mixed Key Generation technique. The proposed approach like any other visual cryptographic approach is very secure, efficient, reliable, fast and easy to implement. The problem in proposed system is that it is only supports Bitmap Color and Grayscale images. We can add more security features to enhancement of security of overall system.

Akshatha M M, Lokesh B and Nuthan A C proposed [5] about Visual Cryptographic technique for enhancing the security of image transaction. In this paper, Chaotic Pseudo – Random Number generation, Zigzag Scan Pattern Method, Method to reduce the degradation of the resultant image is proposed by an extension from gray to colour image. Pixel Index Method is discussed to improve the security for images. An integration of this technique of Visual Cryptography with (n, k, p) gray image is also proposed. The problem in proposed system is that quality of images. Security can be increased by using additional security measures.

3. Extended Visual Cryptography

Traditional visual cryptography supports only black-and-white or binary images. An extended visual cryptography schem is a kind of visual cryptographic scheme which consists of meaningful shares. In this scheme embedding or combining random share into the meaningful shares, so it is called as embedded extended visual cryptography scheme [1]. In this scheme, lack of security measures exists rather than only embedding or combining of meaningful shares procedure.

Due to lack of security, intruder may gain access all random shares as well as meaningful shares to get original secret image. Pixel expansion problem still exist in this system. Following figure describes the actual architecture of Embedded Extended Visual cryptography Scheme

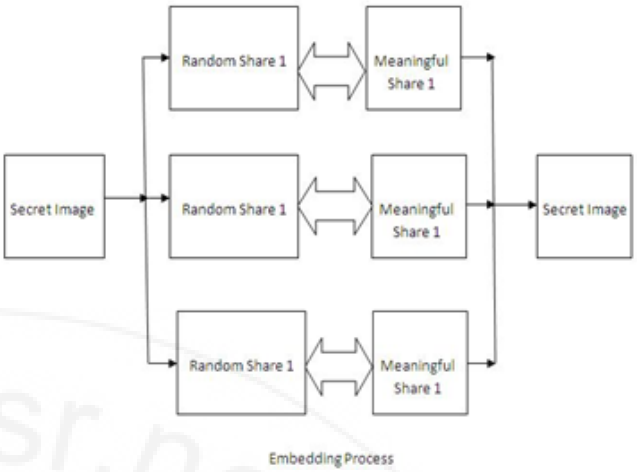

Figure 1: Embedded Extended Visual cryptography Scheme

4. Problem Statement

Most of the traditional Visual Cryptographic Techniques does not support color images. Pixel expansion is a problem because pixel width of the entire image increases thereby increasing its bandwidth. In existing systems, the sender takes a secret image and encodes it into shares. After encoding these shares are sent on the network. The receiver collects the shares and stack to get decoded secret image. Due to lack of security at this stage intruder may gain access to all shares.

Thus, Visual Cryptographic System requires enhancement in security process for transmission of image over network and reducing pixel expansion problem which should support colored images as well as maintain quality of images after decryption.

5. Proposed System

In proposed system, secret image hide by cover image. System uses s symmetric key cryptography for security issues. To add more security to secret sharing of the image, encryption is done before creation of shares. If intruder get all the shares, since secret image itself is encrypted he or she might not get any of the information about secret image. Lossless image compression methodology is apply before encryption for maintain more strengthen cryptography security because compressed image has less redundancy than the original image so cryptaanalysis is difficult. System can apply to different image format like jpeg, png etc.

Before the encryption Pixel Index Reversal technique is use to improve the security then Zigzag Scan Pattern is apply to increase the scrambling, thus increasing the security. System supports gray scale as well as colored images encryption. The problem of pixel expansion is reduced.

System provides more security because it uses symmetric encryption, steganography and visual cryptography is combined together. Following figure describes the actual architecture of Proposed System.

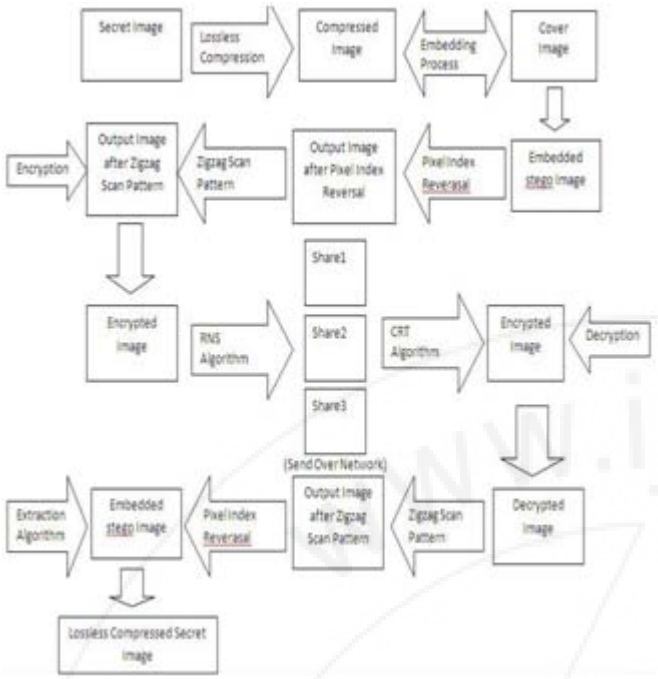

Figure 2: Architecture of Proposed System

6. Conclusion

We have introduced a novel visual cryptographic technique. The traditional visual cryptography system suffers from pixel expansion problem. The proposed technique overcomes this problem. Another drawback of existing VC schemes is if intruder can access all communication channels than reconstruction of secret can be done easily; since symmetric encryption is introduced before sharing secret; our approach overcomes this problem. Proposed system provides facility to transfer the image securely over the network, to support colored image, to reduce pixel expansion problem and to maintain quality of images etc. The concept of symmetric encryption, steganography and Visual cryptography is combined in proposed system to give a secured image sharing system.

7. Acknowledgment

We take this opportunity to thank Ms.H.K.Khanuja for their valuable guidance and for providing all the necessary facilities, which were indispensable in the completion of this paper. We are also thankful to all the staff members of the Department of Computer Engineering for their valuable time, support, comments, suggestions and persuasion. We would also like to thank the institute for providing the required facilities, Internet access and important books.

References

[1] Feng Liu and Chuankun Wu, "Embedded Extended Visual Cryptography Schemes", Ieee transactions on information forensics and security, vol. 6, no. 2,June 2011.
[2] N. Askari, H.M. Heys, and C.R. Moloney, "An extended visual cryptography scheme without pixel expansion for halftone images ", 2013 26th IEEE Canadian Conference Of Electrical And Computer Engineering (CCECE).
[3] 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.
[4] Rajan Kumar, Prasanna Kumar, Sudeepa KB and Ganesh Aithal, "Enhanced security system using symmetric Encryption and visual cryptography", International Journal of Advances in Engineering Technology, July 2013.
[5] 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.
[6] Roberto De Prisco, Alfredo De Santis,"Color visual cryptography schemes for black and white secret images", 2013 Elsevier B.V. All rights reserved.
Naor M. and Shamir A, “Visual cryptography” , In Proc. Eurocrypt 94, Perugia, Italy, May 9–12, LNCS 950, Springer Verlag, 1994, 1–12.