International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-5 Issue-6, August 2016

Lossless Visual Cryptography in Digital Image Sharing

Nikhila A, Janisha A

Abstract— 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. Visual cryptography is a secret sharing scheme which uses images distributed as shares such that, when the shares are superimposed, a hidden secret image is revealed. Visual cryptography schemes (VCSs) generate random and meaningless shares to share and protect secret images. The main issue in visual cryptography is quality of reconstructed image. The secret image is converted into shares; that mean black and white pixel images. There occurs an issue of transmission loss and also the possibility of the invader attack when the shares are passed within the same network. In this paper, a lossless TVC (LTVC) scheme that hides multiple secret images without affecting the quality of the original secret image is considered. An optimization model that is based on the visual quality requirement is proposed. The loss of image quality is less compared to other visual cryptographic schemes. The experimental results indicate that the display quality of the recovered image is superior to that of previous papers. In addition, it has many specific advantages against the well-known VCSs. Experimental results show that the proposed approach is an excellent solution for solving the transmission risk problem for the Visual Secret Sharing (VSS) schemes.

Index Terms— visual cryptography, visual secret sharing.

I. INTRODUCTION

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 Moni Naor and Adi Shamir in 1994 [3] 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. Visual cryptography is regularly used for image encryption. Encryption starts with the use of secret sharing concepts where the secret image is split into shares which are noise-like and secure. These images are then transmitted or distributed over an entrusted communication channel. Recognition of a secret message from overlapping shares and the secret image is decrypted without additional computations or cryptography knowledge. Visual cryptography schemes are characterized by two parameters: the expansion corresponding to the number of sub pixels contained in each share and the contrast, which measures the "difference" between black and white pixels in the reconstructed image. Combined the shares together reveal the information. Minimum two shares are needed for revealing the secret image. The shares are treated as black and white pixel; (n, n) matrix is used for representing black and white pixel. Visual cryptography (VC) proposes the methodology where the single image is encrypted into n shares and these shares are distributed to the various recipients who have authority to hold the original confidential image [1]. Any recipient can decrypt the image only if has 2 or more shares. If there is less number of shares then the proposed threshold for a single recipient will not be satisfied and then he would not be able to decrypt the image. Accumulating the k dividends reveals the confidential image, which is easily identified by human eye. Current shares which consist of many arbitrary and insignificant images are sufficient for protection of the confidential content but suffer from the high conveyance risk because the attackers may gain the information from the noise that are produced by the insignificant shares and try to seize the shares. This possibility leads to the difficulty of transmission losses and inability to deliver the original content to the intended user. Secret images are divided into share images which, on their own, reveal no information of the original secret. Shares may be distributed to various parties so that only by collaborating with an appropriate number of other parties, can the resulting combined shares reveal the secret image. Recovery of the secret can be done by superimposing the share images and, hence, the decoding process requires no special hardware or software and can be simply done by the human eye. Visual cryptography is of particular interest for security applications based on biometrics [2]. For example, biometric information in the form of facial, fingerprint and signature images can be kept secret by partitioning into shares, which can be distributed for safety to a number of parties. The secret image can then recovered when all parties release their share images which are then recombined.

II. RELATED WORKS

Ran –Zan Wang and Shuo-Fang Hsu, proposed a method for implementing visual cryptography (VC) in which an additional tag is attached to each generated share. The proposed ,tagged visual cryptography (TVC)[4] scheme works like a traditional VC scheme does, where the original image is encoded in shares in such a way that the secret can be revealed by superimposing any or more shares, but knowledge of less than shares gets no secret information.

Manuscript published on 30 August 2016.
***** Correspondence Author (s)
Nikhila A*, M.Tech Scholar, Department of Computer Science and Engineering, LBS Institute of Technology for Women, Thiruvananthapuram, India.
Janisha A, Assistant Professor, Department of Computer Science and Engineering, LBS institute of Technology for Women, Thiruvananthapuram, India.

A notable characteristic of TVC is that an extra tag can be revealed by folding up each share, which provides users with supplementary information such as augmented message or distinguishable patterns to identify the shares. The tagging property can easily be applied to any reported VC scheme to endow the generated shares with more capabilities. A common characteristic of both traditional VC and extended VC schemes is that a single share carries no useful information to users. In this letter, a method to endow VC schemes with the ability of displaying tag patterns by folding up a single share is proposed. The tagging property enriches new functions to the target shares. For example, it can display fake message to establish a cheating mechanism to unauthorized inspectors, or the tag pattern can exhibit unique symbol associated with each sharing instance, and provide a user-friendly environment for users to distinguish among and manage to the numerous shares. The proposed method is simple and can easily be applied to any reported VC schemes.

Visual secret sharing for multiple secrets [5].Conventional visual secret sharing schemes are designed for a single secret image so it is inefficient to generate numerous share images for multiple secret images simultaneously. Therefore, a novel visual secret sharing scheme for multiple secret images is proposed in this scheme. In the proposed encryption process, a stacking relationship graph of secret pixels and share blocks is generated to indicate the encryption functions, and a set of visual patterns is defined to produce two share images according to this graph. Based on the stacking properties of these patterns, the secret images can be obtained from the two share images at aliquot stacking angles. In this scheme makes the number of secret images not restricted and further extends it to be general. As a result, the proposed scheme enhances visual secret sharing schemes' ability for multiple secrets. In visual cryptography mainly images are handled, shares are embedded with another carrier images.

The visual cryptography scheme (VCS) is a secure method that encrypts a secret image by breaking it into shares. A distinctive property of VCS is that one can visually decode the secret image by superimposing shares without additional computation .The method presents an approach for embedding visual cryptography generated image shares in the host images to provide authentication for the VC shares and makes these secret shares invisible by embedding them into host images. The secret shares generated from VC encryption are watermarked into some host images using digital watermarking. Digital watermarking is used for providing the double security of image shares. The share is embedded into the host image in frequency domain using Discrete Cosine Transform (DCT). In frequency domain, the obtained marked image must be less distorted when compared to the original image. Thus secret shares are not available for any alteration by the adversaries who try to create fake shares. Every pixel of the binary Visual cryptography share is invisibly embedded into the individual block of the host image. The process of watermark extraction necessitates only the watermarked image and it does not require the original host image.

The scheme provides more secure and meaningful secret shares that are robust against a number of attacks like blurring, sharpening, motion blurring etc. There are various innovative ideas and extensions exist for the basic visual cryptographic model. In the existing VC schemes no security is provided to the secret shares and adversaries can alter its bit sequences to create fake shares. And in the proposed scheme, the vulnerability of these binary secret shares is overcome by hiding them invisibly into some host images. During the decryption phase, the secret shares are extracted from their cover images without needing any of the cover image characteristics because the watermark extraction technique is blind. The overlapping of these shares reveals the secret. The decoded secret image quality is improved. In recent works, the data will embedded to secret shares and send embedded data images to other participants. The other related work is decoded image quality is increased and the security of share is improved by using watermarking methods.

III. PROPOSED SYSTEM

The lossless visual cryptography in digital image sharing includes the following four major phases: (1)Image pre-processing phase (2)Share construction phase (3)Share watermarking phase (4)Image extraction phase. Fig 1 shows the architecture of proposed technique.

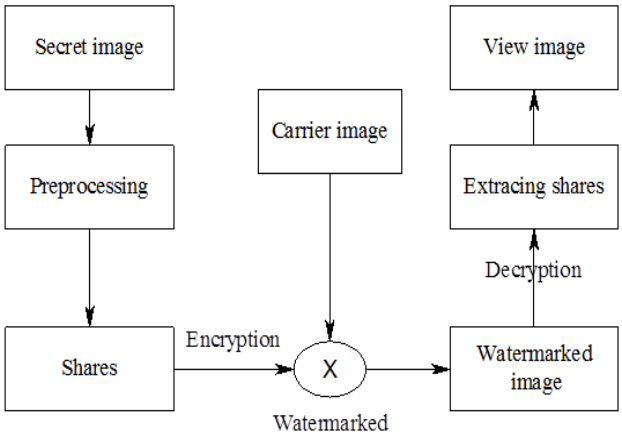

Fig.1: Proposed System Architecture

A. Image Pre-Processing phase

An image is an array, or a matrix, of square pixels (picture elements) arranged in columns and rows. Image processing is any form of signal processing for which the input is an image, such as a photograph or video frame the output of image processing may be either an image or a set of characteristics or parameters related to the image. Most image-processing techniques involve treating the image as a two-dimensional signal and applying standard signal-processing techniques to it. Image processing is computer imaging where application involves a human being in the visual loop. In other words the image is to be examined and acted upon by people.

In the image preprocessing module first select one secret image; and that image is converted into gray scale image and binary image.

B. Share Construction Phase

In this proposed scheme the secret image is divided into shares. The original image is divided into two 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.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

To decode the image, each of these shares is xeroxed onto a transparency. Stacking both these transparencies will permit visual recovery of the secret. In this module the secret image is selected and the white pixels in the image will be removed first and then each black pixel in the image is replaced to different shares. The shares will be stacked together to reveal the secret.

C. Share Watermarking Phase

In this module the share will be encrypted first. RC4 encryption method is used for encryption; first given a key value for share encryption. Key should be character or digits. Then the shares are converted to bit stream and encrypt this bit stream with the keys. The encrypted share is then watermarked to the carrier images. Invisible watermarking, LSB watermarking method is used.

RC4 Encryption: The RC4 algorithm is remarkably simply and quite easy to explain. A variable-length key of from 1 to 256 bytes (8 to 2048 bits) is used to initialize a 256-byte state vector S, with elements S[0], S[1], …, S[255]. At all times, S contains a permutation of all 8-bit numbers from 0 through 255. For encryption and decryption, a byte *k* is generated from S by selecting one of the 255 entries in a systematic fashion. As each value of *k* is generated, the entries in S are once again permuted.

LSB Watermarking: Select carrier image and watermarking the encrypted share to the carrier image. Pixel values of share image and carrier image are converted into binary. The carrier image is of size m x n and the watermark image is of size (m x n)/8. The least significant bit of each pixel of carrier image is replaced by the each bit of watermark image. In this way watermark is embedded and watermarked image is obtained.

D. Image Extraction Phase

At the image reconstruction side the shares will be extracted. The secret data is extracted from the watermarked image. The watermarked images are uploaded and then extracting the encrypted shares from the watermarked image. The encrypted shares are then decrypted using the key and the shares are obtained. Then combining the shares together reveals the secret image. The quality of secret image is same as the original secret image.

IV. Experimental Evaluation

C#.NET, Visual Studio 2010 framework is used to implement the proposed visual cryptography technique. 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. On the other hand, in order to evaluate and compare the performance of different visual cryptography methods, it is necessary to judge the visual quality of the decrypted images.

For evaluating the performance of the proposed technique, it is compared with existing technique, NVSS. Test cases are selected for comparison purposes. The test case includes small number of images selected from the data set. For comparing the Traditional Digital Image Sharing Method is compared with the proposed method. The time consumption during image extraction phase is used for performance evaluation purpose. The graph shown in figure 2 shows the comparison between the execution time of both. The result shows that lossless visual cryptography has faster convergence time compared to NVSS.

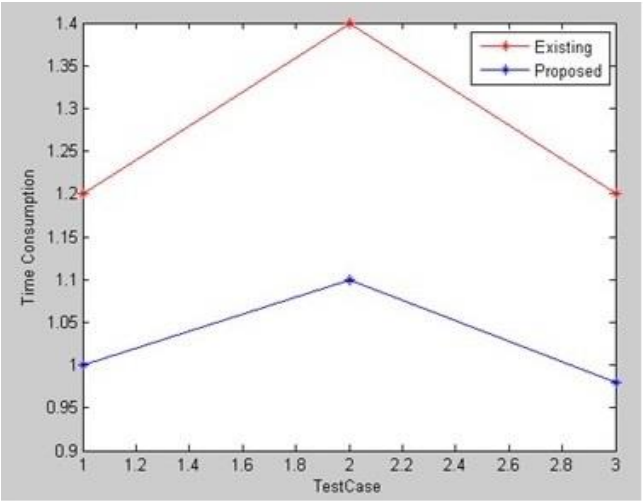

Fig.2: Time consumption (Traditional Method Vs Lossless Visual Cryptography scheme)

In the graph fig 3 the size of reconstructed image in lossless method is larger compared to the size of the reconstructed image in traditional method. Since the size of the image becomes larger the quality of image also increases so in proposed method the reconstructed image has same quality compared to the original secret image. But the traditional method secret image has low clarity compared with the input secret image.

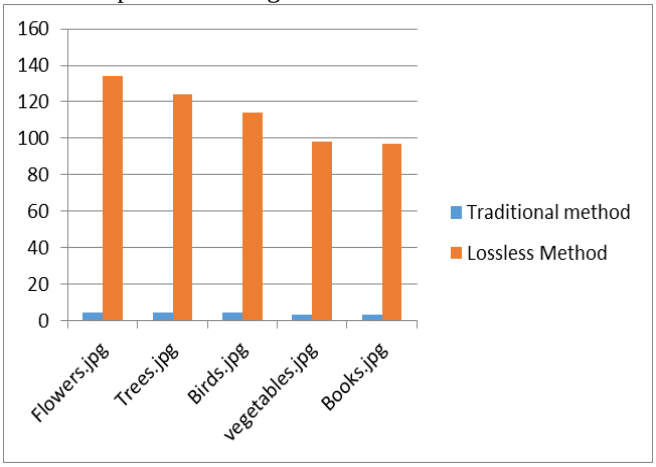

Fig.3: Comparison based on size of the output image in Lossless DCT method and Digital Image sharing in Traditional method

V. Conclusion

Visual cryptography (VC) is a process where a secret image is encrypted into shares which refuse to divulge information about the original secret image. The secret image can be recovered simply by stacking the shares together. In conventional VC at the decoding time the quality of original image will be reduced.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

This problem is overcome by using a lossless tagged visual cryptography scheme, which is one of the most efficient multi-secret visual cryptography (MVC) schemes. Specifically, lossless means that the proposed LTVC scheme encodes the tag image without affecting the rebuilt secret image. This paper provides double security through encryption and watermarking. Encryption provides security by hiding the content of secret information; while watermarking hides the existence of secret information. Earlier works were concentrated on share construction only. The proposed system helps to protect the lossless share with encryption and watermarking. Here invisible watermarking; LSB method and RC4 encryption are used. The algorithm is simple to implement as it is directly performed in the compressed-encrypted domain. This scheme also preserves the confidentiality of content as the embedding is done on encrypted data.

ACKNOWLEDGMENT

We are greatly indebted to our principal, Dr. JAYAMOHAN J, Dr. V. GOPAKUMAR, Professor, Head of the Department of Computer Science and Engineering, Mrs. JANISHA A, Assistant Professor, Department of Computer Science and Engineering, LBS Institute of Technology for Women who have been instrumental in keeping my confidence level high and for being supportive in the successful completion of this paper. We would also extend our gratefulness to all the staff members in the Department; also thank all my friends and well-wishers who greatly helped me in my endeavor. Above all, we thank the Almighty God for the support, guidance and blessings bestowed on us, which made it a success.

REFERENCES

1. Kai-Hui Lee and Pei-Ling Chiu “Sharing Visual Secrets in Single Image Random Dot Stereograms” IEEE Transactions on Image Processing, Vol.23, No. 10, October 2014
2. A. Ross and A. A. Othman, “Visual Cryptography for Biometric Privacy”, IEEE Transactions on Information Forensics and Security, vol. 6, no. 1, pp. 70-81, 2011.
3. M. Naor and A. Shamir, “Visual cryptography,” in Advances in Cryptology-EUROCRYPT 1994, ser. Lecture Notes in Computer Science, A. De Santis, Ed.
4. R.-Z Wang and S.-F. Hsu, “Tagged visual cryptography,” IEEE Signal Process. Lett. vol. 18, no. 11, pp. 627-630, 2011.
5. J.-B. Feng, H.-C. Wu, C.-S. Tsai, Y.-F. Chang and Y.-P. Chu, “Visual secret sharing for multiple secrets, “Patt. Recognition. vol. 41, no. 12, pp.35723581, 2008.