Review On Tagged Visual Cryptography

[1]Nikhila.A, [2]Janisha A
[1]MTech Scholar, [2]Assistant Professor
[1]Department of Computer science and Engineering,
[1]LBS Institute of Technology For women, Thiruvananthapuram, India

Abstract*—*Security has gained a lot of importance as information technology is widely used. 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. The loss of image quality is less compared to other visual cryptographic schemes.

Index Terms*—*Visual cryptography; Shares;

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 [4] 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. The text data is converted to image format and use that textual data as image. 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. White is represented as “0”and black pixel is represented as “1”.

The lossless TVC (LTVC) scheme which hides multiple secret images without a_ecting the quality of the original secret image. As a result, the decoder can rebuild exactly the identical secret image as that of conventional VC. In other words, the shares are losslessly modified to hide the tag images. The shares are watermarked first, an improved image watermarking invisible LSB embedding method, then the embedded image is encrypted by using AES modified encryption method. Using this encryption the security of share is increased.

II. EXISTING WORKS

Visual secret sharing for multiple secrets. 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.

A. Embedded Extended Visual Cryptography Schemes:

A visual cryptography scheme (VCS) is a kind of secret sharing scheme which allows the encoding of a secret image into n shares distributed to n participants. The beauty of such a scheme is that a set of qualified participants is able to recover the secret image without any cryptographic knowledge and computation devices. An extended visual cryptography scheme (EVCS) is a kind of VCS which consists of meaningful shares (compared to the random shares of traditional VCS).Feng Liu and Chuankun Wu, proposed a construction of EVCS which is realized by embedding random shares into meaningful covering shares, and we call it the embedded EVCS. Experimental results compare some of the well-known EVCSs proposed in recent years systematically, and show that the proposed embedded EVCS has competitive visual quality compared with many of the well-known EVCSs in the literature. In addition, it has many specific advantages against these well-known EVCSs, respectively.

B. Tagged Visual Cryptography:

Ran ZanWang 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)[2] 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. 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.

C. A Lossless Tagged Visual Cryptography Scheme:

XiangWang, Qingqi Pei and Hui Li,stated a main issue in visual cryptography is quality of reconstructed image. In this method the quality of reconstructed image is higher, compare with conventional visual cryptographic scheme. The secret image is converted into shares, that means black and white pixel images. Each share is embedded to different carrier images. For security, the shares are encrypted, AES modified encryption method is used. The encrypted shares are send to other participants. At the receiver end receiving the shares and decrypt the shares, then combining these shares together reveal the secret. The quality of rejoined shares and original secret shares are almost same. The loss of image quality is less compared to other visual cryptographic schemes.

As one of the most efficient multi-secret visual cryptography (MVC) schemes, the tagged visual cryptography (TVC) [2] is capable of hiding tag images into randomly selected shares. However, the encoding processes of TVC and other MVC schemes bring distortion to a share, which definitely lowers the visual quality of the decoded secret image. This letter proposes an extended TVC scheme, named as lossless TVC (LTVC). Specifically, “lossless” means that the proposed LTVC scheme encodes the tag image without affecting the rebuilt secret image, i.e., the decoded secret image of LTVC has the same visual quality with that of the conventional VC scheme [4]. Moreover, we propose the probabilistic LTVC (P-LTVC) to solve the potential security problem of LTVC. Finally, the superiority of the proposed scheme is experimentally verified. A model can be proposed for lossless multi-secret visual cryptography method based on conventional Visual Cryptography scheme. We can propose a (k,k) and (k,n) LTVC and P-LTVC schemes that can embed additional k-1 tag images as well as the secret image. Stacking shares together reveals the secret image, and folding up one of k-1 specific shares discloses the tag image. Compared with other multi-secret scheme, the most important advantage of LTVC and P-LTVC is that the embedding of tag images does not lower the quality of the original secret image. The experimental results illustrate that the stacking results of LTVC and P-LTVC has a higher contrast than that of previous tagged visual cryptography method.

D. Digital Image Sharing by Diverse Image Media:

Conventional visual secret sharing (VSS) schemes hide secret images in shares that are either printed on transparencies or are encoded and stored in a digital form. The shares can appear as noise-like pixels or as meaningful images; but it will arouse suspicion and increase interception risk during transmission of the shares. Hence, VSS schemes suffer from a transmission risk problem for the secret itself and for the participants who are involved in the VSS scheme. To address this problem, a natural-image-based VSS scheme (NVSS scheme) that shares secret images via various carrier media to protect the secret and the participants during the transmission phase is proposed. The proposed (*n, n*) - NVSS scheme can share one digital secret image over *n*-1 arbitrary selected natural images (called natural shares) and one noise-like share. The natural shares can be photos or hand-painted pictures in digital form or in printed form. The noise-like share is generated based on these natural shares and the secret image. The unaltered natural shares are diverse and innocuous, thus greatly reducing the transmission risk problem. Possible ways to hide the noise-like share to reduce the transmission risk problem for the share is also considered. Experimental results indicate that the proposed approach is an excellent solution for solving the transmission risk problem for the VSS schemes.

III. CONCLUSION

We propose lossless multi-secret visual cryptography method. We can also develop a scalable and effective heuristic approach to deal with the complexity and limitations. Quality improvement methods can also be proposed, and achieve a better image visual quality. We can detect the global contrast enhancement in both uncompressed and previously JPEG-compressed images.

IV. ACKNOWLEDGMENT

We are greatly indebted to our principal Dr. K. C. RAVEENDRANATHAN, Dr. SHREELEKSHMI R, Professor, Head of the Department of Computer Science and Engineering, Mr. MANOJ KUMAR G., Associate Professor, Department of Computer Science and Engineering, LBS Institute of Technology for Women who has 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] Feng Liu and Chuankun Wu, “Embedded Extended Visual Cryptography Schemes, ”IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 6, NO. 2, JUNE 2011

[2] Ran-Zan Wang and Shuo-Fang Hsu, “Tagged Visual Cryptography,”IEEE SIGNAL PROCESSING LETTERS, VOL. 18, NO. 11, NOVEMBER 2011

[3] Xiang Wang, Qingqi Pei, and Hui Li "A Lossless Tagged Visual Cryptography Scheme " IEEE SIGNAL PROCESSING LETTERS, VOL. 21, NO. 7, JULY 2014

[4] M. Naor and A. Shamir, "Visual cryptography," Advances in Cryptology EUROCRYPT 1994, ser. Lecture Notes in Computer Science, A. DeSantis, Ed. Berlin/Heidelberg, Germany: Springer, 1995, vol. 950, pp. 112.

[5] Kai-Hui Lee and Pei-Ling Chiu," Digital Image Sharing by Diverse Image Media", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 1, JANUARY 2014