Secret Sharing Schemes: A Survey towards its Growth

R. Divya
Research Scholar,
Alagappa University,
Karaikudi, Tamilnadu, India.

Abstract
A secret image kept in a single information-carrier could be easily retrieved or damaged by unauthorized entity. Once the confidential image information is illegitimately retrieved, the unauthorized person makes use of the content for their own benefits. In the gigantic internet communication, the secret image sharing schemes can be used to share a secret image with utmost confidentiality over unsecured public channels. In this scheme a secret image is programmed into \( n \) shadows of arbitrary prototypes. It is possible to decode the secret image visually by superimposing a qualified subset of shadows. Nevertheless, no secret image can be acquired from the superposition of an illegal subset. This paper describes detailed overview of the current trends and previous contributions of the research on digital image security. The limitation of the each paper was studied well to focus better on the future directions on secret image sharing schemes.

1. Introduction

Nowadays transmitting multimedia data by means of all-pervasive Internet is the trend gaining interest [34]. With the advent of e-commerce, it has become extremely essential to tackle the sensitive issues of affording data security, especially in the ever-blooming open network environment of the modern era[35-40]. The encrypting technologies of the time-honored cryptography are generally employed to shelter data safety extensively[41-48]. Cryptography is used to send and receive encrypted information which can be decrypted only by the sender or receiver. This technique is mainly used to store and transmit the data in an appropriate manner that can be read and processed only by the intended person. In the cryptography process,
encryption is the conversion of plaintext (ordinary text or clear text) into cipher text and the reverse process is called decryption and the people who are working in this domain are called as cryptographers[49-55]. With the emergence of multimedia applications, there is a huge demand for transmission and secured storage of information. So security is indispensable for proper data protection. If the information is protected, the intruders may not be able to distort the data. It becomes challenging to transmit the data in a secured and proper manner. Cryptographic techniques afford the confidentiality and security by reducing the prospect of adversaries. Unlike traditional cryptographic methods such as Data Encryption Standard (DES) scheme and Advanced Encryption Standard (AES) scheme, the Visual Cryptography (VC) scheme provides fast decryption without any complex computation. Visual Cryptography (secret sharing scheme) is a modern cryptographic technique used to share the secret data in a secure pattern, maintained with utmost confidentiality[56-61]. A sender transmits the secret data which is divided into shadows and it holds hidden information. When all of these shadows are aligned and stacked together, it tends to expose the secret data information to the receiver [62].

The main role of VC scheme is to encrypt the secret data with the help of partitioning process. The private message cannot be revealed by the help of some split data’s. The original image requires all split data’s to be revealed. The process of visual cryptography is to divide an image into prearranged number of parts and then without any computation or algorithm, the secret data can be revealed by aligning and stacking together. Another, secret sharing scheme is Visual Secret Sharing (VSS), based on the (k-n) threshold concept. This method works out of n shadow with any k or more reconstructed shadows to retrieve the original secret by superimposing the shadows that eliminates complex computations.

2. Development of Secret Image Sharing Schemes

2.1 Evolution of Secret Image Sharing Schemes

With the rapid development of multimedia data, it is important to maintain the confidentiality of such data. The sender transmits the secret data over unsecure channel which can be easily retrieved or ‘damaged’ by unauthorized entity. Once the confidential information is illegitimately retrieved, the unauthorized person makes use of the content for their own benefits. This main issue was solved in the year 1979, by Blakley in [7] and Shamir in [2] introduced the Secret Sharing (SS) schemes in which
the secret data is partitioned into \( n \) shares and distributed to \( n \) participants with utmost confidentiality and availability. The \((k, n)\) threshold schemes \([3, 8, 9]\) possess some properties such as secret data which can be recovered only from \( k \) shares or more than \( k \) shares. In case, if any \( k-1 \) or less than \( k \) shares request for access, the secret data cannot be recovered. To evaluate a secret sharing scheme, four conditions such as security, contrast, computational complexity and pixel expansion are used \([2, 7, 10-12]\). The schemes satisfying the security and recovering the original secret image is without any loss. Unfortunately, computational complexity is high in non-visual SS schemes. To eliminate this issue the VSS (Visual Secret Sharing) schemes were proposed in \([1,5]\) which uses the human visual system in order to share the visual data such as pictures, printed text, documents and also the computational complexity is low in this scheme. But there was a problem of pixel expansion since each original pixel is coded into \( m \) subpixels per shadow image. In 1987, the credit goes to Kafri, Oded, and EliezerKeren for launching the concept of VSS based Random Grids (RG) in \([13]\) without the absence of pixel expansion problem. Various researchers are also solved in \([5, 14, 15]\) the aforementioned drawbacks by probabilistic visual schemes which has no computational complexity and also no pixel expansion. Even though this scheme provides a solution for pixel expansion and complexity problem, still it suffers from reconstruction precision. To overcome this issue, Cimato et al. \([5]\) designed a generalized probabilistic scheme (ProbVSS) by performing two Boolean Exclusive operations, OR (\( \oplus \)) and AND (\&\) that allow to recover the secret image in lossless manner. The previous schemes are applicable only in case of binary images \([16,17]\). After this the number of schemes are proposed for both grayscale images and ‘numerical’ color images in \([1, 18, 19]\).

### 2.2 Recent Trends in Secret Image Sharing Schemes

Wang et al. have proposed \([6]\) a \((2, n)\) scheme for binary images which is called Boolean-based VSS. In this scheme, Boolean AND & Exclusive OR operations are used to attain good performance with no pixel expansion and the original secret image is reconstructed entirely in decoding phase with low computational complexity. It doesn’t support fault tolerance property.

Ran-Zan Wang et al. have developed \([20]\) a method different images are encoded using Huffman codes and the numerical operations of the sharing functions are calculated in \( GF(2^t) \). By using this method, the size of the shadow images is
reduced. Further, the probability of the error propagation problem is also reduced and limits the propagation effect within the block, where the error occurs. Though it achieved good performance with some properties such as restoration of the original image without any loss, if lower than $r$ images are shared, it is not enough to reveal the original secret image. Further the size of the shadow images are also less than $1/r$ when it is compared with confidential original image.

In 2009, Chin-Chen Chang et al. implemented a new $(2, 2)$ Verifiable Secret Sharing (VSS) scheme [21]. In this scheme, an original image is secured followed by the process in which the users are allowed to perform verification on the recovered secret image in the phases of reveal and verify. The author used halftone logo to check whether the recovered original secret image is right or not. The proposed scheme consists of two phases such as ‘shares construction’ phase and ‘revealing and verifying’ phase. The experimental results confirmed that this method yielded better quality images. The research was concluded in their proposed scheme that the participants need not execute the verification procedural steps. They are expected only to execute verification once to find out whether the recovered image is right.

Yung-Yi Lin et al. proposed a $(k, n)$ scheme [22], in which the restored image is lost if $k<n$, lossless in case if $k=n$. It supports the fault tolerance property, but computational complexity is $O(k\log^2 k)$, since they also utilized ‘Thien and Lin’ secret sharing scheme [24]. Kuang-Shyr Wu’s method [23] focused on the improvement of Thien-Lin scheme. In Thien-Lin Scheme [24], the input pixel values must be truncated into 0 to 251. The light pixel values that are greater than 251 of the secret image are lost. This is not suitable for light images. So, Kuang-Shyr Wu’s [23] used the prime number 257 instead of 251 and achieved good performance when restoring secret image without any loss. In addition to that, the size of the shadow images is reduced and computation time is also saved. This proved that scheme is applicable for light images.

Amitava Nag et al. proficiently put forward a new $(k, n)$ secret sharing scheme [25] with the help of Boolean operations. In this scheme, $n-k$ shares are lost, secret image could be recovered using remaining $k$ shares. The restored image is lost in case if $k<n$ and lossless when $k=n$. Moreover, reconstruction complexity is of low means $O(k)$ and expressed better fault tolerance property than other schemes [6, 26].

Tzung-Her Chen et al. developed an algorithm [27] for $(n+l, n+l)$ multi-secret sharing using XOR operations. In this scheme, ‘$n$’ original data (image) is
encoded into \( n+1 \) meaningless shadow images and need all \( n+1 \) share to restore all \( n \) secret images. Moreover, extra random matrix is used to create shared images. This advanced scheme provides some features such as Restoration of original image in lossless manner, absence of pixel expansion problem and also no codebook required. Computational cost is \( O(m) \) for \( n \) secret images.

Xuehu Yan et al. have suggested a \((k, n)\) threshold VSS method [28] that depends upon the RG with AND and XOR operations to accomplish a non-destructive recovery. If less than \( k \) shadow images are collected, information of the secret image cannot be revealed. This scheme has good features such that no pixel expansion, no codebook required and reconstructed image is lossless.

Chin-Chen Chang et al. combined C.C. Chang, M.N. and Wu GSBTC schemes to compress an original secret color image with Shamir’s \((k, n)\) threshold method and introduced a new scheme [29] for sharing confidential color image. In this method, the loss can be overcome during data transfer and size of the each shadow decreases when the number of shadows increases. This scheme doesn’t support the fault tolerance property.

Tsung-Lieh Lin et al. introduced a novel VSSM scheme [30], in which the secrets are divided into two parts and then logic OR operation is executed between the parts of different secrets. The randomness is increased by introducing certain camouflaging. Through this process flow, scheme meets the goal with absence of pixel expansion problem. But the secret has noise because of camouflaging. This problem was resolved in another research study conducted by Lin, Pei-Yu, and Chi-Shiang Chan [32].

Gyan Singh Yadav et al. proposed a multi-secret sharing scheme [32] based on the capabilities of bit-plane flipping and Boolean operations. In this scheme, two levels of encryption are performed. The first level is flipping some of the bit planes in circular order that makes it random. Further, to improve the security, another level of encryption is performed by using XOR. This scheme successfully completes the objective with two layer security, no pixel expansion problem; lossless retrieval of secret image and also no codebook is needed.

Sachin Kumar et al. have developed the method [33] for threshold VSS using Boolean operations. In this method two algorithms are designed to encode a plain image into \( n \) unmeaning shares. Thus, no confidential data is retrieved by exclusive OR of any \( k-1 \) or less shares, otherwise the data is revealed. This scheme is the
extension of Boolean basis of non-threshold VSS into threshold VSS with the achievement of no pixel expansion problem. The benefits of this scheme includes no codebook requirement, no alignment required during decoding process and also encoding binary, gray mode or color images.

3. Conclusion

This paper presented a survey on various studies conducted in the areas of secret image sharing schemes. The secret image sharing features of the existing algorithms are carefully investigated in this paper. From the above investigations, it is found that each SIS scheme has its own merits, even though, there is a need to improve in terms of pixel expansion problems, loss of reconstruction accuracy, reconstruction complexity problem, low quality of the reconstructed image and diminished security of shadows all at the one time.

References


Ito, Mitsuru, Akira Saito, and Takao Nishizeki, “Secret sharing scheme realizing general access structure”, Electronics and Communications in Japan


1397


