Signal Processing: Image Communication 65 (2018) 210–220

Contents lists available at ScienceDirect

Signal Processing: Image Communication

journal homepage: www.elsevier.com/locate/image

A construction method of (t, k, n)-essential secret image sharing scheme

Peng Li [a,*], Zuquan Liu [a], Ching-Nung Yang [b]

[a] Department of Mathematics and Physics, North China Electric Power University, Baoding, Hebei, China
[b] Department of CSIE, National Dong Hwa University, Taiwan

ARTICLE INFO

Keywords:
Secret image sharing
Secret sharing
Essential shadows
Lagrange interpolation

ABSTRACT

Secret image sharing (SIS) is a technique to decompose a secret image into multiple shadows distributed to the corresponding participants. Only qualified subsets of the shadows can reveal the secret image. Usually all shadows have the same importance. However, in some application scenario, some shadows are accorded with the special privilege due to the status or importance of the corresponding participants. A (t, k, n) essential secret image sharing (ESIS) scheme share a secret image into n shadows including t essential shadows and n–t non-essential shadows. A qualified subset of the shadows should contain at least k shadows including all t essential shadows. In this paper, we propose a construction method of (t, k, n) essential secret image sharing (ESIS) scheme. In our scheme, all shadows have the size $1/k$ times of the secret image. It also resolves the problems in the previous ESIS schemes, such as different shadow sizes, concatenation of sub-shadows, using multiple SIS schemes and so on. Theoretical analyses and experimental results show that the proposed scheme is secure and effective.

1. Introduction

Image secret sharing is a kind of technique to prevent secret image from being lost or modified during storage and transmission. A secret image is first shared into multiple shares, also called shadows. If and only if the qualified subset of those shadows can be used to reveal the secret image, while the unqualified subset of the shadows cannot get any information about the secret image.

In 1979, Blakley [1] and Shamir [2] first independently proposed the concept of (k, n) threshold secret sharing scheme. In their scheme, the dealer shares the secret into n shadows, and distributes them to n participants. Any k or more shadows can reveal the secret. However, with less than k shadows, no information about the secret can be revealed. Based on Shamir's work, Thien and Lin [3] extended his work and first proposed a secret image sharing (SIS) scheme by embedding secret pixels into all coefficients of a $(k-1)$-degree polynomial. The shadow size of their (k, n)-SIS scheme is $1/k$ times of the secret image. In [4], the shadow size was further reduced by using Huffman code. SIS schemes have been exploited in many applications as a means to protect secret image. Various SIS schemes with specific functions were introduced, such as SIS schemes with the meaningful shadows [5–7], scalable SIS schemes [8–11], multiple SIS schemes [12–14] and SIS scheme with adversary structure [15].

Since noise-like shadow images would attract the attention of the censorships, it is desirable to design SIS schemes to get the meaningful shadows. In 2004, Lin et al. [5] realized a novel secret image sharing scheme by using steganography and authentication approach. However, their scheme has a distortion of the retrieved secret image and causes pixel expansion of the secret image. To achieve a lossless scheme, Yang et al. [6] improved Lin et al.'s method [5] by using Galois Field GF (2^8). In 2013, Ulutas et al. [7] designed an invertible secret image sharing scheme utilizing the modulus operation, where the quality of the shadow images is highly improved. In addition, a kind of scalable SIS (SSIS) scheme were introduced in the literatures [8–11], which provide progressive decoding. In SSIS schemes, the information amount of the reconstructed image is proportional to the number of shadows participated in the revealing process. A $(2, n)$ scalable secret image sharing scheme was first proposed by Wang et al. [8] in 2007. Then, Yang et al. [9] modified their work and proposed a general (k, n) scalable secret image sharing scheme. However, there is no property of smooth scalability in schemes [8,9]. Soon after, two SSIS schemes with smooth scalability were introduced in [10,11].

The schemes mentioned above only consider sharing one secret image. Some multi-secret image sharing schemes were proposed to share multiple secret images, which refers that each secret image can be revealed in line with the corresponding access structure. Recently, in [12], Guo et al. employed Chan and Chang's multi-secret sharing [13] to propose a new multi-threshold SIS scheme based on the generalized Chinese Reminder Theorem (CRT). Given a qualified subset of the shadows, each secret image can be recovered without distortion. Meanwhile,

* Correspondence to: School of Mathematics and Physics, North China Electric Power University, Baoding 071003, China.
E-mail address: lphit@163.com (P. Li).

https://doi.org/10.1016/j.image.2018.04.002
Received 5 September 2017; Received in revised form 4 April 2018; Accepted 4 April 2018
Available online 12 April 2018

any monotone access structure is possible to be realized with a deletion procedure. Afterwards, a Boolean-based multiple secret image sharing scheme was proposed by Chen et al. [14] to share different sized secret images, which is different from the previous multi-secret image sharing scheme. In 2016, Guo et al. [15] introduced a new concept of a (k, n) threshold secret image sharing scheme with adversary structure. The adversary structure implies that unauthorized groups of participants cannot reveal the secret image. In their scheme, the secret image can be reconstructed without distortion, if and only if the participants involved in decoding process satisfy the threshold condition and are not in the adversary structure. Moreover, other SIS schemes for sharing a secret image with different properties, including two-in-one SIS (TiOSIS) scheme [16–18], cheater detection [19] and so on, were proposed. For more details of the SIS schemes, one can refer to [20].

All of these schemes mentioned above consider each participant plays the same role in the revealing process. However, in some application scenario, some participants are accorded with special privileges due to their status or importance. An essential secret image sharing (ESIS) scheme with different importance of shadows, e.g. (t, s, k, n)-ESIS scheme, were proposed by Li et al. [21]. (t, s, k, n)-ESIS is a special category of SIS, which shares a secret image into two groups: essential ones with s shadows and non-essential ones with $n - s$ shadows. The qualified subset of all shadows should include at least k shadows with at least t essential shadows. The difference between essential shadows and non-essential shadows is that an essential shadows can substitute a non-essential shadows in the revealing process, but not vice versa. The so-called essentiality of (t, s, k, n)-ESIS scheme is that we need k shadows including at least t essential shadows for reconstruction. Subsequently, Yang et al. [22] proposed an essential secret image sharing scheme to reduce total size of shadows by conjunctive hierarchical approach. However, the schemes [21,22] ignored two critical problems: unequal size of shadows and concatenation of sub-shadows, which may bring about the security vulnerability and complicates the reconstruction process in practice, respectively. Li et al. [23] proposed a (t, s, k, n)-ESIS scheme with the same size of shadows and no concatenation of sub-shadows. However the shadow sizes and the total shadow sizes in their scheme are larger than the schemes [21,22]. In 2016, Chen [24] adopted two SIS schemes with different thresholds to share a secret image among essential and non-essential shadows. However, his scheme exhibits a threshold fulfillment problem that satisfying only one threshold requirement partially recovers the secret image. In order to solve this problem, Chen et al. [25] proposed an essential secret image sharing scheme with two-layered structure . Their scheme not only overcomes the threshold fulfillment problem, but also keeps at least two kinds of optimal sharing ratios. Besides, Chen et al. [26] proposed an expandable essential secret image sharing structure with the same shadow sizes which are $1/t$ times of the secret image. However, their scheme needs to save an extra-disturbed image. In this paper, we study a special case of (t, s, k, n)-ESIS when $t = s$, and it is reduced to a (t, k, n)-ESIS scheme. In a (t, k, n)-ESIS scheme, all essential shadows need to be involved in the revealing process. Actually, this is a common situation in a decision system when the unanimity of essential participants is required. Therefore, (t, k, n)-ESIS scheme is worth studying. Although some existing (t, s, k, n)-ESIS scheme can be used in such circumstance, the proposed (t, k, n)-ESIS scheme has the advantages on shadow size and no concatenation operation compared with the literature ESIS schemes. Besides, the sharing and revealing processes are easy to implement.

This paper is organized as follows. In Section 2, we briefly review some related literature works. Section 3 presents the motivation, the proposed (t, k, n)-ESIS scheme and a special construction method for $(t, t + 1, n)$-ESIS scheme. Experiments and comparisons are given in Sections 4.1 and 4.2, respectively. Section 4.3 briefly introduces the application of the proposed scheme and Section 5 is the conclusion.

2. Related works

2.1. The (k, n)-SIS scheme

In 1979, Shamir [2] introduced a (k, n)-threshold secret sharing scheme to share a secret into n shares by using a $(k - 1)$-degree polynomial $f(x) = (a_0 + a_1 x + \cdots + a_{k-1}x^{k-1}) \bmod p$, in which p is a prime number and a_0 is the secret data. Based on Shamir's secret sharing scheme, Thien and Lin [3] proposed a remarkable (k, n) secret image sharing scheme. Different from Shamir's work, k consecutive secret pixels are embedded into all k coefficients of a $(k-1)$-degree polynomial to generate n shadow pixels. The sharing process is briefly described as follows. Since one shadow pixel is generated by sharing k secret pixels, the shadow size is $1/k$ times of the secret image.

In previous secret sharing schemes, the prime number p is often chosen as 251. However, it will lead to distortion of reconstructed image. In order to achieve a lossless scheme, we can conduct the secret image sharing over Galois Field $GF(2^8)$ instead of modulus 251 in this paper.

2.2. Literature reviews

In this subsection, we briefly review four important literatures [21,22,24,25] of essential secret image sharing (ESIS) schemes. A conventional (k, n)-SIS scheme shares a secret image among n shadows and gathering k shadows can reveal the secret image. In the same way, a (t, s, k, n)-ESIS shares the secret image among n shadows, in which s shadows are essential and the left $(n - s)$ shadows are non-essential. When recovering the secret image, two threshold conditions need to be satisfied: one is the threshold condition that k or more shadows should be in involved in reconstruction; the other is the essentiality condition that there are at least t essential shadows in the k involved shadows.

Next, we simply introduce the sharing process of these four (t, s, k, n)-ESIS schemes with $t = s$. Li et al. [21] used a (k, k)-SIS and a series of $(k - t)$ SIS to construct the ESIS. Their scheme first adopted a (k, k)-SIS to share the secret image among k intermediate shadows, the first t intermediate shadows are selected as essential shadows. The remaining $k - t$ intermediate shadows were further shared to $(n - t)$ non-essential shadows by using $(1, k - t, n - t)$-SSIS scheme. Each non-essential shadows is generated by concatenating multiple sub-shadows. In order to decrease the non-essential shadow size, they further present a modified version that the remaining $(k - t)$ intermediate shadows are used as the input of a $(k - t, n - t)$-SIS to generate the non-essential shadows. Afterward, Yang et al. [22] improved previous Li et al. scheme [21] to reduce total size of the shadows. The difference from Li et al. scheme is that each of the remaining $(k - t)$ intermediate shadow is shared into n sub-shadows. The essential shadow is obtained by concatenating one intermediate shadow and $(k - t)$ sub-shadows. A non-essential shadow is acquired by concatenating $(k - t)$ sub-shadows.

Chen [24] used two SIS schemes to construct a new structure for reducing the total size of essential and non-essential shadows. His scheme first partitions the permuted image into some blocks, each block consists of two parts: one has t pixels; the other has k pixels. Then these two parts of each block are applied to (t, t)-SIS and (k, n)-SIS to generate two sets of shadows, respectively. An essential shadow consists of two shadows of from two sets of shadows. Since two thresholds have to be both required in a (t, k, n)-ESIS, Chen's scheme adopts two SIS independently that leads to a threshold fulfillment problem. In order to solve this problem, Chen et al. [25] introduced a two-layered (t, k, n)-ESIS scheme. The 1st-layer SIS scheme is used to partition the permuted secret image into two 1st-layered intermediate shadows. Each 1st-layered intermediate shadow denotes on threshold requirement for recovering the secret image. Two intermediate shadows are then applied to a (t, t)-SIS and a (k, n)-SIS respectively to generate 2nd-layered shadows for composing the essential and non-essential shadows. Their scheme [25] keeps at least two kinds of optimal sharing ratios