Digital Signal Processing 50 (2016) 51–60

Contents lists available at ScienceDirect

Digital Signal Processing

www.elsevier.com/locate/dsp

Essential secret image sharing scheme with the same size of shadows

Peng Li [a,*], Ching-Nung Yang [b], Zhili Zhou [c]

[a] Department of Mathematics and Physics, North China Electric Power University, Baoding, Hebei, China
[b] Department of CSIE, National Dong Hwa University, Taiwan
[c] School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing, Jiangsu, China

ARTICLE INFO

Article history:
Available online 21 December 2015

Keywords:
Secret image sharing
Threshold secret sharing
Essential shadow
Derivative polynomial
Birkhoff interpolation

ABSTRACT

Secret image sharing is a method to decompose a secret image into shadow images (shadows) so that only qualified subset of shadows can be used to reconstruct the secret image. Usually all shadows have the same importance. Recently, an essential SIS (ESIS) scheme with different importance of shadows was proposed. All shadows are divided into two group: essential shadows and non-essential shadows. In reconstruction, the involved shadows should contain at least a required number of shadows, including at least a required number of essential shadows. However, there are two problems in previous ESIS scheme: unequal size of shadows and concatenation of sub-shadow images. These two problems may lead to security vulnerability and complicate the reconstruction. In this paper, we propose a novel ESIS scheme based on derivative polynomial and Birkhoff interpolation. A single shadow with the same-size is generated for each essential and non-essential participant. The experimental results demonstrate that our scheme can avoid above two problems effectively.

1. Introduction

Secret image sharing (SIS) is a technique for image protection using mechanism of secret sharing [1–3]. It encrypts a secret image into multiple shadows and then distributes them to the corresponding participants. In the revealing process, only qualified subsets of participants can cooperate to reveal the secret image with their shadows. Usually, SIS scheme is implemented as a threshold (k, n)-SIS scheme, where $k \leq n$, that divides a secret image into n shadows. Any k shadows can be used for reconstructing the secret image, while any $(k-1)$ or fewer shadows cannot obtain any secret information. Image steganography can also protect secret information from unauthorized parties. However, the secret information cannot be recovered when the stego-image is modified or lost. SIS can avoid this problem when the shadows are transmitted by different channels [4,5]. In 1979, Shamir [1] proposed a novel (k, n) secret sharing scheme to hide a secret data in the constant term of a $(k-1)$-degree polynomial. Thien and Lin [2] extended Shamir's work and first proposed a (k, n)-SIS scheme by embedding secret pixels into all coefficients of a $(k-1)$-degree polynomial. The shadow size of Thien and Lin's (k, n)-SIS scheme is $1/k$ times of the secret image. In [3], 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, and various SIS schemes with specific functions are introduced subsequently. For example, shadows in [2,3] are noise-like and suspected to censorships. Various (k, n)-SIS schemes were proposed by using steganography and shadows reveal meaningful images [6–10]. By adding the detection of the modification of shadows, this scheme is called as a steganographic and authenticated image sharing (SAIS) scheme. SIS schemes and SAIS schemes have the threshold property that recovers either the entire image or nothing. Researchers introduced scalable SIS (SSIS) schemes [11–15], which provide progressive decoding. In SSIS scheme, the information amount of reconstructed image is proportional to the number of shadows involved in reconstruction. Additionally, another kind of SIS scheme with two decoding options was proposed [16–19]. This two-in-one SIS (TiOSIS) scheme combines SIS scheme and visual cryptographic scheme (VCS) [20]. In TiOSIS scheme, a vague secret image can be revealed by stacking shadows, while the original grayscale secret image can be decoded by computation.

All above schemes consider each participant has the same importance in reconstruction. However, there are many examples that some participants are accorded special privileges due to their status or importance, e.g., heads of government, managers of company, ..., and etc. In fact, weighted SIS (WSIS) scheme [21–23] and essential SIS (ESIS) scheme [24–26] have different importance of

* Corresponding author at: School of Mathematics and Physics, North China Electric Power University, Baoding 071003, China. Fax: +86 0312 7525073.
E-mail address: lphit@163.com (P. Li).

http://dx.doi.org/10.1016/j.dsp.2015.12.004
1051-2004/

shadows. WSIS scheme generates shadows with different weights according to priority of the participant. The secret image is recovered if and only if the value of total weights for the involved shadows achieves the threshold. Thus, WSIS scheme does not have the essentiality as in (t, s, k, n)-ESIS scheme. A (t, s, k, n)-ESIS scheme has s essential shadows and $(n - s)$ non-essential shadows. 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.

In [27], Tassa proposed a hierarchical secret sharing by using derivative polynomial function and Birkhoff interpolation. Afterwards, Guo et al. [28] adopted Tassa's hierarchical secret sharing to propose a hierarchical SIS scheme. However, Guo et al.'s [28] SIS scheme embedded secret pixels into all coefficients of a polynomial. This compromises the secrecy that some non-authorized subsets of participants can recover parts of the secret image. Recently, Pakniat et al. [29] enhances Guo et al.'s scheme to propose a secure hierarchical SIS scheme. Although Pakniat et al.'s scheme also embeds secret pixels into all coefficients in polynomials, these coefficients are securely encrypted by using cellular automata and hash function. From the viewpoint of secret sharing, both Guo et al. and Pakniat et al.'s scheme use all coefficients of polynomial to embed secret pixels. Therefore, their schemes are not secure as the original Tassa's scheme.

Both WSIS scheme and ESIS scheme have the different importance of shadows, but only ESIS scheme has the essentiality. However, there are two problems in (t, s, k, n)-ESIS scheme: unequal size of shadows and concatenation of sub-shadows, which are ignored by the previous (t, s, k, n)-ESIS schemes [24,25]. If the sizes of essential shadows and non-essential shadows are different, attackers may detect the status of these shadows from their sizes. In this case, the size of shadows may leak some sensitive information. For the problem of concatenation of sub-shadows, we need not only to record the location of each sub-shadow, but also extra operation to extract each sub-shadow before revealing. In the practical use, the two problems may bring about security vulnerability and make the reconstruction more difficult. In this paper, we propose a (t, s, k, n)-ESIS scheme to solve the two problems based on derivative polynomial and Birkhoff interpolation. In our scheme, the secret pixels are embedded into partial coefficients of a polynomial. The remainder of this work is organized as follows. In Section 2, we review the first (k, n)-SIS scheme, Thien and Lin's [2] (k, n)-SIS scheme, and two previous (t, s, k, n)-ESIS schemes [24, 25]. Two critical problems in (t, s, k, n)-ESIS scheme are introduced in Section 3. In Section 4, we propose the improved (t, s, k, n)-ESIS with the same size of shadows. Experiment, comparison, and discussion are given in Section 5. Finally, the conclusion is provided in Section 6.

2. Previous works

2.1. (k, n)-SIS scheme

In 1979, Shamir [1] introduced a (k, n) 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. The dealer randomly selects this polynomial, and generates n shares $(i, f(i))$, $i = 1, 2, \ldots, n$. Any k shares (say $1, 2, \ldots,$ and k) can be used to recover $f(x)$ by Lagrange's interpolation $f(x) = \sum_{i=1}^{k} f(i) \prod_{j=1, j\neq i}^{k} \frac{(x-j)}{(i-j)} \bmod p$. Then, the secret is derived from $a_0 = f(0)$. However, any $k-1$ or fewer shares cannot recover the polynomial $f(x)$ and thus do not obtain any secret information.

Following Shamir's work, Thien and Lin embedded secret pixels into all k coefficients in a $(k-1)$-degree polynomial to generate n random grayscale values of n noise-like shadows. The sharing process is briefly described as follows. A secret image is first divided into non-overlapping blocks, and every block has k pixels. Every block is then represented as a $(k-1)$-degree polynomial $f(x)$. With each participant ID id, the shadow pixel is generated by $f(id)$. Since it embeds k pixels at each time, the shadow size is $1/k$ of the secret image. When sharing a grayscale secret image, the prime number p is often chosen as 251 (the largest prime number smaller than 255) so that the coefficients are between 0 and 250 and suitable to represent 8-bit grayscale. However, the grayscales (> 250) have to be modified to 250 and has distortion in this case. Obviously, we can use Galois Field $GF(2^8)$ instead of modulus 251 to achieve a distortion-less scheme. In previous literatures, some schemes simply adopt $GF(251)$ while some schemes use $GF(2^8)$ to obtain a distortion-less image.

2.2. (t, s, k, n)-ESIS scheme

In a (t, s, k, n)-ESIS scheme, s out of n shadows are essential. A (t, s, k, n)-ESIS scheme has not only the threshold property (i.e., k or more shadows should be involved in reconstruction) but also the essentiality property (i.e., there are at least t essential shadows in the k involved shadows). For example, k shadows including $(t-1)$ essential shadows and $(k-t+1)$ non-essential shadows cannot be used for reconstructing the secret. The essentiality property is not achieved in this case. Another example of k shadows including t essential shadows and $(k-t)$ non-essential shadows satisfies the conditions of the threshold and the essentiality simultaneously, and it can reconstruct the secret. The condition $t = k$ implies that we do not need non-essential shadows for reconstruction, and thus non-essential shadows do not have any contribution for reconstructing the secret. Regarding $s = n$, all shadows are essential and the (t, s, k, n)-ESIS scheme is reduced to a (k, n)-SIS scheme. For $k = n$, a (t, s, k, n)-ESIS scheme is also reduced to a (n, n)-SIS scheme. Therefore, for a non-trivial ESIS scheme, it is obvious that these values should satisfy $t \leq s < n$ and $t < k < n$.

All shadows of the conventional (k, n)-SIS scheme have the same importance. In various applications of group hierarchical decision making, some participants are more important than others. For example, a group consisting of 2 monitors and 6 soldiers carries out missile launching, which is controlled by a launch password. This password is encoded into 8 noise-like shadows and distributed to 2 monitors and 6 soldiers. Because the launch of a missile is a key issue, the decision of launch requires the affirmative votes of 4 members (i.e., the threshold is $k = 4$) including one monitor's agreement (i.e., $t = 1$). There are total 8 members ($n = 8$) including 2 essential members ($s = 2$). Therefore, this scenario has the threshold property and the essentiality as $(1, 2, 4, 8)$-ESIS scheme.

The threshold of reconstructing a secret image in (t, s, k, n)-ESIS scheme is k, which is the same as that of the conventional (k, n)-SIS scheme. Let P be the set of all participants and Q be the set of participants involved in reconstruction, $Q \subseteq P$. And, let EP and NEP be the sets of essential participants and non-essential participants, respectively, where $P = EP \cup NEP$. Participants in EP and NEP have the different importance of shadows, and the cardinalities of EP and NEP are $|EP| = s$ and $|NEP| = (n - s)$. Let $(Q \backslash NEP)$ denote the set having elements in Q but not in NEP. A qualified subset of participants in (t, s, k, n)-ESIS scheme, should satisfy the threshold condition: $|Q| \geq k$. Meanwhile, the set $(Q \backslash NEP)$, has at least t essential participants (i.e., satisfy the essentiality condition). Both conditions allow any k participants (including at least t essential participants) can reconstruct the secret. The threshold condition and the essentiality condition of (t, s, k, n)-ESIS scheme are formally defined as follows.

$$\begin{cases} \text{(i) Threshold condition: } |Q| \geq k, \\ \text{(ii) Essentiality condition: } |Q \backslash NEP| \geq t. \end{cases} \tag{1}$$