J. Vis. Commun. Image R. 38 (2016) 595–601

Contents lists available at ScienceDirect

J. Vis. Commun. Image R.

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

Two-layered structure for optimally essential secret image sharing scheme ☆

Chien-Chang Chen *, Shih-Chang Chen

Department of Computer Science and Information Engineering, Tamkang University, No. 151, Yingzhuan Rd., Tamsui Dist., New Taipei City 25137, Taiwan

ARTICLE INFO

Article history:
Received 23 November 2015
Revised 18 February 2016
Accepted 6 April 2016
Available online 8 April 2016

Keywords:
Secret image sharing
Essential
Non-essential
Two-layered structure
Optimal sharing ratios

ABSTRACT

This paper presents a two-layered structure for optimally sharing a secret image among s essential and $n-s$ non-essential shared shadows using the (t,s,k,n) essential thresholds, that t essential shared shadows and totally k shared shadows are needed to recover the secret image. The presented two-layered structure includes one user-defined parameter m to determine different kinds of optimal results. $m=1$ leads to minimum size of total shared shadows (ST) and size of an essential shared shadow is close to size of a non-essential shared shadow. On the other hand, $m=t$ leads to size of an essential shared shadow being twice of size of a non-essential shared shadow to signify the importance of an essential shared shadow. Moreover, the proposed structure overcomes the threshold fulfillment problem in Chen's scheme (Chen, 2016). Theoretical analyses and experimental results show that the proposed scheme exhibits secure with optimal sharing ratios among related works.

1. Introduction

Multimedia contents are popularly used over network and the security problems in storing or transmitting multimedia files are more and more important. Secret image sharing techniques share a secret image among shared shadows and then recover the secret image from shared shadows to protect the image secretly.

The first secret image sharing scheme (*SIS*) is presented by Thien and Lin [1], in which the Shamir–Lagrange technique is adopted to share an image secretly. Many researchers have then proposed other *SIS* for sharing a secret image with different properties, including sharing secret image among host images [2–6], sharing both with secret image sharing and visual cryptography [7], scalable sharing [8,9], cheater identification [10], and essential sharing [11–13]. Moreover, many different techniques, including Shamir–Lagrange [1], Blakley geometry [14], Chinese Remainder Theorem [15], cellular automata [16,17], combination theory [18], and Boolean operations [19–21], have been presented for sharing a secret image.

Among these studies, an essential secret image sharing scheme (*ESIS*) [11–13] generates shared shadows including essential and non-essential ones. Since two kinds of shadows meet the requirement of participants with different privileges, the essential secret image sharing problem merits our study. A (t,s,k,n) *ESIS* shares the secret image among n shared shadows, including s essential shared shadows and $n-s$ non-essential shared shadows. Two threshold requirements are needed to recover the secret image, the first threshold requirement is collecting t essential shared shadows and the other threshold requirement is collecting totally k shared shadows including essential and non-essential shared shadows.

In the study of *ESIS*, Li et al. first present the concept of (t,s,k,n) *ESIS* [11]. Yang et al. [12] then modified Li et al.'s scheme [11] to reduce total size of shared shadows. In 2016, Chen adopted two *SIS* with different thresholds to share a secret image among essential and non-essential shared shadows [13]. Among these *ESIS* schemes, Chen's scheme acquires presently optimal sharing ratios on size of essential shared shadows (SE), size of non-essential shared shadows (SN), size of total shared shadows (ST), and size of required shared shadows to recover the secret image (SR). However, Chen's scheme exhibits a threshold fulfillment problem that satisfying only one threshold requirement partially recovers the secret image. This paper improves Chen's scheme to a two-layered scheme to overcome the threshold fulfillment problem but keeps at least two kinds of optimal sharing ratios. A pre-defined parameter m determines the selection of optimal sharing ratio. The first one is $m=1$ that acquires nearly sizes between essential and non-essential shared shadows with smallest ST value. The second one is $m=t$ that obtains size of an essential

☆ This paper has been recommended for acceptance by M.T. Sun.

* Corresponding author.
E-mail address: ccchen34@mail.tku.edu.tw (C.-C. Chen).

http://dx.doi.org/10.1016/j.jvcir.2016.04.004
1047-3203/

shared shadow being twice of size of a non-essential shared shadow to signify the importance of an essential shared shadow. Moreover, the second one has the same optimal results presented by the Chen's scheme [13].

This paper is organized as follows. Section 2 briefly introduces three related literatures [11–13] with discussions of their properties. Section 3 presents our proposed *ESIS*. Section 3.1 introduces the sharing strategy over Galois field GF(2^8). Section 3.2 introduces algorithm of the proposed scheme and Section 3.3 theoretically compares the sharing ratios between the proposed scheme and related works [11–13]. Section 4 presents experimental results of our proposed scheme. Section 5 provides a conclusion and suggestions for future research.

2. Literature reviews

This section reviews three important literatures [11–13] of essential secret image sharing schemes (*ESIS*). A conventional (k,n) secret image sharing scheme (*SIS*) shares a secret image among n shared shadows and gathering k shared shadows recovers the secret image. A (t,s,k,n) *ESIS* shares the secret image among n shared shadows, in which s shared shadows are essential and $n-s$ shared shadows are non-essential. Collecting t essential shared shadows and collecting totally k shared shadows are two threshold requirements to recover the secret image. Three important *ESIS* schemes are briefly reviewed in this section. Section 2.1 introduces the first (t,s,k,n) *ESIS* that is presented by Li et al. [11]. Section 2.2 introduces Yang et al.'s work [12] that improves Li et al.'s scheme [11] to reduce total size of shared shadows. Section 2.3 introduces Chen's *ESIS* to adopt two *SIS* with different thresholds for sharing a secret image [13].

2.1. Review of the Li et al.'s scheme [11]

Li et al. used a $(k,s+k-t)$ *SIS* and a series of $k-t$ *SIS* to construct the *ESIS*. Their scheme first adopted a $(k,s+k-t)$ *SIS* to partition the secret image among $s+k-t$ shadows. The first s shadows are essential shared shadows. The remaining $k-t$ shadows are then applied to a series of $k-t$ *SIS* with thresholds $(1,n-s),(2,n-s),\ldots,(k-t,n-s)$, respectively. A non-essential shared shadow is then acquired from concatenating one generated shadow from each *SIS*. Sizes of essential and non-essential shared shadows are $\frac{1}{k}\times z$ and $\frac{H_{k-t}}{k}\times z$, respectively, where H_{k-t} is the harmonic number and z is size of the secret image.

In order to decrease size of a non-essential shared shadow under the restriction of $s+1\leqslant k$, they further present a modified version that first concatenate shadows $s+1,s+2,\ldots,s+k-t$ to acquire an intermediate shadow and then apply the intermediate shadow to a $(k-s,n-s)$ *SIS* for generating non-essential shared shadow. Size of the modified non-essential shared shadow is $\frac{(1+H_{k-t}-H_{k-s})}{k}\times z$.

2.2. Review of Yang et al.'s scheme [12]

Yang et al. improved previous Li et al.'s scheme [11] to reduce total size of the shared shadows. Their scheme first applied a $(k,s+k-t)$ *SIS* on the permuted secret image to acquire 1st-layered shadows $s_x(0\leqslant x\leqslant s+k-t-1)$. Like the method in previous Li et al.'s scheme, all these 1st-layered $s+k-t$ shadows s_x are partitioned to two groups $s_x(0\leqslant x\leqslant s-1)$ and $s_x(s\leqslant x\leqslant s+k-t-1)$. Each of the second group of 1st-layered shadows $s_x(s\leqslant x\leqslant s+k-t-1)$ is applied to a (k,n) *SIS* to acquire 2nd-layered shadows $s_{x,y}(s\leqslant x\leqslant s+k-t-1,\ 0\leqslant y\leqslant n-1)$. The essential shared shadow $S_i(0\leqslant i\leqslant s-1)$ is acquired from concatenating $s_i(0\leqslant i\leqslant s-1)$ and $s_{x,i}(s\leqslant x\leqslant s+k-t-1)$. On the other hand, a non-essential shared shadow $S_i(s\leqslant i\leqslant s+k-t-1)$ is only acquired from the concatenation of $s_{x,i}(s\leqslant x\leqslant s+k-t-1)$. Therefore, sizes of essential and non-essential shared shadows are $\frac{2k-t}{k^2}\times z$ and $\frac{k-t}{k^2}\times z$, respectively.

2.3. Review of Chen's scheme [13]

Chen used two *SIS* to construct a new structure for reducing total size of essential and non-essential shared shadows. His scheme first permutes the secret image to obtain a permuted secret image. The permuted image is then partitioned to two parts of sizes proportional to $\frac{t}{t+k}$ and $\frac{k}{t+k}$ of the secret image. These two parts are then applied to thresholds (t,s) and (k,n) for generating two sets of shadows. Combining two shadows of one from the first set of shadows and another from the other set of shadows acquires an essential shared shadow. Since $k>t$, each remaining (k,n) shadow forms a non-essential shared shadow. The size of essential and non-essential shadows are $\frac{2}{t+k}\times z$ and $\frac{1}{t+k}\times z$, respectively.

2.4. Properties discussion on three works [11–13]

Li et al. [11] and Yang et al. [12] both required $1+k-t$ *SIS* to share a secret image. The modified method of Li et al.'s scheme requires only two *SIS*. Chen [13] also used two *SIS* to reduce sizes of all shared shadows. Chen's scheme is simple and efficient on sharing a secret image among essential and non-essential shared shadows. Since two thresholds have to be both required in a (t,s,k,n) *ESIS*, Chen's scheme adopts two *SIS* independently leads to a *threshold fulfillment problem* on only meeting one of these two thresholds. Fig. 1 shows two examples of threshold fulfillment problem on only meeting 3 essential shared shadows requirement or totally 5 shared shadows requirement in the Chen's $(3,5,5,8)$ *ESIS*. Experimental results in Fig. 1 show that part of the secret image can be recovered. The problem can be perfectly overcome by adding an extra layer to construct a two-layered structure. Our proposed scheme, introduced in Section 3, shows that the presented two-layered scheme also exhibits optimal shared ratios among (t,s,k,n) *ESIS* [11–13].

3. Proposed scheme

This section presents the proposed (t,s,k,n) *ESIS*. Section 3.1 briefly introduces secret sharing calculation over GF(2^8). Section 3.2 introduces the proposed two-layered (t,s,k,n) *ESIS*. Section 3.3 discusses sharing ratios of our proposed scheme. Theoretically analyses with three works [11–13] are also compared.

3.1. Secret sharing over Galois field GF(2^8)

This section briefly introduces a (k,n) *SIS* to share k secret numbers $c_i(0\leqslant i\leqslant k-1)$ among n shared numbers $f(x_j)$ with keys $x_j\ (0\leqslant j\leqslant n-1)$, respectively. The sharing calculation is performed by the following equation

$$f(x_j)=c_0+c_1x_j+c_2x_j^2+\cdots+c_{k-1}x_j^{k-1}$$

Numbers are represented through polynomials. For example, a number $(193)_{10}=(11000001)_2$ is represented by x^7+x^6+1. Mathematical calculations are also performed through polynomial processing. For example, $(5)_{10}+(20)_{10}$ acquires $(17)_{10}$ by the processing of $(x^2+1)+(x^4+x^2)=x^4+x^2+x^2+1=x^4+1$ and $(5)_{10}\times(20)_{10}$ acquires $(68)_{10}$ by the processing of $(x^2+1)\times(x^4+x^2)=x^6+x^4+x^4+x^2=x^6+x^2$. The polynomial calculation is processed under modulus result of an irreducible polynomial like $x^8+x^4+x^3+x+1$. In recovering calculation, all k secret numbers $c_i(0\leqslant i\leqslant k-1)$ can