Journal of Information Security and Applications 40 (2018) 166–172

Contents lists available at ScienceDirect

Journal of Information Security and Applications

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

An improved threshold multi-level image recovery scheme

Yi-Ning Liu*, Zhen Wu

Guangxi Key Laboratory of Trusted Software, Guilin University of Electronic Technology, Jinji Road, No.1, Guilin 541004, China

ARTICLE INFO

Article history:

Keywords:
Social network
Image sharing
Multi-level recovery
Steganography

ABSTRACT

Nowadays, publishing photos over social network is very popular. In order to obtain more benefit, the new business model is design. For example, the photo should be browsed, or downloaded according to different level. Specifically, a single user only obtains the low quality image, but if he recommends more users to join in, more higher quality image can be obtained. In this paper, an improved (*t, r, n*)-hierarchical threshold multi-level image recovery scheme is proposed. When the number of collaborators is less than *t*, the browsed image's quality is gradually improved with the increasement of the number of collaborators. If the number of the collaborators reaches *t*, the complete image is obtained. Moreover, system analysis shows that the proposed scheme achieves the steganography and practicability.

1. Introduction

With the rapid development of the mobile Internet, social network is booming. More and more users share their happiness over Facebook, Instagram and WeChat [1]. In addition, social network not only is a communication manner, but also a new business platform. For example, the images are published in WeChat, each user can browse or download the image of low quality. If a user recommends more users to give a thumb up, he can browse or obtain the image with higher quality. More users collaborate, higher quality image they can obtain. When the number of users reaches the threshold, the original image is recovered. Obviously, this method can promote more people join this game. More traffic is gathered, more business opportunities are generated.

In fact, the image research has been widely focused, and many excellent literatures have been presented. In 1994, visual cryptography(VC) was proposed by Naor and Shamir [2], which utilized the human visual system to read the secret information of some overlapped shares. In order to achieve more flexibility, progressive visual cryptography (PVCs) schemes [3–5] had drawn much attention in academia, which provided progressively clear appearances of recovered images depending upon the number of stacked shares. However, the disadvantage is that the recovered images are easily distorted.

Due to information theoretically security, Shamir's secret sharing [6] has been widely used to design the secret image sharing (SIS). Thien and Lin [7] proposed a (*t, n*) secret image sharing scheme, in which the secret image was divided into *n* shadows, and nothing was reconstructed with fewer than the threshold number *t* shadows. Meanwhile, all gray values range 250–255 were truncated to 250, which leaded a distortion in the reconstructed secret image, and may not be admissible in sensitive application such as military and medical applications.

In order to achieve the lossless requirement, Thien–Lin's scheme was improved by Wu [8], in which the prime number 257 was used to replace the prime number 251 to avoid the truncation process. However, Wu's scheme seemed to be less efficient than Thien and Lin's scheme, since it required more complicated operations. Subsequently, Algebraic-geometry code was utilized in Wang et al.'s scheme [9], in which all operations were executed over a finite field $GF(2^m)$, where m was the number of bits that represented a gray pixel in actual digital facilities. For example, when $m=8$, there were 256 pixel gray values, where the distinct gray value corresponded to an element in $GF(2^8)$. In this paper, all pixel values are taken from $GF(2^m)$. Therefore, an image is viewed as a pixel value array over $GF(2^m)$, and the set of all such possible pixel value arrays over $GF(2^m)$ is called the domain of this kind of images, where the cardinality of the domain is called the size of the domain. And this method has been utilized in many field such as scalable secret image sharing [10–12] and essential secret image sharing [13].

In some other aspects, it is easy to draw the attention of attacker during the transmission process when the produced shadow images are meaningless. In order to hide the shadow images, steganographic technique was employed to hide them in user-selected cover image [14–22]. Lin and Tsai [14] provided a user-friendly image sharing method to embed the secret data into a cover image. By this way, the distortion was imperceptible between the cover image and the shadow images. In 2007, Yang et al. [17] improved the approach of Lin and Tsai [14] to a distortion-

* Corresponding author.
E-mail address: lyn7311@sina.com (Y.-N. Liu).

https://doi.org/10.1016/j.jisa.2018.03.009
2214-2126/

free scheme over Galois field $GF(2^8)$. Unfortunately, the maximum secret capacity was limited to a quarter of the size of the cover image. In 2009, the modulus operator was employed by Lin et al. [22], in which the shadow image was meaningful with satisfactory quality, moreover, the retrieved secret image and the reconstructed cover image were lossless. Although more complicated steganographic methods have been used besides LSB substitution, the quality of stego images is proved not to be as good as the expected quality. One of the most important reasons is that the size of image shares embedded in the cover images is large, and there is a contradiction between the steganographic capacity and the quality of stego images. Moreover, the size of cover images used in the existing methods [14,16,17,23,24] was four times of a secret image's size, which would not be favorable for their later storage, transmission or other processing.

Traditional secret image sharing scheme assumes that each share is equally treated, however, in the reality, the privilege of different participant is not always same. Hence, the assumption does not reflect the actual situation in real life. Thus, a hierarchical threshold secret sharing scheme is suitable for this situation. Tassa [25] proposed a scheme using Birkhoff interpolation and constructed a polynomial according to an unstructured set of point and derivative values. The secret image shared among a group of participants, with these participants being partitioned into different levels, the access structure was determined by a sequence of threshold requirements. In 2012, Guo et al. [26] improved Tassa's scheme [25] to achieve three contributions: the secret image can be retrieved completely, the problems of overflow and underflow was addressed, and the capacity of the embedded secret data was stable and large. Later, there are some literatures following Guo et al.'s scheme. In 2014, Pakniat et al. [27] employed cellular automata and Birkhoff interpolation proposed a more secure scheme to achieve authentication. In 2015, Yang et al. proposed a more efficient scheme since the size of the generated shadow images was reduced [28].

However, there still exists weakness in the above schemes: the image can be reconstructed with no less than t shares, and nothing is obtained with less than t shares. To address this flaw, an improved (t, r, n) threshold multi-level image recovery scheme is proposed in this paper, in which each shadow image generated from the secret image plays an equivalent role, and the multi-level image can be revealed with the collected shadows. Especially, the proposed scheme not only reveals the image gradually with the increasing number of shadows, but also completely recovers the image when the number of shadow images reaches t. We think the proposed scheme is an convenient and useful tool for image publishing platform over the social network, more users join, more high quality can be achieved.

The proposed scheme's contribution includes the following aspects:

1) The clarity is gradually improved when the number of shares increasing.
2) Each user's priority is equivalent, which is more suitable for the feature of the social network.

The rest of this paper is organized as follows: Preliminaries is introduced in Section 2, and an overview of Guo et al.'s scheme is presented in Section 3. Then the proposed scheme is described in Section 4, and the simulation results and analysis are in Section 5. Finally, the paper is concluded in Section 6.

2. Preliminaries

2.1. (t, n)-threshold secret sharing scheme

In 1979, Shamir proposed a (t, n)-threshold secret sharing scheme using Lagrange interpolation algorithm over Galois field, which allowed n participants to share a secret data. Each participant holds a part of the secret data, called a shadow or a share, and each shadow reveals no information about the original secret data. To reconstruct the secret data, at least t shadows are necessary, where $t \le n$. The whole process consists of two phases: secret sharing phase and reconstruction phase.

Secret sharing phase:

Suppose that a secret data s is shared to participants P_i, $(i = 1, 2, \ldots, n)$.

(1) The dealer selects $(t-1)$ random number $a_1, a_2, \ldots, a_{t-1}$, and a prime number p.
(2) The dealer constructs a $(t-1)$ degree polynomial $f(x) = a_0 + a_1 x + \ldots + a_{t-1}x^{t-1} \bmod p$ where $a_0 = s$, computes the share $f(i)$, and sends $f(i)$ to P_i in a secure manner, $(i = 1, 2, \ldots, n)$.

Reconstruction phase:

(1) Any t or more shadows can reconstruct $f(x)$, all coefficients of the polynomial function $f(x)$ can be derived.
(2) The secret data $s = a_0 = f(0)$ can also be recovered.

2.2. (t, n)-threshold secret image sharing scheme

In 2002, Thien and Lin proposed (t, n)-threshold scheme by performing modular arithmetic operations over Galois Field $GF(p)$, in which a secret image is divided into n shadow images, and distributed n participants. In addition, the size of each shadow image is only $1/t$ of the secret image, which guarantees the efficiency. Truncating all pixel values larger than 250–250, and permuting the pixels of the secret image S by a permutation sequence, the sharing scheme includes the following steps:

1. The secret image S is divided into several sections, each section has t pixels, and each pixel of S belongs to one and only one section.
   For each section, constructing a polynomial $f(x) = s_0 + s_1 x + \ldots + s_{t-1}x^{t-1} \bmod 251$, where $s_0, s_1, \ldots, s_{t-1}$ are the pixels of the section.
2. The n output pixels $f(1), f(2), \ldots, f(n)$ of this section are sequentially assigned to the n shadow images.
3. Repeats Steps 3 and 4 until all pixels of permuted image are processed.

The reveal phase using t shadow images is as follows:

1. Given any t shadow images, the coefficients $s_0, s_1, \ldots, s_{t-1}$ of $f(x)$ can be obtained using Lagrange's interpolation. Hence, the coefficients $s_0, s_1, \ldots, s_{t-1}$ correspond to t pixel values of the permuted image.
2. Repeats Step 1 until all pixels of the t shadow images are processed.
3. Employs the inverse-permutation operation to the permuted image to get the secret image.

3. Review and analysis of Guo et al.'s scheme

3.1. Review of Guo et al.'s scheme

Guo et al. proposed (t,n)-hierarchical threshold secret image sharing scheme to recover the secret image when the threshold requirement is satisfied.

Definition. Suppose U is a set of participants P_i $(i = 1, 2, \ldots, n)$ who are divided into $m+1$ levels $U_k (k = 0, 1, \ldots, m)$, and each level corresponds to a threshold requirement t_k. Given a secret image S with size $M_s \times N_s$, and a cover image O with size $M \times N$.

The detailed scheme is as follow: