Journal of Visual Communication and Image Representation 50 (2018) 135–144

Contents lists available at ScienceDirect

Journal of Visual Communication and Image Representation

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

Partial secret image sharing for (k,n) threshold based on image inpainting☆

Xuehu Yan[a,*], Yuliang Lu[a], Lintao Liu[a], Shen Wang[b]

[a] Hefei Electronic Engineering Institute, Hefei 230037, China
[b] School of Computer Science and Technology, Harbin Institute of Technology, 150080 Harbin, China

ARTICLE INFO

Keywords:
Secret image sharing
Partial secret image sharing
Image inpainting
Linear congruence
Color image
Lossless recovery

ABSTRACT

The traditional (k,n) threshold secret image sharing (SIS) schemes dealt with the full secret image neglecting the possible situation that only part of the secret image needs protection. However, in some applications, only target part of the secret image may need to be protected while other parts may be not in a full image. In this paper, we consider the partial secret image sharing (PSIS) issue as well as propose a PSIS scheme for (k,n) threshold based on image inpainting and linear congruence (LC)-based SIS. The full secret image including the secret target part and other parts will be recovered by collecting any k or more shadow images, which can be further reconstructed losslessly by adding all the inpainted meaningful shadow images. Furthermore, the proposed scheme can share irregular target in a progressive way. Experiments are conducted to evaluate the efficiency of the proposed scheme.

1. Introduction

Through splitting the secret image into noise-like shadow images (also called shadows or shares), secret image sharing (SIS) distributes a secret image among multiple participants. The secret is recovered by collecting sufficient authorized participants (shadow images). SIS can be applied in not only information hiding, but also access control, authentication, watermarking, and transmitting passwords etc. Shamir's polynomial-based scheme [1] and visual secret sharing (VSS) [2] also called visual cryptography scheme (VCS), are the primary branches in this field.

In Shamir's original polynomial-based (k,n) threshold SIS [1], the secret image is generated into the constant coefficient of a random $(k-1)$-degree polynomial to obtain n shadow images distributed to n associated participants. The secret image can be losslessly recovered by collecting any k or more shadow images based on Lagrange interpolation. Following Shamir's scheme and utilizing all coefficients of the polynomial for embedding secret, Thien and Lin [3] reduced share size $1/k$ times to the secret image. The advantage of Shamir's polynomial-based scheme [4–6] is lossless recovery. Shamir's polynomial-based SIS requires more complicated computations, i.e., Lagrange interpolations, for reconstructing and known order of shadow images, although the scheme only needs k shadow images for recovering the distortion-less secret image.

In (k,n) threshold VSS [7–12], the generated n shadow images are printed onto transparencies and then distributed to n associated participants. The beauty of VSS is that, the secret image can be revealed by superposing any k or more shadow images and human visual system (HVS) with no cryptographic computation. Even if infinite computational power is available, less than k shadow images will reveal nothing about the secret. Inspired by Naor and Shamir's VSS work, the associated VSS physical properties and its problems were extensively studied, such as contrast[13], threshold[14], multiple secrets[6], noise-like patterns [15,10,16–18], pixel expansion[7,8,19,20] and so on [21–25]. It is noted that we may increase the efficiency of shadow images management as well as decrease the suspicion of secret image encryption, thus meaningful shadow images are significant.

In most of the existing SIS schemes, the full (entire) secret image is directly generated into the shadow images. The previous SIS schemes dealt with the full secret image neglecting the possible situation that only part of the secret image may need protection. However, there are many examples that only part of the secret image may need to be protected while other parts may be not in the same image, such as improving part design, sensitive information in part of a image and so on. One possible scenario is described as follows. On the basis of multiple traditional design modules in a product, a company improves one module design of them, while the other modules continue to use the traditional original design. At this point for the overall design of this product, the improved module is needed to be protected and the other original modules can be public. Due to business privacy and access control, this product design is kept by the company's n managers. Each manager can display the traditional modules in public display to

☆ This paper has been recommended for acceptance by Zicheng Liu.

* Corresponding author.
E-mail address: publictiger@126.com (X. Yan).

https://doi.org/10.1016/j.jvcir.2017.11.012
Received 23 February 2017; Received in revised form 24 May 2017; Accepted 16 November 2017
Available online 22 November 2017

facilitate the product introduction and other activities. In accordance with business needs, k or more managers together have the right to losslessly recover the full product design including the improved module. In this scenario, we need protect target part of the secret image other than the full secret image as well as need access control with (k,n) threshold.

Thus, in some applications we may only need to encrypt part of the secret image rather than the full secret image for some reasons. However, the previous SIS schemes have not considered this issue. In order to deal with the partial secret image sharing (PSIS) issue, in this paper, we will introduce PSIS problem as well as propose a novel PSIS scheme for (k,n) threshold based on image inpainting [26,27] and linear congruence (LC) [28]. The regular or irregular secret target part of the color secret image is first manually selected and then automatically removed from the original color secret image to obtain the same input cover images (unpainted shadow images). Then, each pixel of the secret target part is embedded into the pixels corresponding to shadow images by threshold-extended LC-based SIS in the processing of shadow images texture synthesis (inpainting), so as to obtain the shadow images in a way that look "reasonable" to the human eyes. As a result, the full secret image including the secret target part and the other parts will be recovered by collecting any k or more shadow images, which can be further reconstructed losslessly by adding all the inpainted meaningful shadow images. Experiments are conducted to evaluate the efficiency of the proposed scheme.

The rest of the paper is organized as follows. Section 2 introduces PSIS problem description and some basic requirements for the proposed scheme. In Section 3, the proposed scheme is presented in detail. Section 4 gives some discussions of the proposed scheme. Section 5 is devoted to experimental results. Finally, Section 6 concludes this paper.

2. Preliminaries

In this section, we give the PSIS problem description and some preliminaries as the basis for the proposed method. The original secret image S is shared among total n shadow images, while the reconstructed secret image S' is reconstructed from t $(k \leqslant t \leqslant n, t \in Z^+)$ shadow images.

2.1. Problem definition

As show in Fig. 1, for the given secret image S in Fig. 1(a), Fig. 1(b) indicates the same input cover image C obtained by manually selecting and removing the secret target part from the original secret image S, where the notations of different parts and their edge are presented in Fig. 1(c) and in general in Fig. 1(d). The region Ω is the secret target part (object), part illustrates the untouched part, and $\partial\Omega$ denotes the edge of the two parts. Shadow images covered secret after sharing are denoted as SC_i, $i = 1,2,...,n$ for (k,n) threshold.

The PSIS problem can be described as follows: From the selected target part Ω and the associated cover images $C_1,C_2,...,C_n$, the PSIS scheme may generate n meaningful shadow images SC_i, $i = 1,2,...,n$, distributed to n associated participants, where each shadow image looks like a nature image. When any k or more shadow images are collected, the full secret image including the secret target part can be reconstructed. Whereas even if infinite computational power is available, less than k shadow images will reveal nothing about the secret target part.

2.2. Linear congruence

Eqs. (1) and (2) are the basic equations for LC secret sharing, by which (k,k) threshold secret sharing can be achieved, where P denotes a number larger than the biggest pixel value, x_i and s represent the i-th shared pixel and secret pixel, respectively. In Eq. (1), a one-to-many mapping between s and all the x_i is established, so the secret value can be recovered losslessly with all the shared values. But there is no direct map relationship between secret value and less than k shared value, thus the method is secure. So Eq. (1) guarantees the feasibility of precise recovery and security for the proposed scheme. At the meanwhile, the condition in Eq. (2) ensures that no duplicate values exist in the first k shared pixels. Eq. (2) is required due to LC recovery method.

$$(x_1 + x_2 + \cdots + x_k) \ mod \ P = s \tag{1}$$

$$x_i \neq x_j, \quad when \ i \neq j. \tag{2}$$

Eq. (3) is the basic equation for LC secret recovery. After removing the duplicate shared values, the rest shared values $x_{i_1},x_{i_2},...,x_{i_l}$ take part in the computation for the recovered secret value s' using Eq. (3).

$$s' = (x_{i_1} + x_{i_2} + \cdots + x_{i_l}) \ mod \ P \tag{3}$$

Fig. 2 indicates an example by directly applying LC method for (2,2) threshold, where the input secret image is the same as Fig. 1. We can see that the secret target part can be reconstructed losslessly, while the corresponding secret target parts of the shadow images are noise-like, which may decrease the efficiency of shadow images management and increase the suspicion of secret image encryption. In the revealing process of the secret image, it only needs to iterate l pixels and execute $l-1$ times addition operation and one time module operation to decode a secret pixel. Obviously, the time complexity is smaller. Hence, LC sharing idea is selected in our scheme as an SIS method. In the proposed scheme shown in Section 3.2, LC will be extended to support (k,n) threshold.

2.3. Image inpainting

Many image inpainting schemes were proposed in the literature, here Criminisi et al.'s approach [26,27] will be applied in our scheme, which is researched widely. We will introduce Criminisi et al.'s image inpainting approach in detail. The keynote of it is the selection of patch priorities order in region-filling. The patch with the highest priority will be filled preferentially. The priorities will be renewed after every filling until the image is inpainted totally in the same manner. The main inpainting process includes:

1. Select the part Ω to be inpainted, and $\Omega = S - \Phi$.
2. Determine the size of template window, denoted as Ψ_p , using image texture feature, where any $p \in \partial\Omega$ exhibits center of template window and the size of the window should be larger than the biggest texture element.
3. Compute patch priorities by Eq. (4) which is defined as the product of the confidence term and data term.

$$W(p) = C(p)D(p) \tag{4}$$

where $C(p)$ and $D(p)$ denote the confidence term and data term, respectively, defined as follows:

$$C(p) = \frac{\sum_{q \in \psi_p \cap \bar{\Omega}} C(q)}{|\psi_p|} \tag{5}$$

$$D(p) = \frac{|\nabla S_p^{\perp} \cdot n_p|}{a} \tag{6}$$

where $|\psi_p|$ indicates the area of ψ_p and a is a normalization factor. $\nabla S_p^{\perp}$ and n_p denote the isophote direction and the normal vector direction at point p, respectively.

The confidence term expresses the amount of reliable information contained in template window. The data term measures the difference between the isophote direction and the normal vector direction. In a word, we may conclude that the template window includes more information and the difference between the isophote direction