Optics & Laser Technology 54 (2013) 389–400

Contents lists available at ScienceDirect

Optics & Laser Technology

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

A new meaningful secret sharing scheme based on random grids, error diffusion and chaotic encryption

Ahmed A. Abd El-Latif [a,b,*], Xuehu Yan [a], Li Li [c], Ning Wang [a,d], Jia-Liang Peng [a,e], Xiamu Niu [a]

[a] School of Computer Science and Technology, Harbin Institute of Technology, 150080 Harbin, China
[b] Mathematics Department, Faculty of Science, Menoufia University, Shebin El-Koom 32511, Egypt
[c] School of Computer Science and Technology, Harbin Institute of Technology, Shenzhen Graduate School, Shenzhen 518055, China
[d] The 23th Institute of the Second Academy, Aerospace Science and Industry Corporation, Beijing 100854, China
[e] Information and Network Administration Center, Heilongjiang University, 150080 Harbin, China

ARTICLE INFO

Article history:
Received 22 December 2012
Received in revised form
25 February 2013
Accepted 13 April 2013
Available online 19 July 2013

Keywords:
Secret sharing
Random grids
Chaotic encryption

ABSTRACT

In this paper, a novel secret image sharing scheme is proposed to encode a secret binary image into meaningful shadow images. It combines random grids (RG), error diffusion (ED) and chaotic permutation. The secret image is first encrypted based on chaotic permutation and then shared among n halftone shadow images RGs generated by error diffusion, while the recovered secret image is recovered from k or more shadow images. The proposed scheme has the advantages of simple computation, alternative order of shadow images in recovery, avoids the design of complex codebook, and avoids the pixel expansion problem. Experimental results and analysis show the effectiveness of the proposed scheme.

1. Introduction

In recent years, secret image sharing techniques have attracted considerable attention to scientists and engineers as another branch alongside conventional cryptography to protect sensitive images from rapacious behaviors. It distributes a secret image among some participants by splitting the secret image into noise-like shadow images (also called shares or shadows) and recovering the secret by collecting sufficient authorized participants (shadow images) [1].

Until now, various secret sharing schemes for digital images have been developed in order to promote communication security. The original visual secret sharing (VSS) scheme is proposed by Naor and Shamir in 1995 [1]. In the threshold-based VSS scheme, a binary secret image is shared by generating corresponding n noise-like shadow images. Any k or more noise-like shadow images are superposed to obtain the secret image based on human visual system (HVS) and probability. The notable properties for VSS proposed by authors in [1] are as follows [2,3]:

(1) *Implement the* (k, n) *threshold secret sharing mechanism*: Share the secret image among n shadow images and need at least k shares to recover the secret image, which could be loss-tolerant and control access.
(2) *Simple generation of the shadow images or recovery of the secret image*: Only simple computation in the two phases.
(3) *The order of the shadow images is alternative*: There is no need to record the order of the shadow images when recovering secret image.

It is noted, however, that the construction of the VSS scheme usually uses the cover pixel block replacing the pixel in the original secret image, and randomly chooses the satisfactory pixel block. Therefore, the good VSS scheme should satisfy more properties as follows [2–10].

(4) *Avoiding the pixel expansion and shape distortion*: The shadow images are not larger than the original secret image, which could reduce the storage and transmission bandwidth.
(5) Avoiding the design of complex codebook. Since the codebook is not easily constructed, especially for some specific applications.
(6) Shadow images are meaningful but not noise-like images, which will not invite the adversary's attention and be user-friendly to manage shadow images.

In this sense, there has been an enormous effort to overcome the drawbacks of Naor's and Shamir's scheme. The scheme in [11] has the property 6, but still lacks 4 and 5. Yang [12] proposed a probability-based VSS scheme which satisfies 4 but not 5 and 6. Wang et al. [5] proposed a secret sharing $(2, n)$ scheme based on Boolean operations (XOR and AND operations) that satisfies properties 5 and 6 but not properties 1 and 4 [13,14] in VSS

* Corresponding author at: School of Computer Science and Technology at Harbin Institute of Technology, 150080 Harbin, China. Tel.: +86 451-86402861.
E-mail addresses: ahmed_rahiem@yahoo.com (A.A. Abd El-Latif), xuehu.yan@ict.hit.edu.cn (X. Yan), lili.isec2008@gmail.com (L. Li), ning.wang@hit.edu.cn (N. Wang), jialiang.peng@hit.edu.cn (J. Peng), xiamu.niu@hit.edu.cn (X. Niu).

0030-3992/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.optlastec.2013.04.018

scheme. Halftoning attempts to alleviate this suspicion by having satisfying visual quality. In [4–17] halftone images can be shared with visual meaningful shadow images which have a higher quality and low computation by employing error diffusion techniques [18]. However, these schemes suffer from unexpected pixel expansion.

Since VSS by random grids (RG) could avoid pixel expansion and has no codebook needed, some other researchers have paid attention to RG-based VSS. Encryption of binary secret images based on random grids (RG) is firstly presented by Kafri and Keren [19], each of which is generated into two noise-like RG (shadow images or share images) that have the same size as the original secret image. The decryption operation is the same as traditional VC. The image encryption by RG [7,20–22] satisfies 4 and 5 but not 1 and 6. For gaining meaningful shadow images, [23–25] exploit some significant efforts based on color shadow images or designing light transmissions, however, they suffer from cross interference of shared images, small pixel expansion, complex generation computation or complementary shadow images, and do not satisfy the property of general (k, n) threshold. Chen and Tsao [6] proposes a visual secret sharing (k, n) scheme based on Boolean operations (XOR and OR operations) that satisfies properties 1, 4 and 5 but not property 6.

Herein, we propose a meaningful threshold VSS scheme based on error diffusion, RG and chaotic encryption. It combines random grids, error diffusion, and chaotic permutation. The proposed scheme has the following properties:

- It generates meaningful shadow images which will be more secure and be user-friendly to manage shadow images.
- Satisfies (k, n) threshold sharing which could be loss-tolerant and achieves the access control property.
- Avoiding the pixel expansion problem, this can save storage and bandwidth.
- Simple computation in the generation phase and recovery phase (needs only superposition).
- Alternative order of shadow images in recovery.
- Avoiding the design of complex codebook.

Simulations conducted show the feasibility, the effectiveness and the security of the proposed scheme.

The outline of this paper is as follows: Section 2 introduces the preliminary techniques. The proposed scheme is presented in Section 3. Section 4 is devoted to experimental results and analysis. Finally, Section 5 concludes this paper.

2. Preliminary techniques

This section introduces the related works of error diffusion technology [18,3], RG-based [6] VSS and the chaotic encryption based on discretized chaotic cat map.

2.1. Error diffusion technique

Dithering is a method that reconstructs the original continuous tone image. Error diffusion technique is to diffuse the error to the neighbor pixels where the error is difference value between the original grayscale value and its final dithered value.

Let I be the normalized $M \times N$ image. For the current pixel $I(i,j)$, $1 \le i \le M$, $1 \le j \le N$, $Q(i,j)$ is its threshold value, $I'(i,j)$ is its halftone value. H is the error diffusion matrix, $E(i,j)$ is the error. Herein, Floyd–Steinberg error diffusion matrix [26] shown in Eq. (6) and adaptive global threshold in [27] are adopted.

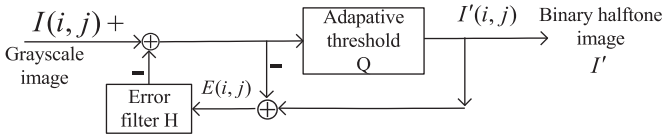

Fig. 1. Error diffusion flowchart.

The flowchart of error diffusion halftoning process is shown in Fig. 1 and the steps are described as follows:

(1) *Adaptive global threshold*: Adaptive global threshold combines the features of image pixels and the computation. It is computed as follows:
The histogram of I is normalized using Eq.(1). In Eq. (1), T is the total number of pixels in I, T_q is the number of pixels with value r_q, L is the number of grayscale levels in I.

$$p_r(r_q) = \frac{T_q}{T}, \quad q = 0, 1, 2, \ldots, L-1 \tag{1}$$

Assume the threshold value is Q, D_0 are pixels with grayscale [0, 1,…, Q−1], D_1 are pixels with grayscale [Q, Q+1, …, L−1]. Choose Q that maximizes inter-class (between class D_0 and class D_1) variance as the adaptive global threshold. The inter-class variance is defined as in Eq. (2). And Q is the adopted threshold value during dithering process.

$$Q = \arg\max_{max}\left(\sigma_B^2 = \omega_0(\mu_0-\mu_T)^2 + \omega_1(\mu_1-\mu_T)^2\right) \tag{2}$$

where

$$\omega_0 = \sum_{q=0}^{Q-1} p_q(r_q), \quad \omega_1 = \sum_{q=k}^{Q-1} p_q(r_q)$$
$$\mu_0 = \sum_{q=0}^{Q-1} qp_q(r_q)/\omega_0, \quad \mu_1 = \sum_{q=Q}^{L-1} qp_q(r_q)/\omega_1, \quad \mu_T = \sum_{q=0}^{L-1} qp_q(r_q) \tag{3}$$

(2) *Quantization*

$$I'(i,j) = \begin{cases} 1 & \text{if } I(i,j) \ge Q \\ 0 & \text{if } I(i,j) < Q \end{cases} \quad 1 \le i \le M, \ 1 \le j \le N \tag{4}$$

If the adaptive global threshold is considered, the quantization is performed by Eq. (4). The pixel value of $I(i,j)$ is quantized from real interval [0, 1] to value 1 or 0 by Eq. (5) with 1 denoting white pixel and 0 black.

(3) *Error computation*

$$E(i,j) = I(i,j) - I'(i,j) \tag{5}$$

The error $E(i,j)$ is the difference value between original value $I(i,j)$ and its final dithered value $I'(i,j)$ computing through Eq. (5).

(4) *Error diffusion*

$$H = \begin{pmatrix} 0 & (i,j) & \frac{7}{16} \\ \frac{3}{16} & \frac{5}{16} & \frac{1}{16} \end{pmatrix} \tag{6}$$

In Eq. (6), (i, j) is the current pixel location. The coefficients in the four directions denote the ratio for the error spreads into these four directions. Error diffusion techniques could spread the error between the original cover image and its dithered