Signal Processing: *Image Communication* 29 (2014) 128–134

Contents lists available at ScienceDirect

Signal Processing: *Image Communication*

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

A novel real-time and progressive secret image sharing with flexible shadows based on compressive sensing

Li Liu [a], Anhong Wang [a,*], Chin-Chen Chang [b,c,**], Zhihong Li [a]

[a] *Institute of Digital Media and Communication, Taiyuan University of Science and Technology, No. 66 Waliu Rd., 030024 Taiyuan, China*
[b] *Department of Information Engineering and Computer Science, Feng Chia University, No. 100 Wenhwa Rd., Seatwen, Taichung 40724, Taiwan*
[c] *Department of Computer Science and Information Engineering, Asia University, No. 500 Lioufeng Rd., Wufeng, Taichung 41354, Taiwan*

ARTICLE INFO

Article history:
Received 15 June 2013
Received in revised form
23 August 2013
Accepted 16 October 2013
Available online 23 October 2013

Keywords:
Compressed sensing
Secret sharing scheme
Progressive transmission
Measurement rate

ABSTRACT

A novel real-time and progressive secret image sharing scheme with flexible-size shadows is proposed. First, a secret image is measured by compressed sensing (CS). Then, the quantized measurement values are divided into n shadows using Shamir's (t,n)-threshold scheme. At the receiver side, the secret image can be reconstructed if any t of n shadows are obtained, but fewer than t shadows reveal no information. Due to the fact that CS's reconstruction quality is flexibly adaptive to the number of measurements, our scheme features flexible shadow size and obtains the property of real-time and progressive transmission as well as error resilient. Experimental results show that the proposed scheme achieves better performance in view of the reconstructed secret image.

1. Introduction

As more digital information is being shared and transmitted over the Internet, this poses a great threat to information security, especially in the fields of commercial services, telemedicine, and the military. Several methods (e.g. information hiding and digital image watermarking) have been proposed to enhance the security of secret images. A common drawback of these techniques is that the protected secret image is kept by a single participant. If this participant intentionally reveals this image, then the secret information will be lost.

Secret sharing (SS), also known as the (t,n)-threshold scheme, shares a secret image into n noise-like images (called shadows) and then distributes them to n different participants. The secret image can be reconstructed if $t(t \leq n)$ of the n shadows are obtained, but no information can be revealed if $t-1$ shadows are received. The protected secret image is kept by different participants; therefore, responsibility can be diffused, and the security of the secret image is assured.

Related research [1–4] aims to develop smaller shadows for easy transmission and storage of the secret image. For mobile or handheld devices which have limited network traffic and storage space, the size of each shadow should be as small as possible to guarantee quality. On the contrary, if a lossless reconstructed image is required in an environment with sufficient network bandwidth, then the smaller shadows are not necessary. Therefore, it is essential to design the sharing schemes that can flexibly adjust the shadow size according to the application environment.

Other topics [5–9] also have been discussed extensively, especially real-time and progressive transmission of secret images. With only a small amount of data, the entire secret image can be reconstructed, and the reconstructed image quality is updated progressively as more data are received. Real-time and progressive secret-sharing also brings some other benefits, like progressive browsing as well as quick feedback when the received rough version shows whether the secret image is the one desired. In 2005, Chen and Lin [10]

* Corresponding author. Tel.: +86 15003512391.
** Corresponding author at: Department of Information Engineering and Computer Science, Feng Chia University, No. 100 Wenhwa Rd., Seatwen, Taichung 40724, Taiwan. Tel.: +886 4 24517250x3790.
E-mail addresses: wah_ty@163.com (A. Wang), alan3c@gmail.com, ccc@cs.ccu.edu.tw (C.-C. Chang).

0923-5965/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.image.2013.10.003

proposed a fault-tolerant and progressive image transmission method which reconstructs the secret image progressively with the number of shadows. However, it affects the real-time property due to the huge data of each shadow. Huang and Li [11] developed a progressive transmission using the reversible integer-to-integer (ITI) wavelet transform. As an extension of the above method, Huang [8] presented an image-sharing framework for real-time and progressive transmission using the JPEG2000-generated bit stream and Shamir's threshold scheme. However, this scheme embeds error control codes and synchronization marks into the generated shadow images in order to improve security and error resiliency, which results in extra overhead.

Following the aforementioned works, this paper offers a novel design with most of the expected merits, including flexible shadow size, real-time and progressive transmission as well as error resilient capability. We employ the theory of compressed sensing (CS) and Shamir's (t,n)-threshold scheme. First, a secret image is measured by CS to produce measurement values which are equally important (reconstruction quality depends only on the number of the received measurement values). Therefore, CS is not sensitive to channel noise and has good robustness. Then, the quantized measurement values are shared in n shadows using the (t,n)-threshold scheme. The original secret image can be reconstructed by using any t or more shadows. Experimental results have proved the expected merits of the proposed scheme.

2. Background

2.1. Shamir's (t,n)-threshold scheme

The (t,n)-threshold scheme states that a secret number S is shared in n shadows $(S_1, S_2, \ldots, S_n)$, and the $(t-1)$ degree polynomial sharing function is defined as

$$f(x) = (a_0 + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1}) \bmod p, \quad (1)$$

where p is a random prime number, $a_0 = S$, and $a_0 < p$. The value of $a_1, a_2, \ldots, a_{t-1}$ is selected randomly from 0 to $(p-1)$. Each S_i can be derived as

$$S_1 = f(1), \ldots, S_i = f(i), \ldots, S_n = f(n). \quad (2)$$

Each S_i is called a shadow. The t-th shadow cannot be derived by using the received $t-1$ shadows. If $t-1$ shadows or fewer than $t-1$ shadows are received, S still cannot be revealed. Given any t of n shadows, the coefficients $a_0, a_1, a_2, \ldots, a_{t-1}$ of $f(x)$ can be calculated using Lagrange's interpolation, and the secret data $S = a_0 = f(0)$ can finally be calculated.

2.2. Compressed sensing

Assume a real-valued k-sparse signal $\mathbf{x}$ (length N) in an orthonormal basis matrix $\mathbf{\Psi}$ (size $N \times N$), $\mathbf{x} = \mathbf{\Psi\theta}$, where $\boldsymbol{\theta}$ has k non-zero significant coefficients only. CS theory states that $\mathbf{x}$ can be reconstructed (with certain accuracy) by m measurements:

$$\mathbf{y} = \mathbf{\Phi x} = \mathbf{\Phi\Psi\theta}, \quad (3)$$

where $\mathbf{y}$ is the measurement vector with length m, and $\mathbf{\Phi}$ is an $m \times N$ measurement matrix which is incoherent with $\mathbf{\Psi}$, $m \geq O(k \log N/k)$, $k < m < < N$. CS is reconstructed to solve the optimization problem [12]:

$$\min_{\boldsymbol{\theta}} |||\boldsymbol{\theta}|_{l_1} \quad s.t. \quad \mathbf{y} = \mathbf{\Phi\Psi\theta}. \quad (4)$$

Finally, $\mathbf{x}$ can be reconstructed by $\widehat{\mathbf{x}} = \widehat{\mathbf{\Psi\theta}}$.

In order to save storage and computing for real-time image processing, a block-based CS (BCS) [13] is proposed. An image is first divided into non-overlapping blocks of size $B \times B$, and each block $\mathbf{x_i}$ is sampled using the same operator. The corresponding measurement vector $\mathbf{y_i}$ (size $m_B \times 1$) can be obtained from $\mathbf{y_i} = \mathbf{\Phi_B x_i}$, where $\mathbf{\Phi_B}$ is an $m_B \times B^2$ measurement matrix with $m_B = \lfloor m/NB^2 \rfloor$.

3. Proposed scheme

The operating steps consist of an encoding phase and a decoding phase, as schematically shown in Fig. 1.

3.1. Encoding phase

3.1.1. Measurement

A secret image I is measured by BCS to obtain $\mathbf{y_i}$ for each block and orderly take down them into the overall matrix $\mathbf{y} = [\mathbf{y_1}, \mathbf{y_2}, \ldots, \mathbf{y_i}, \ldots, \mathbf{y_W}]$, where W is the total number of blocks.

3.1.2. Rearrangement

Since every line of y contains information of the whole image, it is critical to transform matrix $\mathbf{y}$ into row vector $\mathbf{y}'$ through line-by-line scanning in order to achieve real-time and progressive transmission; this is the so-called rearrangement process.

3.1.3. Quantization

Sharing coefficients for the image should be adapted to the range of 0 and 255, so we choose 8-bit non-uniform quantization.

3.1.4. Sharing

Every 8 bit from quantization is processed sequentially into a decimal sharing number, which is then input through the following steps:

(1) Select orderly t sharing numbers as coefficients $a_0, a_1, \ldots, a_{t-1}$ in Eq. (1).
(2) Repeat Step (1) until all sharing numbers are assigned. Then, sharing functions $f_1(x), f_2(x), \ldots f_j(x), \ldots, f_s(x)$ can be generated, where $s = \lceil m_B \times W/t \rceil$ is the number of pixels of every shadow.

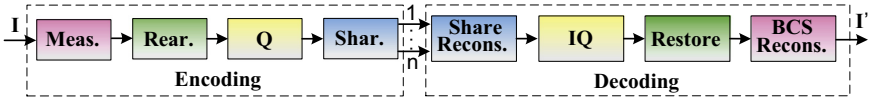

Fig. 1. The block diagram of the proposed system.