Signal Processing 99 (2014) 159–170

Contents lists available at ScienceDirect

Signal Processing

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

# Lossless and unlimited multi-image sharing based on Chinese remainder theorem and Lagrange interpolation

Chin-Chen Chang [a,b,*], Ngoc-Tu Huynh [a], Hai-Duong Le [a]

[a] Department of Information Engineering and Computer Science, Feng Chia University, Taichung 40724, Taiwan, ROC
[b] Department of Computer Science and Information Engineering, Asia University, Taichung 41354, Taiwan, ROC

ARTICLE INFO

*Article history:*
Received 19 November 2012
Received in revised form
16 December 2013
Accepted 20 December 2013
Available online 31 December 2013

*Keywords:*
Multi-image sharing
Chinese remainder theorem
Lagrange interpolation
Losslesss

ABSTRACT

This study proposes a novel multi-image threshold sharing scheme based on Chinese remainder theorem and Lagrange interpolation. The exceptional property of the scheme is its ability to retrieve any secret image without recovering all the other images. Therefore, it works efficiently and reduces computation cost in case it needs to recover only one image from shares. In term of capacity, the scheme has no limitation on number of input secret images, output shares and the recovery threshold. Another advantage of the scheme is that it can be used for many image formats whether it is binary or grayscale or color. Moreover, the scheme can recover the secret images without any distortion.



## 1. Introduction

Secret sharing, which was first independently proposed by Shamir and Blakely in 1979 [1,2], refers to methods for splitting a secret into several parts and distributing them amongst a group of participants, each of whom is assigned a share of the secret. Since then, secret sharing schemes are ideal for information sharing in which the loss of one or more shares will not compromise the confidentiality of the shared information. Conventional methods for encryption are ill-appropriated for achieving high level of security and reliability. This is because when storing the encryption key, we must make a decision whether to keep a single copy of the key in a secret location or to have multiple copies of the key hidden in different places for greater reliability. However, keeping duplicates of the key will decrease secrecy since creating additional keys will increase the possibility of losing them. To achieve the security and reliability of secret information, secret sharing is employed.

Secret sharing schemes have been widely applied in the construction of elaborated cryptographic primitives and several cryptographic protocols [9]. Nevertheless, whenever there are several images to be shared, the participants have to keep many shadows for different secret images. Thus, the conventional secret sharing schemes are inefficient in sharing more than one image; therefore, multiple secret sharing methods are taken into account. Multi-image sharing is an extension of image sharing when there are more than one secret image to be shared [4–7].

In 1989, Benaloh and Leichter [3] proposed a generalized method in which the secret can be revealed by subgroups of participants. These sub-groups of participants are used to form an access structure in which every element is an authorized sub-group. Each participant can possess many shares and he can be in different subgroups. It can be seen that this concept is more flexible and practical. Inspired by this concept, many scholars have expended the idea and applied it in digital image processing. They proposed several schemes to facilitate sharing multiple secret images at the same time with higher flexibility and more efficient [4,7,11,12,13,15,16]. In 2002, Tsai et al. [8] proposed a method to share multi-secret in

* Corresponding author at: Department of Information Engineering and Computer Science, Feng Chia University, No. 100 Wenhward, seatwen, Taichung 40724, Taiwan, ROC. Tel.: +886 4 245 172 50x3790; fax: +886 4 270 664 95.
*E-mail addresses:* alan3c@gmail.com (C.-C. Chang), ngoctu84vn@gmail.com (N.-T. Huynh), duonghaile@gmail.com (H.-D. Le).

0165-1684/$ - see front matter © 2014 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.sigpro.2013.12.022

digital images. In this scheme, each participant is assigned a unique number $N$ and one grayscale cover image. The participant uses this image to generate a set of shares from a secret message and distribute these shares to others. The secret message is embedded in the least significant bits of the cover images. There are only two shares for each secret. It can be retrieved by performing "Exclusive-OR" operations on the certain pairs of shares. Later on, in 2005, Wu and Chang [11] proposed a (2, 2)-visual secret sharing scheme that adjusts circular shares to handle the limitation of the number of rotating angles. Although, this method is more efficient than some previous schemes, it is only applicable when there are exactly two secret images to be shared. Because their image reconstruction is lossy, the contrast of revealed secret images is quite low. In 2007, a study that overcame the limitation on number of secret images in Wu and Chang's method was proposed by Shyu et al. [12]. Their visual secret sharing scheme encrypts a set of $N$ secret images $N \geq 2$ into two circle shares in such the way that the secrets can only be revealed when all the shares are obtained. Each of the shares alone does not leak any meaningful information. In 2008, Feng et al. [14] introduced another method which also creates circular shares from multiple secrets $N \geq 2$. The scheme contrives a *stacking relationship graph* for secret pixels and shared blocks, as well as a set of visual pattern to create two ring shares $R_1$ and $R_2$ such that $R_1$ and $R_2$ are random rings, whereas $R_1 \otimes R_2^{(i-1)a}$ can reveal the $i$th secret, for $1 \leq i \leq N$ and $a = 360^\circ/N$. The pixel expansion of the scheme is $2N$ and it does not put restriction on the numbers of secret images. But the problem of low contrast remains since most of the previous researches for sharing multi-images often apply "turning" or "rotation" on one of the shares to reveal secrets [14, 18,19].

Although many schemes have been proposed, there is no scheme without flaws. The first drawback that is commonly seen in these schemes lies in the extremely low contrast of the output shadows. This might make the reconstructed images unrecognizable and in some cases the hidden texts are illegible. The second drawback is the pixel expansion problem in which the sizes of the outputs are expanded to two or four times larger than the original ones. It causes the quality of the shadows drop drastically and the shadows might reveal a substantial portion of the secret, or even exposing the whole one. Furthermore, these schemes are suitable for binary images, but not for grayscale ones. Last, most of these schemes cannot recover the secret images losslessly. It means there are always inevitable distortions present in the recovered images. We also notice that all the schemes are not able to retrieve an arbitrary image without fully recovering all the secret images.

In general, there are several essential aspects that must be considered in a multiple visual secret sharing scheme such as security, accuracy, and sharing capacity. This study proposes a scheme that can satisfy all of the essential criteria. As we know, moreover, Chinese Remainder Theorem (CRT) has existence and uniqueness of the solution which can easily be found through a non-constructive argument. Due to the purpose of generating a set of unique shadows for multiple secret, we exploit the CRT method in our scheme. Our scheme can share and construct unlimited number of images and shadows. The quality of recovered images is guaranteed to be perfect without any distortion since there is no loss in reconstruction of secret images. And most interested of all, our scheme can retrieve any secret image without recovering all the secrets.

The rest of this paper is organized as follows. In Section 2, the preliminary is introduced. Then, we give a detailed description of our proposed scheme in Section 3. In Section 4, the experimental results and discussions are given. Finally, we conclude our study in Section 5.

## 2. Preliminary (Chinese remainder theorem)

The story behind the "Chinese remainder theorem" (CRT) goes like this. In the first century, Chinese mathematician Sun Tsu solved a problem which is to find a smallest number that leaves the remainders of 2, 3, and 2 when divided by 3, 5, and 7, respectively. The answer for this is the number 23. Based upon his work, the Chinese remainder theorem was generalized.

**Theorem.** Let $n_1, n_2, \ldots, n_k$ are positive integers which are relatively prime and $n = n_1 n_2 \ldots n_k$, then for any given sequence of integers $a_1, a_2, \ldots, a_k$, the following set of simultaneous congruences

$$x \equiv a_1 (\mathrm{mod}\ n_1)$$
$$x \equiv a_2 (\mathrm{mod}\ n_2)$$
$$\vdots$$
$$x \equiv a_k (\mathrm{mod}\ n_k)$$

for $i = 1, 2, \ldots, k$, has a unique solution modulo $n$ for the unknown $x$.

## 3. Proposed scheme

In this paper, we consider a case when there are $m$ secret images needed to be shared among a group of $n$ participants. Each participant is given a unique share computed from the set of original images. In our scheme, these shares are not images, let alone meaningful ones. They are actually just matrices of the same size as the images. In order to recover the secret images the proposed scheme requires only a subset of $k$ shares from the participants. The size $k$ of this subset is called the threshold, and it is chosen by the dealer.

In this scheme, we deploy Chinese remainder theorem and the Lagrange interpolation [17] to accomplish the aforementioned goal. An appealing characteristic of Chinese remainder theorem, which fits in our scheme perfectly, is that its unique solution is, in fact, a synthesis of all the remainders of a set of congruences. If we treat pixel values selected from the secret images as remainders of congruences, Chinese remainder theorem guarantees that there is exactly one solution from which the pixels are recovered losslessly. Next, this solution is used as coefficients in a polynomial function of degree $k$. The outputs when evaluating this function at $n$ integer inputs chosen by the dealer are the shares for the participants.

When we want to retrieve any of the original images, we first collect a set of any $k$ shares. Then, we use Lagrange interpolation to obtain the interpolating function at $k$