Polynomial-Based Secret Image Sharing Scheme with Fully Lossless Recovery

Wanmeng Ding, National University of Defense Technology, Hefei, China
Kesheng Liu, National University of Defense Technology, Hefei, China
Xuehu Yan, National University of Defense Technology, Hefei, China
Lintao Liu, National University of Defense Technology, Hefei, China

ABSTRACT

Lossless recovery is important for the transmission and storage of image data. In polynomial-based secret image sharing, despite many previous researchers attempted to achieve lossless recovery, none of the proposed work can simultaneously satisfy an efficiency execution and at no cost of some storage capacity. This article proposes a secret sharing scheme with fully lossless recovery based on polynomial-based scheme and modular algebraic recovery. The major difference between the proposed method and polynomial-based scheme is that, instead of only using the first coefficient of sharing polynomial, this article uses the first two coefficients of sharing polynomial to embed the pixels as well as guarantee security. Both theoretical proof and experimental results are given to demonstrate the effectiveness of the proposed scheme.

KEYWORDS

Lossless Recovery, Modulo Algebra, Polynomial-Based Secret Sharing, Secret Image Sharing

INTRODUCTION

Security is a big concern when considering the storage and transmission of image information. Traditional cryptography (Assad & Farajallah, 2016; Li, El-Latif, Shi, & Niu, 2012; Zhang & Xiao, 2014) method cannot prevent the data from being lost or corrupted during the transmission. Instead of cryptography, secret sharing is a way to ensure security since it has a property of loss-tolerant. Secret sharing, which comes from key management, was introduced by Shamir (1979) and Blakley (1979) independently. A \( (k, n) \) threshold secret sharing encrypts the secret into shares, and distributes the shares among \( n \) participants \( (k \leq n) \). When any \( k \) or more participants collect together, the secret can be revealed. With this property of loss-tolerant, the secret can be decoded under the case even some shares are lost. Furthermore, secret sharing can be applied in many scenarios (Belazi & El-Latif, 2016; Yan et al., 2017). For example, in distributed storage and transmission, an image can be shared into \( n \) shares by a \( (k, n) \) threshold secret sharing scheme and be stored in \( n \) severs, the secret can be decoded under the case even \( n-k \) or less servers are broken.

Shamir’s polynomial-based scheme (Li, Ma, Su, & Yang, 2012; Li, Yang, Wu, Kong, & Ma, 2013; Lin, S. J., & Lin, J. C., 2007; Shamir, 1979; Thien & Lin, 2002; Yang & Ciou, 2010) encrypts the secret into \( n \) shares using a polynomial and distributes the \( n \) shares to \( n \) participants separately. When any \( k \) or more participants with their shares get together, the secret can be reconstructed by Lagrange interpolation (Bleichenbacher & Nguyen, 2000; Chen, Liu, & Wang, 2008; Werner, 1984).

DOI: 10.4018/IJDCF.2018040107

Copyright © 2018, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
Noar and Shamir (1994) extended the concept of secret sharing from number to image. In 2002, Thien and Lin (2002) used Shamir’s scheme to share secret images in domain $[0, 250]$. The scheme embedded the secret pixels in all the coefficients of the sharing polynomial, thus reducing the size of shadow images to $1/k$ times that of the original secret image. However, the scheme in Thien and Lin’s work truncated all gray values larger than 250 to 250 so that the method cannot actually get a lossless secret image (2002).

In terms of actual applications, the ability to recover image losslessly can be useful in a number of scenarios (Devaki & Rao, 2012; Hu & Jeon, 2006; Li, El-Latif, Yan, & Wang, 2012; Tso, Lou, Wang, & Liu, 2008; Yan & Lu, 2017). In real-world applications, like in area of medicine and military (Cheddad, Condell, Curran, & McKeivitt, 2010), images details are significant and lossless images are important for the transmission and storage of image data.

To losslessly recover the secret images, there are many attempts. Thien and Lin (2002) split the pixel whose value is larger than 250 into two pixels. However, the processes changed the shape of the shadow images and at the cost of storage capacity. Yang et al. in (2010; 2007) used Galois Field GF ($2^8$) rather than the ordinary arithmetic (mod 251) to process all the grayscale values for an 8-bit pixel and achieved a lossless scheme, which improves the previous scheme to a lossless version without additional pixels. In addition, some other schemes [9] also make use of this method to achieve a two-in-one (Li, Yang, & Kong, 2016; Lin, S. J. & Lin, J. C., 2007; Wu & Sun, 2013) image secret sharing scheme. However, the method increased computational complexity because of the polynomial operations in Galois Field GF ($2^8$). Zhao et al. (2016) also employed the technique of dividing a pixel whose value is larger than 250 into two to recover the secret image without loss. But the scheme also needed expansible shares. Despite many previous attempts addressing the lossless recovery, none of the proposed work can simultaneously satisfy two requirements that include the no additional pixels and low computational complexity.

In this paper, the authors proposed the polynomial-based secret sharing scheme with fully lossless recovery. The researchers split the pixels whose value are larger than 250 into two values and save the overflow value as the second coefficient in sharing polynomial. The major difference between the proposed method and traditional polynomial-based schemes is that, instead of only using the first coefficient of sharing polynomial, the authors used the first two coefficients of sharing polynomial to embed the secret pixels as well as guarantee security. The proposed scheme need no expansible shares and is at low computation cost because of modulo algebra when compared with other lossless recovery schemes. Experimental results and analysis are given to demonstrate the effectiveness of the proposed scheme.

The rest of the paper is organized as follows. Section 2 introduces some preliminary techniques as the basis for the proposed scheme. Next, in Section 3, the proposed scheme is presented in detail. Moreover, Section 4 gives experimental results and analyses of the proposed scheme. Finally, Section 5 draws the conclusions of the work.

PRELIMINARIES

Since the proposed scheme is based on Shamir’s scheme, the authors will firstly introduce the Shamir’s scheme in this section as the basic for the proposed scheme. In what follows, the goal is to share the secret image $S$ into $n$ shadow images $SC_1, SC_2, SC_n$ in such a way that: (1) knowledge of any $k$ or more shares make $S$ easily computable; (2) knowledge of any $k-1$ or fewer shares leaves $S$ completely undetermined. The scheme is based on polynomial interpolation: given k points in the 2-dimensional plane $(x_1, y_1), \ldots, (x_k, y_k)$ with distinct $x_i$, there is one and only one polynomial $f(x)$ of degree $k-1$ such that $f(x_i) = y_i$ for all $i$. For example, the authors take a pixel value $s$ as the gray value of the first secret pixel, and then to split $s$ into $n$ pixels corresponding to $n$ shadows. The specific scheme is listed as follows:
Secure Robust Hash Functions and Their Applications in Non-interactive Communications
www.igi-global.com/article/secure-robust-hash-functions-their/47071?camid=4v1a