The Journal of Systems and Software 86 (2013) 485–500

Contents lists available at SciVerse ScienceDirect

The Journal of Systems and Software

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

Invertible secret image sharing for gray level and dithered cover images

Mustafa Ulutas, Güzin Ulutas*, Vasif V. Nabiyev

Department of Computer Engineering, Karadeniz Technical University, Trabzon 61080, Turkey

ARTICLE INFO

Article history:
Received 12 August 2011
Received in revised form 5 July 2012
Accepted 17 September 2012
Available online 26 September 2012

Keywords:
Secret sharing
Exploiting Modification Direction
Invertible
Modulus operator

ABSTRACT

Secret image sharing approaches have been extended to obtain covers from stego images after the revealing procedure. Lin et al.'s work in 2009 uses modulus operator to decrease the share image distortion while providing recovery of original covers. Their work use gray level or binary image as cover. Stego images have approximately 43 dB and 38 dB PSNR for gray level and binary covers respectively. Lin et al.'s work in 2010 provides enhanced embedding capacity but does not support binary covers. Gray level covers' PSNR is reported approximately 40 dB. The proposed method enhances the visual quality of stego images regardless of intensity range of covers. Exploiting Modification Direction method is used to hide the shared values into covers. The method also utilizes modulus operator to recover original cover pixels. Stego image PSNR is approximately 47 dB for gray level covers. The method provides 4–7 dB increase respectively on the stego image quality compared to others. Stego images have also higher PSNR (43 dB) for dithered covers. The proposed method generates stego images with higher PSNR regardless of the intensity range of the cover image.

1. Introduction

The development of network technologies makes the digital distribution of data more convenient. However, distributing the important data over public network makes the data vulnerable to attacks. Therefore, protection of digital data becomes a critical issue in recent years. Some techniques have been developed to overcome this problem. Cryptography and steganography are the two techniques used for protecting data. Former technique uses mathematical transformation to protect the data from the malicious eyes. Secret data is transformed into unreadable form to provide the security. However, latter method hides the data into a cover medium. This medium can be any content such as image, video, audio or a text file. Embedding the secret data into the least significant bits (LSB) of the cover medium is the most frequently used technique known as the LSB embedding in the literature.

Both of these methods accommodate the secret data into one medium. Corruption of the medium results in the loss of the secret data. Secret Sharing Schemes are used to overcome this problem. Shamir (1979) proposed a secret sharing method called (k, n) threshold secret sharing scheme. His method divides the secret among n participants. Each participant gets a piece of secret called share. If any k or more participants gather their shares, secret will be revealed. Otherwise, no information about the secret image is revealed. Shamir's method uses Lagrange's interpolation technique to reconstruct the secret. A $(k-1)$th degree polynomial, $f(x)$, with constant term as the secret is constructed. Evaluation of the polynomial $f(x_i)$ for unique values of x_i constitutes shares. Therefore, shares are unique points on the polynomial $f(x)$. Lagrange's interpolation technique is used for reconstructing the secret from k points gathered from participants.

Blakley (1979) proposed another technique in the same year to share a secret. His method is based on geometric approach. Secret is a point in k-dimensional space according to his method. Shares are constituted as hyperplane equations that intersect on the secret point. Secret point is reconstructed from the intersection of at least k hyperplanes.

After these two pioneering research, Asmuth–Bloom and Mignotte proposed (k, n) threshold secret sharing schemes based on the Chinese Remainder Theorem (CRT) in 1983 (Asmuth and Bloom, 1983; Mignotte, 1983). They use special sequences of integers along with the CRT. However, the former technique is more secure than the latter due to the use of random parameters.

Both Blakley's and Shamir' secret sharing approaches are used to share digital images among participants recently. Chen and Fu (2008) proposed a new secret image sharing technique using Blakley's secret sharing scheme based on geometric properties. In another study, Tso (2008) used Blakley's approach to both share a secret image among participants and enhance the size expansion ratio of shares.

Thien and Lin (2002) used Shamir's polynomial approach to share a gray level secret image. Intensity values of the secret pixels

* Corresponding author. Tel.: +90 533 2277990.
E-mail addresses: ulutas@ieee.org (M. Ulutas), guzin@ieee.org (G. Ulutas), vasif@ktu.edu.tr (V.V. Nabiyev).

0164-1212/$ – see front matter © 2012 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.jss.2012.09.027

are in 0–255 range. Shamir's approach selects a prime value enforcing a unique solution during the recovery procedure. Selected prime value also defines a constraint on the range of the pixel values. Thien and Lin's method used 251, the largest prime value less than 255. This selection enforces truncation of the pixel values larger than 250 before the encoding process which distorts the secret image. However, their method generates noise like images that attracts attention of the malicious users. Lin and Tsai (2004) proposed a method that uses steganography to hide shared values into cover images. Their method also uses parity bits to provide the method authentication ability. Their method embeds one secret pixel into a 2×2 pixel cover block using LSB embedding technique. Yang et al. (2007) emphasized that using the parity bit as an authentication mechanism is not an appropriate way. Instead, their technique uses hash functions to authenticate stego blocks. Furthermore, their method prevents distortion of the secret image using Galois Fields. Chang et al. (2008) reports two shortcomings in these methods. One is the weak authentication due to a single authentication bit which cannot protect the integrity of the stego images. The other shortcoming is poor visual quality of the stego images. Their method proposes a technique that uses the CRT to improve the authentication ability of the previous methods. Their method also enhances the visual quality of the stego images. Yang and Ciou (2009) shows that Chang et al.'s scheme does not improve the stego image quality and instead degrades. Their work also reports the correct PSNR for Chang et al.'s scheme.

Lin et al. (2009) employs the modulus operator for decreasing the stego image distortion. Their method permits involved participants to restore a lossless secret image and to reconstruct a distortion free cover image. Their work emphasize that if covers are significant images, even slight distortion may be intolerable. Therefore, reconstruction of the cover image after the revealing procedure is an important issue in this research area as reported by them. Lin et al. uses modulus operator defined in Thien and Lin (2003) to hide the shared pixel values in the cover images. Stego images generated by their method have a PSNR of 43 dB for $k=4$. Their method is also tested on binary cover images which have approximately 38 dB PSNR. Their method also necessitates adjusting the underflow and overflow conditions. Difference between stego and cover pixels is in $[-3,3]$ range for grayscale cover images and in $[-6,6]$ range for binary cover images. Their method has lower PSNR for binary images due to the underflows and overflows.

Lin and Chan (2010) proposed a method that is based on modulus operation to improve the embedding capacity of Lin et al. (2009). Their method generates stego images with 40 dB PSNR for gray level cover images. However, binary or dithered cover image is not considered by their scheme. Their method has lower PSNR with improved embedding capacity. Difference between stego and cover pixels is in $[-6,6]$ range for grayscale cover images. The method represents the secret data in base m notation. Their results also indicate that cover image pixel values within $[\lfloor 255/m \rfloor \times m, 255]$ cannot be used to embed the shared pixel values.

Method described in Lin et al. (2009) uses modulus operator proposed in Thien and Lin (2003) to embed the shared values into cover images to improve the stego image quality according to traditional LSB embedding scheme. However, the modulus operator causes underflow and overflow for dithered images. On the other hand, embedding strategy in Lin and Chan (2010) based on modulus operator prevents the use of dithered images as cover images. We use Exploiting Modification Direction (EMD) method proposed in Zhang and Wang (2006) with a specially crafted equation to hide the shared values into cover images with less distortion according to LSB embedding and modulus operator. Using EMD during the embedding procedure ensures the visual quality of stego images independent from the intensity range of the cover images (dithered or grayscale) as shown in the experimental results.

The proposed method generates stego images with improved visual quality even for binary cover images. Other works in the literature indicate that visual quality of the stego images depends on the intensity range of the cover images (Lin et al., 2009; Lin and Chan, 2010). Our method generates stego images with enhanced visual quality in either case: 47 and 43 dB PSNR stego images for gray scale and binary cover images respectively. It enhances the stego image quality compared to other methods reported in the literature regardless of the intensity range of the cover images. The difference between stego and cover pixels is in $[-2,2]$ range for gray scale and in $[-4,4]$ range for dithered cover images. Reduced range difference between the cover and stego pixels provides enhanced stego image quality. Lin et al.'s distortion free secret sharing scheme emphasized that even slight distortion may be intolerable if the shared cover images are significant. Our method also recovers cover images after revealing procedure without distortion. Modulus operator is used to recover the original cover pixel values in the revealing procedure.

The rest of the paper is organized as follows. The details of the EMD method, Lee's method and specially crafted EMD function used by the proposed method are given in Section 2. The proposed scheme is explained in detail in Section 3. Some of the experimental results are summarized and compared with Lin et al.'s method according to PSNR values of the stego images in Section 4. Conclusions are drawn in Section 5.

2. Literature review

The proposed method uses a modified version of the EMD method during the embedding procedure. The details of EMD method, its modified version called by 8-ary method and specially crafted function based on EMD are discussed in this section respectively.

2.1. Exploiting Modification Direction method

Mielikainen (2006) proposed a method that exploits direction of modification to the cover pixels. Mielikainen's method is immune to the steganographic attacks because it does not exhibit the asymmetric property of the LSB replacement method. Zhang and Wang (2006) proposed a steganographic method called by EMD to transform the secret data into a stream of secret digits in a $(2n+1)$-ary notational system.

Their method assumes that each secret digit in a $(2n+1)$-ary notational system is carried by n cover pixels and is denoted by $(g_1, g_2, \ldots, g_n)$. Only one pixel is incremented or decremented by one in this group. $2n$ possible ways of modification using a group with n pixels exist. One more case is that no pixel is changed. Therefore, $(2n+1)$ modification can be realized with a group of n pixels.

The secret message to be embedded is converted into $(2n+1)$-ary notational system called by secret digits. Each secret digit varies in $[0,2n]$ range. EMD method uses an embedding function f as weighted sum function evaluated modulo $(2n+1)$. This function is used to calculate a value for each pixel group as in (1).

$$f(g_1, g_2, \ldots, g_n) = (g_1 \times 1 + g_2 \times 2 + \cdots + g_n \times n) \bmod (2n+1) \quad (1)$$

Each cover-pixel group is used to represent one digit in the secret digits. If a secret digit to be embedded into corresponding cover pixel block, $(g_1, g_2, \ldots, g_n)$, is equal to the result of $f(g_1, g_2, \ldots, g_n)$, intensity values of the cover pixels do not change. Otherwise, only one pixel of the cover pixel group has to be modified by either incrementing or decrementing the pixel value by one. Thus, distortion of the cover image due to the embedding procedure is not easy to perceive.