J. Vis. Commun. Image R. 38 (2016) 284–296

Contents lists available at ScienceDirect

J. Vis. Commun. Image R.

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

# Implementation of TiOISSS with meaningful shadows and with an additional authentication image ☆

S. Srividhya [a], R. Sathishkumar [b,*], Gnanou Florence Sudha [a]

[a] Dept. of Electronics & Communication, Pondicherry Engineering College, Puducherry, India
[b] Dept of Electronics & Communication, Perunthalaivar Kamarajar Institute of Engg. & Tech., Puducherry, India

ARTICLE INFO

*Article history:*
Received 7 October 2015
Revised 6 February 2016
Accepted 8 March 2016
Available online 9 March 2016

*Keywords:*
Visual cryptography
Extended visual cryptography
Halftoning
Polynomial image secret sharing

ABSTRACT

Visual Cryptography Scheme (VCS) is a cryptographic technique for protecting secret images. The advantage of using VCS is that decoding can be done without use of any computations. Nevertheless, the reconstructed image has poor visual quality. Therefore, Two in One Image Secret Sharing Scheme (TiOISSS) was proposed which takes the advantage of VCS and provides good quality decoded images. However, the existing TiOISSS has security limitations as it is implemented only for noisy shadows. Hence, in this paper, modified TiOISSS is proposed and implemented for meaningful shadows. To enhance the security of the shares and prevent fake shares that may be introduced by hackers, an authentication image is shared along with the secret image. The quality of the reconstructed image is improved by using adaptive halftoning technique. Experimental results demonstrate the improved security and quality by the proposed scheme.



## 1. Introduction

For the past decade, there has been an enormous development in various information services necessitating secure communications between users. This has motivated advanced cryptographic techniques to be developed to overcome these security threats. Visual Cryptography Scheme (VCS) is one such cryptographic technique which can protect images shared between users. In the encoding process of VCS, the secret image is split into $n$ shares and it is distributed to the users. The secret image can be revealed by stacking the $n$ shares one over the other. This VCS was first proposed by Moni Naor and Shamir in 1994 [1] and its major advantage is that the decoding can be done by the Human Visual System (HVS) itself. In [2], $n$ shares are relaxed to $k$ shares ($k \leqslant n$) during the decoding process in ($k$, $n$) threshold scheme by which the secret image is revealed if the users have at least $k$ shares. To save the storage space and bandwidth, VCS without pixel expansion is developed in [3] where the size of the secret image and reconstructed secret image is the same. The authors in [4,5] propose a scheme that allows more than one secret image to be shared simultaneously in VCS. The VCSs which were initially developed dealt with noise like shares, leading to suspicion and attacks. To overcome this drawback, VCS with meaningful shares was created [6,7]. This VCS with meaningful shares is termed as Extended Visual Cryptography Scheme (EVCS) and was also developed without pixel expansion [8,9]. In [10], the authors used a binary image as the secret image and considered the auxiliary black pixels in the generation of shares to obtain a smooth decoded image. In [11], the author proposed that instead of using same cover image for EVCS, different cover image can also be used. In [12], an authentic image is shared to improve the security; however, the decoded image looks like a vague image.

There is also another category of image secret sharing called as Polynomial Image Secret Sharing (PISS) which can provide perfect reconstruction of secret image in decoding phase but it requires computation [13]. In [14], an Enriched Secret Sharing Visual Cryptography Scheme (ESSVCS) has been developed to improve security which uses VCS, PISS and private key encryption system to share more data. However, this scheme is not able to provide perfect reconstruction of the secret image. Hence, Two in One Image Secret Sharing Scheme (TiOISSS) is used which provides two decoding phases [15]. In the first decoding phase, the method reconstructs the vague image without computation giving the advantage of VCS and in second decoding it provides perfect reconstruction of secret image with computations giving the advantage of PISS. This TiOISSS without pixel expansion is explained in [16]. During the second decoding phase of TiOISSS, due to incorrect extraction of

☆ This paper has been recommended for acceptance by Shujun Li.

* Corresponding author.
*E-mail addresses:* srividhya2207@gmail.com (S. Srividhya), sathish.pkiet@gmail.com (R. Sathishkumar), gfsudha@pec.edu (G.F. Sudha).

http://dx.doi.org/10.1016/j.jvcir.2016.03.012
1047-3203/

PISSS shadows there is speckled reconstruction of secret image. In [17], this problem is overcome and in addition, quality of secret image is improved in the first phase, by replacing subpixels in Gray VCS (GVCS) by q bit gray value where $1 \leqslant q \leqslant 8$. However, the size of shadow increases and the smaller the values of q, better is the quality of the secret image. The quality and security of the secret image in TiOISSS is improved in [18] by using Adaptive Halftoning and by embedding keys in the shadows, however this method is implemented only for noisy shadows.

Thus, there are still limitations in terms of security in the existing TiOISSS. This paper proposes modifications to the existing TiOISSS to improve security of the secret image. To increase security of the shares and prevent fake shares that may be introduced by hackers, an authentication image is shared in addition to the secret image to provide integrity of the secret image. Nevertheless, the existing TiOISSS uses noise like shares which may arouse the attention of hackers. Hence in the proposed modified TiOISSS, meaningful shares are used along with authentication image. Secondly, to improve the quality of reconstructed image after first level of decoding, instead of conventional AM or FM halftoning, adaptive halftoning [18] is used for the secret and cover images. Experimental results indicate that the proposed method overcomes the drawback of the existing schemes and improves the security and quality of the secret image.

The paper is organized as follows. Studies on previous works and limitations are discussed in Section 1. The related works of proposed scheme are discussed in Section 2. The proposed Modified TiOISSS is dealt in Section 3. The simulation results are discussed in Section 4. Performance analysis like Contrast, Structural Similarity Index Measure is discussed in Section 5. Finally, the conclusions of the proposed work are made in Section 6.

## 2. Related works

### 2.1. Extended Visual Cryptography scheme (EVCS)

VCS with meaningful shadows is termed as Extended Visual Cryptography (EVCS) [6,7]. This EVCS overcomes the problem of suspicion which is faced by VCS with noise like shares. Several works using EVCS have been proposed [8–11], however the major drawback is that perfect reconstruction of the decoded image is not obtained and only a vague image is got.

For $(k, n)$ EVCS, two necessary conditions namely contrast and security are required to be satisfied.

#### 2.1.1. Contrast condition

Let $H(OR(B_0^{c_0,c_1\ldots\ldots c_n}|r))$ and $H(OR(B_1^{c_0,c_1\ldots\ldots c_n}|r))$ denote the ORed vector of any $r$ rows of basis matrix $B_0$ and $B_1$ respectively. For good contrast, the condition (1a) is to be satisfied, which means that the white pixels are reconstructed properly in the decoded image. Similarly for black pixels, the condition (1b) needs to be satisfied.

$$H(OR(B_0^{c_0,c_1\ldots\ldots c_n}|r)) \leqslant (m-h) \tag{1a}$$

$$H(OR(B_1^{c_0,c_1\ldots\ldots c_n}|r)) \geqslant (m-l), \quad for\ r=k, \quad where\ 0 \leqslant l < h \leqslant m \tag{1b}$$

In these equations, $c_n$ denotes pixel of $n$th cover image and $n$ denotes the number of cover images or shares. $H(.)$ denotes the Hamming weight function, $B_0^{c_0,c_1\ldots\ldots c_n}$ and $B_1^{c_0,c_1\ldots\ldots c_n}$ denote basis matrices that are constructed for white and black pixels by considering the cover image pixels $(c_0, c_1 \ldots\ldots\ldots c_n)$ (where $c_i \in \{0,1\}, 1 \leqslant i \leqslant n$ denotes $i$th cover image) and the secret image pixels. $h$ and $l$ are referred to as whiteness of white and black pixels of reconstructed secret image, $k$ denotes threshold value $(1 < k \leqslant n)$ such that at least $k$ shares can reconstruct the secret image and $m$ denotes pixel expansion in the shares.

For the Share images, in order to have better contrast, the conditions (2a) and (2b) should be satisfied.

$$H(OR(B_0^{c_0,c_1\ldots\ldots c_n}|i)) \leqslant (m-h_s), \tag{2a}$$

$$H(OR(B_1^{c_0,c_1\ldots\ldots c_n}|i)) \geqslant (m-l_s), \quad for\ i=1,2,\ldots n, \quad where\ 0 \leqslant l_s < h_s \leqslant m \tag{2b}$$

In the case of EVCS, the share images should look like meaningful cover images. Hence, to obtain meaningful share images it should satisfy conditions (2a) and (2b), where $h_s$ and $l_s$ are referred to as whiteness of white and black pixels of reconstructed cover images.

#### 2.1.2. Security condition

The pixels in meaningful share images are uniformly distributed such that if the user picks out any pixels from the forbidden meaningful share images, he/she should not be able to identify whether that particular pixel belongs to black or white pixels. This is expressed in condition (3) which ensures security of EVCS.

$$H(OR(B_0^{c_0,c_1\ldots\ldots c_n}|r)) = H(OR(B_1^{c_0,c_1\ldots\ldots c_n}|r)), \quad r \leqslant (k-1) \tag{3}$$

where $k$ is the threshold such that if users have $k$ or more than $k$ shares, they can reconstruct the secret image and the secret image cannot be reconstructed even when the users have $k-1$ shares.

### 2.2. Polynomial Image Secret Sharing Scheme (PISSS)

Thien and Lin developed PISS to share a secret image [13]. This method is evolved from Shamir scheme. This method can provide perfect reconstruction of secret image in decoding phase however; it requires computations in both encoding and decoding process.

In this scheme, each secret data is encrypted into another value by using the polynomial Eq. (4),

$$f(x) = (a_0 + a_1 x + \ldots. + a_{k-1}x^{k-1}) mod\ p \tag{4}$$

where $a_0$ is the secret data, $a_1$, $a_2$, …. $a_{k-1}$ are the random values and $p$ is a prime number.

To reconstruct the secret data, at least $k$ shares are required. Then, the coefficients of the polynomial function $f(x)$ are obtained by using Lagrange interpolation as,

$$l_i \equiv \prod_{\substack{1 \leqslant j \leqslant k \\ i \neq j}} \frac{x - x_j}{x_i - x_j} \tag{5}$$

In Eq. (5), in order to obtain corresponding $l_i$ coefficient, the variable $x$ is used such that we can identify $k$ pixels from it. This implies that $x_0$ is first pixel, $x_1$ is the second pixel and $x_{k-1}$ is the $k$th pixel. Since, at least $k$ shares are required to reconstruct the secret image, sequentially $k$ pixels are taken from the secret image and is encrypted and embedded in $k$ shares.

Finally, the coefficients and the encrypted values $(s_i)$ are substituted in the polynomial equation,

$$f(x) = \sum_{i=1}^{k} (s_i \times l_i) mod\ p \tag{6}$$

Expanding this equation, the secret data, $f(0)$ can be obtained. Instead of taking random values for the coefficients, Thien and Lin [13] took every non-used $k$ pixels from the secret image in sequential manner and substituted in (4) to obtain the encrypted values. Hence, the shadow size is $1/k$ of the secret image size. For encrypting the grayscale image, a large prime number like 251 can be chosen. However, this may lead to the loss of information