ALGEBRAIC VISUAL CRYPTOGRAPHY SCHEME FOR COLOR IMAGES

Mohsen Heidarinejad[1], *Amirhossein Alamdar Yazdi*[2] *and Konstantinos N. Plataniotis*[1]

[1] The Edward S. Rogers Sr. Department of ECE, University of Toronto, 10 King's College Road, Toronto, Ontario M5S 3G4, Canada
[2] Department of CE, Sharif University of Technology, P.O. Box 11155-9517, Tehran, Iran

ABSTRACT

This paper introduces a novel, cost effective visual cryptography scheme suitable for color image transmission over bandwidth constraint channels. Unlike previously proposed schemes, the solution offers perfect reconstruction while producing shares with size smaller than that of the input image. The maximum distance separable (MDS) code principle used in the design allows for the introduction of a flexible framework that compares favorably to competing solutions as it can be seen by examing the experimental results included in this paper.

Index Terms— Visual cryptography, MDS code, generator matrix, pixel expansion

1. INTRODUCTION

Security of visual data is an important issue in the design of communication systems. Data hiding techniques and visual cryptography are used to introduce confidentiality and security when visual data are transmitted through unsecured communication channels. Data hiding techniques try to embed data in digital media and transmit it in an imperceptible way. On the other hand, in visual cryptography or visual secret sharing (vss), the original input image is shared between a set of participants P by a dealer (secret image holder) [1]. Based on the sharing policy, only qualified subsets of participants can recover the original input image. Two important factors that used to determine the efficiency of any visual cryptography scheme, namely: 1) the quality of the reconstructed image and 2) the pixel expansion (m). Any loss of information during the reconstruction phase leads to reduction in the quality of the recovered image. On the other hand pixel expansion refers to the number of subpixels in the generated shares that represents a pixel of the original input image. For bandwidth constrained communication channels it is desirable to keep m as small as possible. For color images, reducing pixel expansion is of paramount importance since they occupy more space and consume more bandwidth compared to grayscale and binary images. Most of the previous works in this area try to optimize pixel expansion or obtain perfect reconstruction. The proposed scheme in [2] can perfectly recover the original input image for a given set of c colors but it generates shares with dimensions larger than the dimensions of the original input. Improving the algorithm of [3] is the subject of [4]. The authors enhance the quality of the reconstructed image but still the shares are larger in size compared to the input size. The scheme introduced in [5] is an attempt to improve the pixel expansion characteristics of the solutions presented in [6] and [7]. The bit level based visual cryptography scheme for color images was firstly introduced in [8]. The authors in [8] proposed reciprocal encryption and decryption functions that operate directly on the bit plane of the RGB representation of a color image. Their proposed scheme can perfectly recover the original input image but it expands the shares using an expansion factor of $m = 4$. All the above schemes share a common characteristic, namely they operate on the original input image at the pixel level. However, there are proposed solutions that operate on a group of pixels rather than a single pixel. In [9] a polynomial secret sharing solution is used to share pixels of the input image. The secret sharing method of [9] utilizes the pixel values of a group of k pixels to develop a $\{k, n\}$ visual secret sharing scheme thus reducing the pixel expansion factor to $(\frac{1}{k})$. However performing Lagrange interpolation in a finite field with 251 elements (F_{251}) leads to visual quality losses in the reconstructed input image. To perfectly recover the original input image a share size expansion factor should be introduced. The complexity of our proposed method is smaller than that of [9] since a matrix inversion is used instead of Lagrannge interpolation.

The rest of this paper is organized as follows. Section 2 describes the development of the proposed algorithm based on MDS codes. Motivations and design characteristics are discussed in detail. The proposed scheme is compared against some previously proposed solutions. Experimental results reported in section 3 while conclusions are drawn in section 4.

2. PROPOSED METHOD

The goal is to securely sharing a color image S of dimension $(K_1 \times K_2)$. A $(K_1 \times K_2)$ color image S is usually represented in RGB space as $S : Z^2 \rightarrow Z^3$ where each color pixel is represented using 24 bits according to the formula:

$$S_{(i,j)} = [s_{(i,j)1}, s_{(i,j)2}, s_{(i,j)3}] \quad (1)$$

where (i, j) $(1 \leq i \leq K_1$ and $1 \leq j \leq K_2)$ and $c = 1, 2$ and 3 are the spatial position and color channels, respectively. In this paper we denote the color image S as $[S_1, S_2, S_3]$ where $S_c = [s_{(i,j)c}]$ $1 \leq c \leq 3$, $1 \leq i \leq K_1$ and $1 \leq j \leq K_2$ is the matrix constructed by $s_{(i,j)c}$. The proposed scheme operates separately on each S_c. Without loss of generality, we describe the proposed scheme only for one of the c components of the secret image S, which we denote in the rest of the paper as $\mathbb{S}$; $\mathbb{S} \in \{S_1, S_2, S_3\}$.

2.1. Permutation

In order to reduce the correlation of neighboring pixels and increase the security of the proposed scheme we permute the elements of $\mathbb{S}$ prior to any other operation. Let P_i be a $(i \times i)$ permutation matrix which contains only one 1 in each row and column with the rest of the row elements being zeros. The permutation on $\mathbb{S}$ is performed using two matrices P_{K_1} and P_{K_2} such that

$$\mathbb{S}_p = (P_{K_1} \times \mathbb{S}) \times P_{K_2} \tag{2}$$

where $\mathbb{S}_p$ is the permutated version of $\mathbb{S}$. As it can be seen P_{K_1} and P_{K_2} are applied to permute the rows and columns of $\mathbb{S}$, respectively. When secret sharing schemes are used to protect visual data transmitted through communication channels, the permutation matrices should be sent prior to the transmission of the produced secret shares. It should be noted at this point that the permutation matrices can be compressed greatly due to their structure (i.e. using lossless compression) without affecting the overall performance. Suppose that a permutation matrix of dimension $(K_1 \times K_1)$ P_{K_1} should be compressed. Without compression K_1^2 bits are need to be sent. Since each row of P_{K_1} contains only one 1 element, to transmit this matrix knowing this position which is h $(1 \leq h \leq K_1)$ is enough. As a result for transmission of this permutation matrix at most $K_1 \lceil \log_2 K_1 \rceil$ bits are needed. This amount of overhead is small compared to the RGB representation of the original input image. For example for the transmission of a given 512×512 color image the number of required bits is $512 \times 512 \times 24$ and the number of required bits for transmitting the compressed version of permutation matrix is at most $512 \times \log_2 512$, which is approximately less than 0.001 of the color image information. It should also be noted that the permutation matrices need not be accessed by its participant independently, because it would allow each participant to independently detect information beyond to his/her share. Thus, after compression the compressed bits of the permutation matrices are shared using the bit level based $\{k, n\}$ secret sharing scheme proposed in [8]. Since scheme in [8] perfectly recover the original input secret, it can be utilized to securely transmit the needed permutation matrices through the communication channel.

2.2. Proposed Scheme

On the encryption side (dealer side) the following algorithm is applied to $\mathbb{S}_p$ to generate n shares of n participants. At first,

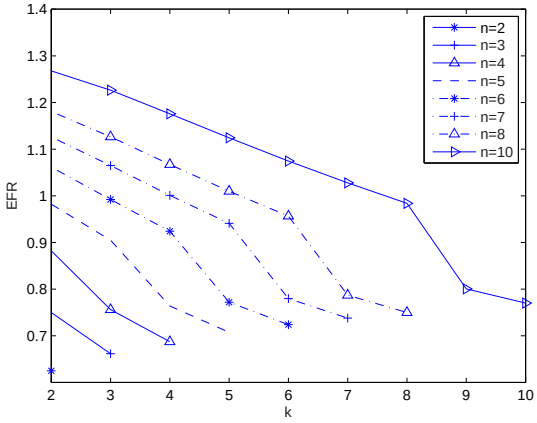

Fig. 1. Comparison of compression rates of our proposed method proposed in [10]. n is the number of participants.

matrix $\mathbb{S}_p$ is reshaped to a new matrix of dimension $\lceil \frac{K_1 K_2}{k} \rceil \times k$. We denote this new matrix afterwards by $\mathbb{S}_p^*$. This matrix is used in the next step to generate the shares. $\mathbb{S}_p^*$ is set up as follows:

$$\begin{cases} \mathbb{S}_p^*(i,j) = \mathbb{S}_p(\gamma, \delta) & \text{for } \begin{cases} 1 \leq j \leq k \\ 1 \leq i \leq \lfloor \frac{K_1 K_2}{k} \rfloor \end{cases} \\ \gamma = (k(i-1) + j - 1)\, div\, K_2 \\ \delta = (k(i-1) + j)\, mod\, K_2 \\ \\ \mathbb{S}_p^*(i,j) = r & \text{for } \begin{cases} j = k \\ \\ i = \lfloor \frac{K_1 K_2}{k} \rfloor + 1 \end{cases} \end{cases}$$

where r is an arbitrary random natural number less than 256 chosen by the dealer and div denotes *integer division* operation; for instance $(7\, div\, 3 = 2)$. The next step is to build up the *Associated matrix*$(\mathbb{A})$. As we will see in the following, values of elements of this matrix will generate the shares of participants. $(\mathbb{A})$ is defined as follows:

$$\mathbb{A} = \mathbb{S}_p^* \times G \tag{3}$$

$\mathbb{A}$ is a matrix of dimension $\lceil \frac{K_1 K_2}{k} \rceil \times n$ and G is the generator matrix of MDS code $[n,\ k,\ n-k+1]$ over $GF(q)$, where

$$q = \begin{cases} 2 & \text{if } n - 1 \leq k \leq n \\ n - 1 & \text{otherwise} \end{cases} \tag{4}$$

To produce the shares we use the columns of two matrices $\mathbb{A}_{mod}$ and $\mathbb{A}_{div}$ which are defined below:

$$\mathbb{A}_{mod} = \mathbb{A}\, mod\, 256 \quad \mathbb{A}_{div} = \mathbb{A}\, div\, 256 \tag{5}$$

Shares of i^{th} participant $(1 \leq i \leq n)$ are $\mathbb{A}_{mod}(c_i)$ and $\mathbb{A}_{div}(c_i)$ i.e. i^{th} column of both matrices $\mathbb{A}_{mod}$ and $\mathbb{A}_{mod}$.

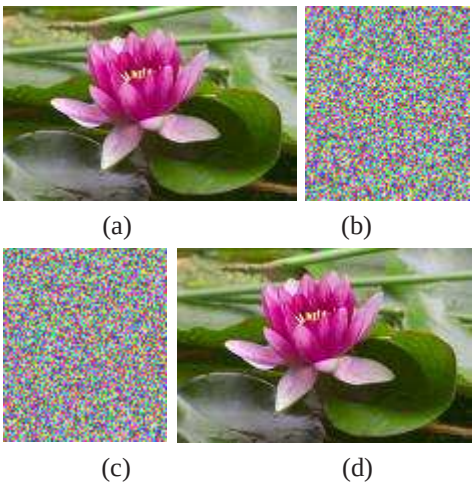

Fig. 2. The proposed method (tested for a color image) $\{2, 2\}$: (a) Original image (b) Share 1 (c) Share 2 (d) Reconstructed image

To recover the secret image every group of k or more participants can recover the secret image. Suppose participants $i_1, \ldots, i_k$ where $\{i_1, \ldots, i_k\} \subset \{1, \ldots, n\}$ are gathered. Without loss of generality we assume $i_1 \leq i_2 \leq \ldots \leq i_k$. Therefore, for $i_1 \leq j \leq i_k$ $\mathbb{A}_{div}(c_j)$ and $\mathbb{A}_{mod}(c_j)$ are readily available. From (5) the columns $i_1, \ldots, i_k$ of matrix $\mathbb{A}$ can be calculated as follows: $\mathbb{A}(c_j) = 256\mathbb{A}_{div}(c_j) + \mathbb{A}_{mod}(c_j)$ where $i_1 \leq j \leq i_k$. From (3), $\mathbb{S}_p^*$ can be obtained:

$$\mathbb{S}_p^* = \mathbb{A}(c_{i_1}, \ldots, c_{i_t}, \ldots, c_{i_k}) \times (G(c_{i_1}, \ldots, c_{i_t}, \ldots, c_{i_k}))^{-1} \quad (6)$$

where $1 \leq t \leq k$. Please note that the second term of the right side of (6) is the inverse of a matrix composed of the columns $c_{i_1}, \ldots, c_{i_k}$ of G. Since the rank of G is k, the inverse of the above matrix always exists since $G(c_{i_1}, \ldots, c_{i_k})$ is full rank for any sequence of $i_1, \ldots, i_k \leq n$. Any subset of participants with $k-1$ or less elements can not gain any information about the secret input image because the inverse of the matrix in equation (6) does not exist. After determining $\mathbb{S}_p^*$, $\mathbb{S}_p$ for $1 \leq i \leq K_1$ and $1 \leq j \leq K_2$ can be computed as follows:

$$\mathbb{S}_p(i,j) = \mathbb{S}_p^*\Big(((K_2(i-1)+j-1)\, div\, k)+1, ((K_2(i-1)+j)\, mod\, k)\Big)$$

Finally after recovering the permutation matrices according to [8], from (2) the input image is reconstructed as follows: $\mathbb{S} = P_{K_1}^{-1} \times (\mathbb{S}_p \times P_{K_2}^{-1})$ Note that matrices P_{K_1} and P_{K_2} are full rank and therefore their inverse always exist. Using the proposed method the secret image can be *perfectly* reconstructed in the presence of at least k participants, therefore the proposed method is an information *lossless* scheme.

As it was previously mentioned, one of the important measures for the efficiency of any visual cryptography scheme is the expansion factor m. Schemes with small m are good candidates for solutions used to secure transmission over limited bandwidth communication networks. The properties of the MDS generator matrices are used in order to calculate the expansion factor of the proposed visual secret sharing scheme here. From equation (4), the number of bits required to represent $\mathbb{A}_{mod}$ and $\mathbb{A}_{div}$ when $1 \leq k \leq n-2$, can be calculated as follows:

$$(8 + \log_2 k(n-2))\lceil \frac{K_1 K_2}{k} \rceil$$

Therefore

$$\begin{aligned} m &= \frac{(8 + \log_2 k(n-2))\lceil \frac{K_1K_2}{k} \rceil}{8K_1K_2} \\ &\leq \frac{(8 + \log_2 k(n-2))(\frac{K_1K_2}{k} + 1)}{8K_1K_2} \\ &= \frac{1}{k} + \frac{(8 + \log_2 k(n-2))}{8K_1K_2} + \frac{1}{8k}\log_2 k(n-2) \\ &\approx \frac{1}{k} + \frac{1}{8k}\log_2 k(n-2) \end{aligned}$$

Let $m_1 = (8 + \log_2(k))\lceil \frac{K_1K_2}{k} \rceil$. When $n-1 \leq k \leq n$ the corresponding number of required bits is respectively:

$$m = \frac{m_1}{8K_1K_2} \approx \frac{1}{k} + \frac{1}{8k}\log_2(k)$$

For commonly used images (i.e. 512×512) terms with the dimensions $(K_1 \times K_2)$ in the denominator could be neglected.

To comparatively evaluate our proposed scheme, from the point of view of expansion factor m, we choose the algorithm proposed in [10] for comparison. The advantages of the method proposed in [10] are: its small expansion factor, its strong protection of the secret image, and its ability to process image in realtime. For most of practical values for $\{k, n\}$ schemes the expansion factor of our method is less than that of the method in [10]. The image shares in [10] have sizes defined as the $\frac{1}{k} + \frac{1}{n}$ of the secret image size. To compare the expansion factor of our solution (denoted by m) to the expansion factor of the solution in [10], namely $(\frac{1}{k} + \frac{1}{n})$, we define the so-called Expansion Factor Ratio (EFR) as follow: $EFR = m \times (\frac{1}{k} + \frac{1}{n})^{-1}$ and we plot it versus k for a given number of participants n (see Fig. 1)

As it can be understood from Figure 1, for most of practical values of $(k, n), 1 \leq k \leq n \leq 10$ our method has a smaller expansion factor compared to the method in [10]. In [9], the proposed method has the expansion factor of $\frac{1}{k}$. Their method is a lossy scheme which in some cases can not *perfectly* reconstruct the secret image. Our proposed method can *perfectly* reveal the secret image by any subset of participants with k or more elements which outperforms the method of [9] in the cost of increasing the size of each share a little.

3. EXPERIMENTAL RESULTS

Simulation results are introduced in this section to confirm the properties of the proposed scheme. To compare our results from the point of view of perfect reconstruction property and expansion factor, the scheme proposed in [10] is applied on the same input image. In Figure 2 the result of applying our

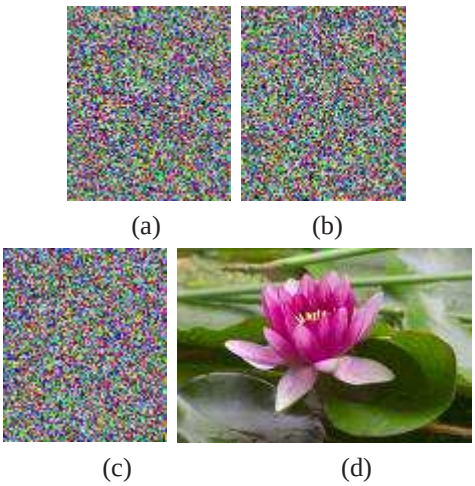

Fig. 3. The proposed method (tested for a color image) $\{2, 3\}$: (a) Share 1 (b) Share 2 (c) Share 3 (d) Reconstructed image by Share 1 and Share 2

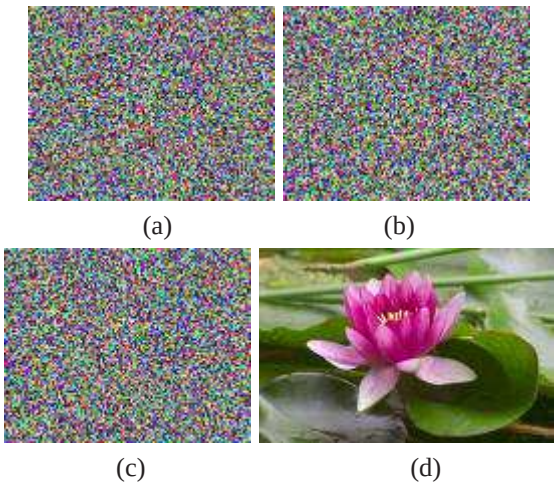

Fig. 4. The proposed method in [10](tested for a color image) $\{2, 3\}$: (a) Share 1 (b) Share 2 (c) Share 3 (d) Reconstructed image using Share 1 and Share 2

solution on the input image (Fig. 2a) is depicted. The size of the generated shares in Fig. 2b-2c is approximately $\frac{1}{2} + \frac{1}{16} = \frac{9}{16}$ of the original input size. As it can be visually seen in Fig. 2d the original input image can be perfectly recovered. Fig. 3 and Fig. 4 show the result of comparison of our method and the proposed method in [10]. In both cases the original input image is Fig. 2a. In Fig. 3 the size of the noise like generated shares is $\frac{1}{2} + \frac{1}{16} = \frac{9}{16}$ of the original input image. The size of the generated shares in Fig. 4 is $\frac{1}{2} + \frac{1}{3} = \frac{5}{6}$ of the original input image which is larger than our pixel expansion factor. It can be concluded that our proposed scheme is a cost effective scheme for bandwidth constraint applications. It should be noted that in both Fig. 3 and Fig. 4 the input image is perfectly recovered.

4. CONCLOUSION

A $\{k, n\}$ visual secret sharing scheme based on MDS codes is presented in this paper. The advantages of the proposed method are its small pixel expansion and its capability of perfect reconstruct of the secret image. Our method is compared to some well known previously methods and it is shown to outperforms these schemes in practical application scenarios. Applying permutation before share generation, the secrecy of the proposed solution is enhanced. The proposed method can be considered a good candidate for securing visual data transmitted in systems with limited bandwidth.

5. REFERENCES

[1] M. Naor and A. Shamir, *Visual Cryptography*, Springer, 1994.

[2] S. Cimato et al, "Colored visual cryptography without color darkening," *Proc. 4th Conf. Security in Communication Networks*, pp. 8–10, 2004.

[3] W.G. Tzeng and C.M. Hu, "A New Approach for Visual Cryptography," *Designs, Codes and Cryptography*, vol. 27, no. 3, pp. 207–227, 2002.

[4] C. Blundo et al, "Visual cryptography schemes with optimal pixel expansion," *Theoretical Computer Science*, vol. 369, no. 1-3, pp. 169–182, 2006.

[5] S.J. Shyu, "Efficient visual secret sharing scheme for color images," *Pattern Recognition*, vol. 39, no. 5, pp. 866–880, 2006.

[6] C.N. Yang and C.S. Laih, "New Colored Visual Secret Sharing Schemes," *Designs, Codes and Cryptography*, vol. 20, no. 3, pp. 325–336, 2000.

[7] C. Blundo et al, "Improved Schemes for Visual Cryptography," *Designs, Codes and Cryptography*, vol. 24, no. 3, pp. 255–278, 2001.

[8] R. Lukac and K.N. Plataniotis, "Bit-level based secret sharing for image encryption," *Pattern recognition*, vol. 38, no. 5, pp. 767–772, 2005.

[9] C.C. Thien and J.C. Lin, "Secret image sharing," *Computers & Graphics*, vol. 26, no. 5, pp. 765–770, 2002.

[10] L. Bai, "A Reliable (k, n) Image Secret Sharing Scheme," *Dependable, Autonomic and Secure Computing, 2nd IEEE International Symposium on*, pp. 31–36, 2006.