A reversible visual cryptography technique for color images using Galois field arithmetic.

Rajesh Kumar N1*, Manikandan G2, Bala Krishnan R1, Raajan NR3, Sairam N2

1Department of Computer Science and Engineering, Srinivasa Ramanujan Centre, SASTRA University, India
2School of Computing, SASTRA University, India
3School of Electrical and Electronic Engineering, SASTRA University, India

Abstract

Nowadays, the most important study to provide confidentiality is digital image encryption. More and more proposals have been committed to inquire about Visual Secret Sharing (VSS) techniques. Traditional scheme was mainly focused on binary images and later investigations were extended to grayscale and color images. Visual cryptography encodes the secret information into n shares and distribute among of group of participants. Qualified participants can reconstruct the original image by superimposing the collected share images. Regrettably, the previous schemes still have weakness during the construction of secret shares and reconstruction on secret image. In this paper we present a reversible visual cryptography technique for color images using Galois field theory. A secret image is split up into two sub images and shared by the cover image to construct the stego images. Additionally Galois field theory is applied to construct brother stego images for effective transmission. Individual stego and brother stego images reveal nothing. The Galois field inverse operation of exponential is employed to reveal the secret image and pair of pixels in the brother stego images reveals cover images.

Keywords: Visual cryptography, Cover image, Stego image, Galois field arithmetic.

Accepted on September 22, 2016

Introduction

The evolution of network computing infrastructure, digital distribution of information Communication is more convenient around the world. Data communication can be made through either wired or wireless channels to the destination. However, data transmission over network makes the indefensible against network hackers. Therefore the protection of various medium of information becomes more crucial problem in the contemporary days. Usually, the human optic system can understand the data formats, like digital images, graphics, animations, video and text. The contents are transmitted over the network using controversial cryptography, steganography and watermarking techniques. However the encryption standards are more complicated and still have the weakness to transmit and receive the multimedia content safely.

Instead of transmitting the encryption resultant unreadable data format, the two famous cryptographer’s Shamir and Naor introduced a new cryptographic scheme called “Visual Cryptography”. In this scheme a secret image is concealed into two or more share images and distributed among group of persons. Only the sufficient number of persons with shadow images could stack the transparencies to reconstruct the secret image. Early visual investigations were attempted to protect the binary secret contents. Later (k, n)-threshold visual cryptography is proposed for binary images. By the concept of VSS [1] binary image is encrypted into n number of unintelligible sub images called shadow images. Human visual system can reveal the secret part by collecting and overlapping the k or more shadow images. Any k-1 or less than threshold value containing secret shares reveals no information about the original content. Based on the ground breaker’s VSS [2,3] scheme, many research works can be carried out by the scientists and researchers. Their investigations led to the foundation for bounds, contrast, pixel expansion [4-6], multiple sharing for gray and color image based visual secret sharing schemes. By the way conventional cryptosystem’s alternative approach “Visual Cryptography” is efficient, but weakness still exists. Unsatisfied recovery of secret image with distorted cover images, meaningless secret shares, large size of secret shares during the construction, high computational cost were the major issues of traditional and extended visual secret sharing schemes.

This paper presents a reversible visual cryptography technique for color images with high visual quality. Finite field application GF (2^8) based visual secret sharing provides a high level security on image sharing scheme. According to the reversible technique, cover image also recovered successfully.
The rest of the investigation is organized as follows. Previous inquiries of visual cryptography are presented in Section 2. In Section 3, the proposed Galois field based reversible visual cryptography scheme for color image is explained. The experimental results are illustrated in Section 4. The conclusion of the visual technique and future directions are presented in Section 5.

**Literature Survey**

In 1994, two Israel scientists investigated Naor et al. [7] traditional visual crypto system distinguished the darkness from whiteness to achieve the concept of secret sharing. The pixel intensities of binary image are converted into image matrix and each pixel value is divided into set of m white and black sub pixels to construct share images. After these shares were printed in closeness to one another, mortal visual perception can view the secret content by stacking.

![Figure 1. Traditional visual cryptography codebook.](image)

Binary image based (k, n) visual crypto system was introduced and constructed collection of M × N Boolean matrices $C_0$ and $C_1$. The codebook is depicted in Figure 1. A refined (r, n)-threshold based Secret Image Sharing (SIS) proposed by Thien et al. [8]. The dimension of each divies is reduced by the ratio $1/r$ of that secret image. With the reduction format of secret shares are effectively stored and transmitted over the communication channels. Followed by the invention of threshold scheme, some visual secret sharing [9-12] methods have been suggested to make a reduction in dimension of the secret shares.

In 2003 three color visual cryptography proposed by Hou [13]. In this color visual scheme, a color secret image was decomposed into three separate channels like cyan, magenta and yellow respectively. After decomposing the color channels are transmitted in the form of halftone images by using halftone techniques. Finally, collect the halftone shares to reconstruct the secret color images. Additionally, five colors [14,15] have been used for color image display: black, red, green, blue and white.

In 2009, Leung et al. and Jen et al. [16,17], analysed the Hou’s color visual scheme and extended the previous approach for color images with detailed security analysis to attain the goal of visual cryptography. Further, they extended the color model implementation, Chaumont et al. [18], suggested meaningful visual cryptography method concealing secret information. The reduced format color rendering algorithm indicates the color image is embedded in the given range of colors.

**Galois field arithmetic**

In our scheme, the generation of stego images is performed by the concept of finite field theory. The polynomial construction of Galois Field GF $(2^p)$ is denoted in Equation 1.

$$\{a_{n-1}x^{n-1}+a_{n-2}x^{n-2}+\ldots+a_1x^1+a_0 \mid a_i \in \{0, 1\}, \ i=0, 1, \ldots n-1\} \rightarrow \text{(1)}$$

In Finite Field, the elements are constructed based on the polynomials. It takes two input arguments such as, prime number $p$ and an integer value $n>1$. After the computation, the field gives $p^n$ elements. For example, different kind of finite field construction schemes are listed based on the input elements.

1. Galois field $(2)$ with two elements, $\{0,1\}$
2. Galois field $(5)$ with five elements, $\{0, 1, 2, 3, 4\}$

The extension of these input elements provides irreducible formats such as Galois field $(2^3)$, $(2^4)$ and $(2^8)$ [19,20].

The main operations of finite fields are Galois field addition, subtraction, logarithms and exponentials. Based on the arithmetic operations, several mathematical methods had suggested solving the difficulty of image protection problem.

**Proposed System**

This nominated visual cryptography practical method composed of two algorithms; such as Galois field based visual secret sharing and retrieving algorithms. The summary of our nominated work is exhibited in Figure 2. First, the proposed visual cryptographic technique expands the confidential image into sub images by pixel division method. After the sub images are shared by the cover image and converted into meaningful stego images. Then, Galois field arithmetic operations are applied on the stego images to heighten the security of the stego images. Now, brother-stego images are dispatched to the participant to make the secure image transmission.

To reconstruct the secret image, the participant can collect all the brother-stego images and apply the exponential inverse of the Galois field theory and extract the pixels from stego images.
to revert the secret image. This nominated work also recovers cover images successfully without the loss of any information. The process of visual secret sharing and recovering procedure is described in Tables 1 and 2.

**Table 1. Secret sharing process for color images.**

<table>
<thead>
<tr>
<th>Input: Secret image I, cover image C with same size</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Output</strong>: Stego images with size of m × n</td>
</tr>
<tr>
<td>1: Check the secret image I is color or not;</td>
</tr>
<tr>
<td>2: If (I=color image) then</td>
</tr>
<tr>
<td>Decompose color image to gray channels;</td>
</tr>
<tr>
<td>G=I(:, :, 1) and I(:, :, 2) and I(:, :, 3)</td>
</tr>
<tr>
<td>else</td>
</tr>
<tr>
<td>G=I;</td>
</tr>
<tr>
<td>3: Divide the secret image pixels into sub pixels to generate the sub images.</td>
</tr>
<tr>
<td>4: Create Galois field array GF (2 ^ 8)</td>
</tr>
<tr>
<td>5: Take the cover image to share the pixels of Sub images and construct stego images.</td>
</tr>
<tr>
<td>6: At the end apply the Galois field theory to construct the meaningful brother-stego images</td>
</tr>
<tr>
<td>7: disp (brother-stego images) S</td>
</tr>
</tbody>
</table>

**Table 2. Reconstruction process.**

1: Procedure: Collect the number brother-stego images
2: Initialize stego_count, recon=0;
3: Cover=(Upper_stego+Lower_stego)/2;
4: for i=1:stego_count
   if S_i=Upper_stego then
     Sub_image (i)=Upper_stego-Cover;
   else
     Sub_image (i)=Cover -Lower_stego;
   End If
End for
5: Stack=add (Sub_image 1, Sub_image 2);
6: Recon=cat (3, stack, I_2, I_3);
6: Display reconstructed color image.
7: End procedure.

**Experimental Results**

We present the obtained experimental observations to estimate the performance of our nominated visual cryptography scheme. We have implemented the proposed work in Matlab 7.7 environment with Intel core i3-3110M CPU, 2.40 GHZ, 2 GB memory, 5000 GB hard-disk capacity, and the operating system is Microsoft Windows 8.

In addition, Table 3 provides the image quality parameters such as Means Squared Error (MSE) and Peak Signal to Noise Ratio (PSNR) which has computed between the original images and recovered images. Furthermore cover image is also recovered successfully without any loss of pixel information. The comparison of PSNR value is also demonstrated in Figure 3.

**Table 3. PSNR values for secret images and recovered images.**

<table>
<thead>
<tr>
<th>Secret</th>
<th>Type</th>
<th>Size</th>
<th>MSE</th>
<th>PSNR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backbone</td>
<td>.bmp</td>
<td>128 × 128</td>
<td>2.29</td>
<td>44.57</td>
</tr>
<tr>
<td>Avion</td>
<td>.bmp</td>
<td>128 × 128</td>
<td>6.92</td>
<td>39.76</td>
</tr>
<tr>
<td>Lenna</td>
<td>.tif</td>
<td>256 × 256</td>
<td>3.38</td>
<td>42.88</td>
</tr>
<tr>
<td>Baboon</td>
<td>.tif</td>
<td>256 × 256</td>
<td>2.99</td>
<td>43.41</td>
</tr>
</tbody>
</table>

The implementation results of nominated visual cryptography technique for color images are illustrated in Figure 4. The color secret image and the corresponding cover image are shown in Figures 4a, 4b, 4g and 4h. Galois field exponential operation on stego images are shown in Figures 4c, 4d, 4i and 4j. At the end the reconstructed result of brother stego images are shown in Figures 4e, 4f, 4k and 4l.

**Figure 4. (a-l) Secret image, cover image, brother-stego images and recovered images.**

**Conclusion**

An emerging research topic in the discipline of visual secret sharing is reconstruction of confidential image with high visual tone and also the recovery of cover images without content loss. Reversible visual cryptographic technique for color images using Galois field theory has nominated for efficient image transmission. This scheme overcomes the previous grayscale image based VSS techniques. A secret color image is converted to grayscale image and split into sub images. A cover image is used to shares the sub images and applies Galois field theory to enhance the high level security. Finally, the experimental results measure the quality of reconstructed secret image. A comparison of PSNR values are also presented.
to show the visual quality of secret image. This cryptosystem can be extended to construct more number of shadow images and participants in future.

References

*Correspondence to
Rajesh Kumar N
Department of Computer Science and Engineering
Srinivasa Ramanujan Centre
SASTRA University
India