Biomedical Research 2017; 28 (5): 2036-2039 *ISSN 0970-938X*
www.biomedres.info

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

Rajesh Kumar N[1*], Manikandan G[2], Bala Krishnan R[1], Raajan NR[3], Sairam N[2]

[1]Department of Computer Science and Engineering, Srinivasa Ramanujan Centre, SASTRA University, India

[2]School of Computing, SASTRA University, India

[3]School 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.

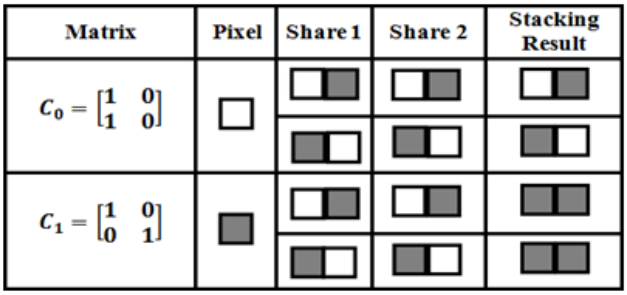

Figure 1. *Traditional visual cryptography codebook.*

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 diwies 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 with more than four colors. By continuing 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^n) is denoted in Equation 1.

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

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.

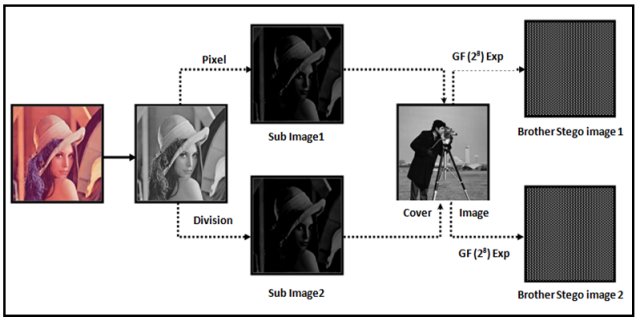

Figure 2. *An overview of proposed color visual secret sharing scheme.*

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.*

Input: Secret image I, cover image C with same size

Output: Stego images with size of m × n

1: Check the secret image I is color or not;

2: If (I=color image) then

Decompose color image to gray channels;

G=I_1(:, :, 1) and I_2(:, :, 2) and I_3(:, :, 3)

else

G=I;

End If;

3: Divide the secret image pixels into sub pixels to generate the sub images.

4: Create Galois field array GF (2 ^ 8)

5: Take the cover image to share the pixels of

Sub images and construct stego images.

6: At the end apply the Galois field theory to

construct the meaningful brother-stego images

7: disp (brother-stego images) S_i

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_iamge 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.

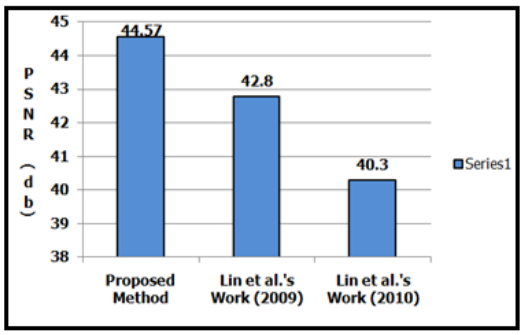

Figure 3. *Comparison of PSNR values between previous schemes.*

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

Secret	Type	Size	MSE	PSNR
Backbone	.bmp	128 × 128	2.29	44.57
Avion	.bmp	128 × 128	6.92	39.76
Lenna	.tif	256 × 256	3.38	42.88
Baboon	.tif	256 × 256	2.99	43.41

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.

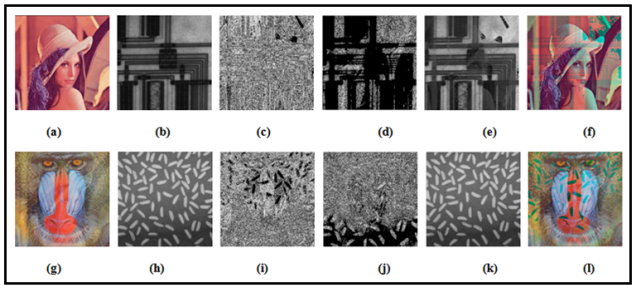

Figure 4. *(a-l) Secret image, cover image, brother-stego images and recovered images.*

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

1. Heinz H, Andreas UHL. Identifying deficits of visual security metrics for images. Sig Proc Imag Commun 2016; 46: 60-75.
2. Mustafa U. Meaningful share generation for increased number of secrets in visual secret-sharing scheme. Math Probl Eng 2010; 2010: 1-18.
3. Mustafa U, Guzin U, Vasif VN. Invertible secret image sharing for gray level and dithered cover images. J Sys Softw 2012; 86: 485-500.
4. Ching C, Lin LHL, Kuo FH, Shih CC. Reversible secret image sharing with high visual quality. Multimedia Tools Appl 2012; 70: 1729-1747.
5. Xiaotian W, Duanhao O, Qiming L, Wei S. A user-friendly secret image sharing with reversible steganography based on cellular automata. J Sys Softw 2012; 85: 1852-1863.
6. Javier H, Alexandre R, German S. New results and applications for multi-secret sharing schemes. Des Codes Cryptogr 2013; 73: 841-864.
7. Naor M, Shamir A. Visual cryptography advances in cryptology. Eurpocrypt Spr Verlag Berlin 1994; 1-12.
8. Chih CT, Ja-Chen L. Secret image sharing. Comp Graph 2002; 5: 765-770.
9. Wei KC. Image sharing method for gray-level images. J Sys Softw 2013; 86: 581-585.
10. Xiaotian W, Wei S. Improving the visual quality of random grid-based visual secret sharing. Sig Proc 2013; 93: 977-995.
11. Li CH, Lin YT, Min SH. A reversible data hiding method by histogram shifting in high quality medical images. J Sys Softw 2013; 86: 716-727.
12. Peng L, Ching NY, Chih CW, Qian K, Yanpeng M. Essential secret image sharing scheme with different importance of shadows. J Vis Commun Imag Represent 2013; 24: 1106-1114.
13. Young CH. Visual cryptography for color images. Pat Recogn 2003; 36: 1619-1629.
14. Hao L, Hua C, Yongheng S, Zhenfei Z, Yanhua Z. Color transfer in visual cryptography. Measur 2014; 51: 81-90.
15. Ales R, Karel S, Otto D, Michal J. A new approach to fully reversible watermarking in medical imaging with breakthrough visibility parameters. Biomed Sig Proc Contr 2016; 29: 44-52.
16. Jen BF, Hsien CW, Chwei ST, Ya FC, Yen PC. Visual secret sharing for multiple secrets. Pat Recogn 2008; 41: 3572-3581.
17. Bert WL, Felix YNG, Duncan SW. On the security of a visual cryptography scheme for color images. Pattern Recogn 2009; 5: 929-940.
18. Chaumont M, Puech W, Lahanier C. Securing color information of an image by concealing the color palette. J Sys Softw 2013; 86: 809-825.
19. Hafid M, Fattehallah G, Mohammed E. Secure watermarking method with smart card. Int J Comp Inform Technol 2013; 5: 874-881.
20. Feng W, Chin CC, Wan LL. The credit card visual authentication scheme based on GF field. Multimed Tools Appl 2015; 24: 11451-11465.

*Correspondence to

Rajesh Kumar N

Department of Computer Science and Engineering

Srinivasa Ramanujan Centre

SASTRA University

India