October 2013

BOOLEAN XOR BASED (K,N) THRESHOLD VISUAL CRYPTOGRAPHY FOR GRAYSCALE IMAGES

RAM KRISHNA JHA

Dept. of Information Technology, BIT Mesra, Ranchi, India, jha751@gmail.com

ABHIJIT MUSTAFI

Dept. of Information Technology, BIT Mesra, Ranchi, India, abhijit@bitmesra.ac.in

Follow this and additional works at: <https://www.interscience.in/ijcsi>

Part of the [Computer Engineering Commons](#), [Information Security Commons](#), and the [Systems and Communications Commons](#)

Recommended Citation

JHA, RAM KRISHNA and MUSTAFI, ABHIJIT (2013) "BOOLEAN XOR BASED (K,N) THRESHOLD VISUAL CRYPTOGRAPHY FOR GRAYSCALE IMAGES," *International Journal of Computer Science and Informatics*: Vol. 3 : Iss. 2 , Article 11.

DOI: 10.47893/IJCSI.2013.1131

Available at: <https://www.interscience.in/ijcsi/vol3/iss2/11>

This Article is brought to you for free and open access by the Interscience Journals at Interscience Research Network. It has been accepted for inclusion in International Journal of Computer Science and Informatics by an authorized editor of Interscience Research Network. For more information, please contact sritampatnaik@gmail.com.

BOOLEAN XOR BASED (K,N) THRESHOLD VISUAL CRYPTOGRAPHY FOR GRAYSCALE IMAGES

RAM KRISHNA JHA¹ & ABHIJIT MUSTAFI²

^{1,2}Dept. of Information Technology, BIT Mesra, Ranchi, India
E-mail : jha751@gmail.com, abhijit@bitmesra.ac.in

Abstract - Secure digital images is very important for today's scenario which combining methods and techniques coming from cryptography and image processing. Visual Cryptography Scheme (VCS) is a new kind of cryptography technique which allows visual information (e.g. printed text, picture etc.) to be encrypted in such a way that decryption can be performed by the human visual system without any complex computation on computers. Here we proposed a Visual Cryptography Scheme based on image division of grey level images for the generation of Secret Shares. In this paper we represent the (k, n) Threshold Visual Cryptography Scheme in which the size of generated Shares as well as Recovered Image have same as the Secret Image rather than other VCS where k is the threshold value. Also we proposed the new technique to generate the Shadow Assignment Matrix with the help of Genetic Algorithm (GA). This Shadow Assignment Matrix helped us to distribute the Temporary shadow to the users according to their occurrence of 1's in a row.

Keywords - Shares; Visual Cryptography; Visual Cryptography Scheme; Temporary shadow; Shadow Assignment Matrix; Threshold; Genetic Algorithm

I. INTRODUCTION

With the rapid development and advancement of Network technology, Digital information is transmitted over the Internet easily. There are various type of confidential digital images are transmitted over the Internet. While using confidential digital images, security issues should be taken into consideration because Intruder may utilize weak link over communication network to steal information that they went. To deal with the security problem of confidential digital images, various image Secret Sharing Schemes [1] have been developed. Visual Cryptography is first Introduced by Moni Naor and Adi Shamir in 1994 [2]. Visual Cryptography is a cryptographic technique which allows Visual information (picture, text etc.) to be encrypted in such a way that the decryption can be done by human visual system without any calculation on computers.

Visual Cryptography scheme eliminates complex computational problem in decryption process and stacking the Secret shares is to be used to getting the Original image. Visual cryptography scheme is a secret sharing technique used for encrypting binary images. It splits a binary image into n shares, and gathering more than k shares can recover the secret. Visual cryptography is a popular solution for image encryption. Using secret sharing concepts, the encryption procedure encrypts a secret image into the so-called shares which are noise-like secure images which can be transmitted or distributed over an untrusted communication channel. The GA is a stochastic global search method that mimics the metaphor of natural Biological evolution. GAs operate on a population of potential solutions

applying the principle of survival of the fittest to produce (hopefully) better and better approximations to a solution. At each generation, a new set of approximations is created by the process of selecting individuals according to their level of fitness in the problem domain and breeding them together using operators borrowed from natural genetics. This process leads to the evolution of populations of individuals that are better suited to their environment than the individuals that they were created from just as in natural adaptation. The main data structures in the Genetic Algorithm toolbox are:

1. Chromosomes
2. Phenotypes
3. Objective function values
4. Fitness values

Phenotypes

The decision variables or phenotypes in the genetic algorithm are obtained by applying some mapping from the chromosome representation into the decision variable space.

II. BASIC MODEL

To encrypt a Secret applying a (2, 2) VC Scheme [2], the original image is divided into two Shares such that each pixel in the original image is replaced with non-overlapping block of two sub-pixels. A white pixel is shared into two identical blocks of sub-pixels. A black pixel shared into two complementary blocks of sub-pixels. To decode the image, stacking both the transparencies will permit the visual recovery of the secret. While creating the shares, if the given pixel p in the original image is white, then the encoder randomly chooses one of the first two columns of Table 1.

If the given pixel p is black, then the encoder randomly chooses one of the second columns of the

Table 1 because both the columns have the equal probability to be chosen. The Key property used to construct Visual Cryptography Schemes for black and white images is the following: - if we stack Shares with black and white pixels, the resulting pixel that our eyes see is black. If at least one of the stacked pixels is black and is white if all stacked pixel are white. This key property does not easily extend to colored pixels. With colored pixels the state of each pixel cannot be represented any more with single bit and the reconstruction operation performed by our eyes is much more complicated than a simple OR.

Table 1. (2, 2) Visual Cryptography Scheme

Pixel
Probability	50%	50%	50%	50%
Share 1
Share 2
Stack 1 & 2

Figure 1 shows the result of basic (2, 2) VC scheme. When the two shares are stacked together, as in Figure 1(d), the black pixels in the Original image remain black and the white pixels become grey. Although some contrast loss occurs, the decoded image can be clearly identified. Since each pixel in the original image is replaced by two sub-pixels in each share, the width of the shares as well as decoded image is twice that of the original image.

ATHI

(a) Binary Image

(b) Share 1

(c) Share 2

(c) Decoded Image

Fig. 1 : Example of (2, 2) Visual Cryptography Scheme

III. PROPOSED SCHEME

Our proposed algorithm is based on Chao and Lin [3] Algorithm. Chao and Lin proposed the algorithm for (k, n) Threshold Visual Cryptography Scheme [4] for greyscale images [5]. Our proposed Scheme Emphasis on generation of Shadow Assignment Matrix. We use the Heuristic approach [6] for generating the Shadow Assignment Matrix by which we assign the temporary shadow to users. For the Heuristic approach we need to define the fitness function is this way:

1. Every row must have only 3 one's and rest will be zero
2. Every column must have only 2 one's and rest will be zero

Our program is implemented using MATLAB, so the Fitness function defined in terms of MATLAB.

Initially, Taking a matrix 'A' 4×6 having the entire element '0'.

A = Zeros (4, 6)

Desire = 2*ones (1, 6)

Sumofcols = sum (A)

Result = abs (sumofcols - desireAns)

Ycols = sum (Result)

Similarly we do for Rows and finally we got the expression for Fitness function.

Fitness function = $\sum (Ycols + Yrows)$

And size of chromosome is 24, Generation limit is 10000, take Selection function as roulette, Mutation function as uniform, Crossover function as double point. The chromosome data structure stores an entire population in a single matrix of size 4 X 6. Initially we are taking the chromosomes like

1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1

IV. RESULT

Our result is based on (3, 4) VCS where 3-out-of-4 is the threshold value and any three shares can be used for the revealing the secret image. In our scheme the original image may have any size and after resizing the original image we got the secret image.

Shadow assignment matrix

$$H = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

Fig. 2 (a) Secret Image

(b) Random Image

(c) XORed Image

(d) Share 1

(d) Share 2

(f) Share3

(g) Share 4

(i) Recovered Image

REFERENCES

- [1] M. Naor and A. Shamir, "Visual cryptography", *Advances in Cryptography: EUROCRYPT'94*, LNCS, vol.950, pp. 1-12, 1995, Springer-Verlag, Berlin
- [2] *International Journal of Computational Intelligence Techniques*, ISSN: 0976-0466 &E- ISSN: 0976-0474 Volume 1, Issue 1, 2010, PP-32-37 by Chandramathi S., Ramesh Kumar R., Suresh R. and Harish S.
- [3] K. Y. Chao and J. C. Lin. Secret image sharing: Boolean-operations based approach combining benefit of polynomial-based and fast approaches. *International Journal of Pattern Recognition and Artificial Intelligence*, 23(2):263-285, 2009.
- [4] International Conference on Advanced Computer Control in Singapore, 22- 24 Jan, 2009 by Debasish Jena, Sanjay Kumar Jena Centre of IT Education, Biju Pattanaik University of Technology, Orissa, India.
- [5] C. Blundo, A. De Santis, and M. Naor, "Visual cryptography for grey level images," *Inf. Process Lett.*, vol. 75, pp. 255-259, 2000.
- [6] L. Booker, "Improving search in genetic algorithms," In *Genetic Algorithms and Simulated Annealing*, L. Davis (Ed.), pp. 61-73, Morgan Kaufmann Publishers, 1987