ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING

National Conference on Advanced Innovation in Engineering and Technology (NCAIET-2015)

Alva's Institute of Engineering and Technology, Moodbidri

Vol. 3, Special Issue 1, April 2015

Enhancement of Security in Visual Cryptography System using Genetic Algorithm

Anisha Maria Coelho Prabhu[1], **Pradyumna G. R.**[2]

P.G. Student, Department of Electronics and Communication Engineering, N.M.A.M.I.T, Nitte, India[1]

Assistant Professor, Department of Electronics and Communication Engineering, N.M.A.M.I.T, Nitte, India[2]

Abstract: Visual Cryptography (VC) is a special type of encryption technique where an image or document is encrypted by breaking it down into shares. These shares are then printed on transparencies. Decryption is done by superimposing the shares. Thus one can visually decode the secret image without computation. However, this property makes VC insecure as a third party can easily retrieve the secret information if he obtains the transparencies. VC can be made more secure by encrypting the shares using Genetic Algorithm. Overlapping these encrypted shares reveals no information about the secret image, increasing the security of the VC scheme.

Keywords: Visual Cryptography (VC).

I. INTRODUCTION

The Internet has greatly changed humanity's way of life. Information and data are being transmitted over the internet more than ever before due to the availability and efficiency of computer networks for communication. Distortion free transmission, compact storage and easy editing along with the various facilities being available for storing, transmitting and accessing the data has increased the amount of information being stored and transmitted over the internet. Humans are dependent on computer systems and networks more than ever before. This dependency has brought many threats to information security. The computer attacks and break-ins are increasing. Hence, there is a great need to handle information in a secure and reliable way.

Secret sharing is a good solution to this problem. Secret sharing or secret splitting refers to a method for distributing a secret among a group of participants, each of whom is allocated a share of the secret. The secret is reconstructed only when all or a sufficient number of shares are combined together. No information is conveyed by individual shares. Thus, intruders need to obtain the sufficient amount of shares to retrieve the information or destroy all the shares if they are seeking to destroy the information.

Visual Cryptography (VC) is a special type of encryption technique where the decryption is done by the Human Visual System (HVS) without any computation. This technique was proposed by Naor and Shamir [1] in 1994. According to them VC is a scheme where a secret image is broken down into *n* shares and printed on transparencies. Only when *n* transparencies were stacked one above the other the secret was revealed, while any *n*-1 shares revealed no information about the original image. Here, there is no need for any complicated computations in order to get back the image, rather it is just done by superimposing the shares.

Since one can visually decode the secret image without computation, VC isn't secure as a third person can easily retrieve the secret image if he obtains the transparencies or if the shares are passing in sequence over the network. Thus, there is a need to secure the shares before sending them over a network or printing them. Various researches have been carried out to improve the security of the VC shares and to prevent unauthorized use of information:

Yan-yan *et al*. [2] first generated shares using VC. These shares were then embedded into meaningful pictures or cover images using watermarking technique. On the receiving end the shares were extracted from the cover images and were overlapped to reveal the secret image. Since the shares are watermarked they can escape notice as they won't be visible on the cover image and also since the cover images are meaningful pictures. Although, use of cover images to hide the shares will require extra memory space.

Liu *et al.* [3] suggested a scheme which shared a colour secret image over (*n*-1) arbitrary natural images and one noise-like share image. Feature extraction was carried out on the (*n*-1) natural images and then bitwise XOR was performed on the (*n*-1) feature images and the secret image to obtain (*n*-1) share images and one noise-like image. Upon reception of the *n* sharing images, decryption end separately extracted feature image from the natural sharing images. Then the (*n*-1) feature images and received noise-like share image was decrypted to obtain the secret image. This approach effectively reduced the transmission risk and made it possible to recover secret images without any distortion. However, the use of (*n*-1) natural images increases storage and bandwidth requirement.

Chen *et al.* [4] implemented an Extended Visual Cryptography Scheme with multiple secrets hidden.

DOI 10.17148/IJIREEICE

Meaningful shares were generated by utilizing the principle of contrast and multiple secret images were hidden by changing the overlapping angle of the shares. Four images were selected, where, two were cover images and the other two were secret images. The first secret image was revealed by overlapping shares Sh1 and Sh2 and the second one was revealed by overlapping $\mathrm{Sh1}^T$ and Sh2. The proposed scheme has a high security level as the two shares are meaningful images and they indicate no secret information is hidden. The poor visual quality of recovered images is its major drawback.

It has thus been observed that VC does not secure the shares. The schemes that used cover images to carry the secret information resulted in overload to the network and required extra storage space. Yet, in other techniques the quality of recovered images was very poor. All these limitations led to finding an alternate way to enhance the security of VC.

This paper aims at securing the VC shares using Genetic Algorithm (GA).

II. VISUAL CRYPTOGRAPHY

VC is a special type of encryption method where the decryption is done by the HVS, the eyes. No complex computation is required for the decryption as it is done by the eyes. VC was introduced by Naor and Shamir in 1994 [1]. It is a type of secret sharing scheme used for the encryption of images. Secret sharing is a method where a secret can be distributed among a group of participants, where each participant only gets a share of the secret. These individual shares reveal no information; but when all shares are combined together, the secret can be reconstructed.

k-out-of-*n* or (*k*,*n*) is a general scheme of VC, where *k* is the threshold and *n* is the number of shares. Here, a secret image is cryptographically encoded into *n* random shares. These *n* shares are meaningless images that are then printed on transparencies and can be distributed among *n* participants. No participant has any knowledge about another's share. Also, as the shares are randomly generated, one participant cannot predict any other share. Any *k* or more participants can reconstruct the secret image by superimposing the *k* transparencies together. *k-1* or fewer participants cannot gain any information about the secret, despite having infinite computational power. If *k*=*n*, i.e., *n*-out-of-*n* scheme, all shares are needed to successfully reconstruct the secret.

A. (2,2) VC Scheme (2 sub-pixels)

The simplest VC scheme is the (2,2) visual threshold scheme, where for every pixel *p* in the secret binary image, a pair of black and white sub-pixels are generated in each of the two share images. If *p* is black, one of the two columns under the black pixel in Fig. 1 is selected. If *p* is white, one of the two columns under the white pixel is selected. The column is randomly selected and each column has 0.5 probability of being chosen. Then, the first pair of sub-pixels in the selected column is assigned to share 1 and the second pair of sub-pixels in the column is assigned to share 2. Irrespective of whether a pixel is black or white, the pixel *p* is encoded into a black-white or white-black pair of sub-pixels. Thus an individual share gives no clues as to whether the pixel *p* is black or white. Also, as each pixel is independently encoded, a group of pixels can reveal no information about *p*. The superposition of the two shares is as shown in the last row of Fig. 1. If the pixel *p* is black, the superimposition yields two black sub-pixels, whereas, one black and one white sub-pixel is obtained if *p* is white, irrespective of the column being chosen during encoding [5], [6].

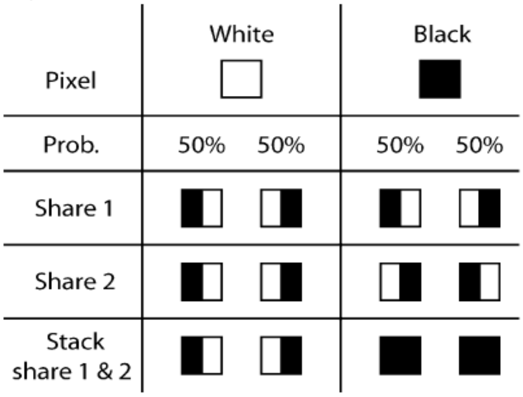


Fig. 1: (2,2) Visual cryptography scheme; a secret pixel is encoded into two sub-pixels in each of the two shares

Mathematically, the white pixel is represented by 1 and the black pixel by 0. For (2,2) VC scheme, the basis matrices S^0 and S^1 are as follows:

$$S^0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad S^1 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}.$$

There are two collection of matrices, C^0 for encoding black pixels and C^1 for encoding white pixels. They are formed by permuting the columns of basis matrices as follows:
C^0 = {Matrices obtained by permuting columns of S^0}
C^1 = {Matrices obtained by permuting columns of S^1}.
That is,

$$C^0 = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\} \text{ and}$$

$$C^1 = \left\{ \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \right\}.$$

To share a black pixel, one of the matrices in C^0 is randomly selected, and to share a white pixel, one of the matrices in C^1 is randomly selected. The first row of the chosen matrix is given to share 1 and the second is given to share 2 [6], [7].

(2,2) VC scheme with two sub-pixels can be illustrated with an example as shown in Fig. 2. The secret image in (a) is encoded into two shares (b) and (c). The secret is retrieved by superimposing the two shares as shown in (d). This decoded image has some contrast loss, however, the secret is easily identified. Since each pixel is encoded into two sub-pixels, the width of the secret image is twice that of the original image. This effect is referred to as *pixel expansion*.

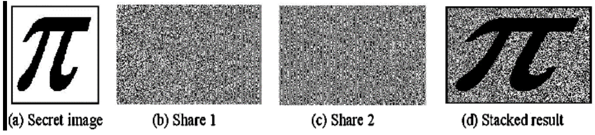


Fig. 2: Example for (2,2) visual cryptography scheme with two sub-pixels

III. GENETIC ALGORITHM

Genetic algorithm is a search technique used to find solutions to optimization and search problems. GA is one the many evolutionary algorithms that use techniques of evolutionary biology such as inheritance, mutation, selection, and crossover, to generate solutions to optimization problems. GAs were invented by John Holland in the 1960s and were developed by Holland and his students and colleagues at the University of Michigan in the 1960s and the 1970s.

A. Description of Algorithm

The algorithm first creates an initial population of possible solutions to the problem and lets them evolve over multiple generations to find better and better solutions. The individuals with a good fitness level are selected as parents, GA operations are performed on them and the new population is generated.

The new population is used in the next iteration of the algorithm. The algorithm terminates when either a maximum number of generations has been produced, or a satisfactory fitness level has been reached for the population [8].

The new population is generated using two main processes:

1) Crossover: Crossover is when vector entries from a pair of individuals in the current population are combined to form a child. Crossover using individuals from current population to create two offsprings who have characteristics of both parents. For example, parent1 is 11101011 and parent2 is 01011010. After crossover the offspring produced are 11111011 and 01001010.

2) Mutation: Mutation is when a child is created by applying random changes to one individual in the current population. An individual may or may not undergo mutation and the points at which it mutates is random. Two individuals before and after mutation are as shown:

Original Offspring1: 01001010
Mutated Offsprng1: 01101011
Original Offspring2: 00010100
Mutated Offsprng2: 01010100 [9].

B. Encryption of Images using GA

Images can be encrypted using GA by modifying the pixel locations using GA operations, such as, crossover and mutations. The image to be encrypted is the initial population. The image is broken down into blocks of pixels, say 1024 pixels. These blocks are the individuals of the population. Since only the locations of the pixels are to be modified, selection is not performed. All individuals are used to create the next generation.

Crossover and mutation can be illustrated using individuals with block size 10. Considering that the image to be encrypted is a binary image, the elements of the individuals are 1s and 0s. The individuals on whom crossover and mutation will be performed are:

A=01110 00101 B=11101 00111.

Crossover is done by switching the last 5 bits of individuals A and B. The offspring C and D obtained after crossover are as shown below:

C=01110 00111 D=11101 00101.

Mutation is applied to individuals C and D by rearranging the order of their bits, in order words, scrambling. The individuals for the next generation, E and F, obtained by mutating C and D are as shown:

E=00011 01111 F=01000 11111.

E and F are individuals of the new generation, which will be used to create the next.

IV. PROPOSED SYSTEM

The proposed scheme, as shown in Fig. 3, first generates shares of the Secret Binary Image using (2,2) VC Scheme. In the next step GA is used to encrypt the generated shares in order to make them more secure and prevent duplication or unauthorized access of information. At the receiving end, the shares are decrypted using GA decryption algorithm and the decrypted shares are stacked together to obtain the secret image. The entire process can be divided into four main phases.

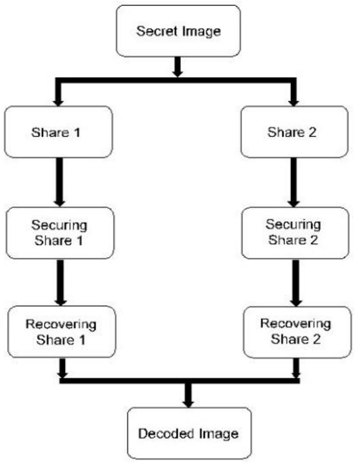


Fig. 3: Methodology or structure of the proposed scheme

DOI 10.17148/IJIREEICE

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

A. PHASE 1 – Generating shares of secret image.

VC Encryption is implemented in this phase. Here (2,2) VC scheme is used generate shares of the secret binary image. Each pixel in the secret image is replaced by four sub-pixels, two sub-pixels in each share. The sub-pixels are randomly chosen with respect to the encoding scheme shown in Fig. 1.

B. PHASE 2 – Encrypting the generated Shares

The second phase deals with encrypting the shares generated in Phase 1 by using GA. First the key for encryption is generated and the shares are encrypted using this key. The output of this stage is the two encrypted shares.

C. PHASE 3 – Decrypting the Shares

This phase takes place at the destination of the secret image. GA decryption is performed on the received shares to obtain the shares in their original form.

D. PHASE 4 - VC decryption

In this phase the secret image is got back by performing VC decryption. The two shares are overlapped by performing AND operation on the decrypted shares in order to retrieve the secret image.

V. RESULTS AND DISCUSSIONS

The proposed scheme is implemented in MATLAB 8.3. The entire process of generating the shares and then encrypting the shares using GA is shown in Fig 4.

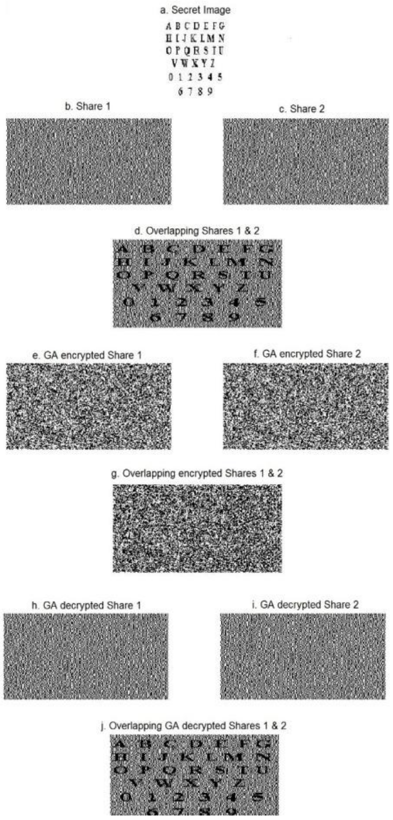
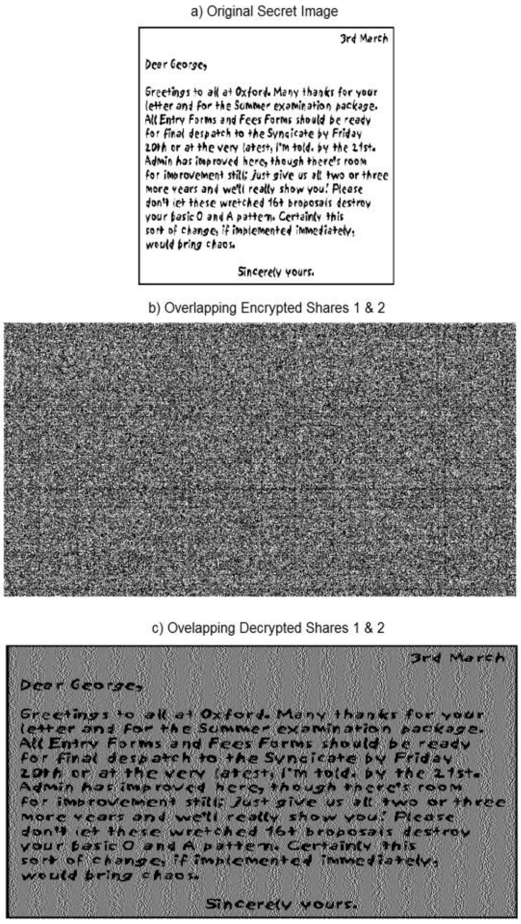


Fig. 4: Securing visual cryptographic shares using genetic algorithm

A secret binary image of size 128x128, shown by 'a' in Fig.4, is taken as input, (2,2) VC is performed in order to obtain the two shares of the secret image, denoted by 'b' and 'c' in the figures. The two shares should reveal the secret image on overlapping as shown in 'd'. Next, the two shares are encrypted using GA. First the keys are generated and then the two shares are encrypted. In the figures, 'e' and 'f' are the encrypted shares. It can be observed from 'g' in the figures that overlapping the two encrypted shares revealed no information about the secret image. Thus an opponent cannot obtain the secret image without the secret key. On obtaining the encrypted shares at the receiving end, GA decryption is performed on them in order to obtain the original shares. First the key for decryption is generated and then the shares are decrypted using this key. Once the original shares, shown in 'h' and 'i' are obtained, VC decryption is done by performing AND operation on the shares in order to obtain the original image back, shown in 'j' in Fig.4.

The proposed methodology is tested by applying it to images of various sizes with varying key lengths. Fig. 5, Fig. 6 and Fig. 7 show the securing of visual cryptographic shares of images of sizes 512x512, 256x256 and 128x128 respectively.


a) Original Secret Image
b) Overlapping Encrypted Shares 1 & 2
c) Ovelapping Decrypted Shares 1 & 2

3rd March

Dear George,

Greetings to all at Oxford. Many thanks for your letter and for the Summer examination package. All Entry Forms and Fees Forms should be ready for final despatch to the Syndicate by Friday 20th or at the very latest, I'm told. by the 21st. Admin has improved here, though there's room for improvement still; just give us all two or three more years and we'll really show you! Please don't let these wretched 16+ proposals destroy your basic O and A pattern. Certainly this sort of change, if implemented immediately, would bring chaos.

Sincerely yours.

Fig. 5: Securing visual cryptographic shares of an image of size 512x512

DOI 10.17148/IJIREEICE

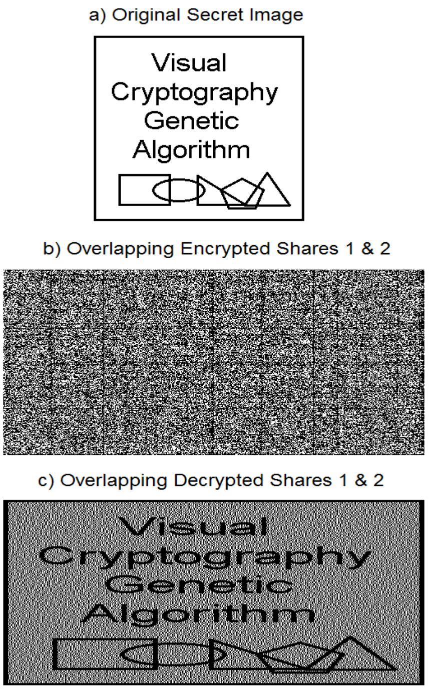

a) Original Secret Image
Visual Cryptography Genetic Algorithm
b) Overlapping Encrypted Shares 1 & 2
c) Overlapping Decrypted Shares 1 & 2
Visual Cryptography Genetic Algorithm

Fig. 6: Securing visual cryptographic shares of an image of size 256x256

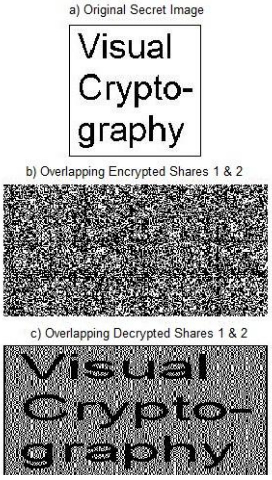

a) Original Secret Image
Visual Crypto-graphy
b) Overlapping Encrypted Shares 1 & 2
c) Overlapping Decrypted Shares 1 & 2
Visual Crypto-graphy

Fig. 7: Securing visual cryptographic shares of an image of size 128x128

In the figures, 'a' is the original secret image which is to be encrypted. VC is performed and the shares are encrypted using GA. Superimposition of the two encrypted shares is shown in 'b'. The receiver decrypts the obtained shares and overlaps them to obtain the secret image, as shown in 'c'. From the figures, it can be observed that overlapping the encrypted shares revealed no information about the secret image, while the secret image was fully recovered by overlapping the decrypted shares. Thus, the system can be applied to different sized images to obtain secure shares.

The system performance in terms of time taken for VC, GA encryption and decryption for images of different sizes with keys of different lengths is shown in Table I. It is visually represented in Fig. 8.

TABLE I SYSTEM PERFORMANCE USING GA

Image Size	Key Length (bits)	Time Taken (s)		
		VC	Encryption	Decryption
128x128	16	0.391	26.854	27.349
	64		8.072	8.019
	256		4.164	3.813
	1024		2.903	2.847
256x256	16	1.424	109.553	106.533
	64		33.663	34.540
	256		15.337	16.258
	1024		13.731	14.053
512x512	16	6.359	417.126	430.655
	64		150.306	152.051
	256		72.574	72.058
	1024		56.782	56.441

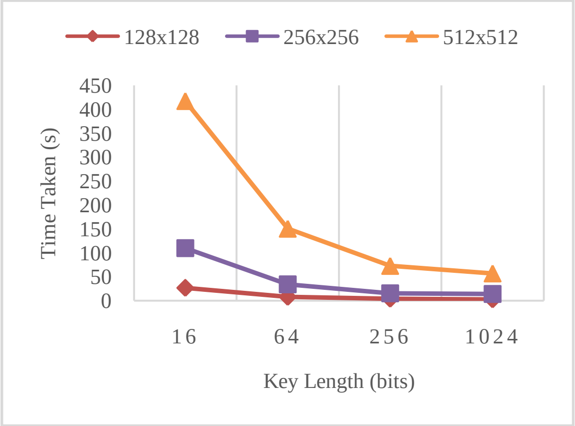


Fig. 8: Time taken for encryption of shares using genetic algorithm for various sized images with different key lengths

From Table I and Fig. 5 it can be observed that as the size of the image increases, the time taken for VC, encryption and decryption increases. However, the system does not have a large time requirement, Also, the time taken for encryption and decryption reduces with the increase in key length. Larger key lengths provide more security. Thus, GA provides good security to VC as keys of large lengths can be used without having the disadvantage of large time requirement.

VI. CONCLUSION

Visual Cryptography is a simple algorithm which can be used to encrypt documents or images. It has a lower computational cost as decryption is done by the eyes and there is no need for a decryption algorithm. This advantage can however turn into a drawback if a hacker comes across both the shares as he has to only overlap the two to recover the secret image. Securing these shares using Genetic Algorithm prevents the hackers from obtaining information by simply overlapping the shares. Even if he obtains the two secured shares and overlaps them he will not be able to retrieve the secret information. This scheme does not have large memory or bandwidth requirement as it doesn't use any cover images. The image quality of the retrieved image is of a visually acceptable level.

The system can be further improved by

- Implementing it for coloured images.
- Implementing it for various image formats.

REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography", Advances in Cryptology EUROCRYPT '94, Lecture Notes in Computer Science, vol. 950, pp. 1-12, 1995.

[2] Han Yan-yan, Cheng Xiao-ni and He Wen-cai, "A Watermarking based Visually Cryptography Scheme with Meaningful Shares", 2011 7th International Conference on Computational Intelligence and Security, IEEE, pp. 870-873, 2011.

[3] Xiao-Yi Liu, Ming-Song Chen and Ya-Li Zhang, "A new colour visual cryptography scheme with perfect contrast", 2013 8th International ICST Conference on Communications and Networking in China, pp. 449-454, 2013.

[4] Qin Chen, Xiaorong Lv, Min Zhang and Yipping Chu, "An Extended Colour Visual Cryptography Scheme with Multiple Secrets Hidden", 2010 International Conference on Computation and Information Sciences, IEEE, pp. 521-524, 2010.

[5] Zhi Zhou, Gonzalo R. Arce and Giovanni Di Crescenzo, "Halftone visual cryptography", IEEE Transactions on Image Processing, vol. 15, issue 8, pp. 2441-2453, 2006.

[6] Nitty Sarah Alex and L. Jani Anbarasi, "Enhanced image secret sharing via error diffusion in halftone visual cryptography", 2011 3rd International Conference on Electronics Computer Technology (ICECT), pp. 393-397, 2011.

[7] Thomas Monoth and Babu Anto P, "Contrast-enhanced visual cryptography scheme based on additional pixel patterns", 2010 International Conference on Cyberworlds, pp. 171-178, 2010.

[8] Melanie Mitchell, "An introduction to genetic algorithms", 1st ed., 1998, pp. 8-10.

[9] Scott M. Thede, "An introduction to genetic algorithms", Journal of Computing Sciences in Colleges, vol. 20, issue 1, pp. 115-123, 2004

DOI 10.17148/IJIREEICE