An Optimized Secret Image Sharing Scheme Based on Ant Colony Optimization Algorithm

M. Ilayaraja [1]

Assistant Professor, Department of Computer Science and Information Technology
Kalasalingam University, Krishnankoil, Virudhunagar (Dt), Tamil Nadu, India.
[1] ilayaraja.m@klu.ac.in

***Abstract*— A secret image kept in a single information-carrier could be easily retrieved or damaged by unauthorized entity. In the gigantic internet communication, the secret image sharing schemes can be used to share a secret image with utmost confidentiality over unsecured public channels. In this scheme a secret image is programmed into *n* transparencies of arbitrary prototypes. It is possible to decode the secret image visually by superimposing a qualified subset of transparencies. Nevertheless, no secret image can be acquired from the superposition of an illegal subset. In this paper, an efficient Ant Colony Optimization (ACO) algorithm is proposed for secret image sharing scheme. The original secret image pixels and key matrix is used to construct the transparencies. Here an ACO algorithm is utilized to optimize the key matrix to improve the transparency image quality. Experiments are conducted to show the security and efficiency of the proposed scheme. Comparisons with previous approaches show the advantages of the proposed scheme.**

Keyword - Secret Sharing; Image Sharing; Ant Colony Optimization; Pixels;

I. INTRODUCTION

Nowadays transmitting multimedia data by means of all-pervasive Internet is the trend gaining interest. With the advent of e-commerce, it has become extremely essential to tackle the sensitive issues of affording data security, especially in the ever-blooming open network environment of the modern era. The encrypting technologies of the time-honored cryptography are generally employed to shelter data safety extensively [1]. Cryptography is used to send and receive encrypted information which can be decrypted only by the sender or receiver. This technique is mainly used to store and transmit the data in an appropriate manner that can be read and processed only by the intended person. In the cryptography process, encryption is the conversion of plaintext (ordinary text or clear text) into cipher text and the reverse process is called decryption and the people who are working in this domain are called as cryptographers. With the emergence of multimedia applications, there is a huge demand for transmission and secured storage of information. So security is indispensable for proper data protection. If the information is protected, the intruders may not be able to distort the data. It becomes challenging to transmit the data in a secured and proper manner. Cryptographic techniques afford the confidentiality and security by reducing the prospect of adversaries [2]. Unlike traditional cryptographic methods such as Data Encryption Standard (DES) scheme and Advanced Encryption Standard (AES) scheme, the Visual Cryptography (VC) scheme provides fast decryption without any complex computation [3]. Visual Cryptography (secret sharing scheme) is a modern cryptographic technique used to share the secret data in a secure pattern, maintained with utmost confidentiality. A sender transmits the secret data which is divided into shadows and it holds hidden information. When all of these shadows are aligned and stacked together, it tends to expose the secret data information to the receiver [4]. The main role of VC scheme is to encrypt the secret data with the help of partitioning process. The private message cannot be revealed by the help of some split data's. The original image requires all split data's to be revealed. The process of visual cryptography is to divide an image into prearranged number of parts and then without any computation or algorithm, the secret data can be revealed by aligning and stacking together [5]. Another, secret sharing scheme is Visual Secret Sharing (VSS), based on the (k-n) threshold concept. This method works out of n shadow with any k or more reconstructed shadows to retrieve the original secret by superimposing the shadows that eliminates complex computations [6].

II. RELATED WORKS

Amitava Nag *et al.* proficiently put forward a new *(k, n)* secret sharing scheme [7] with the help of Boolean operations. In this scheme, *n-k* shares are lost, secret image could be recovered using remaining *k* shares. The restored image is lost in case if $k<n$ and lossless when $k=n$. Moreover, reconstruction complexity is of low means *O(k)* and expressed better fault tolerance property than other schemes.

Tzung-Her Chen *et al.* developed an algorithm [8] for (*n+1, n+1*) multi-secret sharing using XOR operations. In this scheme, '*n*' original data (image) is encoded into *'n+1'* meaningless shadow images and need all *n+1* share to restore all n secret images. Moreover, extra random matrix is used to create shared images. This advanced scheme provides some features such as Restoration of original image in lossless manner, absence of pixel expansion problem and also no codebook required. Computational cost is *O(m)*for *n* secret images.

Xuehu Yan *et al.* have suggested a *(k, n)* threshold VSS method [9] that depends upon the RG with AND and XOR operations to accomplish a non-destructive recovery. If less than '*k*' shadow images are collected, information of the secret image cannot be revealed. This scheme has good features such that no pixel expansion, no codebook required and reconstructed image is lossless.

Gyan Singh Yadav *et al.* proposed a multi-secret sharing scheme [10] based on the capabilities of bit-plane flipping and Boolean operations. In this scheme, two levels of encryption are performed. The first level is flipping some of the bit planes in circular order that makes it random. Further, to improve the security, another level of encryption is performed by using XOR. This scheme successfully completes the objective with two layer security, no pixel expansion problem; lossless retrieval of secret image and also no codebook is needed.

Sachin Kumar *et al.* have developed the method [11] for threshold VSS using Boolean operations. In this method two algorithms are designed to encode a plain image into *'n'* unmeaning shares. Thus, no confidential data is retrieved by exclusive OR of any *k-1* or less shares, otherwise the data is revealed. This scheme is the extension of Boolean basis of non-threshold VSS into threshold VSS with the achievement of no pixel expansion problem. The benefits of this scheme includes no codebook requirement, no alignment required during decoding process and also encoding binary, gray mode or color images.

III.PROPOSED SECRET IMAGE SHARING SCHEME

The original secret holder is secret image which is classified into *'n'* transparencies and distributed into *'n'* dealers. If all the *'n'* transparencies are together only, one can reveal the original secret image. This is general idea behind the image sharing scheme. The proposed image sharing scheme suggested that the following procedures. Initially, the secret color image is distorted into three grayscale images (also matrix format) based on its color components. Generate distinct random matrix with the size of the secret image size. After that, XOR operation is performed with random matrices and color component matrices to create the transparencies as separately. Here, qualities of the transparencies image are varied due to mainly the random matrices and so the random matrices values are optimized with the help of proposed ACO Algorithm. To evaluate the strength of the proposed scheme the sequence of investigations such as statistical and security assessments are carried out on the transparencies. The entire process of proposed methodology is depicted in the following diagram.

A. Ant Colony Optimization (ACO) Algorithm

In computer science and operations research, the ant colony optimization algorithm (ACO) is a probabilistic technique for solving computational problems which can be reduced to finding good paths through graphs [12]. The ACO algorithm is one of the most competent methods that indicate the main aspects of state transition rules and pheromone modernize devices. In each iteration, colonies of ants are sent to a particular place for solution. Each ant works steadily in their state transition rules. Suppose, if an ant completes a work, then the pheromone modernized begins to search another ant with similar strength. But it significantly reduces the opportunities and changes the search methodology.

B. Transparency Images Generation Algorithm

The secret image represents $I_{h\times w}$. Here *I* indicates the pixels values of the secret image (where *h=height, w=width*). The RGB color component pixel values are extracted from the secret image.

$$\mathrm{I}_{\mathrm{h}\times\mathrm{w}} = \sum R_i + G_i + B_i$$

Get the pixel value and then generate sum of *'n'* random numbers which are lesser than the pixel value for individual color component.

If $R_{(1,1)} = 150$ for red component, then generate 4 random numbers (if *transparency=4*) such as *40,80,20,10*.

The process repeated until last pixel values reached to create four matrices and it is considered as basic matrices. Then generate random (key) matrices of size $h \times w$ as the size of original image. Transparencies are generated by using *Exclusive – OR* between key matrices and *RGB* matrices. Transparencies PSNR values are calculated and the value is considered as initial fitness. Every time the fitness value is compared with other solutions and this process is iterated until optimal key values are obtained using ACO algorithm. Finally good and improved transparencies are obtained from the proposed ACO algorithm.

Proposed Ant Colony Optimization (ACO) Algorithm

Step 1: *Initialize the solution* H_i

$$H_i = \{H_1, H_2, ...H_n\}$$

Step 2: *Find the fitness value* (F_i)

$$F_i = PSNR + CC$$

Step 3: *Based on the fitness find Probability transition matrix*

$$P_{ij}^{\ c} = \frac{(\tau_{ij})^{\alpha}(\eta_{ij})^{\beta}}{\sum(\tau_{ij})^{\alpha}(\eta_{ij})^{\beta}}$$

Step 4: *Update pheromone and Evaporation pheromone*

$$\tau_{ij} = (1-\rho) * \tau_{ij} + \sum_{C=1}^{S} \Delta\tau_{ij}^{\ C}$$

Where, ρ *= pheromone evaporation rate, S = number of ants*

$\Delta\tau_{ij}^{c}$ *= is the quantity of pheromone laid on edge (i, j) by* c^{th} *ant*

Step 5: *Find the fitness for* H_{new} *from pheromone evaporation*

$$if(H_{new}) > f(H_i)$$

Step 6: *Store the best solution so far attained*

Iteration=Iteration+1

Step 7: *Stop until optimal key matrix is attained*

C. Transparency ImagesRregeneration Algorithm

RGB color components pixel values are extracted from the transparencies. Then *XOR* operations are performed between the transparency and Optimal key matrices for individual color components to retrieve basic matrices. All basic matrices combined together to retrive the secret image color components individually. Finally retrieve the secret image $(I_{h \times w})$,

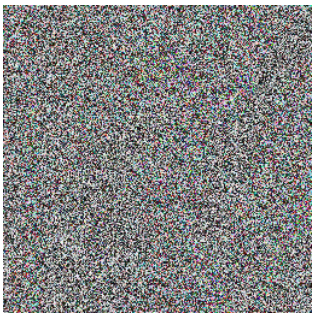
$$I_{h \times w} = \sum S_r + S_g + S_b$$

IV. RESULTS AND ANALYSIS

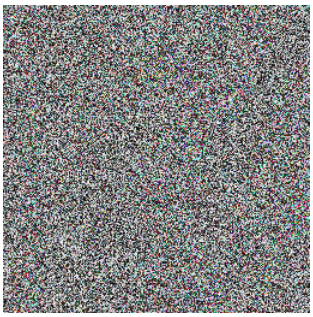
A. Experimental Results

Different test images are used to evaluate the performance of the proposed secret image sharing scheme. This process considers 2 test images [14] such as the Barbara (image1) and Tiffany (image 2) images are used. The experimental result from the implementation of the proposed scheme, the original secret image and its transparency images and decrypted secret image of the Barbara and Tiffany image is represents in the Figure 1 and 2.

(a)



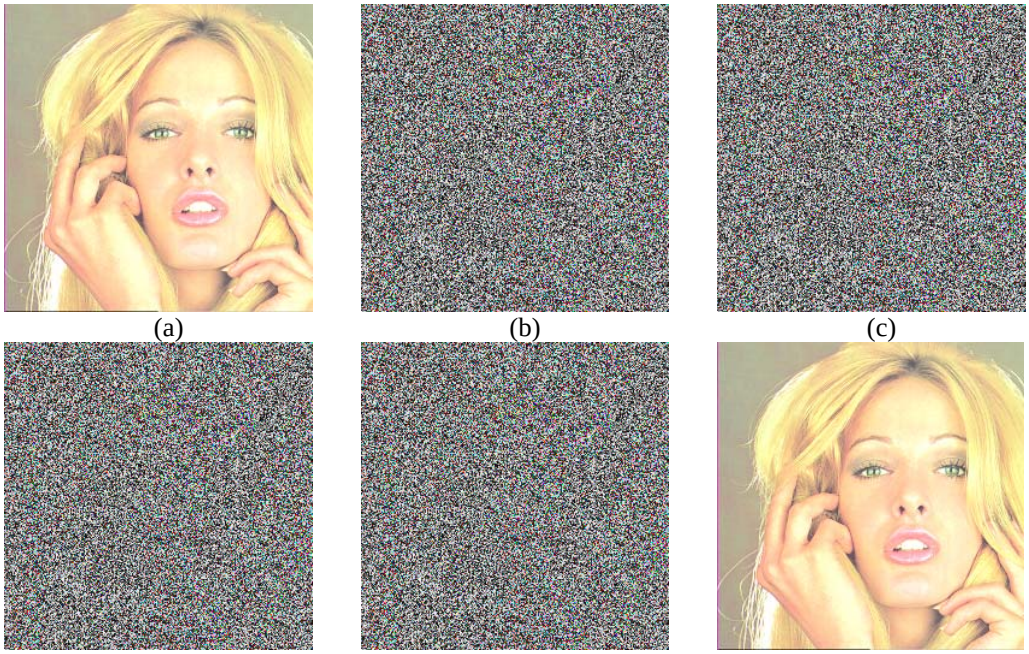
(b)



(c)

(d) (e) (f)

Fig. 1. Results of the Barbara (a) Secret image (b, e) Transparency Images (f) Transparencies to Reconstructed Image;



(a) (b) (c)

(d) (e) (f)

Fig. 2. Results of the Tiffany (a) Secret image (b, e) Transparency Images (f) Transparencies to Reconstructed Image;

B. Performance Analysis

The performance of the proposed scheme is analyzed by using the PSNR value in all images.

1) *Peak Signal to Noise Ratio (PSNR)*: The signal, here, represents the original data, and the noise relates to the flaw triggered by the compression. While analyzing and contrasting the compression codec's, the PSNR constitutes an approximation to human insight of modernization excellence. Even though a superior PSNR usually reveals the fact that the modernization is of superb quality, though there are exceptions to this trend. Therefore, it is highly essential to take utmost care regarding the extent of validity of this metric.

TABLE I. PSNR (in db) Values for Different Sample Images

Image Name	**PSNR**			
	Transparency1	**Transparency2**	**Transparency3**	**Transparency4**
Barbara	6.31	6.78	6.09	6.98
Tiffany	7.27	7.74	6.87	7.45

In table 1, the proposed scheme with their PSNR is employed for various sample test images. When the PSNR value is compared for the original image with encrypted image, the PSNR is low which yields better encryption quality. It is clear that the PSNR values are 6 to 8, which shows low PSNR value, it represents better encryption quality with high security of the secret image.

2) Comparative Analysis: Table 2 shows a comparison between proposed ACO algorithm based secret image sharing scheme and existing scheme [15] (without optimize the key matrix) based on significant parameter of PSNR values.

TABLE II. Comparison of PSNR values of Proposed Schemes with Existing Schemes

Image Name	Proposed ACO for SIS Scheme	SIS Scheme
Barbara	6.54	8.49
Tiffany	7.33	8.45

From the table above, the PSNR value of proposed method remains lower than existing SIS scheme. The transparency qualities are improved by using the proposed scheme with assist of ACO Algorithm. It noticeably shows that the proposed method provides the best security scheme when compared with the existing scheme.

V. CONCLUSION

In this paper an optimized secret image sharing scheme based on ant colony optimization algorithm is presented. In the existing secret image sharing schemes, transparencies are generated with aid of random matrices. The resultant transparency quality and security depends on only those random matrices. This is one of the main drawbacks of the existing schemes. This issue is resolved by using optimization algorithm. In this proposed method optimal random key matrix is generated with help of ACO algorithm. The performance and comparative analysis of the proposed scheme, which shows that the effectiveness of the proposed scheme. So this approach possesses excellent potential for secret image sharing schemes.

ACKNOWLEDGMENT

The author would like to thank the management of Kalasalingam University, Krishnankoil, Tamilnadu, India, for the facilities provided to carry out this research work.

REFERENCES

[1] Y. C. Hou, “Visual cryptography for color images”, Pattern Recognition, vol. 36, page(s): 1619–1629, 2003.
[2] Adi Shamir, “How to share a secret”, Communications of the ACM, vol. 22, no. 11, page(s): 612–613, 1979.
[3] Simmons and Gustavus J, “An introduction to shared secret and/or shared control schemes and their application”, Contemporary cryptology: The science of information integrity, page(s): 441–497, 1992.
[4] K.Shankar and P. Eswaran, “Sharing a Secret Image with Encapsulated Shares in Visual Cryptography”, Procedia Computer Science, vol. 70, page(s): 462–468, 2015.
[5] Cimato, Stelvio, Roberto De Prisco and Alfredo De Santis, “Probabilistic Visual Cryptography Schemes”, The Computer Journal, vol. 49, No. 1, page(s): 97–107, 2006.
[6] Daoshun Wang, Lei Zhang, Ning Ma and Xiaobo Li, “Two secret sharing schemes based on Boolean operations”, Pattern Recognition, vol. 40, issue.10, page(s): 2776–2785, 2007.
[7] Amitava Nag, Sushanta Biswas, Debasree Sarkar and Partha Pratim Sarka, “Secret Image Sharing Scheme Based on a Boolean Operation”, Cybernetics and Information Technologies, vol. 14, issue.2, page(s): 98–113, 2014.
[8] Tzung-Her Chen and Chang-Sian Wu, “Efficient multi-secret image sharing based on Boolean operations”, Signal Processing, vol. 91, issue.1, page(s): 90–97, 2011.
[9] Xuehu Yan, Shen Wang, Ahmed A. Abd El-Latif and Xiamu Niu, “Visual secret sharing based on random grids with abilities of AND and XOR lossless recovery”, Multimedia Tools and Applications, vol.74, issue.9, page(s): 3231–3252, 2015.
[10] Yadav, Gyan Singh, and Aparajita Ojha, “A Novel Multi Secret Sharing Scheme Based on Bitplane Flips and Boolean Operations.” ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of Computer Society of India-Vol I. Springer International Publishing, 2014.
[11] Sachin Kumar and Rajendra K. Sharma, “Threshold visual secret sharing based on boolean operations”, Security and Communication Networks, vol.7, issue.3, page(s): 653–664, 2014.
[12] https://en.wikipedia.org/wiki/Ant_colony_optimization_algorithms
[13] Christian Blum, “Ant colony optimization: Introduction and recent trends”, Physics of Life reviews, vol.2.4, page(s): 353-373, 2005.
[14] http://www.hlevkin.com/TestImages/
[15] K.Shankar and P.Eswaran, “A New k out of n Secret Image Sharing Scheme in Visual Cryptography”, IEEE Explore digital library, ISBN: 978-1-4673-7807-9, IEEE. 2016.