ADV MATH
SCI JOURNAL

Advances in Mathematics: Scientific Journal **10** (2021), no.1, 453–461
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.10.1.45

ANT COLONY OPTIMIZATION BASED OPTIMAL STEGANOGRAPHY TECHNIQUE FOR SECRET IMAGE SHARING SCHEME

K. Shankar[1] and Eswaran Perumal

ABSTRACT. Data hiding earlier to transmission remains as an essential process for reducing the security issues in the cloud based environment. Image encryption and steganography techniques verify the safety of secret data during the transmission over the Internet. This paper presents a new multiple secret share creation (SSC) with ant colony optimization (ACO) based image steganography (SSC-ACO) technique to achieve security over image transmission. Initially, SSC algorithm is applied to generate a set of different shares for the applied image. Then, the ACO algorithm based image steganography technique is employed to generate the stego images for the applied cover and share images. The utilization of image steganography technique comprises a set of shares into the cover image to secure the details of the individual shares. The experimental validation of the projected model is tested using diabetic retinopathy (DR) images and the results are examined interms of peak signal to noise ratio (PSNR). The obtained PSNR values ensured the effective performance of the presented model on all the employed test images.

[1] *corresponding author*

2020 *Mathematics Subject Classification.* 68P25.

Key words and phrases. Secret image sharing scheme, Steganography, ACO algorithm, Diabetic retinopathy (DR) images, PSNR.

Submitted: 20.12.2020; *Accepted:* 06.01.2021; *Published:* 21.01.2021.

1. INTRODUCTION

Actually, prominent enhancements in networks and computer science have raised the usage of Internet and Internet based data transmissions. In most of the significant sectors like interaction of commercial news, military details, the images will be stored with complete security. Massive image-preserving methods like data encryption, steganography and alternate models are presented for enhancing the privacy of confidential images. But, a general disadvantage of previously mentioned approaches is, the strategy of federal storage, where the preserved image is retained in single data carrier. When an intruder predicts the data anomalies in information carrier, then it indicates that an attacker is trying to interrupt and wish to learn the secret inside, or destroy the whole information carrier where the secret is also ruined. Furthermore, the passing the confidential data by similar cover image enhances the doubt of an attacker whether data is transmitted or not. It shows the significance of passing confidential information under diverse cover images.

In order to overcome the above mentioned problems, Secret image sharing has been deployed which is free from these issues. It is operated by classifying the private image as n shadow images which is then conveyed and recorded in separate platform. The actual image can be reformed only using the pre-set value of n shadow images; however, its contribution is less when compared to t shadow images which are inadequate to reveal the private image. A reputed strategy in analog sector is limited trust, which means that, to maintain the secret entity power has to be provisioned. It is one of the fundamental, and secret sharing model for accomplishing this in electronic application. The secret sharing module [1, 2] was utilized extensively for distributing the secret key. Here, all participants have a private shadow and authenticated members with combined shadows work together for recovering the secret key. The main objective of secret distribution is for enhancing the secret key and few shadows are hacked, or lost.

Singha and Ramanb [3] presented a reversible data hiding procedure that is based on Shamir's secret sharing for legitimate leadership in scrambled space. It concealed the cover data with respect to classifying into diverse shares which resembles the inconsistency. In this approach, confidential data should be precised for authorized user, which is then fed into scrambled shares according to a secret key before redistributing to media data. In cloud servers, shares do not uncover the data. At this point, reliable entity with secret keys plans support the extraction of secret data directly from cloud servers.

2. The Proposed SSC-ACO algorithm

The operational principle of the SSC-ACO algorithm is given here. The SSC algorithm creates multiple shares in the primary stage and is further hidden to the cover image using ACO based image steganography technique.

2.1. **Share Construction Scheme.**

In SSC process, a secret image is encoding into n shares called as ‘transparencies’. In entire share contains together black as well as white pixels, in the shape of noise and is very huge in dimension if related to the confidential image. The shares are generated by using multiple visual secret share (VSS) creation procedure [4].

VSS based Share Creation Scheme

(1) Select an secret image of size $w \times h$ of the image, where w is a width and h is a height of the image.
(2) Create two matrices for share 1 and share 2 pixels
(3) Initialize variable font color and index value

```
  Initially set index=1
For w and h is 1 to width and height
Image color=Get pixel color from $w, h$
Index= Choose random number either 0 or 1
    (1) If (index==1)
  Set Share 1 pixel ($w, h$ ) =Image Color
  Set Share2 pixel ($w, h$ ) = Empty
    (1) Else
Set Share 1 pixel ($w, h$ ) = Empty Set Share2 pixel ($w, h$ ) = Font Color
```

2.1.1. *Initialization.*

The digital image is an array of pixels through intensity level I. Assume that grayscale image of size $M_1 \times M_2$, as cover medium. Totally, K ants are arbitrarily allocated on an image C. All pixels of the cover image are regarded as nodes. For initializing a complex part recognition, a first value of all pheromones matrix’s module $\tau^{(0)}$ is initialized to a fixed $\tau_{initial}$.

2.1.2. *Construction.* The construction procedure holds several stages, at the nth construction-step, 1 ant, from an entire of K ants is arbitrarily chosen. The chosen ant is progressed over the cover image to N_{mov} movement steps. A motion of the ant from first node (x, y) to its nearest node (u, v) is completed based on the transition possibility $p^{(n)}_{(x,y),(u,v)}$ as provided by Eq. (2.1)

$$p^{(n)}_{(x,y),(u,v)} = \frac{(\tau^{(n-1)}_{u,v})^{\alpha}(\eta_{u,v})^{\beta}}{\Sigma_{(u,v)\in\Omega_{(x,y)}}(\tau^{(n-1)}_{u,v})^{\alpha}(\eta_{u,v})^{\beta}}, \tag{2.1}$$

where $\tau^{(n-1)}_{u,v}$: Pheromone value at node (u, v), $\Omega_{(x,y)}$: Neighborhood (4 or 8-attached) node of the node (x, y), $\eta_{u,v}$: Heuristic data at node (u, v), α: Control of pheromone matrix, β: Control of heuristic matrix. The heuristic data at some node (u, v) is computed utilizing Eq. (2.2):

$$\eta_{u,v} = \frac{V_C(C_{u,v})}{Z}, \tag{2.2}$$

where Z is the normalization factor and provided by Eq. (2.3):

$$Z = \sum_{u=1:M_1} \sum_{V=1:M_2} V_c\left(C_{u,v}\right), \tag{2.3}$$

where $C_{u,v}$: The intensity level pixel (u, v) of image C. In $V_c(C_{u,v})$ based on the difference in gray levels of strength of pixels in the clique c is signified as by Eq. (2.4):

$$\begin{aligned} y_c(c_{u,v}) = f(&|c_{u-2,v-1} - c_{u+2,v+1}| + |c_{u-2,v+1} - c_{u+2,v-1}| \\ &+ |c_{u-1,v-2} - c_{u+1,v+2}| + |c_{u-1,v-1} - c_{u+1,v+1}| \\ &+ |c_{u-1,v} - c_{u+1,v}| + |c_{u-1,v+1} - c_{u-1,v-1}| \\ &+ |c_{u-1,v+2} - c_{u-1,v-2}| + |c_{u,v-1} - c_{u,v+1}|). \end{aligned} \tag{2.4}$$

For calculating f, there are 4 several functions such as Flat, Gaussian, Sine and Wave and all of them is regarded in these work and are provided now in Eq. (2.5) to Eq. (2.8):

$$f(x) = \lambda x \quad \text{for } x = 0, \tag{2.5}$$

$$f\,(x) = \lambda x^2 \quad \text{for } \chi = 0, \tag{2.6}$$

$$f\,(x) = \begin{cases} \sin\left(\frac{\pi x}{2\lambda}\right), & \text{for } 0 = x = \lambda \\ 0, & \text{otherwise} \end{cases}, \tag{2.7}$$

$$f\left(x\right)=\left\{\begin{array}{cc}\frac{\pi x\sin\left(\frac{\pi x}{\lambda}\right)}{\lambda}, & \text{for } 0=x=\lambda\\ 0, & \text{ptherwise}\end{array}\right. . \tag{2.8}$$

2.1.3. *Updating Stage.* Here, the pheromone matrix is updated in 2 steps. Once the initial update is executed during all the construction steps, behind a progress of all ants, based on Eq. (2.9):

$$\tau_{u,v}^{(n-1)}=\left\{\begin{array}{cc}(1-\rho)\cdot\tau_{u,v}^{(n-1)}+\rho\cdot\Delta_{u,v}^{(k)}, & \text{if } (u,v)\text{, is visited by Kant}\\ \tau_{u,v}^{(n-1)} & \text{otherwise}\end{array}\right. , \tag{2.9}$$

where ρ: The evaporation rates, and $\Delta_{u,v}^{(k)}$: Defined with heuristic matrix is equivalent to $\eta_{u,v}$. If the whole ant finishes their progress in all construction steps, the 2^{nd} updating method is carried out utilizing Eq. (2.10):

$$\tau^{(n)}=(1-\psi)\cdot\tau^{(n-1)}+\psi\cdot\tau^{(0)}, \tag{2.10}$$

where ψ : The pheromone decomposed coefficient The last decision to all pixels at (u,v) is developed on the basis of the pheromone vale $\tau_{u,v}^{(N)}$ at postion (u,v) related by the last threshold value $T^{(l)}$ as provided by Eq. (2.11):

$$E_{u,v}=\left\{\begin{array}{cc}0, & \text{if } \tau_{u,v}^{(N)}=T^{(l)}\\ 1, & \text{otherwise}\end{array}\right. , \tag{2.11}$$

where E: The binary image. When the pheromone value at present position (u,v) is superior to threshold, it is regarded as a component of complex region and rest of the parts are considered as the smooth area pixel.

2.1.4. *Image Steganography Process.* The pixel $C_{u,v}$ is regard as difficult region pixel when its equivalent $E_{u,v}=0$ and is regard smooth area component if $E_{u,v}=1$. Assumes that a secret image m to be concealed in the difficult region of the cover image C and S is last stego image attained behind data hiding.

$$S_{u,v}=\left\{\begin{array}{cc}C_{u,v}*m, & \text{if } E_{u,v}=0,\\ C_{u,v}, & \text{if } E_{u,v}=1\end{array}\right. .$$

2.2. **Share Reconstruction Scheme.** The retrieval of original secret image from the stego image is discussed in the following.

The true receiver, who knows the detail of the embed positions over cover images for the total number of shares, can retrieve the secret shares by performing reverse steganography method. After getting shares, we need to reconstructed the original secret image. Further, all the deciphered shares are amassed together to attain the original image using the below the steps:

$$R_n = R_{s1} \bigoplus R_{s2},$$

$$G_n = G_{s1} \bigoplus G_{s2},$$

$$B_n = B_{s1} \bigoplus B_{s2}.$$

The, final decrypted image can be determined as follows.

$$F_{image} = R_s + G_s + B_s.$$

3. Experimental Validation

For validating the performance of the SSC-ACO algorithm, an extensive set of simulations takes place on DR images.

Table 1. Result analysis of existing with proposed method in terms of PSNR and MSE

Image Name	**SSC-ACO**		**SSC-PSO**	
	PSNR	**MSE**	**PSNR**	**MSE**
DR _Image 1	48.39	0.943	46.51	1.453
DR_Image 2	48.28	0.967	45.95	1.652
DR_Image 3	48.63	0.892	47.21	1.236
DR_Image 4	48.71	0.876	45.65	1.769
DR_Image 5	48.53	0.913	45.23	1.948

Table 1 provides a detailed comparative analysis of the SSC-ACO algorithm with SSC-PSO algorithm interms of PSNR and MSE. the PSNR analysis of the SSC-ACO algorithm on the applied set of images. The figure depicted that the SSC-ACO algorithm has reached to a higher PNSR value over the SSC-PSO algorithm. On the applied DR image 1, the SSC-ACO algorithm has exhibited maximum PSNR value of 48.39dB whereas the SSC-PSO algorithm has depicted minimum PSNR value of 46.51dB. On the applied DR image 2, the SSC-ACO method has demonstrated highest PSNR value of 48.28dB while the SSC-PSO model has depicted least PSNR value of 45.95dB. On the applied DR image 3, the SSC-ACO approach has exhibited maximum PSNR value of 48.63dB but the

SSC-PSO method has shown lowest PSNR value of 47.21dB. On the applied DR image 4, the SSC-ACO algorithm has exhibited maximum PSNR value of 48.71dB whereas the SSC-PSO technique has shown minimum PSNR value of 45.65dB. On the applied DR image 5, the SSC-ACO methodology has demonstrated highest PSNR value of 48.53dB while the SSC-PSO model has exhibited minimum PSNR value of 45.23dB.

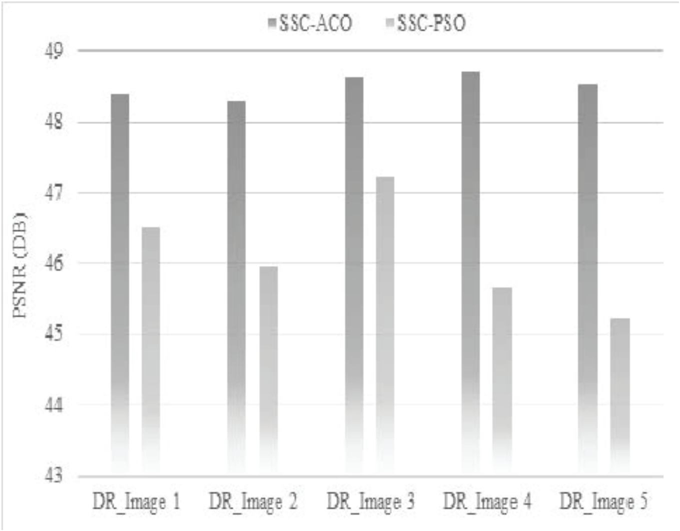

FIGURE 1. PSNR analysis of SSC-ACO model

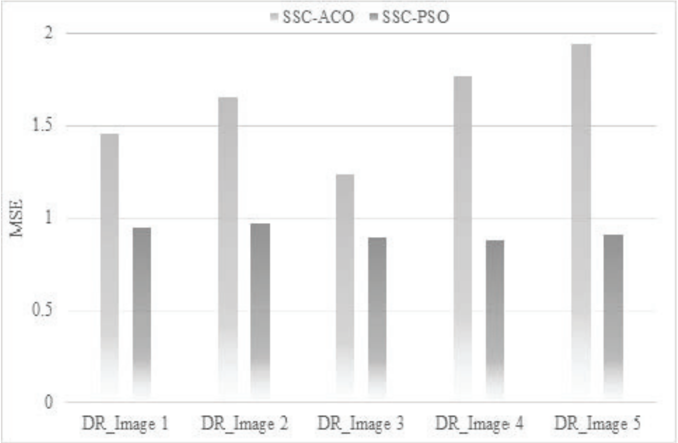

FIGURE 2. MSE analysis of SSC-ACO model

4. MSE analysis of SSC-ACO model

Fig.1 depicts the MSE analysis of the SSC-ACO algorithm on the applied set of images. The figure depicted that the SSC-ACO algorithm has exhibited minimum MSE with the higher MSE value over the SSC-PSO algorithm. On the applied DR image 1, the SSC-ACO algorithm has exhibited lower MSE value of 0.943 whereas the SSC-PSO algorithm has depicted higher MSE value of 1.453. On the applied DR image 2, the SSC-ACO method has performed minimum MSE value of 0.967 while the SSC-PSO methodology has exhibited maximum MSE value of 1.652. On the applied DR image 3, the SSC-ACO technique has demonstrated least MSE value of 0.892 but the SSC-PSO approach has depicted higher MSE value of 1.236. On the applied DR image 4, the SSC-ACO method has shown minimum MSE value of 0.876 whereas the SSC-PSO model has showcased higher MSE value of 1.769. On the applied DR image 5, the SSC-ACO methodology has exhibited lower MSE value of 0.913 while the SSC-PSO model has demonstrated maximum MSE value of 1.948

5. Conclusion

This paper has introduced an effective multiple SSC-ACO technique for achieving secure data transmission. At the earlier stage, SSC algorithm is utilized for the generation of distinct shares for the employed test image. Afterwards, the ACO algorithm based image steganography technique is applied for the creation of stego image the applied cover and share images. The utilization of image steganography technique comprises a set of shares into the cover image to secure the details of the individual shares. The experimental validation of the projected model is tested using DR images and the results are examined interms of PSNR.

6. Acknowledgments

This article has been written with financial support of RUSA–Phase 2.0 grant sanctioned vide Letter No. F. 24-51/2014-U, Policy (TNMulti-Gen), Dept. of Edn. Govt. of India, Dt. 09.10.2018.

7. Conflict of Interest

The authors declare that they have no conflict of interest.

References

[1] A. SHAMIR: *How to share a secret*, Communications of the ACM, **22**(11) (1979), 612–613.

[2] M. NAOR, A. SHAMIR: *Visual cryptography*, De Santis, A. (ed.) EUROCRYPT 1994, Springer, Heidelberg, **950** (1995), 1–12.

[3] P. SINGH, R. BALASUBRAMANIAN: *Reversible data hiding based on Shamir's secret sharing for color images over cloud*, Information Sciences, **422** (2018), 77-97.

[4] K. SHANKAR, P. ESWARAN: *A Secure Visual Secret Share (VSS) Creation Scheme in Visual Cryptography using Elliptic Curve Cryptography with Optimization Technique*, Australian Journal of Basic and Applied Sciences, **9**(36) (2015), 150-163.

DEPARTMENT OF COMPUTER APPLICATIONS,
ALAGAPPA UNIVERSITY, KARAIKUDI, INDIA.
Email address: `drkshankar@ieee.org`

DEPARTMENT OF COMPUTER APPLICATIONS,
ALAGAPPA UNIVERSITY, KARAIKUDI, INDIA.
Email address: `eswaran@alagappauniversity.ac.in`