HIGH CAPACITY AND OPTIMIZED IMAGE STEGANOGRAPHY TECHNIQUE BASED ON ANT COLONY OPTIMIZATION ALGORITHM

A. Priya
PG Student
Alagappa University, Tamilnadu, India.
Email : priya22345@gmail.com

Abstract

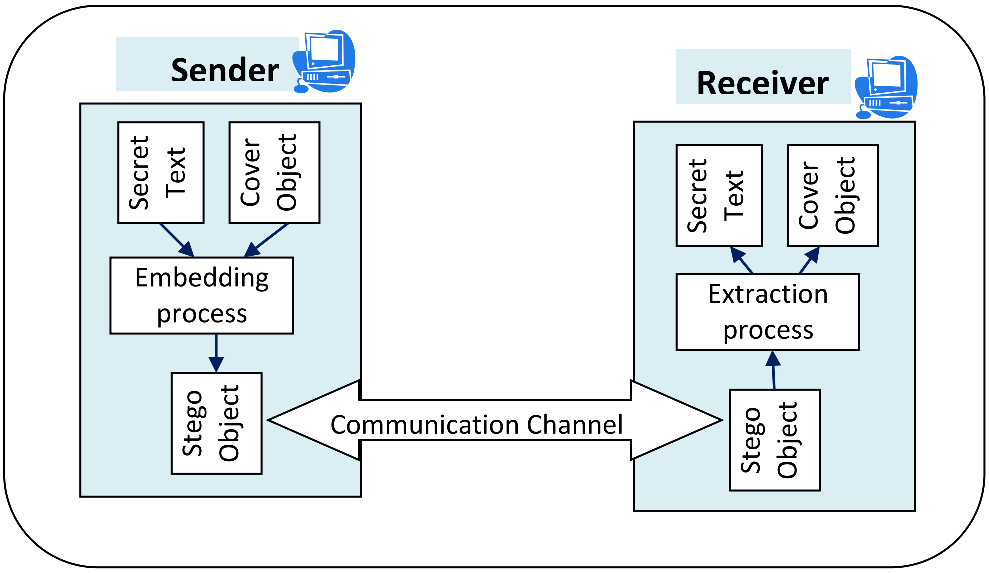
The tremendous development of digital technology, it is mandatory to address the security while transmitting information over network in a way that observer couldn't depict it. Measures to be taken to provide the security by establishing hidden communication using steganography principle which is help to camouflage the secret information in some carrier file such as text, image, audio and video. In this era of hidden data communication, image becoming an effective tool on account of their frequency, capability and accuracy. Image steganography uses an image as a carrier medium to hide the secret data. The main motive of this article is that the uses the combination of frequency domain and optimization method inorder to increasing in robustness. In this article, Integer Wavelet transform is performed into the host image and coefficients have been transformed. ACO optimization algorithm is used to find the optimal coefficients where to hide the data. Furthermore, sample images and information having been demonstrated which proved the increased robustness as well as high level of data embedding capacity.

Keywords: Security, Image, steganography, IWT, ACO (Ant Colony Optimization) algorithm.

1. Introduction

Cryptographic techniques afford the confidentiality and security by reducing the prospect of adversaries [1]. There are two processes in cryptography such as: a) Encryption and b) Key management process. Each security system must supply some security process that guarantees the secrecy of the system [2]. Cryptography is grouped into Symmetric Key and Asymmetric Key Cryptography [3]. In Symmetric key cryptography, a single key is used for both encryption and decryption [4]. The Asymmetric Key Cryptography uses different keys for both processes [5]. In session key; the symmetric key can be changed every time in communication between two parties. It is randomly generated and valid for only one session [6-8]. If an attacker gets the session key, he/she can decrypt only the messages for a particular session. If both parties always used the same key for all sessions, the attacker would be able to decrypt all messages encrypted with this key [9-12]. The underlying mathematical problem of a public-key cryptosystem determines the efficiency of the cryptosystem in a way. Because these problems dictate the sizes of domain parameters and keys, which in turn affect the performance of the arithmetic operations of the public-key crypto algorithms [13-15].

Steganography is the art and science of secret communication between two parties over a public medium that is not detectable by an observer. Steganography is a close cousin of cryptography which is the art and science of secret communication. Cryptography aims to conceal the content of the message whereas steganography hides the very existence of secretive communication as well [17]. For example, figure 1 shows that two users want to sharing information between them. But noticer is examining that communication via Internet Service Provider or local server. To protect this communication, steganography provide a model in which sender A wish to send message M to receiver B. Sender embed M over the cover media C and obtained stego object S then sent it over the insecure channel. The terms cover object is defined as various types of multimedia objects are used to hide the data and stego object is known as which object embedded the secret information[18].



Effective characteristics of steganography [20];

1. Secrecy : With the allowing of intend users, extracting the hidden information [34-37]
2. Imperceptions: The ability to be completely undetectable [38-40]
3. Capacity: Maximum length of the hidden information which can be embedded in cover object.
4. Accuracy: Extracting of the embedded data should be accurate.

Steganography techniques are classified into two types which are spatial domain and frequency domain techniques. In spatial domain, processing is data hidden directly on the pixel values of the image and in frequency domain, image is transformed then data is hidden on the transformed coefficients [21]. Some of the spatial domain techniques are LSB, PVD, EBE, RPE, PMM and Pixel intensity based etc. and some of the frequency domain techniques are DCT, DWT, DFT, IWT and DCVT [22]. Specifically, spatial domain techniques are susceptible to visual attack and pixel alteration [23]. When comparing to spatial domain, transform domain techniques are more robustness because of its hiding scheme in significant areas of cover images [24-28]. Integer wavelet transform (IWT) maps an integer data set into another integer data set . In discrete wavelet transform, the used wavelet filters have floating point coefficients so that when we hide data in their coefficients any truncations of the floating point values of the pixels that should be integers may cause the loss of the hidden information which may lead to the failure of the data hiding system [29].

The remaining of the paper is constructed as below: Relevant works have discussed in section 2. In section 3, explain the workflow of proposed method include algorithms. In Section 4, prove the proposed method has increasing in robust and level of capacity by carried out the experiment on sample image and secret data. Finally, Section 5 concludes the article.

2. Related Work

Discrete Wavelet Transforms are used in JPEG2000 image format and several methods embed information using Integer Wavelet Transform Coefficients. Lai and Chang proposed an adaptive data hiding method in the frequency domain [30]. Seyyedi et al. in [22] proposed a high volume payload and secure steganography technique based on integer wavelet transform. Ghasemi et al. combined Genetic Algorithm (GA), OPAP and Integer Wavelet Transforms to reduce distortion while delivering high embedding capacity in [23].

N. Vinothkumar et al [24**]** have been suggested to embed the data over image on the basis of the combination IWT with Optimal pixel Adjustment Process (OPAP). The method use IWT to transform the coefficients on cover image and OPAP is used to raise the level of hiding capacity. Result shows that minimize difference error betwixt original and encoded image.

Ching-Sheng Hsu et al [25] have been proposed method to determined the optimal LSB substitution using ACO algorithm . This method embeds the data into the last bits of the cover image. Moreover, generate optimal matrix with the help of ACO algorithm to conceal the data at the optimal values.

Rafael Lima de Carvalho et al [26] have been used optimization principle to hide the secret message into the target picture. Optimization done by PSO algorithm and produce better result than classical GA based method.

Amanjot Kaur et al [27] have been proposed algorithm which finding an optimal block on image may be the best position to hide the data. The fitness function to be taken where ratio is maximize of sum of contrast and energy and entropy and homogeneity. Results prove that this algorithm showing superiority than PSO algorithm.

3. Proposed Method

3.1 Overview

The proposed method is splitted into two subsequent parts such as using IWT for transforming coefficients and ACO to find the best values for embedding. In the first part of proposed method, input the color image as carrier and extracting three RGB color components [31]. Integer wavelet transform is applied on these components and results showing transformed coefficients. Second part concerned the Ant Colony Optimization algorithm which inspired the behavior of ants. These ants deposited pheromone on the path to discover shortest best path from nest to food. More pheromone on path increases, that path followed by every other ants of the colony. Ant Colony Optimization Algorithm work on the basis of the similar mechanism and used in proposed method. The secret raw data has been converted into ASCII values and these can be embedding at the optimal coefficients by applying ACO algorithm. After all secret values were embedded; inverse IWT is processed to gain the stego object and ready to send it to receiver. At the recipient side, received it and extract the secret data from it by performing the reverse procedure of embedding method. With the neat sketch, the entire work of proposed method is described in the following figure.

3.2 Algorithm

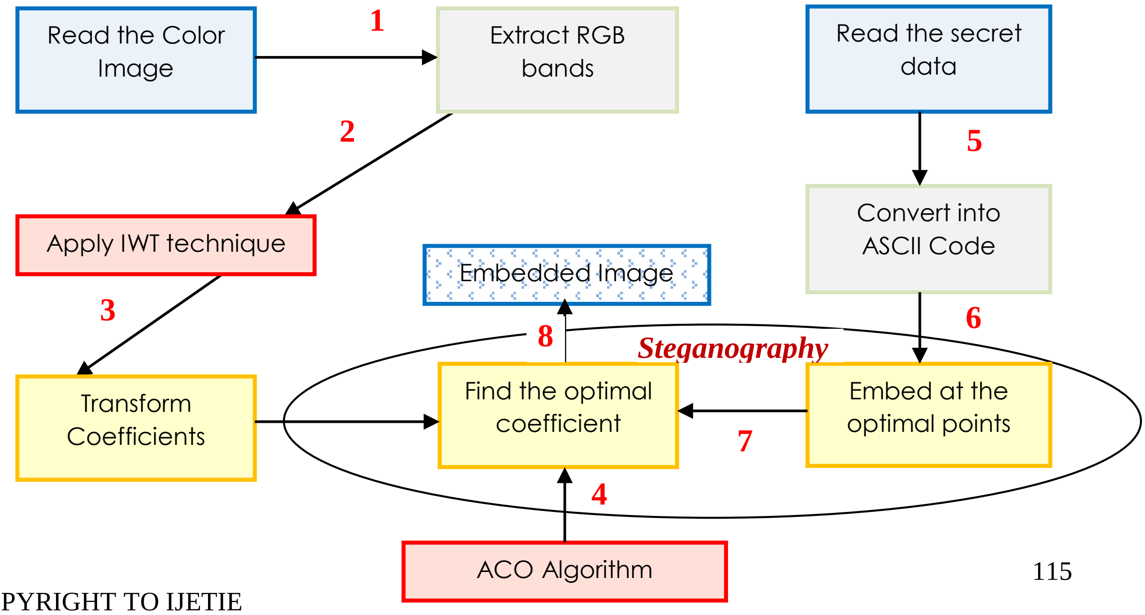
Proposed embedding algorithm is enumerated below to hide the data over the cover image.

1. Given input as color image and secret data
2. Extract RGB components from color image
3. IWT technique is applied on the bands and makes transformation among the coefficients.
4. ACO algorithm is used to find the optimal points.
5. Data is converting into ASCII values. On each row at every location given by the ACO, embed values at those optimal points.
6. Finally, stego image is obtained by process the inverse IWT method.

Whereas the proposed extracting algorithm is explained below;

1. Receive the stego image
2. Data is extracting from the stego image by performing the reverse operation of embedding method.
3. Obtained the secret data.

3.3 Block Diagram



3.4 Ant Colony Optimization 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 [33]. The ACO algorithm is one of the most competent methods that indicate the main aspects of state transition rules and pheromone modernize devices [41-43]. 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.

Step 1:

Initialize the solution H_i

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

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

Step 6: Find the fitness for H_{new} from pheromone evaporation

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

Step 7:

Store the best solution so far attained
Iteration=Iteration+1

Step 8:

Stop until optimal key attained

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

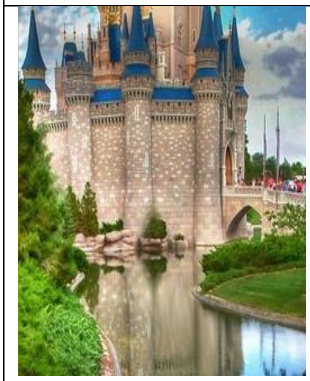
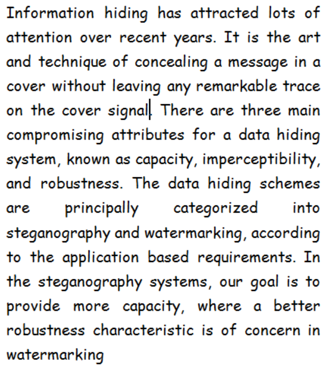
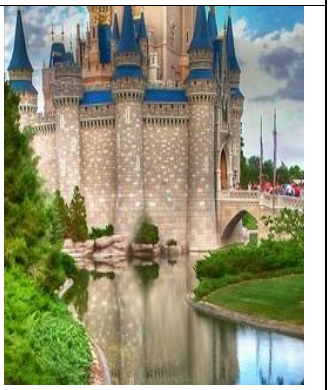
$$\Delta\tau_{ij}^{c} = \begin{cases} Q/Lc; & \text{if ant c used connection (i, j) in its tour} \\ 0\ ; & \text{otherwise} \end{cases}$$

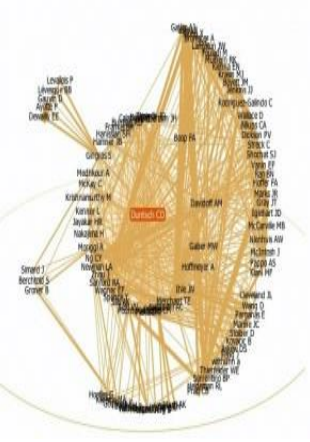
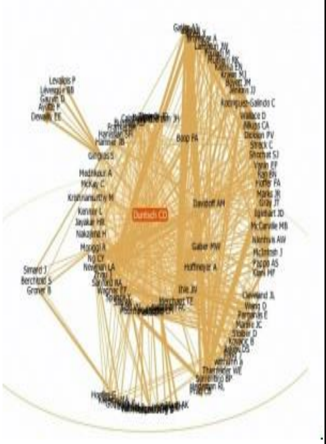
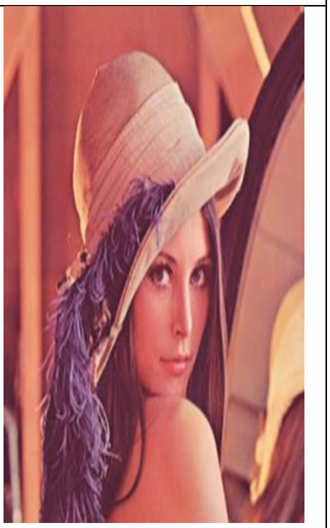
4. Results and Discussion

Our proposed approach has been validated by experimenting with variations of the images. The proposed system has been implemented in Visual Studio 2010, with .NET Framework Version 4.0 using the language of C# windows application. The experiment has been conducted several test images by taking RGB cover images of dimension 512x512. Table 1 shows the original images, secret data and stego images. From the above defined experimental results, we can observe that after secret data embedded, there is no visual difference from the original image. Hence, the existence of the embedded message will not be known to the unauthorized users.

Various performance metrics were also verified from the resultant image such as the Peak- Signal – Noise – Ratio, between the original image and this can further be proved from the Peak-Signal-to-Noise-Ratio (PSNR) between final images and original images.

TABLE I
EXPERIMENTAL RESULTS OF THE PROPOSED TECHNIQUE

Original Image	Sample Secret Data	Stego Image
	 Information hiding has attracted lots of attention over recent years. It is the art and technique of concealing a message in a cover without leaving any remarkable trace on the cover signal. There are three main compromising attributes for a data hiding system, known as capacity, imperceptibility, and robustness. The data hiding schemes are principally categorized into steganography and watermarking, according to the application based requirements. In the steganography systems, our goal is to provide more capacity, where a better robustness characteristic is of concern in watermarking	

	The term steganography is not new today. In fact several examples from the times of ancient Greece are available in Kahn. In recent years, everything is trending toward digitalization and with the rapid development of the Internet technologies, digital media can be transmitted conveniently over the network. Therefore, messages need to be transmitted secretly through the digital media by using the steganography techniques. Steganography differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret.	
	The word steganography is original from the Greek language words „stegos grafia' the meaning is „ covered or concealed writing. In image steganography the information is secreted entirely in images. Steganography is the ability and skill of hidden way of communication. This is fulfilled during hiding secret information in any other information, as a result concealing the presence of the communicated information data.	
	The rapid growth of internet usage over high bandwidth and low cost computer hardware has propelled the explosive growth of steganography. In the present year, secure and hidden communication is the foremost requirement of the people. Therefore steganography is gaining attraction by people due to the security issues over internet. Steganography means covert writing. Steganography has evolved into a digital strategy of hiding a file in some form of multimedia, such as an image, an audio file or even a video file.	

5. Performance Evaluation

For comparing stego image with cover results requires a measure of image quality, commonly used measures Peak Signal-to-Noise Ratio [12]. If SNR and PSNR represent smaller value, then it indicates there is a large between the original (without noise) and distorted image. The main advantage of this measure is ease of computation, but it does not reflect perceptual quality. An important property of PSNR is that a slight spatial shift of an image can cause a large numerical distortion but, there would be no visual distortion and conversely, a small average distortion can result in a damaging visual artifact, if all the error is concentrated in a small important region. The performance values the PSNR calculated from the output image is compared with the PSNR values provided in the existing techniques, in the following tables 2.

TABLE II
COMPARISON BETWEEN EXISTING AND PROPOSED TECHNIQUE BASED ON PSNR

Cover Image	Size	Proposed Algorithm
Sailboat	256x256	65.6274
Goldhill	300x256	66.0808
Peppers	400x400	69.4901
Lena	512x512	71.6319

6. Conclusion

The proposed method is used to increase high capacity and optimized image steganography technique based on ant colony optimization algorithm. The ACO algorithm can find good solutions efficiently even though the search space is so large. Our experimental results show the proposed method provides acceptable image quality and secret message capacity. In future, some data encryption technique can be applied along with ABC to increase the security level. It may also be possible to optimize the fitness function of the current ABC algorithm. Algorithms like AFS and BFO can also be tried to view their performance with respect to the proposed method.

References

[1] Adi Shamir, “How to share a secret”, Communications of the ACM, vol. 22, no. 11, page(s): 612–613, 1979.

[2] 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.

[3] Shankar, K., & Eswaran, P. (2015). ECC based image encryption scheme with aid of optimization technique using differential evolution algorithm. Int J Appl Eng Res, 10(55), 1841-5.

[4] K. Sathesh Kumar, K. Shankar, M. Ilayaraja, M. Rajesh, “Sensitive Data Security in Cloud Computing Aid of Different Encryption Techniques”, Journal of Advanced

Research in Dynamical and Control Systems, Volume. 9, Issue. 18, page(s): 2888-2899, December 2017.

[5] K.Shankar, Lakshmanaprabu S. K, “Optimal key based homomorphic encryption for color image security aid of ant lion optimization algorithm”, International Journal of Engineering & Technology, Volume. 7, Issue. 9, page(s): 22-27, 2018.

[6] Shankar, K., & Eswaran, P. (2016). An efficient image encryption technique based on optimized key generation in ECC using genetic algorithm. In Artificial Intelligence and Evolutionary Computations in Engineering Systems (pp. 705-714). Springer, New Delhi.

[7] Shankar, K., & Eswaran, P. (2016). RGB-Based Secure Share Creation in Visual Cryptography Using Optimal Elliptic Curve Cryptography Technique. Journal of Circuits, Systems and Computers, 25(11), 1650138.

[8] Shankar, K., & Eswaran, P. (2017). RGB based multiple share creation in visual cryptography with aid of elliptic curve cryptography. China Communications, 14(2), 118-130.

[9] M. Ilayaraja, K. Shankar and G. Devika, “A Modified Symmetric Key Cryptography Method for Secure Data Transmission”, International Journal of Pure and Applied Mathematics, Volume 116, Issue. 10, page(s): 301-308, October 2017.

[10] K.Shankar. “An Optimal RSA Encryption Algorithm for Secret Images”, International Journal of Pure and Applied Mathematics, Volume 118, No. 20 page(s): 2491-2500, 2018.

[11] Nur Aminudin, Andino Maseleno, K.Shankar, S. Hemalatha, K. Sathesh kumar, Fauzi, Rita Irviani, Muhamad Muslihudin, “Nur Algorithm on Data Encryption and Decryption”, International Journal of Engineering & Technology, Volume. 7, Issue-2.26, page(s): 109-118, June 2018.

[12] K. Shankar, G. Devika and M. Ilayaraja, “Secure and Efficient Multi-Secret Image Sharing Scheme based on Boolean Operations and Elliptic Curve Cryptography”, International Journal of Pure and Applied Mathematics, Volume 116, Issue. 10, page(s): 293-300, October 2017.

[13] Shankar, K., & Eswaran, P. (2015). A secure visual secret share (VSS) creation scheme in visual cryptography using elliptic curve cryptography with optimization technique. Australian Journal of Basic & Applied Science, 9(36), 150-163.

[14] K.Shankar and P.Eswaran, “A New k out of n Secret Image Sharing Scheme in Visual Cryptography”, 2016 10th International Conference on Intelligent Systems and Control (ISCO), IEEE, page(s): 369–374, 2016.

[15] Pandi Selvam Raman, K.Shankar, Ilayaraja M, “Securing cluster based routing against cooperative black hole attack in mobile ad hoc network”, International Journal of Engineering & Technology, Volume. 7, Issue. 9, page(s): 6-9, 2018.

[16] B.suneetha, Secured Data Transmission Using Video Steganographic Scheme , Int. Journal of Engineering Research and Applications, Vol. 4, Issue.7, pp.243-246, 2014.

[17] Cox, Ingemar, et al. Digital watermarking and steganography. Morgan Kaufmann, 2007.

[18] Anjali Tiwari, Seema Rani Yadav and N.K. Mittal,A Review on Different Image Steganography Techniques, International Journal of Engineering and Innovative Technology (IJEIT), Vol.3, Issue.7, 2014.

[19] Stuti Goel, Arun Rana and Manpreet Kaur, A Review of Comparison Techniques of Image Steganography, Global Journal of Computer Science and Technology Graphics & Vision, Vol.13, Issue 4, 2013.

[20] Amanjot Kaur, Shruti Mittal, Steganography using Social Impact Theory based Optimization (SITO), International Journal of Computer Applications, Vol.101, No.16, 2014.

[21] Bo-Luen Lai and Long-Wen Chang, Adaptive data hiding for images based on harr discrete wavelet transform, Advances in Image and Video Technology, pp: 1085-1093, 2006.

[22] Seyyed Amin Seyyedi and Nick Ivanov, High Payload and Secure Steganography Method Based on Block Partitioning and Integer Wavelet Transform, International Journal of Security and Its Applications, Vol.8, No.4, pp.183-194, 2014.

[23] Elham Ghasemi, Jamshid Shanbehzadeh, Nima Fassihi, "High Capacity Image Steganography usingWavelet Transform and Genetic Algorithm, In Proceedings of international multiconference of engineers and computer scientists, Vol.1, pp.16-18. 2011.

[24] S. Lee, C.D. Yoo and T. Kalker, Reversible image watermarking based on integer-to-integer wavelet transform, IEEE Transactions on Information Forensics and Security, Vol. 2, No.3, pp. 321-330, 2007.

[25] LiFan, Tiegang Gao, QuntingYang, YanjunCao, An extended matrix encoding algorithm for steganography of high embedding efficiency, Volume 37, Issue 6, pp.973-981, 2011.

[26] Souvik Bhattacharyya and Gautam Sanyal, Data Hiding in Images in Discrete Wavelet Domain Using PMM, International Journal of Computer and Information Engineering, Vol.4, No.8, pp.1276-1284, 2010 .

[27] S. Bhattacharyya, A Survey of Steganography and Steganalysis Technique in Image, Text, Audio and Video as Cover Carrier, Journal of Global Research in Computer Science, Volume 2, No. 4, pp.1-16, 2011

[28] N.Vinothkumar and T.Vigneswaran ,Steganographic Method Image Security Based on Optimal Pixel Adjustment Process and Integer Wavelet Transform, International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE), Vol. 2, Issue.3, 2013.

[29] Ching-Sheng Hsu and Shu-Fen Tu. Finding optimal LSB substitution using ant colony optimization algorithm, Communication Software and Networks, 2010. ICCSN'10. Second International Conference on. IEEE, 2010.

[30] Rafael Lima de Carvalho, Warley Gramacho da Silva, Ary Henrique Oliveira de Morais, Optimizing Image Steganography using Particle Swarm Optimization Algorithm, International Journal of Computer Applications, Vol.164, No.7, 2017.

[31] https://en.wikipedia.org/wiki/Ant_colony_optimization_algorithms

[32] Elhoseny, M., Shankar, K., Lakshmanaprabu, S. K., Maseleno, A., & Arunkumar, N. (2018). Hybrid optimization with cryptography encryption for medical image security in Internet of Things. Neural Computing and Applications, 1-15.

[33] Avudaiappan, T., Balasubramanian, R., Pandiyan, S. S., Saravanan, M., Lakshmanaprabu, S. K., & Shankar, K. (2018). Medical image security using dual encryption with oppositional based optimization algorithm. Journal of medical systems, 42(11), 208.

[34] Karthikeyan, K., Sunder, R., Shankar, K., Lakshmanaprabu, S. K., Vijayakumar, V., Elhoseny, M., & Manogaran, G. (2018). Energy consumption analysis of Virtual

Machine migration in cloud using hybrid swarm optimization (ABC–BA). The Journal of Supercomputing, 1-17.

[35] Lakshmanaprabu, S. K., Shankar, K., Khanna, A., Gupta, D., Rodrigues, J. J., Pinheiro, P. R., & De Albuquerque, V. H. C. (2018). Effective Features to Classify Big Data Using Social Internet of Things. IEEE Access, 6, 24196-24204.

[36] Sahu, S., Singh, A. K., Ghrera, S. P., & Elhoseny, M. (2019). An approach for de-noising and contrast enhancement of retinal fundus image using CLAHE. Optics & Laser Technology, 110, 87-98.

[37] Metawa, N., Hassan, M. K., & Elhoseny, M. (2017). Genetic algorithm based model for optimizing bank lending decisions. Expert Systems with Applications, 80, 75-82.

[38] Elhoseny, M., Yuan, X., El-Minir, H. K., & Riad, A. M. (2016). An energy efficient encryption method for secure dynamic WSN. Security and Communication Networks, 9(13), 2024-2031.

[39] Elhoseny, M., Elminir, H., Riad, A., & Yuan, X. (2016). A secure data routing schema for WSN using elliptic curve cryptography and homomorphic encryption. Journal of King Saud University-Computer and Information Sciences, 28(3), 262-275.

[40] Elhoseny, M., Elminir, H., Riad, A. M., & Yuan, X. I. A. O. H. U. I. (2014). Recent advances of secure clustering protocols in wireless sensor networks. International Journal of Computer Networks and Communications Security, 2(11), 400-413.

[41] Elhoseny, M., Elleithy, K., Elminir, H., Yuan, X., & Riad, A. (2015). Dynamic clustering of heterogeneous wireless sensor networks using a genetic algorithm towards balancing energy exhaustion. International Journal of Scientific & Engineering Research, 6(8), 1243-1252.

[42] Elhoseny, M., Yuan, X., Yu, Z., Mao, C., El-Minir, H. K., & Riad, A. M. (2015). Balancing energy consumption in heterogeneous wireless sensor networks using genetic algorithm. IEEE Communications Letters, 19(12), 2194-2197.

[43] Fang, B., Guo, X., Wang, Z., Li, Y., Elhoseny, M., & Yuan, X. (2019). Collaborative task assignment of interconnected, affective robots towards autonomous healthcare assistant. Future Generation Computer Systems, 92, 241-251.