www.ijemr.net ISSN (ONLINE): 2250-0758, ISSN (PRINT): 2394-6962

Volume-7, Issue-3, May-June 2017

International Journal of Engineering and Management Research

Page Number: 221-223

Data Hiding and Security using Steganography

Akshyata[1], Kajol Jain[2]
[1,2]Department of Computer Science, INDIA

ABSTRACT

Communication has to be secure in order to be kept private. The latest developments in the field of digital communication have made secret communication possible. Image hiding is a method in which a secret image is hidden in a cover image thereby forming a hybrid or stego image. In this project, data hiding is performed by taking difference value of three and two neighbouring pixels. But the data is only hidden in edge pixels of the image. *Ant colony optimization* (ACO) is an optimization algorithm inspired by the natural behaviour of ant species that ants deposit pheromone on the ground for foraging. In this project, ACO is used to tackle the image edge detection problem. The proposed ACO-based edge detection approach is able to establish a pheromone matrix that represents the edge information presented at each pixel position of the image, according to the movements of a number of ants which are dispatched to move on the image. Furthermore, the movements of these ants are driven by the local variation of the image's intensity values. This method enhances security and the quality of image in spite of high capacity of concealed information. Error correction mechanism using hamming code is applied to ensure reliable secret communication.

Keywords-- Stegananography, compression,Pheromone, embedding

I. INTRODUCTION

Steganography is the science of invisible communication. Information is transmitted by hiding it in innocuous cover objects to maintain security and confidentiality. In image steganography the cover object is the image and information is embedded in to images which may be colour, greyscaleobinary. A stego image is obtained from the cover image by accommodating the secret message into a digital image using some embedding algorithm that slightly modifies the cover image.

Digital Image Steganographic techniques have grown enormously in order to enhance the security in a communication channel. The stego-image is later transmitted via a public channel. The public channel can have many trespassers who will want to disrupt the data flow from the sender to the receiver or might want to extract the data transmitted without the knowledge of the communicating parties. An effective steganographic scheme has to be implemented that thwarts the attacker from extracting the secret information during transmission and reception.

In this project, ACO is introduced to tackle the image edge detection problem, where the aim is to extract the edge information presented in the image, since it will be used to embed secret data. The proposed approach exploits a number of ants, which move on the image driven by the local variation of the image's intensity values, to establish a pheromone matrix, which represents the edge information at each pixel location of the image. ACO aims to iteratively find the optimal solution of the target problem through a guided search (i.e., the movements of a number of ants) over the solution space, by constructing the *pheromone* information.

II. METHODOLOGY

Firstly, relevant data was collected and various research papers were analyzed and formulation of the project was done accordingly.

User needs to run the application. The user has two tab options – encrypt and decrypt. If user select encrypt, application give the screen to select image file, information file and option to save the image file. If user select decrypt, application gives the screen to select only image file and ask path where user want to save the secrete file.

This project has two methods – Encryption and Decryption.

In encryption the secret information is hidden within the image file.

Decryption is extracting the secret information from the image file.

III. PRIOR APPROACH

ISSN (ONLINE): 2250-0758, ISSN (PRINT): 2394-6962

METHODS ANALYZED:

1.LSB substitution method:

We study plenty of papers where LSB-based methods is used which directly embed the secret data into the spatial domain in an unreasonable way without taking into consideration the difference in hiding capacity between edge and smooth areas. This makes data detection more vulnerable. Majority of the time, authors have adopted Raster scan for data embedding and extracting processes. It traverse the image pixels from left to right and top to bottom so there is a possibility of vulnerability of secret data threat.

2.Zig- Zag PVD method:

Wu and Tsai presented steganographic scheme that offers high imperceptibility to the stego-image by selecting two consecutive pixels as the object of embedding. The payload of Wu and Tsai's scheme is determined by the difference value between the pixels.

But this scheme also lacks in giving required result because If random scan is employed instead of raster scan in secret data embedding, the effectiveness can be improved significantly.

IV. OUR APPROACH

Image Edge Detection Using Ant Colony Optimization Algorithm (most appropriate)

After analyzing various above research papers we found out that above methods not provide security as per need. In these, data can be fetched easily from LSB bit and cross pixels which makes hiding process vulnerable.

In general, the alteration tolerance of an edge area is higher than that of a smooth area so, an edge area can conceal more secret data than a smooth area and also difficult to detect.

So we used ACO method as:

Proposed solution

The proposed method is found to be more secure as randomly pixels are selected for embedding so it will not be possible for attacker to determine that particular random sequence of pixels.

Edges have been detected successfully using ACO(Ant Colony Optimization) algorithm.

Then embedding has been done behind those edges. Hamming code is applied to the message to be sent to enhance the security.

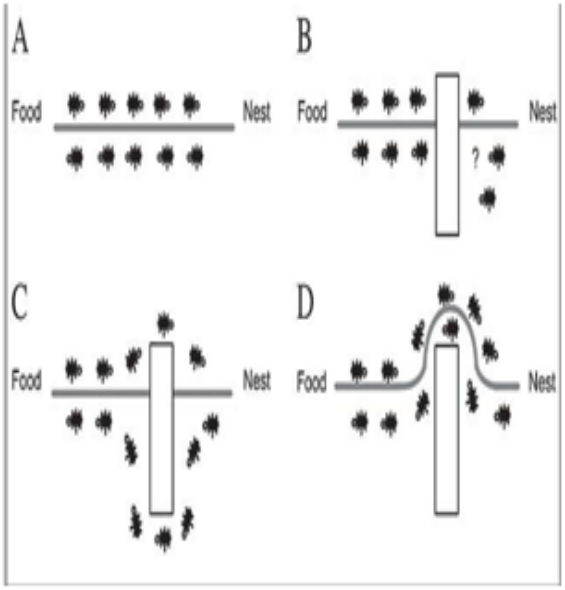
At the time of extraction successfully original message has been extracted.

HOW ACO WORKS:

Ant colonies, and more generally social insect societies, are distributed systems that, in spite of the simplicity of their individuals, present a highly structured social organization. As a result of this organization, ant colonies can accomplish complex tasks that in some cases far exceed the individual capabilities of a single ant. The field of ''ant algorithms'' studies models derived from the observation of real ant's behaviour, and uses these models as a source of inspiration for the design of novel algorithms for the solution of optimization and distributed control problems.

While walking from food sources to the nest and vice versa, ants deposit pheromones on the ground, forming in this way a pheromone trail. Ants can smell the pheromone and they tend to choose, probabilistically, paths marked by strong pheromone concentrations.

In figure B an obstacle interrupts the movement of ants. Initially there are equal numbers of ants on both paths since ants using first path will reach first hence amount of pheromones will be more on that path at the time of returning ants again sense the pheromone and chose the smaller one again. Since ants of second path has not reached yet so there will no pheromone on that path Eventually all ants will chose the path with more pheromone value and second path will be left out due to pheromone evaporation. Pheromone evaporation: In real ant colonies, pheromone intensity decreases over timebecause of evaporation



ERROR CORRECTION:

HAMMING CODE is run over the secret data.

DATA HIDING:

Data is embedded in the edge pixels only.

Edge pixels are selected randomly.

Message is embedded in 3 planes of a pixel in LSBFig 1.1 The image below shows the original image and image after secret data is embedded i.e, steganographed image. Although, both images appears to be identical but actually they are not.

Fig 1.1Original and Steganographed Images

Fig 1.2 First the original coloured image is converted into grey image as shown below.

.

Fig 1.2 Black and White Image

Fig 1.3 Edges of the grey image are calculated using ACO Algo.This approach is able to establish a pheromone matrix that represents the edge information presented at each pixel position of the image, according to the movements of a number of ants which are dispatched to move on the image. Furthermore, the movements of these ants are driven by the local variation of the image's intensity values.

Fig 1.3 Image after Edges Detection

V. CONCLUSION

Edges have been detected successfully using ACO (Ant Colony Optimization) algorithm.Then embedding has been done behind those edges. Hamming code is applied to the message to be sent to enhance the security.At the time of extraction successfully original message has been extracted.The proposed method is found to be more secure as randomly pixels are selected for embedding so it will not be possible for attacker to determine that particular random sequence of pixels

REFERENCES

[1] M. Dorigo and S. Thomas, *Ant Colony Optimization*. Cambridge: MIT Press, 2004.
[2] H.-B. Duan, *Ant Colony Algorithms: Theory and Applications*. Beijing: Science Press, 2005.
[3] M. Dorigo, V. Maniezzo, and A. Colorni, "Ant system: Optimization by a colony of cooperating agents," *IEEE Trans. on Systems, Man andCybernetics, Part B*, vol. 26, pp. 29–41, Feb. 1996.
[4] M. Dorigo, M. Birattari, and T. Stutzle, "Ant colony optimization," *IEEE Computational Intelligence Magazine*, vol. 1, pp. 28–39, Nov. 2006.
[5] C.K. Chan, L.M. Chen, Hiding data in images by simple LSB substitution, Pattern Recognition 37 (3) (2004) 469–474.
[6] Chang, C.C., Tseng, H.W., 2004. A steganographic method for digital images using side match. Pattern Recognition Letter 25 (September), 1431–1437.
[7] Chang, C.C., Hsiao, J.Y., Chan, C.S., 2003. Finding optimal least-significant-bit substitution in image hiding by dynamic programming strategy. Pattern Recognition 36 (July), 1583 – 1595.
[8] Fridrich, J., Goljan, M., Du, R., 2001. Reliable detection of LSB steganography in color and grayscale images.In:Proceedings of ACM Workshop on Multimedia and Security