Steganography Based on Bacterial Foraging Optimization

Divya Malhotra[1] Er. Ravi Malik[2]
[1]M.tech Student [2]Assistant Professor
[1,2]Geeta Engineering College

Abstract— Steganography is the ability of hiding the very occurrence of communiqué by embedding secret messages into innocent looking cover up documents, such as digital images. Recognition of steganography, evaluation of message length, and its extraction belong to the field of steganalysis, which is actually a route for perceiving Stegnography. Bacterial foraging optimization (BFO) is a optimization technique projected by K.M. Passino in 2002, and is one of the latest techniques under Swarm Intelligence. To covenant with multifarious exploration problems of the real world, scientists have been drawing inspiration from environment and natural creatures for years. Bacterial foraging optimization is a burgeoning nature inspired procedure to find the finest elucidation of the problem. In this paper an algorithm for perceiving Steganography has been introduced using the BFO Technique. The test to the RGB model based imagery through the proposed algorithm will help out to detect if something is steganographed in the image or not.

Keywords: Swarm Intelligence, Bacteria Foraging Optimization, Steganography and Steganalysis

I. INTRODUCTION

A. *Swarm Intelligence*

Swarm intelligence is the emergent collective intelligence of groups of simple autonomous agents. Here, an autonomous agent is a subsystem that interacts with its environment, which probably consists of other agents, but acts relatively independent from all other agents.

B. *Bacterial Foraging Optimization:*

The course of action of likely choice tends to eradicate animals with poor foraging strategies (methods for locating, handling, and ingesting food) and support the propagation of genes of those animals that have successful foraging strategies, since they are more likely to enjoy reproductive sensation (they obtain enough food to enable them to reproduce).

C. *Steganography*

It is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the message.

D. *Steganalysis*

It is the art of identifying stegogrammes that contain a surreptitious message. Steganalysis does not however consider the successful mining of the message; this is usually a requirement for cryptanalysis.

II. TECHNIQUE USED: BFO

The Bacterial Foraging system consists of four principal mechanisms, namely chemotaxis, swimming, reproduction and elimination-dispersal.

A. *Chemo taxis*

This process simulates the movement of an E.coli cell through swimming and tumbling via flagella. Biologically an E.coli bacterium can move in two different ways. In the original BFO, a unit walk of the bacteria with random direction represents a "tumble" and a unit walk with the same direction in the last step indicates a "run".

B. *Reproduction*

The least healthy bacteria eventually die while each of the healthier bacteria (those yielding lower value of the objective function) asexually split into two bacteria, which are then placed in the same location. This keeps the swarm size constant. In the reproduction step only the first half of the population survives.

C. *Elimination and Dispersal*

Gradual or sudden changes in the local environment where a bacterium population lives may occur due to various reasons e.g. a significant local rise of temperature may kill a group of bacteria that are currently in a region with a high concentration of nutrient gradients. Events can take place in such a fashion that all the bacteria in a region are killed or a group is dispersed into a new location.

Fig. 1: swimming , tumbling and chemo tactic behavior of E.coli

III. CHALLENGES

Steganography has a wide array of uses. It can be used for digital watermarking, E-commerce, and the transport of sensitive data. Steganography involves embedding hidden watermarks, or identification tokens, into an image or file to show ownership. Steganography can also be employed in following areas:

Encoding Secret Messages in Text
Encoding Secret Messages in Images
Encoding Secret Messages in Audio

IV. STEGANOGRAPHY

In modern terms, steganography is usually implemented computationally, where cover Works such as text files, images, audio files, and video files are tweaked in such a way that a secret message can be embedded within them .The techniques are very similar to that of digital watermarking. Steganography on the other hand, focuses on making it extremely difficult to tell that a secret message exists at all. If an unauthorized third party is able to say with high confidence that a file contains a secret message, then

steganography has failed. Steganography also differs from cryptography because the latter does not attempt to hide the fact that a message exists.

A. How is steganography used?

Steganography is the dark cousin of cryptography, the use of codes. While cryptography provides privacy, steganography is intended to provide secrecy.

The goal of cryptography is to make data unreadable by a third party, the goal of steganography is to hide the data from a third party.

Hiding a secret photo in a cover picture is even easier. Line them up, pixel by pixel. Take the important four bits of each color value for each pixel in the secret photo (the left ones). Replace the unimportant four bits in the cover photo (the right ones). The cover photo won't change much, you won't lose much of the secret photo, but to an untrained eye you're sending a completely innocuous picture.

An encrypted file may still hide information using steganography, so even if the encrypted file is deciphered, the hidden message is not seen.

When a steganographic system is developed, it is important to consider what the most appropriate cover Work should be, and also how the stegogramme is to reach its recipient. The embedding process is concerned with hiding a secret message within a cover work, and is the most carefully constructed process of the two. A great deal of attention is paid to ensuring that the secret message goes unnoticed if a third party were to intercept the cover Work. The extracting process is traditionally a much simpler process as it is simply an inverse of the embedding process, where the secret message is revealed at the end.

Fig. 2: Steganography Sudoku View

(1) Secret Message- It is usually a text file that contains the message you want to transfer.
(2) Cover Work- It is used to construct a stegogramme that contains a secret message The next step is to pass the inputs through the Stego-system Encoder. The stego-system encoder will usually require a key to operate, and this key would also be used at the extraction phase. This is a security measure designed to protect the secret message.

V. PROPOSED WORK

The presented work will cover the following objectives:

- Study of BFO architecture respective to Image processing.
- Define a BFO based algorithm to identify the high intensity area where the data will be stored
- Store the digital content in Input image using proposed algorithm.

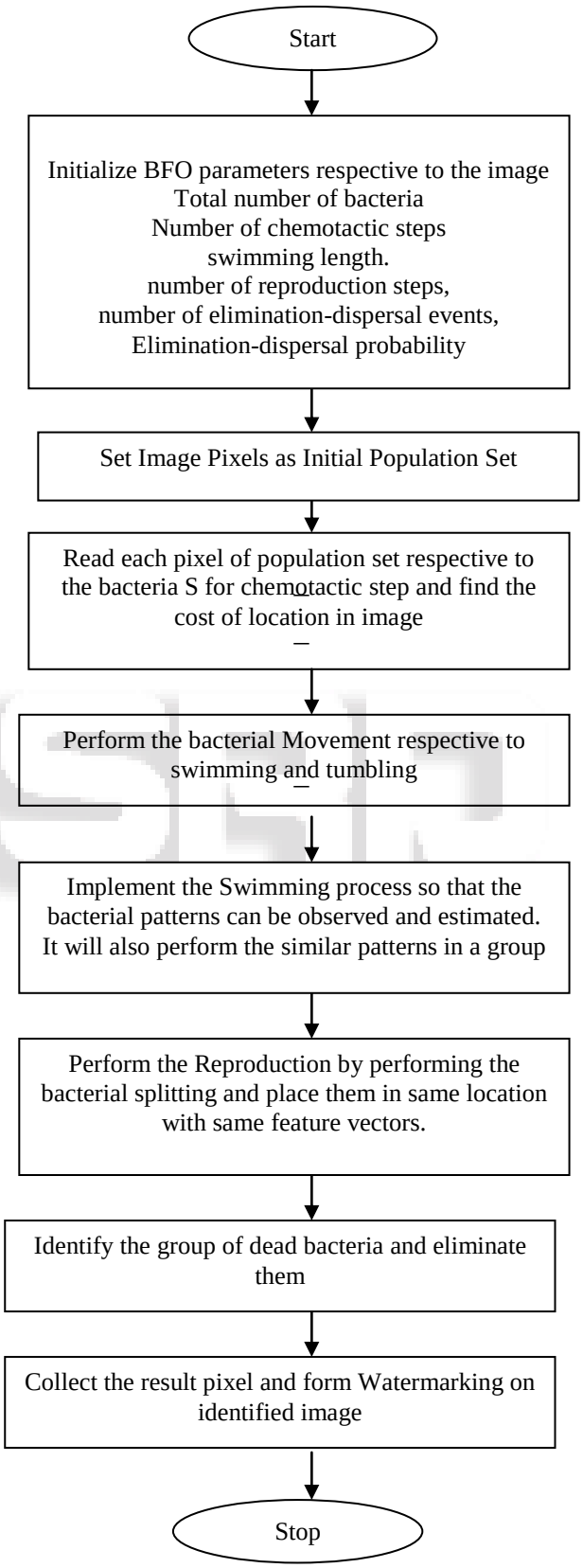

Fig. 1: Flow of Presented Work

- To perform the extraction back from the Stegano-image.
- To analyze the effectiveness of the work under different parameters
- Analyze the work under different Attacks

VI. EXISTING WORK

In this work, A BFO based approach is presented to identify the high intensity areas over the image so that the data can be hide in these extracted areas.The presented work is divided in two main layers. In first layer, the BFO is applied over the image to identify the valid areas where data can stored effectively. Once the areas are identified, the embedding of data over the cover image is performed. The work is about the design of a algorithm based on BFO to hide data in digital images. The presented work is implemented in matlab environment. The results shows the significant results in terms of data strorage and successful reterival. The work is also tested under different kind of attacks. The results shows the robustness of proposed work under these attacks.

VII. RESULTS

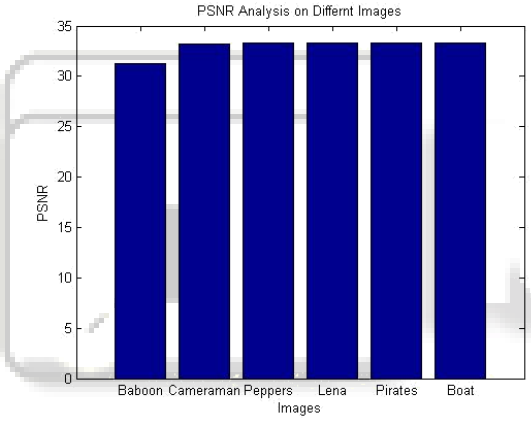

Fig. 3: PSNR Analysis on Different Images

Higher the PSNR value, more effective the results will be.

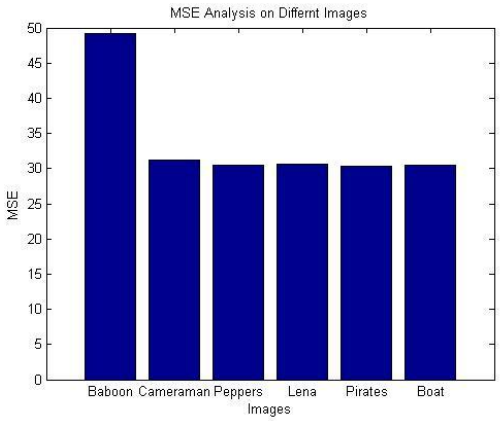

Fig. 4: MSE Analysis on Different Images

Lower the MSE value, more effective the results will be.

As the stegno image has been changed because of presented work. The differences in the source and the result image is shown.

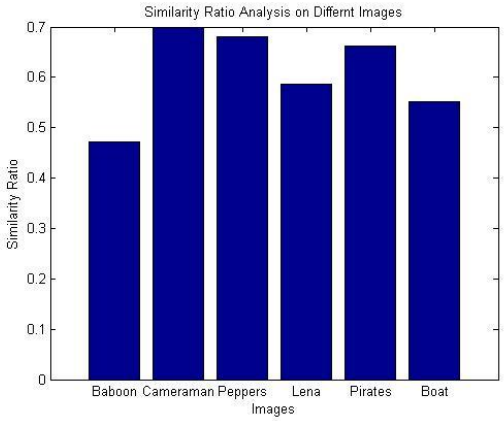

Fig. 5: Similarity Analysis on Different Images

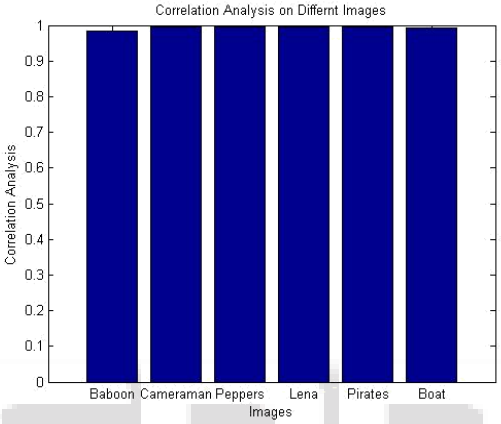

Fig 6: Correlation Analysis on Different Images

VIII. CONCLUSION

Steganography can be used for hidden communication. A stego-key has been applied to the system during embedment of the message into the cover image. This steganography application software provided for the purpose to how to use any type of image formats to hiding any type of files inside there.

REFERENCES

[1] E. Shaw, “The schooling of fishes," Sci. Am., vol. 206, pp. 128-138, 1962.
[2] E. Bonabeau, M. Dorigo, and G. Theraulaz, Swarm Intelligence: From Natural to Articial systems. NY: Oxford Univ. Press, 1999.
[3] R. Arkin, Behavior-Based Robotics. Cambridge, MA: MIT Press, 1998.
[4] N.Provos. "Defending against Statistical Steganalysis", Proceedings of the 10 USENIX Security Symposium, vol.10, pp.323-335, 2001.
[5] N.Provosand P.Honeyman. "Hide and Seek: An Introduction to Steganography", IEEE: Security & Privacy, vol.1, pp.32-44, 2003.
[6] S. Dumitrescu, X.Wu, and Z.Wang. "Detection of LSB Steganography via Sample Pair Analysis", Lecture Notes in Computer Science, vol.2578, pp.355-372, and 2003.
[7] H.Farid. "Detecting Hidden Messages Using Higher-Order Statistical Models", Proceedings of the

International Conference on Image Processing, Rochester, NY, USA, 2002.
[8] J. Fridrich, M. Goljan, and D.Hogea. "Attacking the Out Guess", Proceedings of the Information Hiding Workshop on Multimedia and security 2002, Juan-les-Pins, France, 2002.
[9] Johnson, N.F. and Jajodia S. (1998) "Exploring steganography: Seeing the unseen", IEEE Computer, vol. 31(2),(1998), pp.26-34.
[10] Kasmani, S., & Naghsh-Nilchi A. (2008) "A New Robust Digital Image Watermarking Technique Based on Joint DWT-DCT Transformation", Convergencef

