Volume 4, Issue 7, July 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Review paper on- Route to Perceive Steganography

Divya Malhotra
M.TECH Student,
Geeta Engineering. College
Panipat, Haryana ,India

Ravi
Head of Department
Engineering. College ,E,
India

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 Stegnography 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 Stegnographed in the image or not.

Keywords—Swarm Intelligence, Bacteria Foraging Optimization, stegnography and steganalysis.

I. NTRODUCTION

Swarm Intelligence: Long time before, people discovered many different and interesting insect or animal behaviors in the nature. A flock of birds sweeps across the sky. A group of ants forages for food. A school of fish swims, turns, flees together, etc.. We call this kind of aggregate motion “swarm behavior." Recently biologists, and computer scientists in the field of “artificial life" have studied how to model biological swarms to understand how such “social animals" interact, achieve goals, and evolve. Moreover, engineers are increasingly interested in this kind of swarm behavior since the resulting “swarm intelligence" can be applied in optimization (e.g. in telecommunicate systems), robotics], traffic patterns in transportation systems, and military applications. 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.

Bacterial Foraging Behaviour : 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). After many generations move on, poor foraging strategies are either eliminated or shaped into good ones (redesigned).Plausibly, such evolutionary principles have led scientists in the field of foraging theory to hypothesize that it is appropriate to model the activity of foraging as an optimization practice: a foraging animal takes actions to maximize the energy obtained per unit time spent foraging, in the face of constraints presented by its own physiology(e.g., sensing and cognitive capabilities) and environment(e.g., density of prey, risks from predators, physical characteristics of the search area). Evolution has evenhanded these constraints and essentially engineered what is sometimes referred to as an optimal foraging policy (such terminology is especially justified in cases where the models and policies have been ecologically validated).Optimization models are also valid for social foraging where groups of animals communicate to courteously forage.

Steganography: The term Steganography refers to the knack of clandestine interactions. By implementing steganography ,it is possible for Alice to send a secret message to Bob in such a way that no one else will know that the message exists. Classically, the message is rooted within another item known as a face Work, by tuning its properties. The resulting output, known as a stegogramme is engineered such that it is a near identical perceptual model of the face Work, but it will also contain the hidden message. It is this stegogramme that is sent between Alice and Bob. If anybody intercepts the message, they will obtain the stegogramme, but as it is so similar to the cover, it is a difficult task for them to tell that the stegogramme is anything but above suspicion. It is therefore the duty of steganography to ensure that the opposition regards the stegogramme and thus, the communication-as inoffensive.

Steganalysis: Steganalysis 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. Typically, steganalysis begins by identifying any artifacts that exist in the suspect case as a result of embedding a message. None of the steganographic systems that are known today achieve perfect defense, and this means that they all leave hints of

embedding in the stegogramme. This gives the steganalyst a useful way in to identifying whether a secret message exists or not.

II. THE TECHNIQUE USED: BFO

The Bacterial Foraging system consists of four principal mechanisms, namely chemotaxis, swarming, reproduction and elimination-dispersal. A brief description of each of these processes along with the pseudo-code of the complete algorithm is described below.

1. ***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. It can swim for a period of time in the same direction or it may tumble, and alternate between these two modes of operation for the entire life time [8]. 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". Suppose $ø^i$ *(j, k ,l)* represents the bacterium at j^{th} chemo tactic ,k^{th} reproductive, and l^{th} elimination-dispersal step. Let N_c be the length of the life time of the bacteria's measured by number of chemo tactic steps taken by them during their life cycle, C(i) is the chemo tactic step size during each run or tumble (i.e., run-length unit). Then in each computation chemo tactic step, the movement of the i^{th} bacterium can be represented as

   $$ø^i (j+1,k,l) = ø^i (j, k, l) + c(i)\, \Delta(i) / \sqrt{\Delta^T (i)\, \Delta (i)}$$

   where Δ(i) is the direction vector of the jth chemo tactic step. When the bacterial movement is run , Δ(i) is the same with the last step; otherwise , Δ(i) is random vector whose elements lie in [-1,1].

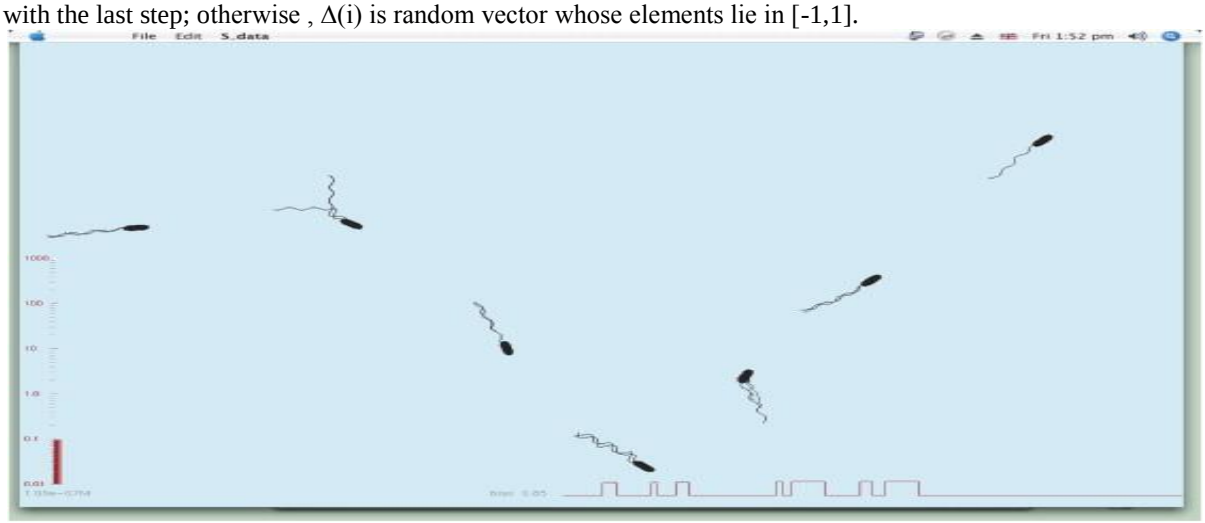

Figure 1 : swimming , tumbling and chemo tactic behavior of E.coli

If at $ø^i$ (j+1,k,l) the cost is better (lower)than $ø^i$ (j,k,l) then another step of size c(i) will be taken in the same direction, again, if that step resulted in a position with a better cost value than at the previous step, another step is taken. This swim is continued as long as it continues to reduce the cost, but only upto a maximum number of steps,[Ns] this represents that the cell will tend to keep moving if it is headed in the direction of increasingly favorable environments.

2. ***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. All bacteria are stored in descending order according to health status. In the reproduction step only the first half of the population survives. The surviving population is divided into two identical ones, which are then placed in the same locations at which their parents were. Thus the total population of bacteria keeps constant.

3. ***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. To simulate this phenomenon in BFOA some bacteria are liquidated at random with a very small probability while the new replacements are randomly initialized over the search space.

What is the effect of elimination and dispersal events on chemotaxis? They have the effect of possibly destroying chemotactic progress, but they also have the effect of assisting in chemotaxis, since dispersal may place bacteria near good food sources. From a broad perspective, elimination and dispersal are parts of the population-level long-distance motile behavior.

III. STEGNOGRAPHY

One of the oldest examples of steganography dates back to around 440BC in Greek History. Herodotus, a Greek historian from the 5 Century BC, revealed some examples of its use in his work entitled "The Histories of Herodotus". One

elaborate example suggests that Histaeus, ruler of Miletus, tattooed a secret message on the shaven head of one of his most trusted slaves. After the hair had grown back, the slave was sent to Aristagorus where his hair was shaved and the message that commanded a revolt against the Persians was revealed. In this example, the slave was used as the carrier for the secret message, and anyone who saw the slave as they were sent to Aristagorus would have been completely unaware that they were carrying a message. As a result of this ,the message reached the recipient with no suspicion of covert communication ever being raised. 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, however one big distinction must be highlighted between the two. In digital watermarking, the focus is on ensuring that nobody can remove or alter the content of the watermarked data, even though it might be plainly obvious that it exists. 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. Instead, cryptography merely obscures the integrity of the information so that it does not make sense to anyone but the creator and the recipient. The adversary will be able to see that a message exists, and the inverse process of cryptanalysis involves trying to turn the meaningless information into its original form. With this said, it is still highly likely that a complete steganographic system might employ cryptographic measures as a safety net to protect the content of the message in the event that the steganographyis broken.

How is Steganography Used?

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. With the Internet offering so much functionality, there are many different ways to send messages to people without anyone knowing they exist. For example, it is possible that an image stegogramme could be sent to a recipient via email. Alternatively it might be posted on a web forum for all to see, and the recipient could log on to the forum and download the image to read the message. Of course, although everyone can see the stegogramme, they will have no reason to expect that it is anything more than just an image. In terms of development, Steganography is comprised of two algorithms, one for embedding and one for extracting. 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.

Figure 2: Stegnography Sudoku View

1. Secretmessage- usually a text file that contains the message you want to transfer

2. CoverWork used to construct a stegogramme that contains a secret message The next step is to pass the inputs through the Stego-system Encoder, which will be carefully engineered to embed the message within an exact copy of the cover Work, such that minimum distortion is made; the lower the distortion, the better the chances of undetectability. 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. Without a key, it would be possible for someone to correctly extract the message if they managed to get hold of the embedding or extracting algorithms. However, by using a key, it is possible to randomize the way the stego-system encoder operates, and the same key will need to be used when extracting the message so that the stego system decoder knows which process to use. This means that if the algorithm falls into enemy hands, it is extremely unlikely that they will be able to extract the message successfully. The resulting output from the stego-system encoder is the stegogramme, which is designed to be as close to the cover Work as possible, except it will contain the secret message. This stegogramme is then sent over some communications channel along with the key that was used to embed the message. Both the stegogramme and the key are then fed into the stego-system decoder where an estimate of the secret message is extracted. Note that we can only ever refer to the output of the extraction process as

an estimate because when the stegogramme is sent over a communications channel, it may be subjected to noise that will change some of the values. Therefore, we can never be sure that the message extracted is an exact representation of the original. Also, the recipient will obviously never know what the original message was, and so they have nothing to compare it to when it is extracted. This is probably the most common system of image steganography today, with the focus mainly on developing the stego-system encoder carefully. It is of paramount importance in steganography that the stegogramme contains no trail of embedding a secret message if it is to be successful. In recent years, many steganographic algorithms have been made publicly available, and so it is very easy for anyone with even a limited knowledge of steganography to be able to communicate covertly. Most of the systems make use of everyday images as the basis for the models ,and of course, the information that is hidden within those images can range from anything between harmless gibberish and messages that are a threat to national security. Subsequently, there is a growing concern as to how we can identify whether any image contains steganography, such that we can be sure the technology is not used for the wrong purposes. This counter-activity is referred to as Steganalysis, and much resource and research has been put into determining whether an image is innocent or not.

IV. ROUTE TO PRECIEVE STEGNOGRAPHY IS - STEGANALYSIS

Steganalysis refers to art and science of bias between stego-objects and cover-objects. Steganalysis need to be done without any knowledge of secret key used for embedding and may be even the embedding algorithms. However, message does not have to be gleaned; just its presence is detected.

Figure 3: Image goes uncovered

Basic technique: The quandary is generally handled with statistical examination. A set of basic files of the same type, and supremely from the same source (for example, the same model of digital camera, or if possible, the same digital camera; digital audio from a CD MP3 files have been "ripped" from; etc.) as the set being inspected, are analyzed for various statistics. Some of these are as straightforward as spectrum analysis, but since most image and audio files these days are compressed with lossy compression algorithms, such as JPEG and MP3, they also attempt to look for inconsistencies in the mode this data has been compressed. For example, a common artifact in JPEG compression is "edge ringing", where high-frequency workings (such as the high-contrast edges of black text on a white background) distort neighboring pixels. This deformation is predictable, and simple steganographic indoctrination algorithms will produce artifacts that are detectably unlikely. One case where detection of suspect files is undemanding is when the unique, basic carrier is available for comparison. Comparing the package against the original file will yield the differences caused by encoding the payload—and, thus, the payload can be extracted.

V. APPLICATIONS IN THE FIELD OF BFO, STEGNOGRAPHY AND STEGANALYSIS

The first practical application of **BFO** was done by Passino K.M. "Biomimicry of Bacterial Foraging for Distributed Optimization and Control,". Many more areas of application have been explored ever since, including telecommunications, control, data mining, design, combinatorial optimization, power systems, signal processing, and many others. To date, there are hundreds of publications reporting applications of bacteria foraging optimization. The main objective is to explain how motile behaviors in both individual and groups of bacteria implement foraging and hence optimization.

The applications in the field of **stegnography** and **steganalysis** are as follows: Detection of LSB Steganography via Sample Pair Analysis, Detecting Hidden Messages Using Higher-Order Statistical Models, Steganalysis of JPEG Images:

Breaking the F5 Algorithm, Feature-Based Steganalysis for JPEG Images and Its Implications for Future Design of Steganographic Schemes, JPEG Steganalysis Using Empirical Transition Matrix in Block DCT Domain, Improved Detection of LSB Steganography in Grayscale Images, Category Attack for LSB Steganalysis of JPEG Images, Steganalysis Based on Image Quality Metrics.

VI. CONCLUSIONS AND FUTURE WORK

From the above analysis and basic study of the optimization technique we concluded that BFO algorithm as the data clustering algorithms by implementing swarm behavior. BFO is a clustering algorithm in the areas of mutli-objective, and constraint handling. BFO can be analyzed and studied for future enhancement such that new research could be focused to produce better solution by improving the effectiveness and reducing the limitations. And we are working for image steganalysis based on bacterial foraging technique soon we'll be ready with the working environment of the above mentioned algorithm.

REFRENCES

[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] G. Beni and J.Wang, "Swarm intelligence in cellular robotics systems," in Proceeding of NATO Advanced Workshop on Robots and Biological System,1989.
[5] M.Pachter and P.Chandler,"Challenges of autonomous control," IEEE Control Systems Magazine,pp.92-97, April1998.
[6] Yang Liu and Kevin M. Passino Dept. of Electrical Engineering The Ohio State University "Swarm Intelligence : literature overview", March 2000.
[7] Passino K. M. " Biomimicry of Bacterial Foraging for Distributed Optimization and Control," IEEE Control Systems Magazine, Vol. 22, No. 3, pp. 52-67, June 2002.
[8] Sambarta Dasgupta , Arijit Biswas , Swagatam Das , Bijaya Ketan Panigrahi and Ajith Abraham, "A Micro-Bacterial Foraging Algorithm for High-Dimensional Optimization
[9] Liu Yanfei, Passino K.M., "Biomimicry of Social Foraging Behavior for Distributed Optimization: Models, Principles, and Emergent Behaviors," Journal of Optimization Theory and Applications, Vol. 115, No. 3, pp. 603-628, Dec. 2002.
[10] Beni, G., Wang, J. Swarm Intelligence in Cellular Robotic Systems, Proceed. NATO Advanced Workshop on Robots and Biological Systems, Tuscany, Italy, June 26–30 (1989)
[11] Kaveh, A.; Talatahari, S. (2010). "A Novel Heuristic Optimization Method: Charged System Search". *Acta Mechanica* **213** (3-4): 267–289. doi:10.1007/s00707-009-0270-4.
[12] "Swarm_intelligence"from S. Dumitrescu, X.Wu, and Z.Wang. "Detection of LSB Steganography via Sample Pair Analysis", Lecture Notes in Computer Science, vol.2578, pp.355-372,2003.
[13] H.Farid. "Detecting Hidden Messages Using Higher-Order Statistical Models", Proceedings of the International Conference on ImageProcessing, Rochester ,NY, USA, 2002.
[14] 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,
[15] France,2002.
[16] N.Memon, I.Avcibas, and B.Sankur. "Steganalysis Based on Image Quality Metrics", emph IEEE: Security and Watermarking of Multimedia Contents,vol.4314, 2001.
[17] C.Ming, Z.Ru, N.Xinxin, and Y.Yixian. "Analysis of Current Steganography Tools: Classifications & Features", Intelligent Information Hiding and Multimedia Signal Processing 2006, pp.384-387,2006.
[18] N.Provosand P.Honeyman. "Detecting Steganographic Content on the Internet", CITI Technical Report,vol.1,pp.1-11,2001.
[19] N.Provos. "Defending Against Statistical Steganalysis", Proceedings of the 10 USENIX Security Symposium, vol.10, pp.323-335, 2001.
[20] N.Provosand P.Honeyman. "Hide and Seek: An Introduction to Steganography", IEEE: Security & Privacy, vol.1, pp.32-44, 2003.

