An Extensive Literature Survey on Steganography using Genetic Algorithm

Himani Mehra [1], Dr. Vinod Kapse [2], Prof. Tarun Kumar Sahu[3], Prof. Garima Tiwari[4]
[1]M-Tech Research Scholar, [2] HOD, [3,4]Research Guides
Department of Electronics & Comm., Gyan Ganga Institute of Technology & Sciences, Jabalpur

Abstract-Steganography is derived from the Greek word steganographic which means covered writing. It is the science of secret communication. The objective of steganography is to hide the existence of the message from unauthorized party. The modern secure image steganography presents a task of transferring the embedded information to the destination without being detected by the attacker. Many different carrier formats can be used, but digital images are the most popular because of their frequency on the Internet. For hiding secret information in images, there exist a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points. In the current world we cannot imagine our lives without computers. However with the use of computers a question of secure data transfer appears rather soon. Information coding and cryptography is essential, but efficient privacy has been given by encryption and information hiding methods that can be misused for covering criminal activities. Therefore is important to develop tools and methods for forensic analysis. Steganography and cryptography are normally connected together.

Keywords:- Steganography, Steganalysis, visual cryptography, Genetic Algorithm (GA).

I. INTRODUCTION

Steganography, as art of hiding information, has been known for over 2500 years. Back then steganography was mainly used for diplomatic, military and a very few people used it for personal purposes along with cryptography. Steganography as well as cryptography have a goal to secure transmitted information between the sender and the recipient, but both systems are used in a different way. Cryptography is aimed on transformation of input data into unreadable output. Level of information security depends on the quality of cryptographic algorithm [3] and correct cipher key selection. Steganography has a different approach, stegomessages also referred as steganograms are made in such a way that they do not attract attention to themselves. Even transfer remains undetected if steganography is used correctly. No matter how strong cipher can be used, there is always an attempt to wiretap the crypted message and try to break cipher or recover cipher key. However if it is not possible to determine message itself there is nothing to do. The very best solution for securing messages and transport medium is to use cryptography for transforming message into unintelligible gibberish, referred as cipher text, and steganography to cover a whole message along with transport medium [4].

However there is an email monitor between the terminal and the email gateway which checks all the outgoing emails for viruses as well as its body plus attachments for internal business information. In this case, the security monitor detected that an email attachment contains sensitive VIP customer information [11]. The security department was immediately informed about this incident and the employee will be charged for information fraud.

This means that a skilled user is familiar with the computer security policy and the cracker expects some kind of testing of sent messages. Cryptography is strong in the usage of the key and the message is coded. Sending such an unsecure message can cause attention from people who are not supposed to know the secret message. Steganography helps with the secure transfer of secret messages. It codes a message inside the picture, video file or data stream. If you saw picture with steganographic content, you would not recognize that there is a secret message.

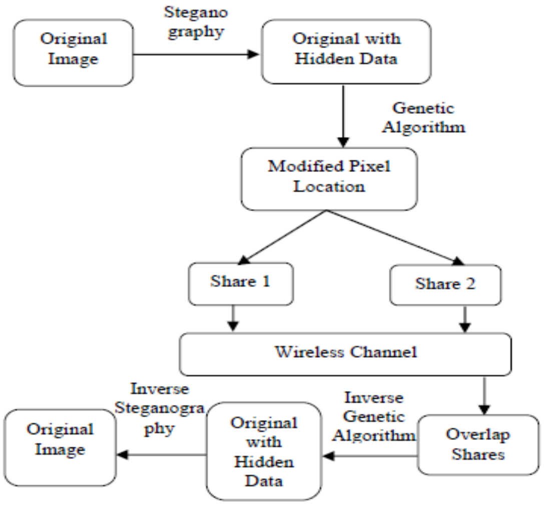

Fig.1. Block Diagram

II. SYSTEM MODEL

In the computer science field of artificial intelligence, a genetic algorithm (GA) is a search heuristic that mimics the process of natural selection. This heuristic (also sometimes called a met heuristic) is routinely used to generate useful solutions to optimization and search problems.[1] Genetic algorithms belong to the larger class of evolutionary algorithms (EA), which generate solutions to optimization problems using techniques inspired by natural evolution, such as inheritance, mutation, selection, and crossover. Genetic algorithms find application in bioinformatics, phylogenetics, computational science, engineering, economics, chemistry, manufacturing, mathematics, physics, pharmacometrics and other fields.

The simplest way to hide binary data on an image is to use a lossless image format (such as a Bitmap) and replace the least significant bits of each pixel in scan lines across the image with the binary data. This is not secure as an attacker can simply repeat the process to quickly recover the hidden information. This technique, known here as “BlindHide” because of the way it blindly hides information, is also not good at hiding – the initial portion of the image is left degraded while the rest remains untouched. The proposed project work consist of mainly two algorithms which are (i) Steganography using Genetic Algorithm (ii) Visual Cryptography with Threshold. The application initiates with Steganography module where the cover image will be encrypted to generate Stego image. The stagnographic image generated in this module will act as an input for visual cryptographic module.

The proposed scheme is based on standard visual cryptography as well as visual secret sharing. The implementation of the algorithm yields in better result with insignificant shares when stego images are normally with light contrast. It can also be seen that the algorithm gives much darker shares in gray output the proposed scheme is based on standard visual cryptography as well as visual secret sharing. The implementation of the algorithm yields in better result with insignificant shares when stego images are normally with light contrast. It can also be seen that the algorithm gives much darker shares in gray output. This algorithm gives better results in terms of image quality and stegnalysis.

III. LITERATURE REVIEW

In the year of 2013 Prema, G.; Natarajan, S.,[1] Investigated on Image steganography is an emerging field of research for secure data hiding and transmission over networks. The proposed system provides the best approach for Least Significant Bit (LSB) based steganography using Genetic Algorithm (GA) along with Visual Cryptography (VC). Original message is converted into cipher text by using secret key and then hidden into the LSB of original image. Genetic Algorithm and Visual Cryptography has been used for enhancing the security. Genetic Algorithm is used to modify the pixel location of stego image and the detection of this message is complex. Visual Cryptography is used to encrypt the visual information. It is achieved by breaking the image into two shares based on a threshold. The performance of the proposed system is experimented by performing steganalysis and conducting benchmarking test for analysing the parameters like Mean Squared Error (MSE) and Peak Signal to Noise Ratio (PSNR). The main aim of this paper is to design the enhanced secure algorithm which uses both steganography using Genetic Algorithm and Visual Cryptography to ensure improved security and reliability.

In the year of 2012 Nickfarjam, A.M.; Azimifar, Z.,[2] studied a novel approach for image steganog-raphy by taking the advantages of Particle Swarm Optimization (PSO) and Least Significant Bits (LSBs) replacement. This technique is based on hiding the Most Significant Bits (MSBs) of secret image pixels in LSBs of a host image. The proposed method finds the best pixel in order to embed. Authors define four feature functions and four corresponding coefficients to rank the pixels. The features and the coefficients are defined based on the MSBs of host image. Their method defines a special secret key for each host image based on PSO in which, each particle represents a potential solution and authors can evaluate all of them. This novelty causes better exploration of search space in order to find suitable pixel ranking and higher security. The experimental outcomes show the superiority of this approach over the state-of-the-art methods.

In the year of 2012 Sanchez, A.; Conci, A.; Zeljkovic, E.; Behlilovic, N.; Karahodzic, V.,[3] presented the study on increasing range of data types which are exchanged over this network (video, audio, text messages...), emphasize the security problem that this way of communication has. The flood of multimedia contents in the structure of transmitted data has made the appearance of images in this network quite normal. This revived the use of steganography (hiding data within images) in order to hide information to avoid unauthorized access. A much used technique for this purpose, the LSB (Least Significant Bits) technique, still leads to visible changes in the original image, which was chosen to be the message carrier. These differences make quite a path for a cryptanalyst to doubt the authenticity (independence) of the picture itself. However, by using GA (Genetic Algorithm), the differences between the original image and the image embedded with secret data can be reduced. However, the difference between the original image and the image with embedded information still remains, while the achieved improvements are paid with an increase of computational complexity. Naturally a question arises: Can the image be embedded with information in a way so that it does not undergo any changes? Most fast responses would be that it is not possible. This paper shows that this is in fact possible.

In the year of 2012 Qiangfu Zhao; Akatsuka, M.; Cheng-Hsiung Hsieh, [4] proposed the study of an image morphing based method for information hiding. The basic idea is to hide a secrete image into a morphed image which is obtained from the secrete image and another reference image. To make this method practically useful, it is necessary to produce natural morphed images. This is a necessary condition conceal the existence of the secret image. To produce natural morphed images, we should choose a proper feature point set (FPS) for morphing. This is a tedious work if we do it manually, because the number of possible FPSs is very large. To solve the problem more efficiently, we adopted interactive genetic algorithm (IGA) in this study and conducted experiments for generating facial images.

Outcomes show that, if we provide a relatively good initial FPS, IGA can finetune the FPS, and produce more natural facial images with limited number of evaluations.

In the year of 2012 Khosravi, M.; Soleymanpour-Moghaddam, S.; Mahyabadi, M.,[5] investigated a novel steganographic method is proposed which is based on the spatial domain: Least Significant Bit (LSB). The LSB matching method proposed by Mielikainen utilizes a binary function to reduce the number of changed pixel values. While in this paper a bipolar evaluating system is proposed to assess the performance of different orders for LSB matching. Afterward a genetic algorithm strategy is employed to search for an optimal solution among all the permutation orders. The experimental outcomes show that by employing the proposed bipolar evaluating system, the distortion of the stego-image is reduced while the probability of detection is decreased.

In the year of 2011 Brazil, A.L.; Sanchez, A.; Conci, A.; Behlilovic, N.,[6] The study of Internet connects more people, increasing the need for transmitting secure information. One way to protect the data sent over the web is to conceal the relevant information inside a typical image, hiding the data from intruders. This paper proposes a hybrid heuristic, combining a genetic algorithm and the path relinking metaheuristic to efficiently solve this problem. Computational outcomes show that the proposed algorithm outperforms the LSB (least significant bits) substitution technique, concerning the quality of solutions. In this way, the inclusion of a path relinking procedure can significantly improve the performance of a genetic algorithm for the problem considered.

In the year of 2011 Bhowal, K.; Sarkar, D.; Biswas, S.; Sarkar, P.P.,[7] presented the Audio Steganography that is a method that ensures secured data transfer between parties normally in internet community. In this paper, authors present a novel, principled approach to resolve the remained problems of substitution technique of Audio Steganography. In the first level, here authors first extract image data from an image file. In the second level, authors use a powerful GA (Genetic Algorithm) based LSB (Least Significant Bit) Algorithm to embed the image data into audio data. Here image data bits are embedded into random and higher LSB layers, consequential in increased robustness against noise addition. On the other hand, GA operators are used to reduce the distortion.

In the year of 2011 Mandal, J.K.; Khamrui, A.,[8] proposed a study of Image steganography that is the art of hiding information onto the cover image. In this paper a Genetic Algorithm based color image authentication/data hiding technique through steganographic approach, in frequency domain using Discrete Fourier Transform (DFT) termed as GASFD, has been proposed. 2×2 masks are taken from the source image in row major order where DFT is used to transform original image (cover image) block from spatial domain to frequency domain. Three bits of the hidden image are embedded per byte of the source image onto the rightmost 3 bits of each pixel excluding the first byte of each mask, as a effect large volume of message/ image is embedded in frequency domain. 2×2 embedded image mask is transformed from frequency domain to spatial domain using inverse DFT. Resulting image mask of size 32 bits are taken as initial population. New Generation and Crossover are applied on the initial population to obtain stego image. In the process of embedding dimension of the hidden image followed by the content of the message/hidden image are embedded. Reverse process is followed during decoding. Genetic algorithm is used to enhance the security level. Various statistical parameters computed are compared with the existing Discrete Cosine Transformation based steganographic algorithms devised by Hashad A. I. et al. [9] which shows that proposed GASFD obtained better outcomes in terms of large message embedding and consistent PSNR.

IV. PROPOSED METHODOLOGY

The proposed work is basically a framework designed in MATLAB with two modules e.g. Steganography using Genetic Algorithm and Visual Cryptography. The proposed system model of the Steganography using Genetic Algorithm and Visual Cryptography is shown in the Figure 1. An input image is accepted as cover image which is used to hide the secret message. An input image is accepted as cover image for the input message in plain text format. After embedding the secret message in LSB (least significant bit) of the cover image, the pixel values of the stego-image are modified by the genetic algorithm to keep their statistic characters. The experimental results should prove the proposed algorithm’s effectiveness in resistance to steganalysis with better visual quality. The user can select their targeted information in terms of plain text for embedding the secret message in LSB of the cover image.

The implications of the visual cryptography will enable the pixels value of the stego-image to keep their statistic character. LSB steganography has low computation complexity and high embedding capacity, in which a secret binary sequence is used to replace the least significant bits of the host medium. This is also one of the strong algorithms which keeps the information proof from any intruder channel. In a pure steganography framework, the technique for embedding the message is unknown to Intruder and shared as a secret between Alice and Bob. However, it is generally considered that the algorithm in use is not secret but only the key used by the algorithm is kept as a secret between the two parties, this assumption is also known as Kerchoff’s principle in the field of cryptography. The secret key, for example, can be a password used to seed a pseudo-random number generator to select pixel locations in an image cover-object for embedding the secret message (possibly encrypted).Intruder has no knowledge about the secret key that Alice and Bob share, although she is aware of the algorithm that they could be employing for embedding messages.

V. CONCLUSIONS

Steganography is an elective way to hide sensitive information. In this paper we have reviewed the various Techniques on images to obtain secure stego-image insertion using the visual cryptography scheme for gray scale image in various platforms. The image resolution doesn't change much and is negligible when we embed the message into the image and the image is protected with the personal key. So, it is not possible to damage the data by unauthorized personnel. The algorithm is usage for both 8 bit and 24 bit image of the same size of cover and secret image. This paper focuses on the approach like increasing the security of the message and increasing PSNR and reducing the distortion rate. Training data sets can be analyzed from the JPEG samples could be used for future research for benchmarking different methods of teaching artificial neural networks. Future analysis could be aimed on self arranged network typology by methods of symbolic regression like Genetic Programming, Grammatical Evolution, Analytic Programming and others, i.e. superstructure of evolutionary optimization algorithms.

The future work could be towards the enhancing visual cryptography scheme for gray scale image in various platforms.

REFERENCES

[1] Prema, G.; Natarajan, S., "Steganography using Genetic Algorithm along with Visual Cryptography for wireless network application," *Information Communication and Embedded Systems (ICICES), 2013 International Conference on* , vol., no., pp.727,730, 21-22 Feb. 2013.

[2] Nickfarjam, A.M.; Azimifar, Z., "Image steganography based on pixel ranking and Particle Swarm Optimization," *Artificial Intelligence and Signal Processing (AISP), 2012 16th CSI International Symposium on* , vol., no., pp.360,363, 2-3 May 2012.

[3] Sanchez, A.; Conci, A.; Zeljkovic, E.; Behlilovic, N.; Karahodzic, V., "A new approach to relatively short message steganography," *Telecommunications (BIHTEL), 2012 IX International Symposium on* , vol., no., pp.1,4, 25-27 Oct. 2012.

[4] Qiangfu Zhao; Akatsuka, M.; Cheng-Hsiung Hsieh, "Generating facial images for steganography based on IGA and image morphing," *Systems, Man, and Cybernetics (SMC), 2012 IEEE International Conference on* , vol., no., pp.364,369, 14-17 Oct. 2012.

[5] Khosravi, M.; Soleymanpour-Moghaddam, S.; Mahyabadi, M., "Improved pair-wise LSB matching steganography with a new evaluating system," *Telecommunications (IST), 2012 Sixth International Symposium on* , vol., no., pp.982,986, 6-8 Nov. 2012.

[6] Brazil, A.L.; Sanchez, A.; Conci, A.; Behlilovic, N., "Hybridizing genetic algorithms and path relinking for steganography," *ELMAR, 2011 Proceedings* , vol., no., pp.285,288, 14-16 Sept. 2011.

[7] Bhowal, K.; Sarkar, D.; Biswas, S.; Sarkar, P.P., "Secured image transmission with GA based Audio Steganography," *India Conference (INDICON), 2011 Annual IEEE* , vol., no., pp.1,4, 16-18 Dec. 2011.

[8] Mandal, J.K.; Khamrui, A., "A Genetic Algorithm based steganography in frequency domain (GASFD)," *Communication and Industrial Application (ICCIA), 2011 International Conference on* , vol., no., pp.1,4, 26-28 Dec. 2011.

[9] H. C. Huang, J. S. Pan, Y. H. Huang, F. H. Wang, and K. C. Huang, Progressive watermarking techniques using genetic algorithms, Circuits, Systems, and Signal Processing, vol. 26, no. 5, pp. 671{687, 2007.

[10] E. Kawaguchi and R. O. Eason, Principle and application of bpcs-steganography, Proc. Of SPIE:Multimedia Systems and Applications, pp. 464{472, 1998.

[11] A. R. S. Marcal and P. R. Pereira, A steganographic method for digital images robust to rs steganal-ysis, Lecture Notes in Computer Science, pp. 1192{1199, 2005.

[12] N. Provos, Steganography detection with stegdetect, http://www.outguess.org/detection.php.

[13] A.Westfeld, F5-a steganographic algorithm, Proc. of the 4th International Workshop on Information Hiding, Lecture Notes in Computer Science,2137.Springer-Verlag, pp. 289{302, 2001.

[14] A. Westfeld and A. P_tzmann, Attacks on steganographic systems, Proc. of Information Hiding-Third International Workshop, 1999.

[15] A. Westfeld and A. P_tzmann, Attacks on steganographic systems, Lecture Notes in Computer Science, pp. 61{76, 1999.

[16] D. C. Wu and W. H. Tsai, A steganographic method for images by pixel-value di_erencing, Pattern Recognition Letters, pp. 1613{1626, 2003.

[17] X. Zhang and S. Z. Wang, Statistical analysis against spatial bpcs steganography, Computer-Aided Design & Computer Graphics, pp. 395{406, 2003.

[18] X. Zhang and S. Z. Wang, Vulnerability of pixel-value di_erencing steganography to histogram analysis and modi_cation for enhanced security, Pattern Recognition Letters, pp. 331{339, 2004.