IJCSE International Journal of Computer Science and Engineering Open Access
Research Paper Volume-2, Issue-3 E-ISSN: 2347-2693

Image Steganography for Message Hiding Using Genetic Algorithm

Chaitali R. Gaidhani[1*], Vedashree M.Deshpande[2] and Vrushali N.Bora[3]

[1*,2,3] *Pune University, India, chaitaligaidhani@gmail.com*

www.ijcaonline.org

Received: 12 March 2014 Revised: 18 March 2014 Accepted: 28 March 2014 Published: 30 March 2014

Abstract-Considering the need for higher security in Secrete Message transmission we introduce Image Steganography for Message Hiding Using Genetic Algorithm. We are going to propose a system in which we can share a secrete message without letting anyone know the presence of that message behind any sample image, this term is called Steganography. To make it more powerful and secure than before we are introducing Genetic Algorithm in this technique.

Keywords- Steganography; Cryptography; Secrete Message; Image Shelter

I. INTRODUCTION

In today's world we know the serious terrorism is growing so fast that people are looking to kill each other for a piece of land or something that is not so precious than lives. Being Indians we know the Kashmir problems and the Pakistan Government/Agencies are trying hard to get the position on the Real Indian Territory. For the security of Kashmir Indian Government has employed Armours. Traditionally the Armours were so dynamically intelligent that they used to do their jobs without using high end Technologies. But now a day they need to improve their technology to compete with enemies, example use of Computer/Internet to pass the Secrete Plan of action, Messages, Orders to Subordinates, etc.

The technology has enhanced to the level that the day-to-day life has become "Computerised", i.e. the day-to-day transitions are happening via Computers or Internet, example, E-banking, E-Commerce, E-learning, E-mails, etc. This has improved the Standard of living of people. But as there are Advantages of any technology there are even Drawbacks of it. Today as the Computer is the mediator for many essential, confidential communications; there are multiple problems that hamper the trustworthy networks between two communicators, example data leakage, data alteration, data loss, hacking etc.

Now a day's all transaction is done through computer but there are chances of hacking of confidential data. Hacking is process in which data is stolen by unauthorized user. In the hacking process unauthenticated user is trying to gain access to confidential data. So hacking can lead to great loss for our country. So we are going to propose new system in which we are going to provide security to confidential data. Considering the need for higher security in Secrete Message transmission we introduce Image Steganography for Message Hiding Using Genetic Algorithm. Image will be treated as Shelter to hide the message, Steganography is a technique to hide the message, Genetic Algorithm optimizes the large solution yet giving Powerful & Secure than other existing techniques.

We are going to propose a system in which we can share a secrete message without letting anyone know the presence of that message behind any sample image, the term is called Steganography. To make it more powerful and secure than before we are introducing Genetic Algorithm.

II. SURVEY OF LITERATURE

For any project literature survey is considered as the backbone. Hence it is needed to be well aware of the current technology and systems in market which is similar with the system to be developed. Basically there are three techniques are present for data hiding i.e. data management, watermarking and steganography. Watermarking is technique for data leakage detection. Watermarking is one of the old techniques which contain a unique code. This unique code is embedded in each copy which is then distributed to the clients by the user. If any particular client leaks the given data to the third parties i.e. unauthorized users, then this leaked data and the leaker can be identified by the means of this watermarking technique. Watermarking is very useful technique but it has some disadvantages because of which there is a great chances of getting the data leaked[1]. Digital watermarking tech- unique is also there in which the code is embedded in the digital file like audio or video files. If the watermarking technique is used then the code which is embedded in the data can be modified because of which it becomes very difficult to identify the guilt agent or leaker. Furthermore these watermarks can be destroyed if the data recipients are malicious. E.g.: data of private firms, corporate sectors or the research centres.

Corresponding Author: Chaitali R. Gaidhani

Presently the secrete message sharing is done with technique called cryptography and steganography. Secrete Message Hiding using Cryptography is nothing but hiding message in Unreadable format.[1] In this single message is hidden behind single image. Secrete Message Hiding using Steganography Uses single image to hide the message. In this single message is hidden behind single image.[1]

Steganography/Data hiding is a secure communication method that conveys secret messages in the form of plaintexts so that the appearances of the secret messages will not draw eavesdropper's attention while they are being transmitted through an open channel. The word steganography which is composed of the two Greek words steganos and graphia, mean "hidden writing" or "covered writing". The earliest study concerning modern steganography was presented by Simmons in 1983.[1] In the story of Prisoner's Problem explains what capabilities and merits steganography has to offer when the public communication channel is insecure.[1]

In recent years, Steganography and Steganalysis are two important areas of research that involve a number of applications. Based on the analysis of steganography tools' algorithms, we partition these tools into two categories:

A. Spatial domain based steganography:
Spatial steganography mainly includes LSB (Least Significant Bit) steganography Least significant bit (LSB) insertion is a common, simple approach to embedding information in a cover image . The least significant bit (in other words, the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message.[2,3] This method is used, but similar transforms are for example the Discrete Fourier Transform (DFT). These mathematical transforms convert the pixels in such a way as to give the effect of "spreading" the location of the pixel values over part of the image.[2] The DCT transforms a signal from an image representation into a frequency representation, by grouping the pixels into 8 × 8 pixel blocks and transforming the pixel blocks into 64 DCT.[2,3].

B. Transform Domain Based Steganography:
Basically there are many kinds of power level transforms that exist to transfer an image to its frequency domain, some of which are Discrete Cosine Transform, KL Transform and Wavelet Transform. The Discrete Cosine Transform (DCT). [2,3]This method is used, but similar transforms are for example the Discrete Fourier Transform (DFT). These mathematical transforms convert the pixels in such a way as to give the effect of "spreading" the location of the pixel values over part of the image. The DCT transforms a signal from an image representation into a frequency representation, by grouping the pixels into 8 × 8 pixel blocks and transforming the pixel blocks into 64 DCT[2]. Problem with technique is that the secrete message is going to be hide by replacing last bit of pixel of image. But it reduces security level of message because it is easy to predict the message from given bits of embedded message. In this technique robustness against the statistical attack is low and robustness against image manipulation is low. In DCT algorithm image is going to divide into 8*8 blocks of pixel block and after dividing the image secrete message is embed with pixels of image using LSB algorithm.[2,3] So that there can be distortion of image occur which reduces security level. Hackers can get the idea from distorted image that something is hidden behind this image. This technique is time consuming as well as complex.[2]

Genetic Algorithms are a family of computational models inspired by evolution. These algorithms encode a potential solution to a specific problem on a simple chromosome-like data structure and apply recombination operators to these structures as as to preserve critical information. Genetic algorithms are often viewed as function optimizer, although the range of problems to which genetic algorithms have been applied are quite broad.[4]

An implementation of genetic algorithm begins with a population of (typically random) chromosomes. One then evaluates these structures and allocated reproductive opportunities in such a way that these chromosomes which represent a better solution to the target problem are given more chances to `reproduce' than those chromosomes which are poorer solutions. The 'goodness' of a solution is typically defined with respect to the current population [4].

III. PROPOSED SYSTEM

Technology is a never ending process. To be able to design a product using the current technology that will be beneficial to the lives of others is a huge contribution to the community. Considering the need for higher security in Secrete Message transmission we introduce Image Steganography for Message Hiding Using Genetic Algorithm. Image will be treated as Shelter to hide the message; Steganography is a technique to hide the message. It embeds the secret message in the cover media (e.g. image, audio, video, etc.) to hide the existence of the message. Steganography is often used in secrete communication. In recent years, many successful steganography methods have been proposed. Genetic Algorithm optimizes the large solution yet giving Powerful & Secure than other existing techniques.

We are going to propose a system in which we can share a secrete message without letting anyone know the presence of that message behind any sample image, the term is called Steganography. To make it more powerful and secure than before we are introducing Genetic Algorithm in this technique, wiz we will convert textual message into binary form then by encrypting it we will convert it in numeric form after that we will divide this numeric form by single digits. And we will get deviser, dividend, quotient and reminder. These will be treated as individual file. Now multiple images

are as shelter to hide these files. We have to then calculate LSB (Least Significant Bit) of each pixels of each image. This LSB is replaced by the bit of secrete message one by one.

Receiver will then get multiple images behind which there will be hidden messages as numeric files. Receiver will again calculate the LSB of each pixel, then he will have to convert that pixels into bits of numeric characters and these characters will be further go through the decryption process to get the alphabets that is textual message.

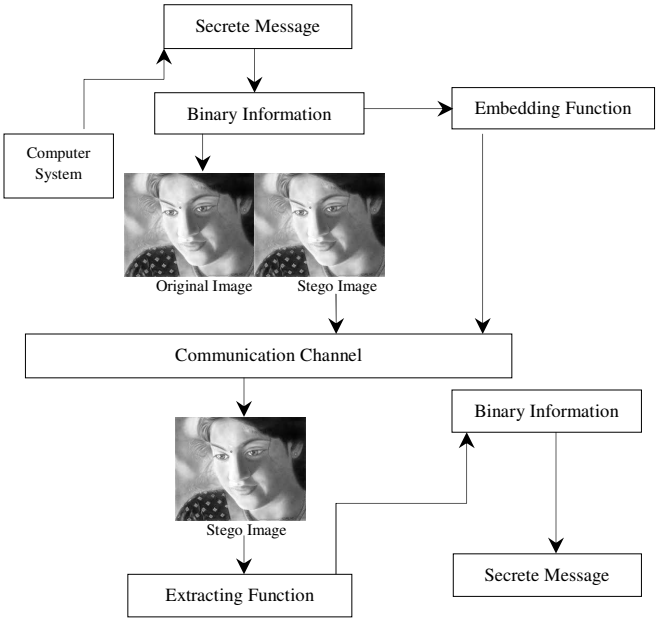

Figure 1. Architecture of proposed system

Algorithm to retrieve text message:-
Step 1: Read the stego image.
Step 2: Calculate LSB of each pixels of stego image.
Step 3: Retrieve bits and convert each 6 bit into Binary mapped value.
Step 4: Convert Binary mapped value into Binary value
Step 5: Binary value is then converted into original message.

Algorithm: Genetic Algorithm
Input: Stego-Image
Output: Re-assembled message
Step 1: Read Stego-Image generated.
Step 2: The Secrete message is breaked into parts.
Step 3: This parts are treated as individual files and are hidden behind multiple shelter images
Step 4: The message is re-assembled and the extracted data will be gained again.

IV. RESULT ANALYSIS

In the previous system we have compared with respect to parameters given in the table 1 and analysed that in previous system the original image gets drastically changed after embedding text into it, the change may be , increased and/or decreased size of image, decreased intensity of pixels of image. As this change is highly noticeable by human eyes, so probability of image getting hacked was increased

(*ii*) *Mean Square Error*: It is defined as the square of error between cover image and the stego image. The distortion in the image can be measured using MSE.

$$MSE = \frac{(\mathrm{Cov}(i,j) - \mathrm{steg}(i,j))2}{n * n}$$

(*iii*) *Peak Signal to Noise Ratio*: It is the ratio of the maximum signal to noise in the stego image

$$PSNR = 10\log \frac{M * N * (255)2}{\sum_{i,j}^{n}(y - x)2}$$

Parameters	Steganography	Proposed Method
Mean Square Error (MSE)	High	Low
Hiding Capacity	90,500 Bits	105630 Bits
Pick Signal to Noise Ratio (PSNR)	25dB	51dB
Security Level	Medium	High
Rate of Distortion of image after embedding text	High	Very Low
Rate of tampering of secure message while decrypting	Medium	Very low
Image format supported by Project	Bitmap	PNG, Bitmap, JPEG, JPG

Table 1: Comparative study of Steganography and Proposed System

The analysis of LSB and Genetic Algorithm based steganography has been done on basis of parameters like PSNR, MSE, Hiding capacity, Security, Rate of distortion of image after embedding text,. PSNR computes the peak signal to noise ratio, in decibels, between two images. This ratio is used as a quality measurement between two images. If PSNR ratio is high then images are best of quality.

V. CONCLUSION

The proposed system has discussed implementation of securely using steganography using genetic algorithm along with cryptography. It can be concluded that when normal image security using steganographic and cryptographic technique is applied, it makes the task of the investigators unfeasible to decrypt the encoded secret message. The security features of the steganographic are highly optimized using genetic algorithm.

We have presented a method of applying genetic algorithms for image steganography. Software is implemented for the proposed method, and its operations are described in detail using pseudo-code. A number of experiments have been carried out using a benchmark data set in order to show the efficacy of the developed software.

REFERENCES

[1] Kai Wang, Xukai Zou, Yan Sui. "A Multiple Secret Sharing Scheme based on Matrix Projection". 33rd Annual IEEE International Computer Software and Applications Conference. Department of Computer and Information Science,0730-3157/09,(400-405), 2013

[2] Guarmeet Kaur, Arati Kochhar. "A Steganography implementation based on LSB and DCT". International Journal for Science and Emerging Technologies with latest Trends 4(I), (35-41), November 2012

[3] Dr. Mohammad Abbas Fadhil Al-Husainy. "Message Segmentation to Enhance the Security of LSB image Steganography". International Journal for Computer Science and Application vol 3,no.3,(57-62) 2012

[4] Mantas Paulinas. "A Survey of Genetic Algorithms Applications for Image Enhancement and Segmentation". ISSN 1392-124X Information Technology and Control.vol 36,no 3,(278-283),2012

[5] lham Ghasemi, Islamic Azad University Science and Research Branch Tehran, Iran. "A Steganographic method based on Integer Wavelet Transform and Genetic Algorithm", IEEE, 978-1-4244-9799-7/11, (42-45), 2011.

[6] *Liping ZHANG, Xiutan WANG, Yong HUANG, Yingning PENG,* "A Time Domain Synthesized Binary Phase Code Side lobe Suppression Filter Based on Genetic Algorithm", Proceedings of ICSP IEEE, 0-7803-5747-7/00, (1907-1910),2000.

[7] S.Geetha, Siva.S.Sivatha Sindhu, Dr.N.Kamaraj, "Evolving GA Classifier for breaking the Steganographic Utilities : Stools, Steganos and Jsteg", International Conference on Computational Intelligence and Multimedia Applications, IEEE, 0-7695-3050-8/07, (230-234), 2007.

[8] Elham Ghasemi, Shanbehzadeh, "A Steganographic method based on Integer Wavelet Transform and Genetic Algorithm", IEEE,978-1-4244-9799-7/11,42-45,2011.

[9] Liaojun Pang, Huixian Li, Ye Yao, and Yumin Wang, "A ver- ifiable (t, n) multiple secret sharing scheme and its analyses", International Symposium on Electronic Commerce and Security, (22–26), 2013.

[10] B.Raja Rao,P.Anil Kumar, "A Novel Information Security Scheme using Cryptic Steganography", Indian Journal of Computer Science and Engineering ,Vol. 1 No. 4, (327-332),March 2010.

AUTHOR'S PROFILE

Chaitali R. Gaidhani
B.E.Computer
Late G.N.Sapkal College of Engineering
Nasik,India
chaitaligaidhani@gmail.com

Vedashree M.Deshpande
B.E.Computer
Late G.N.Sapkal College of Engineering
Nasik,India
veddeshpande@yahoo.com