A Technique for Information Hiding in Image Steganography and Cryptography by using Genetic Algorithm

MOHD.ABDUL.KHADER .KHAN[1],
Dr.SYED ABDUL SATTAR[2]

[1]Research Scholar, CMJ University, Meghalaya, India

[2]Professor & Dean of Academics, Royal Institute of Technology & Science, Andhrapradesh, India

E-Mail: khader_all@yahoo.co.in

Abstract: This current manuscript suggests an enormous requirement of internet applications, which needs information to be transmitted in a safe path. Cryptography & steganography supports in giving information security. Steganography hides the message continuation through inserting information in several digital media such as picture or audio or video format and cryptography translates data into cipher text, which might be in indecipherable format to ordinary client. For engaging the protection of data thrashing & communication over network, the expected framework utilizes “cryptographic algorithm along with Steganography”. In the expected framework, the record that we need to create secured is firstly compacted to shrink in size & then the compacted information will be converted into cipher text through utilizing “AES cryptographic algorithm” and then the encrypted information may be hidden in the picture. The GA will be utilized for pixel combination of picture whereas information is to be hidden so that identification of undercover data gets to be diverse.

Keywords-Steganography; Cryptography; AES Cryptographic algorithm; Genetic Algorithm;

1. Introduction

Steganography & Cryptography are recognized and broadly utilized modus operandi, which control data (messages) so as to hide their truth consistently. Steganography will be the science & art of opposite in a path that hide the actuality of the correspondence. Cryptography scuttles the message so it might not be implicit; the Steganography hide a message so it can't be discerned.

Steganography hide a message actuality through implant information in other digital media such as picture or audio or video framework and cryptography redesign information into cipher text, which might be in indecipherable plan to typical client. In this project, we will spotlight to develop a framework that utilizes steganography and cryptography for superior confidentiality & safety. Even whether we blend these modus operandi directly, there will be an opportunity, which the interloper might recognize the real message. Consequently, our suggestion is to apply both of them at the same time with more levels of security and to acquire an extremely secured framework for hiding of data.

In our new framework to prevent Steganalysis effect is method, the GA will be utilized for pixel combination of picture where information may be to a chance to be disguised so that finding of secret data turns into diverse. Utilizing GA, the framework is get computationally unfeasible to interruption. The Genetic algorithms are team for computational methods belonging to the “class of heuristic evolutionary algorithms”.

The key point of recommended work will be to improve the “stenographic information potency by coordinate the soft-computing feature” in the information characteristic determination.

2. Related Work

2.1 Cryptography

The real information, which has to be put on air, will be known as plaintext, the particular case that might a chance to be comprehensible & decipherable either by a computer or by a human. While the covered information did not purport cipher text that is scribbled, machine nor person might appropriately practice it until it will be decrypted. A framework, which gives decryption & encryption, is known as cryptosystem. There are different sorts of cryptographic arrangements & strategies are accessible. Based on encryption nature, these strategies might be categorized into 2 categories- asymmetric & symmetric key encryption.

2.2 Steganography

Steganography will be the practice of hide a “file, message, image, or video in another file, message, image, or video”. So steganography will be secured writing. The fundamental cause of steganography will be ambiguous the reality of correspondence. In this the sender embedded its message under the “text, image, audio, or video document” so that hackers won't be aware of the message.

LSB strategy will be utilized to conceal the secret messages through utilizing algorithm. LSB deviates the picture declaration moderately clear as well as it will be simple to attack. It will be clear that “LSB modifications the picture revelation when the smallest notable bits add in the binary picture format, so that picture nature get burst & there turned into so much variation in the real picture & encoded picture in the respect of picture quality. With the goal will beat this problem, the work [10] recommended modify the LSB method thereabouts that we might get same picture nature as it has before encoding? The fundamental thought to get better picture quality, by changing the unseen technique of LSB, in this step they will conceal two bits through 2 bits by taking such as values.

The work [12] provides a survey of steganography, its numerous modus operandi, its benefits & difficulties, applications it is integration with strategies of cryptography.

This segment offers the newly made efforts on steganography & numerous methods established.

The work [7] suggested “Integer Wavelet Transform” will be executed on gray level cover picture and in turn “embeds message bit stream under the LSB's of integer wavelet coefficients” of a the picture. The primary motivation of the predicted work is tofocus on “civilizing embedding aptitude” and brings down the deformity happening in the picture. The adjustment of strategy acts as important role to attain low deformity rate &higher implant capacity. The evaluation outcomes demonstrate that the assessment metric like PSNR will be improved in higher route. The evaluation result represent that the method has a great indiscernibility &high ability.

3. Proposed Method

The provided segment gives the comprehensive sympathetic of the predicted work & their included problems and characteristics. Besides a sweeping method will be also offered in this segment, which gives the result of suggested work.

3.1 Transform Domain method

In the “transform domain method”, pictures are initial distorted & then the message will be settled in cover picture [3].

The “transform domain steganography systems hide messages” in more foremost regions of cover picture, and this require the cover picture to divide into low, middle, and high incidence component. Since the vast majority of the signal energy will be focused in the mediocre frequencies that will be very essential in visibility, thus, secret information will be embedded in the predominant frequencies to evade picture deformation.

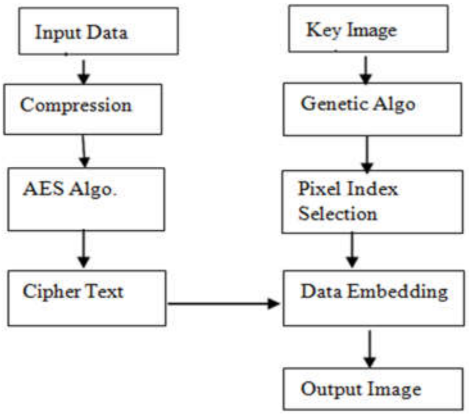

Figure.1. Block diagram of Embeds data

Beneficial defense & hardiness against picture maneuvering and statistical attack are the most important compensation of these systems. Though, high computational complexity will be the fundamental anxiety here.

3.2 Spatial Domain methods

In the “spatial domain approaches”, messages are settled in the power of the pixels reliably. The famous model is to embed secret messages under the swathe picture by straightly “least-significant bit (LSB) plane” [4, 5]. In LSB substitution, LSB bits of cover picture may be swapped with secret bits. One critical negative part of this system will be that the secret message could be distinguished very clearly [6]. Despite it is not the better stenographic technique, it is claim concentrating on it due to its easiness.

3.3 Domain overview

In workstation based advanced information security, the distinctive strategies i,e steganography & cryptography will be usually utilized, for recovering security during the network communiqué & information substitute. In our current method, the main purpose to consider both strategies for securing information from deceitful customer. The predicted model may be based on information cryptographic technique & picture steganography. Accordingly, numerous study articles are surveyed and it will be obtain that “conventional picture steganographic systems” are basically utilized with the “MSB or LSB based concepts, chaos map based strategies” &substitution based are also utilized to hide valuable information. However, these methods are computationally cost compelling and requires a long operation time for troupe information on the key picture.

In picture steganography the picture data may be used to hide the data, the information that has to be hidden might be a “picture, text or different delicate or private data, which is need to place on the air in unreliable nature”. Accordingly, the current project provides an “innovative modus operandi that hide distinctive formats of data in intension picture”. This will be executed toward picking those pixels and integrates information on it. Consequently, for picking the advantageous pixels in provided picture for concealing data, the “feature assortment strategy” might support. Therefore, the suggested method includes the implementation of the “soft computing based modus operandi” to be known as GA that will be utilized to choose better probable pixels for incorporating the information. Since GA will be a heuristic based strategy, thus, fewer adjustments are essential in conventional GA for direct pixel choice. The following segment gives the study of conventional GA.

3.4 Genetic Algorithm

The GA will be hereditarily motivated search procedure on theory of Darwin’s & discovers the better probable result in “enormous multidimensional search space”. The accessible results are hereditarily treated to discover the fittest reaction among numerous results that will be fundamentally an iterative strategy for define more appropriate elucidation. The GA utilizes the 3 fundamental operators for result discovery: “reproduction, diversity, and natural selection of genes” [12].

The GA methodology a pair of results. These results are the arrangement of symbols, which are contending in result space. The novel generation will be generated utilizing the determination procedure and hereditarily motivated operators. The illustration of the overall search procedure may be provided as:

Generate initial population– The “genetic algorithms are kick off with randomly engender progression”, with the permitted binaries for genes.

Check for termination of the algorithm–To stop the GA a stopping standard is needed to fix for discovering “optimum solution or fixed number of function evaluations”. It is probable to end the “genetic optimization process” by utilizing 3 methods; they are “fitness function value, fixing the number of generations, and more number of iterations”
According to the found description in [13] the classical GA might be defined utilizing the below provided pseudo code.

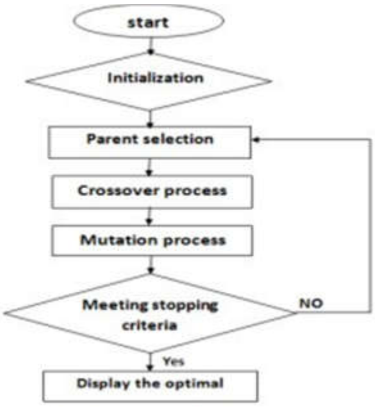

Figure.2. Flow chart

4. Implementation

The suggested working method for picture steganography is shown in figure 2. The modules of suggested method are defined as:

Input data: It is message that will be need to hide, therefore the suggested framework usage the formats of file by that the message is generated as input to framework, which might be in any format but require to compare the size of data to be hide due to large data on small picture can't be hidden.

Compression: Larger data form key picture will be first compressed utilizing the compression strategy or utilizing the ZIP utility. This decreases the original data size that will be need to hide in a provided key picture.

4.1 AES algorithm for Cryptography:

This strategy specifies "Rijndael algorithm", a symmetric block cipher, which might procedure data blocks of 128 bits, utilizing cipher keys with "lengths of 128, 192, and 256 bits". The input, output & cipher key for Rijndael are each bit sequences containing "128, 192 or 256 bits" with the constraint that the input and output sequences has the same length. The length of the input & output sequences might be any of the 3permitted values but for the AES the only length allowed is 128.

4.1.1 Key image: The key picture will be the picture that is utilized to hide sensitive data. Consequently that might be utilized in any size depends upon the amount of information, which is need to hide in picture.

4.1.2 Genetic algorithm: GA usage the 3 main stages, they are "selection, crossover &mutation". But the involved operators are usages the random selection procedure for searching the key data. Thus the recovery of real data that will be hidden in picture will be suspected. So it is require adding few heuristics during selection procedure to acquire the fixed set of pixels by evaluation of column &row pixels.

4.2 Modification on genetic algorithm/ Proposed Algorithm:

Firstly picture will be treated in row method& utilized for data embedding. Whether the data remains to hide thus the procedure hides the information in "column based manner". Consequently the picture of M X N is utilized& the selection of random rows of result will be utilized with threshold input, in subsequent method:

5. Results

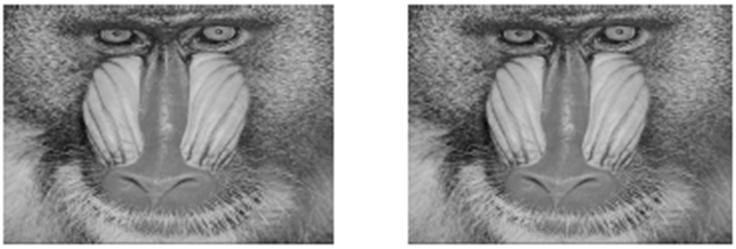

Figure.3. a) Original Image b) Stego

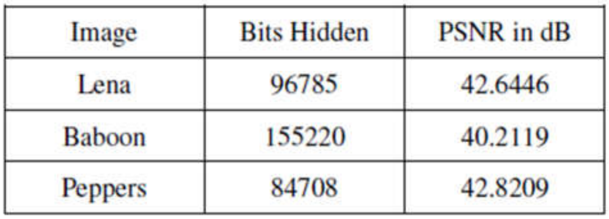

Image	Bits Hidden	PSNR in dB
Lena	96785	42.6446
Baboon	155220	40.2119
Peppers	84708	42.8209

Table.1. Value weighted embedding only in edge pixels

By observing the two tables 1 it can seen that in our method not only the hiding capacity has increased but also the visual quality is high compare to the Four neighbors and Diagonal neighbors method.

6. Conclusion

The project suggested in this manuscript might be précised with the following points: We have offered a new model for combination of steganography & cryptography utilizing GA for protected data communication in future. The recommended model offers adequate picture qualities with tiny deformation in picture that is Stegno pictures, which have PSNR values, are very high. The key aim of this framework is that the model utilized for AES, encryption will be much safe and the utilization of "GA in LSB Substitution Steganography technique" makes information revealing very inflexible.

References

1. Soleimanpour, "A Novel Technique for Steganography Method Based on Improved Genetic Algorithm Optimization in Spatial Domain" Iranian Journal of Electrical & Electronic Engineering, Vol. 9, No. 2, June 2011
2. Silman J., "Steganography and Steganalysis: An Overview", SANS Institute, 2001.
3. Lee Y. K. and Chen L. H., "High capacity image steganographic model", IEEE Proceedings of Visual Image Signal Processing, Vol. 147, No. 3, pp. 288-294,2000.
4. Ker A., "Improved detection of LSB steganography in grayscale image", Lecture Notesin Computer Science, pp. 97-115, 2005.
5. Mahdavi, Samavi Sh., Zaker N. &MHashemi.,"Steganalysis Method for LSB Replacement Based on Local Gradient of Image Histogram", Iranian Journal of Electrical& Electronic Engineering, Vol. 4, No. 3, pp. 59-70, 2008.
6. Mohammed AbuTaha, Mousa Farajallah and Radwan Tahboub, "Survey Paper: Cryptography Is the Science of Information Security", International Journal of Computer Science and Security (IJCSS), PP. 298- 309, Volume 5, 2011.
7. Prakash Kuppuswamy, and Saeed Q. Y. Al-Khalidi, "Hybrid Encryption/Decryption Technique Using New Public Key and Symmetric Key Algorithm", MIS Review: An International Journal, Volume 19, No. 2, PP. 1-13, March 2010.
8. Priyanka B. Kutade and Parul S. Arora Bhalotra "A Survey on Various Approaches of Image Steganography", International Journal of Computer Applications (0975 – 8887) Volume 109 – No. 3, January 2011
9. Silman J., "Steganography and Steganalysis: An Overview", SANS Institute, 2001.
10. Lee Y. K. and Chen L. H., "High capacity image steganographic model", IEEE Proceedings of Visual Image Signal Processing, Vol. 147, No. 3, pp. 288-294, 2000.
11. Ker A., "Improved detection of LSB steganography in grayscale image", Lecture Notesin Computer Science, pp. 97-115, 2005.
12. Mahdavi, Samavi Sh., Zaker N. & M Hashemi.,"Steganalysis Method for LSB Replacement Based on Local Gradient of Image Histogram", Iranian Journal of Electrical & Electronic Engineering, Vol. 4, No. 3, pp. 59-70, 2008.
13. Manish Trehan and Sumit Mittu, "Steganography and Cryptography Approaches Combined using Medical Digital Images", International Journal of Engineering Research & Technology (IJERT), Volume 4 June 2011.
14. David E. Goldbrg, "Genetic Algorithm in Search, Optimization & Machine Learning",Pearson Education Asia.
15. Genetic Algorithms for optimization, Programs for MATLAB Version 1.0 User Manual