Data Security Throws Image processing by Blowfish Algorithm, Genetic Algorithm and LSB

Md. Raihan Uddin
Dept. of ETE
Daffodil International University
Dhaka, Bangladesh

Kh. Mohaimenul Kabir
Dept. of CSE
Dhaka International University
Dhaka, Bangladesh

Md. Mehedi Hasan
Dept. of CSE
Dhaka International University
Dhaka, Bangladesh

ABSTRACT

The paper will represent the recent cryptographic technology to increase the security level in image processing technology and data security in Network system. Blowfish algorithm, Steganography algorithm least significant bit (LSB) and Genetic algorithm are mainly used in the paper for better security system. Blowfish algorithm provides a good encryption rate in software. it has a 64bit block size and a variable key length from 32bits up to 448 bits. The cryptographic society needs to make available the world with a new encryption standard. In the other side steganography in one of the most powerful way to conceal the existence of hidden secret data inside a cover object. All encrypted data will be hidden by Least Significance Bit (LSB). Genetic algorithms (GA) are directed random search techniques used to look for parameters that provide a good solution to a problem. Essentially they are nothing more than educated guessing. The 'education' comes from expressive the correctness of previous candidate solutions and the 'guessing' comes from combining the fitter attempts in order to evolve an improved solution. [1] For image processing system this algorithm is better. So hope paper will give most output performance.

General Terms

Pattern recognition, Database, GA, LSB, Steganography.

Keywords

Cryptography, Encryption, Decryption, Blowfish, LSB, Image Processing, Steganography, Genetic Algorithm, Crossover.

1. INTRODUCTION

Security means the system to protect information, data, message from unauthorized access by guessing, mathematical algorithms and other methods. Cryptography is the system to achieve this goal. The Cryptography has a vital role to process encrypted and decrypted data and message. Mainly Cryptography builds a process the readable message in a non-readable format to send to the other end.

Blowfish algorithm considers as algorithm of symmetric encryption which encrypt and decrypt the data, messages are same secret key. It is fastest block ciphers based on data development. This symmetric key block cipher uses a 64-bit block size and variable key length. Blowfish consists of two parts: key-expansion and data encryption. For the duration of the key development stage, the in-putted key is converted into several sub key arrays total 4168 bytes. There are the P array, which is eighteen 32-bit boxes, and the S-boxes, which are four 32-bit arrays with 256 entries each. [2]

Steganography is a technique which is used to information for hide their object. Now a day, this technique is rapidly used to in computer science, protect email messages, ATM card information, official data and other related fields. This paper strongly tried to represent the Cryptography and Steganography methods in data security of image processing.

Genetic Algorithm is a heuristic search algorithm. Chromosomes are the main parameter of GA. It is used to search and optimizing the problem.

It compares with the classification of chromosomic sample image.

2. METHODOLOGY

Encryption method:

Step 1: Data to be encrypted will generate a key for blowfish encryption.

Step 2: Text to be encrypted and image will be processed throw Blowfish encryption Algorithm method.

Step 3: The processed data will be encrypted by Steganography in LSB.As known as the Steganography hide secrete data inside a cover object.

Final Step: The encrypted data will be saved in a secured database.

Decryption Method:

Step 1: For decrypting data the Sample image will be matched with the encrypted data image throw Genetic Algorithm formula.

Step 2: After matching the Sample the encrypted data will be generated

Final Step: Finally the data will return the original text and key perspective of an image.

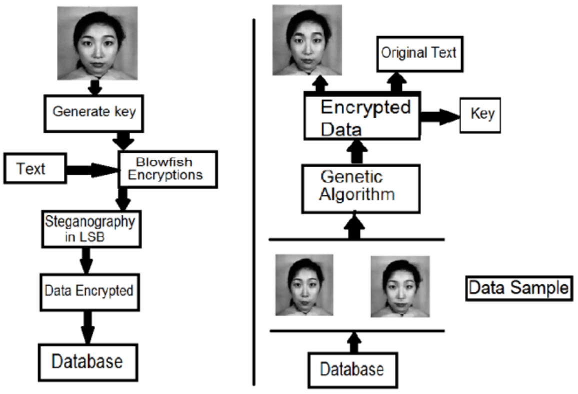


Fig 1: Encryption & Decryption Block Diagram

The main theme of the methodology is to ensure the two layer high security.

3. IMPLIMENTATION

3.1 Blowfish

Blowfish uses the same secret key to both encrypt and decrypt massages that's why it's known as symmetric encryption algorithm.

A graphical representation of the Blowfish algorithm is shown in **Figure 2**. In this Statement, a plaintext message of 64-bit is estranged into 32-bits. The "left" 32-bits plaintext are XORed with the first element of a P-array to create a value as a P, other hand a transformation function as a F, then the "right" 32-bits of the message with XORed to produce a new value as F'. F' replaces the "left" half of message and P' replaces the "right" half of the message and this process repeats in 15 more times with successive members of the P-array. In resulting the P' and F' are then XORed with the last two entries in the P-array, and reorganized to produce the 64-bit ciphertext.

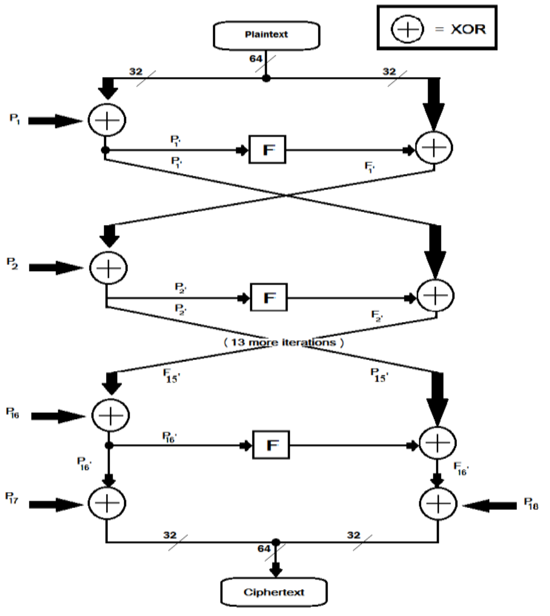


Figure 2. Blowfish algorithm

Algorithm:

The input is a 64-bit data element== x.

Divide x into two 32-bit halves: xL, xR.

Then,

for i = 1 to 16:

xL = xL XOR Pi

xR = F(xL) XOR xR

Swap xL and xR

After the sixteenth round,

swap xL and xR again to undo the last swap.

Then,

xR = xR XOR P17 and

xL = xL XOR P18.

Finally, xL and xR to get the cipher text.

A Graphical representation of 'F shown in Figure 2. The system separates a 32-bit input into four bytes and uses those as indices into an S-array. Output is produced by add of lookup result and XORed together.

The P-array and S-array values used by Blowfish are precompiled bashed on the user's key. In effect, the user's key is transformed into the P-array and S-array; the key itself may be discarded after the transformation [5].

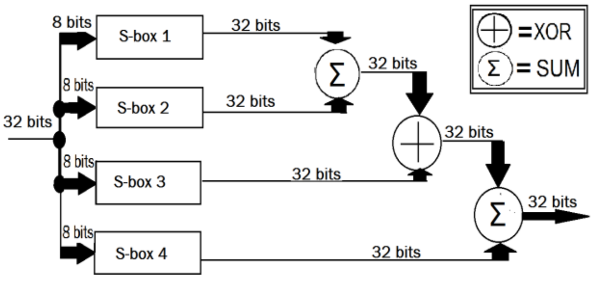


Figure 3. Graphical representation of F.

3.2 Least Signification Bit (LSB)

The Least Signification Bit in Steganography is rapidly used to hide the cover images. The LSB in various words, the 8th bit of all of the bytes inside an image is change to a bit of the secret message. Byte is represented when they are using a 24-bit image; a bit of each can be the red, blue, green color components. In another words, one can store 2 bits in each pixel. The image is 800 × 600 pixel, in here a total amount of 1,440,000 bits or 180,000 bytes stores of embedded data[3]. Example of a grid for 3 pixels of a 24-bit image can be as given below:

(0010110**1**0001110**0**1101110**0**)

(1010011**0**1100010**0**0000110**0**)

(1101001**0**1010110**1**0110001**1**)

When the number 200, then the binary representation is 11001000, is embedded into the LSB bits of this part of the image, the resulting grid is given bellow:

(0010110**1**00011101 11011100)

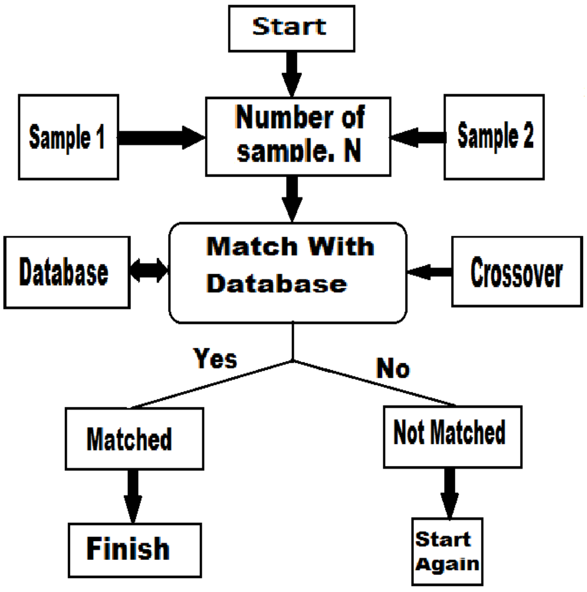
(1010011**0**11000101 00001100)

(1101001**0**10101100 01100011)

Even though the number is embedded into the first 8byts of the grid, only the 3 underlined bits needs to be changes according to embedded message. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size [3]. Since there are 256 possible intensities of each primary color, changing the LSB of a pixel results in small changes in the intensity of the colors. These changes cannot be perceived by the human eye - thus the message is successfully hidden. With a well-chosen image, one can even hide the message in the least as well as second to least significant bit and still not see the difference [4].

3.3 Genetic Algorithm

Genetic Algorithm is a heuristic search algorithm. Chromosomes are the main parameter of GA. It is used to search and optimizing the problem. Basic operations of Genetic Algorithm are Reproduction, Crossover and Mutation. Input image is selected from the test Database. Then small data is taken from the selected image. For the next steps, an image is selected from the train database and small data is taken from that. In third steps We do crossover and point out the amount of change of the test image to be like the train image. In four steps we calculated ten generations and add up each amount. Finally, we select the image whose sum value is minimum [6].



4. EXPERIMENTAL RESULTS

The used database consists of different image. Here JAFFE face database is used for this experiment. For this experimental result, the data and images is sent in ARM LPC 2148 by the serial communication port from the PC with VB GUI. And the encrypted data is sent in database by zigbee. Than the encrypted data will received by the zigbee and it reprocess by the ARM IPC 2148 kit. Its shown in PC with GUI. This experimental result is shown below.

Table 1: The result table on Blowfish algorithm, LSB algorithm and Genetic algorithm

Steps	Blowfish Algorithm (%)	LSB Algorithm (%)	GA (%)	Avg and total
Encryption Cycle	76	86	78	80
Decryption Cycle	82	88	88	86
Memory Utilization	95	95	88	92.66

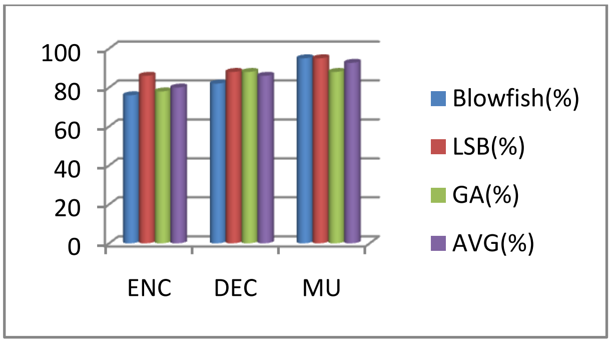


Fig1: Performance analysis chart

5. CONCLUSIONS

As the final result is shown in the graph which clearly declares that the given paper gives better solution for the technique. Then used algorithms (Blowfish, LSB, Steganography, Genetic Algorithm) and the combination of those algorithms are so much efficient for the task.

6. REFERENCES

[1] S. N. Sivanandam, S. N. Deepa, “Introduction to Genetic Algorithms”, Publisher Springer Publishing Company, Incorporated ©2007. Pp- 1-6.

[2] IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. X (Mar-Apr. 2014), PP 80-83

[3] Mamta juneja 1, parvinder singh sandhu2 “designing of robust image steganography technique based on lsb insertion and encryption” 2009 international conference on advances in recent technologies in communication and computing.

[4] Menezes, A., Van Oorschot, P., and Vanstone, S. “Handbook of applied cryptography.” CRC Press, (1996).

[5] Journal of Embedded Systems, 2015, Vol. 3, No. 1, 11-15 Available online at http://pubs.sciepub.com/jes/3/1/2 © Science and Education Publishing DOI:10.12691/jes-3-1-2.

[6] International Journal of Computer Applications (0975 – 8887) Volume 113 – No. 13, March 2015