Random Pixel Selection Based Improved LSB Image Steganography Method Using 1 D Logistic Map and AES Encryption Algorithm

Hasi Saha
Assistant Professor, Department of CSE
HSTU, Dinajpur, Bangladesh

MST. Rafia Chowdhury
Student ID, 1502043
HSTU, Dinajpur, Bangladesh

G C Saha*
Assistant Professor, Department of CSIT
BSMRAU, Gazipur, Bangladesh

Masum Billah
Assistant Professor, Department of CSIT
BSMRAU, Gazipur, Bangladesh

Suraiya Yasmin
Assistant Professor, Department of CSIT
BSMRAU, Gazipur, Bangladesh

Abstract:- Steganography program is mainly concerned about covering the way that a mystery message is being sent, just as hiding the substance of the message. Any computerized picture is contained pixels of various sizes of lattices; different picture steganography algorithms have been created. In this research, it has been exploited the irregular pixel selection based improved LSB exchange technique to hide a message into a cover image. We have considered a mystery message and a spread picture. In the LSB approach, the essential thought is to supplant the Least Significant Bits (LSB) of the spread picture with the bits of the message to be covered up without wrecking the property of the spread picture altogether. The LSB-based system is the most testing one as it is hard to separate between the spread item and stego-object as not many LSB bits of the spread article are supplanted. In digital image there are diverse types of file setup available such as Bitmap, PNG, JPEG, GIF etc. The proposed method focused on BMP images as it is uncompressed and convenient file format to implement LSB steganography technique. Before applying the proposed steganography method, we apply AES cryptography technique to encrypt the top-secret message to improve the security and it will alter the top-secret message to into cipher text. Then through our propose method, we embed the ciphertext into the LSB of the blue component among RGB value. We select pixels randomly through using 1 D logistic map. This method uses X-OR operation for embedding and extracting. Various size data are embedded into the images and PSNR are also considered for these images. It is being expected that the suggested technique will able to hide large amount of data and retaining the advantages of the LSB method.

Keywords:- *Steganography; Cryptography; 1 D Logistic Map; AES Algorithm; Stego Image; PSNR.*

I. INTRODUCTION

The steganography approach relies on hiding secret messages inside innocent-looking messages or documents in order to dissuade the enemy from attempting to find the secret message. There are numerous zones of security innovation that manages the assurance of secret information; the most significant of these systems are cryptography and steganography. The principal system is cryptography which is alluded to as "the study of secret". It incorporates encryption and decoding forms, encryption is the way toward changing over typical content to mixed up structure, where the sender utilizes an encryption key to scramble the message to transmit it through the unreliable open channel. Unscrambling is the way toward changing over encoded content to typical content in the decipherable structure; subsequently the recreation of the first message is conceivable just if the beneficiary has the decoding key [1].

The subsequent system is steganography which is characterized as a technique for security that shrouds information among the bits of a spread document, where the secret message is embedded in another medium with the goal that the very presence of the mystery message isn't perceivable. The spread document can be picture, sound or video; the most normally utilized being the picture records, in which unused or irrelevant bits are supplanted with the secret information [2].

However, in our work we first encrypt the message by using AES algorithm. Then we embed the secret message into randomly selected pixels through our proposed methodology of embedding ciphertext into cover image. We also use a password for filtering.

II. RELATED LITERATURES

LSB steganography is the most broadly utilized steganographic strategies because of its effortlessness and clear methodology. The secret message is put away at all noteworthy piece plane of the spread document. This strategy gets hard to recognize as in limited quantity of changes is being made in the spread picture. Various creators have utilized the straightforward LSB methods where LSB of pixels are supplanted by the secret bits [3]. This idea may once in a while represent some genuine security issues. Variations to the basic LSB based steganography can be seen in [4] [5]. E-XOR encrypting algorithm is used [6] to raise the security feature of LSB method. In this, one RGB channels of shield image is designated and two LSBs of secret data are implanted in it. In [7], data are embedded by analyzing the block complexity. Al-Bayati, M. have used stowing away of interactive media secret records in double RGB spread pictures utilizing LSB steganography systems. Mehdi and Mureed improved the Kekre's algorithm on LSB strategy and expanded the implanting limit while holding the nature of stego picture [8]. Disorderly Map Based Random Image Steganography Using LSB Technique is utilized by Sujarani Rajendran [9]. Singh S. & Kaur J. proposed a method of Steganography in Exact Color Imageries by Even Odd Bit Carving [10].

III. RESEARCH METHODS

Data security is a biggest concern of any organization. We propose “Dual Layer Security of data using LSB image steganography method through random selection of Pixels and AES encryption algorithm”. The main idea of our work is to provide dual layer of security to sensitive data or messages by hiding it behind the digital images using proposed Improved LSB image steganography algorithm and the second layer security is given by encryption of secret message using AES-128 bits encryption algorithm.

128 bits AES cryptographic algorithm takes a key and encrypt the plaintext into ciphertext. This ciphertext will be embedded into a cover image using our steganographic technique based on randomness. We select pixels randomly through filtering and the filtering is done by using the MSB and a password. This method uses a 10 characters or 80 bits password for both filtering and embedding technique .The characters are first converted to their ASCII value and these ASCII values are converted to binary. From this binary password 3 bits block is obtained and used in a circular manner. The concept is shown below:

Secret password: SeCrEtWoRk
ASCII value of password: 83 101 67 114 69 116 87 111 82 107

Binary of password:
010100110110010101000011011100100100010101110100
01010111011011110101001001101011

R=10100011	**MSB of RGB= 110**
G=10101101	**3 bit block = 010**
B=01001101	**X-OR value= 100**
R=00110101	**MSB of RGB=011**
G=11010001	**next 3bit block= 100**
B=10101101	**X-OR value= 111**

Our proposed technique embeds the size of the message first then it embeds the secret message (binary representation of ASCII value of each character) in the rest of the pixels.

A. Embedding Algorithm

- Get the secret message
- Encrypt the message with AES algorithm
- Convert the AES cipher into binary
- Get the cover image
- Generate a chaotic sequence for selecting ‘x’ co-ordinate by using 1 D logistic map where x_0=0.12, r =3.95 and n=length of the message, then multiply the sequence with the number of row and round the result
- Generate a chaotic sequence for selecting ‘y’ co-ordinate by using 1 D logistic map where x_0=0.15, r =3.97 and n=length of the message, then multiply the sequence with the number of column and round the result
- Select pixels randomly according to the value of (x , y)
- Get the 10 character password
- Convert the password to binary
- Get consecutive 3 bits of the password in circular order
- Collect the MSB bits of a pixel(Red ,Green, blue color component)
- Perform X-OR operation between the collected MSB bits and 3 bits block of the password
- Convert the result of X-OR operation in decimal, D_n
- X-OR the message bit with the blue component D_n th bit
- Embed the result into LSB of blue component

B. *Embedding Flowchart*

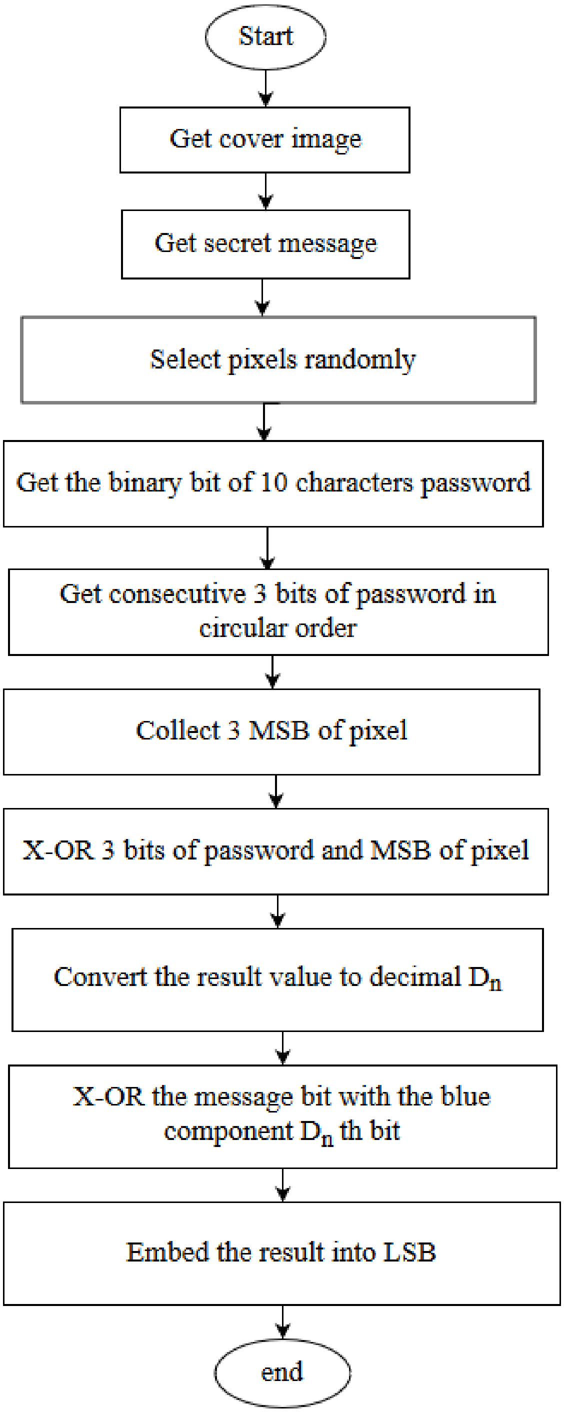
Start
Get cover image
Get secret message
Select pixels randomly
Get the binary bit of 10 characters password
Get consecutive 3 bits of password in circular order
Collect 3 MSB of pixel
X-OR 3 bits of password and MSB of pixel
Convert the result value to decimal D_n
X-OR the message bit with the blue component D_n th bit
Embed the result into LSB
end

Fig 1:- Flowchart of Embedding Process

IV. RESULTS AND CONCLUSION

24 bit image Oiky.png was used for experiment. The output of the program run is remarkably similar to the original image. The experimental results by applying our proposed method on different standard images are compared with other methods we have reviewed.

The proposed algorithm uses random sequence to embed message bits and changes very small number of bits when embedding a large cipher. The proposed technique applies a circular password and X-OR operation for embedding the secret message. The message bits are not directly embedded in the LSBs of the pixel which makes more difficult to retrieve the cipher by Stegoanalyst. In addition, the histogram is also showing very negligible changes.

As the project merges the AES Cryptography with Steganography, if someone would crack the cipher from cover image (all though, it’s not possible), the attacker will have to provide the encryption password to decrypt the cipher. And an assumption says that, the attacker will need about 10^{22} years to try all possible keys/password for the weakest version AES 128 [11].

The aim of our work is to improve the efficiency of LSB steganography by proposing an improved technique in which pixels are selected randomly by using 1 D logistic map for embedding message bit. The goal of our technique is to make difficult to determine the presence of the secret message and to excess the message. We have used a secret password and the most significant bits of the pixels for performing X-OR operation. Here we do not focus on the capacity of embedding the message in the image rather we focus on enhancing the security. In our proposed technique we didn't embed the message bit directly into the LSB. Rather we have done X-OR operation of the message bit before embedding and embed the result into the LSB. Our method also use AES cryptography algorithm to covert the secret message into cipher text to add another layer of security. Our method provides better PSNR value and lower distortion. So our proposed technique fulfills the requirements of steganography technique.

ACKNOWLEDGMENT

The authors wish to thank Dr.Ruzinoor Che Mat, School of Creative Industry Management & Performing Arts (SCIMPA), Universiti Utara Malaysia, Malaysia, Kedah 06010 for his patronage to the dissemination of knowledge, his valuable instructions, able guidance and keen interest throughout the research. The author is also grateful for his encouragement, precious comments and valuable suggestion in preparation for this work.

REFERENCES

[1]. Thakur, J., & Kumar, N., "DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis", International journal of emerging technology and advanced engineering, 2011.

[2]. Singh, S., & Siddiqui, T. J., "A security enhanced robust steganography algorithm for data hiding", International Journal of Computer Science Issues (IJCSI), 2012, vol. 9, no. 1. pp. 131-139.

[3]. Shahin Shabnam , Prof K Hemachandran, " 1 LSB based Steganography using Bit masking method on RGB planes", 2016.

[4]. Ziad Alqadi, Bilal Zahran, Qazem Jaber, BelalAyyoub, Jamil Al-Azzeh, "Enhancing the Capacity of LSB Method by Introducing LSB2Z Method", 2019.

[5]. Rohit Chaudhary, Rishabh Kaushik and TuariqBeg, "Imagesteganography using improved lsb algorithm", 2018.

[6]. Sandeep Kumar, "Image steganography using improved lsb and exor encryption algorithm improved lsb and exor encryption algorithm", 2014.

[7]. Gowtham dhanarasi, dr. A. Mallikarjunaprasad, "Image steganography using block complexity analysis", 2012.

[8]. AL-Shatnawi, A. M., &alfawwaz, B. M., 'An Integrated Image Steganography System with Improved Image Quality. Applied Mathematical Sciences", 2013, Vol. 7, no. 71, pp. 3545-3553.

[9]. Sujarani Rajendran, ManivannanDoraipandian, "Chaotic Map Based Random Image Steganography Using LSB Technique", 2017.

[10]. Singh S., & Kaur J., "Steganography in True Color Images Using Even Odd Bit Slicing", International Journal of Engineering and Computer Science, 2015.

[11]. Satwinder Singh, "Dual Layer Security of data using LSB Image Steganography Method and AES Encryption Algorithm", 2015.