IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Multimedia Encryption For Enhancing Data Security Using AES and Logistic Mapping

[1]Meghana N, [2]Prof. Sapna P J

Department of Electronics and communication Engineering
Dayananda Sagar College of Engineering, Bangalore, India

Abstract—**In the field of technology and communications, There are billions of technological services and applications available to us. These technological developments, applications, and services combined, with the expansion and proliferation of the internet, the frequency of data transfers across the internet has dramatically increased. *As digital world is increasing the complexity of securing is becoming unfeasible.* This has led to an increase in the vulnerability of data hacking during its transfer from one part to another. On the other hand, malicious parties abilities to circumvent security measures and reveal personal information have improved and grown tremendously. The Two dimensional logistic map and AES used for image encryption. The proposed methods are able to encrypt an image into random –like from the statistical point of view and the human visual point of view.**

Keywords— Encryption; Steganography; LSB; Security; Histogram; password verification.

I. INTRODUCTION

Security is a prime aspect in day-to-day life to stay away from gougers. As the world becomes more sophisticated and humans update to smart city standards, security becomes increasingly important. With rapid growth in digital communication, sharing and transmission of texts and images over the Internet is unsecured due to eavesdropping. Various cryptography algorithms are worked in order to provide secured data communication by preventing cipher attacks and snooping. Unexpected exposure of private photos and divulged military and governmental classified images emphasizes the importance of the text and image security again and again. With the fast development of digital storages, computers and the world wide network, For a digital image and text within seconds, it can be duplicated to mobile storage or transported to the other side of the planet.

Steganography differs from encryption, as encryption transforms the confidential image and message into an unrecognized one, while Steganography hides the image and message in another medium to become invisible. As a result, combining encryption and steganography will provide a higher level of protection for highly confidential material. Among various image security technologies, the image encryption is a simple and straight-forward one with concerns in encrypting an image to an unrecognized and unintelligent one, where the source image and the encrypted image are referred to as plaintext image and ciphertext image respectively. The two-dimensional Logistic map for image encryption with the careful considerations for the diffusion and confusion properties and possible attacks as well.

The Rijndael block cipher algorithm was chosen by NIST as the new advanced encryption standard (AES).

One of the easiest ways in spatial domain is changing the least significant bit (LSB), where each pixel is transformed to binary code, then the lowest significant bit of this pixel will be replaced by the next bit of secret information. Normally, the insertion starts from the first pixel, then the second, and so on. Another method depends on insertion in the pixel that the level of difference between it and its neighbour is larger than the threshold instead of insertion in all pixels, but that will decrease the amount of data that can be hidden. To address the issue of the amount of data that can be hidden, some methods relied on encoding the data before hiding it, where this encoding will not decrease the size of data and enhance the security at the same time.

II. LITERATURE REVIEW

In this part, some recent and previous techniques used for encrypting an image and text and steganography are discussed [1] The nature of digital data represented by 0 & 1 allowed such techniques in hiding operations, as they are usually integrated with some encryption algorithms. In [2] The cover is usually a text file or an audio, image or video file. If the cover is text, some letters, spaces, or special characters are changed, but the

meaning must be guaranteed not to change, which is a great challenge. Therefore, sound is considered easier as it can be hidden within the sections of silence or noise, but it does not create a defect in the sound that can be noticed. The easiest and preferred method is to hide within an image by modifying some bits that do not cause color changes perceptible by the human eye. Similarly, video can be used in conjunction with cloaking, which is useful for concealing enormous amounts of data. In [3] Steganography differs from encryption, as encryption makes the confidential information unreadable, whereas steganography makes the message invisible by hiding it in another medium. Hence, the integration of encryption with Steganography will create a stronger level of protection for high-confidential data [4] the authors have suggested zipping the data in the beginning, especially if the data was text with a different language such as Arabic. In [5] Others tried with prediction of error rate which will result after insertion, and then they select the pixels which will output less error rate. In [6], used deep learning to detect the objects of images and their properties, and then the insertions will be in the parts which do not belong to these objects. In [7] Others tried with prediction of error rate which will result after insertion, and then they select the pixels which will output less error rate. In [8] That also enhanced the security and the amount of hidden data. Another method used the insertion in the histogram of the image. In [9] One of the easiest ways in spatial domain is changing the least significant bit (LSB) where each pixel is converted to binary code, then the lowest significant bit of this pixel will be replaced by the next bit of secret information. Normally, the insertion starts from the first pixel, then the second, and so on.

III. PROPOSED SYSTEM

The main idea is to duplicate the process of steganography itself by using two covers in addition to encryption. So, the secret data will be inserted in the first cover in the first step, and then the second data will be inserted in the cover and taken it as second cover, then the first step result will be considered as input (secret data) for the second cover. Thus the result of step one, will be inserted in the second cover as step two. However, before both steps, the main data will be encrypted by the 2D Logistic Mapping and AES algorithm. Then there would be two layers for hiding in addition to encryption.

Step 1: In addition to the shared key or password for AES, the user enters his secret message.

Step 2: Apply hashing function (MD5) on the key to ensure fixed length (128 or 256), whatever key the users selected. Then, the message will be encrypted using the AES technique, with the MD5 result key.

Step 3: Using the LSB technique, place the bits of the encrypted message in the first cover. Each pixel will be converted to binary before being replaced with another encrypted message bit (usually, in the first, we store the length of the message, then the message itself).

Step 4: Read the results of the previous step (image) into three matrices (one for each colour layer: Red, Green, and Blue) with the same dimensions for all matrices. We read pixel by pixel and convert it to binary, and then place each bit in a pixel of second cover in LSB.

Step 5: The resulting image from the previous step is sent to the receiver. Then, the extracting will be reversed steps.

A. AES

Advanced Encryption Standard (AES) the latest encryption standard approved by NIST is by far becoming the default choice for encryption in networked applications. The image will be a coloured one initially. But the stored images are in the converted into grey scale images to make easy for features extraction and the captured images are stored in a separate folder called dataset.

B. 2D LOGISTIC MAPPING

Although the 2D logistic map has various behaviors according to different system parameters, in the paper we concentrate on the parameter interval $r \in [1.1, 1.19]$, where the system is chaotic. The proposed image encryption method using the 2D logistic map and the internal loop is composed of 2D Logistic Permutation, 2D Logistic Diffusion and 2D Logistic Transposition where each stage itself is an image cipher and they together form the permutation-substitution network. Similar to the encryption procedure, the decryption procedure is nothing but reverse the order of processing using the decryption key. In short, the encryption process can be written as C = Enc(P,K), and the decryption process is P = Dec(C,K)

C. *STEGANOGRAPHY*

The well-known strategy that is utilized for steganography is the LSB. And additionally the prominent technique for present day, steganography is to utilize LSB of picture‘s pixel data. This investigation is utilized for one piece of the LSB. It inserts each piece of the double content piece with one piece of every pixel in the first picture. This strategy works when the record is longer than the message document and if picture is grayscale, when applying LSB strategies to every byte of a 24 bit picture, three bits can be encoded into every pixel .

Image to Image :- Using the stego key, a picture is put within another image in image steganography.

Text to Image :- In this, the text is inserted within the image and sends the image with the help of the symmetric key.

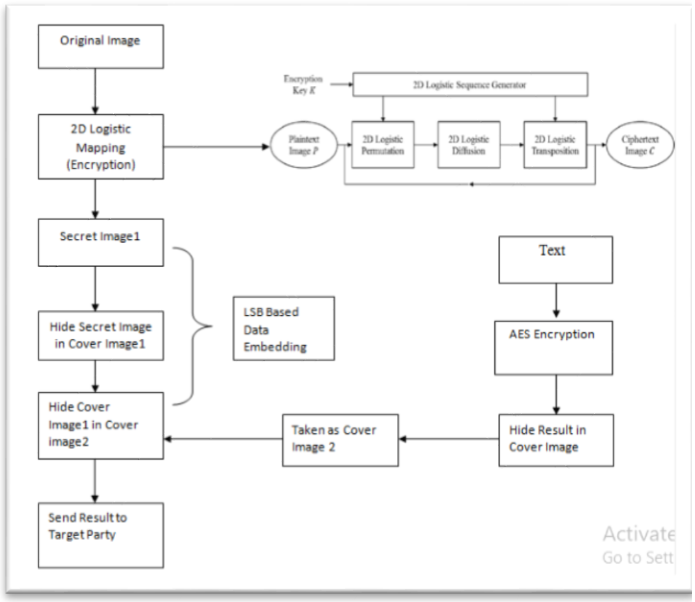

Figure 1. Block Diagram of Proposed Method

IV. Testing and Results

To prove the efficiency of the proposed the method and its applicability, we implemented it as a real application by using GUI(Graphical User Interface). Fig 2 and 3 show the Result of Encryption and Decryption .

LSB technique used in both 2D Logistic Mapping for encryption and AES for encryption. The application interfaces are depicted in the following diagrams. Fig.2 presents the hiding phase, where the user has to select the first cover, and second cover (in the future we can generate the first cover digitally). Then the user will enter the secret message and the shared password with receiver (Key of AES). We divided the steps to be clearer, so the first button will show the result of encryption, then the result image (Cover 1) after insertion. The second button will apply the second insertion in Cover 2 and show the result. Finally, the user can save the result as an image file to send it to the receiver (See Fig.3). Fig.3 Represents the extracting phase; here, the user has to select the received image and enter the shared key to get the secret message. The similarity was computed between the end result and the cover to prove the quality of the proposed method. Also, calculated the Mean Squared Error (MSE) metric and Bit Error Rate (BER) to Measure the rate of changes after hiding and rate of errors. Figure.3 shows the Correlation, MSE and BER results, among other things.

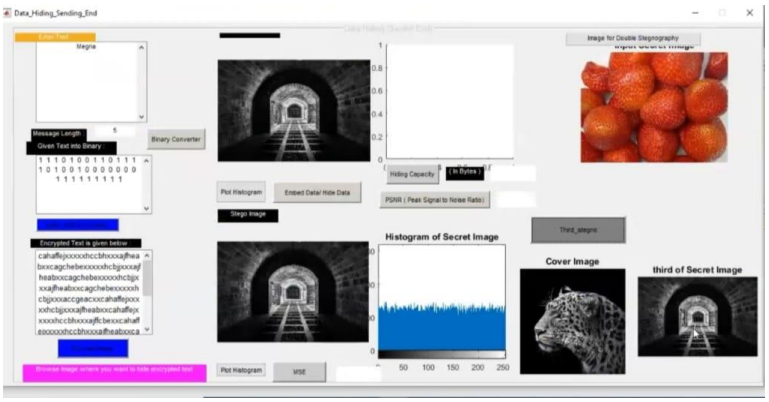

Figure 2. Block diagram of Transmitter End.

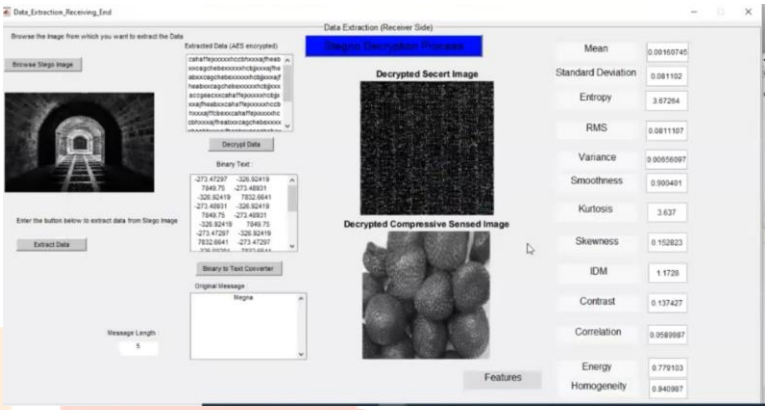

Figure 3. Block Diagram of Receiver End

CONCLUSION

In the paper it aims to develop a new idea to enhance the level of protection and security of secret data which hides inside another medium (Cover Image). Here applied the proposed method with LSB algorithm and 2D Logistic mapping along with AES to prove the applicability, usability and effectiveness. Later on, intend plan to apply on different secret data to provide most secure and resistant method for encryption and steganography.

ACKNOWLEDGEMENT

This paper was supported by Prof. Sapna P J, DEC, Dayananda Sagar college of Engineering, Bangalore.

REFERENCES

[1] M. Hussain, A. W. A. Wahab, Y. I. B. Idris, A. T. Ho, and K. H. Jung, "Image steganography in spatial domain: A survey," Signal Processing: Image Communication, vol. 65, pp. 46-66, 2018.

[2] A. M. Basahel, M. Yamin, and A. A. A. Sen, "Enhancing Security of Transmitted Data by Improved Steganography Methods," International Journal of Computer Science and Network Security, vol. 19, no. 4, pp. 239-244, 2019.

[3] M. Douglas, K. Bailey, M. Leeney, and K. Curran, "An overview of steganography techniques applied to the protection of biometric data," Multimedia Tools and Applications, vol. 77, no. 13, pp. 17333-17373, 2018.

[4] S. Malalla and F. R. Shareef, "Improving Hiding Security of Arabic Text Steganography by Hybrid AES Cryptography and Text Steganography, Journal of Engineering Research and Applications, vol. 6, no. 6, pp. 60-69, 2016.

[5] M. S. Al-Rahal, A. A A. Sen, and A. A. Basuhil, "High level security based steganoraphy in image and audio files," Journal of Theoretical and Applied Information Technology, vol. 87, no. 1, 2016.

[6] R. Meng, Z. Zhou, Q. Cui, X. Sun, and C. Yuan, "A novel steganography scheme combining coverless information hiding and steganography," Journal of Information Hiding and Privacy Protection, vol. 1, no. 1, 2019.

[7] M. S. Al-Rahal, A. A A. Sen, and A. A. Basuhil, "High level security based steganoraphy in image and audio files," Journal of Theoretical and Applied Information Technology, vol. 87, no. 1, 2016.

[8] X. Li, W. Zhang, X. Gui, and B. Yang, "A novel reversible data hiding scheme based on two-dimensional difference-histogram modification," IEEE Transactions on Information Forensics and Security, vol. 8, no. 7, pp. 1091-1100, 2013.

[9] C. K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," Pattern Recognition, vol. 37, no. 3, pp. 469-474, 2014.