Abstract— Digital image processing is the use of computer algorithms to perform image processing on digital images. Both the image and text are encrypted by AES encryption technique. Initially the text/information is encrypted and the encrypted information is transferred through e-mail or by any other storage medium. Then the key used for encrypting and decrypting the text is embedded into the image which is encrypted later. Now the sender needs to select the required image that needs to be sent. After the selection of the image the sender will now split the image into sub-images. The image is split into different parts. The splitting of image is done in order to reduce the loss of information. Now the sender will select any one mini image for embedding the private key of the encrypted text. This private key that is embedded in image will be used for decrypting the text. Now the image that is split is now again merged into a single image. The image is then further encrypted. The encrypted image is also transferred through e-mail or any other storage medium along with the encrypted text. Now for the decryption of the image the receiver must have the private key which would be shared by the sender through any means of communication.

In the previous system no private key encryption was available which made it a less secure. Hence, The decryption process is secured by a ciphering technique known as S-cipher. By using this technique it gives further security to the private key. The receiver on receiving the key, will enter the key in required field. After entering the valid data the decryption process of the image will take place. After decryption of image the receiver will get the private key that is used for the decryption of text/information send by the sender.

Keywords— Image processing , Sender, Splitting, Embedding, Merged, Receiver , S-cipher

I. INTRODUCTION

Sometimes, Image Processing is defined as “a discipline in which both the input and output of a process are images. The growing research interests in the field of digital image processing during the last decade have changed this estimation about a picture. Now pictures in their digital representations speak much more than a thousand words, thanks to the digital image data hiding technique known as Steganography. Steganography is a process of secret communication where a piece of information (a secret message) is embedded into another piece of innocent looking information, popularly called a cover, in such a way that the very existence of the secret information remains concealed without raising any suspicion in the minds of the viewers. The stego-image is send to the receiver. On the other side, it is processed by the extraction algorithm using the same key. During the transmission of stego-image unauthenticated persons can only notice the transmission of an image but can’t see the existence of the hidden message.

The objective of this project is to encrypt the information within the image by placing the information at the desired lattice points. Once the information is placed at desired lattice points, The encrypted information will be stored. And for further security purpose the image which have the
message will be encrypted. For decryption of this image and the message, two private keys are used. These private keys can be obtained from the user. Furthermore, in this project a new ciphering technique for private key will be used which is known as S-cipher. This project is especially used for military purpose. This ciphering of private key using S-cipher can be matured by constantly updating and then the error fixing should be constantly done to provide the updated security.

II. EXISTING SYSTEM

A set of papers focuses on the encryption and decryption of the image as well as the encryption and decryption of the text. The Permutation is a commonly used primitive in multimedia (image/text) encryption schemes, and many permutation-only algorithms have been proposed in recent years for protection of multimedia data. In permutation-only image ciphers, the entries of the image matrix are scrambled using a permutation mapping matrix which is built by a pseudo-random number generator. In existing concept, both the text and image will be encrypted and transfer of the images is done by using private key production. There is no private key encryption process. Image security is provided by using private key only.

III. PROPOSED SYSTEM

In the proposed concept, both the image and text are encrypted by AES encryption technique. Initially, the text/information is encrypted and the encrypted information is transferred through e-mail or by any other storage medium. Then the key used for encrypting and decrypting the text is embedded into the image which is encrypted later. Now the sender needs to select the required image that needs to be sent. After the selection of the image the sender will now split the image into sub-images. The image is split into different parts. The splitting of image is done in order to reduce the loss of information. Now the sender will select any one mini image for embedding the private key of the encrypted text. This private key that is embedded in image will be used for decrypting the text. Now the image that is split is now again merged into a single image. The image is then further encrypted. The encrypted image is also transferred through e-mail or any other storage medium along with the encrypted text. Now for the decryption of the image the receiver must have the private key which would be shared by the sender through any means of communication. The use of new ciphering technique S-cipher will make the private key more secure. More than one key is needed to attain the decryption of image. Placing the information at the desired location within image will ensure and will help the users know whether loss of information has occurred or not. In the previous system no private key encryption was available which made it a less secure. Hence, The decryption process is secured by a ciphering technique known as S-cipher. By using this technique it gives further security to the private key. The receiver on receiving the key, will enter the key in required fields. After entering the valid data the decryption process of the image will take place. After decryption of image the receiver will get the private key that is used for the decryption of text/information send by the sender.

IV. MAIN CONCEPT

Objective of the project is to encrypt the information within the image by placing the information at the desired lattice points. Once the information is placed at desired lattice points, The encrypted information will be stored. And for further security purpose the image which have the message will be encrypted. For decryption of this image and the message, two private keys are used. These private keys can be obtained from the user. Furthermore, in this project a new ciphering technique for private key will be used which is known as S-cipher. This project is especially used for military purpose.
V. ARCHITECTURE

5.1 Architecture Diagram Explanation:
The block diagram gives an explanation about the process done in both the sender side and also in the receiver side. Initially in the sender side, the sender will encrypt the information which has been stored in a file and then generate the private key for that encrypted file.

Then the sender will select new image. Then the selected image will be split into many images as mini-images. Then the key to decrypt the information is encoded in any one of the mini-images (sender’s choice). When the encode has been finished the splitted images will be merged together. Then the merged image is encrypted.

A key will be generated to decrypt the image; both the keys will be secured by using S-Cipher. The encrypted information and the encrypted image along with the keys will be send to the receiver through the e-mail or any other storage medium.
In the receiver side, the receiver will get the encrypted information, then the encrypted image and the keys from the e-mail or from any other storage medium through which the sender had send it.

The receiver will decrypt the image by using the key. Then the receiver will get the decrypted image. Then the decrypted image will be splitteded to decode the key. The decoded key will be used to decrypt the encrypted information. Once the information has been decrypted the original information will be displayed to the receiver.

Both the image and the information will be encrypted and decrypted by using the AES algorithm. Both keys which is used in the decryption of the image and in the decryption of the image will be secured by using cipher technique called S-Cipher.

5.2 MODULES:
These are the following modules that are followed for the encryption of information, image and private key ciphering using S-cipher.

1. Splitting of images: The Sender will first select an image in an format. Then the selected will be splitted into different parts known as mini-images.
2. Encoding and Decoding the key within image: The information which should be send to the receiver will be encrypted and then a private key will be generated. Then the generated private key will be encoded in any one of the mini-images (sender’s choice) which has been splitted before by the sender. The receiver will decrypt the received image and then the decrypted image will be splitted as mini-images. Then the receiver will decode the private key from the mini-image.
3. Merging of mini-images: The information will be stored then the mini-images will be merged together for encryption.
4. Encryption and Decryption for information and the image: In the sender side, the sender will encrypt the information and then generate a private key. The encrypted image and the information will be sending to the receiver. Then in the receiver side, the receiver first decrypts the received image by using the private key in the S-Cipher. Then the decoded key is used to decrypt the received information. Then the original information will be retrieved.

VI. ALGORITHM USED

6.1 Advanced Encryption Standard (AES):
The Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST). The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data.

Among the requirements were that the new algorithm should allow key sizes of 128, 192 and 256 bits, it should operate on the blocks of 128 input bits, and it should work on a variety of different hardware, for example, 8-bit processors that could be used in smart cards and the 32-bit architecture commonly used in personal computers.

The speed and the cryptographic strength were important considerations. The AES algorithm consist of 10 rounds when the key has 128 bits (when the key has 192 bits, 12 rounds are used, when the key has 256 bits, 14 rounds are used). There is also a 0th round key, which is the original key.

A round starts with an input of 128 bits and produce an output of 128 bits. There are four basic steps, called layers, that are used to form rounds:
1. **The ByteSub Transformation (BS):** The non-linear layer is for resistance to differential and linear cryptanalysis attacks.

2. **The ShiftRow Transformation (SR):** The linear mixing step causes diffusion of the bits over multiple rounds.

3. **The MixColumn Transformation (MC):** This layer has a purpose similar to ShiftRow.

4. **AddRoundKey (ARK):** The round key is XORed with the result of the above layer.

5. And then the Round is

   ![AES Round Diagram](image)

**Figure No. 6.1 The Round In Advanced Encryption Standard**

In present day cryptography, AES is widely adopted and supported in both hardware and software. Till date, no practical cryptanalytic attacks against AES has been discovered. Additionally, AES has built-in flexibility of key length, which allows a degree of ‘future-proofing’ against progress in the ability to perform exhaustive key searches.

However, just as for DES, the AES security is assured only if it is correctly implemented and good key management is employed. This module performs server-side encryption of the messages.

The Advanced Encryption Standard (AES) algorithm requires two input functions to produce the encrypted message which is to be saved on to the mongoDB database. The two input functions are data and the key.

The features of AES are as follows –

- Symmetric key symmetric block cipher.
- 128-bit data, 128/192/256-bit keys.
- Stronger and faster than Triple-DES.
- Provide full specification and design details.
- Software implementable in C and Java.
AES is an iterative rather than Feistel cipher. It is based on ‘substitution–permutation network’. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).

Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes.

**6.2 Algorithm for S-cipher:**

**Step1:** Start  
**Step2:** Get the private key from the sender.  
**Step3:** Enter the private key in the first field.  
**Step4:** Now for the second field count the letters in the private key using string length function  
Example: private key=1  
String length for 1 is one = 3  
3 is the string length for 1(one).  
**Step5:** Now enter the string length of the primary key in the secondary key field.  
**Step6:** For the third key field add both the string length of the primary and secondary key and add the numeric private key for final result.  
**Example:** private key=1  
If 1=one,3= three, then one+three  = 8  
Then add 1+8=9  
**Step7:** If all the fields satisfy the S-cipher condition, then decrypt the image and text in respective manner, else invalid key is entered.  
**Step8:** Stop.
VII. CONCLUSION

In this project, we are going to provide more security to the encrypted image by providing two private keys: one for encryption and decryption of the image and another one for encryption and decryption of the information. The Private Key will be stored at the desired position within the image. The above two private keys will be encrypted by using a new technique called S-cipher. In this project, the data loss will be reduced.

For the Future Work, the S-Cipher should be constantly updated and then the error fixing should be constantly done to provide the updated application.

REFERENCES

I. Alireza Jolfaei, Xin-Wen Wu, and Vallipuram Muthukumarasamy, “Compressing encrypted images with auxiliary information”, IEEE TRANSACTION ON IMAGE PROCESSING, 2017


