Encrypting and Decrypting Message via Image Slicing

Sudeshna Khedekar [1], Digvij Akre [2], Vishakha Mulik [3], Prof. Bhavna Arora [4]

[1], [2], [3]Student, Department of Computer Engineering, Atharva College of Engineering, Mumbai
[4]Professor, Department of Computer Engineering, Atharva College of Engineering, Mumbai

---

Abstract - Communication via message has become a major and effective part of our day-to-day life. Even though it is convenient to send messages and receive data. One of the main problems that we face these days is Data Security. That is where encryption and decryption of the data comes into play and there exists multiple encryption and decryption algorithms to serve the purpose. But, using only one algorithm for this, is generally not secure enough. So, by using effectives encryption and decrypting standards for effective approach to provide Message encryption

Key Words*: *Cryptography, Steganography, Encryption, Decryption, AES (*Advanced encryption standard*), LSB (least significant bit).

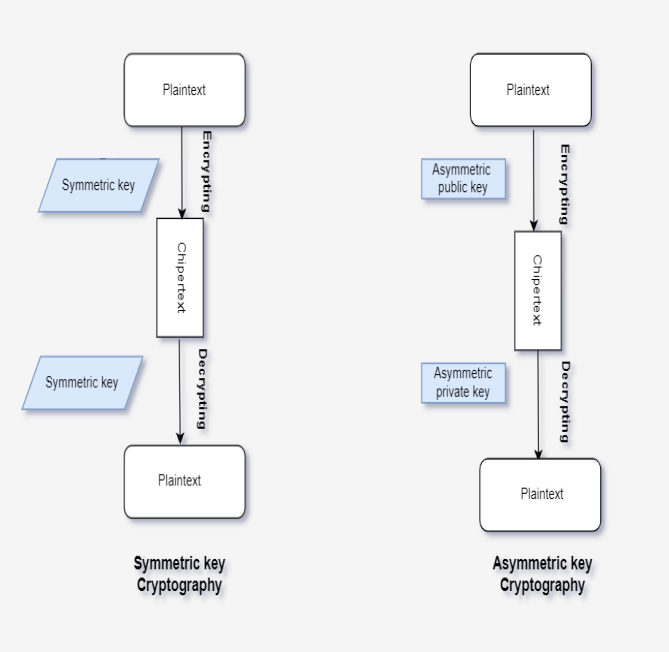
1. INTRODUCTION

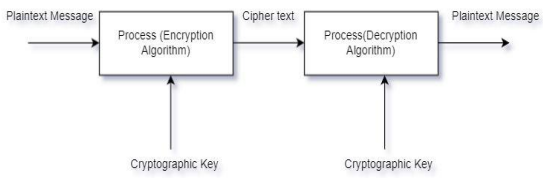
In today's world, we use many types of digital data. The information between mobile devices and computers is transmitted via one network in various form. But, do you think your confidential information and the security of that data over the internet are secure? No, the confidential data and information in today's advanced world are not safely transferred via the network. And Our data is stolen by unauthorized users on daily basis. Hence, ensuring the Security and Confidentiality of data transmission is a very important and current necessity. This security can be achieved by different techniques. One of the techniques is Steganography and Cryptography.

Cryptography techniques can be described into two types' Symmetric- key cryptography and Asymmetric-key cryptography. [11]Under Symmetric-key cryptography, only one key is carried out process between the sender and the receiver. Whereas In Asymmetric-key cryptography we have two different keys one is a public key and another one is the private key. A public key is revealed to all, and a private key is secretly known to the authorized recipient of that data. In the Cryptography technique, even if the data is sent securely, it gives the clue of the existence of secret data to the third-party source. However, In the Steganography technique, there is no such clue given that will unintended recipient as the secret data is hidden inside another data.

1.1 MOTIVATION OF PROJECT

As per the knowledge the technology is going advanced and growing day by day. Our main motto is to send data securely over the internet. The idea behind our project can be used by many sectors like financial services, defence, detective agencies, government sectors.





1.2 BASIC CONCEPT

Our solution is to transfer the data securely via image. To Securely carry out the process of hiding the data in image. Algorithm like image slicing, image stitching, AES, LSB are used. To maintain real time integrity and authenticity of the process it will asked to enter a 16-bit AES key to encrypt the data and same key is used by receiver to decrypt the data in between this process LSB, image slicing and image stitching techniques will be applied to securely encrypt and decrypt the data.

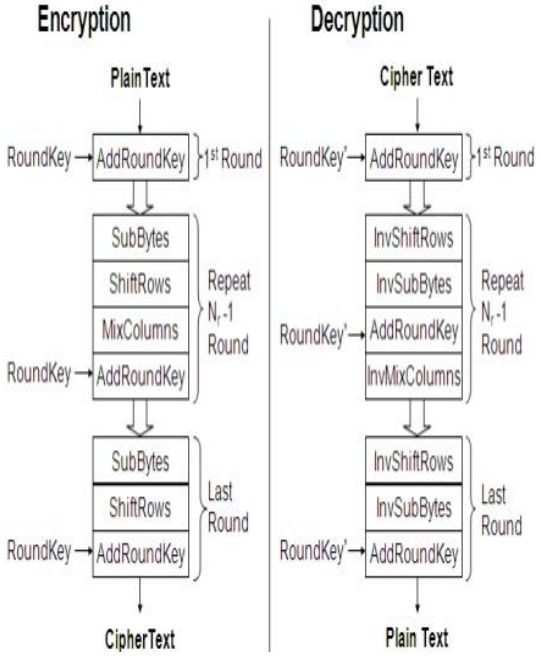
2. BACKGROUND STUDY

The basic ideology of this project came from a background study of [5] Information hiding in images using a steganography technique paper written by Ramadhan Mstafa and Christian Bach. Where they have used steganography and different watermarking technique for securely transferring the data and from other paper [3] Image Security using Image Encryption and Image Stitching paper written by Jyoti T.G. Kankonkar and Prof. Nitesh Naik, where image stitching techniques are used to securely transfer the data. So, in an effort to make the process more secure, our idea of using image slicing and image stitching with cryptography and steganography techniques to provide more security of data that is to be transmitted over an internet.

3. OVERVIEW OF ALGORITHMS:

1. ADVANCED ENCRYPTION STANDARD (AES)

The advanced encryption standard (AES) is a symmetric-key block cipher that was published by the (NIST) National Institute of Standards and Technology in December 2001.[9] AES is a non – Feistel cipher. It encrypts and decrypts 128 bits data blocks. How many rounds will be carried out will depend on the key length i.e. If the key length is 128 bits it has 10 rounds, if the key length is 192 bits there are 12 rounds to carry out. Whereas if the key length is 256 it has bit 14 rounds.

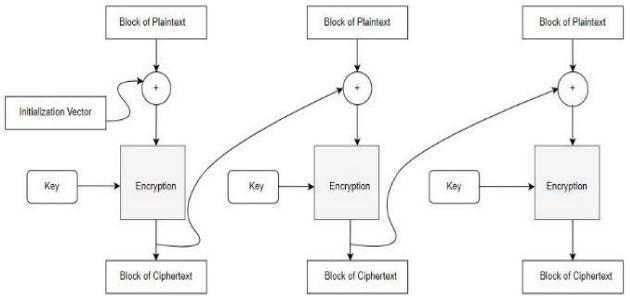


[4] AES has three different AES versions: AES-128, AES-192, and AES-256. Every round has sub bytes, shift rows, mix columns and add round key. In the sub bytes, we interpret the byte as two hexadecimal digits. Where the row defines the left digits and the column that defines the right digit. The function of the two hexadecimal digits of the row and column is the new bytes. Shift rows are shifting to the left. In the Mix column step, it is to mix the column matrix. In add round key step it adds the round keyword with every state column matrix

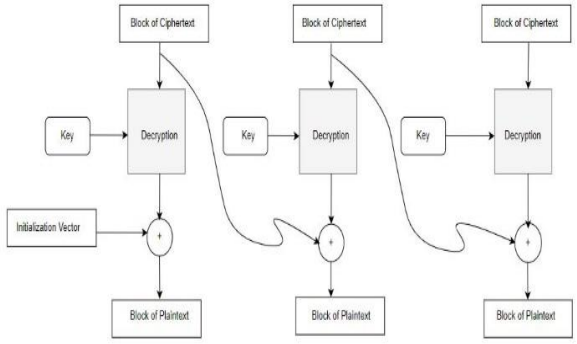
1.1 CIPHER-BLOCK CHAINING (CBC) MODE

The CBC mode is as for including XOR to every plaintext block to the cipher text block that was created prior. Keeping the use of same approach where cipher algorithm used for encrypting the result. The first block act as resultant block of cipher text, every following block of plaintext is then XOR with the preceding block of cipher text prior to encryption, the action perform is termed as chaining that comes in cipher block chaining. To keep away from making identical output cipher text blocks from identical plaintext data this mode is being implied for encryption in CBC mode i.e. Cipher block chaining mode which will only be done using one thread.

Despite this disadvantage, this could be a really common approach that makes use of block ciphers. CBC mode is used in lots of applications. all through decrypting of a cipher text block, one should add XOR the output data acquired from the decoding(decrypting) algorithms to the preceding cipher text block. due to the receiver is aware of all of the cipher text blocks simply when getting the encrypted message, he's going to decipher the message by the use of numerous threads on the same time. Decryption in the CBC mode works in the opposite order. while decrypting the final block of cipher text, the ensuing data is XOR'd with the preceding block of cipher text to recover the initial plaintext.



- Encrypting in the CBC Mode.



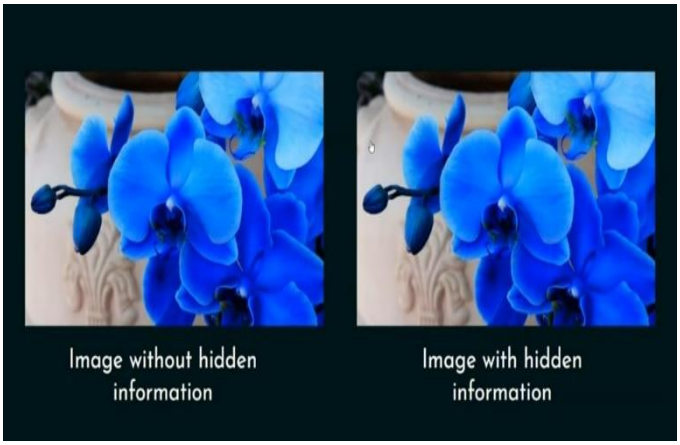
-Decrypting in the CBC Mode.

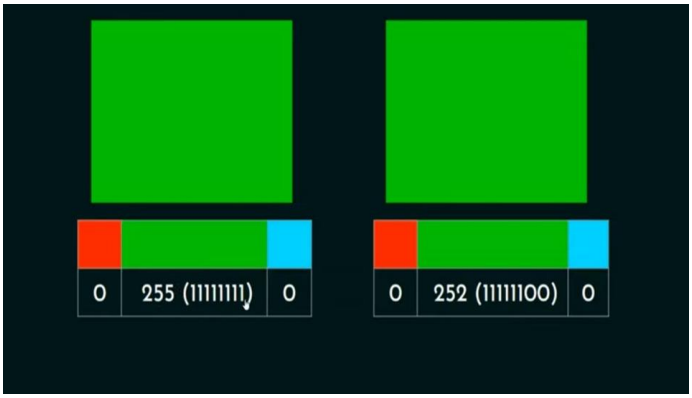
2. LEAST SIGNIFICANT BIT

LSB steganography is one technique that merge the hidden data inside an image. In a Gray scale image, every pixel is represented in 8 bits. The last bit of the pixel is called as Least Significant bit as its value will affect the pixel value only by "1". [7] In short LSB technique is used to hide the data in the image. If someone considered the last two bits as a LSB bits it will affect the pixel value only by "3". This helps in hiding extra data.

LSB steganography is a technique where the last bit of any selected image is replaced with a data bit. As this method is vulnerable to steganalysis so as to make it more secure, we first encrypt that data in a raw manner. Before merging the data in the image. While it increases time complexity during encryption process, it provides higher security also.

This approach is very simple. In this method, the LSB bits of some or all of the bytes present within an image are replaced with bits of the secrete message. [2] To hide message with in several multimedia carrier data by using one of the basic techniques called LSB approach. LSB embedding may even applied in specific data domains - to give an example, embedding a hidden message into the color values of RGB bitmap data, or inside the frequency coefficients of a JPEG image. We can also applied LSB embedding approach to a variety of data formats and types. Therefore, Nowadays LSB embedding is a primarily important and popular steganography technique.





3. IMAGE SLICING

Image slicing is method is simple process of cutting the images into pieces without any changing in dimension or changing any features of the image image is slide into matrix form by increasing size of matrix number of sliced images can be increased

4. IMAGE STITCHING

[4] Image stitching is the process which is carried out where the image is stitched without changing any dimension or changing any features of the image it is an opposite of image slicing process

4. PROPOSED SYSTEM

4.1 IMPLEMENTATION

Process flow is as follow:

Sender side:

Step 1: The data which is shared over the internet is unsafe and easy to access. To protect them using key, which will be in the 128-bit format. The key is shared between only sender and receiver to access the confidential data.

Step 2: After entering plain text it will get encrypted by using AES algorithm. Advance Encryption Standard

algorithm is used to encrypt the plain text which is entered by the sender using key. It converts original data to an unreadable format so that stranger or attacker is not able to read or understand the original data. The plain text if hard to read is known as cipher text.

Step 3: After converting the data into cipher text It will hide inside cover medium using LSB steganography. [8] The cover medium can be in various form like audio, image, video or text document. The size of the image is depending on the amount of data which is entered by the sender. After done with all process the image called as stego image.

Step 4: Image Slicing is simple process of cutting the images into pieces without any changing in dimension or changing any features of the image. Image is slide into matrix form. By increasing size of matrix number of sliced images can be increased.

Step 5: Finally, receiver received the data via stego image in slices without any changing in dimension or changing any features of the image. By increasing size of matrix number of sliced images can be increased.

Receiver side:

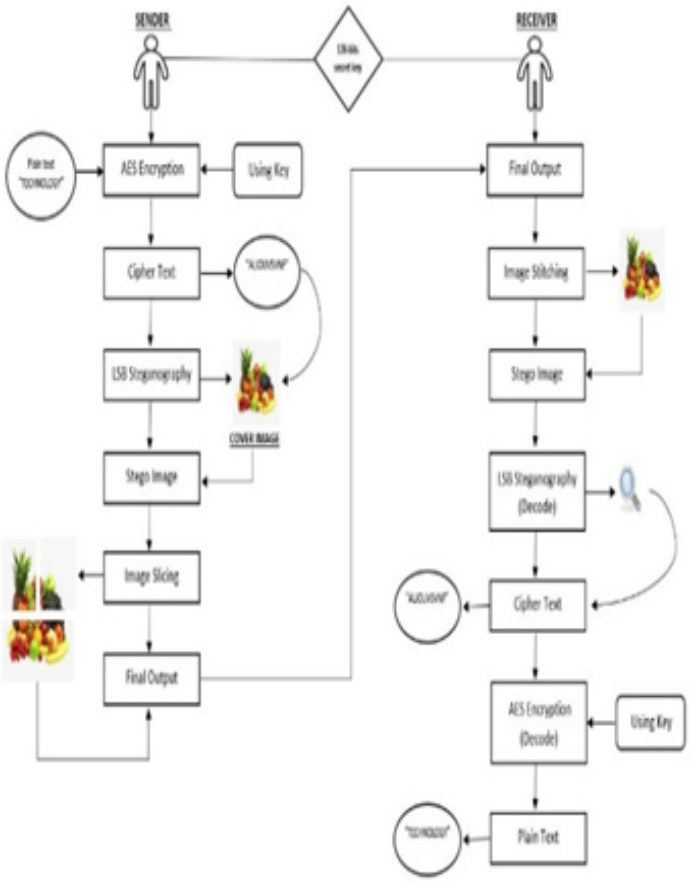
Step 1: Receiver received the data via stego image in slices without any changing in dimension or changing any features of the image. Now, the image in slices will get stitched using image stitching process. process where the image is stitched without changing any dimension or changing any features of the image. It is an opposite of Image Slicing process. After this process the entire image is called as stego image.

Step 2: We got the image then apply the LSB decoded algorithm. For the algorithm we used the image got after image stitching apply the algorithm then we find the cipher text which is hidden inside the stego image.

Step 3: Using this cipher text and 128-bits key which is shared between sender and receiver as input we apply AES decode algorithm to get the original data file. The process of decryption of an AES cipher text is opposite to the AES encryption process. Each round consists of the four processes conducted in the reverse order 1. Add round key, 2. Mix columns, 3. Shift rows, 4. Byte substitution.

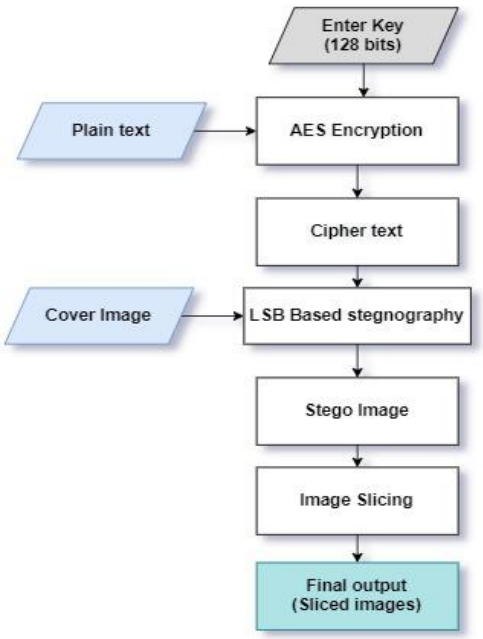
Step 4: Finally, receiver received the confidential data safely without any anonyms attack.

4.2 SYSTEM DESIGN

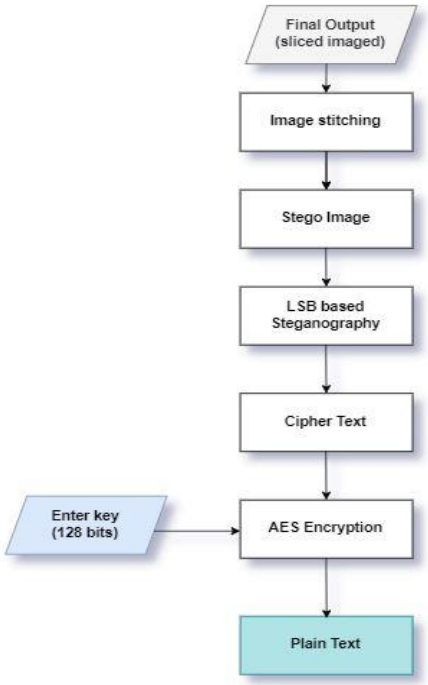


5. DESIGN DETAIL

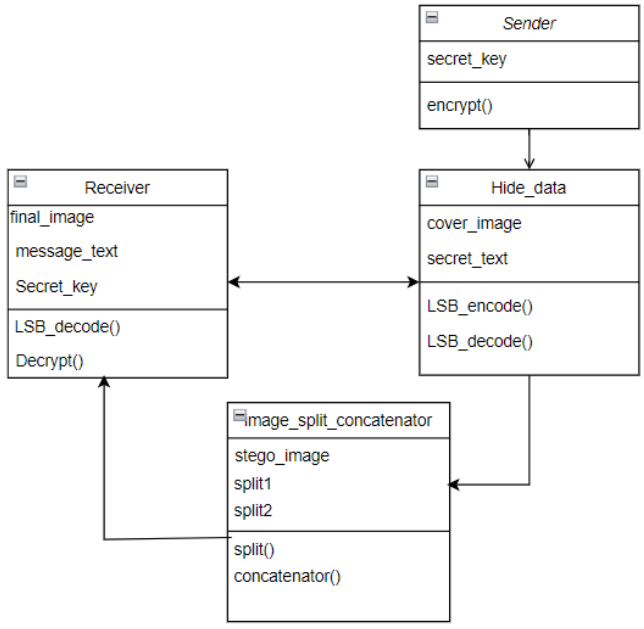
5.1 SENDERS FLOWCHART



5.2 RECEIVER FLOWCHART



5.3 CLASS DIAGRAM



6. FUTURE SCOPE

This idea and approach that we have implemented does not end here. There can be a future scope for development we can extend this particular project into multiple platforms. Particularly, we can incorporate additional algorithm together to make is more appealing.

One other scope of improvement in expanding the idea hiding the data into a video format so that the application can be more secure so that different sector can use this to secure the way of communication between the user and themself. As specially, since the sensitive data can be stored without anyone knowing about it. Such that storing sensitive data won't be a problem it as we add higher level of security.

7. CONCLUSION

In this project we have combine different data security technique to share data on an unreliable channel. This Hybrid technique consist of AES Cryptography, LSB Steganography, Image slicing and image stitching process. Using this Hybrid technique, we are able to retrieve the data at receiver end without any Data loss. so, we believe various sector and entity can greatly benefit from our application in the current scenario, also maintaining authenticity and integrity of the entire

REFERENCES

[1] Wafaa Mustafa Abduallah and Abdul Monem S. Rahma,"A Review on Steganography Techniques", American Scientific Research Journal for Engineering, Technology, and Sciences (ASRJETS), ISSN (Print) 2313-4410, ISSN (Online) 2313-4402

[2] Rajarathnam Chandramouli and Nasir D. Memon, "Analysis of LSB based image steganography techniques", 2001 International Conference onVolume: 3, DOI: 10.1109/ICIP.2001.958299

[3] Jyoti T.G.Kankonkar and Prof. Nitesh Naik,"Image Security using Image Encryption and Image Stitching", Proceedings of the IEEE 2017 International Conference on Computing Methodologies and Communication

[4] Ako Muhammad Abdullah, "Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data"

[5] Ramadhan J. Mstafa and Christian Bach, "Information Hiding in Images Using Steganography Techniques", Northeast Conference of the American Society for Engineering Education (ASEE)At: Norwich University David Crawford School of Engineering, DOI:10.13140/RG.2.1.1350.9360

[6] Nikhil Patel and Shweta Meena, "LSB based image steganography using dynamic key cryptography", 2016 International Conference on Emerging Trends in Communication Technologies (ETCT), DOI:10.1109/ETCT.2016.7882955

[7] Arun Kumar Singh, Juhi Singh and Dr. Harsh Vikram Singh, "Steganography in Images Using LSB Technique", International Journal of Latest Trends in

Engineering and Technology (IJLTET), ISSN: 2278-621X

[8] Dr. Amarendra K, Venkata Naresh Mandhala, B.Chetan gupta, G.Geetha Sudheshna, V.Venkata Anusha, "Image Steganography Using LSB", international journal of scientific & technology research volume 8, issue 12, december 2019, issn 2277-8616

[9] M.Pitchaiah, Philemon Daniel and Praveen, "Implementation of Advanced Encryption Standard Algorithm", International Journal of Scientific & Engineering Research Volume 3, Issue 3, March -2012,ISSN 2229-5518

[10] M. Pavani1, S. Naganjaneyulu, C. Nagaraju, "A Survey on LSB Based Steganography Methods" International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 2 Issue 8 August, 2013 Page No. 2464-2467

[11] Akshay Kekunnaya, Rajeshwari Gundla , Siddharth Nanda, "A research Paper for Symmetric and asymmetric cryptography", ijrece vol. 7 issue 2 (april-june 2019), issn: 2393-9028 (print) | issn: 2348-2281 (online)