Information Hiding Secretly Using Image Steganography

Akinapally Manideep[1*], Chiluka Nandu Vardhan Reddy[2], Bangaru Srujana[3],
Sarikonda Sree Hari Raju[4]

[1,2,3]B.Tech. Student, Department of Computer Science and Engineering, Nalla Narasimha Reddy Education Society's Group of Institutions, Hyderabad, India

[4]Associate Professor, Department of Computer Science and Engineering, Nalla Narasimha Reddy Education Society's Group of Institutions, Hyderabad, India

***Abstract*: Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Cryptography is a technique associated with the process of converting ordinary plain text into unintelligible text and vice-versa. In contrast to cryptography, steganography is not to keep others from knowing the hidden information, but it is to keep others from thinking that the information even exists. Together cryptography and Steganography can provide a powerful basis for data security. The main purpose of this project is to produce a security tool based on steganography and cryptography techniques for sending and receiving sensitive information over the internet. The program first encrypts the message data using AES algorithm and then embeds the result of encrypted data in the provided image file using steganography technique. The system also provides the feature for extracting the hidden data from the corresponding image file and decrypting the extracted data for eventually finding the original message. The embedding process follows image's LSB replacement algorithm. To obtain the hidden message, the process is reversed. Using the system produced, messages were successfully encrypted and hidden inside an image file. Also, using the generated stego image, the hidden message was extracted and decrypted successfully.**

***Keywords*: Steganography, Least Significant Bit (LSB), Cryptography, Advanced Encryption Standard (AES).**

1. Introduction

In this present era, the security of information has become a fundamental issue. Maintaining the integrity and confidentiality of sensitive information, blocking the access of sophisticated hackers is very important. Steganography is a technique of hiding information in digital media Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Many different carrier file formats can be used, but digital images are the most popular ones because of their frequency on the internet. Similarly, Cryptography is the science of protecting information by transforming it into a secure format. In contrast to cryptography, steganography is not to keep others from knowing the hidden information but it is to keep others from thinking that the information even exists.

Both Steganography and Cryptography are data hiding techniques with different but related fields of applications. Steganography prevents the detection of hidden messages whereas cryptography converts ordinary plain text into encrypted unintelligible text and vice-versa by applying encryption tools. Generally, steganography is used to supplement encryption. An encrypted file or message may also be hidden using steganography, so even if the encoded stego image is decoded, the hidden message is still not understandable. Thus, together cryptography and steganography can provide a powerful basis for data security.

With growing digitization in every field, digital security has become a fundamental aspect. Also, because of development in internet technology, digital media can be transmitted conveniently over the network. This calls for security over the internet. Throughout history steganography and cryptography have been used to secretly communicate information between people. In the past, means of cryptography and steganography were carried out using traditional methods of pen and paper, using invisible ink, etc. Therefore, with the increasing use of communication of information over digital medium, security for digital methods are to be developed. Steganography hides data onto a stego medium. Steganography along with cryptography tools can ensure even more data security.

The main objectives of this project are:

- To produce security tools based on steganography and cryptography techniques combined.
- To avoid drawing suspicion to the existence of a hidden message.

2. Algorithm and Technique

A. Advanced Encryption Algorithm

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) in 2001. AES is widely used today as it is a much stronger than DES and triple DES despite being harder to implement.

Points to remember:

- AES is a block cipher.

[*] Corresponding author: akinapallymanideep25@gmail.com

- The key size can be 128/192/256 bits.
- Encrypts data in blocks of 128 bits each.

That means it takes 128 bits as input and outputs 128 bits of encrypted cipher text as output. AES relies on substitution-permutation network principle which means it is performed using a series of linked operations which involves replacing and shuffling of the input data.

B. Least Significant Bit

A common approach of hiding data within an image file Least Significant Bit (LSB). Each pixel of image is composed of 3 values(Red, Green, Blue) these can be represented using binary code. In this we can take the binary representation of the hidden and overwrite the LSB of each byte within the cover image. Right most bit is the least significant bit, if we change the rightmost bit it will have less impact on the final value. Which a human naked eye can't recognize the changes in sight changes.

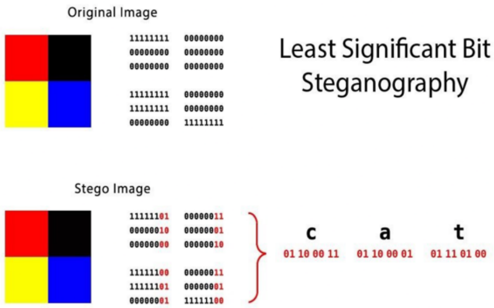

Fig. 1. LSB steganography

3. Implementation

A. Encryption

Encryption is a way of scrambling data so that only authorized parties can understand the information. In technical terms, it is the process of converting human-readable plain text to incomprehensible text, also known as cipher text. In simple terms, Encryption is the method by which information is converted into secret code that hides the information's true meaning. The science of encrypting and decryption information is called cryptography. In computing, unencrypted data is also known as plain text, and encrypted data is called cipher text. Encryption plays an important role in securing many different types of information technology assets. It provides confidentiality and also more security to the data. There are two different types of encryption. The primary purpose of encryption is to protect the confidentiality of digital data stored on computer systems or transmitted over the internet or any other computer network. They are symmetric encryption and Asymmetric encryption. Symmetric encryption, also referred to as secret key encryption, uses a single key. The most widely used symmetric key cipher is the Advanced Encryption Standard (AES), which was designed to protect government-classified information. Asymmetric encryption also known as public key encryption, which uses two different keys. The Rivest Shamir Adleman (RSA) encryption algorithm is currently the most widely used public key algorithm. With RSA, the public or the private key can be used to encrypt a message; whichever key is not used for encryption becomes the decryption key.

In this system, for the encryption process it uses Algorithm. AES Algorithm is an symmetric algorithm which means it uses a single key for encryption and decryption. AES is widely used today as it is much stronger than DES and triple DES despite being harder to implement. The AES Encryption algorithm is a symmetric block cipher algorithm with a block size of 128 bits. It converts these individual blocks using keys of 128, 192, and 256 bits. With respect to key size they are the number of rounds to be performed. For key lengths 128,192 and 256 bits the respective number of rounds are 10, 12 and 14 rounds. Once it encrypts these blocks, it joins them together to form the cipher text. It is based on a substitution-permutation network, also known as an SP network. Some of the steps are involved in

AES Algorithm are as follows:

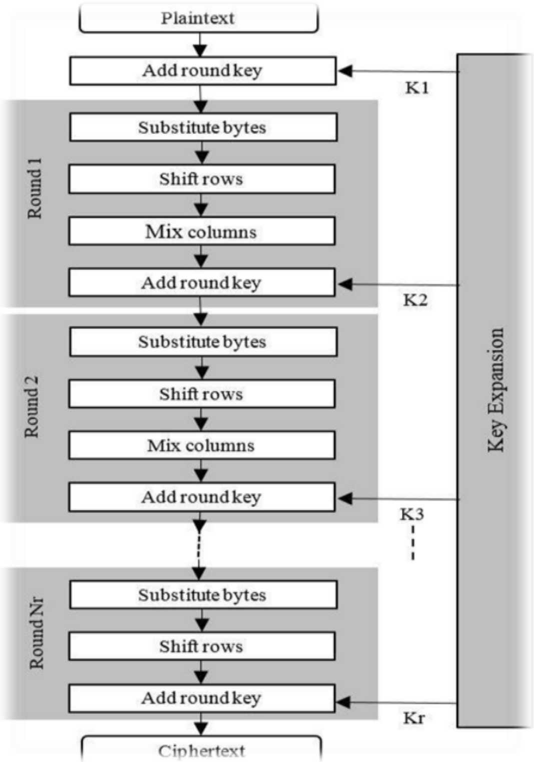

Fig. 2. LSB steganography

Since a single block is 16 bytes, a 4x4 matrix holds the data in a single block, with each cell holding a single byte of information. The matrix is known as a state array. Similarly, the key being used initially is expanded into (n+1) keys, with n being the number of rounds to be followed in the encryption process. The mentioned steps are to be followed for every block sequentially. Upon successfully encrypting the individual blocks, it joins them together to form the final cipher text. The steps are

- *Add Round Key:* You pass the block data stored in the state array through an XOR function with the first key generated. It passes the resultant state array on as input to the next step.

- *Shift Rows:* It swaps the row elements among each other. It skips the first row. It shifts the elements in the second row, one position to the left. It also shifts the elements from the third row two consecutive positions to the left, and it shifts the last row three positions to the left.
- *Mix Columns:* It multiplies a constant matrix with each column in the state array to get a new column for the subsequent state array. Once all the columns are multiplied with the same constant matrix, you get your state array for the next step. This particular step is not to be done in the last round.
- *Add Round Key:* The respective key for the round is XORed with the state array obtained in the previous step. If this is the last round, the resultant state array becomes the cipher text for the specific block; else, it passes as the new state array input for the next round.

B. *Encode*

Encode is a technique which embeds the cipher text into the cover image, generates a stego image. For embedding the data into image it uses LSB (Least Significant Bit) Algorithm. The Least Significant Bit (LSB) steganography is one such technique in which the least significant bit of the image is replaced with a data bit. Human naked eye can't recognize the sight changes in the stego image. Each pixel of image is composed of 3 values (RGB) i.e., Red Green Blue.

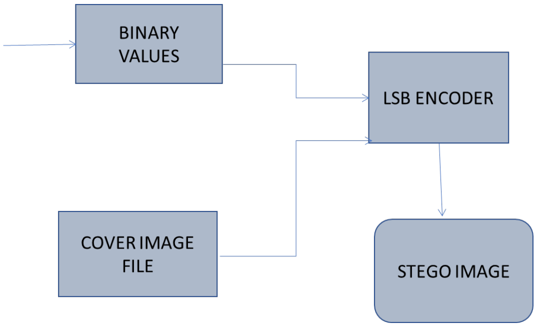

Fig. 3. Encode process

C. *Decode*

Decode allows you to extract data from Stego images. For extracting the data from the image it uses the LSB Algorithm. The Least Significant Bit (LSB) steganography is one such technique in which the least significant bit of the image is replaced with a data bit. First of all, the decoder takes the stego image as input, and then it extracts the each of LSB bit from the stego image until to find out the end bit. Reconstruct the collecting LSB bits from the stego image.

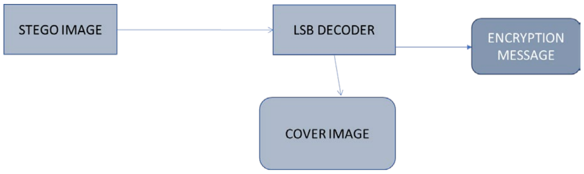

Fig. 4. Decode process

D. *Decryption*

Decryption is the process of transforming data that has been rendered unreadable through encryption back to its unencrypted form. The conversion of encrypted data into its original form is called Decryption. It is generally a reverse process of encryption. For the decryption process it uses AES (Advanced Encryption Standard) Algorithm. It takes 128-bit key length.

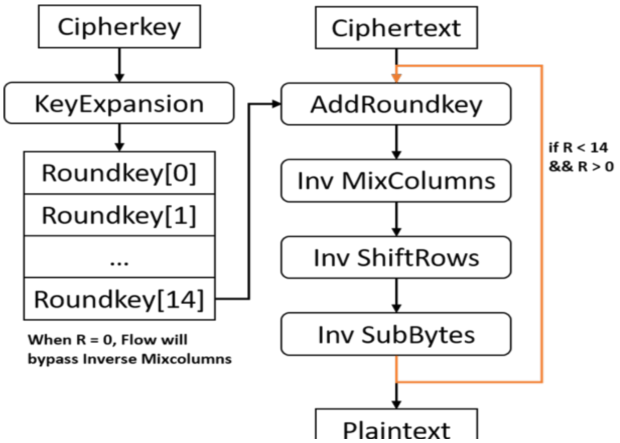

Fig. 5. Encryption process flow

4. Experimental Result

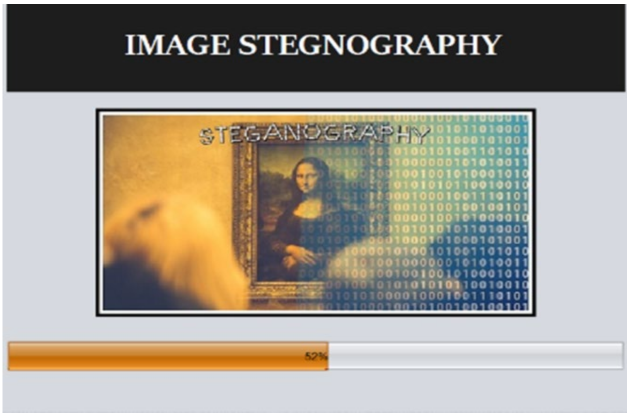

Fig. 6. Home page

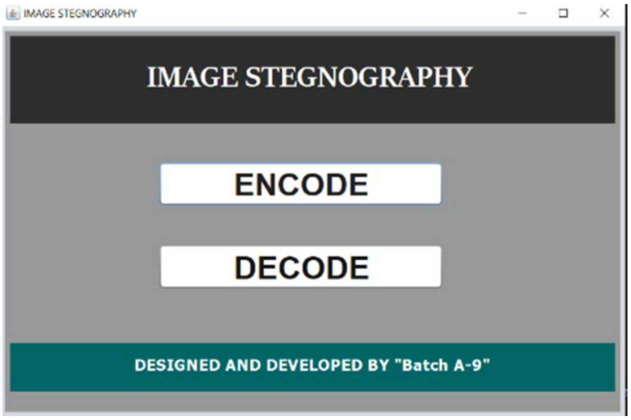

Fig. 7. Main page

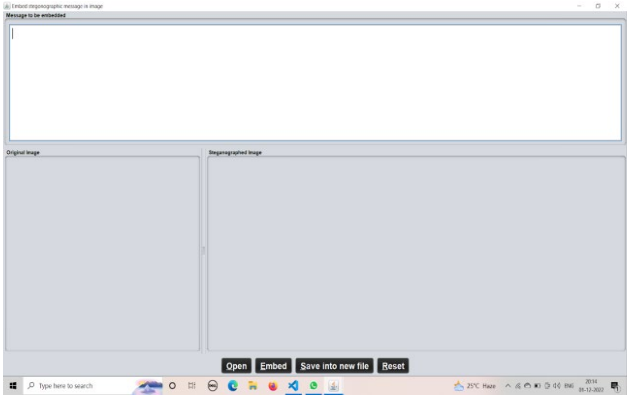

Fig. 8. Encode page

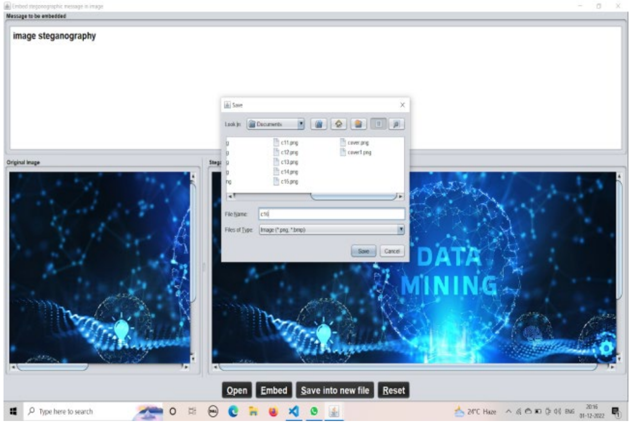

image steganography

Fig. 9. Save

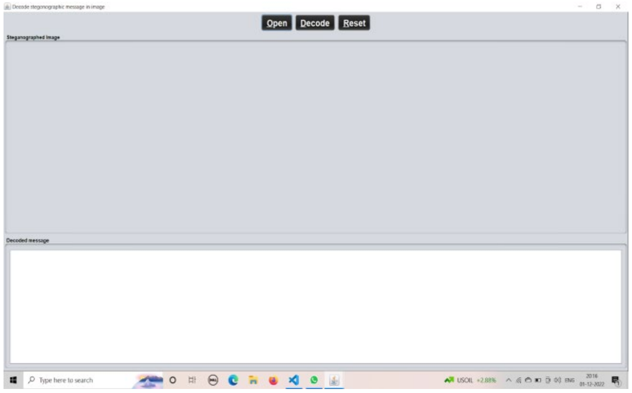

Fig. 10. Decode page

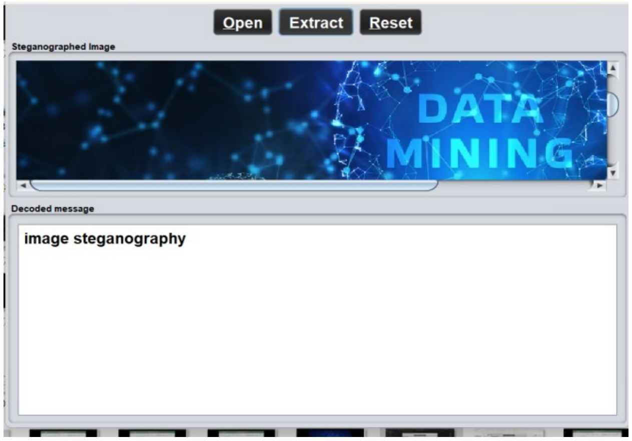

image steganography

Fig. 11. Hidden message

5. Conclusion

The final product of the project is a system that can take a cover image file, hidden message and a secret key as input and provide a stego-image as output as well as extract the secret message hidden in the stego-image when provided with a key and the corresponding stego image. On the sender's side, the hidden message is first encrypted with AES technique with the help of a provided secret key and the encrypted text is then embedded onto the cover image file to produce stego-medium. The embedding process follows image's LSB replacement algorithm. On the receiver's side the process includes extraction of the encrypted message then its decryption with the original key for obtaining the original message. During extraction of hidden cipher text, the bits at LSB are extracted and finally through a series of steps, converted to the encrypted text.

6. Future Enhancement

If needed, the system will be open for future enhancements. The future enhancements might include audio/video steganography with improved algorithms.

References

[1] S. Sugathan, "An Improved LSB Embedding Technique for Image Steganography," in 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), 2016.

[2] L. Xiaoqin, L. Wei, C. Xiuxin, Z. Xiaoli and D. Zhengang, "Application of the Advanced Encryption Standard and DM642 in the image transmission system," in 7th International Conference on Computer Science & Education (ICCSE), Melbourne, 2012.

[3] M. R. Garg, "Comparison of Lsb & Msb Based Steganography in Gray-Scale Images," International Journal of Engineering Research and Technology (IJERT), vol. 1, no. 8, 2012.

[4] E. Walia, P. Jain and Navdeep, ""An Analysis of LSB & DCT based Steganography," Global Journal of Computer Science and Technology, vol. 10, no. 1, 2010.[1] S. Singh, Literature Review on Digital Image Steganography and Cryptography Algorithms, 2015.

[5] S. Singh, Literature Review on Digital Image Steganography and Cryptography Algorithms, 2015.

[6] K. Joshi and R. Yadav, "A New LSB-S Image Steganography Method Blend with Cryptography for Secret Communication," in Third International Conference on Image Information Processing, 2015.

[7] William Stallings, "Cryptography and Network Security - Principles and Practice," Pearson Education, 6th Edition

[8] A. Soni, J. Jain and R. Roshan, "Image steganography using discrete fractional Fourier transform," Intelligent Systems and Signal Processing (ISSP).

[9] Akhtar, N.; Johri, P.; Khan, S., "Enhancing the Security and Quality of LSB Based Image Steganography," Computational Intelligence and Communication Networks (CICN).

[10] A. N, A. V. K and N. R, "Sharing Confidential Images with Abbreviated Shares using Steganography and AES Algorithm," 2022 2nd International Conference on Intelligent Technologies (CONIT), 2022, pp. 1-5.

[11] R. Cogranne, Q. Giboulot and P. Bas, "Efficient Steganography in JPEG Images by Minimizing Performance of Optimal Detector," in IEEE Transactions on Information Forensics and Security, vol. 17, pp. 1328-1343, 2022.

[12] https://github.com/SKocur/Image-Cipher