Secure Communication across the Internet by Encrypting the Data using Cryptography and Image Steganography

Dr P Rajesh[1], Dr Mansoor Alam[2], Dr Mansour Tahernezhadi[3], T Ravi Kumar[4], Vikram Phaneendra Rajesh[5]
Associate Professor, KLEF University, India[1, 4]
Professor, Northern Illinois University, USA[2, 3]
Researcher, KLEF University, India[5]

***Abstract*—Sharing the information has become a facile task nowadays just like one-tap which can take the information to any component of the world. This whole thing transpired over the evolution of the cyber world, which avails to stay connected with the entire world. Due to the wide-spread utilization of the cyber world, it leads a peril of data breaching by some incognito or unauthorized people while it is being sent from one utilizer to another. Unauthorized people can get access to the data and extract utilizable information from it. The confidential data being sent through the web which may get tampered while reaching the other end-utilizer. So, to dispense this data breaching, we can encrypt the data being sent and the receiver can only decrypt the message so that we can conceal the data. It routes a tremendous way to do this, the most popular one is cryptography, and another is steganography. Anteriorly there subsist many ways in these techniques like Image Steganography, Secret key Cryptography, LSB method, and so on which are being used to encrypt data and secure communication. One of the algorithms of cryptography is utilized along with Image Steganography to encrypt the data to ascertain more security which resembles the two-step verification process. In proposed paper we utilized new Huffman coding algorithm in step of the Image Steganography to ascertain that even an astronomically immense data can fit into a minute image. The ciphertext is compressed utilizing Huffman Coding and then it gets embedded into an image utilizing LSB method of Image Steganography in which the least paramount bits of the image are superseded with the data from the antecedent step. We implemented the analytical using python and it shows better compression results with large volumes of data to transfer easily through network.**

Keywords*—Cryptography; image steganography; least significant bits; secure communication; Huffman coding; data encryption; data compression

I. Introduction

A. Encryption

Encryption is a process that a message to be encoded to be private so then it will read by a Specific Person or Specific people [1]. The message in encrypted data is referred to as a secret message that uses an algorithm to enhance more security [2]. A plaintext or a message is converted to ciphertext by using an algorithm that encrypts data and uses a symmetric key that will receive by the destined party to unencrypt or decrypt the encrypted data to grab the message or information from the ciphertext [3]. There are three types of Encryption, they are:

1) Symmetric Encryption (Fig. 1)

In this encryption, a single key is used for both encryption and decryption, also called secret-key cryptography [4].

In the process of encrypting the message, a Symmetric key is injected into the Encryption.

In the process of decrypting the message, the same key is injected to decrypt the information from the ciphertext [5].

It is mainly used for confidentiality and privacy.

2) Asymmetric Encryption (Fig. 2)

In this encryption, one key is for encryption and another key is for decryption, also called public key cryptography [6].

In the process of encrypting the message, a public key is injected into the Encryption.

In the process of decrypting the message, a private key is injected to decrypt the information from the ciphertext [7][8].

It is mainly used for non-repudiation, authentication, and key exchange.

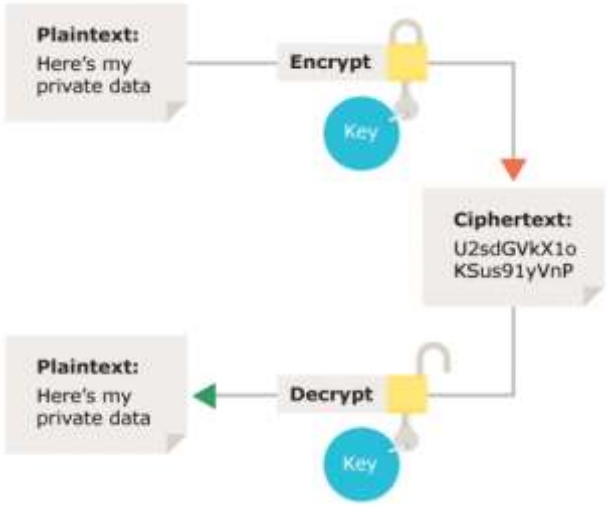

Fig. 1. Symmetric Encryption of Data.

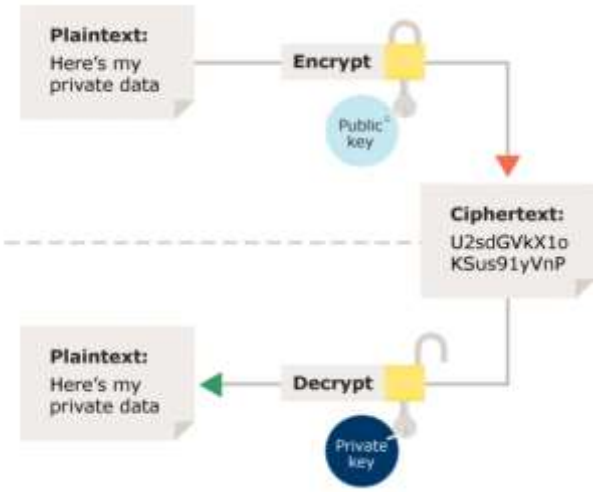

Fig. 2. Asymmetric Encryption of Data.

3) Hash Functions

- In the process of encrypting, a mathematical transformation is used to encrypt the information irreversibly by providing a digital fingerprint.
- It is mainly used for message integrity.

B. Decryption

The process of converting the encoded data to the useful information by following the needs of transformation like algorithm and a shared key or a private key depending on the type of encryption that the information is molded with a ciphertext [9][10] (see Fig. 3). And it is a reverse process of Encryption. To grab the information through a ciphertext an authorized user can only be the person to unscramble the encoded data through a password or a key [11].

C. Steganography

Steganography is a technique used to hide the top-secret data with an ordinary image or audio or video to avoid the cyberattacks and the hided data is unscrambled at the end receiver [12][13]. The use of steganography is to encrypt the secret message with a Symmetric key using one of the algorithms and this encryption is embedded into an ordinary resource as mentioned above. For computer applications like text, sound, etc. it replaces the unwanted bits at the time of encryption so that the resource that we use will remain same.

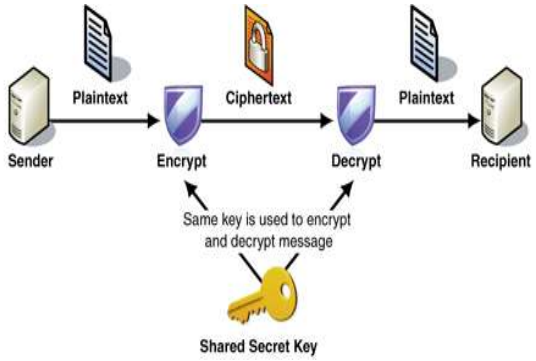

Fig. 3. Process of Encryption and Decryption of Data.

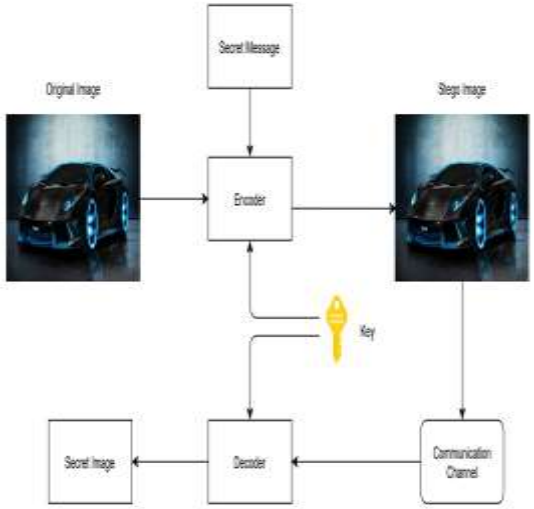

Fig. 4. Formation of Normal Image to a Stego-Image.

If we differentiate the cryptography with steganography the main part that the steganography concentrates on the advancement of security to the secret message that to embedding the bits into any type of digital object will be ordinary to all over the world as the cryptography is masking only on the content of the message and sending to the end receiver it may have some more reveal factor to the world while it is in World Wide Web (WWW) [14][15] (Fig. 4). Steganography can use the combination with encryption, the encrypted data can be inserted into an image or the other normal things and if the case occurs of decrypting the ciphertext the hidden message will remain secure [16].

1) Types of steganography

a) Direct embedding: This type of Steganography approach will lead to an increase in the size of the normal file or an ordinary image depending upon the secret message by embedding the secret message into the resource [17].

b) LSB embedding: This type has a different approach to solve the above type of embedding, to reduce the size by fitting the bits of a secret message into the unwanted bits or fewer priority bits of available normal objects [18].

There are four types of objects where we can insert the bits:

- Image
- Audio
- Video
- Document

2) Image steganography

Images are the most used resource in steganography. An image is an ordinary object that we use in real life but in computer applications, it is a group of bytes or matrices or pixels also called Digital Images [19][20]. Using these Bytes of an image, a secret message is passed through the network where we can achieve more security. By looking intensely, every byte will contain 8 bits in the image and changing the

least significant bits in every byte will attain to hide the data [21][22]. It may lead to exists a drawback in this technique, if message size in bits exceeds the size of the image then the algorithm will not work for this type of case.

In cryptography, the encrypted data that is the coded data will be visible to the unapproved users, but can't use them unless they decrypt it using appropriate technique whereas, in the steganography, the encrypted data cannot be seen directly, can be seen in digital format, makes unapproved users difficult to tamper the data [23].

The most popular usage of these techniques is encrypting the data with both the flavors like using steganography along with cryptography [24][25]. In this research, an encrypted key is generated with the data at the sender's side using cryptography, and then the data is encrypted into multimedia tools such as image, video, or audio using steganography.

3) Steps involved in this process:

- Encryption key generation with the input data using Cryptography.
- Data encryption using LSB method of Image steganography.
- Data compression using Huffman coding.
- Sending the stego image along with the generated encryption key at the receiver side, retrieve the hidden data in the stego image and then decrypt it using the encryption key.

II. Block Diagram for Proposed System

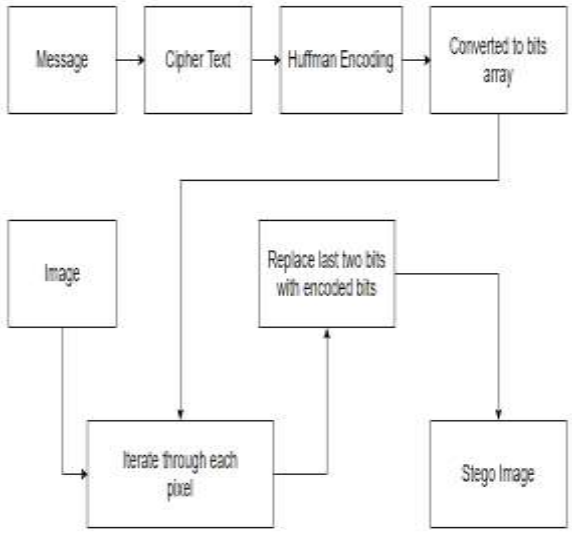

Fig. 5. Block Diagram for Proposed Methodology.

III. Implementation

The main theme is that the message should be seen only by the receiver. So, in this paper, the encryption key is merged to the message and converted to ciphertext so that the one person knows and reads the encryption key and then the ciphertext is hidden inside the image.

A. Encryption Key Generation using Cryptography

Cryptography is a standard method used to encrypt the data, the data say a text is converted some other text in an illegible format called as ciphertext using encrypting algorithms and send the original data along with encryption key, then the receiver should know the decryption key so that the data can be retrieved using that key when it has arrived. Most of the time, those encryption keys are private since the receiver of the data can only use the data.

B. Data Encryption using LSB Method of Image Steganography

Mainly the steganography is used to hide messages inside the image. So many ways are making their way to existing methodology to store the message inside the image. Here, the LSB method means the least significant bits method is used. Every image has so many pixels, each pixel is the smallest individual element of the image. In the color imaging system, color is represented by three or four components such as RGB (Red, Green, Blue), CMYB (Cyan, Magenta, Yellow, and Black). The CMYB is mainly used in printers.

Each pixel is composed of three value RGB having 8-bit values. The rightmost bits have less impact on the image. So, the last two bits are changed, and the result is an altered image also called stego image.

Here, Fig. 6 is an RGB pixel representation. In each 8-bit representation, the last two bits are changed because of having less impact on the resultant image that can be difficult to identify the difference with the naked eye.

Each Image can store only a certain number of bits it can be calculated by the (height*width*(color component) *2)/8000 (KB of data).

C. Data Compression using Huffman Coding

Huffman coding is a data compression algorithm. In this algorithm, all the characters are replaced with numbers because the character's bit length is more than the number's bit length. While transmitting the message, a table that maps the character and the number bits of the message will be sent. So after ciphertext is generated, a number will be mapped to each unique character in the message and a mapping function is generated so that all the characters in the message are replaced by that corresponding number, the bit representation of a number is less than the bit representation of character so it can reduce the size of the message to a great extent.

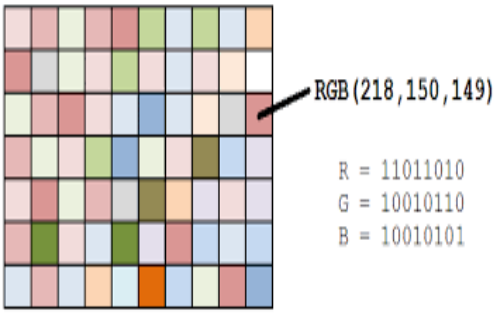

Fig. 6. RGB Pixel Representation.

Example:

"**Hi, this is the secret message**" is the message to be encoded in the image and send it to the receiver, Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video hence the message remains confidential.

Length of the binary representation of cipher text is:1816 (0.227KB).

Length of the binary representation of cipher text Applying Huffman approach is:1429 (0.1786KB).

Huffman table for the above message:

1 --> (space)	2 -->(,)	3 --> A	4 --> B	5 --> C	6 --> D	7 --> E
8 --> F	9 --> G	10 --> H	11 --> I	12 --> L	13 --> M	14 --> N
15 --> O	16 --> P	17 --> R	18 --> S	19 --> T	20 --> V	21 --> W
22 --> Y						

So, the message size is reduced. In this way, a long message can be stored in small images.

D. Sending the Stego Image along with Generated Encryption Key

The image generated after the data compression using Huffman coding that is from the step-3 is sent to the receiver along with the encryption key, generated from the step-1.

At the receiver end, this image is then converted to binary bits, and then by the reverse of the Huffman approach, it is decoded as strings then decoded as the original message by using the encryption key.

E. Results

Fig. 7 is the image where the message to be stored. Image shape: 1024*1820*3 and can store 1397.76 KB of information. Then this image is converted to binary and the last two bits are replaced with message bits using LSB method of image steganography.

Fig. 8 is the final image generated after data compression using Huffman coding that helps to store large information.

Fig. 7. Original Image.

Fig. 8. Stego Image.

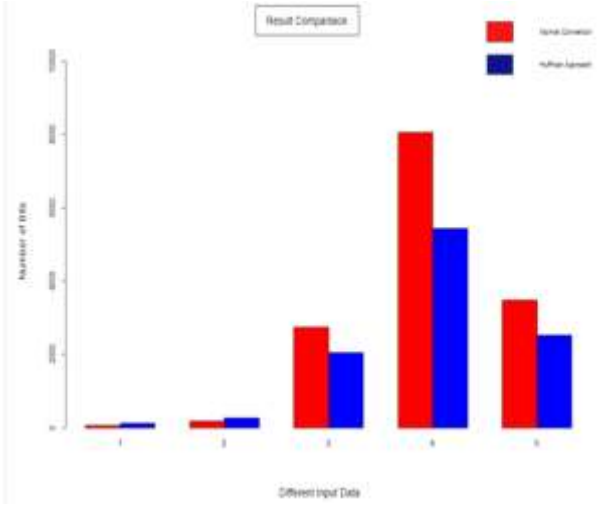

Fig. 9. Histogram Analysis for Steganography.

So, it means this image contains the information, but it seems to look the same as the original image. This is the main advantage of encrypting the data and then send it to the receiver.

Fig. 9 clearly states information about the bits of a Normal Conversion and Huffman Approach Conversion, taking the different sets of data with differences in their sizes by the above graph we can say that the algorithm will reduce the bits by approaching Huffman encoding and decoding method. Conclusion and Future Scope

Encryption of data and Decrypting back is to protect the crucial data that will use mainly by companies to safeguard their data like formulas or particulars of their clients etc., by using this steganography method with the conjunction of cryptography we can accomplish more security to provide for the user. This research came into the action to provide an algorithm to send the message over the expectation through an average resolution image and for a situation where we cannot send a message through image due to the size or the resolution or low pixels quality of the image then our research made the situation easier to handle.

- Multilevel Steganography by fitting the Image steganography into another ordinary image.
- In the future, by using this Huffman optimization method we can reduce the duplicate bytes and assigning every unique byte with a unique symbol and replacing all the duplicate bytes with the unique symbol gives a solution for fitting the heavier Steganography image into an average resolution image.

REFERENCES

[1] MehtapUlker, Bilgehan Arslan(2018). “A Novel Secure Model: Image Steganography with Logistic Map and Secret Key”, IEEE.

[2] Pooja Chandarana, Prof. Purnima Ahirao. “ADVANCED IMAGE STEGANOGRAPHY”, International Journal of Innovative Research in Information Security, Issue 07, Volume 5, (September 2018.

[3] Huma Jabeen, Professor Abdul Wahid. "Image Steganography using Pseudo-Random Number Generator", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 8, Issue 3, March 2019.

[4] K. Surekha, J. S. S. Sekhar, V. Devi Prasanna, P. Srividya, S. S. S. S. Anusha, V. Manogna. “Hidden Secrets Behind the Images”, International Journal for Research in Applied Science & Engineering Technology (IJRASET), Volume 8 Issue V May 2020.

[5] Dong Wu. “minimizing distortion in steganog-raphy based on image feature”, International Journal of Computer Science & Information Technology (IJCSIT) Vol 11, No 1, February 2019.

[6] Aung Myint Aye. "LSB Based Image Steganography for Information Security System", International Journal of Trend in Scientific Research and Development (IJTSRD) International Open Access Journal, ISSN No. 2456 – 6470, Volume-3, Issue-1, Nov-Dec 2018.

[7] Urvashi Kodwani, Sakshi Agrawal, JuiDiwale, Samiksha Thakur, Devishree Naidu. “Secure and transparent file encryption system”, International Journal of Advance Research, Ideas and Innovations in Technology, Volume 5, Issue 1, 2019.

[8] Giridhar Maji, Sharmistha Mandal. “Secure and Robust Image Steganography Using a Reference Image as Key”, International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8, Issue-7, May,2019.

[9] Ernest Andreigh C. Centina. “Image Steganography of Multiple File Types with Encryption and Compression Algorithms”, Asia Pacific Journal of Multidisciplinary Research, Vol. 5, No. 3, August 2017.

[10] srishti Rajvanshi, Shrikrishna Sawant, Vedant Tiwari, Anurag Waghmare, ManjiriGogate. “Image Steganography”, International Journal for Research in Applied Science & Engineering Technology (IJRASET) ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177 Volume 7 Issue XI, Nov 2019.

[11] Walaa Ali H. Jumiawi, Haider A. Abbas Mohammed. “Chained QR Keys Generation Based on Chaotic Hybrid Encoding and Fourier Transform Shifting for Image Encryption”, DOI 10.5013/IJSSST.a.21.02.09.

[12] Salah Harb, M. Omair Ahmad, M.N.S Swamy. “Design and hardware implementation of a separable image steganographic scheme using public-key cryptosystem”, Electrical and Computer Engineering Department, Concordia University, 1440 De Maisonneuve, Montreal, Canada.

[13] Abhijeet Bhaskar, Mr. Upendra Kumar Acharya. “Image Steganography Using Modified LSB”.

[14] J. K. Mandal, Debashis Das. “Colour Image Steganography Based on Pixel Value Differencing in Spatial Domain”, International Journal of Information Sciences and Techniques (IJIST) Vol.2, No.4, July 2012.

[15] Anusha T and Venkatesan R, PSG College of Technology, India. “Steganography Based Asymmetric Key Cryptosystem Using Trellis Coded Genetic Algorithm Random Key Generator”, International Journal of Embedded Systems and Applications (IJESA), March 2019, Volume 9, Number 1.

[16] Dr P Rajesh, Dr M Alam, " A Data Science Approach to Football Team Player Selection" at 20th Annual IEEE International Conference On Electro Information Technology (eit2020). July 31 - August 1, 2020, USA. https://ieeexplore.ieee.org/document/9208331.

[17] Dr Dr P Rajesh, Dr M Alam, " Machine Learning and Statistical Analysis Techniques on Terrorism" at The 6th International Conference onFuzzy Systems and Data Mining (FSDM 2020)November 13-16, 2020, Xiamen, China.

[18] Dr.P.Rajesh, Sai Prasanna " A Forensic Approach To Perform Android Device Analysis " at National Women Conference on Technological Innovations", 2019, Scopus, with Best paper award of conference.

[19] SK.Wasim Akram, P.Rajesh "Avoiding Cross Site Request Forgery (CSRF) Attack Using TwoFish Security Approach" in International Journal of Computer Trends and Technology.2015.

[20] P.Rajesh, Dr.G.Narsimha, " Cerebration Of Privacy Preserving Data Mining Algorithms" in International conference on machine learning and data analysis ICMLDA_ 2014, USA in association with springer, IEEE Explore, DBLP.

[21] P.Rajesh, Dr.G.Narsimha, "Fuzzy based privacy preserving classification of data streams." in ACM conference (CUBE), Pune, PP: 784-788, 2012, DBLP, ISBN: 978-1-4503-1185-4.

[22] Sahu, Aditya Kumar; Swain, Gandharba , Data hiding using adaptive LSB and PVD technique resisting PDH and RS analysis, International Journal Of Electronic Security And Digital Forensics,2019, 10.1504/IJESDF.2019.102567.

[23] Ranjeeth Kumar M , Srinivasu N, Reddy, Advanced hybrid approach to provide privacy for cross-site and XSS attacks in cloud computing, Journal of Advanced Research in Dynamical and Control Systems (2018).

[24] Srinivasu N, Sahil M, Francis J, Security enhanced using honey encryption for private data sharing in cloud, International Journal of Engineering and Technology(UAE) (2018).

[25] Balakrishna A, Srinivasu N, Security analysis for control policy in OSNs, ARPN Journal of Engineering and Applied Sciences (2016).