IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 8, Issue 4, April 2019

Cryptography Technique for Information Security

Priyanka S. Pandhare[1], Pallavi S. Raut[2], Shital S. Patil[3], Pranjali T. Pawar[4]

Department of Computer Engineering, SSBT College of Engineering, Jalgoan, India[1,2,3,4]

Abstract: In today's computer world security, integrity, the confidentiality of the organization data is the most important issue. The confidentiality of data files which is transmitted over the internet. Data encryption is widely used to ensure the security of the data files. In the existing system, the image was hiding in the image they are using watermarking for image hiding. In the proposed system we are using DES, Run length encoding and steganography techniques for providing security to the secret data files. This system not only embeds the secret data files like text, image, audio, video in the image but also embed that secret data files in a cover data files like image, audio, video, etc. By using these Techniques third parties cannot percept the existence of secret data embedded in the cover files such as image, audio, video. The properties of the cover data file remain the same after hiding the secret data files. The goal of steganography is to avoid suspicion to the transmission of hidden message, such that it is highly secured. For secret data files compression Run-length encoding technique used. Run-length encoding (RLE) is a very simple form of lossless data compression in which runs of data are stored as a single data value and count, rather than as the original run. Security is provided by Encrypting the secret data files that are embedded in cover data files using the DES algorithm.

Keywords: Steganography, DES, Run Length Encoding, Compression

I. INTRODUCTION

Cryptography is an art and science of hiding messages to introduce secrecy in data and information security while steganography is simply the art of secret writing, The Crypto-steganographic method is aimed at amalgamating both the cryptography and steganography methods for better information security. The primary purpose of this paper is to build up a new method of hiding secret text messages and data files like image, audio, video in an image and data files such as image, video, audio, by combining cryptography and steganography. Growing prospects of modem communications need the exceptional means of security especially in computer network communication. Network security is gaining importance as the data being exchanged on the Internet increases. Therefore, confidentiality and data integrity are required to protect against unauthorized access. It leads to an explosive growth in information hiding including copyright protection for digital media. It would be rather more sensible if the secret message is cleverly embedded in another media so that no one can guess if anything is hidden or not. idea results in steganography, a branch of information hiding by masking secret information within other information. The word steganography comes from the Greek Stegano which means covered or secret and Gra means writing or drawing. Steganography means literally covered writing. Data should not diverge much from the original cover data file and image. Cryptography and steganography are widely used in the field of data hiding and has received significant attention from both industry and academia in the recent past.

II. LITERATURE SURVEY

'**D. Debnath**': This paper provides security scheme in which steganography is used along with cryptography to provide better security to embedded data. In their method first data is encrypted when it is embedded into the cover image using a steganographic method. The proposed algorithm transforms any kind of message into text with the help of manipulation tables, and then carries out hill cipher methods to it and finally hides the data into red, blue, and green pixels of the cover image. They use the number of image quality parameters like MSE, PSNR, AD, SC, NAE and MD.[1]

'**Michael Backes**': This Paper presented the output from Huffman's algorithm can be viewed as a variable-length code table for encoding a source symbol (such as a character in a file). The algorithm derives this table from the estimated probability or frequency of occurrence (weight) for each possible value of the source symbol. As in other entropy encoding methods, more common symbols are generally represented using fewer bits than less common symbols. Huffman's method can be efficiently implemented, finding a code in time linear to the number of input weights if these

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 8, Issue 4, April 2019

weights are sorted. However, although optimal among methods encoding symbols separately, Huffman coding is not always optimal among all compression methods.[2]

'**Orhun Kara and Cevat Manap**': In that paper presented bcrypt is a cross-platform file encryption utility. Encrypted files are portable across all supported operating systems and processors. Passphrases must be between 8 and 56 characters and are hashed internally to a 448-bit key. However, all the characters supplied are significant. The stronger your passphrase, the more secure your data.[3]

III. ALGORITHMS

A. Run Length Encoding(RLE)

Run-length encoding (RLE) is a very simple form of lossless data compression in which runs of data (that is, sequences in which the same data value occurs in many consecutive data elements) are stored as a single data value and count, rather than as the original run. RLE works by reducing the physical size of a repeating string of characters. This repeating string, called a run, is typically encoded into two bytes. The first byte represents the number of characters in the run and is called the run count. In practice, an encoded run may contain 1 to 128 or 256 characters; the run count usually contains as the number of characters minus one (a value in the range of 0 to 127 or 255). The second byte is the value of the character in the run, which is in the range of 0 to 255, and is called the run value.

B. Data Encryption Standard(DES)

The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST). DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only). DES is based on the two fundamental attributes of cryptography: substitution and transposition (also called as diffusion). DES consists of 16 steps, each of which is called as a round.

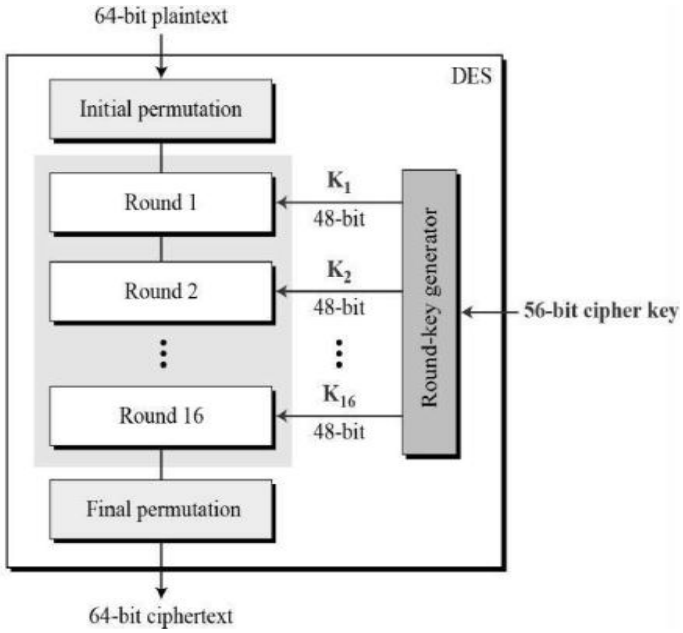

Figure 1.Structure of DES Algorithm

IV. PROPOSED SYSTEM

Reason behind choosing this model is the security, efficiency with original data. Most interesting thing in this technique is the combination of two different techniques. This proposed technique is a approach of security that combines two or more security technique and usually a combination of compression and steganography to take benefit of the strengths of each type of encryption. The proposed concept provide security to information in the form of text, image, audio and video. It uses the data encryption standard, run length coding for transmit information securely. The information in any form as per the user choice gives input and using the run length algorithm this information will be compressed. The compressed data will be embedded with the image, audio or video then data encryption standard algorithm is used. Private key value will known only to sender and receiver. After producing cipher data proposed concept will be called as steganography method where a cover data will pass as an input.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 8, Issue 4, April 2019

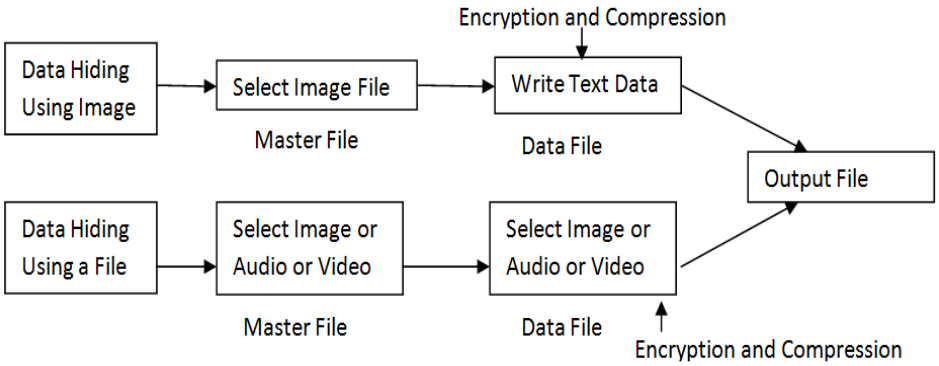

Figure 2. Sender Side System Architecture

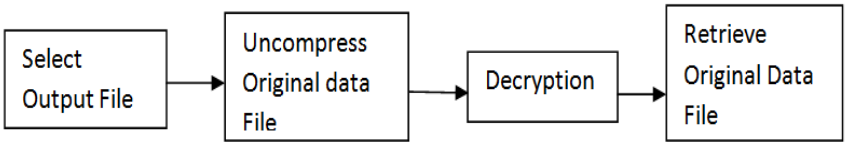

Figure 3. Receiver Side System Architecture

C. Step of RLE Algorithm:

For example, if the input string is wwwwaaadexxxxxx, then the function should return w4a3d1e1x6.

1. Pick the first character from source string.
2. Append the picked character to the destination string.
3. Count the number of subsequent occurrences of the picked character and append the count to destination string.
4. Pick the next character and repeat steps b) c) and d) if end of string is NOT reached.

V. RESULT

In the project , There is main home page for hiding a text message into a image and hiding a data file into cover file and retrieving original data from file. If we want to embed text message into image then click on hiding data using image button. Then select master file for embedding text message into that selected master file. Give name of output file which send to receiver for Decryption.

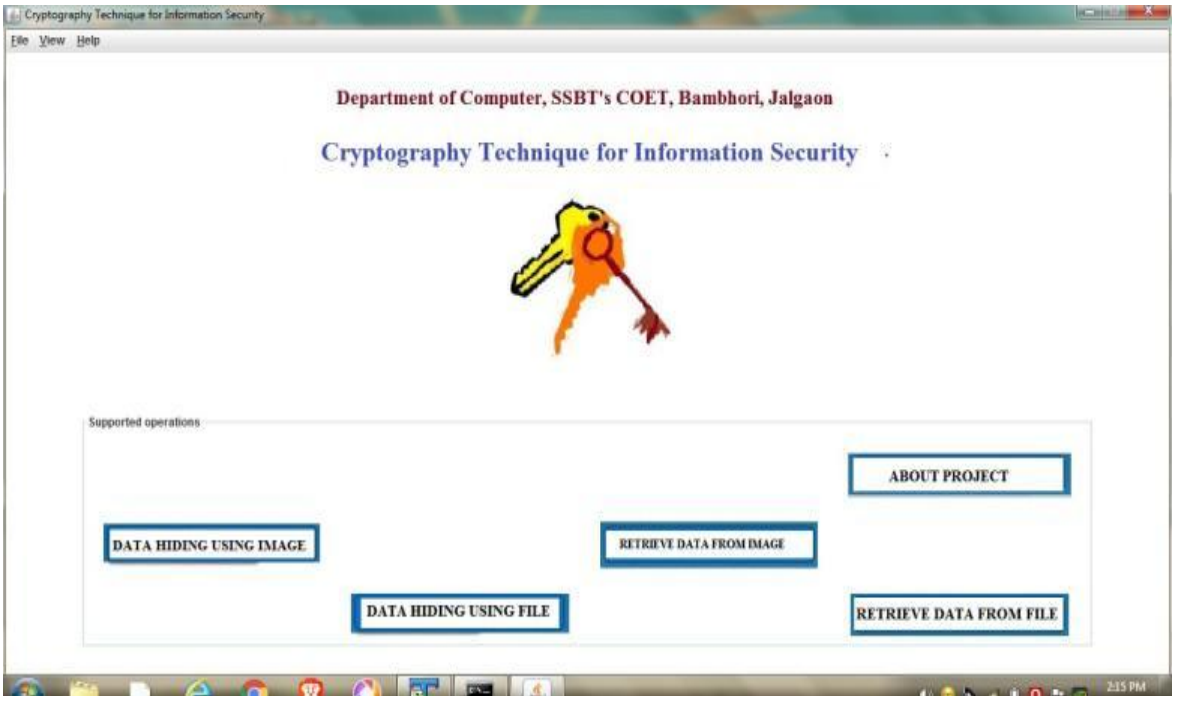

Figure 4. Home Page of Project

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 8, Issue 4, April 2019

Type text secret message and Compress secret message and give a private key password.

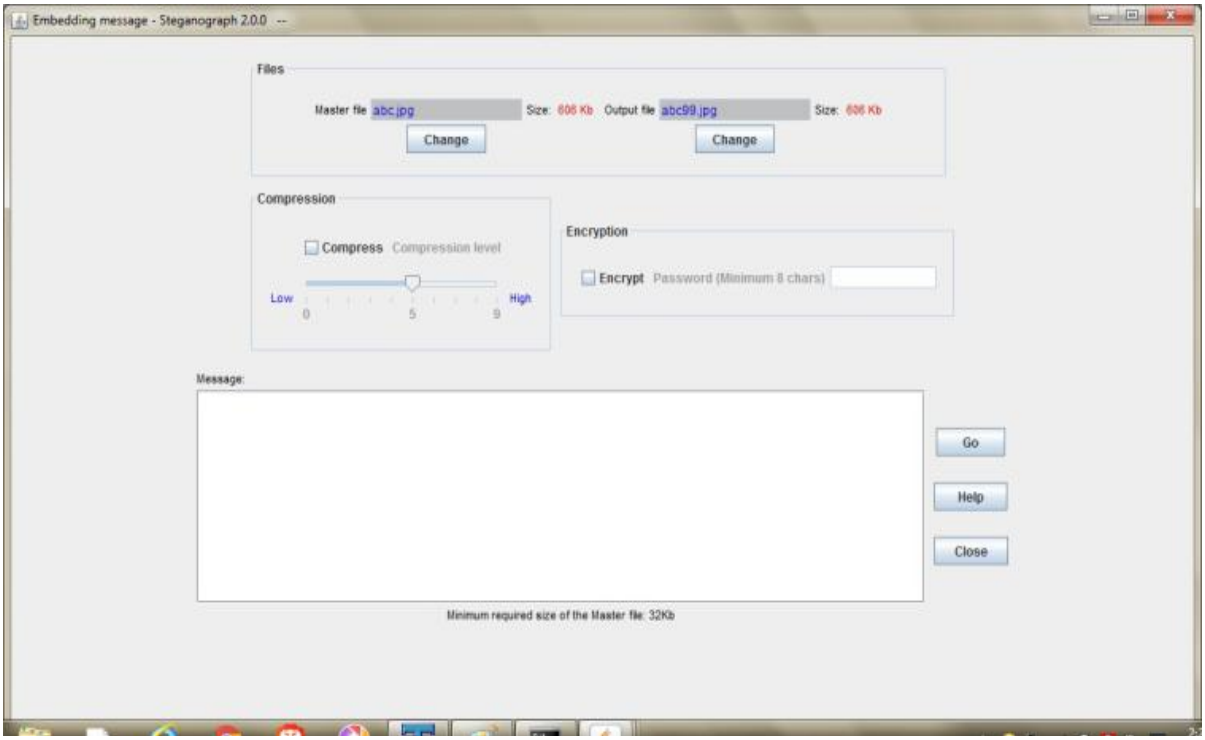

Figure 5. Encryption of Secret Message

Figure 6. Type a Private Key Password for Decryption

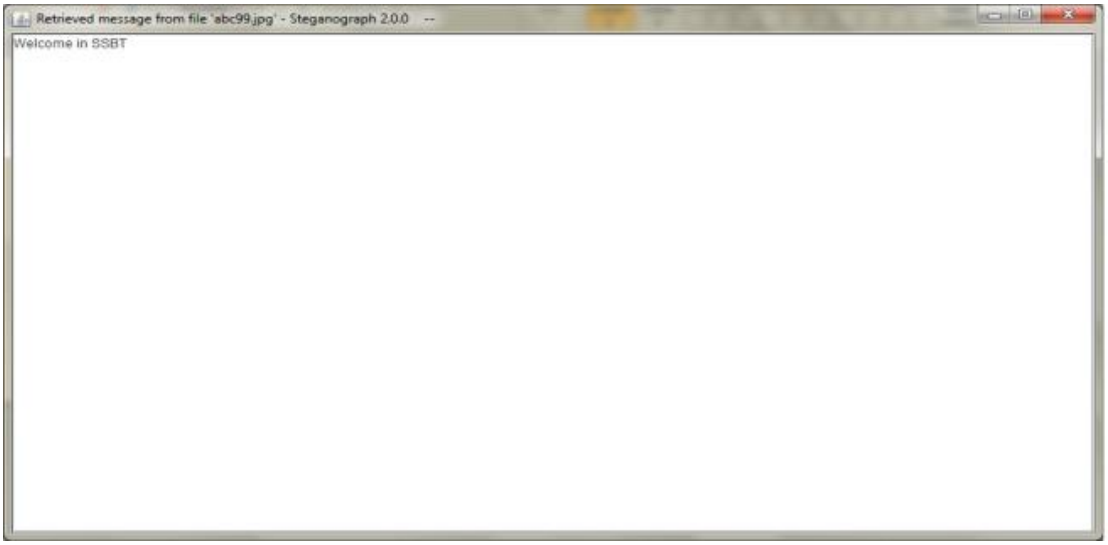

Figure 7. Retrieved Secret Message

DOI 10.17148/IJARCCE.2019.8453

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 8, Issue 4, April 2019

VI. CONCLUSION

The encryption algorithm plays a very important role in communication security. Research work surveyed the performance of DES encryption technique used to provide security. DES algorithm techniques are the two main factors in the proposed system which gives assurance for secured data message transmission which is made available to the authorized personnel. Based on the texts used and the experimental result it was concluded that the DES algorithm consumes the least encryption. It also observed that the Decryption of DES algorithm is better than other Hence, both authentication and confidentiality shall be provided with more accuracy. The proposed system provides double security to the data.

REFERENCES

[1]. D. Debnath, "Robust and Secure Image Steganography Based on Elliptic Curve Cryptography ", IEEE, 288-291, 2012.
[2]. Michael Backes, "Flexible stego-system for hiding text in image of personal computer based on user security priority ", IEEE, 2014, 250-256.
[3]. Orhun Kara and Cevat Manap, "Method for the Construction of Minimum-Redundancy Codes", IEEE,1952, 10981101.
[4]. Gallager, R.G., van Voorhis, D.C., "Optimal source codes for geometrically distributed integer alphabets", IEEE Transactions on Information Theory, 228230, 2017.
[5]. Panagiotis Papadimitriou, "Data security cryptographic technique", IEEE, 345240, 2017.
[6]. R. Agrawal and J. Kiernan, "Watermarking Relational Databases", IEEE, 28th Intl Conf., 2016, 155-166.
[7]. Ashokkumar C., Ravi Prakash Giri, and Bernard Menezes, "Highly Efficient Algorithms for AES Key Retrieval in Cache Access Attacks", IEEE, Archived from the original, 2017-05-14.
[8]. L. A. MacPherson, "Grey Level Visual Cryptography for General Access Structures", IEEE, 768-128, 2002.
[9]. W. Zhou and A. C. Bovik, "A universal image quality index", IEEE, 79-81, 1981.