International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 04 | Apr -2017 www.irjet.net p-ISSN: 2395-0072

Secure Data Transmission

Prateek Kumar Singh[1], Pratikshit Tripathi[2], Rohit Kumar[3], Deepak Kumar[4]

[1]UG Scholar, Dept. of IT, GCET, Greater Noida, UP, India
[2]UG Scholar, Dept. of IT, GCET, Greater Noida, UP, India
[3]UG Scholar, Dept. of IT, GCET, Greater Noida, UP, India
[4]Assistant Professor, Dept. of IT, GCET, Greater Noida, UP, India

---

Abstract - *In the present scenario, any type of communication over the internet and other network applications need to be secure due to their increasing utility. For this task, lots of algorithms for security have been implemented and used so far. With these developments, attackers have also come up with the new ideas to penetrate the communication mediums. Till now cryptography has been the mainstay for defending the secure data transmission [1]. With the increasing threat, Steganography has also taken space for security purpose. In cryptography, we change the natural form of data by using different security algorithms, which leads to increasing security of the communication process. In Steganography information is kept hidden from the attacker for communicating the information safely with the use of images, audios, videos etc. So for more security during data transmission, we have proposed the method of using both the techniques cryptography, and steganography. In cryptography we will perform three level encryption with the use of AES, DES and Blowfish algorithms. In steganography, we will be embedding the data file in any audio, video or image with the use of LSB, DWT and DCT technique and then we will communicate the secure data to the receiver end.*

Key Words: *Cryptography, Steganography, DWT Steganography, DCT Steganography, LSB Steganography, AES Encryption Standard, DES Encryption Standard, Blowfish Algorithm.*

1. INTRODUCTION

Nowadays communication has become the most desired requirement for each and every one and for this desire, we need a channel through which the information can be passed upon due to the growing importance of the communication channel it becomes vulnerable to a large variety of attacks. Our main task is to defend the transmission passage against all sort of attacks and transmit our information safely to the receiver. For this purpose, we are using cryptography. Generally in cryptography people encrypt the message with any encryption algorithm but in the wake of increasing attacks on data we will be implementing three algorithms for algorithms to make our data defendable against cyber-attacks. The algorithms we will be using are Advanced Encryption Standard (AES)-128, Data Encryption Standard (DES) and Blowfish. Our next level of security will be the steganography using audio, video and image [2]. In steganography, we will be using LSB algorithm for embedding the encrypted data file into the audio/image/video frames. After this multilevel encryption and embedding, we will transmit it through the secure communication channel to the opposite end.

1.1 Motivation

In cryptography, the reason of selecting the AES algorithm is that it is the highly defendable algorithm for encryption till now. We are using a 128-bit key and it goes through 10 rounds to complete the encryption [3]. For giving a perfect shot we have used blowfish algorithm also as Blowfish is the strongest and fastest in data processing and storing in comparison to other algorithms. We got the thought of using steganography to distract the attention of the attacker because when the attacker will be desperately in the search of any text file or doc file we can silently slip of audio or video file embedded with the secret document. In this manner, we can complete our task of transmission of data securely.

1.2 Objective

The objective of our proposed work is to find an alternative to the problem faced by the different organization, companies and people for transmitting their critical and important data. In the earlier days, when we encrypted our data with an encryption with a single algorithm it was considered as a big invention for security but with the increasing use of internet, attackers have become aware of the methodology to take on these security algorithms. So for effectively countering it, there are multiple methods:

a) To develop new security algorithms at regular intervals to avoid the formation of any pattern or similarity in the secured data.
b) To apply multi-fold security using already present security algorithms like AES, DES Blowfish.
c) To use different security approaches together like cryptography and steganography.

We have chosen the third approach as the suitable and an effective solution due to its property of multi-fold security as well as the data-hiding concept of steganography.

2. CRYPTOGRAPHY

It is a technique of securing the communication process from attackers. Cryptography is about using protocols that prevent attackers from accessing data, various aspects in information security such as data confidentiality, data integrity, authentication and non-repudiation are the base of the modern cryptography.

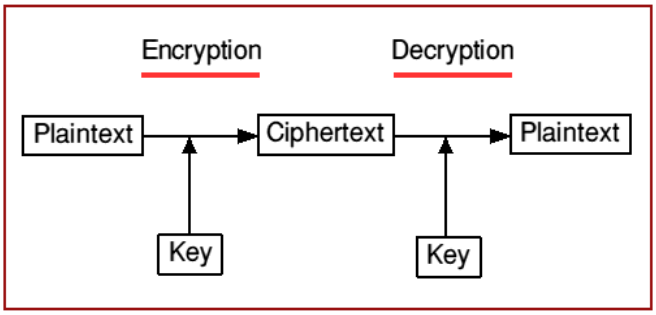

Fig-1: Cryptography

Cryptography includes different encryption and different decryption techniques for encrypting and transferring data [4]. Encryption techniques are of two types:

a) Symmetric: It uses the same key at the time of encrypting and decrypting the data. Eg. AES, DES etc.
b) Asymmetric: It uses different keys at the time of encrypting and decrypting the data. Eg. RSA etc.

In Symmetric encryption and decryption process, both the sender end and the receiver end use the same key to encrypt as well as decrypt data. In Asymmetric encryption and decryption process, both the sender end and receiver end use the different key and this proposes the concept of using public and private key in encryption and decryption phenomenon in the communication process. Receiver's public key is broadcasted and available to everyone and it is used for encryption but the decryption of the encrypted file can be done only using receiver's private key which is only known to the receiver.

3. STEGANOGRAPHY

Steganography is a technique which protects the important information by hiding it inside video, audio, images and then being transmitted [5]. Steganography system consists of different components:

A) Cover Media
B) Secret Information

The sensitive information is merged in the cover media by replacing the information which is already present in the cover media [6]. Steganography provides a big opportunity in a manner that someone cannot detect the presence of the hidden message and therefore they will not be able to access it.

Steganography is a phenomenon by which we embed the message in a cover frames without leaving any significant traces on the original data file. There are 4 different kinds of Steganography:

a) Text
b) Audio
c) Video
d) Images

Generally, Image Steganography is the most preferred choice of the users [7]. It provides the secure and simple way to communicate the sensitive information through the internet. Along with this, we have taken care of properly implementing the video steganography using LSB, DCT and DWT techniques.

4. PROPOSED WORK

4.1 DES (Data Encryption Standard)

DES was developed in the 1970s and it used the Feistel Structure. It is a symmetric algorithm and thus uses the same key for both encryption and decryption. So the sender end and receiver end must know the private key. The length of the key is 64-bits, where a number of bits taken for parity check are 8-bits. It undergoes 16 rounds of permutation process for encrypting the message.

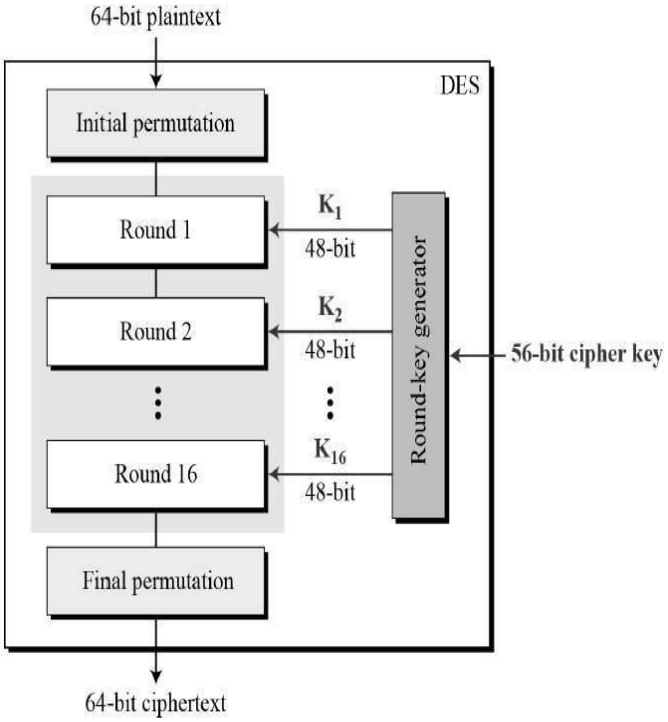

Fig-2: Block Diagram of DES

Almost the encryption process and decryption process is same except, the decryption is done in reverse order. The attack that is possible on DES is the brute-force attack. Three more attacks possible on DES algorithm are:
a) Differential Cryptanalysis
b) Linear Cryptanalysis
c) Davies Attack

4.2 Blowfish

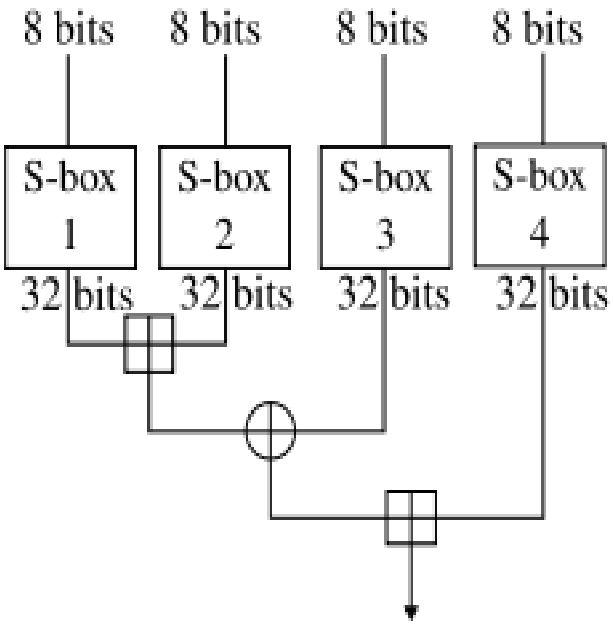

Fig-3: Block Diagram of Blowfish

Blowfish has a 64-bit block size as shown in Fig-3 and a key of variable length i.e. from 32 bits up to 448 bits. It is a process with 16-round Feistel cipher and also it uses large key-dependent S-boxes. In blowfish algorithm, a 64-bit plaintext message is equally divided into 32 bits and each line represents 32 bits. The algorithm consists of the two sub-key arrays: the 18-entry P-array and four 256-entry S-boxes. The S-boxes accept 8-bit input and produce 32-bit output. A single entry of the P-array is used in every round, and after the final round completion, every half of the data block is XORed with one of the two remaining P-entries which were not used earlier [8]. Throughput is calculated in MB/Sec. Secure Image Hiding Algorithm using Cryptography and Steganography is done. The F-function partitions the 32-bit input into four equal eight-bit quarters, and uses those quarters as the input to the S-boxes. The outputs are added modulo 2 32 and XORed to produce the final output of 32 bit. Decryption works exactly the same as encryption, except that P1, P2,..., P18 are used in a reverse manner. This is not so obvious because XOR has the property of being commutative and associative.

4.3 AES (Advanced Encryption Standard)

AES is of three types: AES-128 type, AES-192 type, and AES-256 type [9]. Each cipher first encrypts and then decrypts the data in blocks of 128 bits using cryptographic keys of 128-bits, 192-bits, and 256-bits, respectively. The Rijndael cipher was developed to accept additional sizes of the block and length of keys, but for AES, those functions were not accepted.

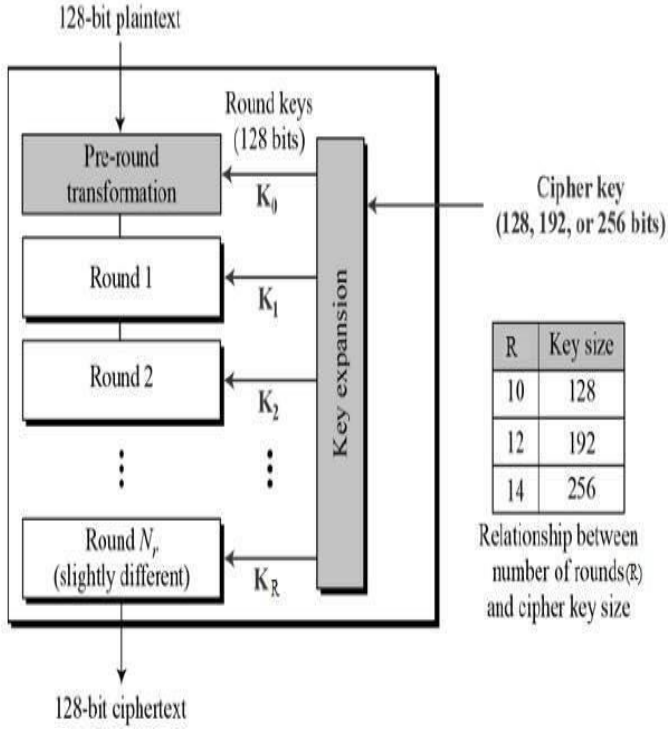

Fig-4: Block Diagram of AES

Symmetric ciphers use the same key for the process of encryption and decryption, so at the sender end and the receiver end must both know -- and use -- the same secret key. All the keys with their respective lengths are considered sufficient to safely communicate the critical information up to the "Secret" level requiring either 192- or 256-bit key lengths. In AES encryption process 10 rounds given for 128-bit keys, 12 rounds given for 192-bit keys and 14 rounds given for 256-bit keys. A single round consists of many processing steps that include substitution, transposition process and mixing of the input plaintext and converts it to the final output of cipher text.
The AES encryption algorithm defines a number of changes that are to be performed on data of the file i.e. stored in the array. The beginning step of the cipher is to insert the data into an array, after which the cipher modifications are processed again and again for the encryption process. The total number of rounds are determined by the key length, with 10 rounds allotted for 128-bit keys, 12 rounds allotted for 192-bit keys and 14 rounds allotted for 256-bit keys [10].

The first transformation in the AES encryption cipher is the substitution of data by another data using a substitution table, the second transformation shifts the data rows, and the third transformation mixes columns. The last transformation is XOR operation which is being performed on every column using different parts of the encryption key, and longer the key the more rounds are needed to complete.

4.4 LSB Based Steganography

The Algorithm used for LSB based Steganography technique is as follows:-

Step 1: Read the available frames of the cover image and encrypted file which is to be hidden inside the cover image [11].
Step 2: Convert text message in the encrypted file in binary.
Step 3: Identify the LSB of each and every pixel of the cover image that is to be transferred over the network for the communication process.
Step 4: Substitute the LSB of each and every pixel of the cover image i.e. to be communicated, with each and every bit of the parts of the critical message or the secret message i.e. present in the encrypted file, one by one.
Step 5: Finally write the stego image.

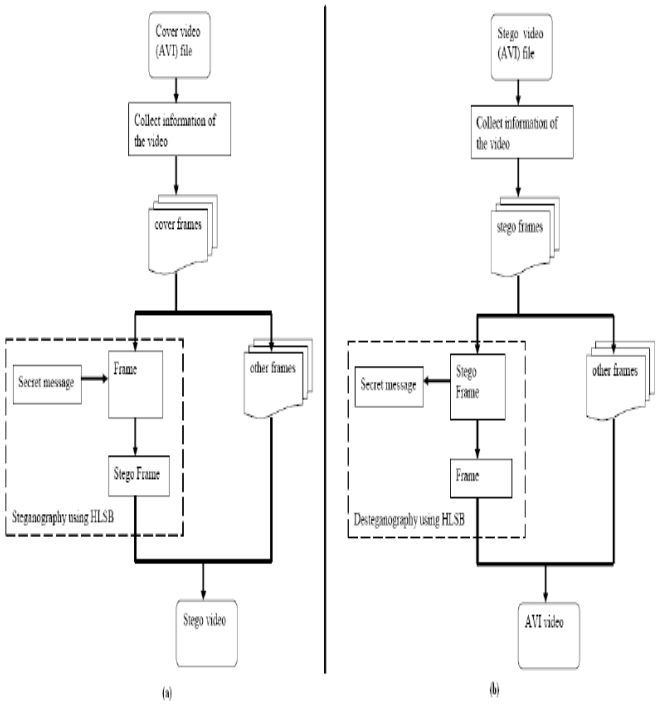

Fig-5: Block Diagram of LSB

Algorithm to retrieve text message:-

Step 1: Read the stego image.
Step 2: Calculate the LSB of the each and every pixel of stego image that is received at the receiver end and sent from the sender end [12].
Step 3: Retrieve the bits and change every 8 bit into character [13].

4.5 DCT Based Steganography

The Algorithm to embed text message:-

Step 1: Read the cover image i.e. received at receiver's end and is transferred from sender end [14].
Step 2: Read the secret message and convert it in the binary form.
Step 3: The cover image provided for merging it to the secret text is then broken into fixed 8×8 block of pixels [15].
Step 4: Working from the extreme left to extreme right, from top to the bottom subtract 128 in the each and every block of the pixels.
Step 5: DCT is then applied to the each block.
Step 6: Each and every block is then compressed through the quantization table [16].
Step 7: Calculate the LSB of each and every DC coefficient and then replace it with each and every bit of the secret message in the encrypted file.
Step 8: Finally write the stego image.

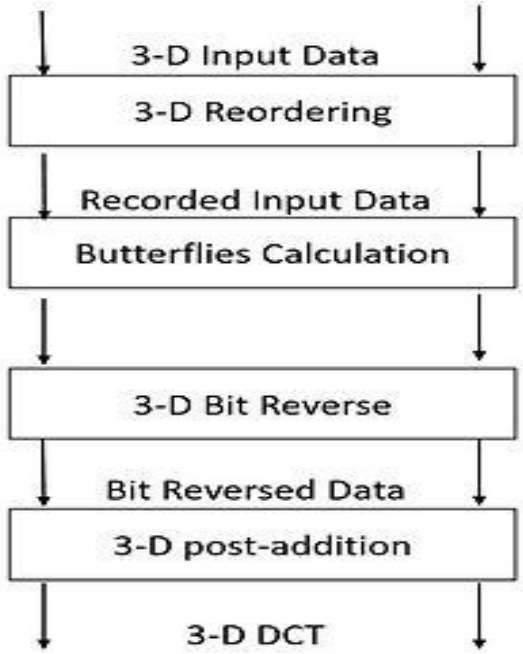

Fig-6: Block Diagram of DCT

Algorithm to retrieve text message:-

Step 1: Read the stego image.
Step 2: Stego image which is received from sender end is then broken into a fixed 8×8 block of pixels [17].
Step 3: Proceeding from extreme left to right, from top to bottom subtract 128 in each and every block of pixels of the cover image [18].
Step 4: DCT is then applied to each and every block.

Step 5: Each block is then compressed through the quantization table.
Step 6: Calculate the LSB of each and every DC coefficient.
Step 7: Retrieve and change each and every 8 bit into the character.

4.6 New Idea to Implement

The new research idea which we have explained in this research paper in detail can prove to be a milestone for the data security. Now we will use the above- mentioned algorithms together to increase the level of security multiple times. For eg. We will browse a file and encrypt it with the help of AES after this the extension of file will be changed to algorithm used i.e. .aes format, after that we will be encrypting the already encrypted file with the next encryption algorithm i.e. DES algorithm, then its extension will be changed to algorithm used i.e. .des format after which the last encrypting algorithm will be Blowfish which will change the extension to .blowfish format.

Once all the levels of encryption are completed we will proceed to the steganography. In this, we will select a video, audio, image file which is to be merged with the encrypted file.
Now we will select the .blowfish extension file and embed it into the video file. After that, the file will be transferred to the receiver.

The key point of our proposed work is that we can encrypt the data file in any of the desired order. For eg.
1) AES->DES->Blowfish
2) DES->AES->Blowfish
3) Blowfish->AES->DES, etc.

So it will always provide us with the benefit of the doubt against the attacker who is attacking the data file because he will never be able to predict the order of encryption algorithms used for encryption in such a small period of time.

5. CONCLUSION AND FUTURE WORK

Our proposed work in the research paper gives an idea about the use of different algorithms in a spectrum where the encryption and decryption process works simultaneously with the added punch of steganography which provides us with a much-needed teeth. We have tried to use the most versatile, secure, user-friendly algorithms.
It can be used in different fields like private companies, different govt. organizations like aeronautical agencies, research and development organizations, intelligence agencies etc.
In the future the levels of encryption process can be increased multiple times and also the technique used in steganography can be optimized and can be made much better to make this research more versatile and agile.

6. REFERENCES

[1] M. K. S. V. Shrivastav, "An Effective Approach to Information Hiding for Secure Message Transmission," *International Journal of Computer Trends and Technology,* 6-June 2013.

[2] D. A. S. Ambhaikar, "Audio Steganography using RPrime RSA and GA Based LSB Algorithm to Enhance Security," *ResearchGate,* November2012.

[3] S. H. O. M. M. S. H. N. Youssouf Mahamat Koukou, "Comparative Study of AES, Blowfish, CAST-128 And DES Encryption Algorithm," *IOSR Journal of Engineering,* vol. 06, no. 06, June 2016.

[4] V. k. V. Sandip Thitme, "A Recent Study of Various Encryption and Decryption Techniques," *International Research Journal of Advanced Engineering and Science.*

[5] S. M. Thampi, "Information Hiding Techniques: A Tutorial Review".

[6] I. B. a. G. S. Souvik Bhattacharyya, "A Survey of Steganography and Steganalysis Technique in Image, Text, Audio and Video as Cover Carrier," *Journal of Global Research in Computer Science,* vol. 2, no. 4, April 2011.

[7] P. C. Mandal, "A Study of Steganography Technique using Discrete Wavelet Transform," *Journal of Global Research in Computer Science.*

[8] A. Takiedeen, "Design and Implementation of Hybrid Encryption Algorithm".

[9] "Adanced Encryption Standards(AES)," in *Federal Information Processing Standards Publication 197*.

[10] K. S. S. K. Sean Laurel Rex Bashyam, "Hybrid cryptography using symmetric key encryption," *Research Gate,* no. 6, July 2015.

[11] J. M. a. P. D. Kousik Dasgupta, "Hash Based Least Significant Bit Technique For Video Steganography," *Internation Journal of Security, Privacy and Trust Management,* vol. 1, no. 2, April 2012.

[12] R. N. A. S. a. G. J. Aayushi Verma, "Implementation of Image Steganography Using 2-Level DWT Technique," *International Journal of Computer Science and Business Informatics.*

[13] G. K. S. S. Arjit Basu, "A Video Steganography Approach using Random Least Significant Bit Algorithm," *International Journal of Science and Research,* 2012.

[14] P. J. N. Dr. Ekta Walia, "An Analysis of LSB & DCT based Steganography," *Global Journal of Computer Science and Technology,* vol. 10, no. 1, April 2010.

[15] J. J. Monika Gunjal, "Image Steganography Using Discrete Cosine Transform (DCT) and Blowfish Algorithm," *International Journal of Computer Trends and Technology,* vol. 11, no. 5, May 2014.

[16] M. S. A. S. R. C. S. C. N. D. Soumyo Bose, "Effect of Watrermarking in Vector Quantization based Image Compression," *Internaional Conference of Control, Instrumentation, Communication and Computational Technologies,* 2014.

[17] H. K. V. R. K. S. C. K. S. Himakshi, "Bi-directional Pixel-Value Differencing Approach for Steganography," *Springer Link,* March 2014.

[18] J. A. S. N. A. L. G. M. B. Shabir A. Parah, "Robust and Blind watermarking technique in DCt domain using inter-block coefficent differencing," *ScienceDirect,* vol. 53, no. 6, June 2016.