IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 13, Issue 5 (Jul. - Aug. 2013), PP 01-06
www.iosrjournals.org

Secure Image Hiding Algorithm using Cryptography and Steganography

Ms. Hemlata Sharma,Ms. MithleshArya, Mr. Dinesh Goyal
Department of Computer Science and Engineering Suresh GyanViharUniversity,Jaipur
Assistant Professor,Department of Computer Science &Engineering,Maharishi Arvind Institute ofEngineering&Technology
Associate Professor,Department of Information&Technology, Suresh GyanViharUniversity,Jaipur

Abstract: *In the present scenario, any communication of internet and networks application requires security.Lots of data security and data hiding algorithms have been developed in the last decade.Cryptography and steganography are the two major techniques for secret communication.In this paper,the secret image is first encrypted by using BLOWFISH algorithm which has very good performance and is a most powerful technique compared to other Algorithms. Now this encrypted imageis embedded with videoby using LSB Approach of steganography. Our proposed model gives two layers of security for secret data, which fully satisfy the basic key factors of information security system that includes: Confidentiality, Authenticity, Integrity and Non – Repudiation.*

Keywords: *Cryptography, Steganography, Encryption,BlowfishAlgorithm,LSB.*

I. Introduction

In the present era, communication through computer network requires more security. Attacks may affect the quality of the data. There are n numbers of approaches available for it. In this paper we are introducing a new technique for image security. We are securing image by using combination of cryptography and steganography.

Cryptography

Cryptography is the art and science of achieving security by encoding message to make them non-readable [1]. Means it is used to protect the user data .Cryptography involves two basic functions that are encryption and decryption. Encryption is the process of transforming plain data(which is readable original data file) into the cipher text(data which is unreadable).Whereas decryption is just opposite process of encryption process in which we retrieve the original plain text from cipher text. Cryptography is basically used to hide the original data into a coded data so that unauthorized access can be prevented. To encrypt the data various cryptographic algorithms such as DES, 3DES, Blowfish, AES[2], etc. are used . But Blowfish is strongest and fastest in data processing and storing compare to other algorithms.

Steganography

Steganography is a technique to hide information from the observer to establish an invisible communication [3]. This steganography system consists of a cover media into which the secret information is embedded. The embedding process produces a stego medium by replacing the information with data from hidden message. To hide hidden information, steganography gives a large opportunity in such a way that someone can't know the presence of the hidden message and thus they can't access the original message.

Steganography is the art of concealing a message in a cover without leaving a remarkable track on the original message.

There are 4 different types of steganography[4]:

1.Text 2.Image 3. Audio 4. Video

- Text Steganography: They have a very small amount of redundant data, thereforethey are very oftenly used.
- Audio/Video Steganography: They are very complex in use.
- Image Steganography: It is mostly used for hiding process of data. It provides a secure and simple way to transfer the information over the internet. It is categorized in various types:

- Transform Domain: It includes JPEG.
- Spread Spectrum: It includes patch work.
- Image Domain: It includes->LSB and MSB in BMP and LSB and MSB in JPG

II. Proposed Work

Researchers have done work on various algorithms of cryptography and steganography. But on keeping in mind the present scenario, We have tried to introduce the combination of both the techniques i.e. cryptography and steganography in a different manner.

a).Proposed Architecture:

In our proposed work the system encrypts the plain image (which is in BMP Format) using BLOWFISH Algorithm and give cipher image. Now Steganography is done on this cipher image. This process gives stego video in which cipher image is hidden into video. To get original image first of all steganography process is applied on stego video. From this process cipher image is obtain.

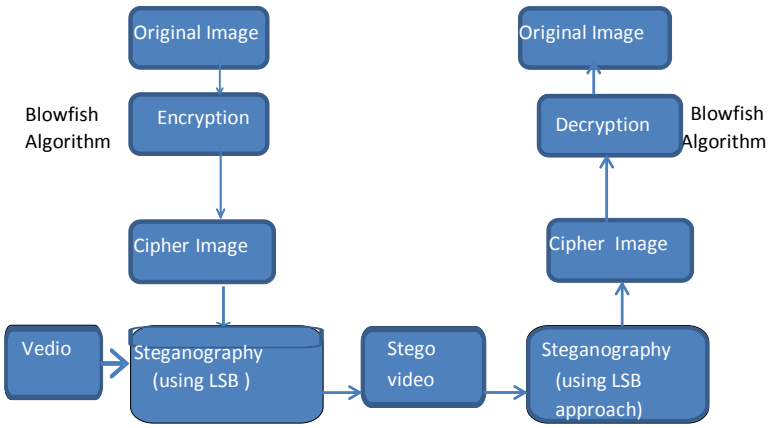


Figure 1.Block diagram of proposed system

Then again BLOWFISH Algorithm is applied on this cipher data to obtain the original image. In our whole proposed work steganography process is done using least significant bit approach.

b)Blowfish Algorithm

First question that arise in your mind is that "Why we have used Blowfish Algorithm for our proposed work?" Answer of this question depends on the following advantages of Blowfish Algorithm.

A study is done on 6 different encryption algorithms namely: AES, DES, 3DES, RC6, Blowfish, and RC2. They were implemented, and their performance was compared by encryption input files of varying contents and sizes. Testing of their performance[5] is done on 2 different machines P-II 266MHZ and P-4 2.4GHZ.The results showed that Blowfish had a very good performance compared to other algorithms. When encryption of different

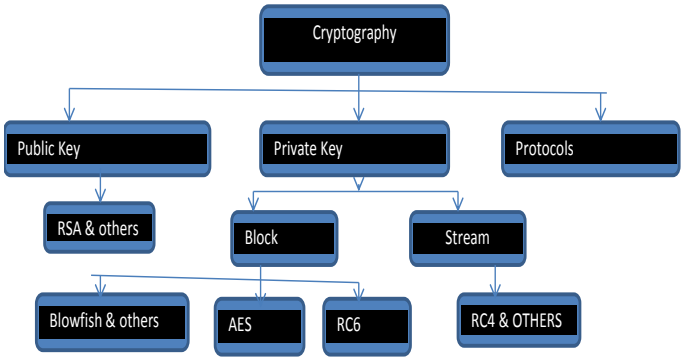


Figure 2.Category of encrption algorithms

Packet size is done using these encryption algorithms. The results show the superiority of Blowfish Algorithm over other algorithms in terms of processing time. The encryption time is used to calculate the throughput of an encryption scheme and when decryption of different packet size is calculated we find that Blowfish is the better than other algorithms in throughput and power consumption and RC6 require less time than all algorithms except Blowfish Algorithm.

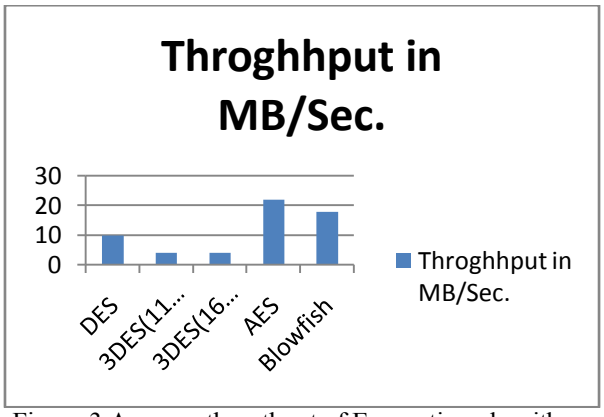


Figure 3.Average throuthput of Encryption algorithms

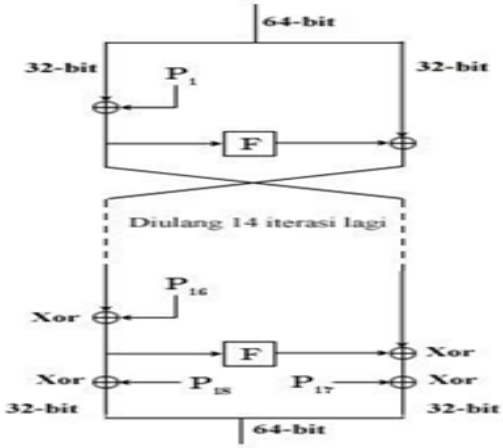


Figure 4.Blowfish algorithm

Blowfish has a 64-bit block size as shown in figure.4 and a variable key length from 32 bits up to 448 bits. It is a 16-round Feistel cipher and uses large key-dependent S-boxes [6].In blowfish algorithm a 64-bit plaintext message is first divided into 32 bits. Each line represents 32 bits. The algorithm keeps two subkey arrays: the 18-entry P-array and four 256-entry S-boxes. The S-boxes accept 8-bit input and produce 32-bit output. One entry of the P-array is used every round, and after the final round, each half of the data block is XORed with one of the two remaining unused P-entries.

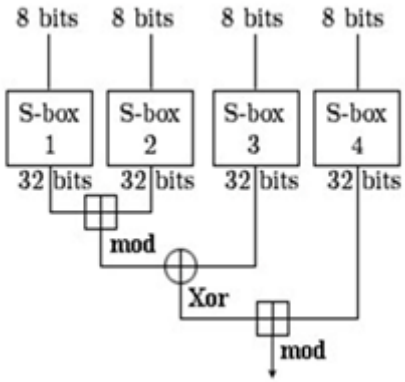


Figure 5. Work of F-function in Blowfish

The F-function as we can see in figure 5 splits the 32-bit input into four eight-bit quarters, and uses the quarters as input to the S-boxes. The outputs are added modulo 2^{32} and XORed to produce the final 32-bit output. Decryption is exactly the same as encryption, except that P1, P2,..., P18 are used in the reverse order. This is not so obvious because xor is commutative and associative.

c) Least Significant Bit (LSB):

Other question which may arise in your mind may be "Why we have used least significant bit approach for steganography and bmp format of the image?"

Before answering this question want to share some important things.Image Steganography technique can be divided into two groups: Image Domain and Transform Domain[7]. Image Domain technique embed message in the intensity of the pixel directly whereas in transform domain technique, images are first transformed and then the message is embedded in image.Image Domain technique encompasses bit wise methods that apply bit insertion and noise manipulation and are sometimes characterized as "simple system" but the transform domain involves the manipulation of algorithms and image transforms .

The LSB method is used to embed the image. Least Significant Bit(LSB) insertion is a common, simple approach to embedding information in a cover file which is video[8] . The algorithm of LSB method used in the system is described here with the help of example.

Example: The letter A can be hidden in three pixels (assuming no compression). The original raster data for 3 pixels (9 bytes) may be:

(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)

The binary value for A is 10000011. Inserting the binary value for A in the three pixels would result

(00100111 11101000 11001000)
(00100110 11001000 11101000)
(11001000 00100111 11101001)

To hide an image in the LSBs of each byte of a 24-bit image, you can store 3 bits in each pixel. Example: A image of dimension 640X480 has the potential to hide 372800 pixels or 7372800 bits (921600 byte).

Remember whenever we want to embed an image into a video. The video will be divided into number of frame. These numbers of frames depend upon the execution time of the video and also on the quality of the video means whether the video is compressed or uncompressed. If it is compressed then it will execute 22 frames per second and if it is uncompressed it will execute 18 frames per second [9].

Example: Suppose we have taken the bmp image of 640X480 dimensions and a video (uncompressed video) of the same dimension. Suppose video takes 20 seconds to execute then number of frames which is going to be generated by this video will be 20X18=360 frames. Each pixel of the hidden image uses the 8pixels of the video frames. Therefore each frame of the video contains (640X480)/8=46600 pixels

We have used BMP Image for our proposed work because by comparing between stego techniques as shown in figure 6 we find that LSB coding in BMP image is the simplest one with great invisibility and payload capacity

Characteristics	LSB in BMP	LSB in GIF	JPEG Compression	Patch Work	Spread Spectrum
Invisibility	High	Medium	High	High	High
Payload Capacity	High	Medium	Medium	Low	Medium
Robustness against statistical attacks	Low	Low	Medium	High	High
Robustness against image manipulation	Low	Low	Medium	High	Medium
Independent of file format	Low	Low	Low	High	High
Unsuspicious File	Low	Low	High	High	High

Figure 6.Comparision in stegno techniques

III. Result Analysis

Experimental results are given in this section to demonstrate the performance of our proposed method.

Step 1:Cryptography on baboon image

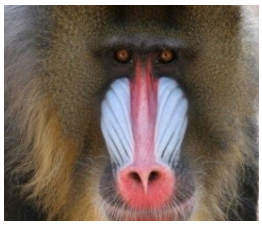


Figure 7.Original Image

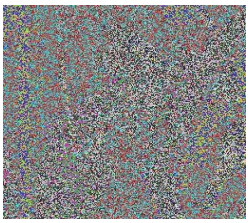
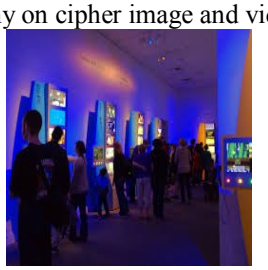


Figure 8.Cipher image after applying blowfish algorithm

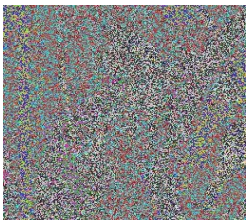
In step one we are applying blowfish algorithm on baboon image .Fig 8 is the cipher image of baboon. In step 2 we are hiding cipher image into video but as we know that video is a sequence of image and each frame of the video contains a image.

Step 2:Apply LSB approach of Stegnography on cipher image and video.



(a)

+



(b)

(c)

Figure 9. (a)Video (b)Cipher image (c)Stego Video

According to our method without the knowledge of bits no one able to know the exact position where the cipher data is placed.Because each bit of cipher data is placed at LSB of video

IV. Conclusion

We have worked on two major techniques of data security i.e. Cryptography and Steganography. In our system these two techniques provideshigher security to our data. Initially the information is encrypted by using Blowfish algorithm which is better than other encryption algorithms then the encrypted information is hidden by LSB approach . So it is very difficult for the unauthorized users to identify the changes in the stego image. The use of the blowfish algorithm and LSB gives a way to secure the information from illegal user and provide better PSNR value. In our paper we used a LSB to hide hidden image into video, which provides the new dimensions to the image steganography. It is very difficult to recover the hidden image for the third party without knowing the bits of the frames.Finally we can conclude that the proposed technique is effective for secret data communication.

References

[1]. Satinsown,D."Cryptography:Theory and practice"
[2]. RatinderKaur,V.K.Banga "Image Security using Encryption based Algorithm" International Conference on Trends in Electrical,Electronics and Power Engineering(ICTEEP 2012)July 15-16,2012 Singapore.
[3]. Zaidoon kh.AL-Ani, A.A.Zaidan, B.B.Zaidan and Hamdan.O.Alanazi "Overview: Main Fundamentals for Steganography" Journal of computing,Volume 2,Issue 3,March 2010 ISSN 2151-9617
[4]. Advanced Steganography Algorithm using encrypted secret message,JoyshreeNath and AsokeNath,InternationalJournalof Advanced Computer Science and Application(IJACSA) Vol-2 No.3,Page 19-24 ,March 2011
[5]. JawaharThakur,Nagesh Kumar, "DES, AES and Blowfish: symmetric key cryptography algorithms simulation based performance analysis",in International Journal of Emerging Technology and Advanced Engineering Volume1,Issue 2,December 2011.
[6]. B.Schneier,Description of a new Variable-Length Key,64-bit Block Cipher(Blowfish)Fast Software Encryption,Cambridge Security Workshop Proceedings(December 1993),Springer-Verlag,1994,pp.191-204.
[7]. Rafael C Gonzalez,Richard E. Woods "Digital Image Processing "Book Second Edition,Pearson Education.
[8]. Prof. DP Gaikwad, TruptiJagdale ,Swati Dhanokar, AbhijeetMoghe, AkashPathak"Hiding the Text and Image Message of Variable Size Using Encryption and Compression Algorithm in VedioSteganography"International Journal of Engineering Research and Application(IJERA) Volume 1,Issue2, pp.102-108
[9]. MrithaRamalingam, "Stego Machine – Video Steganography using Modified LSB Algorithm" ,World Academy of Science, Engineering and Technology 50 2011.