A New Approach For Image Cryptography Techniques

Harpreet Singh[#1], Dr.Naveen Dhillon[*2], Sukhpreet Singh Bains[@3]

[1]*M. Tech, Department of ECE, RIET, Phagwara, Punjab, India*
[2] *HOD, Department of ECE, RIET, Phagwara, Punjab, India*
[3] *AP, Department of ECE, RIET, Phagwara, Punjab, India*

***Abstract*-With the progress in data exchange by electronic system, the need of information security has become a necessity. Due to growth of multimedia applications, security becomes an important issue of communication and storage of images Encryption and Decryption is used to securely transmit data in open networks. Each type of data has its own features; therefore different techniques should be used to protect confidential image data from unauthorized access.The principle goal of designing any encryption and decryption algorithm is to hide the original message and send the non readable text message to the receiver so that secret message communication can take place over the web. The strength of an algorithm depends on the difficulty of cracking the original message. In kind of algorithm .a combination of four S –boxes lookups, multiplications as well as fixed and data dependant rotations will be used. In this paper we would be obtaining our results by simulating the image processing by Encryption and Decryption part in MATLAB.**

***Keywords*- Image encryption, Block cipher, Decryption**

I. INTRODUCTION

Cryptography is usually referred as “the study of secret”. The world has globally connected with internetworking, where in sharing of data has become more important .Internet is used in different ways to increase in the growth of the business. The networks have become more tasks critical and more vulnerable to malicious intents. The rapid growth of computer networks allowed large files, such as digital images, to be easily transmitted over the internet .Data encryption is widely used to ensure security however, most of the available encryption algorithm are used for text data.

Cryptography plays a very vital role in keeping the message safe as the data is in transit. Encryption and decryption converts the original message in to non-readable format and sends the message over an insecure channel. Almost all networks are being installed, interconnected to the global network. The information is not only text, but also audio image and other multimedia images have been widely used in our daily life. The digital images are commonly used are represented in 2-D array. this paper is about encryption and decryption of images using a secret –key block cipher called 64- bits blowfish which is an evolutionary improvement over DES,3DES etc designed to increase security and to improve performance. This algorithm will be used as a variable key size up to 448 bits. It employs Feistel network which iterates simple function 16 times. Specifically; in this algorithm, a combination of four S- boxes lookups, multiplications as well as fixed and data dependent rotations will be used.

II. BACKGROUND

Image encryption schemes have been increasingly studied to meet the demand for real –time secure image transmission over the internet and through wireless networks. Encryption is the process of transforming the information for its security with the huge growth of computer networks and the latest advances in

digital technologies, a huge amount of digital data is being exchanged over the various type of networks The security of digital image has become more and more important due to rapid evolution of the internet in the digital world today. The security of digital images has attracted more attention

recently, and many different image encryption methods have been proposed to enhance the security of these images. Image encryption techniques try to convert an image to another one that is hard to understand. On the other hand, image decryption retrieves the original image from the encrypted one. There are various image encryption systems to encrypt and decrypts the data and there is no single encryption algorithm satisfies the different image types. Following are the various goals of encryption/decryption which are commonly used for images.

Confidentiality: Information in the computer is transmitted and has to be accessed only by the authorized party.

Authentication: The information received by any system has to check the identity of the sender that whether the information is arriving from an authorized person or a false identity.

Integrity: Only the authorized party is allowed to modify the transmitted information. No one in between the sender and receiver are allowed to alter the given message.

Non Repudiation: Ensures neither the sender, nor the receiver of message can deny the transmission.

Access Control: Only the authorized parties are able to access the given information.

Most of the algorithm specifically designed to encrypt digital images are proposed in the mid 1990s.There are methods that offer light encryption (degradation), while others offer strong form of encryption.

There are two main categories of cryptography:

Secret key cryptography

Public key cryptography

Secret key cryptography is also known as symmetric key cryptography. With this type of cryptography, both the sender and receiver know the same secret code, called the key .Messages are encrypted by the sender using the key and decrypted by receiver using the same key.

Public key cryptography, also called asymmetric key cryptography, uses a pair of keys for encryption and decryption. With public key cryptography, keys work in pairs of matched public and private keys.

Cryptography technique is used when secret message are transferred from one party to another over a communication line. Cryptography technique needs some algorithm for encryption of data. The encryption/decryption process refers to the operation of dividing and replacing an arrangement of the original image .the image can be decomposed into blocks; each one contains a specific number of pixels. The blocks are transferred into new locations. For better process the block size should be small, because fewer pixels keep their neighbors. In this case the correlation will be decreased and thus it becomes difficult to predict the value of any given pixel from the values of its neighbors. At the receiver side, the original image can be obtained by the inverse transformation of the blocks. A general block diagram o this method is shown in figure below.

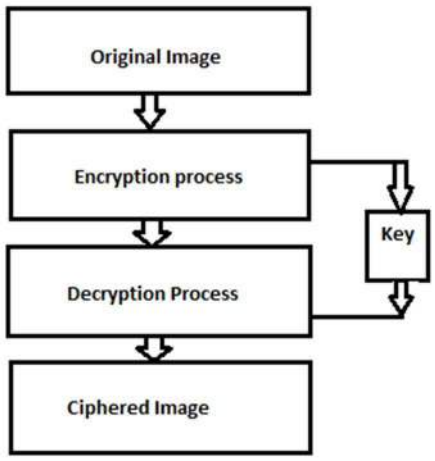

Fig: Genereal Block Diagram of Encryption/Decryption Process

PROPOSED ALGORITHM

Proposed Architecture: Proposed architecture is shown in figure below:

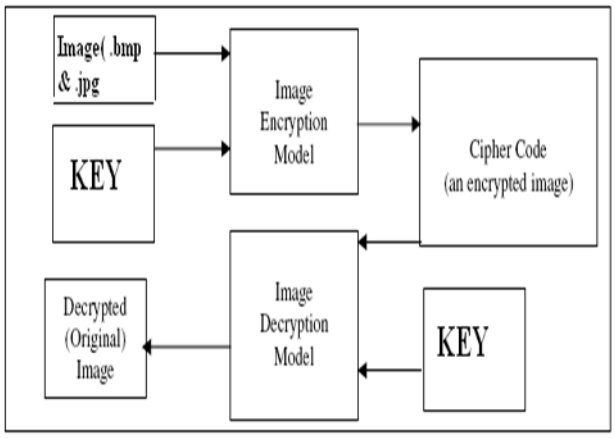

Fig: Proposed Architecture

The original message is divided into a random number of blocks that are then shuffled within the image .The transformed image is then fed to the blowfish encryption algorithm. The main idea is that an image can be viewed as an arrangement of blocks. Initially in proposed image encryption system requires .bmp or jpeg type of image file that is to be hidden. It has two modules encrypt and decrypt shown in figure. Microsoft .net framework prepares a huge amount of tools and options for programmers that they simples programming. Here some .net tools in this software called "Image Crypto System (ICS)" that is written in VB.Net language and we can use this software to hide our visual information in .bmp or .jpeg type of pictures .the encrypts module is used to hide visual information like .bmp or .jpeg image; no one can see that visual information in bmp file or jpeg files. This module requires bmp or jpeg type of image message and gives the only one image file in destination. The decrypt module is used to get the hidden visual information in original image. It takes the cipher image file as an output and gives one file at destination folder, is that bmp or jpeg image file.

Some specifications of Blowfish algorithm are as follows:

A 64 Bit block cipher with a variable key length.

There is a P-array and four 32 bit S-boxes.the P-array contains 18 of 32 bit sub keys, while each S –boxes contains 256 entries.

The algorithm consists of two parts: a key–expansion part and a data–encryption part.

Key expansion converts a key of t most 448 bits into several sub key array totaling 4168 bytes.

The data encryption occurs via a 16 round Feistel network. Each round consists of a key–dependent permutation, and a key and data – dependant substitution.

All operations are XORs and additions in 32–bit words.

The input is a 64 bit data element.

The proposed algorithm divides the image into random number of blocks with predefined maximum and minimum number of pixels, resulting in a stronger encryption and a decreased correlation.

Blowfish Encryption Algorithm:

1. Divide X into two 32-bit halves: XL, XR

2. For i = 1 to 16

   XL=XL Pi

   XR=F (XL)XR

3. Swap XL and XR (undo the last swap)

4. XR=XRP17

5. XL=XLP18

6. Concatenate XL and XR

III. RESULTS AND DISCUSSION

This method of encryption can be applied to any of the formats of images like jpg, tif, ppm, pgm, png from the browser option. The decryption for the encrypted image was carried out. The decrypted image was obtained after the transformation and blowfish algorithm was obtained. The above cases show that using the proposed algorithm followed by blowfish algorithm resulted in a lower correlation and higher entropy compared to using the blowfish alone . Dividing the image into large number of blocks made the performance even better. The results showed that the correlation was reduced even further and the entropy was increased as the number of blocks is increased .JPEG is an international image compression standard and has been widely applied to image compression .since JPEG requires 64 element quantization table for encoding/decoding, our scheme can be applied to jpeg.

In this paper we have simulated the image processing part of Encryption and Decryption in MATLAB software. Here we would taking an image. Firstly we would be obtaining the matrix and pixels of chosen image and then we would be encrypting the image matrix using blowfish algorithm. The result shows original image ,encrypted image and the decrypted image .the text in the image will be hidden using a specific key and image hidden with data is encrypted and decrypted by a 32 bit iteration loop and display in MATLAB we will clearly see that the decrypted image is same as the original image .

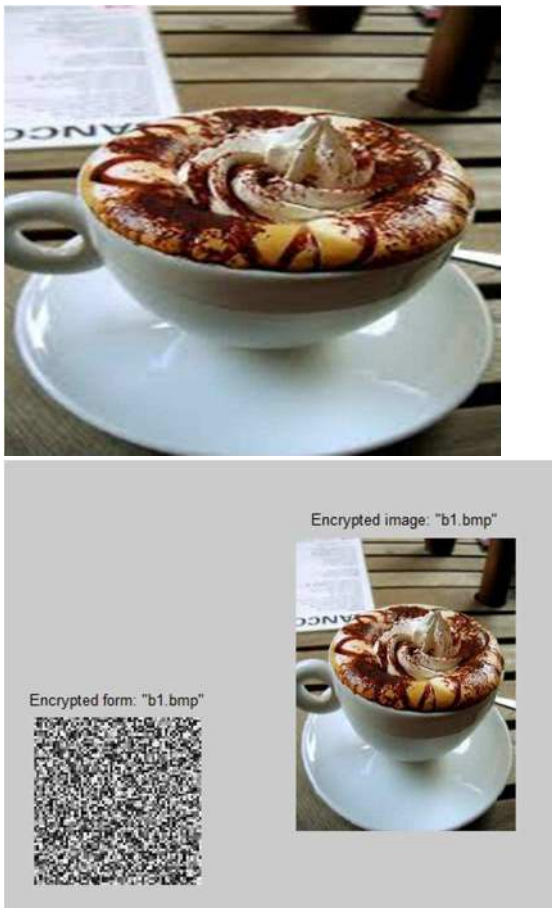

FIGURE: Original image is encrypted and message is hidden.

Display panel of output that consist the 16 iterations loop, OR, XOR commands and the algorithm code with a key that encrypts and decrypts the image that consists of a hidden text.

FIGURE: Display window in MATLAB

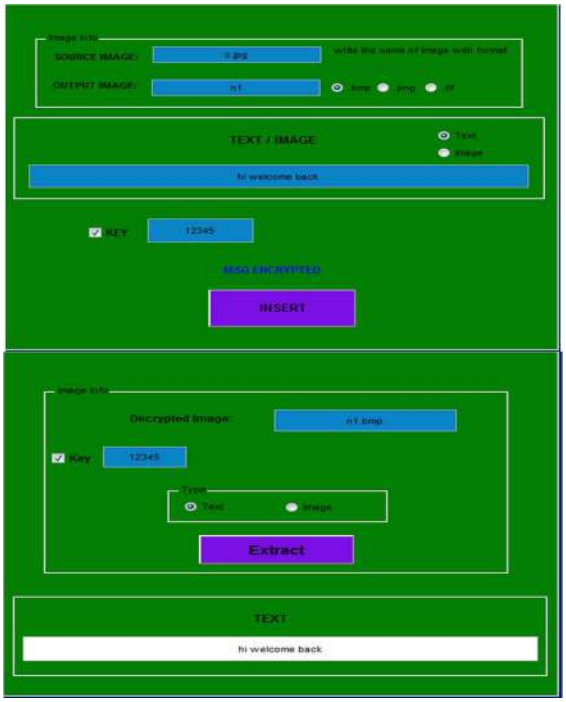

FIGURE: Input and Output window of MATLAB.

IV. CONCLUSION AND FUTURE SCOPE

The presents simulation results showed that blowfish has a better performance than other common encryption algorithms used. Since blowfish has not any known security week points so far, this makes it an excellent candidate to be considered as a standard encryption algorithm. Data encryption is a good means of security but it takes time for their operations to be performed which reduces the speed of data transfer and the capabilities of the network. When compared to many commonly used algorithms, the proposed algorithm resulted in the best performance; the lowest correlation and the highest entropy . based on the benefits of blowfish algorithm we have proposed and implemented a new approach to further enhance the existing algorithm to achieve better results in terms of parameters such encryption time, decryption time and throughput. the proposed system can be improved by using blowfish algorithm in the intrusion detection system. Better key length will provide better symmetric algorithm implementation and security. The security of proposed cryptosystem is high but hardware complexity also increases when compared with other cryptosystems.

REFERENCES

[1] William Stallings-Cryptography and network security: Principle & Practice, second edition.

[2] Onwutalobi Anthony -Claret "using encryption technique" Department of computer science, University of Wollongong Australia.

[3] M.V. Droogenbroech , R. Benedett, "Techniques for selective encryption of uncompressed and compressed images, "In acivs 02,ghent,Belgium.proceedings of advanced concepts for intelligent vision systems,2002.

[4] S. Changgui, B. Bharat, "An efficient MPEG video encryption algorithm,"Proceedings of the symposium on reliable distributed systems, IEEE computer society Press, 1998, pp. 381-386

[5] "Data Encryption Standard," Federal Information Processing Standards Publication No. 46, National Bureau of Standards, January 15, 1977.

[6] Noohul Basheer Zain Ali, and James M Noras "OPTIMAL DATAPATH DESIGN FOR A CRYPTOGRAPHIC PROCESSOR: THE BLOWFISH ALGORITHM" Malaysian Journal of Computer Science, Vol. 14 No. 1, June 2001.

[7] P. Dang and P. M. Chau, "Image Encryption for Secure Internet Multimedia Applications', IEEE Transactions on Consumer Electronics, voI.46,no.3,pp.395-403, Aug.2000.

[8] Chengqing Li, "On the security of a class of Image Encryption Scheme", IACR's Cryptology ePrint Archive: Report 2007/339, Aug. 2007.

[9] A. Sinha, K. Singh, "A technique for image encryption using digital signature," Source: Optics Communications, vol.218(4), pp.229-234, 2003.

[10] RasulEnayatifar and Abdul Hanan Abdullah , 2011,Image Security via Genetic Algorithm,International Conference on Computer and Software Modeling IPCSIT vol.14 (2011) IACSIT Press, Singapore.