A Research: Image Encryption using Chaotic & Logistic Map & Pixel Hobbling

Manju Devi[1] Uma Mehta[2]
[1]M.Tech. Student [2]Assistant Professor
[1,2]Department of Computer Science
[1,2]JCDMCOE Sirsa (Haryana), 125055, India

Abstract— Due to the rapid growth of digital communication and multimedia application, security becomes an important issue of communication and storage of images. As the use digital techniques for transmitting and storing images are increasing, it becomes an important issue that how to protect the confidentiality, integrity and authenticity of images. There are various algorithm which are discovered from time to time to encrypt the images to make images more secure. In this paper we survey on exiting work. Which is used different algorithm for image encryption It additionally focuses on the functionality of Image encryption algorithm.

Key words: Asymmetric Key Cryptography, Decryption, Encryption, Image Encryption, Symmetric Key Cryptography. AES, DES, RC4

I. INTRODUCTION

Image encryption techniques try to convert original image to another image that is hard to understand; to keep the image confidential between users, in other word, it is essential that nobody could get to know the content without a key for decryption. Image encryption, video encryption, chaos based encryption have applications in many fields including the internet communication, transmission, medical imaging, Tele-medicine and military Communication, etc. Encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption does not of itself prevent interception, but denies the message content to the interceptor. In an encryption scheme, the intended communication information or message, referred to as plaintext, is encrypted using an encryption algorithm, generating cipher text that can only be read if decrypted. For technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm. Encryption is also used to protect data in transit, for example data being transferred via networks (e.g. the Internet, e-commerce), mobiles, wireless microphones, wireless intercom systems, Bluetooth devices and bank automatic teller machines. There have been numerous reports of data in transit being intercepted in recent years. Color images are being transmitted and stored in large amount over the Internet and wireless networks, which take advantage of rapid development in multimedia and network Technologies. In recent years, plenty of color image encryption approaches have been proposed. Until now, various data encryption algorithms have been proposed and widely used, such as AES, RSA, or IDEA most of which are used in text or binary data. It is difficult to use them directly in multimedia data and inefficient for color image encryption because of high correlation among pixels. For multimedia data are often of high redundancy, of large volumes and require real-time interactions.

The image encryption algorithms can be classified into three major groups:

1) position permutation based algorithm [1]
2) value transformation based algorithm and [2, 3]
3) visual transformation based algorithm [1]

– Plaintext: An original message is known as plaintext.
– Cipher text: Coded message is called cipher text.
– Encryption: The process from converting plain text to cipher text is called Encryption or Enciphering.
– Decryption: Restoring plain text from cipher text is called decryption or Deciphering.
– Cryptography: Cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages; various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation are central to modern cryptography. There are two main types of cryptography:
  1) Symmetric Key Cryptography
  2) Asymmetric Key Cryptography

Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key. Symmetric key ciphers are implemented as either block ciphers or stream ciphers.

– Stream ciphers encrypt the digits (typically bytes) of a message one at a time.
– Block ciphers take a number of bits and encrypt them as a single unit, padding the plaintext so that it is a multiple of the block size.

Blocks of 64 bits have been commonly used. This type of cryptography technique involves two key crypto systems in which a secure communication can take place between receiver and sender over insecure communication channel. Since a pair of keys is applied here so this technique is also known as asymmetric encryption. In this method, each party has a private key and a public key. The private is secret and is not revealed while the public key is shared with all those whom you want to communicate with. If Alice wants to send a message to bob, then Alice will encrypt it with Bob's public key and Bob can decrypt the message with its private key

II. RELATED WORK

Today security is the main concern about the transmission of data. We need a cryptosystem which ensures that our data will be secure during the transmission over the network. In secured communication the information is converted from the Intelligible to unintelligible structure using certain coding operation at the transmitter. There are some techniques are used for making the data secure during conveying information over the network one of these are known as encryption and decryption.

In this paper we used both symmetric and asymmetric key and define various algorithm for image encryption. A cryptographic key is a special kind of

information that helps the sender to convert original data into encrypted form and at other end it helps the receiver to access the encrypted data. At sender side the message or data is converted into a special data format called cipher text using various encryption algorithm and secret key. The receiver side performs the same operation but in reverse order. It takes cipher text as input and then converts it into the original message. In this paper both stream cipher and block cipher type of algorithm are define such as RC4, AES and DES and proposed work. Our proposed algorithms implement in MATLAB.

A. Stepwise Explanation of Proposed Algorithm

1) Converting Image into Blocks

Read the image and divide it into three blocks of same size. In the Matlab implementation following code read the image and divides it into three blocks.

2) Reshape each block into horizontal vectors to individually pass them into the algorithm.

3) Iterate the chaotic logistic map three times to generate the three Initial Vectors.

4) Reshape each block into horizontal vectors to individually pass them into the algorithm.

5) Iterate the chaotic logistic map three times to generate the three Initial Vectors.

6) Generate three dynamic key with the help of IVs generated from chaotic logistic map.

7) Reshuffle the pixels of each block by sending them into the modified key scheduling algorithm with the three different dynamic keys obtained from the logistic map and generate three randomized S-box.

8) Send these three randomized S-boxes to modified pseudorandom generation algorithm to generate three bytes of key sequence at a time.

9) XOR the bits of the Key-sequence with the three blocks of images to generate three cipher blocks.

10) Three cipher blocks to generate the final encrypted image.

B. DES

DES (and most of the other major symmetric ciphers) is based on a cipher known as the Feistel block cipher. It consists of a number of rounds where each round contains bit-shuffling, non-linear substitutions (S-boxes) and exclusive OR operations. The key size used in DES algorithm is 56-bits for 64-bit input data. [1,2] The remaining 8 bits are used for parity checking. The encryption process is made of two permutations, initial and final permutations, and 16 Feistel rounds. In each round a different 48 bit round key is used which is produced by the cipher key.DES is therefore a symmetric, 64 bit block cipher as it uses the same key for both encryption and decryption and operates on 64 bit blocks of data at a time5 (be they plaintext or cipher text). The output of this final permutation is the 64 bit cipher text.

1) Function of DES

The 64 bit DES key is reduced to 56 bit key by ignoring every 8 bit. These left out bits are used for parity checking to ensure the key is bugs free. After obtaining the 56 bit key a different 48 bit sub key is generated for each round of the DES function. The next step in DES algorithm is computation of the DES function. This function is applied on a 48 bit key to the rightmost 32 bits (Ri-1) to produce a 32 bit output. This function is made up of four sections. Expansion P-box operations used to expands the size of right half from 32 bit to 48 bit. Expansion permutation is performed by duplication of certain bits. In a 4 bit input block produces the output of 6 bit by repeating first and fourth bit. This provides longer result which is compressed during substitution operation. S-box permutation is performed on the compressed key with the expanded block, moves the 48 bit result to a substitution operation. The S boxes are nonlinear and the critical giving the DES algorithm Maximum security. In P-box permutation each input bit is mapped using a straight permutation (each bit is used only once and none is left out). Final permutation is same as initial permutation but it works in reverse order. The Decryption process in DES algorithm is same as encryption but the only difference is that it performs all the operations in reverse order.

In the figure 1 below shows, the analysis of encryption/decryption process data recorded from DES to encrypt/decrypt an RGB image is as follows:

- Encryption Time (in seconds): 232.227
- Decryption Time (in seconds): 230.513
- Encryption Speed is: 0.68981
- NPCR: 99.6209
- PSNR: 8.7934
- MSE: 8585.0568
- UACI: 29.9153

Fig. 1: Encryption of Image with DES

C. AES

The need for coming up with a new algorithm was actually because of the perceived weakness in DES. The 56-bit keys of DES were no longer considered safe against based on exhaustive key searches and 64-bit blocks were also considered as weak. AES was to be based on 128-bit blocks, with 128-bit keys. AES supports key lengths and plain text block sizes from 128 bits to 256 bits, in the steps of 32 bits. The key length and the length of the plain text blocks need to be selected independently. AES mandates that the plain text block size must be 182 bits and key size should be 128,192 or 256 bits. In general, two versions of AES are used: 128-bit plain text block combined with 128-bit block and 128-bit plain text block with 256-bit key block.

1) Function of AES

AES uses the basic techniques of substitution and transposition (i.e. permutation).The key size and the plain text block size decide how many rounds need to be executed. The minimum number of rounds is 10(when key-size and the plain text block size are each 128 bits) and the maximum number of round is 14.One key differentiator

between DES and AES is that all the AES operations involve entire byte and not individual bits of a byte.

a) Do the following one-time initialization processes
- Expand the 16-byte key to get the actual key block to be used.
- Do one time initialization of the 16-byte plain text block (called a state).
- XOR the state with the key block.

b) For each round, do the following:
- Apply S-box to each of the plain text bytes
- Rotate row k of the plain text block by K bytes.
- Perform a mix columns operation.
- XOR the state with the key block.

In the figure below 2 shows, the analysis of encryption/decryption process data recorded from AES to encrypt/decrypt an RGB image is as follows:
- Encryption Time (in seconds): 29.6407
- Decryption Time (in seconds): 34.1327
- Encryption Speed is: 126178
- NPCR: 99.6114
- PSNR: 8.7767
- MSE: 86180686
- UACI: 29.9221

Fig. 2: Encryption of Image with AES

D. RC4

RC4 is a stream cipher design in 1987 by Ron Rivest for RSA to encrypt data therefore RC4 also called as Ron's Code 4 or Rivest Cipher also. IEEE 802.11standard use RC4 encryption algorithm to enhance security. RC4 is widely used stream cipher because of simple and efficient. This section organized as follow; Encryption and Decryption mechanism and finally vulnerability present in RC4. RC4 has become part of some widely used encryption techniques and standards, including wireless Equivalent Privacy (WEP) and WPA for wireless cards and TLS. RC4 generates a pseudorandom stream of bits (a key stream). As with any stream cipher, these can be used for encryption by combining it with the plaintext using bit-wise exclusive-or; decryption is performed the same way (since exclusive-or with given data is an involution).

1) Working of RC4

RC4 generates a pseudorandom stream of bits called as keystream**.** This is combined with the plain text using XOR for encryption. Even decryption is performed in a similar manner. There is variable length key consisting of 1 to 256 bytes. This key is used to initialize a 256-byte state vector with elements identified as S[0], S[1]……S[255]. To perform encryption or decryption operation, one of these 256 bytes of S is selected and processed; one will call the resulting output as K. After this the entries in S are permuted once again. The permutation is initialized with a variable length key, typically between 40 and 256 bits, using the key-scheduling algorithm (KSA). Once this has been completed, the stream of bits is generated using the pseudo-random generation algorithm (PRGA).

In the figure 3 below shows, the analysis of encryption/decryption process data recorded from RC4 to encrypt/decrypt an RGB image is as follows:
- Encryption Time (in seconds): 0.44108
- Decryption Time (in seconds): 0.428367
- Encryption Speed is: 847.919
- NPCR: 100
- PSNR: 8.7445
- MSE: 8662.1117
- UACI: 30.1125

Fig. 3: Encryption of Image with RC4

E. Encryption of Image with Proposed Algorithm

In the figure 2.4 below shows, the analysis of encryption/decryption process data recorded from proposed algorithm to encrypt/decrypt an RGB image is as follows:
- Encryption Time (in seconds): 0.00512398
- Decryption Time (in seconds): 0.00409918
- Encryption Speed is: 72990.2
- NPCR: 99.9366
- PSNR: 42.1135
- MSE: 3.997
- UACI: 0.78375

Fig. 2.4: Encryption of Image with Proposed Algorithm

III. CONCLUSION

In the digital world nowadays, the security of digital images become more and more important since the communications of digital products over open network occur more and more frequently. In this paper, we have surveyed existing work on

image encryption. We also give general guide line about cryptography. The results of the simulation show that every algorithm has advantages and disadvantages based on their techniques which are applied on images. Each technique is unique in its own way, which might be suitable for different application. Everyday new encryption technique is evolving hence fast and secure conventional encryption techniques will always work out with high rate of security. In this paper we study about the various cryptography algorithm such as DES AES AND RC4 as compare to my proposed algorithm .our algorithm is better algorithm. In general, a well-studied, fast and secure conventional cryptosystem should be chosen, surely those algorithms, which provides higher security.

In this research work we have shown that our proposed modification to the existing Algorithm makes it more secure and robust in terms of image Privacy. Our proposed system works well with the existing hardware and gives an edge over the present encryption Algorithm.

REFERENCES

[1] M. Zeghid, M. Machhout, L. Khriji, A. Baganne,R. Tourki,―A Modified AES Based Algorithm for Image Encryption‖,World Academy of Science, Engineering and Technology 27 2007.
[2] S.H. Kamali, R. Shakerian "A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption" 2010 International Conference on Electronics and Information Engineering (ICEIE 2010).
[3] Rasul Enayatifar , Abdul Hanan Abdullah, ―Image Security via Genetic Algorithm‖, 2011 International Conference on Computer and Software Modeling IPCSIT vol.14.
[4] Sesha Pallavi Indrakanti, P.S.Avadhani,‖ Permutation based Image Encryption Technique‖, International Journal of Computer Applications (0975 – 8887) Volume 28– No.8, 2011.
[5] Kamali, S.H., Shakerian, R., Hedayati, M.,Rahmani, M.,‖ A new modified version of Advance Encryption Standard based algorithm for image encryption‖,Electronics and Information Engineering (ICEIE), 2010 International Conference.
[6] M. Zeghid, M. Machhout, L. Khriji, A. Baganne,R. Tourki, A Modified AES Based Algorithm for Image Encryption‖, World Academy of Science, Engineering and Technology 27 2007.
[7] Qian Gong-bin, Jiang Qing-feng and Qiu Shui-sheng "A New Image Encryption Scheme Based on DES Algorithm and Chua's Circuit"
[8] Mohammad Ali Bani Younes and Aman Jantan Image Encryption Using Block-Based Transformation Algorithm‖ IAENG International Journal of Computer Science, 35,2008.
[9] Aloha Sinha, Kehar Singh, "A technique for image encryption using digital signature", Optics Communications, Vol-2 I 8 (2203), 229-234.

