Image Encryption and Decryption Using Selective Block Encryption Technique

Megha Seth, Reader*
Dept. of Information Technology
Rungta College of Engineering and Technology
Bhilai, India
meghaseth1983@gmail.com

Kaminee Salam*
Dept. of Computer Science and Engineering
Rungta College of Engineering and Technology
Bhilai, India
kaminee14.salam@gmail.com

Abstract— In the recent world, the need of information security has became a necessity with the progress in data exchange and communication by electronic system. Because of the growth of multimedia application, security becomes an important issue of communication, storage and transmission of data. Cryptography is an art which is defined as the science of writing in secret code. The cryptography algorithms are categorized into Symmetric Key Cryptography and Asymmetric Key Cryptography algorithms. Encryption is one of the best alternative way to ensure security. Moreover, there are various image encryption techniques have proposed, each algorithm has its own strength and weakness. The prime goal leading the design of an encryption algorithm must provide security against unauthorized attack. In this paper, a selective block encryption technique is proposed to achieve the different goals of security i.e., Availability, Confidentiality and Integrity. This new technique is based on the symmetric key encryption approach.

Keywords- Cryptography, Image encryption, Image decryption, Selective block encryption, Block cipher, Symmetric key algorithm.

I. INTRODUCTION

Now a day, computer has become an essential electronic device and the main use of this device is to store data and transfer the data from one location to another location. The information that is shared must be transported in a secure manner. So data may be encrypted to some formats that are unreadable by an unauthorized person. Cryptography is the science of information security which has become a very critical aspect of modern computing systems to secure the data transmission and storage.

Image encryption and decryption has become an important research area because of the increasing demand for information security and it has broad applications. In the present era the field of encryption is becoming very important. Many image encryption algorithms have been proposed. Image encryption and decryption has applications in multimedia systems, medical imaging, internet communication, military communication, etc. We must encrypt the data before it is transmitted or stored to make the data secure from various attacks and for the integrity of data. Protecting confidential data is a legal requirement because most of the information is now collected and stored on electronic computer and transmitted across network to other computer.

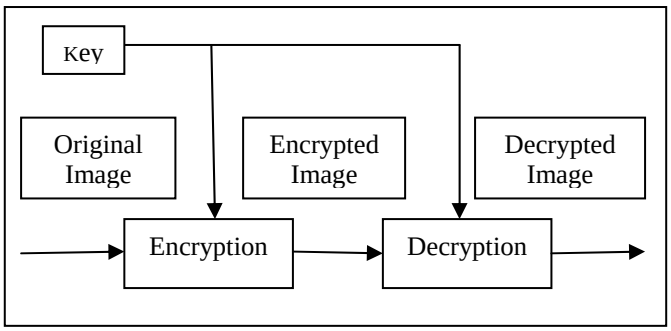

Figure1. Symmetric Key Cryptography

So in this paper, we are implementing selective block encryption algorithm. The selective encryption can reduce the overhead spent on data encryption/decryption, and improve the efficiency of the network. The main purpose of selective encryption is to just encrypt a certain portions of the messages with less overhead consumption. To provide the reliable safety to secure the transmitted message confidentiality sufficient messages are encrypted by this algorithm. Through selective encryption, not all messages are necessary to be encrypted while the entire data transmission can be viewed to be secure on the whole. The algorithm is a symmetric key algorithm that encrypts and decrypts data. Encryption process converts an original image into encrypted image. Decryption process is reverse of encryption; it is to convert the encrypted image back to original so that it can be read. It enables us to achieve three primary security goals i.e., Availability, Confidentiality, and Integrity. Usually image processing deals with an image, the selective block encryption algorithm is not only for the text data, it can also be applied for the images. The aim behind the design of this proposed algorithm is to get the best security and performance tradeoff over images

II. PROPOSED SYMMETRIC KEY ALGORITHM

This new proposed Selective Block Encryption algorithm is a block cipher. It divides data into blocks of pixels of equal length. Some blocks of pixels are selected and the only selected blocks of pixels are encrypted using a special mathematical set of functions known as key. Symmetric key technique is used in this algorithm for both encoding and decoding i.e. same key is used at both ends. Some additional tasks are performed to provide strong security to this algorithm like shuffling. There is another plus point of this algorithm is that it protects the cipher image from unauthorized access such as Brute-force as selection process is applied and the key is changed many times in the encryption process. It will be very hard to attain original image from cipher image.

III. ENCRYPTION PROCEDURE

In this algorithm, two task shuffling and selection are performed before encryption process. The shuffle process shuffles all the pixels of input image and then selection process select certain portion of pixels for encryption process. Two stacks have been taken which are predefined. Some specially chosen symbols are stored in the first stack and a random number from a preselected range is contained in second stack using predefined RNG method to make the code sequence more secure. A variety of binary functions used in the encryption process like Shift Left Operation on data to protect it against unauthorized attack.

The steps of encryption process are given as follow:

1. An image is taken as input.
2. The pixels of image are shuffled.

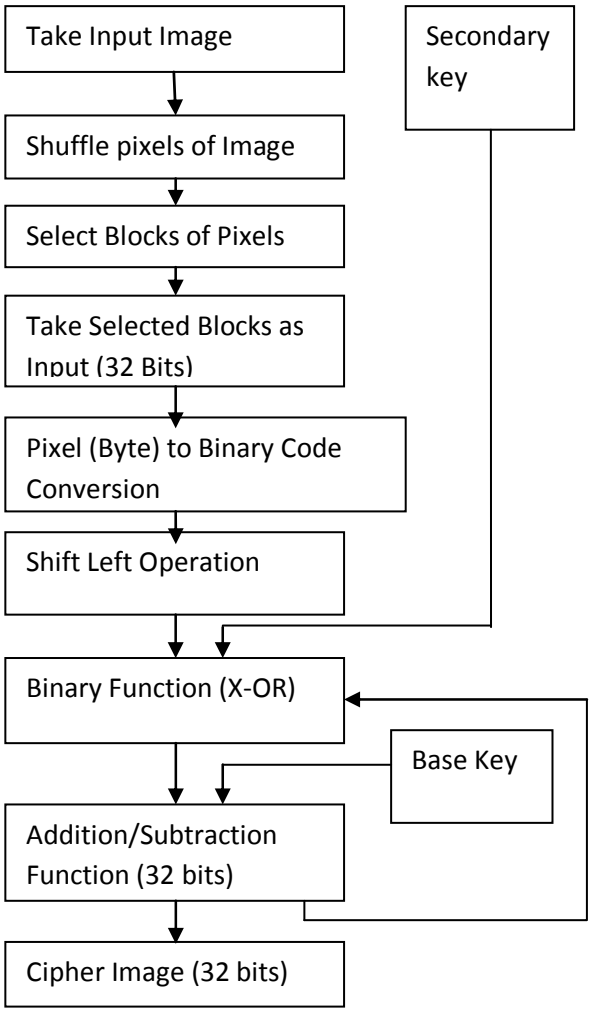

Figure 2. Encryption Procedure

3. A range is given for random numbers and a random number is chosen from the given range and converted into 16 bits binary number.
4. A sequence symbol is randomly selected from a preselected range and converted into ASCII code and then finally into binary number of 8 bits.
5. The 8 bit binary code is then appended to the 16 bits binary number resulted from random number and the result is stored as Base key or Primary key.
6. Then with the help of a binary operation the key is applied on the modified image.
7. In the next step new key is generated from a different random number and different sequence symbol.
8. A new key is generated every time and the new key is applied on the resulted cipher image of previous step and a new cipher image is obtained.
14. This process is repeated 10 times so that a different key is produced ten times and this key is applied ten times on the plaintext image or cipher image of previous round.
15. The encryption process is continued for next pixels (32 bits) of input image until end of file is reached.

IV. DECRYPTION PROCEDURE

The decryption process is exactly the reverse of the encryption process of this algorithm. The steps of decryption are given as follow:

1. The cipher image (32 bits) read from received file.
2. The key is read from central database server.

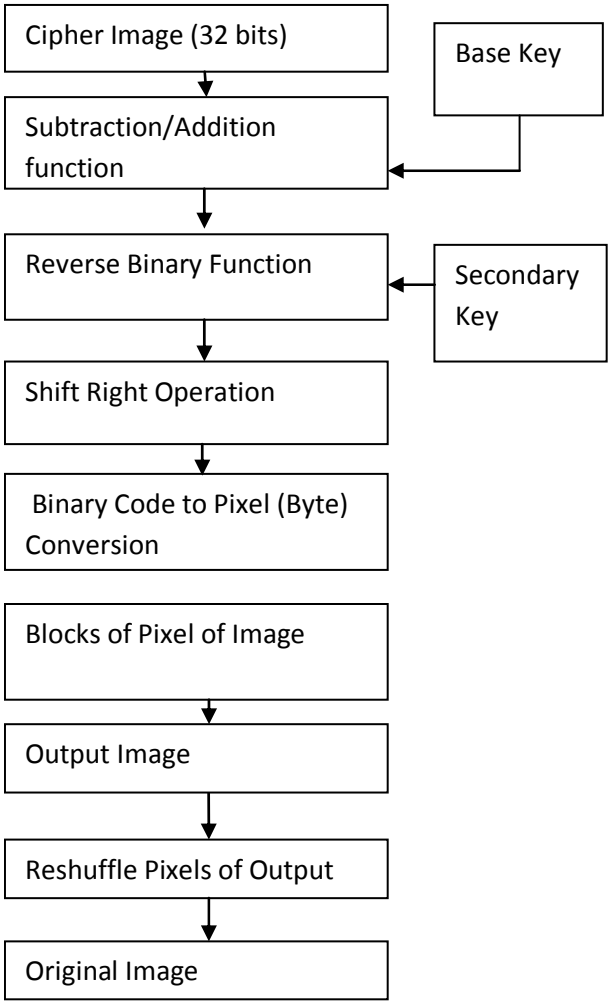

Figure 3. Decryption Procedure

3. The binary operations are performed similarly on cipher image depending upon the nature of the key.
4. To get the modified cipher image steps 1 to 3 are performed 10 times.
5. Then with the help of 32 bits Secondary key reverse binary operation is done on the modified cipher image.
6. In next step 10 times shift-right operation is performed 10 times on the result of previous step.
7. Steps 1 to 6 are repeated till the end of the cipher image and output is stored in binary form.
8. The binary output is altered into bits form (pixels).
9. These blocks of pixels give an output image and finally the pixels of the output image are reshuffled to obtain the original image.

V. PERFORMANCE EVALUATION

There are some popular block ciphers and their basic feature is that they all are fully dependent on key and the key remains same for the whole plaintext image. Every time when a key is applied to the plaintext image the block cipher produces same cipher text image. This is the major disadvantage of block cipher. The proposed Selective Block Encryption algorithm is best possible solution for the above mentioned drawback. The algorithm uses selective encryption to reduce the cost and execution time and keeps changing the key based on randomly selected integer number and sequence symbol. These features make the algorithm more safe and secure. It does different binary operations on plain text image or cipher text image to make it harder to crack.

A. Timing Analysis

The speed of encoding and decoding of data is the core advantage of any cryptographic algorithm. The Selective Block Encryption algorithm is specially designed to reduce the cost and execution time of the process. The following table shows the performance analysis of Selective Block Encryption algorithm against the some well known algorithms.

Table I. PERFORMANCE ANALYSIS OF SELECTIVE BLOCK ENCRYPTION ALGORITHM

IMAGE SIZE	ENCRYPTION TIME (SEC)	DECRYPTION TIME (SEC)	TOTAL EXECUTION TIME (SEC)
128*128	322.36	409.72	732.08
196*196	648.49	1003.63	1652.12
256*256	1611.81	1950.24	3562.05

B. Memory Requirements

The following table shows the memory required by the Selective Block Encryption algorithm and other encryption algorithms like DES encryption algorithm and AES encryption algorithm. The memory requirement of Selective Block Encryption Algorithm is half as compare to these two algorithms.

Table II. MEMORY REQUIREMENT OF SELECTIVE BLOCK ENCRYPTION ALGORITHM

ENCRYPTION ALGORITHM	KEY LENGTH (BITS)	PLAINTEXT IMAGE BLOCK SIZE (BITS)	CIPHER TEXT IMAGE BLOCK SIZE (BITS)
DES	56	64	64
AES	128	128	128
Selective Block Encryption	24	32	32

VI. SIMULATION AND RESULT

In this paper, the encryption and decryption part have been simulated in MATLAB. Here, an image is taken as input. Firstly, the pixels of the image is obtained and shuffled. Some blocks of pixels of the image are selected for encryption process and that certain portion of the image is encrypted using Selective Block Encryption algorithm. The encrypted image is decrypted by using decryption process which is reverse of encryption process. The decrypted image is reshuffled to obtain the original image. The result shows the original image, encrypted image and decrypted image. We will see that the decrypted image is same as the original image.

The input image which is encrypted and decrypted is shown below:

(a)Input Image (b) Shuffled Image (c) Encrypted Image

(d)Decrypted Image (e) Reshuffled or Original Image

Figure 4. Results of Encryption and Decryption Process

The original image which is taken for experiment is given in figure 4. The input image is shown in figure 4(a). The pixels positions are shuffled and the shuffled image is obtained and shown in figure 4(b). The encrypted and decrypted images are shown in Figure 4(c) and 4(d) respectively. At the last pixels positions of the decrypted image are reshuffled and original image is obtained and shown in figure 4(e).

VII. CONCLUSION

Security of images is very important in this internet world nowadays. In this paper, Image encryption and decryption using selective block encryption algorithm is designed and implemented to protect the confidential image data from an unauthorized access. It has been successfully implemented on the image data. Selective encryption which is used in this algorithm is one of the best solutions to reduce the cost and overhead of data protection. The procedure of encryption and decryption is considered to be having better security. The performance of selective block encryption has been compared against some well-known Symmetric Key Algorithms. The proposed algorithm is comparatively faster and provides the strong security features than the other Symmetric Key Algorithms. Hence, Selective encryption is more efficient than full encryption and this algorithm proves to be a very efficient technique for transferring confidential data from sender to receiver, achieving confidentiality as well as message authentication.

VII. REFERENCES

[1] Akhil Kaushik, Manoj Barnela, and Anant Kumar, “Block Encryption Standard for Transfer of Data,” 2010.
[2] Yonglin Ren, Azzedine Boukerche, and Lynda Mokdad, “Performance Analysis of a Selective Encryption Algorithm for Wireless Ad hoc Networks,” 2011.
[3] Bibhudendra Acharya, Saroj Kumar Panigrahy, Sarat Kumar Patra, and Ganapati Panda, “Image Encryption Using Advanced Hill Cipher Algorithm,” vol. 1, May 2009.
[4] Zhang Yun-peng, Liu Wei, Cao Shui-ping, Zhai Zheng-jun, Nie Xuan and Dai Wei-di, “Digital Image Encryption Algorithm Based on Chaos and Improved DES,” 2009.
[5] Musheer Ahmad and M. Shamsher Alam, “A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping,” vol. 2, pp. 46-50, 2009.
[6] Seyed Mohammad Seyedzade, Reza Ebrahimi Atani and Sattar Mirzakuchaki, “Novel Image Encryption Algorithm Based on Hash Function,” 2010.
[7] Kamali S.H., Shakerian R.,Hedayati M. and Rahmani M, “New Modified Version of Advance Encryption Standard Based Algorithm for Image Encryption,” 2010.
[8] Sesha Pallavi Indrakanti and P.S.Avadhani, “Permutation Based Image Encryption Technique,” 2011.
[9] Qais H. Alsafasfeh and Aouda A. Arfoa, “Image Encryption Based on the General Approach for Multiple Chaotic Systems,” 2011.
[10] K. Sakthidasan Sankaran and B. V. Santhosh Krishna, “A New Chaotic Algorithm for Image Encryption and Decryption of Digital Color Images,” vol. 1, June 2011.
[11] Alireza Jolfaei and Abdolrasoul Mirghadri, “Image Encryption Using Chaos and Block Cipher,” vol. 4, January 2011.
[12] Minati Mishra, Priyadarsini Mishra, M.C. Adhikary and Sunit Kumar, “Image Encryption and Decryption Using FIBONACCI-LUCAS Transformation,” vol. 2, September 2012.
[13] Manoj B. and Manjula N Harihar, “Image Encryption and Decryption Using AES,” vol. 1, June 2012.
[14] Sara Tedmori and Nijad Al-Najdawi, “Lossless Image Cryptography Algorithm Based on Discrete Cosine Transformation,” vol. 9, September 2012.
[15] Monish Sharma, Chandrasekhar Kamargaonkar and Amit Gupta, “A Novel Approach of Image Encryption and Decryption by Using Partition and Scanning Pattern,” vol. 1, September 2012.
[16] Gamil R. S. Qaid and Sanjay N. Talbar , “Encryption and Decryption of Digital Images Using Color Signal,” vol. 9, March 2012.
[17] Irfan.landge, Burhanuddin Contractor, Aamna Patel and Rozina Chaudhary, “Image Encryption and Decryption Using Blowfish Algorithm,” April 2012.
[18] Quist-Aphetsi Kester, “A Cryptographic Image Encryption Technique for Facial-Blurring of Images,” vol. 3, May 2013.
[19] Nithin N, Anupkumar M Bongale and G. P. Hegde, “Image Encryption Based on FEAL Algorithm,” vol. 2, March 2013.
[20] Quist-Aphetsi Kester, “Image Encryption Based on the RGB pixels Transposition and Shuffling,” pp. 43-50, June 2013.
[21] S. Reddy Jyoteeswara Prasad and R. V. S. Sathyanarayana, “Image Encryption Using Color Key Images,” vol. 2, October 2013.
[22] M. Surya Bhupal Rao and Dr. V. S. GiridharAkula, “Chaotic Algorithm Used for Encryption and Decryption on Moving Images,” vol. 2, August 2013.
[23] Shetty Deepesh Sadananda and Anusha Karkala, “Image Encryption and Decryption Using Image Gradient Technique,” vol. 3, January 2013.
[24] Atul, Kahate, Cryptography and Network Security, (Second Edition 2008).