Color Image Encryption and Decryption Using DES Algorithm

Manjula K G[1], M N Ravikumar[2]

M.Tech (EC) (4th SEM), Dept. of ECE , Malnad College of Engineering , Hassan, India[1]

Associate Professor, Dept. of ECE , Malnad College of Engineering , Hassan, India[2]

---***---

Abstract - *Data Encryption Standard was the most well known utilized cryptographic scheme and it is symmetric key block cipher algorithm. DES was a widely used cryptosystem for securing the classified data transmissions. In this project DES algorithm is utilized to image file encryption and decryption. The software implementations results are done with MATLAB. With detailed analysis Experimental results are explained and proposed plan has strength to resist the developing attacks on security of image file transmissions. The acquired results demonstrate that DES algorithm could be utilized as a highly secure algorithm.*

***Key Words*: DES, decryption, encryption**

1. INTRODUCTION

These days the data security is the important aspect of digital data communications. Since this information happen to more significance and secrecy like managing account information, military information, delicate data like medical records, and multimedia data, for example image, sound, or video. This requires a need of satisfactory and successful cryptographic algorithm to secure these sorts of information transmissions from an unauthorized user revealing. Then again, the pace of the innovation and the improvements in the field of computational processing speed in our lives is turning out to be quicker and speedier. These improvements facilitate the threats and attacks on the information or data to uncover its secrecy progressively and load the enormous test of fulfill the undertaking of securing the communications.

Best approach of security assurance is Encryption. For changing input image into another image, encryption system used many techniques. So that changed image is difficult to understand by other unauthorized person and to maintain the secret of images between clients. Another advantages of encryption technique is can’t access the image information without decryption key. Main application of image encryption is multimedia frame work.

Here we are using established cryptographic algorithm that is Data Encryption Standard (DES). DES was a generally utilized cryptosystem for securing the characterized information transmissions. DES is a symmetric key cryptosystem that is nothing but for both encryption process and decryption process, using same secret key. Many algorithm keeps DES as their core design for cryptographic design. By upgrading DES's security, other algorithm' security, for example, Triple-DES and IDEA will be improved. In this project, a capable change is proposed to bring the legacy DES to live by strengthening its security.

2. CRYPTOSYSTEM

Cryptography is art of making a cryptosystem is shown in Figure.1, equipped for giving data security. Cryptography manages the genuine securing of advanced information. It refers to the outline of systems in view of mathematical algorithms that give major data security administrations.

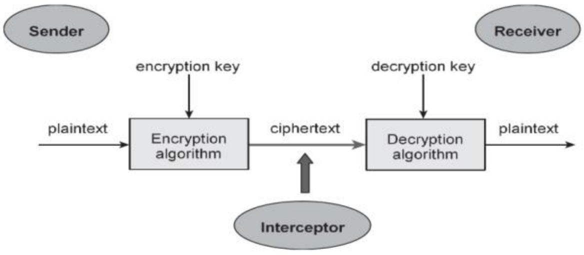

Figure 1: Cryptosystem

2.1 Security services of Cryptography

Authentication- Identity of the receiver and sender should be verified in communication system, before sending as well as receiving the information in system.

Secrecy or confidentiality-In the secured system, this is a task of the system to how best security which people maintain. Authorized users are capable to understand and access the data in the system.

Integrity-Assurance of the transmitted data has to be free for any alternation between sender and receiver in communication.

Non repudiation- guarantees the package security, element can't decline the responsibility for past activity. This is nothing but information sender and receiver certification.

3. DATA ENCRYPTION STANDARD

DES considered as symmetric key block cipher algorithm. The implementation structure of DES is Fiestel cipher. In Fiestel structure as 16 rounds of steps are used.64 bit block size is used for DES structure .It has 64 bit key length, but DES utilizes only 56 bit key. Remaining 8 bits is used later but not used for encryption.

Considering the method, Encryption process includes two inputs to the function of encryption. That in plain text is an input and key. In encryption process of DES used 64 bit plain text and 56 bit length key.

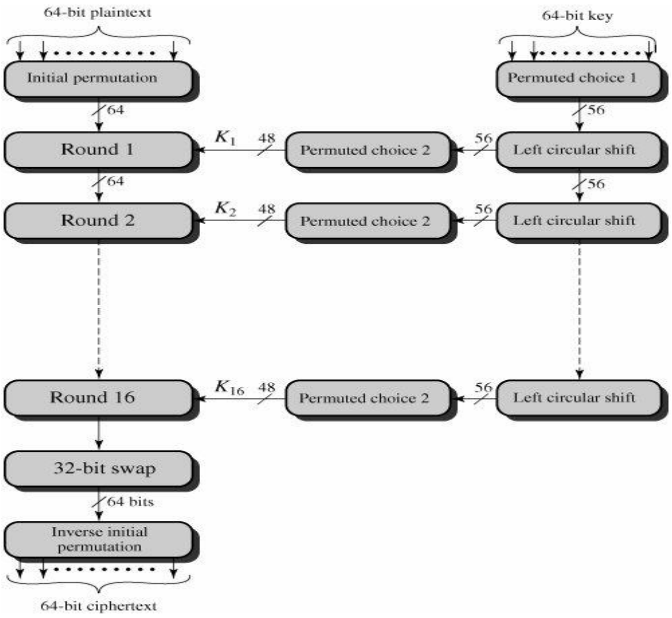

Figure 2: Basic structure design of DES encryption

Three steps of plain text processing are shown in the left side of the above figure.2. First step is initial permutation, 64-bit blocks input plain text is rearranges the bits. That is considered as permuted input, which means arranged bits. This step followed by 16 rounds of operation coninously.These 16 rounds process involves the permutation, substitution function, Last 16th round considered as output. So this last round had 64 bits. The key and function of output data is of 64 bits. Swapping the right and left side output halves. Swapped data is called as preoutput, last step includes inverse permutation process of preoutput that is called as reverse operation of initial permutation that is final permutation it has 64 bit length output.

56 bit key is produced in the right side of the figure, this key is passed in permutation block for encryption .Key can written as by name sub key K_i ,it is a combination of permutation and left circular shift. Same permutation function is used but produced sub keys are different because shift of the key bits are repeated.

3.1 DES Algorithm

As already mentioned DES is symmetric key block cipher algorithm. Currently this algorithm use identical secret key for both encryption process and decryption process. General algorithm design 64 bit plaintext used as input. The algorithm transforms input into series of block which is 64 bit cipher text.16 rounds of encryption process is handled for every plaintext block. Decryption process is done in reverse manner of encryption method, by introducing sulky k_i introduced by main key k where i=1……….16.

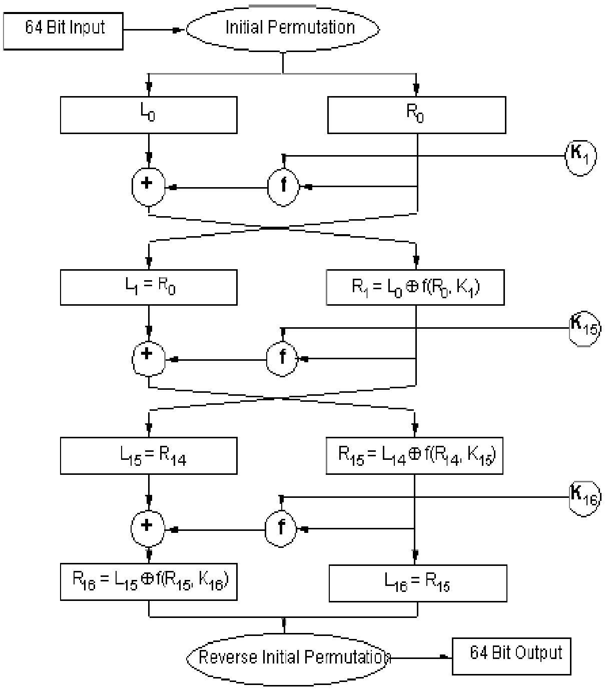
64 Bit Input
Initial Permutation
L_0
R_0
K_1
+
f
$L_1 = R_0$
$R_1 = L_0 \oplus f(R_0, K_1)$
K_{15}
+
f
$L_{15} = R_{14}$
$R_{15} = L_{14} \oplus f(R_{14}, K_{15})$
K_{16}
+
f
$R_{16} = L_{15} \oplus f(R_{15}, K_{16})$
$L_{16} = R_{15}$
Reverse Initial Permutation
64 Bit Output

Figure.3: DES algorithm structure

3.2 Single DES round Operation

As shown in figure 4, DES algorithm structure three phase of operation is considered for plain text. Input data undergone initial permutation in first phase of operation. In second phase produced permuted output that is rearranged. IP blocks split into two parts named R_0, L_0.Performs substitution and permutation process by function f and sub key Ki. Function f XORed with 32 bit right half data. Final phase is swapping between left and right half of system algorithm. This procedure repeated for next 15 round it considering the below equations.

$L_i = R_{i-1}$

$R_i = L_{i-1} \oplus f(R_{i-1}, k_i)$.

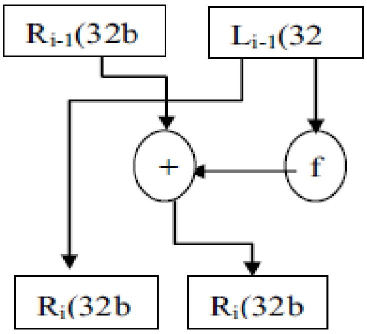

Figure 4: DES single round method

R16 and L16 swapped again after the 16th round process. Reverse operation of initial permutation is called final permutation, to get cipher text. Finally we got output of 64-bit data same as input data.

4. IMAGE ENCRYPTION AND DECRYPTION

4.1 Image Encryption

In the encryption method we considered two inputs, one is encryption secret key and another one is original color image. Image file can be reshaped or divided pixel block of original image and express DES encryption process and defining the key for encryption that is secret key. By using DES algorithm procedure finally original image is encrypted with security, this is encrypted image. Image file encryption practice is presented in figure 5.

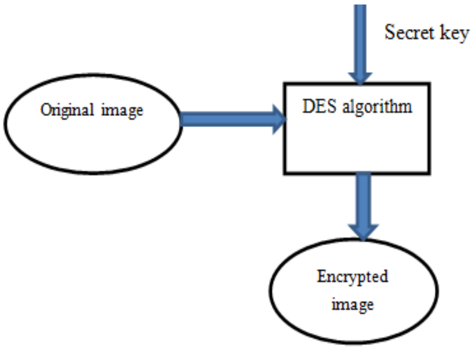

Figure 5: Encryption

4.2 Image Decryption

It is a reverse process of Image encryption. In this method encrypted image is considered as input for DES algorithm structure for decryption. Encrypted image is divided again into pixel blocks that are same as DES algorithm block length. Primarily function blocks of 64-bit size are entered. Then same secrecy key that is decryption key used for process of decryption which one is used for encryption. Here we follow a reverse ordered procedure of encryption. After completion of decryption, obtained output is considered as decrypted image, it follows the same characteristic of original image.

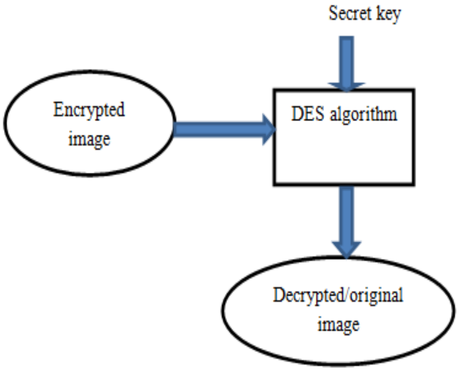

Figure 6: Decryption

5. RESULTS

In this paper we represented the color image encryption and decryption with MATLAB. Here we select the Lena image with size 225x225.The proposed DES algorithm is applies on the Lena image. The input image is split into 8x8 block based on the 64 bit constrain. The results of image encryption and image decryption using ECC based DES algorithm is done successfully.

The Lena image is considered as input image is shown in Figure 7 and the image representation in green red and blue plane shades is shown in figure 8.

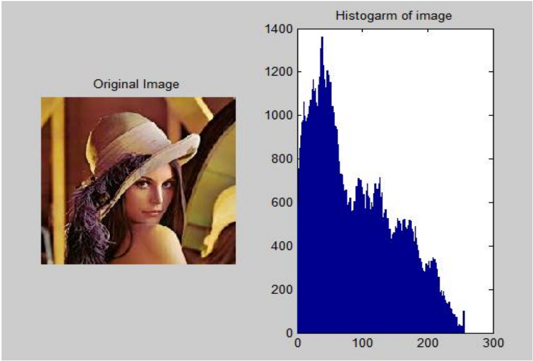

Figure 7: Input image

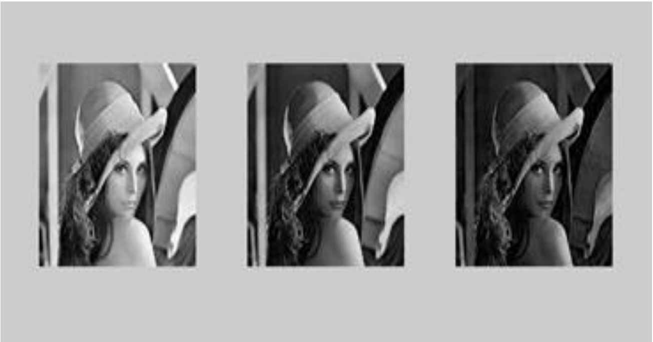

Figure 8: Image shades in different plans

Secured Image file transmission in communication channel will do with help of encryption. We converted Lena image to another form using encryption method, the changed image is in encrypted form, and to get back the image which one is send by the sender, we reversed the encryption operation, it is called as decryption of image .The input image, encrypted image then decrypted image is as presented in Figure 9.

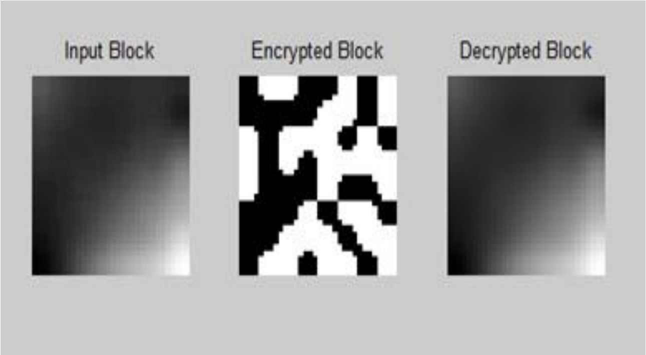

Figure.9: Encrypted and Decrypted image

6. CONCLUSION

Color image encryption and decryption is done by using DES algorithm, by providing required security for image between two authorized users or clients. In our project DES guarantee the unbreakable security for color image. In the project image encryption is done using DES algorithm, Experimental consequences of proposed DES algorithm is very motivating. The implementation approach shows the encrypted and decrypted image and also historical analysis is done with enhanced techniques.

Future work of our project is based on enhancing T-DES security level by implementing DES technique, by repeating three times of DES key to generate three sets of key for T-DES algorithm for make T-DES algorithm more secure. Another future plan is of applying this proposed DES method for encrypting the video file to providing secure transmission in communication channels.

REFERENCES

[1] R. Huang and K. Sakurai,"A robust and compression-combined digital image encryption method based on compressive sensing,".The7t International Conference on IIH-MSP, Dalian, Oct.2014–16 2011, pp. 105–108.

[2] A K Mandal, C Parakash and Mrs. A Tiwari, "Performance Evaluation of Cryptographic Algorithms: DES and AES", IEEE Students' Conference on E and E,C S, pp. 1-5, 2012.

[3]A. Yahya and A. Abdalla, "A shuffle image-encryption algorithm, "Journal of Computer Science, pp. 999–1002, Dec. 2008.

[4] Mayank, P Singh, C Garg," A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping "International Journal of Information & Computation Technology. Volume 4, Number 7 (2014), pp. 741-746

[5] Zhang Yun, Liu Wei, Shui-ping, Zhai Z-jun , "Digital image encryption algorithm based on chaos and improved DES", IEEE Conference on Systems, Man and Cybernetics, 2009.

[6] Sesha P Indrakanti , P.S.Avadhani, Permutation based Image Encryption Technique, International Journal of Computer Applications (0975 – 8887) Volume 28– No.8, 2011

[7] Mohammad Ali B Y and Aman J, "An Image Encryption Approach Using Combination of Permutation Technique Followed by Encryption", International Journal of Computer Science and Network Security, VOL.8, April 2008.

[8] Amitava Nag, Jyoti Prakash, Srabani Khan, Saswati Ghosh," Image Encryption Using Affine Transform and XOR Operation ",International Conference on ICSCCN 2011.

[9] Diaa Salama Abdul. Elminaam, Hatem Mohamed Abdul Kader and Mohie Mohamed Hadhoud, "Performance Evaluation of Symmetric Encryption Algorithms", IJCSNS International Journal of CS and NS, VOL.8 No.12, pp. 280-286, December 2008.

[10] Shashi Mehrotra Seth, Rajan ishra, "Comparative Analysis of Encryption Algorithms for Data Communication", International Journal of Computer Science and Technology, Vol. 2, Issue 2, pp. 292-294, June 2011.

[11] W. Stallings, Cryptography and Network Security, 5th ed. New York, USA: Prentice Hall, 2011, pp. 77–96.