INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

A Modified Image using DES Algorithm – A Review

Kushal S. Patel [1]

[1] ***Vidya Pratishthan's College of Engineering, Baramati, Maharashtra***
Email: *patelkushal4444@gmail.com*

Abstract

Image encryption is distinct from text encryption. Normal text encryption algorithms are not work efficiently on multimedia objects. To increase security of multimedia data we propose a novel technique. In this paper, we propose a novel scheme to encrypt image object to protect it from external attacks in transmission. This method is based on Data Encryption Algorithm and can be used in data parallel fashion to reduce the time required time to encrypt and decrypt image so that we can attain the purpose of high speed. The method is implemented by block cipher method. Key generation is done using amplitude modulation technique and provides more security against attacks. Pixels of image are rearranged and algorithm is applied on the basis of channels. Basics are very much similar to DES algorithm with some new schemes related to image processing. Significant increment in security is expected to be achieved in the proposed method.

Keywords: *image encryption; DES; amplitude modulation; block cipher.*

1. INTRODUCTION

Cryptography is an art or science which deals which security. Now a day due high usage of information science in all areas, there is requirement to transfer data in secured form. In most of the cases data is necessarily kept hidden from third party can Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Cryptography applications include ATM cards, computer passwords, and electronic commerce [1].

There are various techniques are available to encrypt and decrypt the plaintext data. Such algorithms are classified mainly into two categories Asymmetric key cryptosystem and Symmetric key cryptosystem. In Asymmetric key cryptosystem, two keys are associated with an algorithm. One of them is private key i.e. which is known to all the parties including untrusted parties while another one is private key which is kept secret. In symmetric key cryptosystem, algorithm uses only one key for encryption and decryption of data. This key is secreting to valid sender and valid receiver. If unauthorized party gats this key then the security of this algorithm breaks down. The main problem with this concept is the key exchange.[2] To exchange the secrete key the slandered algorithms like diffieHelman key exchange methods are used.

As these algorithms are designed for textual data, they cannot be used directly for multimedia objects like image. Complexity of these methods goes very large when used as it is for multimedia objects.

There are various cryptographic techniques are available in the area of information security to encrypt the multimedia objects. This image container is encrypted to have more security in communication channel. Some sophisticated algorithms provides much security of confidential data and used for image data.

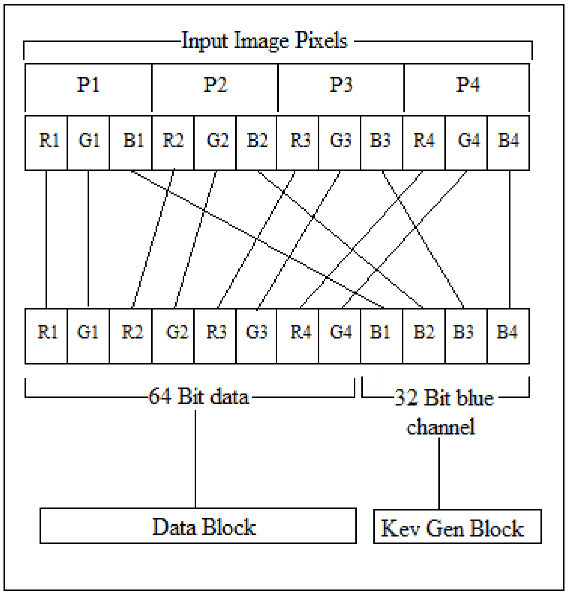
2. CONCEPT OF CHANNELS AND AMPLITUDE MODULATION

Let $I(m, n)$ be a color image of size $m \times n$. i.e. an input image. In the concept of amplitude modulation any image is viewed as collection of three hypothetical channels. Transmission of image deals with transmission of these three channels. The RGB color system is used, then $I(m, n) = \{R(m, n), G(m, n), B(m, n)\}$. As we have to encrypt the image using amplitude modulation, encryption is done on the basis of channels. After encryption the image becomes $I'(m, n) = \{R'(m, n), G'(m, n), B'(m, n)\}$. In the color image these three channel values are placed in alternate fashion. Each pixel in these type of object is made up from logical channels each of 8 bit wide. Total visual effect of the pixel is dependent on resultant of these values[4].

To encrypt image this characteristics is used in the proposed method. In this method, pixels are combined together to form a sufficient length of input and from that bit sequence key is generated. Gathering of values of particular channel leads to generation of key. At the destination side this key is not available so, to decrypt data this channel values to be appended to reconstruct the image at destination. In this technique, two channels are encrypted using third channel value as key.

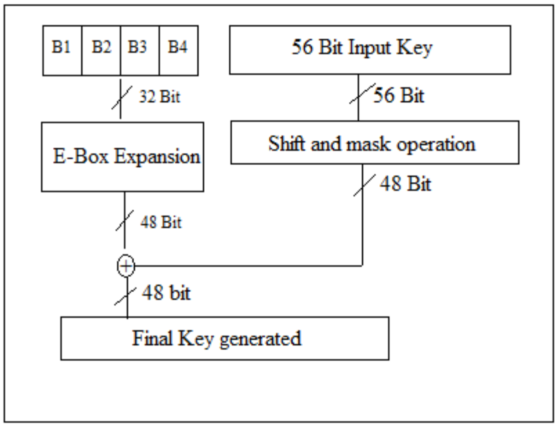
To encrypt image channels in pixel are used to embed information. Blue channel is generally used as key because blue color has less sensitive to human eyes comparing with the red or the green ones, so better invisibility can be achieved[2]. At the receiver end the image is decrypted to achieve actual image. Encrypted image $I'(m, n) = \{R'(m, n), G'(m, n), B(m, n)\}$. Here B(m,n) is kept as it is for retrieval of data.

3. COMBINATION OF PIXELS AND KEY GENERATION



(Figure 2. Channel seperation and combination)

In this method, blue channel values in each pixel are separated out to form a 32 bit value. This value is then used for key generation mechanism. Four successive pixels are combined together to form a data block of size 64 bits. This data block contains only R and G channel values while blue channel is used for key computational purpose.



(Figure 1. Key generation)

Once the channels are separated out, this 32 bit value is supplied to E-box(which is covered in later sections.) E-box produces 48 bit output which is compatible with the key input. These two values are EX-ORed to form actual key for this algorithm. This key value is used in each round for encryption. Once the encryption is done blue channel values are simply appended to the encrypted block so that the destination key computations can be done.

4. Conclusion

Thus we proposed a novel methodology for encryption of digital images using amplitude modulation technique and DES algorithm. This algorithm generates key value based on channel value of image pixel and tends to more secure cipher image as output. This key transformation is kept hidden from unauthorized third party and key value calculated each time is different for different block. This method is based on DES and simple to compute on today’s advance computers and provides more security against attack. This method provides encryption to achieve data protection effectively while with reasonably costs.

References

[1] C. K. Huang , H. H. Nien, “Multi chaotic systems based pixel shuffle for image encryption,” Optics Communications 282 (2009) 2123–2127.

[2] L. Zhang, X. Liao, X. Wang, “An image encryption approach based on chaotic maps,” Chaos Solitons Fractals 24 (2005) 759.

[3] K. Wang, W. Pei, L. Zou, A. Song, Z. He, “On the security of 3D Cat map based symmetric image encryption scheme,” Phys. Lett. A 343 (2005) 432.

[4] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett. 20, 767-769,1995.

[5] M. Jarova, M. Kakuta, M. Yamaguchi, N. Ohyama, "Optical implementation of the stream cipher based on the irreversible cellularautomata algorithm," Opt. Lett. 22, 1624-1626. 1997.

[6] B. Javidi, A. Sergent, E. Ahouzi, "Performance of double phase encoding encryption technique using binarized encrypted images," Opt. Eng. 37, 565-569,1998.

[7] Zhenjun Tang, Weimin Wei, “Fast Algorithm for Color Image Scrambling”, Computer Engeering, 2008, Vol. 34, No. 6: 153-157.J.

[8] Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[9] Feng Huang, Yong Feng, “Image Encryption Approach Based on a New Invertible Two-Dimensional Map”, Optical Technology, 2007, Vol. 33, No. 6: 823-826.

[10] Zhenjun Tang, Xing Lu et al., “Image Scrambling Based on Bit Shuffling of Pixels”, Journal of Optoelectronics Laser, 2007, Vol. 18, No. 12: 1486-1489.