International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Partial Image Encryption Using Block Shuffling and Pseudo Random Number Generator

Rakhi Lande[1], Rekha Pandit[2]

[1]M. Tech, Computer Science and Engineering, LNCT College affiliated to RGPV, BHOPAL, MP, India

[2]Assistant Professor, Dept. of CSE, LNCT College affiliated to RGPV, BHOPAL, MP, India

Abstract: ***This paper is a review on the partial image encryption. The main motivation is to reduce the computational time for real time application. Each type of data has its own features; therefore different techniques should be used to protect confidential image data from unauthorized access. In this paper we would like to describe a general approach to generate secure image by using partial image encryption using block shuffling and pseudo random number generator.***

Keywords: Real time applications, partial image encryption, random number.

1. Introduction

Internet applications are growing day by day, with this immense increase in the growth of internet and technologies; there is also an increase of breakdown of security. Information that is transmitted on the internet is more in form of multimedia i.e. it contains text, images audio and video. Image plays an important role, because this one of important method of authentication of various entities. Image information is different from text data, it has larger amount of data, higher redundancy and stronger correlation between pixels. Security of such images becomes very crucial. Cryptography technique is used to provide security to text as well as images. Image encryption is used to protect and transmit images into various forms. There are a number of encryption algorithms available which perform the task of encryption. Some of the algorithms are fully layered which can perform the encryption of the whole content of the images. But sometimes there is a need of partial image encryption so that there is reduced computational time and hence increases in performance. Partial image encryption is a secure encryption algorithm which is used to encrypt only selected part of the image. The main advantage of the partial image encryption technique is that it can provide equally, privacy and computational requirements without tradeoffs.

Encryption algorithm such as RSA, AES and IDEA are used to encrypt text and binary data. But in case of image encryption it is difficult because of the high correlation among pixels, high redundancy, bulk capacity of data, so these algorithm are not suitable for real time application [9].

Image encryption has found a significant place in both public and private services such as military surveillance, satellite information system, secure electronic health record ,system has been an emerging technology that allows medical personals to create, manage, and control medical data electronically, banking applications , multimedia system etc[1][2].

This paper is organized as follows (I) Introduction section describe the need of image encryption (II) contains literature survey (III) describes about the proposed methodology for image encryption (V) conclusion.

2. Literature Survey

Panduranga H T and Naveen Kumar S K, describes the partial image encryption in two ways using Hill Cipher Techniques. First encryption uses two slightly different keys to construct two self invertible matrices which are used in two different stages to get partially encrypted images. Second encryption technique use one key to construct oneself invertible matrix and it is first stage. In second stage same key matrices along with few modifications in diagonal values are used to construct another self invertible matrix which leads to partial image encryption [3].

Nitumoni Hazarika,Monjul Saika Paper proposed a selective encryption technique using spatial or DCT domain. A chaotic logistic map is used to perform different encryption-decryption operation in this proposed method [4].

Sukalyan Som ,Sayani Sen"A non adaptive partial encryption of Grayscale Image based on chaos" have proposed a non adaptive Partial Encryption of grayscale images Based on Chaos. They decompose the original gray scale image into its corresponding binary eight bit planes then encrypted using couple tent map based pseudorandom binary number generator(PRBNG).The four significant bit planes determined by 5% level of significance on contribution of a bit plane in determination of a pixel value, are encrypted using keys which are obtain by applying recurrence relation of tent map base PRBNG.Then four significant bit planes along with encrypted bit place are combined to form the final cipher[5].

Yong-Hong Zhanghas presented an image encryption using extended chaotic sequences. In this manuscript, the chaotic cryptographic technique is used called a key cryptography. The extended chaotic processes are generated by using the n-mark rational Bezier curve. This technique achieves the high key space and good security level [6].

Varsha S. Nemade, R. B.Wagh A new encryption algorithm based on chaotic map which produced pseudo random sequence on image and makes double time encryption with improved DES. The combination of chaos and improved DES makes the final algorithm more secure, faster and more suitable for digital image encryption [7].

J.C. Yen, J.I. Guo A new encryption method based on chaotic system called CKBA (Chaotic Key Based Algorithm),in which a binary sequence as key is generated using a chaotic system. Then the image pixels are rearranged according to the generated binary sequence and then XORed and XNORed with the selected key [8].

A. Gautam, M. Panwar, Dr.P.R Gupta Introduced a block based transformation algorithm, where the image is divided into a number of blocks. These blocks are transformed before going through an encryption process. At the receiver side these blocks are transformed into their original position and decryption process is performed [9].

Daniel J. Costello, Jr. and G. David Forney A encryption algorithm was introduced based on chaos system .In which firstly, the image is converted into binary data stream by masking these data with a random key stream generated by the chaos based PRKG, then the encrypted image is formed[10].

3. Proposed Methodology for Image Encryption

3.1 Image Encryption using Linear Congruential Generator-

It is most commonly used method for pseudo random number generation [11], defined by the following equation:-

$x(k+1)=a\,x(k)+c \bmod m$ ……..(i)

where a is multiplier is modulers,c constant to be added x(k) is an arbitrary starting seed value is needed in equation (i) with above mentioned parameters for generation of random numbers which have range up to the value of modulus(m).Random numbers sequence is generated based on equation(i) by choosing appropriate parameter and seed value. Then by using value of these random numbers, image permutation occurs by shuffling of pixel blocks of image.

From the analysis new technique for image encryption is proposed to encrypt image by permutation of pixel block using Linear Congruential Generator.

Figure: Image Encryption

4. Conclusion

In this paper we presented a survey of some recent image encryption techniques. Traditional algorithm like DES, RSA and IDEA are not suitable for image data encryption because of the high correlation among pixels. To provide security to the image, encryption is used which convert an image into another non readable form. According to the survey, the comparison from previous technique and proposed algorithms shows that the proposed algorithm is more efficient in terms of performance as compared to previous techniques.

References

[1] S.Fong-In,S. Kiattisin, and Leelasantitham ”A Partial Encryption Scheme Using Absolute-Value Chaotic Map for Secure Electronic Health Records” (JICTEE-2014).
[2] Borko Furht, Daniel Socek, Ahmet M. Eskicioglu “Fundamentals of Multimedia Encryption Techniques”.
[3] Panduranga H T Naveen Kumar S K”Advanced Partial Image Encryption using Two – stage Hill Cipher Technique” International Journal of Computer Applications (December 2012).
[4] Nitumoni Hazarika,Monjul Saikia “A Novel Partial Image Encryption using Chaotic Logistic Map” International conference on Signal Processing and Integrated Networks(SPIN)2014.
[5] Sukalyan Som, Sayani Sen,”A Non-adaptive Partial Encryption of Grayscale Image based on Chaos”, First International Conference on Computational Intelligence: Modelling, Techniques and applications (CIMTA-2013).
[6] Yong-Hong Zhang, “Image encryption using extended chaotic sequences”, IEEE Transactions International Conference on Intelligent Computation Technology and Automation pp. 143-146,2011.
[7] Varsha S. Nemade, R. B.Wagh “Review of different image encryption techniques” National Conference on Emerging Trends in Computer Technology (NCETCT-2012).
[8] J.C. Yen, J.I. Guo, A new chaotic key based design for image encryption and decryption, Proceedings of the IEEE International Symposium Circuits and Systems, vol. 4, 2000, pp. 49–52
[9] A. Gautam, M. Panwar, Dr.P.R Gupta “A New Image Encryption Approach Using Block Based Transformation Algorithm” 2011 (IJAEST) Vol No. 8, Issue No. 1, 090 - 096 .
[10] Daniel J. Costello, Jr. and G. David Forney, Jr“Channel Coding: The Road to Channel Capacity“ IEEE | Vol. 95, No. 6, June 2007.
[11] C.E. Shannon, "Communication Theory of Secrecy System" , Bell Syst. Tech. J. 28, pp. 656-715, 1949.