Vol 2 Issue 9 March 2013

Impact Factor : 0.1870

ISSN No :2231-5063

Monthly Multidisciplinary
Research Journal

Golden Research Thoughts

Chief Editor
Dr.Tukaram Narayan Shinde

Publisher
Mrs.Laxmi Ashok Yakkaldevi

Associate Editor
Dr.Rajani Dalvi

Honorary
Mr.Ashok Yakkaldevi

IMPACT FACTOR : 0.2105

Welcome to ISRJ

RNI MAHMUL/2011/38595 **ISSN No.2230-7850**

Indian Streams Research Journal is a multidisciplinary research journal, published monthly in English, Hindi & Marathi Language. All research papers submitted to the journal will be double - blind peer reviewed referred by members of the editorial Board readers will include investigator in universities, research institutes government and industry with research interest in the general subjects.

International Advisory Board

Editorial Board

Address:-Ashok Yakkaldevi 258/34, Raviwar Peth, Solapur - 413 005 Maharashtra, India
Cell : 9595 359 435, Ph No: 02172372010 Email: ayisrj@yahoo.in Website: www.isrj.net

Golden Research Thoughts
Volume 2, Issue. 9, March. 2013
ISSN:-2231-5063

Available online at www.aygrt.isrj.net

ORIGINAL ARTICLE

SECURE IMAGE DATA BY USING DIFFERENT ENCRYPTION TECHNIQUES A REVIEW

GAYATHRI D.

Department, PIT, Waghodia, Dist.-Vadodara, Gujarat, India.

Abstract:

Information security is an increasingly important problem in the present era of advanced technology, because of which encryption is becoming very important to ensure security. Popular application of multimedia technology and increasing transmission ability of network gradually leads us to acquire information directly and clearly through Images. The digital images, which are transmitted over the internet, must be protected from unauthorized access during storage and transmission for communication, copyright protection and authentication purposes. This can be accomplished using image encryption which is an intelligent hiding of information. In this paper, I survey on existing work which is used different techniques for image encryption and also give the general introduction about cryptography.

KEYWORDS:

Asymmetric key cryptography, Decryption, Encryption, Image encryption, Symmetric key cryptography.

I.INTRODUCTION:

With the ever-increasing growth of multimedia applications, security is an important issue in communication and storage of images, and encryption is one the ways to ensure security. 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. Furthermore, special and reliable security in Storage and transmission of digital images is needed in many applications, such as cable-TV, online personal photograph album, medical imaging systems, military image communications and confidential video conferences, etc. In order to fulfill such a task, many image encryption methods have been proposed.

The image encryption algorithms can be classified into three major groups: (i) position permutation based algorithm [1] (ii) value transformation based algorithm and [2, 3] (iii) visual transformation based algorithm [1]

This paper is organized as follows In Section 1; we present general guide line about cryptography. In Section 2, we survey on already existing research paper. Finally, we conclude in section 3.

Plaintext [4]: An original message is known as plaintext.

Cipher text [4]: Coded message is called cipher text. Encryption or Enciphering [4]: the process from converting plain text to cipher text is called Encryption or Enciphering.

Decryption or Deciphering [4]: Restoring plain text from cipher text is called decryption or Deciphering. Cryptography [4]: The many schemes used for enciphering constitute the area of study known

Source:Golden Research Thoughts [2231-5063]GAYATHRI D.. yr:2013 vol:2 iss:9

as cryptography.

TYPES OF CRYPTOGRAPHY:

There are two main types of cryptography:

secret key cryptography
public key cryptography

Secret key cryptography is also known as symmetric key cryptography. With this type of cryptography, both the sender and the receiver know the same secret code, called the key. Messages are encrypted by the sender using the key and decrypted by the receiver using the same key.

Public key cryptography, also called asymmetric key cryptography, uses a pair of keys for encryption and decryption. With public key cryptography, keys work in pairs of matched public and private keys.

Cryptography technique is used when secret message are transferred from one party to another over a communication line. Cryptography technique needs some algorithm for encryption of data.

Nowadays when more and more sensitive information is stored on computers and transmitted over the Internet, we need to ensure information security and safety. Image is also an important part of our information .Therefore it's very important to protect our image from unauthorized access. There are so many algorithms available to protect image from unauthorized access which is described in next section.

II.LITERATURE SURVEY

A New technique for Image Encryption Using Digital Signature

In this method, the digital signature of the original image is added to the Encoded version of the original image. Image encoding is done by using an appropriate error control code, such as a Bose-Chaudhuri Hochquenghem (BCH) code. At the receiver End, after the image is decrypted, the authenticity of the image is verified using the digital signature. An error control code is used based on the size of the input image, in the encryption technique. The original image is obtained using the specific error control code. The dimension of the image also changes due to the added redundancy which is an additional difficulty to decrypt the image.[25]

A New algorithm for Image encryption using chaotic system

In this proposed scheme a new non linear chaotic algorithm (NCA) is used which has a power function and tangent function instead of linear function. These functions instead of linear function provide much random sequence which provides more security. In this algorithm a one-time-one password system is designed. The structural parameters are calculated. The results show that this proposed algorithm has advantage of large key space and more improved security, with acceptable efficiency.[26]

An Asymmetric Image Encryption Based on Matrix Transformation

In this paper a novel asymmetric block encryption scheme is proposed based on a matrix transformation. This technique can be used to encrypt images with large amount of data. In the proposed algorithm, with the help of matrix transformation pair of key is generated. Then it is encrypted using private key in the transformation domain. At the receiver end, a public key is used by the receiver to decrypt the encrypted images. The results show that it has less computation complexity and better security. [27]

A New Image Encryption Approach using Combinational Permutation Techniques

This paper proposes a new approach for image encryption using a combination of different permutation techniques. The main idea is that an image can be viewed as an arrangement of bits, pixels and blocks. The intelligible information present in an image is due to the correlations among the bits, pixels and blocks in a given arrangement. Security of image encryption is increased by decreasing the correlation among the bits, pixels and blocks using certain permutation techniques. From the results, it is observed that the permutation of bits is effective in reducing the correlation thereby decreasing the perceptual information, whereas the permutation of pixels and blocks are good at producing higher level security compared to bit permutation. This proposed technique is observed to be useful for security applications.[28]

Digital Image Encryption Algorithm Based on Composition of Two Chaotic Logistic Maps

In This paper, an efficient chaos-based stream cipher is proposed which comprises two chaotic logistic maps and a large enough external secret key for image encryption. The initial conditions are derived using the external secret key for the chaotic maps. Then, two chaotic maps are used to provide more security. With this proposed algorithm the relationship between the cipher image and the plain image is not easily understood by any intruder. For mixing the current encryption parameters with previously encrypted data, an encryption algorithm is proposed which uses an iterative cipher module based feedback and data-dependent inputs mechanism. The secret key is then changed after encryption of each pixel of the image, which makes the cipher more robust against any attack. The results show that this is an efficient encryption algorithm for real time.[29]

A novel Image Encryption scheme based on spatial chaos map

In this paper, the traditional chaos process is used for image encryption. In the traditional method binary sequences are used for the image permutation. Chaos sequences are the real valued sequences, so to convert it into binary sequence requires an extra logic operation and then to generate the integer pseudo random number for image permutation is a very time consuming process. [30]

Image Encryption Approach using a block-based transformation

They have proposed an Image Encryption Approach using a block-based transformation on an encrypted image using a famous encryption algorithm called blowfish algorithm. They have used a seed as a key to generate a pseudo random sequence. The image is then divided into number of blocks and using this pseudo random sequence they have transformed the pixel position of the image. Using this technique the correlation among the pixels decreased and entropy increased. [4]

An Image Encryption Approach Using a Combination of Permutation Technique followed by Encryption

They proposed An Image Encryption Approach Using a Combination of Permutation Technique followed by Encryption. This permutation Technique is based on the combination of image Permutation and a popular encryption algorithm called RijnDael. The image is divided into number of blocks, and these blocks are then rearranged into permuted image using an algorithm proposed here, and then the resulting image is encrypted using the RijnDael algorithm. The results showed that the Correlation between image elements was significantly decreased by using the combination technique and higher entropy was achieved. [31]

A Shuffle Image-Encryption Algorithm

In any Image encryption technique, the encrypted image needs to be secure by resisting statistical attacks. In this proposed technique, a new algorithm, called Shuffle Encryption Algorithm (SEA), applies nonlinear s-box byte substitution. Then, a shuffling operation is performed which partially depends on the input data and uses the given key. The statistical analysis is done using histograms, correlation and covariance with which security of encryption algorithm is analyzed. [32]

Image Encryption Using DCT and Stream Cipher

In this paper, Image encryption is done by selecting specific higher frequencies of DCT coefficients which are the characteristic values, and then these DCT coefficients are encrypted. Then, these encrypted blocks are shuffled using a pseudo-random bit sequence. This method reduces the computational requirements for huge volumes of images. In this method fist the image is decomposed into 8x8 blocks, these blocks are transformed from the spatial domain to frequency domain by the DCT. Then, the DCT coefficients of higher frequencies are encrypted using Non-Linear Shift Back Register (stream cipher). The concept behind the technique is that, the image details are situated in the higher frequencies, while the human eye is most sensitive to lower frequencies than to higher frequencies. The proposed algorithm is lossless. The results show that this technique is effective and time complexity is highly reduced. [12]

Image Encryption Using an Enhanced Block Based Transformation Algorithm

They proposed an Enhanced Image encryption algorithm which uses the chaos sequence to permute the blocks of the image. Chaotic systems are sensitive to the initial Condition, and with a Slight variation of initial condition produces a different sequence. In this paper, a new index based chaotic system is proposed. The results are tested on a gray scale Image. The pixel of the image is permuted on the basis of index position of the chaotic sequence and then the blocks of image are permuted using this chaotic sequence by mapping it with index position and encryption is done. The results show that initial conditions are the key to this algorithm and slight variation will lead to a different encrypted image and without which the decryption is not possible. [34]

II.CONCLUSION

In this digital world, 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, I have surveyed existing work on image encryption. I have also given general guide line about cryptography. I conclude that all techniques are useful for real-time image encryption. Techniques describes in this paper that can provide security functions and an overall visual check, which might be suitable in some applications. So no one can access image which transferring on open network.

In general, a well-studied, fast and secure conventional cryptosystem should be chosen, surely those algorithms, which provides higher security.

REFERENCES:

[1] Stallings, W. Cryptography and Network Security.2005. 4th edition, Prentice Hall.

[2] Chinmaya Kumar Nayak, Anuja Kumar Acharya and Satyabrata Das," Image Encryption Using an Enhanced Block Based Transformation Algorithm "International Journal of Research and Reviews in Computer Science (IJRRCS)

[3] Mohammad Ali Bani Younes and Aman Jantan," An Image Encryption Approach Using a Combination of Permutation Technique followed by Encryption", IJCSNS International journal of computer Science, 35:1, IJCS_35_1_03

[4] A. Mitra, , Y V. Subba Rao, and S. R. M. Prasnna, "A new image encryption approach using combinational permutation techniques," Journal of computer Science, vol. 1, no. 1, p.127, 2006

[5] Ismail Amr Ismail, Mohammed Amin, and Hossam Diab2," A Digital Image Encryption Algorithm Based A Composition of Two Chaotic Logistic Maps", International Journal of Network Security, Vol.11, No.1, PP.1{10, July 2010}.

[6] Han Shuihua* and Yang Shuangyuan," An Asymmetric Image Encryption Based on Matrix Transformation" ECTI TRANSACTIONS ON COMPUTER AND INFORMATION TECHNOLOGY VOL.1, NO.2 NOVEMBER 2005

[7] Aloha Sinha, Kehar Singh, "A technique for image encryption using digital signature", Optics Communications, ARTICLE IN PRESS, 2003, 1-6, www.elsevier.com/locate/optcom

[8] Lala Krikor.et.all.," Image Encryption Using DCT and Stream Cipher", European Journal of Scientific Research ISSN 1450-216X Vol.32 No.1 (2009), pp.47- 57 © EuroJournals Publishing, Inc. 2009