RESEARCH ARTICLE OPEN ACCESS

Dynamic Key Exchange Method for Image Encryption

P. Rajesh kannan [1], Dr. Mala [2]
Dept. of Computer Applications
Marudu Pandiyar College
Tamil Nadu – India

ABSTRACT

In recent years, a variety of image encryption scheme has been proposed. A new color image encryption method based on dynamic key exchange is proposed in this paper. For real time image encryption and lesser amount of time. The algorithm lacks of the characteristic of diffusion because each pixel is operated individually and a chosen/known-plaintext attack can break the scheme. The 192-bit-long external secret-key(bigger key space). In the result of several experimental statistical analyses and key sensitivity tests prove the security robustness of the proposed cryptosystem.

Keywords:- Cryptosystem , Bigger Key Space, Encryption

I . INTRODUCTION

Image encryption schemes have been increasingly studied to meet the demand for real-time secure image transmission over the Internet and through wireless networks. Traditional image encryption [5] algorithm such as data encryption standard (DES), has the weakness of low-level efficiency when the image is large. The chaos-based encryption [5,] has suggested a new and efficient way to deal with the intractable problem of fast and highly secure image encryption. After Matthews proposed the chaotic encryption algorithm in 1989, increasing researches of image encryption technology are based on chaotic Systems .Recently there have been many papers on chaotic encryption scheme. Chaotic systems have many important properties, such as the sensitive dependence on initial conditions and system parameters, pseudorandom property, no periodicity and topological transitivity, etc. Most properties meet some requirements such as diffusion and mixing in the sense of cryptography. Therefore, chaotic cryptosystems have more useful and practical applications. One-dimensional chaotic system with the advantages of high-level efficiency and simplicity, such as Logistic map, has been widely used now. But their weakness, such as small key space and weak security, is also disturbing

Cryptography studies how to design good (secure and fast)encryption algorithms, and cryptanalysis tries to find security weaknesses of existing algorithms and studies. An encryption scheme is called a cipher (or a cryptosystem). The encryption and decryption procedure of a cipher is depicted in Figure 1.

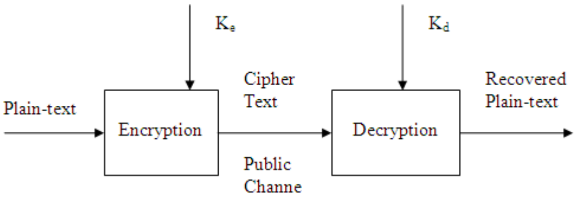


Figure 1. Encryption and Decryption procedure of a Cipher

The message for encryption is called plaintext, and the encrypted message is called cipher-text, which are denoted here by P and C, respectively. The encryption procedure of a cipher can be described as C=Eke(P), where Key is the encryption key and E(.) is the encryption function. Similarly, the decryption procedure is P=Dkd (C), where Kd is the decryption key and D(.) is the decryption function. When Ke=Kd, the cipher is called a private-key cipher or asymmetric cipher For private key ciphers, the encryption-decryption key must be transmitted from the sender to the receiver via a separate secret channel. When Ke=!Kd, cipher is called a public-key cipher or an asymmetric cipher. . For public-key ciphers, the encryption key Ke is published, and the decryption key Kd is kept secret, for which no additional secret channel is needed for key transfer. The cryptosystems can be classified with respect to the structure of encryption algorithm as stream ciphers and block ciphers. Stream cipher is the method in which a key generator produces a bit stream (the Key stream) which plain-text bit stream by simple modulo 2 additions. A stream cipher system thus hides the plain-text bit by changing the bits of it in a random way. An interceptor, who does not know the key, will not know which bits have been changed (corresponding to the occurrence of "1" in the key stream), or which ones remain unchanged ("0" in the key stream). An ideal stream cipher would use a physical (true) random number generator a Key generator. Since its output cannot be reproduced, however, decipherment would be impossible, unless the whole Key stream, with the same length as the plain-text, is transported to the legitimate receiver via a safe channel. This procedure is often impractical. There for mostly so-called pseudo-random number generators with special properties controlled by a relatively short Key have to be used instead as key generators. Unlike the stream ciphers, where only one bit at a time is ciphered, whole blocks of bits are treated simultaneously. In this case the plain-text information is hidden by the fact that, depending on the key, a cipher-text block can be deciphered to any combination of plain-text bits or to as many combinations as the keys. If the keys are chosen with equal probability, then to the interceptor observing a cipher text block, all the possible plain-text blocks are equally likely to have occurred. Cryptography is a permanent field of interest at all time. At present secret communication plays an increasing role in many fields of common life, like banking, industry, commerce, telecommunication etc. Owing to the advance in network technology, information security is an increasingly important problem. Popular application of multimedia technology and increasing transmission ability of network gradually leads to us to acquire information directly and clearly through images. Hence, data security has become a critical and imperative issue. Encryption is such a way that its content can be reconstructed only by a legal recipient. The technology of encryption is called cryptology. Cryptology is the branch of science dealing with the theory of secure communication algorithms. Cryptography is the process of transforming information (plain-text) into unintelligible form (cipher-text) so that it may be sent over insecure channels or it may be stored in insecure files. Cryptographic procedures, can also be used for personal identification, digital signature, access control etc..

II. RELATED WORKS

The chaos-based image cryptosystem mainly consists of two stages [2]. The plain image is given at its input. There are two stages in the chaos- based image cryptosystem. The confusion stage is the pixel permutation where the position of the pixels is scrambled over the entire image without disturbing the value of the pixels and the image becomes unrecognizable. The pixel permutation is carried out by a chaotic system [1,2]. The chaotic behavior is controlled by the initial conditions and control parameters which are derived from the 16-character key. To improve the security, the second stage of the encryption process aims at changing the value of each pixel in the whole image an important tool to protect image from attackers. The basic idea of encryption is to modify the message in In the diffusion stage, the pixel values are modified sequentially by the sequence generated from one of the three chaotic systems selected by external key. The whole confusion-diffusion round repeats for a number of times to achieve a satisfactory level of security. The randomness property inherent in chaotic maps makes it more suitable for image encryption.

III. ARCHITECTURE OF AN CHAOS BASED IMAGE CRYPTOSYSTEM

The chaos-based image cryptosystem mainly consists of two stages. The plain image is given at its input. The typical architecture of the chaos-based image cryptosystems is depicted in Figure 2. There are two stages in the chaos based image cryptosystem The confusion stage is the pixel permutation where the position of the pixels is scrambled over the entire image without disturbing the value of the pixels and the image becomes unrecognizable.

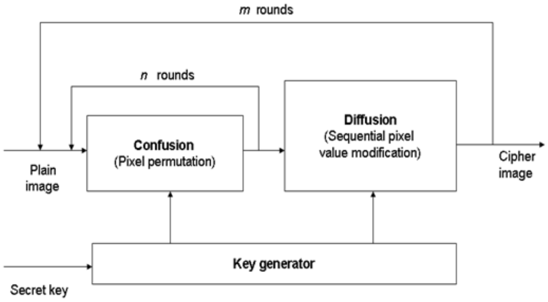


Figure 2. Architecture of proposed Chaos-based image cryptosystem

Therefore these initial conditions and control parameters serve as the secret key. It is not very secure to have only the permutation stage since it may be broken by any attack. To improve the security, the second stage of the encryption process aims at changing the value of each pixel in the whole image. The process of diffusion is also carried out through a chaotic map which is mainly dependent on the initial conditions and control parameters. In the diffusion stage, the pixel values are modified sequentially by the sequence generated from one of the three chaotic systems selected by external key. The whole confusion-diffusion round repeats for a number of times to achieve a satisfactory level of security. The randomness property inherent in chaotic maps makes it more suitable for image encryption.

IV. PROPOSED CRYPTOSYSTEM

A. *Encryption System*

The proposed scheme is Different Chaotic systems are employed in confusion and diffusion stages. Also complex chaotic maps are chosen rather than the simple ones to further enhance the complexity of the algorithm and thereby improving the security. The input to the cryptosystem is the plain image which is to be encrypted. Architecture of proposed Chaos-based image cryptosystem. The first stage is the confusion stage and the second one is the diffusion stage. Among the three chaotic dynamic systems namely Lorenz, Chen and LU one is selected by the system parameter which is obtained from the key and it is applied to the digital color image encryption because of higher secrecy of high-dimension chaotic system. The second step of the encryption process is to encrypt the shuffled image by changing its pixel values based on one of the three high-dimensional chaotic systems (Lorenz, hen and LU) . This is referred to as the diffusion stage. The initial conditions and the control parameters used to generate the chaos sequence in both the stages serve as the secret key in the two stages. The resulting image is the Cipher image. Separate key is used for permutation and diffusion stages of the encryption process to improve security of the algorithm

B. Decryption System

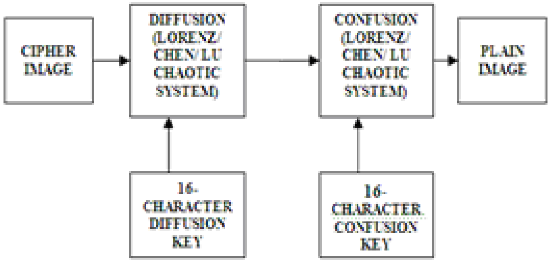

CIPHER IMAGE
DIFFUSION (LORENZ/ CHEN/ LU CHAOTIC SYSTEM)
CONFUSION (LORENZ/ CHEN/ LU CHAOTIC SYSTEM)
PLAIN IMAGE
16-CHARACTER DIFFUSION KEY
16-CHARACTER CONFUSION KEY

Figure 3. Chaos based Decryption system The decryption system is illustrated in the Figure 3. The First stage in the decryption process is the diffused imaged encryption stage. In the encryption process, the pixel value diffusion was carried out with any one of the three chaotic systems. Therefore, in the decryption process to retrieve the original pixel values, again any one of the chaotic system (Lorenz, Chen, Lu) is employed in the first stage of decryption. The first stage of decryption process uses the three dimensional sequence generated by any one of the chaotic system .It is a kind of high-dimensional maps and complex enough the initial conditions that were used in the encryption process should be used here and this serves as the decryption key for the first stage. Second, in the encryption process, the pixel position permutation was carried out with any one of the chaotic system. The initial conditions and control parameters for generating the chaos-sequence were used as the confusion key. Therefore in the decryption process, the same chaotic systems with same confusion key are used to get the original position of the image. The output of the decryption system gives the original image.

V. RESULTS AND DISCUSSION

The proposed image encryption system uses any one of the chaotic system for pixel position permutation and one of the same chaotic system for pixel value modification. Color Lena image of size 256 × 256 was taken as the test image. In Pixel position permutation stage, the Lorenz, Chen and Lu chaotic systems are used. The original image taken for the work is given in Figure 5.

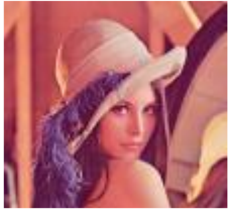


Figure 5. Original image

The decryption for the encrypted image was carried out. The decrypted image after the first stage by un diffusion.

And this will serve as the input image for the second stage of decryption.

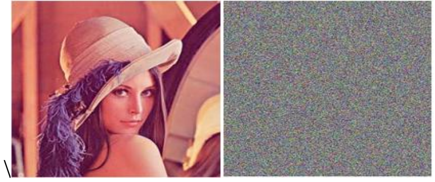
\ 

Figure 6, Encryption image

VI. SECURITY ANALYSIS

To test the robustness of the proposed scheme, security analysis was performed. Key space analysis, statistical analysis and sensitivity analysis were carried out to demonstrate the satisfactory security of the new scheme. The image-histogram illustrates how pixels in an image are distributed by graphing the number of pixels at each color intensity level. It is observed that the histogram of the original image Therefore, the diffusion function is carried out. The histogram of the final encrypted image is fairly uniform and is significantly different from that of the original image.

In addition to the histogram analysis the correlation between two vertically adjacent pixels, two horizontally adjacent pixels and two diagonally adjacent pixels in plain Image/cipher image are analyzed respectively. The correlation coefficient analysis pixels in the cipher image. In the new scheme the correlation among adjacent pixels is lower than that of the original image.

A. Sensitivity Analysis

An ideal image encryption procedure should be sensitive with respect to secret key. The change of a single bit in the secret key should produce a completely different encrypted image. To prove the robustness of the proposed scheme, sensitivity analysis with respect to key is performed. High key sensitivity is required by secure image cryptosystems, which means the cipher image cannot be decrypted correctly even if there is only a small difference between the encryption and decryption keys. For testing the key sensitivity the following test is performed. blue component

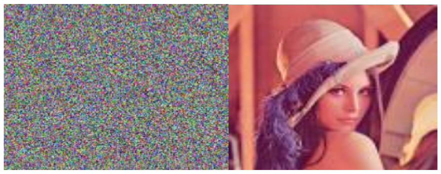


Figure 7. decrypted Image

This demonstrates the high key sensitivity of the new encryption scheme. This guarantees the security of the proposed scheme against brute-force attacks to some extent

VII. FUTURE ENHANCEMENT

Currently the chaos-based scheme was designed for still images. The chaos-based image encryption scheme can be applied to moving images as well. The prevalence of multimedia technology in the society has promoted digital images and videos to play a more significant role than the traditional texts, which demands a serious protection of users' privacy. To fulfill such security and privacy needs in various applications, encryption of images and videos is very important to frustrate malicious attacks from unauthorized parties. Hence in the second phase of the paper, it is purposed to design a chaos-based image encryption scheme for moving images (videos).

VIII. CONCLUSION

The new image encryption scheme was designed. Dynamic Key Exchange system key space is increased. Repeated permutations are avoided but pixel values are changed by the diffusion function. By incorporating all these features, the proposed cryptosystem avoids all the crypto graphical Weaknesses. Number of security analysis were carried out on the new algorithm and simulation results show that encryption and decryption are good and the algorithm has good security and robustness.

REFERENCES

[1] Design and Implementation of Image Encryption Algorithm Using Chaos Sandhya Rani M.H.1, K.L. Sudha International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970) Volume-4 Number-2 Issue-15 June-2014 660

[2] Image Encryption using Elliptic Curve Cryptography Laiphrakpam Dolendro Singh∗ and Khumanthem Manglem Singh National Institute of Technology, Manipur 795 001, India Eleventh International Multi-Conference on Information Processing-2015 (IMCIP-2015)

[3] A New Fast and Simple Image Encryption Algorithm Using Scan Patterns and XOR.

[4] Reza Moradi Rad, Abdolrahman Attar, and Reza Ebrahimi Atani Department of Computer Engineering, University of Guilan,Rasht, Iran reza.moradirad@gmail.com, a.attar.q@gmail.com, rebrahimi@guilan.ac.ir International Journal of Signal Processing, Image Processing and Pattern Recognition Vol.6, No.5 (2013), pp.275-290 ISSN: 2005-4254 IJSIP Copyright 2013 SERSC

[5] dongming chen, youpong change "a novel Image encryption Algorithm based on logistic maps". Advanced in Information science and service , volume 3,number7, Augest 2011.

[6] Sapna sasi daran and Deppu sleeba Philip "A Fast partial image Encryption Scheme with Wavelet Transform and RC4"

international journal of advanced in Engineering and technology,sept2011.

[7] Shujun li and xuan zheng “on the security of an Image encryption Method. IEEE international conference on Image processing(ICID2002) vol.Zpp.925.928.2002,IEEE

[8] K.Smarty&R.tamilselvi “Comparison of Encryption levels for Image Security using various Transforms” International conference on information on information and Network Tecnology”2011, Singapore.

[9] Seyyed Mohammed Reza Farshchi&Iman Dehghon Ebrahimi “A novel Encryption Algorithm for Transmitting Secure Data based on Generic Hyper chose Map”,2011. International Confance on computer Communication and Management Singapore.

[10] Encryption -Compression Method of Images. IADIS, International Journal on Computer Science and Information systems vol.4,no.1, pp.30-41.

[11] NPCR and UACI Randomness Tests for Image Encryption JSST April Edition 2011.

[12] Rajneesh Kumar and umesh Chandra Jaiwal “Experimental Investigation of Image encryption Technique using Public key” Int.j.tech Jan-june 2011.

[13] C-Jimanez, C.Torres “Fractional Hartley Transform applied to Optional Image Encryption” published on IOP conference 279(2016)012041.

[14] (G.K.Haung, C.W.Liao”Implimentation of gray image Encryption by single chaotic system” Telecommunication System, June2016.