www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 04 Issue 12 Dec 2015 Page No. 15117-15118

A Study on Chaos-Based System for Improved Encryption of Images

Kukoo Anna Mathew
M.Tech, Mahatma Gandhi University, Kerala
kukooanna90@gmail.com

Abstract:

In modern world, encryption technology has been developed rapidly the chaos based cryptographic algorithms. Chaos based cryptographic recommend a variety of features over the traditional encryption algorithms such as high security, speed, and prudent computational overheads and power. Chaos theory studies the performance of dynamical systems that are enormously sensitive to initial conditions, which means that a small change in the initial state can be lead to a big diverse action in the final state. This paper presents a study on chaos based system for improved encryption of images using RSA public key cryptography.

Keywords: Chaos-based cryptography, Chaos System, Confusion, Diffusion, Decryption, Encryption, Public key cryptography.

1. Introduction

The term cryptography is used with the encryption of visual information. It is considered necessary to protect the exposure of confidential or personal information particularly in a scheme where the information is transferred through the open or insecure channel. The chaotic cryptography techniques are generally made by combination of two operations called permutation/ Shuffling and diffusion. Both these operations are repeatedly performed till the sufficient encryption level is achieved. The worth of encryption is tested by its capacity to preserve different attacks like known plaintext attack, cipher text only attack, statistical attack, deferential attack, and brute-force attack. The defending potential from each attack depends upon definite properties of the selected map and its configuration parameters. The process diffusion means spreading out the influence of a single plaintext digit over many cipher text digits, so that the statistical structure of the plaintext becomes indistinct. Yaobin Mao and Guanrong Chen [1], an XOR plus modulo (mod) function is inserted to each pixel in between every two adjacent rounds of the map used. In their scheme the one dimensional logistic map is used for generating the diffusion template. Another approach based on W7 stream cipher is projected by Alireza Jolfaei, Abdolrasoul Mirghadri [2].The process confusion, on the other hand, means using transformations that complicate the dependence of the statistics of the cipher text on the statistics of the plaintext. In paper [2] the Hanon map based shuffling approach is used. The Henon map is a prototypical 2D invertible iterated map represented by the state equations with a chaotic attractor and is a simplified model of the Poincare map for the Lorenz equation proposed by Henon in 1976. A good image encryption algorithm ought to be sensitive to the cipher key, and the key space should be large enough to make brute-force attacks infeasible. Here in this paper it suggests public key encryption method. It is computationally straightforward for a user to create their public and private key-pair and to use them for encryption and decryption. The potency lies in the fact that it is impractical (computationally infeasible) for a properly generated private key to be determined from its subsequent public key. As a consequence the public key may be published without compromising security, while the private key must not be exposed to anyone not endorsed to read messages or perform digital signatures. Public key algorithms, unlike symmetric key algorithms, do not require a safe and sound initial exchange of one (or more) secret keys between the parties [3].

2. Proposed System

Select an image which is a color image and where the pixels are represented using minimum 24 pixels. The pixels should be represented in the RGB model. A standard chaotic map will be generated, when the keys have been entered by the user in any form. The chaotic map which is generated by means of Mathematical equations and theory is entirely reversible, capable enough to produce diffusion on the whole image pixels and the computation time is less. The chaotic map formed is then used for diffusing the image pixels. The image obtained from this chaos is absolutely distorted and the output is not identifiable by the end user. So as to provide chaos to rectangular images an approach known as sliding window approach is used. In this method a fixed square window is run on the image and all the pixels within the series of the window is shuffled [4]. The window is then shifted by one column to produce diffusion on more part of the image.

3. Key Generation

The public key cryptography algorithms are those which have two independent keys, one is a public key P_u is used to encrypt the message and the other is a private key P_v which is used to decrypt the message. Despite the fact that the key P_u which was used to encrypt the message is the public and is believed to be known to all, decoding the message using that key or

recovering the private decoding key P_v out of the public key P_u can't happen [3]. The foremost benefit of using the public key encryption is that they keep away from the need of sharing any shared key between the transmitter and the receiver through a secure channel. In a shared key encryption system the transmission of a private key through a secure channel can cause complete danger to the encryption process. For certain applications the transmission of a shared key using a secure channel is speculative [3].

4. RSA Algorithm

The RSA cryptosystem, is named after its inventors R. Rivest, A. Shamir, and L. Adleman. It is the most commonly used public key Cryptosystem. It is used to provide both secrecy and digital signatures. Also its security is based on the intractability of the integer factorization. The RSA algorithm involves three steps: Key generation, Encryption and Decryption [5].

4.1 Key Generation

RSA uses a public key and a private key. The public key will be known to everyone and this public key is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a realistic amount of time by means of the private key. The keys for the RSA algorithm are generated in the following way:

To generate the two keys, first choose two random large prime numbers i and j. For greatest security, choose i and j of equal length. Calculate the product

$$K = I * J \quad (1)$$

Then arbitrarily choose the encryption key e such that e and (i −1) (j −1) are relatively prime. Finally, apply the extended Euclidean algorithm to figure the decryption key d such that

$$d = e^{-1} \bmod((i-1)*(j-1)) \quad (2)$$

Note that d and n are also relatively prime. The numbers e and K are the public key; the number d is the private key. The two primes i and j are no longer needed. They should be discarded, but never exposed [6].

4.2 Encryption

At first receiver transmits his/her public key (n, e) to sender and keep the private key as a secret. If the sender desires to send message M to receiver, then the sender changes the message M into integer m, such that $0 \leq m<n$. Then the sender computes the cipher text c equivalent to

$$c \equiv m^e \pmod{n} \quad (3)$$

4.3 Decryption

The receiver can recuperate m from c by via his/her private key exponent d by computing

$$m \equiv c^d \pmod{n} \quad (4)$$

5. Assumptions

The main assumption in this algorithm is that the image is represented using jpeg or gif format. All the pixels are 8 bit values. The images should be represented using RGB color model [7].

6. Conclusion

There are definite elements of chaos theory that make it hypothetically applicable to cryptography. For this reason, there has been considerable research done in chaos-based cryptosystems. The chaos based public key cryptosystem is a good idea of building very complicated asymmetric cryptosystem, which has been faster and security than traditional asymmetric encryption schemes. Also in RSA the plaintext is mixed along with Chaos sequence and then applied for encryption and decryption process. It is therefore observed that RSA with chaos take less time to execute and is more secure.

References

1. Yaobin Mao and Guanrong Chen "A Novel Fast Image Encryption Scheme Based on 3d Chaotic Baker Maps" International Journal Of Bifurcation and Chaos, Vol. 14, No. 10 (2004) 3613–3624
2. Alireza Jolfaei,Abdolrasoul Mirghadri "An Image Encryption Approach Using Chaos And Stream Cipher" Journal of Theoretical And Applied Information Technology 2010
3. Jaydip Sen, ―Theory and Practice of Cryptography and Network Security Protocols and Technologies‖, InTech, 2013.
4. Zhang, G. J., Liu, Q. "A Novel Image Encryption Method Based on Total Shuffling scheme" Optics Communications,284, pp. 2775--2780 (2011)
5. R.L. Rivest, A. Shamir, and L. Adleman," A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,"
6. William Stalling," Cryptography and Network Security: Principles and Practice", 3rd Edition, Prentice Hall, 2003.
7. Deep Desai, Appoorv Prasad, Jackson Crasto," Chaos-Based System for Image Encryption," International Journal of Computer Science and Information Technologies, Vol. 3 (4), 2012,4809-4811

Author Profile

Kukoo Anna Mathew received B.Tech degree in Computer Science & Engineering from Rajagiri School of Engineering and Technology in 2011 and M.Tech degree from Viswajyothi College of Engineering and Technology in 2014, respectively. During 2014 -2015, she worked as Assistant Professor on Contract in Computer Science Department of Mar Athanasius College of Engineering, under Mahatma Gandhi University, Kerala. Her interests focus on the area of cryptography.