International Journal of Communication Networks and Security

Volume 1 | Issue 4 Article 17

April 2012

AN EFFICIENT CHAOS-BASED OPTIMIZATION ALGORITHM APPROACH FOR CRYPTOGRAPHY

RASHI VOHRA
Shri Ram Institute of Technology, Jabalpur (M.P.), gaurav.rashi@gmail.com

BRAJESH PATEL
Shri Ram Institute of Technology, Jabalpur (M.P.), BRAJESH@gmail.com

AN EFFICIENT CHAOS-BASED OPTIMIZATION ALGORITHM APPROACH FOR CRYPTOGRAPHY

RASHI VOHRA[1], BRAJESH PATEL[2]

[1,2]Shri Ram Institute of Technology, Jabalpur (M.P.)
[1]Email: gaurav.rashi@gmail.com

Abstract: The utmost negative impact of advancement of technology is an exponential increase in security threats, due to which tremendous demand for effective electronic security is increasing importantly. The principles of any security mechanism are confidentiality, authentication, integrity, non-repudiation, access control and availability. Cryptography is an essential aspect for secure communications. Many chaotic cryptosystem has been developed, as a result of the interesting relationship between the two field chaos and cryptography phenomenological behavior. In this paper, an overview of cryptography, optimization algorithm and chaos theory is provided and a novel approach for encryption and decryption based on chaos and optimization algorithms is discussed. In this article, the basic idea is to encrypt and decrypt the information using the concept of genetic algorithm with the pseudorandom sequence further used as a key in genetic algorithm operation for encryption: which is generated by application of chaotic map. This attempt result in good desirable cryptographic properties as a change in key will produce undesired result in receiver side. The suggested approach complements standard, algorithmic procedures, providing security solutions with novel features.

Keywords*: Cryptography, genetic algorithm, chaos theory, chaotic map, PRNG.*

.

1. INTRODUCTION

In this information age, due to widespread computerization and their interconnection via network, information security has become the most fascinating and interesting technology field in today's world. Information security is a process of safeguarding information against intentional and malicious attacks to ensure its CIA triad [1] [2]. The CIA triad stands for three major tenets to information security: confidentiality, integrity and availability.

Confidentiality prevents un-authorized disclosure of sensitive information. Integrity prevents unauthorized modification of information thereby assuring the accuracy of information. Availability ensures that the information is available for use when it is needed by preventing loss of access to information.

The outline of the paper is as follows:

Section 2; provide a gentle and interesting introduction to cryptography and highlights important concepts of cryptography. In recent year most of the researches on cryptography are based on genetic algorithm, it is useful to have a basic grasp of the concept of genetic algorithm. Section 3; provide an overview of genetic algorithm, operators in genetic programming and example to clarify the concept. The most important development in recent year in cryptography is the adoption of chaos theory, section 4 provides introduction of chaos theory, concepts of chaos theory. This will also cover a thorough discussion on the relation between the chaos and cryptography and generation of pseudo random sequences using chaotic map, further used as a key for encryption and decryption process. In section 5, a new approach of cryptography based on genetic algorithms (GA) with pseudorandom sequence generated by use of chaotic map, to encrypt data stream is proposed. In Section 6; we draw the conclusions and some discussions about future work. Finally, in section 7 we point out the references.

2. CRYPTOGRAPHY

Over the last few decades, the internet grew dramatically leading to a heightened awareness of the need to protect data and resources from disclosure, to guarantee the authenticity of information and to protect system from security based attacks. From thousand of years Cryptography play a central role in information security and is becoming increasingly important as a building block for information security [3] [4]. It has long been used by militaries and governments to facilitate secret communication. Cryptography is a study of design of technique to provide secret communication as it protects the information transmission from the influence of adversaries who may present a threat to information CIA triad and those who involve in such an art are called cryptographers.

Cryptography is composed of two process encryption and decryption, performed by using a set of codes, termed as cipher. Cryptography synonymous with encryption, deals with transformation of user information (plaintext) into an unintelligible gibberish (cipher text) that make it unusable by anyone other than an authorized entity and protect it from unauthorized or accidential disclosure while information is in transit and in storage. [5] [6].The

plaintext can be restored from the cipher text by the process decryption, opposite of encryption. The security offered by cryptographic-based systems depends on both the strength of the cryptographic algorithms chosen for encryption /decryption and the strength of the keys used with those algorithms.

Cryptosystems individualize on the basis of: Type of operations used - Substitution/Transposition, Way in which plaintext is processed - Block/Stream, Number of keys used - Symmetric / Asymmetric. Objective of cryptography:
1. Confidentiality: It is a service which is used to protect identifiable information from forced disclosure to avoid a malicious use of them.

2. Data integrity: Integrity means no data modification, providing an assurance that information can only be accessed or modified by those authorized to do so.

3. Authentication: Authentication gives the ability to know the identity of a user, without saying anything about the access rights of the individual.

4. Non-repudiation: As per non-repudiation neither sender nor the recipient can deny later from sending or receiving the message respectively. It can be viewed as an extension to the identification and authentication service.

The Principal categories of cryptographic algorithms are: private-key cryptography, public-key cryptography and Cryptographic hash functions. Public-key cryptography is sometimes referred to as secret key cryptography or symmetric cryptography because a single key is shared between sender and receiver (key distribution) for enciphering and deciphering by keeping the key secret. The security of the algorithm depends upon how well the key is protected and on the number of bits of the key. For the secret key cryptosystem, with the plaintext X and encryption key K as input in encryption algorithm E. The system can be described as: Y=EK(X) where Y is the ciphertext. The notation for deciphering will be X=DK(Y) where D is the decryption algorithm and Y, K are the input to D.

Some popular encryption algorithms developed using this symmetric cryptography includes DES, 3DES, AES, and RC4. The DES was published by the NIST and is based on Feistel-network version of Lucifer. It takes plaintext (64-bit) and key (56-bit) as input. The plaintext is first passed through initial permutation, followed by 16 round of function (composed of both permutation and substitution function), then swapping is performed between the two half of the output so far generated, the pre-output is then passed through a permutation (inverse of initial permutation function), finally producing ciphertext (64-bit). The decryption algorithm proceeded as encryption algorithm, except with the application of the sub-keys is reversed. With the key length of 56 bits, DES is vulnerable to brute force attack.

To overcome the vulnerability to brute force attack, 3DES is issued by NIST in 1999. The principal drawback of 3des is the algorithm is relatively sluggish in software, slower (having 3 times rounds as des), use of 64-bit block size. To replace 3des so as to support block length of 128 bits and key length of 128,192, and 256 bits, AES is published in November 2001 by NIST. In AES, 4 stages are used in each round, one of permutation (shiftrows) and three for substitution (substitute bytes, mix columns, add round key).

The essence of public key cryptography was introduced by Diffie and Hellman in 1976, which eliminate the use of key distribution process. It is more efficient then secret key encryption for concealing the sensitive information. It is also referred as asymmetric cryptography as it uses two different key for encryption and decryption process. The sender locks the data i.e. Encrypt the data by using the public key (known to everyone), whereas the receiver unlock the data i.e. decrypt it to plaintext form by using another key termed as private key (known only to the owner of the key).

The most popular public key cryptosystem is RSA, first published in 1978 and is based on the concept of IFD, which is finding the prime factor of very large integer. It is the most predominant algorithm used today for public-key cryptography. Diffie and Hellman issued by NIST uses the concept of DLP to provide authentication mechanism. Elliptic Curve Cryptography was proposed by cryptographers Victor Miller (IBM) and Neal Koblitz (University of Washington) in 1985, is based on the difficulty of solving the Elliptic Curve Discrete Logarithm Problem (ECDLP). Given two points, P and Q, on an elliptic curve, find the integer n, if it exists, such that p= nQ. It combines the concept of number theory and algebraic geometry

Symmetric encryption algorithms is normally used to encrypt private data for its extremely fast, and low complexity, whereas asymmetric encryption imposes a high computational burden, and tends to be much slower and often used for digital signature and key distribution.

Cryptographic hash functions also known as message digests, because it condenses a message into an irreversible fixed-length hash value. It is a form of

cryptographic security but differ from encryption process. Encryption process completes in two stages: first is to encrypt the data and second is to decrypt the data on the other hand, hash function is used to generate a short fixed length random string from the original message, often used for checking the integrity of the message. Hash function is commonly used to encrypt password in many operating system. It is also termed as a one way function because the original text cannot be recovered from the hash value. Hashing algorithm is generally used for error checking without the use of any secret key

3. GENETIC ALGORITHM

In 1960s, I. Rechenberg introduced the concept of evolutionary computation. The genetic algorithm belongs to the family of evolutionary computing as a useful tool for search optimization problems, along with genetic programming, evolution strategies, and evolutionary programming. The genetic algorithm is an adaptive heuristic search algorithm derived from the concept of natural selection and natural genetics. The word “genetics” is derived from the Greek word “genesis” meaning “to grow”. It is the branch of science that differentiates between heredity and variations and account for the resemblances and differences during the process of evolution.

GA handles a population of individuals where each individual represents a possible solution and is represented by a chromosome. The chromosomes can be encoded using bits, numbers, trees, lists, or any other objects, depending upon the type of problem to be solved. Each chromosome is associated with fitness value which corresponds to an evaluation of how good the individual is.

The GA loops over an iteration process containing the stages of selection, reproduction, evaluation and replacement. The algorithm is stopped when the population converges toward the optimal solution. The iteration stops under the various conditions such as maximum generations has evolved, specified time has elapsed, when there is no change in fitness value for a specified number of generations, due to stall generations and stall time limits. The termination stage finally brings the process to a halt [7].

The basic operators in genetic algorithm for performing it operations are: encoding, selection, and recombination and mutation operator. Encoding is process of representing chromosomes. It may be binary, octal, hexadecimal, permutation, value or tree representation. Selection is a process of choosing two individuals from the population to create an offspring for the next generation on the basis of their fitness value.

Higher the fitness value, higher will be the chance of better chromosomes selection. The population fitness over successive generation get improved by the GA selection pressure, as higher the selection pressure, greater will be chance of getting better individual to be favored for reproduction. Recombination also termed as crossover, is a process of producing offspring from the previously selected individuals. It makes clone of good strings but does not create the new ones.

Various crossover techniques are: single-point crossover, two-point crossover, multi-point crossover, uniform crossover, three-parent crossover etc. After crossover, generated offspring’s are subjected to mutation, which prevents the algorithm from being trapped in local minimum and maintain diversity in the population.

The advantages of GA are: parallelism, liability, wider solution space, complexity in the fitness landscape, and easy discovery of global optimum. It encounters some limitation too, they are: the problem to identifying the fitness function, computational time, definition of representation of the problem and occurrence of premature convergence.

4. CHAOS THEORY

Chaos theory is a branch in mathematics applications in various disciplines such as physics, engineering, economics, biology and philosophy. In common usage, “chaos" means “A condition or place of great disorder or confusion”. Chaos theory studies the behavior of systems that follow deterministic laws but appear random and unpredictable or we can say a dynamical system that has a sensitive dependence on its initial conditions; small changes in those conditions can lead to quite different outcomes [10]. This dependency of a dynamical system on its initial condition is popularly referred to as the butterfly effect. One example of chaotic behavior is the flow of air in conditions of turbulence.

"Chaos is a name for any order that produces confusion in our minds" [George Santayana Dominations and Powers]

A dynamical system must satisfy following chaotic properties, to be referred as chaotic:

1. it must be sensitive to initial conditions;
2. it must be topologically mixing; and
   Its periodic orbits must be dense

In mathematics, a chaotic map is a map that exhibits some sort of chaotic behavior. Chaotic Maps may be classified by a discrete-time or a continuous-time parameter. Discrete maps usually take the form of iterated functions. The Hénon map is a discrete-

time dynamical system, takes a point (x_n, y_n) in the plane and maps it to a new point. There are at least two maps known as the Hénon map.

The first is the two-dimensional dissipative quadratic map given by the coupled equations:

$$x_{n+1} = 1 - \alpha x_n + y_n$$
$$y_{n+1} = \beta x_n$$

(Hénon 1976).

It depends on two parameters, a and b, which for values of a = 1.4 and b = 0.3 act as canonical Hénon map and is chaotic in nature. For other values it may be chaotic, intermittent, or converge to a periodic orbit. Unlike the logistic map, the canonical Hénon map is interesting because, its orbits defy a simple description [11].

They are potential candidate for making a pseudorandom number generator because of their random like, unpredictable dynamics, inherent determinism and simplicity of realization property [11].

A second Hénon map is the quadratic area-preserving map

$$x_{n+1} = x_n \cos\alpha - (y_n - x^2_n) \sin\alpha$$
$$y_{n+1} = x_n \sin\alpha + (y_n - x_n) \cos\alpha$$

(Hénon 1969), which is one of the simplest two-dimensional invertible maps.

5. THE PROPOSED METHOD

The working of the proposed approach of encryption is illustrated in the above block diagram. It consists of pseudorandom sequence generator, crossover operator, and encryption and decryption modules [12] [13]. The pseudorandom number generated will be used as a crossover point, to perform the crossover operator in the message to be encrypted.

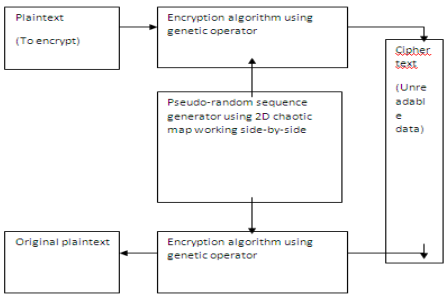

Figure: Block diagram of the proposed method.

The Encryption Process:

The encrypting process emulates the working of the crossover operator using pseudorandom sequence. The steps for the data encryption as follows:

1. Generate the pseudorandom binary sequence using the chaos as Y_n.
2. Convert the binary pseudorandom sequence into decimal pseudorandom sequence ranging from 0 to 7 as Z_n.
3. Read 16 consecutive bytes from the data file as $A_0 \ldots A_{15}$.
4. Initialize i=0.
5. Modify the consecutive bytes by using bytes substitution method for creating confusion, as per as standard.
6. do
7. Take two consecutive bytes of the data stream as A_i and A_{i+1}.
8. Perform the crossover on two consecutive bytes of the data stream as B_i and B_{i+1} by using the number Z_i.
9. Encrypt data as C_i and C_{i+1}, where
   $X_i = Z_i \oplus (Z_i \lll 4)$
   $X_{i+1} = Z_{i+1} \oplus (Z_{i+1} \lll 4)$
   $C_1 = B_1 \otimes X_i$
   $C_2 = B_2 \otimes X_{i+1}$
10. i = i+2.
11. Repeat steps 7 to 10 while i < 16.
12. Again perform the byte substitution over the encrypted 16 consecutive bytes for further creating confusion.
13. Repeat steps 3 to 12 until end of the data in the file.

The Decryption Process

The decryption process will work just opposite of encryption. First, generate the pseudorandom number using chaos and then use that pseudorandom sequence to decrypt the cipher text.

6. CONCLUSION & FUTURE WORK

With the increase in vulnerability to adversary attacks in the transmission of data every year, information security has taken center stage in today's world. In this article, various data encryption mechanism using the concept of genetic algorithm and chaotic map are surveyed, and some existed problem is also discussed [9]. A novel encryption approach has been presented to solve these problems. The use of genetic algorithm along with the randomness property of chaos theory resulted in highly reliable and safe approach from the dangerous clutches of message hackers for data encryption [8] [12].

Another interpretation of the discussion is that the proposed encryption scheme can be a potential candidature for encryption, as the presented approach increases the key size, thus making the proposed encryption process immune of brute force,

known/chosen plaintext, differential and statistical attack [14].

Following are the open subject for future work:

- Adding some extra features to enhance its performance.
- Hardware realization for this concept is concerned that can be further used for highly secure data transmission application.
- Comparative study of other chaotic map performance using the same proposed process.
- More detail study of security analysis of the proposed scheme.
- Determining possible cryptanalysis techniques for this chaos and genetic algorithm based cryptography scheme.

REFERENCES

[1] http://www.mhprofessional.com/downloads/products/0072254238/0072254238_ch01.pdf

[2] Kinamik, "the CIA triad: have you thought about integrity", © kinamik data integrity, 2007.

[3] http://www.garykessler.net/library/crypto.html

[4] http://en.wikipedia.org/wiki/Cryptography

[5] https://class.coursera.org/crypto/lecture/preview

[6] http://www.udacity.com/overview/Course/cs387/CourseRev/apr2012

[7] http://www.scribd.com/doc/31235552/Genetic-Algorithm-Implementation-Using-Matlab

[8] A. Kumar, M. K. Ghose, "Overview of Information Security Using Genetic Algorithm and Chaos", Information Security Journal: A Global Perspective, 18:306–315, 2009.

[9] V. Patidar, K. K. Sud, N. K. Pareek, "A Pseudo Random Bit Generator Based on Chaotic Logistic Map and its Statistical Testing", Informatica 33, pp. 441–452, 2009.

[10] J.M. Amigo, L. Kocarev, J. Szczepanski," Theory and practice of chaotic cryptography", Physics Letters A 366, pp. 211–216, 2007.

[11] S. MADHEKAR, "Cryptographic Pseudo-Random Sequences from the Chaotic Henon Map", Sadhan ¯ a¯ Volume 34, Part 5, pp. 689–701, October 2009.

[12] R. A. Joshi, S. S. Joshi, G. P. Bhole, "Improved Image Encryption Algorithm using Chaotic Map", International Journal of Computer Applications (0975 – 8887), Volume 32– No.9, October 2011.

[13] L. Shujuna, M. Xuanqinb, C. Yuanlongc, "Pseudo-Random Bit Generator Based on Couple Chaotic Systems and its Applications in Stream-Cipher Cryptography", Progress in Cryptology - INDOCRYPT 2001, LNCS, Volume 2247, pp. 316-329, Springer-Verlag, Berlin, 2001.

[14] F. Zheng, X. Tian, J. Song, X. Li, " Pseudo-Random Sequence Generator Based on the Generalized Henon Map", The Journal of China Universities of Posts and Telecommunications, Volume 15, Issue 3, Pages 64–68, September 2008.