Binary Journal of Data Mining & Networking 4 (2014) 37-40

http://www.arjournals.org/index.php/bjdmn/index

Research Article

ISSN: 2229 -7170

Genetic Algorithms: A Technique For Cryptography Real Time Data Transmission

Prempratap Singh[1], Gouri Gosawi[1], Sulakshana Dubey[1]

*Corresponding author:

Prempratap Singh

[1]CSE department ,
Unique College Bhopal

Abstract

The growing adoption of Internet for business applications has exposed users to unwanted risks and attacks. Now more than ever, we find individuals/corporate houses exchanging critical information over the Internet. However, a lack of security infrastructure makes this information exchange vulnerable to outside intervention. To meet these challenges, businesses are opting for modern security measures, such as e-security. E-security measures are designed to preserve the confidentiality and integrity of the users' data on the Internet.We introduce a new approach for e-security applications using the concept of genetic algorithms with pseudorandom sequence to encrypt and decrypt data stream. The feature of such an approach includes high data security and high feasibility for easy integration with commercial multimedia transmission applications. An experiment is performed in which several images are encrypted and decrypted. The experimental results show that the proposed technique achieved high throughput rate that is fast enough for real time data protection.

Keywords: Cryptography, Pseudo-random Sequence, Genetic Algorithms.

Introduction

Cryptography is a method of storing and transmitting data in a form that only those it is intended for can read and process. It is a science of protecting information by encoding it into an unreadable format. Cryptography is an effective way of protecting sensitive information as it is stored on media or transmitted through network communication paths. Although the ultimate goal of cryptography, and the mechanisms that make it up, is to hide information from unauthorized individuals, most algorithms can be broken and the information can be revealed if the attacker has enough time, desire, and resources. So a more realistic goal of cryptography is to make obtaining the information too work-intensive to be worth it to the attacker.

As encryption evolved, it was mainly used to pass messages through hostile environments of war, crisis, and for negotiation processes between conflicting groups of people. Throughout history, individuals and governments have worked to protect communication by encrypting it. As time went on, the encryption algorithms and the devices that used them increased in complexity, new methods and algorithms were continually introduced, and it became an integrated part of the computing world. There are two types of cryptographic schemes: symmetric cryptography and asymmetric cryptography [3, 5]. The symmetric scheme uses the same key for encryption and decryption. Two keys is used in asymmetrical cryptography, one for encryption, known as the public key, and the other for decryption, known as the private key.

Asymmetric cryptography is often used in key distribution and digital signature for its slow processing speed. The symmetric cryptography is normally used to encrypt private data for its high performance. Moreover, none of the most used symmetrical ciphering systems like DES, IDEA and AES make use of the most recent developments in information processing technology. There have been various data encryption techniques [4, 8] on multimedia data proposed in the literature. Genetic Algorithms (GAs) [9] are among such techniques.

Genetic algorithms based on breeding process. In this process the search process create new and hopefully fitter individual. The breeding cycle consist of following steps: selection, crossover, mutation and reproduction. Reproduction and crossover together give genetic algorithms most of their searching power.

Many genetic algorithms based encryption have been proposed. A. Tragha et al.[6, 7], describe a new symmetrical block ciphering system named ICIGA (Improved Cryptography Inspired by Genetic Algorithms) which generates a session key in a random process. The block sizes and the key lengths are variable and can be fixed by the user at the beginning of ciphering. ICIGA is an enhancement of the system (GIC) "Genetic algorithms Inspired Cryptography" [6].

In this paper, we propose a new approach for encrypting real time data transmission. First we generate pseudorandom sequence using Non-Linear Feedback Shift Register (NLFSR) [1, 2]. The NLFSR is a mechanism for generating extremely well pseudorandom binary sequence. Second, we use the generated pseudorandom sequence with crossover operator for encrypting the data. The rest of the paper is organized as follows. In Section

2, we introduce the proposed method. Section 3 discusses the experimental results. Section 4, discusses about the analysis of the proposed method. Section 5 concludes the paper.

The Proposed Method

The proposed method block diagram is shown above in figure 1. It consists of pseudorandom sequence generator, crossover operator, and encryption and decryption modules, which are explained in the following subsections.

When the register is loaded with any given initial value (except 0 which will generate a pseudorandom binary sequence of all 0's), then pseudorandom binary sequence is generated with very good randomness and statistical properties.

The only signal necessary for the generation of the binary sequence is a clock pulse. With each clock pulse a bit of the binary sequence is produced.

The generated period of sequence by NLFSR is the maximum, if we use the primitive polynomial. To design any stream cipher system, one needs to consider the NLFSR with primitive feedback polynomials as the basic building blocks.

The usefulness of these sequences depends in large part on their having nearly randomness properties. Therefore such sequences are termed as pseudorandom binary sequences. The balance, run and correlation properties of these sequences make them more useful in the selection of secret keys.

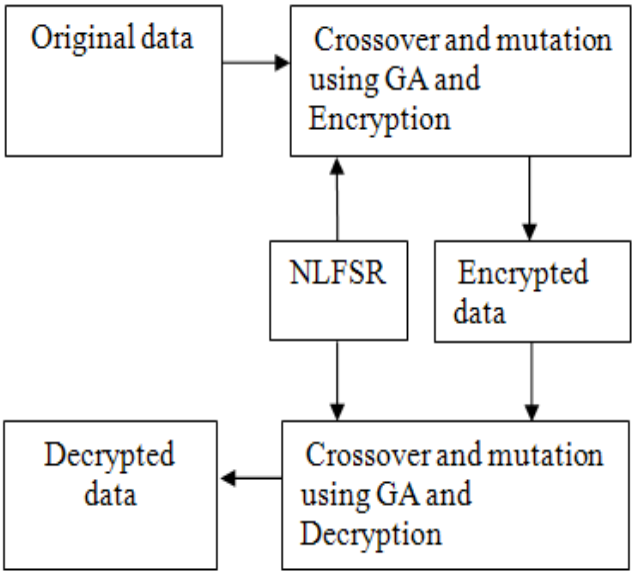


Figure 1: The block diagram of proposed method

A. The pseudorandom sequence Generator

Figure 2 shows a general model of NLFSR. It is a non linear forward feedback shift register with a feedback function *f* and non linear function *g*.

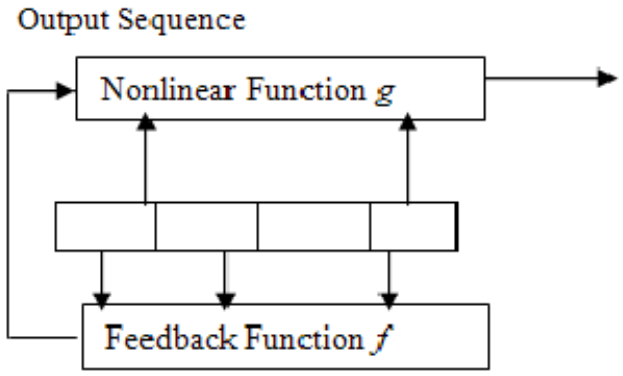


Figure 2: A General model of 4 bit NLFSR

B. Crossover operator process

The crossover is the process in which the strings are able to mix and match their desirable qualities in a random fashion. Crossover proceeds in three simple steps:

1. Two new random strings are selected as shown in figure 3a.
2. A random location in both strings is selected as shown in figure 3b.
3. The portions of the strings to the right of the randomly selected location in the two strings are exchanged as shown in figure 3c.

In this way information is exchanged between strings, and portions of two strings are exchanged and combined.

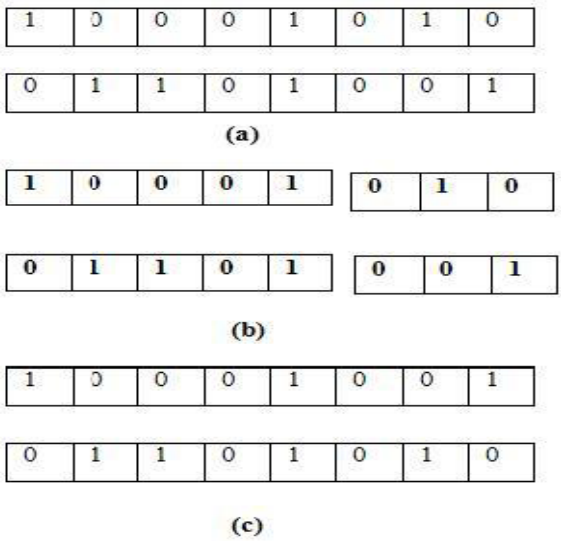


Figure 3: Illustration of the Crossover opera

C. Mutation operator process

After crossover, the strings are subjected to mutation. Mutation plays the role of recovering the lost genetic materials as well as for randomly disturbing genetic information. It is an insurance policy against the irreversible loss of genetic material. Mutation has

traditionally considered as a simple search operator. If crossover is supposed to exploit the current solution to find better ones, mutation is supposed to help for the exploration of the whole search space. Mutation is viewed as a background operator to maintain genetic diversity in the population. It introduces new genetic structures in the population by randomly modifying some of its building blocks. It also keeps the gene pool well stocked, and thus ensuring ergodicity. A search space is said to be ergodic if there is a non-zero probability of generating any solution from any population state. Mutation proceeds in three simple steps:
1. A string is selected after the crossover as shown in figure 4a.
2. Mutation string is randomly generated as shown in figure 4b.
3. For a 1 in mutation string, the corresponding bit in selected string is flipped (0 to 1 and 1 to 0) and new string is produced as shown in fig 4c .

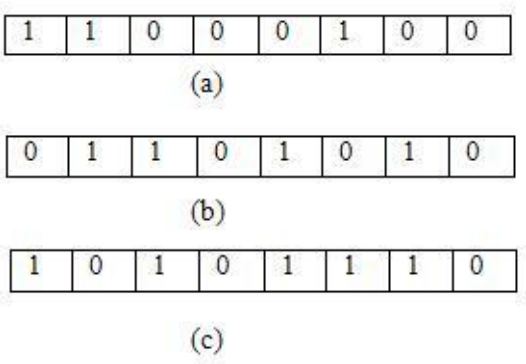


Figure 4: illustration of the Mutation operat

D. The encryption process

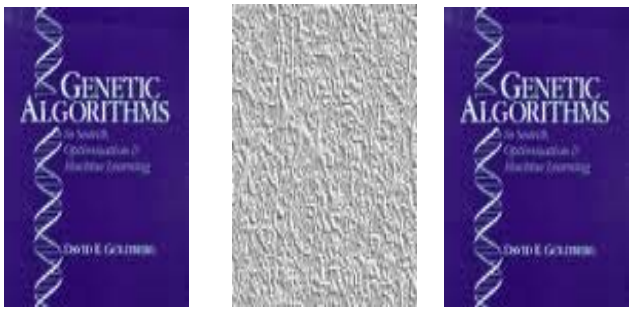
The encrypting process emulates the working of the crossover operator using pseudorandom sequence. It comprises the following steps:
1. Generate the pseudorandom binary sequence using the NLFSR as Zn .
2. Take mod 8 of the pseudorandom sequence to get the decimal value ranging from 0 to 7
Zn= mod (Zn,8).
3. Initialize 0 = i
4. Take two consecutive bytes of the data stream as A1 and A2
5. Crossover the two consecutive bytes of the data stream as B1 and B2 using Zi
6. Encrypt data as C1 and C2. Where
Xi=Zi Zi<<4
Xi+1=Zi+1 Zi+1<<4
C1=M1 Xi
C2=M2Xi+1
And i=i+2
7. Repeat steps 4 to 6 until end of the data.

E. The decryption process

The steps for decryption are just reversal of the encryption. First, generate the pseudorandom sequence using NLFSR after that using the generated pseudorandom sequence and crossover operator to decrypt the data.

Experimental Results

In the simulation, several images are used. As representatives, only the image of "BOOK" is shown in figures 5(a). The most direct method to decide the disorderly degree of the encrypted image is by the sense of sight. On the other hand, the fractal dimension can provide the quantitative measure on the randomness of the encrypted image. The encrypted result of the representative image by this method is shown in figures 5(b). According to the figure 5, the encryption result of the method is completely disordered and cannot be distinguished from the original image. The figures 5(c), shows the decrypted image of "BOOK". Since the proposed method is losable, we can find that there would be no encryption/decryption errors in using the proposed technique.



(a) (b) (c)

Figure 5: Encryption/decryption example

As an example, we consider two consecutive
bytes of the data stream A1 & A2 as
A1=11100010
A2=11001001
if the feedback function is $f = 1 + x + x2$ and the non linear function g defined by an-1.an-3 an-2.an-4 for Non linear Feed Forward Shift Register Generator, then, the generation of the pseudorandom sequence can be achieved as follows:
1. If the initial bit values (1111) are used, then the output sequence generated by NLFSR is periodic of the period 15

Zn= 0 1 1 1 1 1 0 0 0 ... …
2. The decimal value sequence is
Zn=2, 3, 1, 5 …
3. The value of
Zi= 2 & Zi+1=3.
Now, perform crossover operation with the generated pseudorandom sequence, in the operation

the various values generated are
B1=11100001
B2=11001010
M1=11001001
M2=11001110
Xi=00100010
Xi+1=00110011
C1=11101011
C2=11111101
The values of C1 and C2 are two consecutive encrypted data.

Performance Analysis

It is of interest to know if a message is encrypted by the proposed technique is easily decrypted or not. Since there are T combinations to encrypt 2 consecutive data bytes, thus the number of possible encryption result is T(N/2), where N is the total number of the data bytes to be encrypted and M is the length of one data byte. For example, we consider an image of size 256*256 pixels and color depth of 8 bit per pixel. In this case, T equals 8 and N equals 65536. All the possibilities are 832768. The speed of the algorithm is the important factor for a good encryption algorithm. We have measured the encryption/decryption rate for several gray scale images of different size. The average time taken by the algorithm for different size of a few images is shown in table 1.

Conclusions

In this paper, we have proposed a new way to encrypt the data travel over Internet. We used the concept of genetic cryptography with the randomness properties of NLFSR. Transmission of secret information is highly safe and reliable with the proposed method. In this case, without the knowledge of the pseudorandom sequence and mutation string no one will be able to extract the message since mutation string is act as a private key for decrypting the data. Since the NLFSR pseudorandom binary sequence is unpredictable it is very difficult to decrypt correctly an encrypted signal by making an exhaustive search without knowing the initial value and the feedback function *f* and non linear output function *g* of the NLFSR.

References

[1]. Ahmad A, Al-Musharafi M J, Al-Busaidi S. “A new algorithm procedure to test m-sequences generating feedback connections of Stream cipher’s LFSRs”, Proceedings of the IEEE TENCON’01, pp. 366-369, 2001.

[2]. Ahmad A, Al-Musharafi MJ, Al-Busaidi S, Al-Naamany A, Jervase JA. “An NLFSR Based Sequence Generation for Stream Ciphers”, Proceedings of International Conference on Sequences and their Applications, pp. 11-12, 2001.

[3]. Daemen J. and Rijmen V. “The Design of Rijndael, Advanced Encryption Standard”, ISBN 3-540-42580-2, Springer-Verlag, Berlin, 2002.

[4]. Douglas R. Stinson, “Cryptography - Theory and Practice”, CRC Press, 1995. Goldberg D.E., “Genetic algorithms in search optimization & Machine learning”,

[5]. National Bureau Standards, “Data Encryption Standard (DES),” FIPS Publication 46; 1977.

[6]. Tragha A, Omary F, Kriouile A. “Genetic Algorithms Inspired Cryptography” A.M.S.E Association for the Advancement of Modeling & Simulation Techniques in Enterprises, Series D: Computer Science and Statistics, 2005.

[7]. Tragha A, Omary F, Mouloudi A.”ICIGA: Improved Cryptography Inspired by Genetic Algorithms”, Proceedings of the International Conference on Hybrid Information Technology (ICHIT'06), pp. 335-341, 2006.

[8]. Wenbo M. “Modern Cryptography: Theory and Practice”, Publisher: Prentice Hall PTR, Copyright: Hewlett Packard, 2004.

[9]. Sivanandam SN, Deepa SN. “Introduction to Genetic Algorithms”, Publisher: Springer, Copyright: Springer-Verlag Berlin Heidelberg 2008.