International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 6 | ISSN : 2456-3307

Security Enhancement of TDMRC Encryption System by Increasing Randomness

[1]Antu Annam Thomas, [2]Varghese Paul

[1]Department of Computer Application, Mar Thoma College, Thiruvalla, Kerala, India
[2]Department of Information Technology, Rajagiri School of Engineering and Technology, Rajagiri Valley, Kakkanad, Kerala, India

ABSTRACT

Time Dependant Multiple Random Cipher Code is a novel approach in cryptography. It follows a symmetric key method and a poly-alphabetic substitution coding system. TDMRC is 'Mega Extended ASCII Code'. Complexities involved in TDMRC Code are Time Dependency, Poly Alphabetic Nature and use of Pseudo Random number generation technique for code generation. Key of TDMRC Code consists of three elements Master Key that is derived from Real Time Clock, Poly Alphabetic Coefficient(PAC), P, that decides the block size and P number of 4 digit subkeys. Randomness comes at three points in the algorithm while deciding PAC(P), while deciding P number of subkeys and while deciding P number of random series. Thus randomness can be improved by enhancing the random number generator Linear Congruential Generator(LCG) used in TDMRC.In this paper improved behaviour of Nested Linear Congruential Generator(NLCG) is coupled with TDMRC to improve the behaviour of TDMRC.

Keywords : Cryptography; Data Security; True Random Number Generator; Pseudo random number generator; Linear Congruential Generator; Time Dependant Multiple Random Cipher Code(TDMRC); Nested Linear Congruential Generator (NLCG)

I. INTRODUCTION

In this ever growing cyber world where millions and trillions of bytes of data is transferred everyday over the internet, the security of this data is a top priority and a major challenge. [1] Data Security is the practice of protecting a database from destructive forces and the unwanted actions of unauthorized users. Data Security can be achieved through either Access Control Methods or Encryption Methods.

Access Control Methods deal with security features that control how users and systems communicate and interact with one another. Access Control can be implemented by using methods like Password matching, Biometric Identification or Firewall Methods. Face recognition (computer application for automatically identifying or verifying a person from a digital image) which is one among the Biometric Identification method has become one of the most active research areas since the early 1990s . Powerful feature extraction algorithm together with powerful classifiers can very effectively do the job of recognition. A new improved face recognition method based on Simplified Fuzzy ARTMAP (SFAM) was experimented. The system proved to be efficient, fast and adaptive. [2][3][4]

Cryptography is the study and the practice of the techniques where in the plaintext by encryption is converted to an obfuscated and non - readable text (ciphertext or cryptogram). [1] Symmetric-key and Public-key encryption are the two basic encryption schemes. Symmetric key encryption is also called private key encryption or secret key encryption. The problem with secret keys in Symmetric Key Encryption is exchanging them over the Internet or a large network while preventing them from falling into the wrong hands. Anyone who knows the secret key can decrypt the message. Here comes the significance of asymmetric encryption where a key pair consisting of Public Key and Private Key is used. Here, the encryption key is published for anyone to use and encrypt messages, however, only the receiving party has access to the decryption key and is capable of reading the encrypted messages. Public Key encryption is also called asymmetric key encryption.

Time Dependant Multiple Random Cipher Code is a novel approach in cryptography. It follows a symmetric key method and a poly-alphabetic substitution coding system. TDMRC is 'Mega Extended ASCII Code'. Complexities involved in TDMRC Code are Time Dependency, Poly Alphabetic Nature and use of Pseudo Random number generation technique for code generation. Key of TDMRC Code consists of three elements Master Key that is derived from Real Time Clock, Poly Alphabetic Coefficient(PAC), P, that decides the block size and P number of 4 digit subkeys.[5]

Progress in cryptanalysis may threaten the security of existing algorithm. Thus the choice of key space and the key derivation method is very critical. Chosen cryptographic keys should be unpredictable, exhibit independence of values, have uniform distribution and be irreproducible. Randomness ensures generated values to be Independent, Uniformly distributed and Unpredictable. Random values cannot be reliably reproduced. Only randomness can make the generated keys to have all the above mentioned properties. Thus security of cryptographic systems is strongly related to randomness.

Depending on the randomness source, generators can be classified into three categories True Random Number Generators (TRNG), Unpredictable Random Number Generator (URNG) and Pseudo Random Number Generator (PRNG). For True Random Number Generators source is a natural physical phenomenon. Unpredictable Random Number Generator is based on unpredictability inherent to human computer interaction. Source of randomness in Pseudo Random Number Generators is a random initial value called seed which is expanded by means of random recursive formula. [6][7][8].

A strong need for further research in ensuring randomness was identified. Randomness can be improved at three points in the algorithm while deciding PAC(P), while deciding P number of subkeys and while deciding P number of random series. Increased level of randomness will increase the level of security offered by the code. So the paper revolves around Security Enhancement of TDMRC Encryption System by Increasing the Random Aspect of Key Generation.

II. Time Dependant Multiple Random Cipher Code (TDMRC)

TDMRC is an encryption system that uses symmetric key method and uses less complex mathematical operations compared with any other schemes. It is a substitution coding system.

The complexities involved in TDMRC are given below.

1. TDMRC Code is time dependant. The codes used for any character differs depending upon time. Even for centi second difference, the codes will change.

2. It is poly alphabetic. The code used for the same character at different locations of the plain text are different. Poly Alphabetic Coefficient (PAC) decides the number of codes used corresponding to each plain text character.

3. It uses pseudo random number generation technique for code generation. Depending upon the random seed the codes will change.

The Key of TDMRC Code consists of 3 elements.

1. Master Key derived from the Real Time Clock. It is an 8 digit number obtained by combining the values of hour, minute, second and centi second.

2. Poly Alphabetic Coefficient (PAC) which is actually a single digit number, P, indicating the number of codes simultaneously used for any character in an encrypting session. This is to be decided at encryption stage. P can be any value, (need not be limited to single digit value) but a value of 3 will be sufficient to achieve computational security.

3. P number of4 digit Sub Keys to be decided at the encryption stage.[5]

III. Randomness in TDMRC

Randomness comes at three points in the algorithm while deciding PAC(P), while deciding P number of subkeys and while deciding P number of random series. Randomness in TDMRC is generated by traditional random number generator algorithm known as Linear Congruential Generator(LCG). LCG is simple and easy to implement.

Random series is generated based on a piecewise linear equation given below.

$$X_{n+1}=(aX_n+c\ )\bmod m \qquad (1)$$

Here,

X is the sequence of random numbers
m, 0<m - modulus
a,0<a<m- multiplier
c,0≤c<m- increment
X_0,0≤X_0<m- seed value

Though LCG is fast and requires very less memory, LCG is not suitable for applications like cryptography where high security is demanded.[9][10]

IV. Improving Randomness in TDMRC

Randomness in TDMRC can be improved by improving LCG's performance or rectifying the shortcoming in LCG. In LCG the main drawback was that the period depends upon the value of modulus, increment and multiplier. In our improved system known as Nested Linear Congruential Generator there is no concept of period that is a sequence of numbers never repeat in the series being generated or in other words period is always infinity. Hence by introducing this improved LCG or NLCG the performance of TDMRC is improved.

V. Nested Linear Congruential Generator(NLCG)

In Nested LCG concept of nesting is introduced into traditional LCG. The series is generated based on the equation given below. The equation is the same linear piecewise equation as the traditional LCG. But here multiplier and increment is not a constant value as 'a' and 'c' in equation (1). 'multi' and 'incr' are the random numbers generated by two other random number series.

NLCG consist of three steps:

i. Getting the seed value
ii. Generating the series

A. *Getting the seed value:*

Based on the current system clock value read a pixel value of the current picture captured by system camera is read.

Based on the pixel value read two prime numbers $p1_0$ and $p2_0$ are generated. Here $p1_0$ is the greatest prime number less than the read pixel value and $p2_0$ is the smallest prime number greater than the read pixel value.

Seed value is given by,

$$X_0=p1_0*p2_0 \bmod m \qquad (2)$$

m is relatively prime to $p1_0*p2_0$

Thus seed value X_0 is the product of two prime numbers. Generated seed value is cryptographically secure due to two factors, difficulty in factorizing product of two prime numbers and true randomness introduced, clock value and pixel value.

The above mentioned complexity increases the efficiency of the system and makes the job of cryptanalyst difficult or rather impossible.[13]

B. Generating the series

$$X_i=(X_{i-1}*b_i+a_i)\bmod m \qquad (3)$$

$$b_i=f_i*p1_{i-1}*p2_{i-1} \qquad (4)$$

f_i is the pixel value read from the image based on $p1_{i-1}$ and $p2_{i-1}$

Now based on $p1_{i-1}$ and $p2_{i-1}$ next pair of prime numbers is generated $p1_i$ and $p2_i$.

$$a_i=p1_i*p2_i \qquad (5)$$

Equations (3), (4) and (5) together generate the random number series. The next element in the generated random sequence 'X_i' not only depends on previous value X_{i-1} but also on a_i and b_i which are next elements of two other random series generated by the equations (3) and (4).

Thus two random series values contribute for final random series generation. That is two random series is nested within another series.

Nesting ensures that sequence is never repeated within the final series being generated and period is infinity. NLCG algorithm is pictorially represented in the flowchart given below. [13]

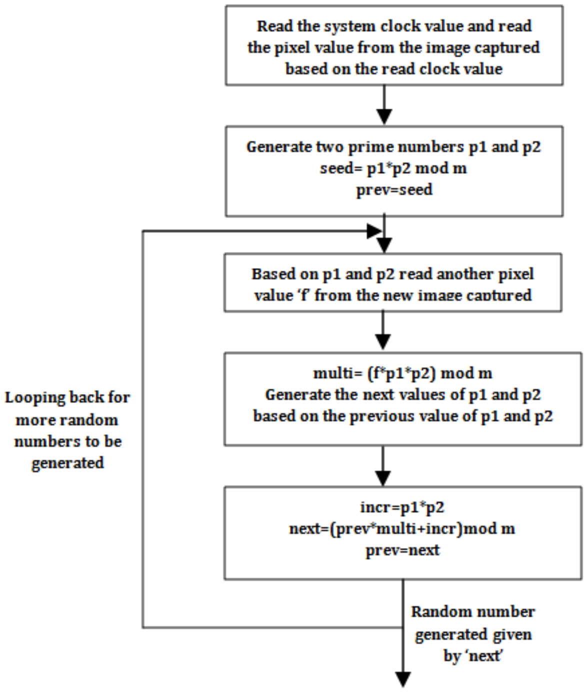
Read the system clock value and read the pixel value from the image captured based on the read clock value
Generate two prime numbers p1 and p2
seed= p1*p2 mod m
prev=seed
Based on p1 and p2 read another pixel value 'f' from the new image captured
multi= (f*p1*p2) mod m
Generate the next values of p1 and p2 based on the previous value of p1 and p2
incr=p1*p2
next=(prev*multi+incr)mod m
prev=next
Looping back for more random numbers to be generated
Random number generated given by 'next'

Figure 1. Flowchart of NLCG

NLCG is cost effective since no expensive hardware is required. Seed value generated is sufficiently complex since true randomness and prime factorization problem is used in this step. Nested concept used during series generation makes the series unpredictable and random and subsequence never repeats in the generated sequence. [11][12]

Complexities involved in this method include true entropy sources introduced in the generation, prime factorization problem, concept of nesting used in the algorithm. [13]

VI. CONCLUSION

Performance enhancement of TDMRC was made possible by improving the performance of Random number generator used in TDMRC. Nesting was introduced into traditional LCG so that concept of period is removed from the generated series or the period is always infinity. True random source, prime factorization problem and nesting all together contributes to the improved performance of NLCG. This improved behavior of NLCG made it apt for cryptographic and other security related activities. Hence NLCG when coupled with TDMRC made the encryption system more efficient and secure.

VII. REFERENCES

[1]. Harshavardhan Kayarkar, Sugata Sanyal, "Classification of Various Security Techniques in Databases and their comparative analysis", ACTA TECHNICA CORVINIENSIS –Bulletin of Engineering, Fascicule 2 [April–June],2012,pp. 135-138

[2]. Antu Annam Thomas and M.Wilscy, "Face Recognition Using Simplified Fuzzy ARTMAP", Signal & Image Processing : An International Journal(SIPIJ) Vol.1, No.2, pp. 134-146, December 2010

[3]. Antu Annam Thomas and M.Wilscy "An Improved and Adaptive Face Recognition method using Simplified Fuzzy ARTMAP", In Proceedings of the First International Conference on Computer Science and Information Technology (COSIT 2011), Jan. 2 - 4, 2011, Bangalore, India.

[4]. Antu Annam Thomas and M.Wilscy "A comparative study of Simplified Fuzzy ARTMAP and Feedforward neural network in the context of face recognition", In Proceedings of the Second International Conference on Networks & Communications (NETCOM 2010), Jan. 2 - 4, 2011, Bangalore, India

[5]. "Data Security in Fault Tolerant Hard Real Time Systems, Use of Time Dependant Multiple Random Cipher Code", A thesis submitted by Varghese Paul in partial fulfillment of the requirements for the degree of Doctor Of Philosophy of Cochin University of Science and Technology

[6]. Kinga Marton, Alin Suciu, Losif Ignat, "Randomness in Digital Cryptography: A Survey" Romanian Journal Of Information Science and Technology ,Volume 13, Number 3, 2010, 219–240

[7]. Norm Matloff, "Random Number Generation",February 21, 2006

[8]. Harald Niederreiter, "Random Number Generation and QuasimMonte Carlo Methods",

Society for Industrial and Applied Mathematics, Philadelphia, 1992.

[9]. "Linear Congruential Generators" by Joe Bolte, Wolfram Demonstrations Project.

[10]. Donald E. Knuth (6 May 2014). Art of Computer Programming, Volume 2: Seminumerical Algorithms. Addison-Wesley Professional. pp. 4–. ISBN 978-0-321-63576-1.

[11]. "True Random Number Generators Secure in a Changing Environment", Boaz Barak, Ronen Shaltiel, and Eran Tromer, Department of Computer Science and Applied Mathematics, Weizmann Institute of Science , Rehovot, ISRAEL

[12]. Adi A. Maaita, Hamza A. A. Al_Sewadi, "Deterministic Random Number Generator Algorithm for Cryptosystem Keys", International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol:9, No:4, pp 972-977, 2015

[13]. Antu Annam Thomas and Varghese Paul, "Performance Enhancement of Cryptographic Algorithms by Increasing Randomness through Nesting In Random Number Generators", Antu Annam Thomas, Varghese Paul , International Journal of Scientific Research in Computer Science, Engineering and Information Technology, Volume 2, Issue 5, May 2017, pp. 203- 209

[14]. Antu Annam Thomas and Varghese Paul, "Nested Random Number Generator", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 7, Issue 5, May 2017, pp.767-773