Volume 5, Issue 8, August 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Multimedia Data Security Using Operations Analogous to Biological Processes

Mst. Jahanara Akhtar*
Department of Computer Science &Engineering
Dhaka International University,
Bangladesh

Riyad Bin Zaman
Department of Computer Science &Engineering
Shahjalal University of Science & Technology,
Bangladesh

Abstract- ***Encryption is the most important method in transferring data through internet and cellular phone. Due to increasing incidents of cyber attacks, the demand for effective internet security is increasing. Cryptography is the science and study of system for secretes communication. Cryptography is used in applications like security of ATM cards, computer passwords, electronic commerce, telemedicine, e-health, telecommunication, and so on. In this paper, an encryption and decryption method is proposed to generate offspring of multimedia data using operations analogous to biological processes.***

Keywords- cryptography; encryption; metamorphosis; intersect; offspring; generation.

I. INTRODUCTION

Recently, with the greater demand in digital signal transmission and the huge losses from illegal data access, data security has become a critical and imperative issue in multimedia data transmission applications. In order to protect valuable information from undesirable readers or against illegal reproduction and modifications, various types of cryptographic schemes are needed. The Vernam cipher [21], although originally implemented with electromechanical relays, may well mark the start of modern cryptography. A Vernam cipher directly combines a stream of plaintext data with a pseudo-random confusion stream using what we now know of as mod 2 addition. This same combining function is also known as the Boolean logic exclusive-OR, and is widely available in digital integrated circuits and as an instruction on most computers and microcomputers.

A newly developed technique named, "A new Symmetrickey Cryptography Algorithmusing extended MSA metod: DJSA symmetric key algorithm" [22], are suggesting a symmetric key method where they have used a method which was proposd by Nath in MSA algorithm. The paper [23] have proposed a new cryptography algorithm which is based on block cipher concept. Since each ciphertext element from a Vernam combiner is the (mod 2) sum of two unknown values, the plaintext data would seem to be well hidden. Such appearances are deceptive, however, and a Vernam cipher is susceptible to several cryptanalytic attacks, including known-plaintext and probable words [14]; if some part of the plaintext is known (or even guessed), the cryptanalyst can directly obtain some of the confusion stream [8, 9]. And if the confusion sequence can be penetrated and reproduced, the cipher is broken [13, 18, 6]. Similarly, if the same confusion sequence is ever re-used, and the overlap identified, it becomes simple to break that section of the cipher [14]. For these reasons, the modern Vernam cipher generally relies on an analysis-resistant pseudo-random sequence generator for security [e.g. 13]. But the design of such a generator is non-obvious [1, 24], and is even more difficult than it might seem, since the cryptanalyst might well possess analytical knowledge and capabilities superior to those of the designer of the generator. Future analysts may be even more capable. Accordingly, constructs which may seem complex to the designer [5, 112, 2] may well yield, eventually, to the superior knowledge and computational resources of a cryptanalyst [18, 15, 11].

An alternate approach to the design of a secure stream cipher is to seek combining functions which can resist attack; such functions would act to hide the pseudo-random sequence from analysis [17, 18, 19]. Such cryptographic combining functions could be used to replace the Vernam exclusive-OR combiner (if they have an inverse) [16], or they might just combine pseudo- random sequences to make a more complex sequence [10, 25] which is harder to analyze.

Classical simple substitution replaces each letter of the alphabet with one fixed substitute [4, 20]. Simple substitution is normally considered to be a very weak cryptographic operation [7,26] mainly because substitution in no way obscures the letter- frequency distribution of the source text. That is, for a particular language and topic, a statistical analysis of the enciphered data will tend to match the general statistics for that language. The fundamental operation of substitution is pervasive in cryptography [3]. But in all known previous systems the substitution is static. That is, each substitution table is fully defined (either by the designer or the key) before starting encryption, and the contents of each substitution table remain unchanged for the duration of that particular cipher or message.

II. PROPOSED METHOD

Data encryption of the proposed method is block cipher concept. The proposed method consist of a key generator, generate random number (maximum value is given) and create next key from given key value (SelectionKey) using

shifting and XOR operation. First digit is used for intersect point of Item1 and Item2. Exchange operation interchanges the bits of Item from the intersect point [27]. The second digit is used for metamorphosis of offspring1 and third digit for metamorphosis of offspring2. This method has been used multiple rounds and creates new generation. Flowchart of the proposed method is shown in figure 1.

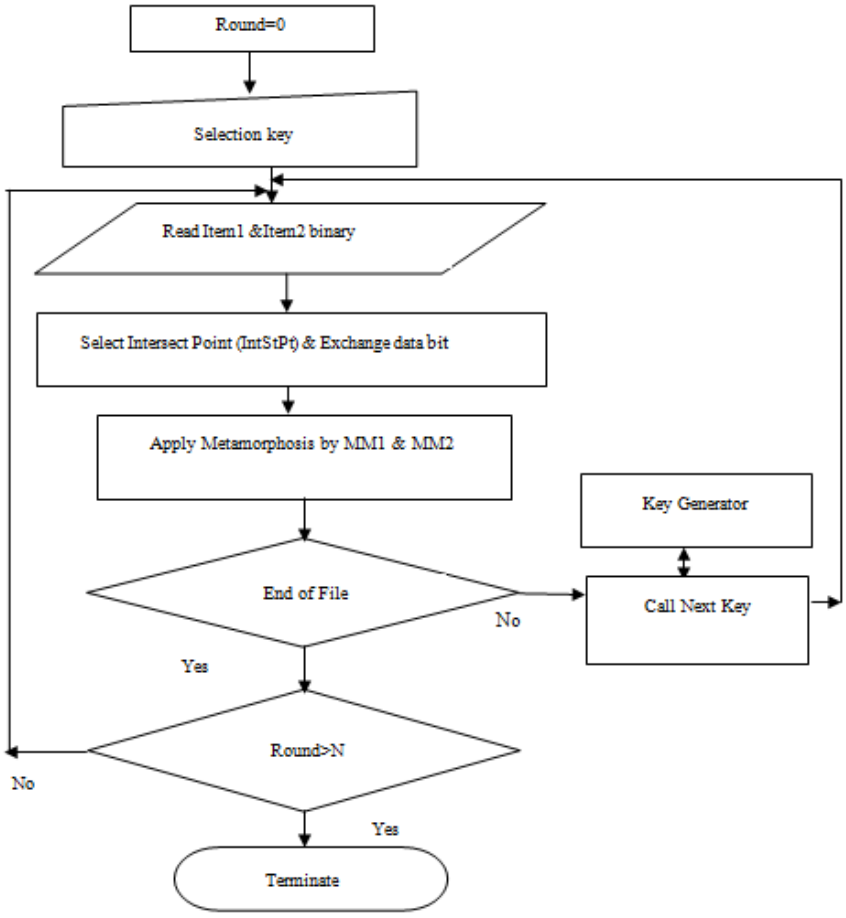

Figure 1. Flowchart of the proposed method

Encryption algorithm of the proposed method is given bellow.

Algorithm Encryption (Item1, Item2, IntStPt ,MM1 , MM2)

For first round this algorithm create offspring from input file using intersect, exchange and metamorphosis. Intersect Item1 and Item2 using the value of IntStPt. Exchange the bits if Items. Apply metamorphosis Item1 using MM1 and Item2 using the value of MM2.

1. Round=0, N= No. of Round
2. Input SelectionKey
3. Repeat step 4 to 8 until End of File
4. Read Item1 and Item2 as binary.
5. Select intersect point IntStPt from Selection Key.
6. Apply exchange operation.
7. Apply metamorphosis operation using the key value MM1 and MM2 (If bit is 1 then change it 0 and vice versa).
8. Call key generator for next key value.
9. Increment Round.
10. If Round less equal N then go to step 2.

Decryption is the reverse process of encryption using same key.

Example: Suppose selection key is 362, binary values (7 bit ASCII Code) of Item1 and Item2 are 1001110 and 0110100. 3 is the intersect point. 6 and 2 are used as MM1 and MM2. After exchange the new data become, 0111110 and 1000100 and after metamorphosis operation, the offspring are 0111100 and 1000110. Generate new key and apply same process for next items for round 1 until end of file.

Apply the operations N times and generate the encrypted data.

III. PERFORMANCE ANALYSIS

In this method, bit level encryption is used and any data in binary form can be encrypted and decrypted. For block cipher concepts this method is time consuming. If input size is M MB bit and No. of round is N then $!N * 2^{M*7*10^6}$ combinations is possible.

IV. CONCLUSION

A new approach for encryption and decryption of multimedia data is proposed in this paper. Number of round increase the security level. The total way of transferring secret information is highly safe and reliable. Programming language C is used for encryption and decryption.

V. LIMITATIONS AND FUTURE WORK

Different key for encryption and decryption and the random selection of items to create new generation to increase security is the future plan of this work.

REFERENCES

[1] Blum, L., M. Blum, and M. Shub, 1983, Comparison of Two Pseudo-Random Number Generators. *Advances in Cryptology-Proceedings of Crypto 82.* New York: Plenum Press. 61-78.
[2] Ciarcia, S. 1986. Build a Hardware Data Encryptor. *Byte.* September. 97-111.
[3] Feistel, H. 1973. Cryptography and Computer Privacy. *Scientific American.* 228: 15-23.
[4] Gaines, H. 1956 (original publication 1939). *Cryptanalysis.* New York: Dover Publications.
[5] Geffe, P. 1973. How to protect data with ciphers that are really hard to break. *Electronics.* January 4. 99-101.
[6] Meier, W. and O. Staffelbach. 1988. Fast Correlation Attacks on Stream Ciphers (extended abstract). *Advances in Cryptology--Eurocrypt 88.* New York: Springer-Verlag. 301-314.
[7] Mellen, G. 1973. Cryptology, Computers, and Common Sense. *National Computer Conference, 1973, Proceedings.* 569-579.
[8] Meyer, C. and W. Touchman. 1972. Pseudorandom codes can be cracked. *Electronic Design.* 23: 74-76.
[9] Meyer, C. 1973. Design considerations for cryptography. *National Computer Conference, 1973, Proceedings.* 603-606.
[10] Michener, J. 1987. The Use of Complete, Nonlinear, Block Codes for Nonlinear, Noninvertible Mixing of Pseudorandom Sequences. *Cryptologia.* 11: 108-111.
[11] Pearson, P. 1988. Cryptanalysis of the Ciarcia Circuit Cellar Data Encryptor. *Cryptologia.* 12: 1-9.
[12] Pless, V. 1977. Encryption Schemes for Computer Confidentiality. *IEEE Transactions on Computers.* C26: 1133-1136.
[13] Reeds, J. 1977. "Cracking" a Random Number Generator. *Cryptologia 1,* pp. 509-515.
[14] Rubin, F. 1978. Computer Methods for Decrypting Random Stream Ciphers. *Cryptologia 2,* pp. 493-508.
[15] Rubin, F. 1979. Decrypting a Stream Cipher Based on J-K Flip-Flops. *IEEE Transactions on Computers.* pp. 283-293.
[16] Sancho, J. 1987. Enumeration of Multivariable Decipherable Boolean Functions. *Cryptologia.* 11: 172-180.
[17] Siegenthaler, T. 1984. Correlation-Immunity of Nonlinear Combining Functions for Cryptographic Applications. *IEEE Transactions on Information Theory.* IT30: 776-780.
[18] Siegenthaler, T. 1985. Decrypting a Class of Stream Ciphers Using Ciphertext Only. *IEEE Transactions on Computers.* C34: 81-85.
[19] Siegenthaler, T. 1986. Design of Combiners to Prevent Divide and Conquer Attacks. *Advances in Cryptology--CRYPTO '85, Proceedings.* New York: Springer-Verlag. 273-279.
[20] Sinkov, A. 1966. *Elementary Cryptanalysis: A Mathematical Approach.* Washington, DC: The Mathematical Association of America.
[21] Vernam, G. 1926. Cipher Printing Telegraph Systems. *Transactions AIEE.* 45: 295-301.
[22] Dripto Chatterjee, Joyshree Nath, Suvadeep Dasgupta, Asoke Nath "A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm" International Conference on Communication Systems and Network Technologies, 2011, 978-0-7695-4437-3/11.
[23] Vishwa gupta, Gajendra Singh , Ravindra Gupta, "Advanced Cryptographic algorithm for improving data security", International Journal of Advanced Research in Computer Science and Software Engineerg, Volume 2, Issue 1, January 2012, ISSN: 2277 128X.
[24] Symmetric key cryptography using random key generator, A.Nath, S.Ghosh, A Mallik, Proceedings of Internationalconference on SAM-2010 held at Las Vegas(USA) 12-15 July, 2010, Vol-2, P-239-244.
[25] Data Hiding and Retrieval, A.Nath, S.Das, A.Chakrabarti, Proceedings of IEEE conference on Computer Intelligence and Computer Network held at Bhopal from 26-28 Nov, 2010.
[26] Menzes A.J., Paul,C., Van Dorschot, V., Vanstone, S.A.,2001, "Handbook of Applied Cryptography", CRS press 5th printing; pp.15,16.
[27] Tragha A., Omary F., Mouloudi A.,2006 "IVIGA: Improved cryptography inspired by genetic Algorithms", Proceedings of the international Conference on Hybrid Information Technology (ICHIT'60), pp. 335-341.

