International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-1S4, December 2019

A Novel Encryption Algorithm Based on Pseudo Random Sub Blocks of Data Blocks

M. Venkatesulu, S. Ponkeerthana, M. Swathi, C. Anitha

ABSTRACT: ***In this paper, we propose data encryption algorithm based on randomized sub blocks XORing of data blocks. The data is divided into number of square blocks (in terms of bits) of equal size. The last block is padded with zeros if required. The proposed algorithm uses pseudo random keys to generate the order of sub blocks of data blocks for encryption. The encryption is done on sub blocks and therefore much faster and highly sensitive for small changes in the keys.***

Key words: pseudo random key, encryption, decryption, plaintext, cipher text, XORing

I. INTRODUCTION

In the modern digital world, all documents are stored and transmitted electronically. Hence the security of these digital documents is of vital importance as there are stored and transmitted in the third party infrastructure. Encryption is a scheme that protects the documents from unauthorized users and hackers. There are two types of methods of encryption namely block ciphers and stream ciphers. Examples Of Block ciphers are DES, RC2, 3 DES, AES, Blowfish, Camellia, Serpent and Two fish. Examples of stream ciphers are RC4, a5/1, a5/2, Chameleon, FISH. Also there are two types of encryption algorithms namely symmetric key and asymmetric key encryption algorithms. AES is a symmetric key algorithm and RSA is an asymmetric key algorithm. Of course there are number of such algorithms. S.Arul Jothi and M.Venkatesulu (1) proposed a new approach to randomized key in the symmetric key block cipher encryption algorithm. The scheme has key generation, encryption and decryption process. Data is stored as abinary matrix and the bits are encrypted randomly using the key.

II. PROPOSED ALGORITHM:

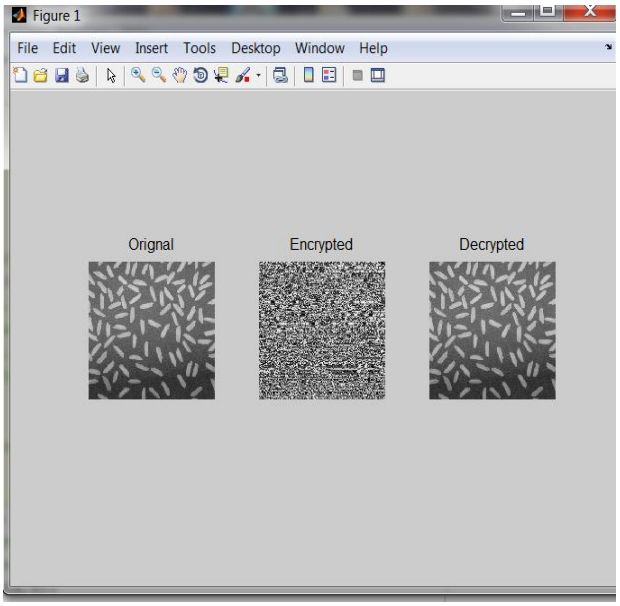
In our proposed algorithm the data is stored in bytes as matrix. The plain text/data is sub divided into sub matrices of size (8 by 8) bits (1 byte along a column and 8 bytes along a row).Suppose that the block size is (8n by n) bytes matrix where n is a positive integer. We sub divide the block in to n2 sub blocks of size (8 by 8) bits each. There are n^2 such sub blocks and each block is represented by the position (i, j) of the sub block. The key generates these positions randomly.

Manuscript published on 30 December 2019.
* Correspondence Author (s)
M. Venkatesulu, Sr Professor, Department of Information Technology, Kalasalingam Academy of research and education, Krishnankoil, India.
S. Ponkeerthana, Department of Information Technology, Kalasalingam Academy of research and education, Krishnankoil, India.
M. Swathi, Department of Information Technology, Kalasalingam Academy of research and education, Krishnankoil, India.
C. Anitha, Department of Information Technology, Kalasalingam Academy of research and education, Krishnankoil, India.

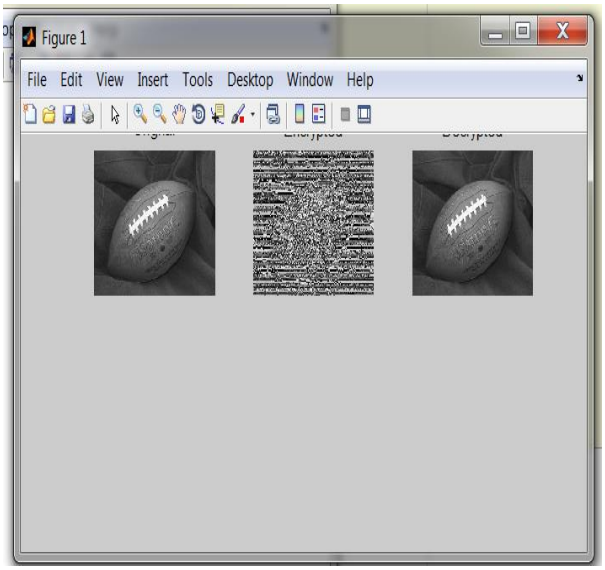
Input:
Plain text of size (8n by n) bytes matrix where n is a positive integer
Output: Cipher text of size (8n by n) bytes matrix
Method:
Step1: Generate a pseudo random position key K: (i,j), 1,j=1,2....,n.
Step2: Divide the plain text into n^2 number of sub blocks of size 8×8 matrix.
Step3: Consider the sub block at position (1, j). Then XOR of all sub blocks at positions {(1,j),(2,j).....(i-1,j),(i,j),..(i+1,j)….(n,j) (i,1), (i, 2),.....(i, j-1), (i,j+1), (i, j+2).....(i, n)}. The resulting block is the Cipher text corresponding to the original sub block at position (i,j).
Step 4: We repeat the step 3 for all sub blocks of the plain text following the order (first to last) specified by the key K. The result is the cipher block of the original block.
Step 5: Applying the key K in the reverse direction (last to first) in steps3 and 4 on the cipher text, results in the original plain text.

III. EXPERIMENTAL RESULTS:

The proposed algorithms is 64 times faster than the encryption proposed by Arul Jothi and Venkatesulu since a sub block of size 8x8 bits is encrypted at time instead of 1 bit at a time as done in



Left most: Original image
Middle: Encrypted image
Right most: Decrypted image



Left most: Original image
Middle: Encrypted image
Right most: Decrypted image

IV. CONCLUSION AND REMARKS:

This paper explained a new encryption algorithm with a novel use of randomized key in symmetric block cipher scheme. If implemented encryption of all 64 bits in the 8 by 8 bit block size our algorithm definitely ensures very fast encryption of O (64) timesfaster than compared to the encryption algorithm [1].

REFERENCES:

1. Arul Jothi.S and Venkatesulu.M[2013], A new approach to randomized key in thesymmetric block cipher encryption algorithm, Vol.63, No.7, pp.190-199
2. Bruce Schneier[1996], Applied Cryptography: Protocols, Algorithms, and Source Codein C, Wiley
3. Ferguson, N. Schneier, B., & Kohno, T. (2010). Cryptography Engineering: DesignPrinciples andPractical Applications. New York: John Wiley & Sons.
4.Gunasundari.T and, Elangovan.K.[2014], "A Comparative Survey on Symmetric KeyEncryption Algorithms", IJCSMA, Vol.2 Issue, 2, , pg. 78-83
5. John Justin Mand ManimuruganS[2012]"A Survey on Various Encryption Techniques".IJSCE, Volume-2, Issue-1, pp. 429-432
6. Kapsepatil A. and Shah P[2012]., "A Literature Survey on Symmetric Encryption Algorithmsfor Digital data", IJAIR, pp. pp.306-308
7. Patil A and GoudarR[2013], "A Comparative Survey Of Symmetric Encryption Techniques
For Wireless Devices", IJSTR, Vol 2, Issue 8, Aug 2013, pp. 61-65,
8. Simion, E. (2015). The Relevance of Statistical Tests in Cryptography, IEEE Security &
Privacy, 13(1), pp. 66:70.
9. Stallings, W. (2006). Cryptography and Network Security: Principles and Practice, 4th
ed, Englewood Cliffs, NJ: Prentice Hall
10. Thakur J., Kumar N(2011)., "DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis", IJETAE, ISSN 2250
2459, Volume 1, Issue 2, pp. 6-12
11. Watanabe, D. (2015), Improving the Security of Cryptographic Protocol Standards.
IEEE Security & Privacy, 13(3), pp. 24:31.

AUTHORS PROFILE

Dr.M.Venkatesulu did his under graduation in Mathematics from the University of Madras, Post-graduation in Mathematics in Mathematics from Sri Venkateswara University, Tirupati and obtained PhD in Mathematics from the Indian Institute of Technology, Kanpur. He was a faculty member in the department of mathematics and Computer Science at Sri Sathya Sai Institute of Higher Learning (Deemed to be University), Prasanthinilayam, Andrapradesh, India. He worked as a consultant for a short duration in Satyam Computer Services Limited, Secunderabad, India during 2002. He has joined Kalasalingam Academy of Research and Education in 2004 as Senior Professor in Mathematics. He was a visiting Professor in the Department of Mathematics and Statistics, University of Missouri, Kansas City, USA during 2006-2007. He has published more than 70 papers in peer reviewed journals and Conferences and guided 14PHDs in Mathematics and Computer Science areas. He has completed 4 R&D projects funded by RDDO and DST, Government of India. He is a reviewer for 2 International journals published by Elsevier.

S. Ponkeerthana has completed her Under Graduationin Information Technology from Kalasalingam Academy of Research and Education,Krishnankoil. Her area ofinterestis java and Mat Lab.

M.Swathi has completed her Under Graduationin Information Technology from Kalasalingam Academy ofResearch and Education,Krishnankoil. Her area of interestis Database and Mat Lab.

C.Anitha has completed her Under Graduationin Information Technology from Kalasalingam Academy ofResearch and Education,Krishnankoil. Her area of interestis Data mining and Mat Lab.