RESEARCH ARTICLE OPEN ACCESS

A Symmetric Key Cryptographic Technique Through Swapping Bits in Binary Field Using p-Box Matrix

Subhranil Som[1], Soumasree Banerjee[2], Jhilik Sikdar[3]
[1,2,3]Department of Computer Application, JIS College of Engineering

Abstract
In this paper a symmetric key cryptographic algorithm named as "A Symmetric Key Cryptographic Technique Through Swapping Bits in Binary Field Using p-box Matrix" is proposed. Secret sharing is a technique by which any information can be break down into small pieces. The secret can be reconstructed only when a sufficient number of pieces of shares are combined together; individual shares are of no use on their own. Traditional secret sharing scheme possesses high computational complexity in both generating and reconstructing of share. In the proposed algorithm key has been taken from the user of n bits. Depending on the size of input stream a straight p-box will be generated to make the proposed algorithm unique. The Key and the p-box will be needed for encryption and decryption process. The block division process is introduced in the input stream. In the process of encryption swapping in binary input stream will be taken place.
Keyword: Plain Text, Cipher Text, Encryption, Decryption, P-Box and Key Image.

I. Introduction

Secret images are used in many commercial and military applications. The recent past years we used many image processing techniques like image hiding [1], watermarking [2], image steganography [3] etc. For every technique the prime concern to hide the secret. A common drawback for all the early mentioned method viz. image hiding, watermarking and steganography is that the secret image is stored and transmitted as a single unit. Thus any intruders capture this single unit, it does not remain secret. Hence these drawbacks scientists have lead to evolve others scheme where a single secret can be transmitted via multi channel. Secret image sharing [4] is the art and science about the protection of important images by distributed storages. The problem of secret sharing first proposed by Shamir [4] (1979) and Blakley [5] (1979) where a secret S can be distributed among n shares. The n shares can be distributed among n channels. Each share t individually has no meaning. Anyone can reconstruct the secret S if sufficient number of shares k is available, where $k \leq n$. The Shamir's scheme [4] relies on the concept that you can fit a unique polynomial of degree (t-1) to any set of t points that lie on the polynomial. Blakely's [5] technique assumes that secret is a point in a k-dimensional space. Hyper planes intersecting at this point are used to construct the shares. Coefficients of n different hyper planes constitute the corresponding n shares. In [6] authors are proposed a proactive secret sharing scheme to update shares periodically such that an attacker has less time to compromise shares. Some sharing scheme relies on Chinese Remainder Theorem [7, 8]. Mignotte's threshold secret sharing scheme [9] and Asmuth-Bloom threshold secret sharing scheme [10] both also based on the Chinese remainder theorem. Ito, Saito,and Nishizeki [11], Benaloh and Leichter [12] give constructions for more general secret sharing schemes. The notion of ideal structures of secret sharing scheme proposed by Brickell [13] .The concept of multi secret sharing scheme was proposed by Jackson et al. [14] multiple secrets are generated and distributed during one secret sharing process. Thien and Lin [15] proposed a (k, n) where threshold-based image secret sharing scheme by cleverly using Shamir's secret sharing scheme [4] to generate image shares. Karnin et al. [16] suggested the concept of perfect secret sharing (PSS) where zero information of the secret is revealed for an unqualified group of (k -1) or fewer members. In [17] the authors are proposed a secret sharing scheme based on random matrix. In this paper, we propose a secret image sharing method where at least two shares and a key image needed to reconstruct the source images at the receiver end.

In section II the scheme of proposed technique is discussed. In section III the example is given for the proposed algorithm. Section IV is discussed computational complexity. Conclusive discussion and future scope is discussed in section V and VI respectively. References are noted down in section VII.

II. The Scheme

Input Streams of 'n' length bits and a key (K) of 'b' length bits are taken for encryption. Using block division process input stream are divided into different equal blocks of size 's' bits. K has been taken from user input. Key is symmetric in nature. 'n'

bits input stream is equally divided into different subparts. All the block division and key generation will be done in binary field. A1, A2, A3 and A4 are blocks of input stream contains 'm' number of bits denoted by {m3, m2, m1, m0}, where $m_i \in \{1, 0\}$. A1, A2, A3 and A4 are arranged in a cyclic manner. Bits of key R_k are scanning from right to left taking two bits at a time to swap bits of the index location as per value of bits, taken from the key, between A1, A2; A2, A3; A3, A4 and A4, A1 respectively. Straight p-box matrix has been generated depending on block division size of input stream and element of the p-box matrix is populated randomly generated number between 0 to 's'. Depending the values in p-box A1, A2, A3 and A4 are converted into decimal number. 'm' bits A1, A2, A3 and A4 are converted into 'm+2' bits and represented as L1, L2, L3 and L4 respectively. 2's compliment is applied into bits of L1, L2, L3 and L4. L1, L3, L2 and L4 are concatenated to get the 'n*3' cipher bits. Cipher blocks will be divided into '(n*3)/8' blocks to get the equivalent ASCII code of each block and corresponding character to get the final cipher of input stream. Decryption will be done through the reverse process of encryption.

III. Example

Let, plain text is **AB**

Encryption:

Binary equivalent of A is p1 = 01000001
Binary equivalent of B is p2 = 01000010
Let, the key is given by the user character P
Binary equivalent of P is R1 (Key) = 01010000
p1 is divided into two segments A1 = 0100 and A3 = 0001, each segment contains 4 bits.
p2 is also divided into two segments A2 = 0100 and A4 = 0010, each segment contains 4 bits.
A1, A2, A3 and A4 are divided into two segments and addressing each segment as 1 and 0 as shown Figure: 1.

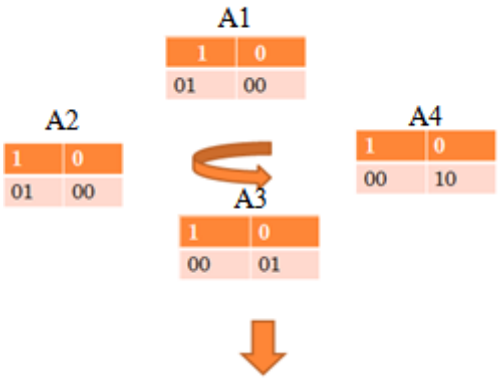


Figure: 1

Taking two bits of R1 (Key) in reverse order.

As per the proposed technique, 00 in reverse is taken from the key R1 and swapping the value in between A1 and A2 segment at 0,0 location (Figure: 2).

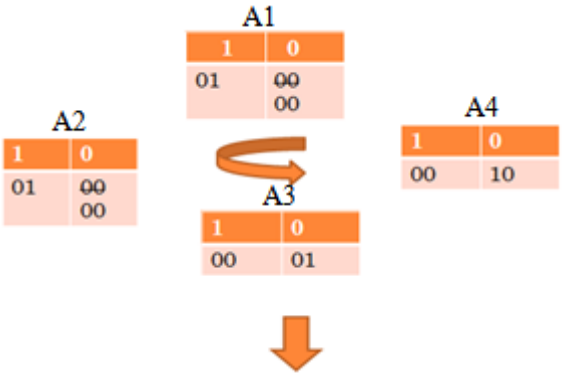


Figure: 2

Next 00 in reverse is taken from the key R1 and swapping the value in between A2 and A3 segment at 0,0 location (Figure: 3).

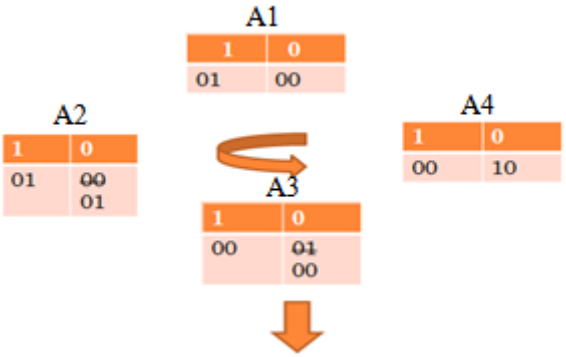


Figure: 3

Next 10 in reverse is taken from the key R1 and swapping the value in between A3 and A4 segment at 1,0 location (Figure: 4).

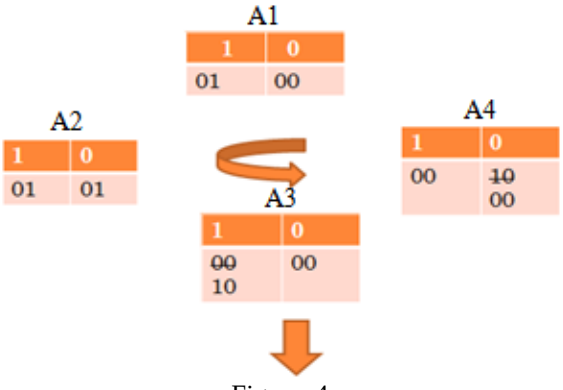


Figure: 4

Next 10 in reverse is taken from the key R1 and swapping the value in between A4 and A1 segment at 1,0 location (Figure: 5).

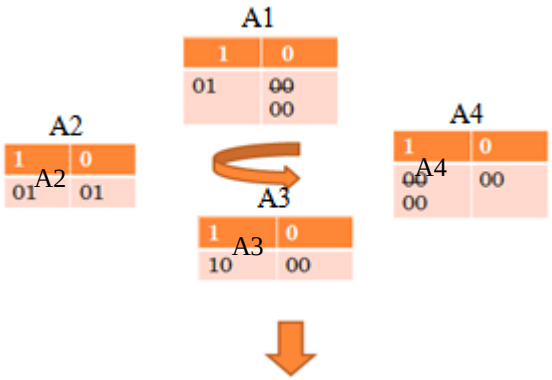


Figure: 5

As per the proposed technique the final figure of A1, A2, A3 and A4 is shown below in Figure 6:

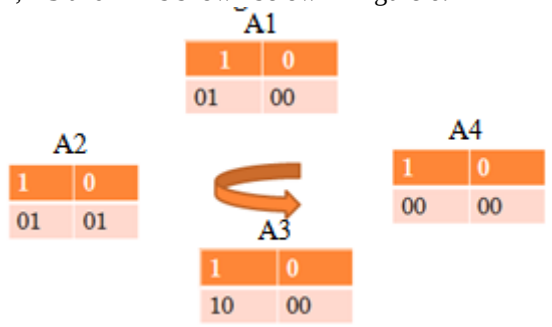


Figure 6:

Final bits value of A1 = 0100
A2 = 0101
A3 = 1000
A4 = 0000

2 X 8 straight P-box is generated and 16 numbers are generated randomly to initialize the p-box shown in Figure 7:

9	8	1	2	6	14	13	7
4	11	0	5	12	10	15	3

2 X 8 straight p-box
Figure: 7

In the above figure all the numbers 9, 8, 1, 2, 6, 14, 13, 7, 5, 11, 0, 4, 12, 10, 15 and 3 are generated randomly within 0 to 15 as because the example is repressing 16 bits binary value.

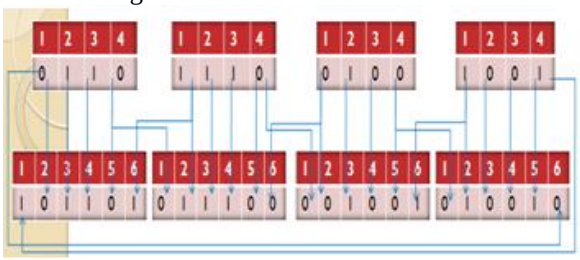
The final Bits value of A1 = 0100
The equivalent decimal value of A1 is 4
In p-box the forth index value is 6
The A1 value is replaced by the binary value of 6, that is 0110
The value of A1 is now 0110

The final Bits value of A2 = 0101
The equivalent decimal value of A2 is 5
In p-box the fifth index value is 14
The A2 value is replaced by the binary value of 14, that is 1110
The value of A2 is now 1110

The final Bits value of A3 = 1000
The equivalent decimal value of A3 is 8
In p-box the eighth index value is 4
The A3 value is replaced by the binary value of 4, that is 0100
The value of A3 is now 0100

The final Bits value of A4 = 0000
The equivalent decimal of A4 is 0
In p-box the zero index value is 9
The A4 value is replaced by the binary value of 9, that is 1001
The value of A4 is now 1001

A1, A2, A3 and A4 is now converted into 6 bits shown in Figure: 8



6 bits representation of A1, A2, A3 and A4
Figure: 8

6 bits representation of A1, A2, A3 and A4 are:
L1 = 101101
L2 = 011100
L3 = 001001
L4 = 010010

2's compliments of each L1, L2, L3 and L4 are:
2's compliments of L1=010011
2's compliments of L2=100100
2's compliments of L3=110111
2's compliments of L4=101110

Concatenating L1 and 2's compliments of L1, L2 and 2's compliments of L2, L3 and 2's compliments of L3, L4 and 2's compliments of L4 we get.
L1 = 101101 010011
L2 = 011100 100100
L3 = 001001 110111
L4 = 010010 101110

To make the proposed technique more complex and secure swapping again between the last six bits of L1 and Last six bits of L3 (which are the 2's compliment part), the last six bits of L2 and Last six bits of L4 (which are the 2's compliment part). After

swapping the new value of L1, L2, L3 and L4 are given below:
L1 = 101101 110111
L2 = 011100 101110
L3 = 001001 010011
L4 = 010010 100100

Binary representation of final 48 bits cipher is L1+L3+L2+L4.

8 bits representation of L1 + L3 + L2 + L4 is:

10110111011100100101001101110010111001001010100

À r S r õ ñ

Final Cipher: **ÀrSrõñ**

Decryption:

Cipher Text is **ÀrSrõñ**

Key R1 = P (Binary form: 01010000)

2 X 8 straight p-box is:

9	8	1	2	6	14	13	7
4	11	0	5	12	10	15	3

The key R1 and Straight p-box have to be known by the receiver for decryption.
The cipher text has to be converted into binary value. Separate 48 bits into 4 segments, so that each segment contains 12 bits value, to get L1, L2, L3 and L4.
L1 = 101101 110111
L2 = 011100 101110
L3 = 001001 010011
L4 = 010010 100100

Last 6 bits of L1, L2, L3 and L4 has to be removed to get new L1, L2, L3 and L4 as
L1 = 101101
L2 = 011100
L3 = 001001
L4 = 010010

First and last bit has to be removed from L1, L2, L3 and L4 and will be called A1, A2, A3 and A4. The value of A1, A2, A3 and A4 will be:
A1 = 0110
A2 = 1110
A3 = 0100
A4 = 1001

Binary value of A1, A2, A3 and A4 is converted into decimal values and the values are 6, 14, 4 and 9 respectively.
6, 14, 4 and 9 are present in straight p-box in the index 4, 5, 8 and 0 respectively. Therefore, the value of A1, A2, A3 and A4 will be:
A1 = 4
A2 = 5
A3 = 8
A4 = 0

The value of A1, A2, A3 and A4 will be converted into binary form and it will be:
A1 = 0100
A2 = 0101
A3 = 1000
A4 = 0000

A1, A2, A3 and A4 are divided into two segments and addressing each segment as 1 and 0 as shown Figure: 9.

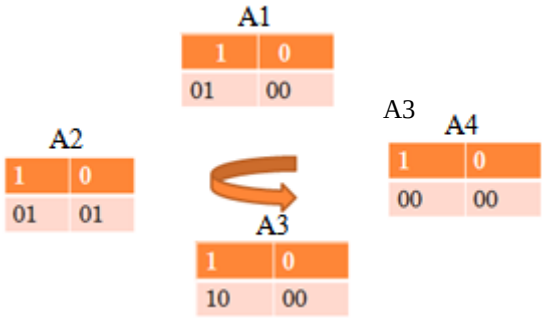


Figure: 9

From the binary value of the key 2 bits has been taken (from left to right. Point to be noted at the time of encryption 2 bits has been taken from right to left) one after another at a time and first swap the bits of 0,1 location of A1 and A4, second swap the bits of 0,1 location of A4 and A3, third swap the bits of 0,0 location of A3 and A2, fourth swap the bits of 0,0 location of A2 and A1 as reverse order of encryption process.

Swapping bits in deferent segment just in the reverse way of encryption process the final bits value of A1, A2, a3 and A4 will be A1 = 0100, A2 = 0100, A3 = 0001 and A4= 0010.

A1 and A3; A2 and A4 has been concatenated and named as p1, p2. The bits value of p1 and p2 will be:
p1 = 01000001
p2 = 01000010

The equivalent decimal number of p1 and p2 will be 65 and 62. The corresponding character

representation of ASCII value of 65 and 66 is A and B.

The plaintext will be **AB**

IV. Computational Complexity

The proposed technique employs only some bits exchange rather than any geometry calculation, thus it lead to low computational complexity. Our proposed methodology depends on three basic operations, like XOR operation, key based bit exchange and P-Box. These three operations computationally linear in nature thus the computational cost is O (N), whereas N is the (total no of bits/2) of any input stream. Hence the proposed algorithm achieves low computational complexity.

V. Conclusive Discussion

The objective of this paper is to facilitate the development of applications that include advanced cryptography through above said technique for secured transmission of the messages [18]. The proposed technique is a symmetric key based algorithm. The straight p-box matrix is introduced to make the technique susceptible from the attacker. Block division process in binary field and swapping in bits confirms the more security of the algorithm. Swapping is totally depends on binary value of input symmetric key. The proposed block division process of input stream and cyclic manner representation with addressing mode of bits of input stream for swapping purpose makes the proposed technique unique.

VI. Future scope

The future of encryption is brighter than ever before. The demand for more control and protection of corporation information assets and third-party information is increasing dramatically [18]. Character frequency distribution in source file and encrypted file has to be performed and analyzed for proposed algorithm. Some testing like non-homogeneity between source and encrypted file, chi-squire value test, has to be done to measure the security of proposed technique with well known existing techniques. Time complexity in terms of comparison of Encryption, decryption time for different category of files with existing algorithm in the market will be performed in future. All above said parametric test will confirm the good security of the proposed algorithm in the present age of global communication system.

References

[1] Abbas Cheddad, Joan Condell, Kevin Curran, and Paul McKevitt. *Digital image steganography: Survey and analysis of current methods*. Signal Processing, 90:727–752, 2010.

[2] F.A.P. Petitcolas, R.J. Anderson, and M.G. Kuhn. *Information hiding: A survey*. Proceedings of IEEE, 87(7):1062{1078, July 1999.

[3] C.I.Podilchuk and E.J.Delp. *Digital watermarking: algorithms and applications*. IEEE Signal Processing Magazine, pages 33, 46, (2001).

[4] Naor, M., And Shamir, *A. Visual Cryptography*. In Advances In Cryptology-Eurocrypto94 (1995), Vol. 950, Springer-Verlag, Pp. 1–12.

[5] Samir, *A. How To Share A Secret*. Communications Of Acm 22, 11 (1979), 612–613.

[6] Herzberg, Amir; Jarecki, Stanislaw; Hugo, Krawczyk; Yung, Moti (1995). *"Proactive Secret Sharing Or: How to Cope With Perpetual Leakage"*. CRYPTO '95: Proceedings of the 15th Annual International Cryptology Conference on Advances in Cryptology (London, UK: Springer-Verlag): 339–352. ISBN 3-540-60221-6. Retrieved June 14, 2010.\

[7] Oded Goldreich, Dana Ron and Madhu Sudan, *Chinese Remaindering with Errors, IEEE Transactions on Information Theory*, Vol. 46, No. 4, July 2000, pages 1330-1338

[8] Sorin Iftene. *General Secret Sharing Based on the Chinese Remainder Theorem with Applications in E-Voting*. Electronic Notes in Theoretical Computer Science (ENTCS). Volume 186, (July 2007). Pages 67–84. Year of Publication: 2007. ISSN:1571-0661.

[9] M. Mignotte. *How to share a secret. In T. Beth, editor, Cryptography-Proceedings of the Workshop on Cryptography*, Burg Feuerstein, 1982, volume 149 of Lecture Notes in Computer Science, pages 371–375. Springer-Verlag, 1983.

[10] C. A. Asmuth and J. Bloom. *A modular approach to key safeguarding*. IEEE Transactions on Information Theory, IT-29(2):208–210, 1983.

[11] M. Ito, A. Saito, and T. Nishizeki. *Secret sharing scheme realizing general accessstructure*. In Proceedings of the IEEE Global Telecommunications Conference, Globecom '87, pages 99–102. IEEE Press, 1987.

[12] J. Benaloh and J. Leichter. *Generalized secret sharing and monotone functions*. InS. Goldwasser, editor, Advanced in Cryptology-CRYPTO' 88, volume 403 of Lecture Notes in Computer Science, pages 27–35. Springer - Verlag, 1989.

[13] E. F. Brickell, ―"*Some ideal secret sharing schemes*", J. Comb, Math.Comb, Comput., vol. 6, 1989, pp. 105-113.
[14] W. A. Jackson, K. M. Martin, and C. M. O'Keefe, -"*On sharing many Secrets*", In Advances in Cryptology-Asiacrypt, Springer-Verlag, 1994, pp 42–54.
[15] C.C. Thien, J.C. Lin, ―"*Secret image sharing*", Computers & Graphics, vol. 26, no. 5, 2002, pp. 765–770.
[16] E. D. Karnin, J. W. Greene and M. E. Hellman, ―*On secret sharing, systems*'' Information Theory, 29(1), 1983, pp.35–41.
[17] J. P. Singh, A. Nag, and T. Bhattacharjee, ―"*Random matrices based image secret sharing*", International Journal of Advanced Research in Computer Science, 2(4), Aug 2011, pp. 104–108.
[18] S. Som, M. Banerjee, "*Cryptographic Technique Using Substitution through Circular Path Followed By Genetic Function*", CCSN-2012, 1st International conference on Computing, Communication and Sensor Network, November 22nd and 23rd, 2012, Roukela, India.

Dr. Subhranil Som received his Master degree in Computer Application in 2003. His PhD in Computer Science and Engineering Technology from University of Kalyani, West Bengal, India in the year of 2012. He is an empanelled PhD supervisor in the area of technology in the West Bengal University of Technology. He is working as a Principal Investigator of an UGC funded project. He holds a distinction in Physics and Mathematics in Graduation. His fields of interest include Cryptography and Network Security, Robotics, Core Java, C++, C. He is currently Asst. Professor in the Department of Computer Application, JIS College of Engineering, West Bengal, India. He was attached with a WHO's International Research Project on "e-Health for Health Care Delivery", University of New South Wales, Sydney, Australia. He has finished several courses related to computer Application, object oriented analysis and design, Software Engineering and Project Management. He has more than 8 years teaching and research experience.

Soumasree Banerjee is pursuing bachelors in Computer Application from JIS College of Engineering under West Bengal University of Technology (WBUT). She has participated in several student paper competitions.

Jhilik Sikdar is pursuing bachelors in Computer Application from JIS College of Engineering under West Bengal University of Technology (WBUT). She has participated in several student paper competitions.