ISSN 2320-9984 03 >
9 772320 998022

Volume 2 Issue 3 | September 2014 ISSN: 2320-9984 (Online)

International Journal of Modern Engineering & Management Research

Website: www.ijmemr.org

Design a Very Highly Avalanched Encryption Technique for Secure Networks

Shikha Patel
Research Scholar
Gyan Ganga College of Technology,
Jabalpur (M.P.) [INDIA]
Email: staishvits@yahoo.co.in

Prof. Papiya Dutta
Head of the Department
Department Electronics and Communication
Gyan Ganga College of Technology,
Jabalpur (M.P.) [INDIA]

Abstract*—The nature of the information that flows throughout modern data communications networks has evolved noticeably since the early years of the first generation systems, when only voice sessions were possible. With moderns networks it is requires to transmit voice and data, also e-mails, pictures and video. The importance of the security is higher in existing data networks than in older systems because users are provided with the systems to fulfil very critical operations like sharing of confidential and important, banking transactions which needs high quality protection. Weaknesses in security architectures allow successful eavesdropping, message tampering and masquerading attacks to occur, with disastrous consequences for end users, companies and other organizations. Encryption is a solution for the issue related to data security but the encryption cannot consider as necessary requirement in data communication and one should try to develop the encryption system very complex so no one can decipher it and it should not consume lots of hardware and time to generate cipher exiting systems are no doubt complex enough but they also requires huge area and significant time. Proposed work can be a better solution through existing data security systems are itself an achievement but it can be more optimised in terms of speed and area, and as speed of encryption gets high it will improve throughput. Proposed paper shows a new approach for achieving highly secure and highly throughput Encryption technique.*

1. INTRODUCTION

The thesis work is an new approach in the encryption area, the motivation behind the work is that Encryption and decryption is an very important requirement now a days but it is not the compulsory requirement for the data communication it is just a important need, the work done in the area till now is itself an achievement and very robust, but it is also an overhead for the system and the hardware and time requires for the encryption and decryption is just a overhead for the system, proposed work is an highly secure encryption techniques for data communication with less amount of hardware and less time, the proposed work is the encryption technique which is less complicated and uses proposed new unique transform encoding, the work will do encryption of analog signals.

Encryption is the conversion of data into a form, called a cipher signal that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood.

The use of encryption/decryption is as old as the art of communication. In wartime, a cipher signal, often incorrectly called a code, can be employed to keep the enemy from

obtaining the contents of transmissions. Signal encryption is facing more and more challenges nowadays. Optical systems are of growing interests for signal encryption because of their distinct advantages of processing two dimensional complex data in parallel and at high speed. In the past decade, a number of optical encryption methods have been proposed. Among them, the most widely used and highly successful optical encryption scheme is double random phase encoding proposed by. This method uses two random phase masks, one in the input plane and the other in the Fourier plane, to encrypt the primary data into stationary white noise. As the generalization of the conventional Fourier transform, the fractional Fourier transform (FRFT) has recently shown its potential in the field of optical security.

2. OBJECTIVE

- To encrypt and decrypt signal by proposed new encryption architecture and to compute Mean square error and signal to noise ratio.
- To compare our results with existing work in this area
- To do literature survey and go through every specific technical aspects of related work.
- To design optimized feasible module on MATLAB Tool and verify the results.

3. METHODOLOGY

The original idea for the work is to design an very much secure and fast encryption of a signal in analog domain itself because if we go for the digital domain it requires undesired A/D and D/A conversion for the encryption and decryption Our proposed concept is to have a unique key of 64 bit length and to generate a unique filter equation from it let say if X is our key and the.

The arrangement of key as a matrix is show below it will be diagonally serpentine in below if key is

Key==

1010100111010011111110101110100001011101
0111101111011101111101001

$$X = \begin{matrix} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{matrix}$$

The C_k coefficient generation

$C_k = x(p,1) + x(p+(-1)^k,2) + x(p,3) + x(p+1,4) + x(p+1,5) + x(p+1,6) + x(p+1,7) + x(p+1,8)$

Where

p = 1 when k=0

& p=2 when k=1

p = 3 when k=2

& p=4 when k=3

p = 5 when k=2

& p=6 when k=5

p = 7 when k=2 & p=8 when k=7

$C_0=x(1,1)+x(2,2)+x(1,3)+x(2,4)+x(1,5)+x(2,6)+ x(1,7)+x(2,8)$

$C_1=x(2,1)+x(1,2)+x(2,3)+x(1,4)+x(2,5)+x(1,6)+ x(2,7)+x(1,8)$

$C_2=x(3,1)+x(4,2)+x(3,3)+x(4,4)+x(3,5)+x(4,6)+ x(3,7)+x(4,8)$

$C_3=x(4,1)+x(3,2)+x(4,3)+x(3,4)+x(4,5)+x(3,6)+ x(4,7)+x(3,8)$

$C_4=x(5,1)+x(6,2)+x(5,3) +x(6,4)+x(5,5)+x(6,6)+ x(5,7)+x(6,8)$

$C_5=x(6,1)+x(5,2)+x(6,3)+x(5,4)+x(6,5)+x(5,6)+ x(6,7)+x(5,8)$

$C_6=x(7,1)+x(8,2)+x(7,3)+x(8,4)+x(7,5)+x(8,6)+ x(7,7)+x(8,8)$

$C_7=x(8,1)+x(7,2)+x(8,3)+x(7,4)+x(8,5)+x(7,6)+ x(8,7)+x(7,8)$

The C_k parameters explained above will be computed when input signal with no phase shift appears. The formula for generating C_k will get changed as phase change.

The concept is that as per the input signal appearance the computation of parameters of systems will get changed in that case the intruder needs to know both first the 64 bit key and phase of the signal. As 2^64 possible combination intruder need to try to decipher the data along with proper phase.

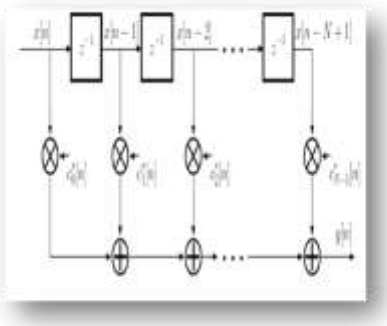
In a transversal filter of length N, as depicted in fig. 1, at each time n the output sample y[n] is computed by a weighted sum of the current and delayed input samples x[n], x[n − 1], . . .

Here, the $c_k[n]$ are time dependent filter coefficients (we use the complex conjugated coefficients $c_k[n]$ so that the derivation of the adaption algorithm is valid for complex signals, too). This equation re-written in vector form, using x[n] = [x[n], x[n − 1], . . ., x[n − N + 1]]^T, the tap-input vector at time n, and c[n] =[c0[n], c1[n], . . ., cN−1[n]]^T, the coefficient vector at time n, is

$$y[n] = c^H[n]x[n]$$

Both x[n] and c[n] are column vectors of length N, $c^H[n]$ = (c*)T [n] is the hermitian of vector c[n] (each element is conjugated *, and the column vector is transposed ^{T} into a row vector).As explained above the difference equation of the system is been designed as per the key and it will consider as cipher system.

$$y(n)==x(n)c^H(n)$$
FT
$$y(k)=x(k).c^H(k)$$
$$x(k)=inv(c^H(k)).y(k)$$
IFT



x(n)

Figure1: Transversal filter

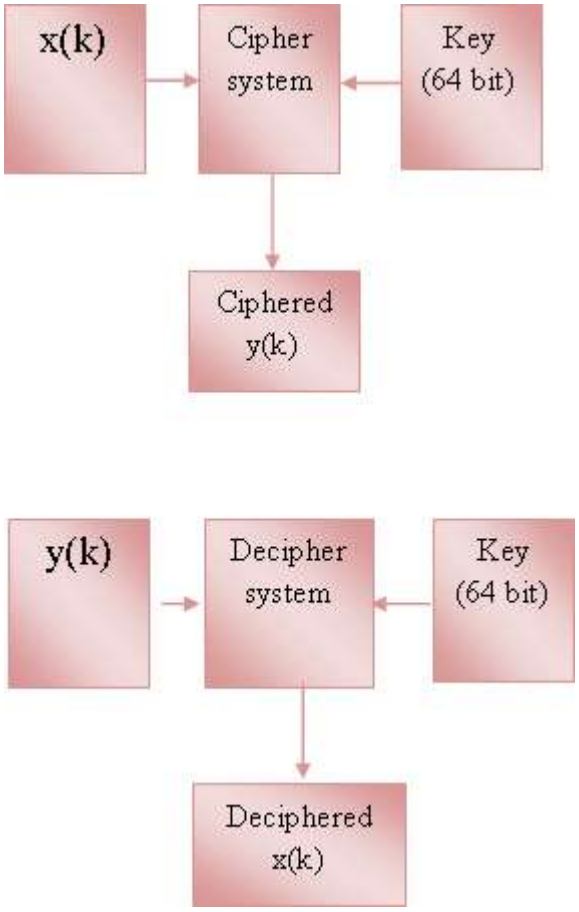


Figure 2: proposed method flow

4. EXPECTED OUTCOMES

As known for cryptography or steganography the performance parameter are SNR (signal to noise ratio), MSE (mean Square Error) and avalanche in data, avalanche is the data change from original data to cipher data. As proposed work is a 64 bit cipher so proposed work is expecting to achieve SNR in range of 85-90 which will be 5-8% better than reference [1] and also expecting MSE in range of 0.05-0.08 which will be less than reference [1] and [2].proposed work is expecting all this resulting while maintaining avalanche of 45 bit change or more.

5. CONCLUSION

One can conclude on behalf of literature survey for which we have gone through many research papers, books, Datasheets of EDA tools and references mansion in this paper that proposed work is a better cryptograph method in terms of area and throughput, as known

cryptography is just a overhead for any system and it should not took lots of area or time so proposed work can be solution for the same as proposed work will requires very less area and time as compare to other existing work in the same research area.

REFERENCES:

[1] Yang Fengxia, Computer Department Cangzhou Normal University, DCT Domain Color Image Block Encryption Algorithm based on Three -dimension Arnold Mappin, 2013 International Conference on Computational and Information Sciences, IEEE

[2] Anjali Dadhich, Abhishek Gupta, Surendra Yadav, Swarm Intelligence based Linear Cryptanalysis of Four-round Data Encryption Standard Algorithm, 978-1-4799-2900-9/14/2014 IEEE

[3] Aditya Goel and Anand Agrawal, Fresnel Transform Encoding of Time-Varying Signals of WDM Systems, Research India Publications, Advances in Wireless and Mobile Communications, ISSN 0973-6972 Volume 4, Number 1 (2011), pp. 71–80

[4] 'Wavelength-division multiplexing Fresnel transform encoding of time-varying signals,'' Christian Cuadrado -Laborde and Ricardo Duchowicz, 'Opt. Lett. 54(8), 5442-5444 (2008)

[5] "Time-variant signal encryption by lensless dual random phase encoding applied to fiber optic links," C. Cuadrado-Laborde, Opt. Lett. 32(19), 2867–2869 (2007)

[6] "Spread-space spread spectrum technique for secure multiplexing," B. M. Hennelly, T. J. Naughton, J. McDonald, J. T. Sheridan, G. Unnikrishnan, D. P. Kelly, and B. Javidi, Opt. Lett. 32(9), 1060– 1062 (2007).

[7] "Optical color image encryption by wavelength multiplexing and lensless Fresnel transform holograms,", L. Chen and D. Zhao, Opt. Express 14 (19), 8552–8560 (2006).

[8] "Ultrafast optical signal processing based upon space-time dualities," J. van Howe and C. Xu, J. Light wave Technol. 24(7), 2649–2662 (2006).