IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

IMAGE ENCRYPTION USING SECURE FORCE ALGORITHM WITH AFFINE TRANSFORM FOR WSN

P.Lakshmi Sowjanya*, K.J.Silva Lorraine
*PG Student,Dept.of.ECE,Sir C R Reddy college of Engineering, Eluru, India
Assistant Professor,Dept.of.ECE,Sir C R Reddy College of Engineering, Eluru, India

DOI: 10.5281/zenodo.59669

ABSTRACT

With the ever increasing growth of multimedia applications,security is an important issue in communication and storage of images. Encryption is one of the ways to ensure security.Image encryption techniques try to convert original image to another image that is hard to understand. There are various techniques which are discovered from time to time to ecrypt the images to make images more secure like Key Generation using Genetic algorithm,Secure force algorithm,Block based transformation algorithm etc. In this paper,a low complexity symmetric cryptographic algorithm denoted as Secure Force With Affine Transform has been proposed. The encryption part can be implemented by using simple architecture that only consists of basic mathematical operations (AND, OR,XOR,XNOR,SHIFTING,SWAPPING).This can help to reduce the burden on encoder,because the more complex key expansion process is only carried out at the decoder. The objective of this paper is to perform security analysis and performance evaluation of the proposed algorithm. Results of the proposed algorithm have been tested upon different kinds of images and comparitive analysis with other techniques has been presented.

KEYWORDS: Cryptography;Symmetric key;Key management protocol;Affine transform.

INTRODUCTION

Security of data (image) to maintain it's confidentiality,proper access control,integrity and availability is a major issue in data communication as soon as a sensitive message was etched on a clay tablet or drawn on the royal wall,then it must have been foremost in the sender's mind that the information should not get intercepted and read by a rival. The exchange of data among two potential parties must be done in a secure method so as to avoid tampering. The unintended user who may try to overhear this conversation can either tamper with this information to change it's original meaning or it can try to listen to the message with intension to decode it to use his/her advantage. Both these attacks violated the confidentiality and integrity of the data passed.Providing intended access and avoiding unintended access is a very challenging task. Cryptography is one of the major data hiding techniques[1,2]. Crypt means "hidden or secret" and graphien means "writing" .The term has been derived from Greek language. Cryptography is an art of transforming data into unreadable format called cipher text[3,4]. The receivers at the other side,deciphers or decrypt the data into plain text. Cryptography provides data confidentiality,data integrity and authentication.Cryptography technique needs some algorithm for encryption of data. There are various techniques which are discovered from time to time to encrypt the image to make them more secure. This paper presents an algorithm for encryption which is called as Secure force(SF) algorithm with affine transform.

SECURE FORCE ALGORITHM

The design of SF algorithm provides a low complexity architecture for implementation in wireless sensor network(WSN)[5,6]. To improve the energy efficiency,the encryption process consists of only five encryption rounds.It has been suggested by E.Biham and A.Shamir that a lower number of encryption rounds will results less power consumption. In order to enhance the security,each operation will be done only on 4 bit data (designed to be compatable with 8 bit computing devices for WSNs).This is to create enough confusion and diffusion of data to encounter different types of attacks.

As shown fig.1 the Key expansion process, which involves complex mathematical operations (Multiplications,Permutations,Transposition and Rotation) to generate keys for the encryption process is implemented at the decoder. This shifted the computational burden to the decoder and indirectly,this will helps to increase the lifespan of the sensor nodes.However,the generated keys must be transmitted securely to the encoder for the enctyption process. In this case,the LEAP(Localised Encryption and Authentication Protocol)[7] is adopted. It is an energy efficient,robust and secure key management protocol that is designed for the WSN.

The encryption process is initiated once the keys generated by the key expansion block are securely received by the encoder through the secure communication channel created by using LEAP protocol. The decryption process is just the reverse procedure of the encryption process.

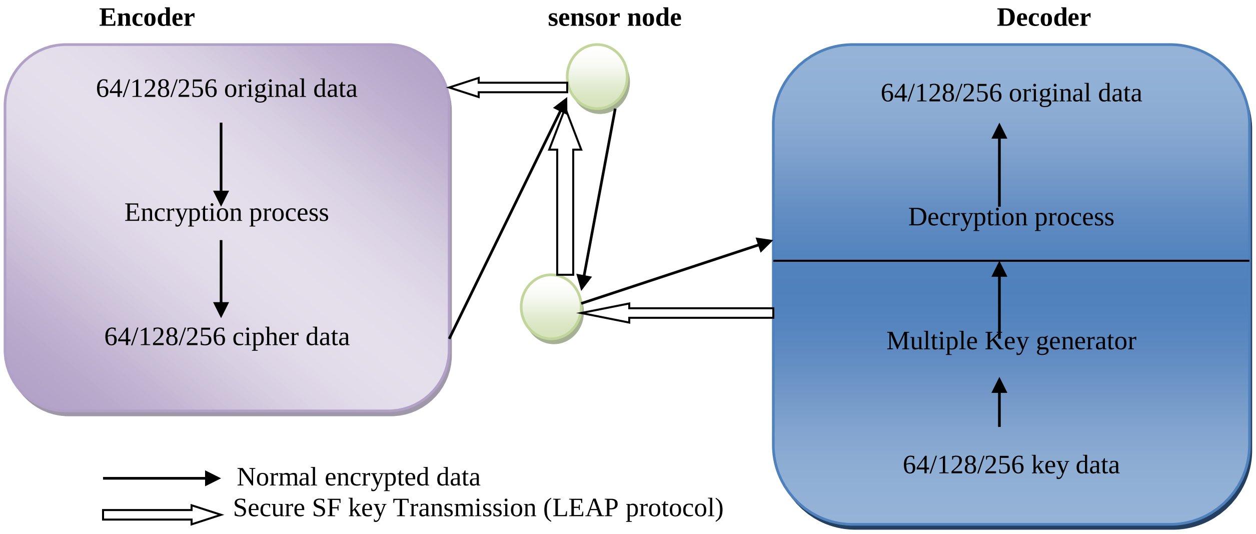

Fig.1 System flow of SF

AFFINE TRANSFORMATION

Affine transformation is a linear mapping method that preserves points,straight lines,and planes. Sets of parallel lines remain parallel after an encryption transformation. The affine transformation technique is typically used to correct for geometric distortions or deformations that occur with non-ideal camera angles.

$$x' = (K0 + K1 * x) \bmod N \quad (1)$$

$$y' = (K2 + K3 * y) \bmod N \quad (2)$$

Where (x,y) is old points of pixel
(x’,y’) is new point of pixel and K0,K1,K2,K3 are keys
N is used as length and width of the image

The old point pixel and new point poixel are swapped. The formula is used for all the pixels. There are four basic types of affine transformation

- Translate: Moves a set of point a fixed distance in x and y
- Scale: Scales a set of points up or down in the x and y directions
- Rotate: Rotates a set of points about the origin
- Shear: Offsets a set of points a distance proportional to their x and y coordinates

PROPOSED ALGORITHM

The process of the proposed Secure force algorithm with affine transform consists of 5 major blocks.
Step1:Key expansion
Step2:Key management protocol
Step3:Apply affine transformation to the original image

Step4:Encrypt the transformed image usig SF algorithm
Step5:Decryption

Key expansion:

The input cipher key is a linear array of 64 bits, which is divided into four halfs of 16 bits. Each 16 bit is arranged into a 4*4 matrix row wise on which left shift(LS) operation is applied. The resultant is then arranged in a 4*4 matrix column wise and logical operations (XOR,XNOR) are then performed. The output results of these operations are combined to form a 64 bit linear array.

The obtained 64 bits are then passed through P-table and arranged in 4*4 matrix row wise on which left shift operation is performed later. The left shift matrix is then multiplied with a fix matrix (FM) that transforms the 16 bits data into 64 bits. The transformed 64 bits are then arranged row wise and left shift is perfomed on it. Each left shifted 64 bits are then divided into four column-wise 16 bits blocks on which AND & XOR operations are performed to transfer them to a single 16 bits block. Now the generated 16 blocks are further subdivided into 4 bits arranged column-wise and XOR operation is applied to produce the 4 bit keys. These keys are used by substitution and tansposition techniques on the 16 bit blocks to produce 4 sub keys (K1,K2,K3,K4) of 16 bits that will be used in the first four encryption rounds. The fifth sub key (K5) is generated by XOR the four sub keys and will be used in the fifth encryption round.

Key management protocol:

The LEAP [7] key management protocol works in such way that it first uses the pre-distribution key to help establish and update all the four types of keys for each node. The individual key is first established by using a seed function and node ID. Then a neighbour detection process is initiated for the pair wise shared key phase,to broadcast the respective node IDs. The receiving node will calculate the shared key among it all of its neighbouring nodes by using the seed function and initial key. Later,the initial and any intermediate keys generated are erased. Once pair wise keys are established,the cluster key is distributed by the cluster head using pairwise communication secured with the pair wise secured key.Finally,the base station will broadcast the group key. In order to prevent a compramising nodefrom imitating as the base station during the broadcasting,an authentication mechanism denoted a µTESLA is used.

Once all the keys are generated and established,a secure communication channel is created in between the sender and receiver nodes in WSN,and then it can be used for the secure transmission of encryption keys.

Affine transformation:

Apply the affine transformation to the original image which is to be sent.

Encrypt the transformed image using SF algorithm:

Once the keys generated by the key expansion block are securely received by the encoder through secure communication channel created by using LEAP protocol. In the encryption process, simple operations which include AND,OR,XOR,XNOR,left shit,substitution (S-boxes) and swapping operations, performed to create confusion and diffusion.

The plain text is a linear array of 64 bits,which is divided into two halfs of 32 bits and each 32 bit half is further subdivided into two halfs of 16 bits. In each rounds swappimg of 16 bits blocks are performed. The major purpose of this function is to change the original position of data to get more complex cipher. Subkeys (K1,K2,K3,K4,K5) are XNOR with the left and right half of each round respectively.

The output of each round becomes the input of next round as well as it is mapped with the F-function. It involves substitution,AND,OR and left shift operation.

$$F=OR(S\text{-}boxes(AND(LS(16\ bits/4)))) \quad (3)$$

F-function is the major element of encryption algorithm that induces diffusion of data. It performs S-boxes, AND &OR operations and left shifting operations on 16 bits of data. The output from the F-function is XOR with the swapped 16 bits of the same round resulting in confuson of data. This brings the end to the encryption process.

Decryption:

The decryption is just reversed procedure of the encryption process.

ISSN: 2277-9655
Impact Factor: 4.116

SIMULATION RESULTS

The performance of the proposed technique can be evaluated by using histogram, MSE and PSNR parameters.

Histogram:

Histogram is a graphical representation of data. It is the estimation probable distribution of a continuous variable. Histogram is used to plot the density of data.

Mean square error(MSE):

MSE is one of the most commonly used measures of the avalanche effect. It is the average squared difference between two images. It is computed pixel-by-pixel as follows

$$MSE = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \left[I(i,j) - K(i,j) \right]^2 \tag{4}$$

Where I and K are two cipher text images with keys differ by one bit. M and N are the dimensions of the images, i and j are pixel positions with in the images. The MSE should be less then we will get more secure image. This proposed algorithm will give less MSE.

PSNR(Peak Signal to Noise Ratio):

PSNR is defined as the ratio of significant signal information to noise. It shows quality measure of an encryption technique.

$$PSNR = 10 \log_{10} \left(\frac{MAX_1^2}{MSE} \right) \tag{5}$$

Here, MAX$_1$ is the maximum possible pixel value of the image. Better PSNR value gives the better performance.

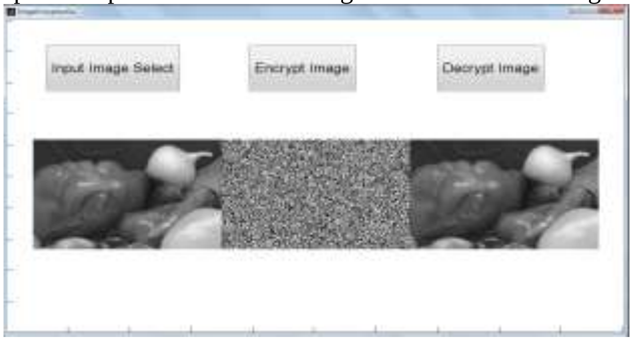

Fig.2.Encryption and decryption of onion image using Key generation algorithm

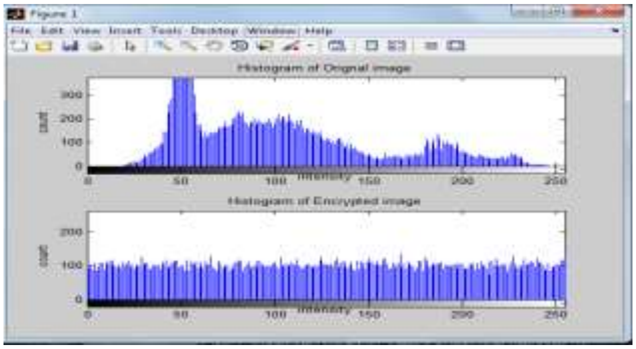

Fig.3.Histogram of original and encrypted image of onion image using Key generation algorithm

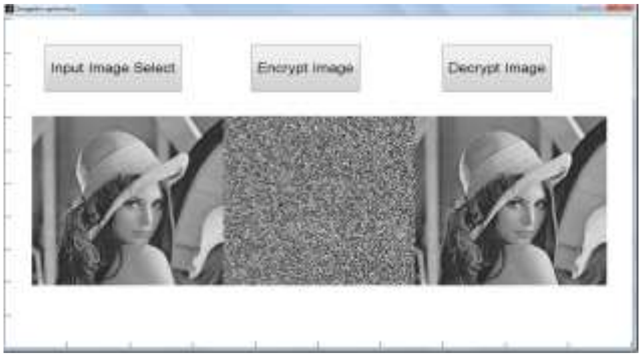

Fig.4.Encryption and decryption of Lena image using Key generation algorithm

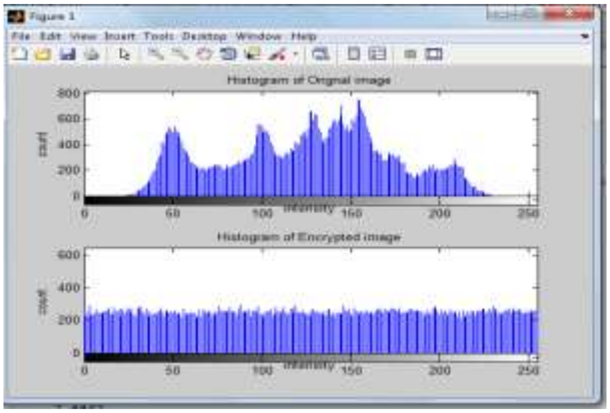

Fig.5.Histogram of original and encrypted image of lena image using Key generation algorithm

Fig.2 and Fig.4 shows the encryption and decryption of Onion and Lena images using Key generation algorithm where as Fig.3 and Fig.5 shows the histogram of Onion and Lena images.

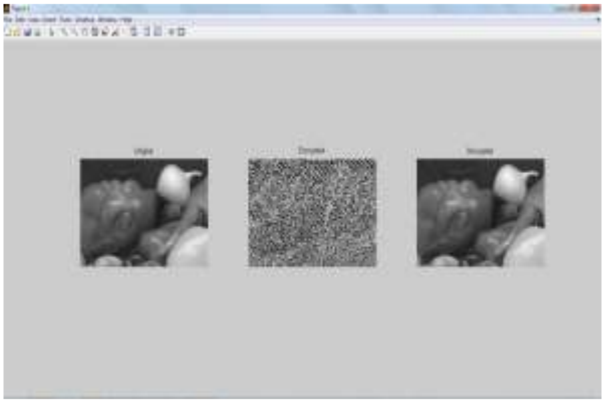

Fig.6.Encryption and decryption of onion image using SF algoritm

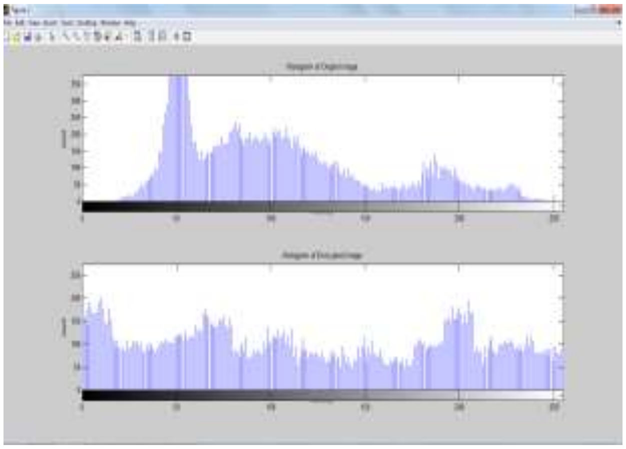

Fig.7.Histogram of original and encrypted image of onion image using SF algorithm

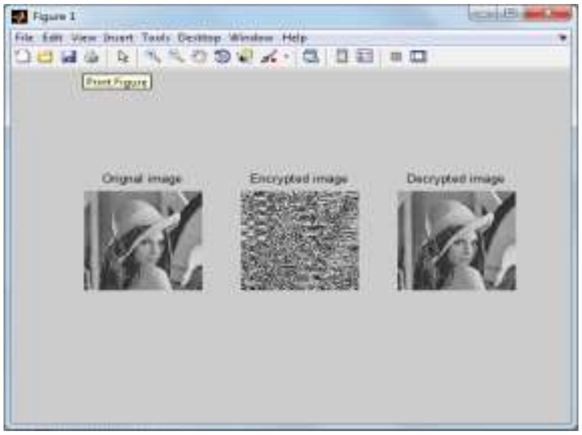

Fig.8.Encryption and decryption of Lena image using SF algorithm

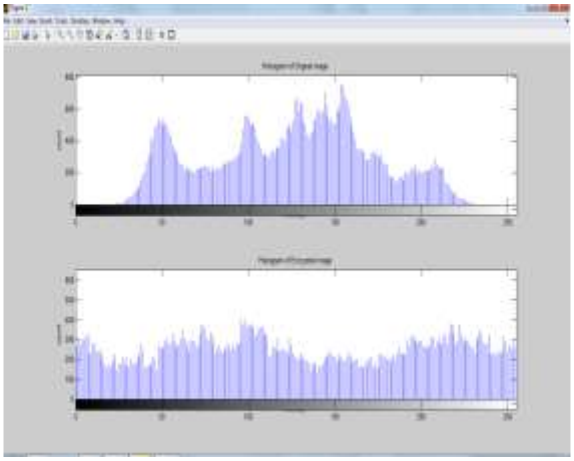

Fig.9.Histogram of original and encrypted image of onion image using SF algorithm

Fig.6 and Fig.8 shows the encryption and decryption of Onion and Lena images using SF algorithm where as Fig.7and Fig.9 shows the histogram of Onion and Lena images.

Using Proposed Algorithm:

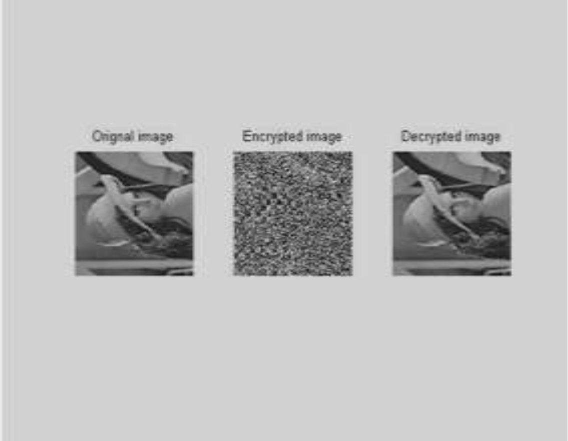

Fig.10.Encryption and decryption of Lena image using proposed algorithm

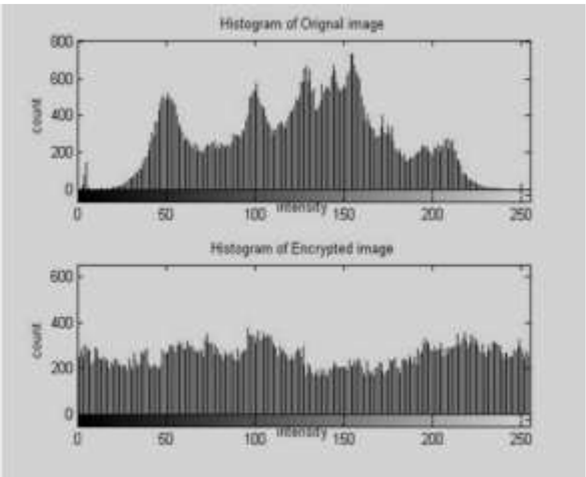

Fig.11.Histogram of original and encrypted image of lena image using proposed algorithm

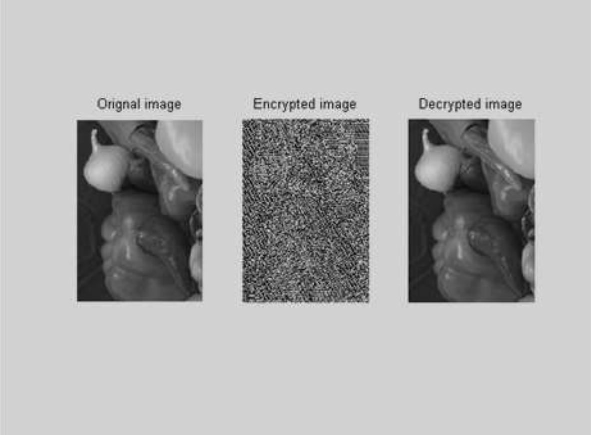

Fig.12.Encryption and decryption of onion image using proposed algorithm

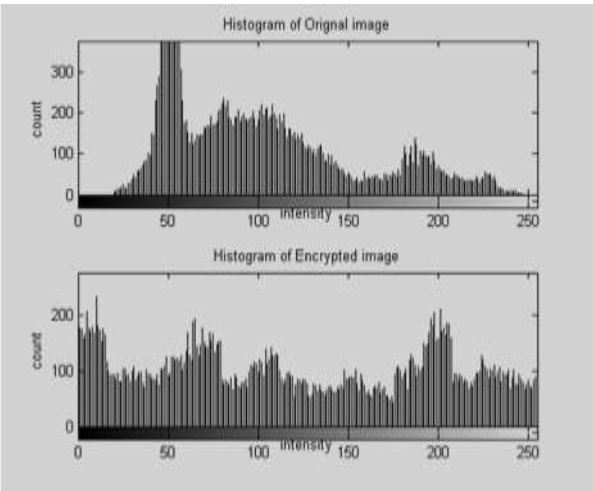

Fig.13.Histogram of original and encrypted image of onion image using proposed algorithm

Fig.10 and Fig.12 shows the encryption and decryption of Onion and Lena images using proposed algorithm where as Fig.11 and Fig.13 shows the histogram of Onion and Lena images.

Table 1 gives the comparitive analysis of the proposed algorithm with the existing algorithms like SF and key generation. It can be observed that the proposed algorithm yields better PSNR and less MSE values. For Lena image by using proposed algorithm PSNR has found to be 11.6490 and MSE 4.4482e+003. For Onion image, PSNR is 9.2520 and MSE 7.7247e+003.

Table 1. Comparitive Analysis

Image	Algorithm	MSE	PSNR
Lena	Key generation with genetic algorithm	6.2162e+003	10.1955
	Secure force	5.4149e+003	10.7949
	Proposed algorithm	**4.4482e+003**	**11.6490**
Onion	Key generation with genetic algorithm	8.4894e+003	8.8420
	Secure force	8.4911e+003	8.8412
	Proposed algorithm	**7.7247e+003**	**9.2520**

CONCLUSION

The evaluation of encryption is moving towards a future of endless possibilities. The image data have special properties such as bulk capability,high redundancy and high correlation among the pixels. Encryption techniques are very useful tools to protect secret information. Everyday new encryption technique is evolving, each technique is unique in its own way,which might be suitable for different applications. So there is need of better algorithm. At present times where major communication is done wireless using internetwork to transfer data. So, major concerns are regarding the security of such personal or nations defence data. In this paper, analysis of the proposed algorithm based on different parameters has been done. By comparing the results it can be concluded that the proposed algorithm will give better performance.

REFERENCES

[1] S. R. Z. Li and G. Gong, “A survey on security in wireless sensor networks”, Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario, Canada, 2008.

[2] K. Sharma, M.K. Ghose, D. Kumar, R.P.K. Singh, and V.K. Pandey “A comparative study of various security approaches used in wireless sensor networks” CSE, International Journal of Advanced Science and Technology Vol. 1 17777, April, 2010.

[3] Perrig, R. Szewczyk, J. Tygar, V. Wen, and D. Culler, “Spins: security protocols for sensor networks”. ACM/Kluwer Wireless Networks, 8(5):521–534, 2002.

[4] Karlof, N. Sastry, and D. Wagner. TinySec: A link layer security architecture for wireless sensor networks. In Proc. Of the 2nd ACM SenSys, 2004.

[5] G.F Piret, “Block Ciphers: Security Proofs, Cryptanalysis, design, and fault attacks”, Ph.D. Thesis, Universite' Catholique de Louvain (UCL), January 2005.

[6] E. Biham and A. Shamir, “Differential cryptanalysis of data encryption standard”. Berlin, Germany: SpringerVerlag, 1993. R. Chandramouli, S. Bapatla, and K. P. Subbalakshmi, “Battery power-aware encryption”, ACM Transactions on Information and System Security, Vol. 9, No. 2, May 2006, , pp. 162–180.

[7] S. Zhu, S.Setia,, S. Jajodia, “LEAP: Effcient security mechanisms for large scale distributed sensor networks”. In Proc. of the 10th ACM Conf. on Computer and Communications Security. Washington DC USA, (2003), pp. 62-72.