Journal of Telematics and Informatics (JTI)
Vol.3, No.2, September 2015, pp. 27~33
ISSN: 2303-3703

Ortho Linear Feedback Shift Register Cryptographic System

T Narendra Babu, D L Pravallika Kaja*, B mounika, K Tejaswi, Y Harish
Departement of Electronics and Computer Engineering, K L University
Guntur, Andhra Pradesh, India

*Corresponding author, email: kaja.pravallika@gmail.com

Abstract

In this article, an encryption algorithm with an error detection technique is presented for highly secured reliable data transmission over unreliable communication channels. In this algorithm, an input data is mapped into orthogonal code first. After that the code is encrypted with the help of Linear Feedback Shift Register (LFSR). The technique has been successfully verified and synthesized using Xilinx by Spartan-3E FPGA. The results show that the error detection rate has been increased to 100% by proposed encryption scheme is effective and improves bandwidth efficiency.

Keywords*: Encryption, LFSR, Orthogonal code, FPGA*

INTRODUCTION

A. Cryptography

Cryptography is a process of transmitting stored data in a particular form i.e. ciphers text where only the permitted person can access it. Simply we can say that it is the process of securing data by scrambling into an incomprehensible arrangement, called cipher text (encryption). Just the individuals who have a secret key can decode the message into plain content (decryption). Encryption can be defined as changing the original message into other form which can be again retained by using the key. Decryption is the process of converting cipher text back to plaintext. The originator of a encrypted message imparted the decoding procedure expected to recoup the first data just with proposed beneficiaries, accordingly blocking undesirable persons to do similar. Encoded messages can here and there be broken by cryptanalysis, likewise called code breaking. Cryptographers are the name given to those who practice this type of cryptographic system.

Cryptography concerns mainly with four characteristics they are confidentiality, integrity, non repudiation, authentication. Only those systems and protocols which satisfy all the above mentioned characteristics are known as cryptosystems. Cryptosystems are often thought to refer only to mathematical procedures and computer programs. Cryptosystems are classified into two categories they are symmetric key and asymmetric key or public key cryptographic systems.

Symmetric key can be briefed as an encryption method which has only one key which is shared only between the sender and receiver. Block ciphers or stream ciphers are the ways to be implemented in this type of system.. A block cipher enciphers input in blocks of plaintext , the input form used by a stream cipher.

Public key cryptography can be briefed as an encryption technique where two keys are present in this system. One is the public key which is shared along with the message and other is the private key which is shared only between sender and receiver. Only when both the keys are used the original message can be obtained.

B. Error Detection codes

Error detection and correction or error control are the methods that enhance the secured delivery of digital data over unsecured communication channels . In the field of information theory and coding where the applications of computer science and telecommunications play an important role in using these error detection techniques. During transmission most of the communication channels add on to some additional data to the original data which is predominantly known as noise. Due to this many unwanted data or errors occur

during the transmission of data from sender to receiver. In order to limit this problem we have error detection and correction techniques. The error detecting method is used to detect that particular error while the error correction methods are used to reconstruct the original data.
Generally the definition of these terms is given below

Error detection is defined as the method of detecting the errors which are caused due to external noise or any other sources Error correction is defined as the method of reconstructing the original data and transmit the error free data to the receiver.

Other reasons such as noise and cross talk etc…combine to the corruption of original data. Top layers of the network architecture are expected to have error free error free transmissions between systems. Most of the applications does not work as expected due to the presence of errors but, some of the audio and video files are not effected even though errors are present. Errors are most commonly identified by using hash functions. These functions provides an additional function at the received end so that the user can use that particular information to know that the original message has occurred or not by checking the length of the data. One of such example is the cyclic redundancy which checks the performance in detecting burst errors.

The various types of error detection methods are parity check which is used for short messages and is performed by using the number of 1's used in the message. Secondly comes the block sum check which enables the user to check the information in given memories by using vertical and horizontal parities are formed. Next comes the cyclic redundancy code which are used for long messages. There are some other different methods where the error detection and correction both come in the same technique. Convolution codes ,Hamming codes , Goley are of this type. In this paper we have used the orthogonal code in order to increase the reliability of the original message which converts the length of the input bits and the is encrypted to the desired cipher text.

DESIGN METHODOLOGY:

Since LFSR generates pseudo random numbers where each number is used to encrypt the a-bit input data. Our approach is not only to encrypt the input data but also to encode the data before the encrypting into orthogonal code. Once the input data is encoded, the encoded data is xor'd with the random number generated by LFSR method. This following approach is to improve the error detection rate by increasing its reliability. Orthogonal code technique involves major blocks i.e. transmitter and receiver which are described below.

Transmitter:

An encoder, encryptor and a shift register all the three blocks combine to form the basic transmitter in this method. The output of encoder is set to $n=2^{a-1}$ bits where the input is a-bit data which is fed to the encoder. This 2^{a-1} bit data is sent to the encryptor where it is xor'd with the pseudo random number generated by the LFSR. In order to transmit this code need to be changed as a serial. For this transformation we use the shift register as shown in the fig. Thus by using raising edge of the clock pulse the generated cipher text is transmitted using the shift register.

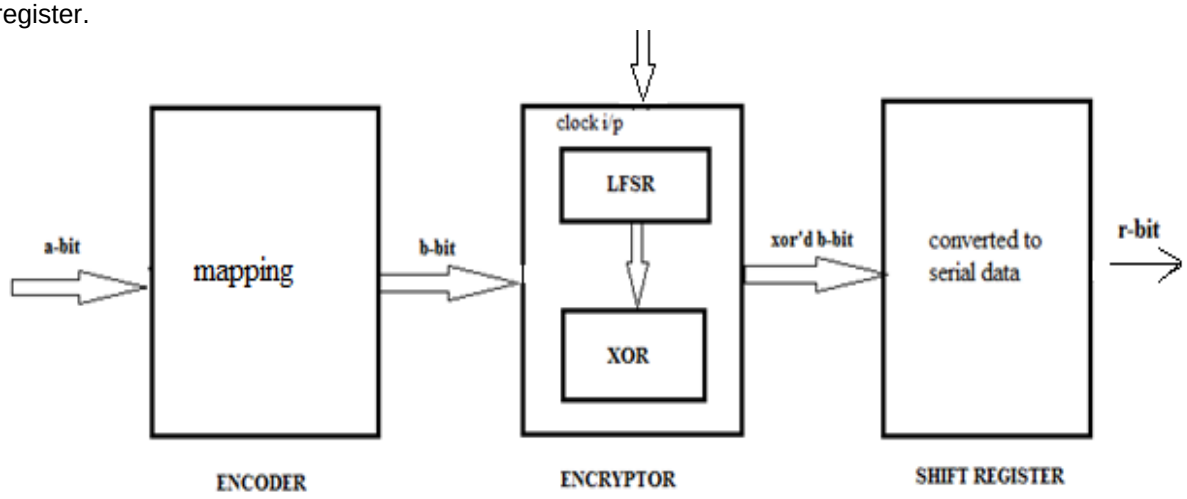

Fig represents the block diagram of transmitter

Receiver:

The inverse arrangement of the transmitter acts as a receiver i.e. a shift register, decryptor and a decoder combine to form the basic receiver component.

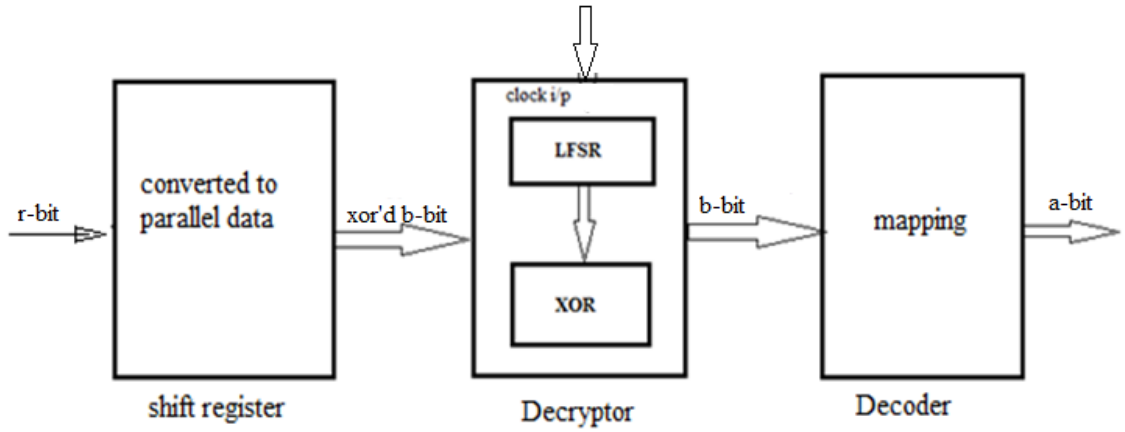

fig represents block diagram of receiver

Related Work

Xuanxia yao and Zhi Chenproposed the technique used is a lightweight no-pairing ABE scheme based on elliptic curve cryptography (ECC) is proposed to address the security and privacy issues in IoT. A Non-adaptive Partial Encryption of Gray scale Images Based on Chaos has been proposed by Sukalyan som and Sayanisen.We decompose the original gray scale image into its corresponding binary eight bit planes then encrypted using couple tent map based pseudorandom binary number generator. A trusted third party based encryption scheme for ensuring data confidentiality in cloud environment by yed Rizvi, Katie Cover, Christopher Gates proposed a new scheme capable to secure client information from both inside and outside threats. In particular, they developed an encryption scheme by combining both symmetric and asymmetric cryptographic algorithms.

Marius Iulian and Mihailescu came out with the technique used is to create a strong and unique authentication process of the biometric templates and to guarantee the safety of the biometric data . Hossein Rahmani proposed the technique used is to create , XaaS concept, we design an Encryption as a Service in order to get rid of the security risks of cloud provider's encryption and the inefficiency of client-side encryption. Gilles Brassard proposed the technique used is to create a radically different foundation for cryptography, . the uncertainty principle of quantum physics. In conventional information theory and cryptography.

Orthogonal codes have equal number of one's and zero's and are binary valued. A k-bit orthogonal code has k/2 1's and k/2 0's; i.e., there are k/2 positions where 1's and 0's are differed. Hence zero parity is generated by all the orthogonal codes.. It has 8-orthogonal codes and 8 -antipodal codes for a total of 16-biorthogonal codes. The inverse of these orthogonal codes gives the antipodal codes; and are orthogonal among them. Since there is an equal number of 1's and 0's, each orthogonal code will generate a zero parity bit. Therefore, each antipodal code will also generate a zero parity bit. Therefore, if there is a transmission error, the receiver will be able to detect it by generating a parity bit at the receiving end. Before transmission a k-bit data set is mapped into a unique n-bit. For example, a 4-bit data set is represented by a unique 8-bit orthogonal code which is transmitted without the parity bit. When received, the data are decoded based on code correlation. It can be done by setting a threshold midway between two orthogonal codes.

IMPLEMENTATION AND RESULTS

In Order to test the code an ISE Xilinx software and a hardware board of Spartan-3 were used. Modelsim XE software is used to perform simulation. The output of the simulation or the final results are checked for most of the 5-bit combinations of input and 16-bit orthogonal

code. The process of software simulation along with the working of clock cycles is briefed further for both transmitter and receiver.

TRANSMITTER

The internal process of transmitter and the simulation results can be observed in fig.3. The 5-bit t_data input signal for the encoder is 01001 where the orthogonal code works on it and a 16-bit output i.e. n=5 orthogonal code output 2^(n-1) = 2^(4)= 16 is obtained. The t_ortho signal as shown in the fig represents the output of the encoder “aaaaH” (1010101010101010) which is fed as input to the encrypter. The output of the encrypter t_out “aaabH” is obtained for the respective input. To enable the transmission of serial bit data reset signal is used for every rising edge of the clock.

RECIEVER

Once the data is obtained at the receiver the serial data is transformed into parallel data. The r_data signal represents this input signal of receiver as shown in fig. This data is decrypted and an orthogonal code is obtained which is represented by r_ortho signal . This data acts as a input to the decoder unit. A counter variable is used which counts the number of 1’s in the result obtained when the received code is XOR’d with all the possible combinations of orthogonal code. The original data is obtained by checking the minimum count of the received data. There would be 4 cases for all the simulation results available. In the first case the received data r_data=1010101010101011 has the correct match in the look up table hence count =0 as shown in the figure. There by we can understand that the input data is not in correct and the final data obtained is “01001” which is represented by t_out signal as shown in the fig.

In the second case the r_data= 1000101010101011 is obtained as input for the encrypter and there is no match in the look up table and hence the closest match is to be found for that particular input which reveals there is an error in the message. The related orthogonal code r_ortho = “8aac” and the count value is r_count= “00010”. The closest match is obtained and finally the r_out = “00010” is obtained.

In the third case the r_data= 1001101010101011 is obtained as input for the encrypter and there is no match in the look up table and hence the closest match is to be found for that particular input which reveals there is an error in the message. The related orthogonal code r_ortho = “8aab” and the count value is r_count= “00011”. The closest match is obtained and finally the r_out = “00010” is obtained.

In the fourth case the r_data= 1001110010101011 is obtained as input. But there is no closest match obtained for the respective orthogonal code and the count value is more than the number of errors produced. In this case the output is not obtained and the r_req goes high which requests the sender to resend the message.(crypt analysis)(time slides-timing constants)(future work-to maintain constant time)

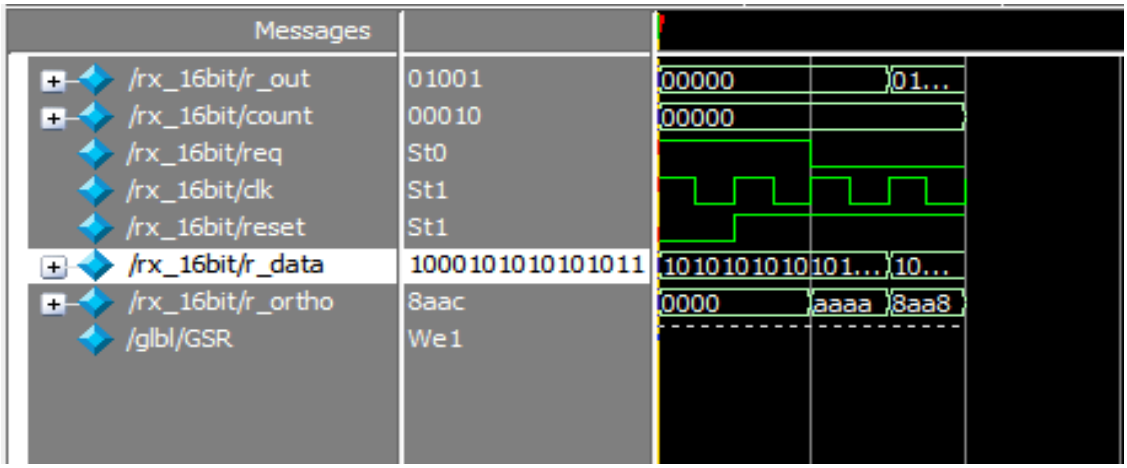

Fig represents simulation result of 1-bit error

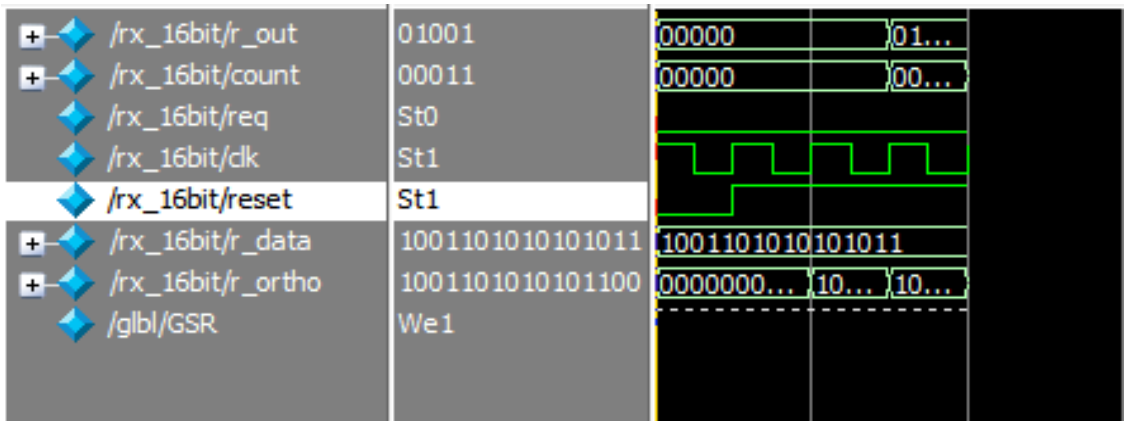

Fig represents simulation result of 2-bit error

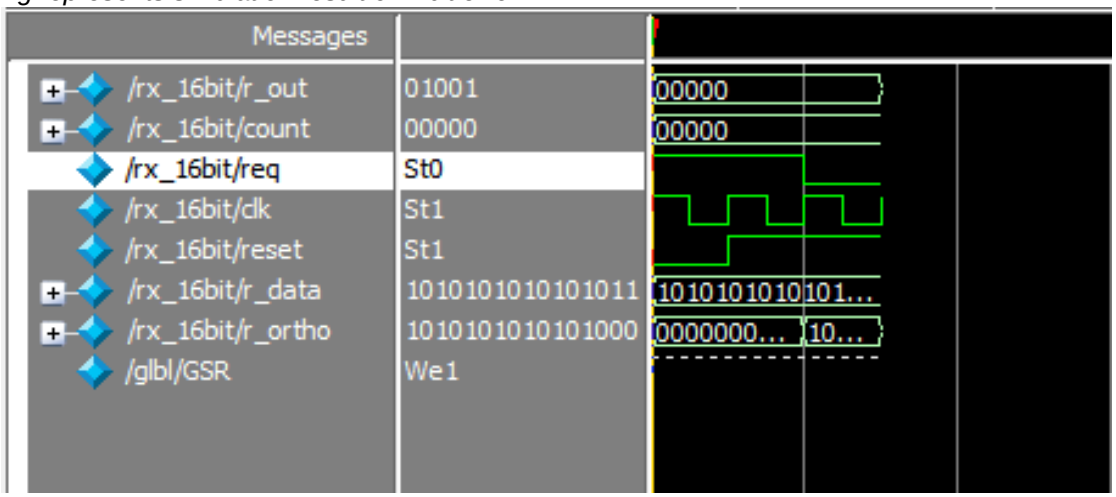

Fig represents simulation result of decryption

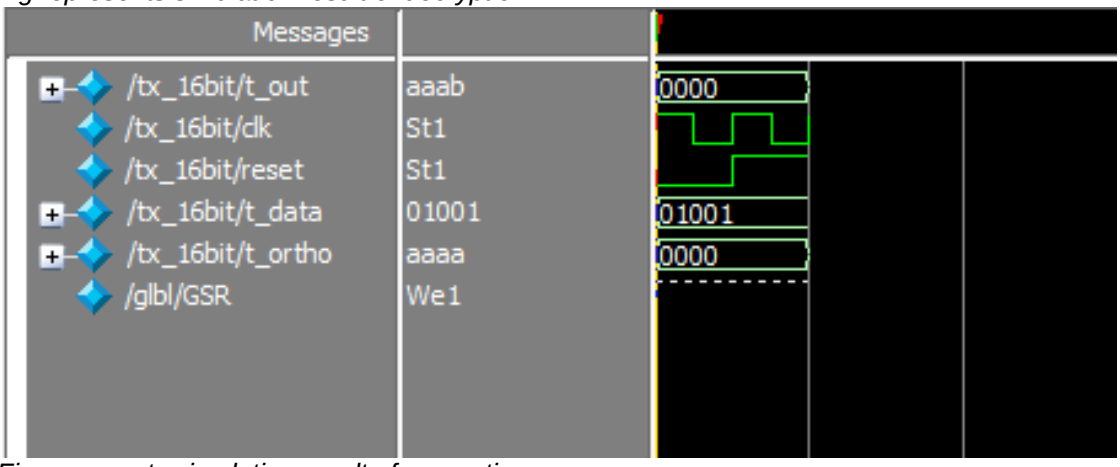

Fig represents simulation result of encryption

RESULTS

The simulation results show that for an a-bit data encoded into b-bit orthogonal data and is encrypted into a cipher text. A varying number of orthogonal code combinations are obtained which is able to detect any faulty combination. 2^a is the total number of orthogonal code combinations obtained. The error detection and correction percentage=$(2^b-2b)/2^b$. The total system can detect and correct till (b/4)-1 bit error and similarly the number of clock cycles necessary for the data received to get processed is (2b+2). Consider an example like 5-bit data therefore the total number orthogonal code bit length is $2^b=2^{5-1}=16$, and the total number of orthogonal code combinations are 2^{16}. In order to encrypt the data, the key length should be of

the same size as that of the data obtained from the encoder i.e. 16-bit key is required to encrypt the data. Hence each 5-bit data has a unique 16-bit orthogonal code so a 16-bit key required to encrypt that data. The 16-bit key is obtained using a pseudo random generator LFSR. The delay time for encryption and decryption is 6.840ns when the input bit length is 5, similarly when the input is a 6-bit data the delay times are 7.042ns which shows that there is an increase in the delay times as the input data increases. So, as the input data increases the orthogonal bit length also increases which results in more security as there is an increase of key length to encrypt the data. There by as input increases the encryption time also increases for individual systems and the synthesis reports for the delay time are shown in Table II. The percentage of error correction and detection obtained is $(2^{16}-2*16)/2^{16}$ =99.95% with error correcting ability and the number errors it can detect is 3. Similarly the error correction and detection percentage for 32 bit orthogonal code is 99.99% and the number of errors that can be detected are 5. Hence the possible number of combinations received at the receiver will be able to detect the correct code with the orthogonal code available.

Table I shows the error correction and detection rates from the simulation results obtained for 4-bit, 5-bit, 6-bit, 7-bit, 8-bit data as input.

Table II shows the delay timings for both transmitter and receiver along with the internal block delays obtained during synthesis. We can observe the as the input bit length and the key length to encrypt the data increases the delay times for the individual systems also increases.
Table I shows a summary of results and their error correction and detection results .

Input Bits (a)	*Ortho code out put bit length (b)*	*No of errors(t)*	*% of errors detected and corrected*
4	8	1	93.75
5	16	3	99.95
6	32	7	99.99
7	64	15	99.99
8	128	31	100
a	$b=2^{(a-1)}$	t=(b/4)-1	$\%=(2^b-2b)/2^b$

Table II shows a summary of transmitter and receiver delay times obtained from the synthesis reports for 5-bit, 6-bit, 7-bit and 8-bit.

Input data in bits	*Encoder delay (ns)*	*Encryptor delay (ns)*	*Transmitter delay(ns)*	*Decryptor delay(ns)*	*Decoder delay(ns)*	*Receiver delay(ns)*
4	4.283	6.054	6.054	6.054	16.786	14.898
5	4.283	6.840	6.840	6.840	19.133	18.766
6	4.283	7.032	7.032	7.032	23.853	24.089
7	4.283	7.062	7.062	7.062	44.163	45.478
8	4.283	7.082	7.082	7.082	63.718	64.238

CONCLUSION

The results of the present work show that the error detection and correction rate has been increased to 100% when the input length is an 8-bit data. The encryption and decryption time delays are also increased when the input data is increased as observed from the results of

5-bit, 6-bit, 7-bit and 8-bit data as input. Future work includes maintaining constant time delays for varying input length by using crypt analysis techniques and band width limitation.

REFERENCES

[1]. Sukalyan Son, Sayani Sen "A Non-adaptive Partial Encryption of Grayscale Images Based on Chaos", Science Direct, Procedia Technology 10,pp 663-671, CIMTA-2013.
[2]. Hossein Rahmani, Elankovan Sundararajan "Encryption as a Service (Eaas) as a Solution for Cryptogrpahy in Cloud", Science Direct, Procedia Technology 11, pp 1202-1210, ICEEI-2013.
[3]. Reviriego.P "Optimised decoding of odd-weight single error correction double error detection codes with 64bits", Volume:49 Issue:25,pp:1617-1618, IEEE journals and magazines-2013
[4]. Rukmani. R "Error Detection and Correction Architecture for Motion Estimation in video coding systems" pp:1-5, IEEE Conference-2013
[5]. Jayarani M.A, Jagadeeswari .M "A novel fault detection and correction technique for memory applications" pp:1-6, IEEE Conference ICCCI-2013.
[6]. Reviriego P, Pontarelli S "Reducing the Cost of Single Error Correction with Parity Sharing" Vol:13, Issue:3, pp:420-422, IEEE Transactions-2013.
[7]. Anton C, Ionescu L "Error detection and correction using LDPC in parallel Hopfield networks" pp:1-4, IEEE Conference ISEEE-2013.
[8]. Bo Dai, Zhensen Gao "Orthogonal DPSK/CSK Modulation and Public Key Cryptograpgy Based Secure Optical Communications" vol:25, Issue:19,pp:1897-1900, IEEE-2013.
[9]. Lamonica M "Long-Distance quantum cryptography", vol:50 ,Issue:8,pp-12-13,IEEE Journals and magazines-2013.
[10]. Xuanxia Yao, Zhi Chen " A Light weight attribute-based encryption scheme for the internet of things", Elsevier-2014.
[11]. Syed Rizvi, Katie Cover, "A Trusted third party based Encryption Scheme for Ensuring data confidentiality in cloud environment", Science direct, pp:381-386,2014.
[12]. Charles H, Gills Brassard, "Quantum cryptography: public key distribution and coin tossing", ELSEVIER-2014.
[13]. Marius Iulian, "New Enrollment Scheme for Biometric Template using Hash Chaos-Based Cryptography", Science Direct, Procedia Engineering 64,pp:1459-1468, 2013.
[14]. Saiz-Aadalid, Gil p,"Modified hamming codes to enhance short burst error detection in semiconductor memories, pp:62-65, IEEE ConferenceEDCC-2014.
[15]. Baskar S, "Error recognition and correction enhanced decoding of hybrid codes for memory application", pp:1-6, IEEE Conference ICDCS-2014.
[16]. Xiaotian Wu, Wei Sun, "Entended Capabilities for XOR-based visual cryptography", vol:0 Issue:10, pp:1592-1605, IEEE journals-2014.