ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

FPGA Based Encryption Algorithm for Secure Communication

U.Subhashini[1], Dr.M.Jagadeeswari[2]

P.G. Student, Department of ECE(PG), Sri Ramakrishna Engineering College, Coimbatore, India[1]

Head of the Department , Department of ECE(PG), Sri Ramakrishna Engineering College, Coimbatore, India[2]

ABSTRACT*:* Security is the major issue in the communication applications. Cryptography is a technique that provides security for the sender and receiver to transfer their data over a network. Security is a very important factor in every field such as Government Agencies, Research Organization, E-commerce and etc. where internet is being used. To provide a secured communication and data transition proposed an AM cryptographic algorithm, is the Symmetric key stream cipher algorithm which uses same key for encryption and decryption. The algorithm uses Random key generation, key selection and transposition. The algorithm is developed for 128 bit data in XILINX DESIGN SUITE ISE 14.2 which is coded in VHDL and implemented in Spartan 6 kit which is compared with the AES algorithm .The proposed algorithm results in high security, the time for encryption and decryption is minimum and the memory space is also reduced.

KEYWORDS*:* Cryptography, AM Cryptographic Algorithm, stream cipher, Symmetric key, Random key generation, key selection, VHDL, AES

I INTRODUCTION

Network security is important while transmitting the data over the wireless channel .cryptography is the technique is used to provide the original data from the sender to receiver by encrypting the data(converting original data into different format which cannot be understood by everyone).similarly at the receiver side the ununderstandable for mat of the data is converted into the original data by decryption(converting the different format into original data).keys used for encryption is of symmetric key cryptography and asymmetric key cryptography. Symmetric key cryptography uses the same key for encryption and decryption, whereas in asymmetric key cryptography uses different key for encryption and decryption. Only authorized person can read the data (who knows the key) which results in secure transmission of the data. The symmetric key algorithm are AES, DES, TDES and Blowfish, Modified Blowfish, RC5,RC6. The asymmetric key algorithm are RSA,Diffie-Hellman, Elliptic Curve Cryptography (ECC) these algorithms have their own merits and demerits. The main thing to consider is storage space if the space is high the time takes to transmit the data is also high so the storage space should be minimum to obtain this AM algorithm is used. The AM Encryption algorithm used is the Symmetric key stream cipher algorithm. In a stream cipher each of the plain text is encrypted one at a time with the corresponding digit of the key stream and gives a digit of the cipher text stream. A block cipher is a deterministic algorithm operating on fixed-length groups of bits with an unvarying transformation as that is specified by asymmetric key.

Paper is organized as follows. Section II deals with the literature review of the project. Section III deals with the Existing AES Algorithm. Section IV deals with the Proposed AM Algorithm. Section V summarizes the simulation results and discussion. Section VI discusses the conclusion and future works

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

II. RELATED WORK

Arithmetic Coding[1] is the technique which has advantage of compress the data and perform xor operation but Disadvantage of problem with the precision ,during decompression the accurate character is lost.AES[7] has Advantage that it is fast and flexible and Disadvantage of t he space of the cipher is larger than the plain text. DES[11] has disadvantage that it is not secure, due to its key length.RC4 [4]has advantage of The data stream is simply XORed with the series of generated keys and Disadvantage is RC4 failed to provide high level of security because of its poor key scheduling . Triple Data Encryption Standard(TDES) has disadvantage that it takes 3 times moere space than the DES but it is secure than DES.

III. ARCHITECTURE OF AM ALGORITHM

AM Encryption algorithm consists of Encryption and decryption block. The plain text is given as input along with the key to the encryption. The Encryption algorithm consists of Random key generation, random key selection and Transposition of the Key which is shown in Fig.1. As a result cipher text will be generated which is not understandable by the person except the authorized person who knows the key. At the place of decryption side the cipher text and the key will be given as input and as a result the plain text will be obtained if the correct key is given as input or else the plain text will be obtained correctly.

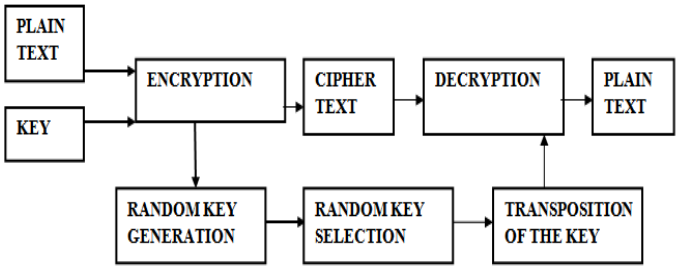

Fig . 1Block diagram of AM Algorithm

In Random Key Generation, Random key will be generated by following steps, Depending upon the length of the key number of rounds of the encryption algorithm. In each of the rounds random key generation generates key from the previous key. Random key is generated using ASCII value and the position of the each character in key. After generating random key we have 2 keys, first key is previous key and second key is newly generated key.

Random Key Selection is used to select one key between key1 ,key2. It takes 2 key as input and convert it into its equivalent binary and checks the LSB of the both keys. If LSB are same it selects key1 and if is not same it selects key2.

Transposition of the Key is a method where the each character of the key is replaced by another character of the key. To transpose the key ,calculate the random number and also calculate sum of the total of random number.

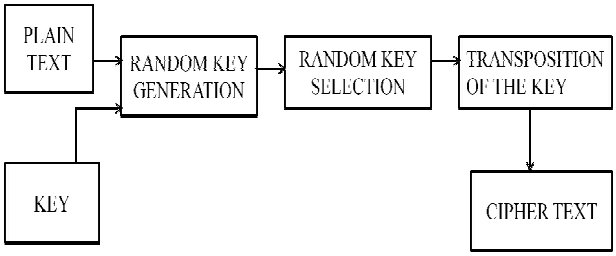

Fig.2 Block diagram of AM Encryption Algorithm

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

The overall block for encryption is shown in Fig.2 The decryption is done in reverse process.

IV. AM ALGORITHM

Steps for the encryption/decryption involves the plain text and the key is given as input, find the length of the key. The new key is generated from random key generation. From 2 keys one of the key is selected from the random key selection based upon the LSB of the both keys. If both the key LSB are same means key 1 will be selected or else key 2 will be selected. During Transposition of the key where each character is replaced by another another character of the key depending upon the random value number. To encrypt the plain text perform xor operation with the final key that is with transposition key. For decryption the cipher text is performed xor operation with the transposition key.

In Random key Generation first read the key sent as a parameter (Key1) ,Find the length of key1.find the reverse of the key1.Convert each character of key1 into its equivalent ASCII code. After that Calculate total number of random value RV= L, Rand(Max), Max= ∑ASCII * Sequence of each character. Then Find the sum of total random value, mod of sum_of_random,M= Mod(sum_of_random, l).Apply matrix on key1 and rev_key ,Add 'Mod' to each bit of matrix _key1.Apply XOR operation with matrix_rev_key and matrix_key1.Obtained new matrix as new_matrix.Now Convert binary of new_matrix to change into character and stored in new matrix (Key2)and then return two keys (key1, key2) .

In Random key selection ,Read two keys from random key generation Convert each character of key1 and key2 into its equivalent ASCII and multiply each ASCII with the value 'M' (M obtained in RKG) convert into binary.Find the Least Significant Bit of both keys as LSB1 and LSB2 and check for If both the LSB equal ,LSB1= = LSB2,thenSelect key1 and Transpose function with key1 else Call transpose function (key2).

In Transposition of the Key ,Read selected key as key1, Read sum= Sum_of_random and also Read each character of sum individually. Then the character of the key1 Will be replaced by the character which is indexed on the (value-1) of corresponding number in sum. Increase the index of key1 .Repeat the process till the last index of the key and finally obtain the key to encrypt and decryption.

V. RESULTS AND DISCUSSION

The simulation and synthesize report of the Random key generation, Random key selection, Transposition of the key, Encryption and Decryption is done in Xilinx design suite 14.2 and Implementation is done in Spartan 6 and MATLAB is used to view the Encrypted and Decrypted text.

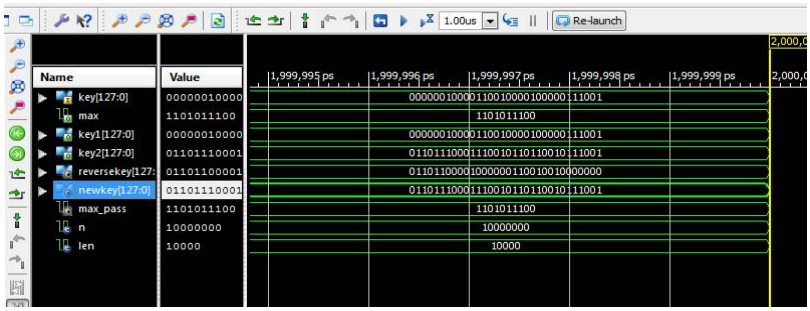

Fig.3 Random key generation

In Random key generation, the xor operation is performed on key1 and reverse key to obtain new key.The key 1 and max value is given as input which is shown in Fig 3

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

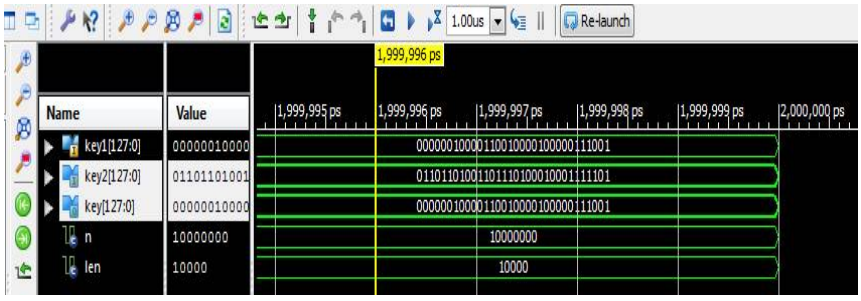

Fig.4 Random key selection

In Key Selection the LSB1 and LSB2 is compared if it is same key 1 is selected it is shown in Fig 4

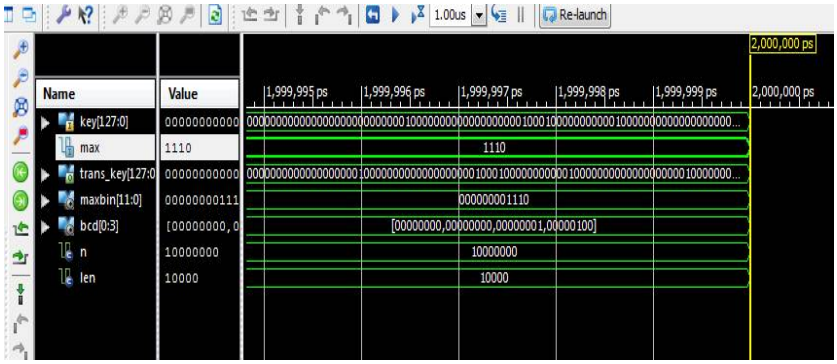

Fig.5 Transposition of the key

The key is swapped based on the max value and the transposition key is the final key. The transposed key is the final key which is xored with plain text for encryption it is shown in Fig 5

Fig.6 Encryption of the plain text

For encryption ,the plain text and key is given as input in the XILINX design suite 14.2 and the cipher text is generated by performing xor operation with plain text and final key and it is shown in Fig 6

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

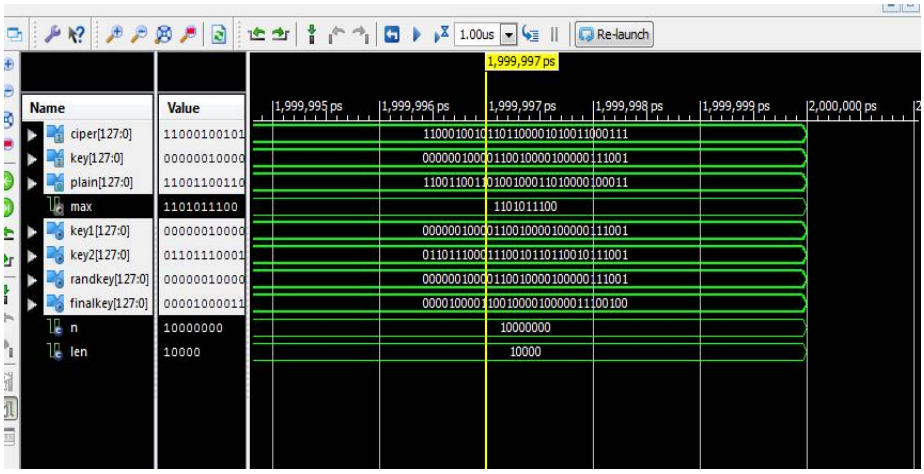

Fig.7 Decryption of the plain text

For decryption ,the plain text is obtained as result by performing xor operation with cipher text and final key given in the XILINX design suite 14.2 and it is shown in Fig 7

The AM algorithm is implemented in Spartan 6 kit, the simulation is done in Xilinx design suite 14.2,the kit implementation is shown in Fig 8.

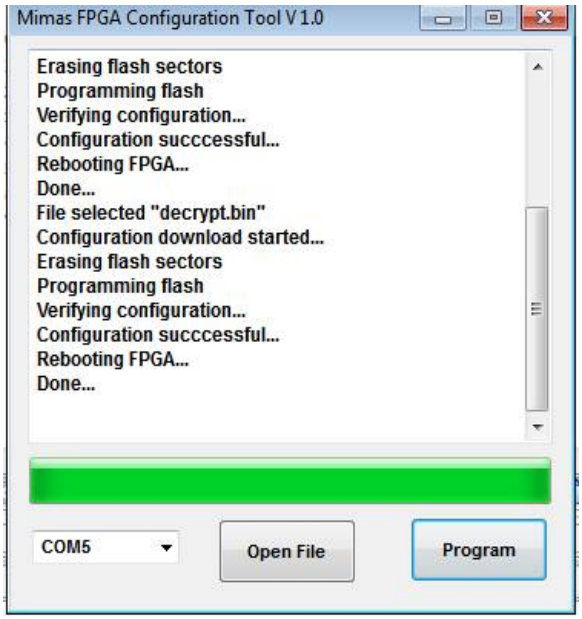

Fig 8. Implemenation of AM algorithm in mimas FPGA configuration tool

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

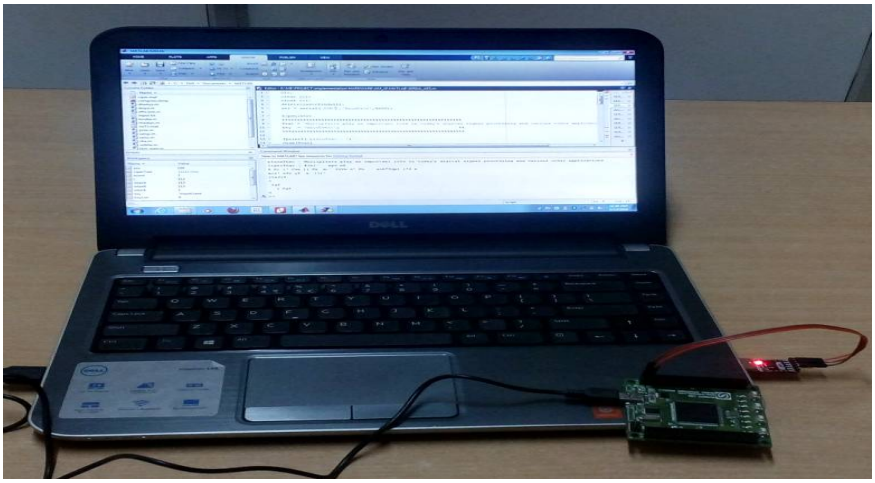

Fig 9. Overall module set up of AM algorithm

The overall module set up of AM algorithm is shown in Fig 9.The output of the encryption is viewed in Matlab 2014b and it is shown in Fig 10.

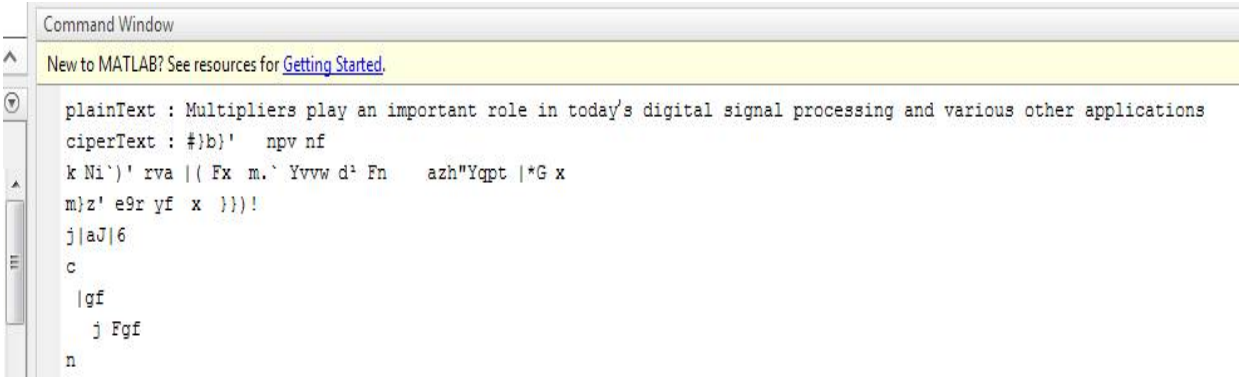

Fig 10 Encryption output in matlab

The output of the decryption is viewed in matlab 2014b and it is shown in Fig 11.

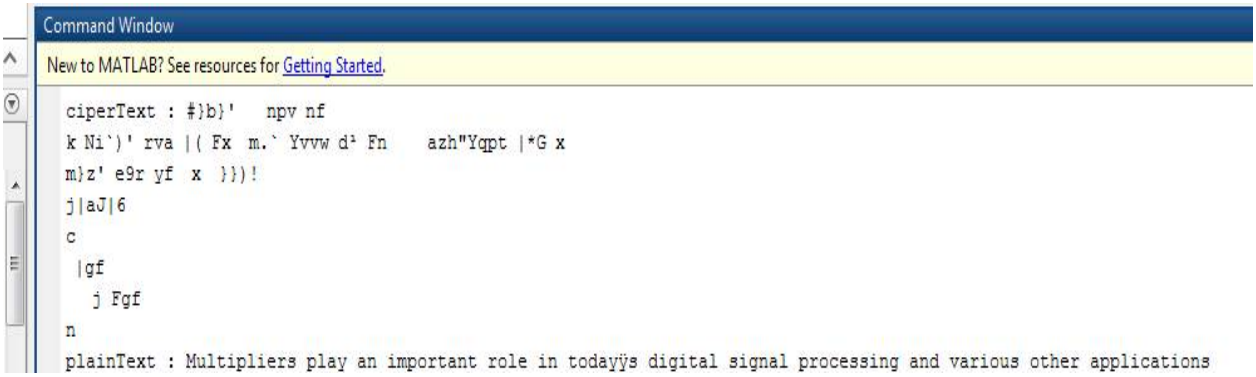

Fig 11. Decryption output in matlab

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

TABLE I COMPARISON FOR ENCRYPTION OF VARIOUS PERFORMANCE PARAMETERS OF AM ALGORITHM AND AES ALGORITHM

PARAMETER	AM ALGORITHM	AES ALGORITHM
AREA		
No of sliced LUTs	**2717 OUT OF 207360(1%)**	9722 OUT OF 207360(1%)
No of occupied Slices	**1121 OUT OF 51840(2%)**	2983 OUT OF 51840(2%)
No of Bonded IOBS	**384 OUT OF 960(40%)**	384 OUT OF 960(40%)
TIMING		
Total REAL time to Xst completion	**127 secs**	140 secs
Total CPU time to Xst Completion	**127.33 secs**	139.81 secs
DELAY	**54.431ns**	30.437ns
POWER	**3.516w**	3.516w

From the above table I clearly suggests that proposed **AM ALGORITHM is better than AES ALGORITHM is better in terms of area, timing and power**.

TABLE II COMPARISON FOR DECRYPTION OF VARIOUS PERFORMANCE PARAMETERS OF AM ALGORITHM AND AES ALGORITHM

PARAMETER	AM ALGORITHM	AES ALGORITHM
AREA		
No of sliced LUTs	**2717 OUT OF 207360(1%)**	9722 OUT OF 207360(1%)
No of occupied Slices	**1215 OUT OF 51840(2%)**	2983 OUT OF 51840(2%)
No of Bonded IOBS	**384 OUT OF 960(40%)**	384 OUT OF 960(40%)
TIMING		
Total REAL time to Xst completion	**127 secs**	419s
Total CPU time to Xst completion	**127.28sec**	418.32secs
DELAY	**54.431ns**	42.2347ns
POWER	**3.516w**	3.516w

From the above table II clearly suggests that proposed **AM ALGORITHM is better than AES ALGORITHM is better in terms of area, timing and power.**

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

VI. CONCLUSION & FUTURE WORK

An AM Algorithm is used for secure communication with reduced space for the memory. AM algorithm is compared with the existing algorithm AES from the results the proposed algorithm provides better performance than AES in terms of lower area no of sliced LUTS 2717 out of 207360(1%), no of occupies slices 1121 out of 51840(2%), no of bonded IOBS 384 out of 960(40%) , and power of 3.516w. The advantage of using AM algorithm is that it provides security over network since the random key is generated, one of the key is selected and transposed the key, so the finding of the key to hack the data is very difficult process. In future it can be extended to higher bits and can be combined with other encryption technology to result higher security.

REFERENCES

[1] Amit Pande, Joseph Zambreno and Prasant Mohapatra(2010), "Joint V ideo Compression and Encryption using Arithmetic Coding and Chaos",978-1-4244-7932-0/10, IEEE.
[2] Anjali Patil, Rajeshwari Goudar(2013), "A Comparative Survey of Symmetric Encryption Techniques for Wireless Devices",International Journal Of Scientific & Technology Research Volume 2,Issue 8.
[3] Archana.V.Nair.S, G.Kharmega Sundararaj, T. Sudarson Rama Perumal (2012), "Simultaneous compression and encryption using Arithmetic codingwith Randamized bits", International Journal of Computer Technology and Electronics Engineering (IJCTEE) Volume 2, Issue 2.
[4] Asif Mushtaque.] Md and Mr. Khushal Singh(2014), "Feasibility Evaluation of Symmetric Key Encryption Techniques for Wireless Channel and Disk Storage", IJRASET, Vol. 2 Issue V.
[5]Guang-liang Guo, Quan Qian, Rui Zhang(2015) "Different Implementations of AES Cryptographic Algorithm", International Symposium on Cyberspace Safety and Security (CSS), and 2015 IEEE 12th International Conf on Embedded Software and Systems (ICESS).
[6]Khaled Shehata, Hanady Hussien, Sara Yehia(2014) "FPGA Implementation of RSA Encryption Algorithm for E-Passport Application", International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol:8, No:1.
[7]Manju Rani, Dr. Sudesh Kumar, (2015)," Analysis on Different Parameters of Encryption Algorithms for Information Security", International Journal of Advanced Research in Computer Science and Software Engineering,volume 5,Issue 8.
[8]Mona Mudaliar, L K Bhaiya(2013), "Analysis of symmetric MPLS Network", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-5.
[9] Nidhi Sethi and Deepika Sharm(2012), "A Novel Method Of Image Encryption Using Logistic Mapping", International Journal of Computer Science Engineering, Vol. 1 No.02
[10]Prashanti.G, Deepthi.S, Sandhya Rani.K (2013), "A Novel Approach for Data Encryption Standard Algorithm" International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-5.
[11] Tiwari.M.A, Parakash.C and Mandal. AK (2012)"Performance Evaluation of Cryptographic Algorithms: DES and AES", IEEE Student's Conference on Electrical, Electronics and Computer Science.
[12] .Dr.M. Jagadeeswari(2015)Real Time Video Processing using ZYNQ 7000 SOC",International Journal of Applied Engineering Reasearch,Vol 10,No.1.pp.734-738,ISSN:0973-4562.