Volume 4, Issue 5, May 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Simulation and Error Analysis of Rijndael Algorithm

Renjith V Ravi*
Research Scholar,
Karpagam University
Coimbatore, India

Dr.R. Mahalakshmi,
Professor and HOD,
Dept. of Electrical and Electronics Engineering,
Sree Krishna College of Technology, Coimbatore, India

Abstract-- As data security being one of the vital point in present day industry progressions over security,* Rijndael *or AES algorithm is the champion amongst the most prominent systems for data encryption. In this paper, we create software reference model for AES algorithm and analyze its execution as far as encryption and decryption ability utilizing different sets of data vectors. The information vectors of 128 bits with more than 40 frames of 128 bits are utilized as experiments to assess the exhibitions. Info data is encrypted utilizing 10 separate sets of keys and decrypted utilizing the same set of keys. Error is introduced in the encrypted data and the decryption is analyzed for its competence. Picture size of 1024x1024 is considered for encryption and decryption. The results acquired show the exhibitions of AES algorithm.

Key words --* Rijndael, *AES algorithm; encryption; decryption, software model; image encryption

I. INTRODUCTION

As cellular telephones assuming an imperative part in making life more straight forward for human being, a number of the managing an account transactions, web access, information exchange continues happening at the palm top. Information exchange through open system is constantly unsecured; hence security is one of the real difficulties that need to be tended to guarantee the dependable information exchange. The security issue subsequently turns into a vital issue in today's wired or remote Internet provisions. A standout amongst the most helpful systems to ensure information is utilizing a cryptographic framework, as the configuration of figure calculations is focused around a propelled numerical hypothesis. It generally blends diverse sorts of cryptosystems in a protected convention to give a safe channel to information transmission. As a rule, unbalanced key cryptosystems, and RSA here stands for Rivest, Shamir and Adelman who first freely depicted it in 1978. Symmetric-key cryptosystems, for example, Data Encryption Standard (DES) or Advanced Encryption Standard (Rijndael), are utilized to encode mass information in the transmission stage. Because of restricted registering assets in convenient requisitions, the framework as a rule off-burdens the security methodology to devoted uncommon equipment. As of late, there have been numerous takes a shot at outlining practical encryption fittings utilized as a part of convenient requisitions [1]–[10]. A few works [1]–[5] concentrate on range lessening of AES, while others [6]–[10] propose to lessen equipment cost for both ECC and RSA cryptosystems. Picture preparing is discovering significance in different requisitions as since the time that most recent 10 years. Interactive media provisions are ruled by picture handling. It is compulsory to secure or ensure sight and sound substance from unapproved access. Ensuring the picture or feature content in a sight and sound information is of essential essentialness as picture passes on more data than any viable wellspring of information. Pictures are extensive in size and oblige huge capacity unit, thus encryption of picture substance is additionally prolonged [14]. Customary encryption calculation set aside a few minutes devouring for expansive size of picture information, thus encryption calculations ought to be altered for bigger picture sizes and need to be speedier. [13,14,15] reports that symmetric key calculation have computational time short of what unbalanced key calculations. Symmetric key calculations, for example, AES, DES have been effectively utilized for encryption of information, fittings calculations for AES have made them quick and thus devour exceptionally remains time, however for pictures with huge information size AES is still prolonged. Picture transforming is discovering significance in different provisions as since the time that most recent 10 years. Mixed media provisions are overwhelmed by picture transforming. It is compulsory to secure or ensure media content from unapproved access. Securing the picture or feature content in an interactive media information is of essential significance as picture passes on more data than any viable wellspring of information. Pictures are huge in size and oblige extensive capacity unit, consequently encryption of picture substance is additionally prolonged [12]. Conventional encryption calculation set aside a few minutes devouring for huge size of picture information, consequently encryption calculations ought to be redone for bigger picture sizes and need to be speedier. [11, 12, 13] reports that symmetric key calculation have computational time short of what uneven key calculations. Symmetric key calculations, for example, AES, DES have been effectively utilized for encryption of information, fittings calculations for AES have made them quick and thus devour exceptionally remains time, however for pictures with substantial information size AES is still prolonged. In [14, 15, 16] quick symmetric architectures for fittings execution of AES calculation is accounted for. These calculations have not been approved for picture encoding. A focal thought for any cryptographic framework is its defenselessness to conceivable assaults against the encryption calculation, for example, factual strike, differential assault, and different beast

ambushes. Lapses in channel additionally degenerate the encoded information and subsequently there is a requirement for suitable strategy that could be utilized to locate and right the failures. In this paper, the break down exhibition of AES calculation for different inputs, keys and disorder in channel is done. Execution dissection did helps in recognizing a suitable error rectifying calculation for AES. Section II examines cryptography calculation in short. Section III talks about programming calculation for AES, Section IV examines programming reference model advancement for AES calculation. Section V presents results and exchange and conclusion is introduced in Section

II. BACKGROUND THEORY ON CRYPTOGRAPHY

Cryptography is the investigation of numerical strategies identified with parts of data security, for example, confidentiality, data integrity, entity authentication, and data origin authentication. There are two sorts of cryptography: symmetric and asymmetric framework. Symmetric crypto calculation is suitable for handling mass information and is utilized frequently while exchanging colossal mass information in system or military gadget. In 2001, advanced encryption standard (AES) was chosen to take the spot of information encryption standard (DES), which was the common standard symmetric crypto calculation in the previous twenty years. It is demonstrated that AES(Rijndael) is more secure and stronger than DES. Deviated crypto calculations can give verification, information respectability and non-disavowal. Rivest-Shmir–adleman (RSA) and Elliptic bend cryptography (ECC) are two delegates of deviated crypto framework. Advanced encryption standard (AES) calculation is the best accessible private key cryptographic calculation today. Advanced Encryption Standard (AES) is a symmetric piece figure that procedures information squares of 128 bits utilizing the figure key of length 128, 192, or 256 bits. The AES calculation [2] sorts out the information hinder in a four-line and column significant requested network. The first AES encryption/decoding technique is indicated in Figure 1. In both encryption and unscrambling, the AES calculation utilizes a round capacity, which comprises of four diverse byte-situated changes:

1)sub Bytes substitutes each one State of the information hinder with a substitution table (S-box) worth of that byte.

2)shift Rows moves the each one column of the State show by diverse counterbalances cyclically, and the counterbalance relies on upon line record.

3)mix Columns changes every segment of the lattice by increasing it with a steady GF polynomial.

4)add Round Key adds a Round Key to the State by a straightforward bitwise XOR operation

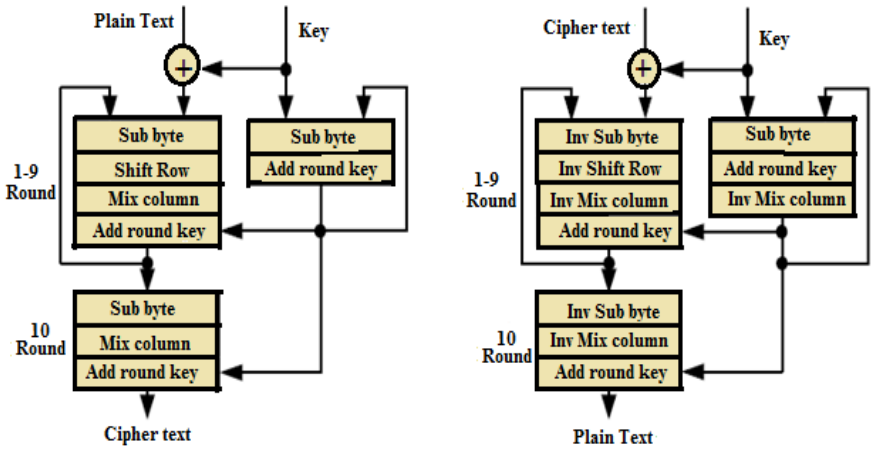

Figure 1 AES Encipher and Decipher

In Figure one a 128 bit information referred to as plain text enters the cipher core and every bit of the transformations area unit performed, finally reworking it to the encrypted cipher text. The cipher text along side of the secret is decrypted to plain text by the inverse transformation techniques. Majority of AES transformations embrace matrix vector multiplication which might be done expeditiously by number. The number also can be accustomed to implement different cryptography algorithms that use substantial quantity of matrix vector multiplications. This paper aims at the planning and FPGA implementation of a 128 x 32 bit multimode number for Advanced Encryption standard (AES) application which might even be used as a twin field Montgomery number. It performs standard multiplication over the finite fields of GF(p) and GF(2n) exploitation Montgomery's algorithm[1].Standard multiplication lies at the core of standard coding algorithms like AES. Therefore a number design which will perform quick standard multiplications and takes lesser space becomes the necessity of the hour. The planned work aims at coming up with a quick and price effective number to reinforce the AES performance. The planned work aims at coming up with a quick and price effective number to reinforce the AES performance.

Multiplication in a finite field is essential to many encryption algorithms including AES and public key algorithms like RSA and elliptic curve cryptography.

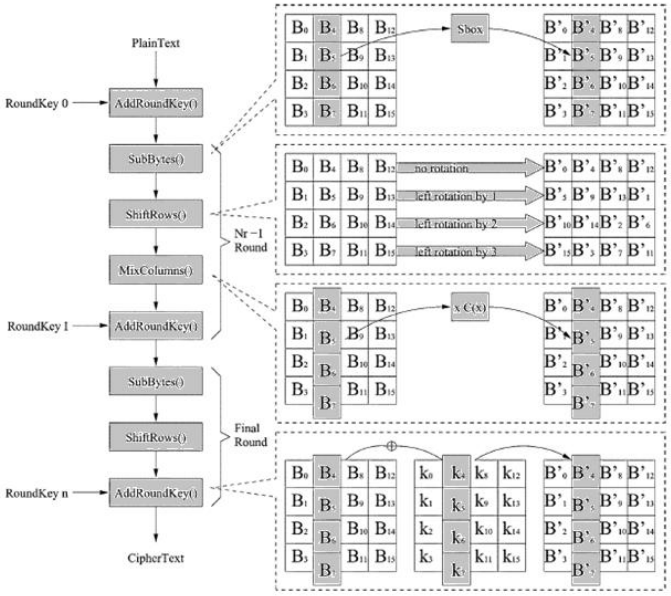

Figure 2 AES algorithm

A. AES (*Rijndael*) *Algorithm*

AES could be a private-key block cipher algorithmic rule, that consists of 3 key procedures: the secret writing, decryption, and round-key enlargement processes. It deals with information blocks of 128 b victimization keys with 3 customary lengths of 128, 192, or 256 b. Fig. 1 shows the AES algorithmic rule. every 128-b data is organized as a 4 x 4 state, operated by four primitive transformations. throughout the encryption/decryption method, the four primitive transformations area unit dead iteratively in Nr rounds, wherever the worth of Nr are going to be 10, 12, or 14, looking on that key size is chosen. Within the secret writing procedure, the incoming information can initial be bitwise XORed with Associate in Nursing initial key, and then, four transformations area unit dead within the following order: Sub-Bytes, ShiftRows, MixColumns, and AddRoundKey. Notice that the MixColumns transformation isn't performed within the last spherical. The execution sequence is reversed within the secret writing method, wherever their inverse transformations area unit InvSubBytes, InvShiftRows, InvMixColumns, and AddRoundKey, severally. Since every spherical desires a spherical key, Associate in Nursing initial secret's accustomed generate all spherical keys before encryption/decryption. within the AES algorithmic rule, the SubBytes transformation could be a nonlinear byte substitution composed of 2 operations: 1) 1) standard inversion over GF(28), modulo Associate in Nursing irreducible polynomial $p(x) = x8 + x4 + x3 + x + 1$ and 2) transformation outlined as $y=Mx +v$, wherever M is Associate in Nursing 8 x 8 b matrix, v is Associate in Nursing 8-b constant, and x/y denotes 8-b input/output. within the MixColumns transformation, the 128-b information organized as a 4 x 4 state area unit operated column by column. The four components of every column kind a four-term polynomial that's increased by a relentless polynomial $C(x) = x3 + x2 + x +$ modulo $x4 + 1$. The ShiftRows transformation may be a straightforward operation within which every row of the state is cyclically shifted right by completely different offsets. The AddRoundKey transformation may be a bitwise XOR operation of every spherical key and current state.

III. RIJNDAEL (ADVANCED ENCRYPTION STANDARD)

Advanced Encryption Standard (AES) could be an even block cipher that processes information blocks of 128 bits with exploitation of cipher key of length 128, 192, or 256 bits. The AES secret writing consists of four main operations [5], they are:

- Byte Substitution
- Shift Rows
- Mix Columns
- Add round key

A. S-box generation

The step by step procedure for AES rule is bestowed below:

Step 1: notice Inverse of the part over GF(28) modulo the irreducible polynomial given in equivalent. 1

x8 + x4 + x3 + x + one ---------- equivalent.1

Step 2: Apply transformation of the shape y = magnetic flux unit + C to the inverse, wherever M = 8 x8 bit matrix, C = 8-bit constant and x/y = 8-bit input/output.

B. Shift Rows

Shift rows suggest that cyclic shift of every row to the left by a predefined offset.

Figure 3 shows the shift rows transformation. Within the figure, S11, S12 etc area unit bytes of input organized as 4 x 4 state matrix.

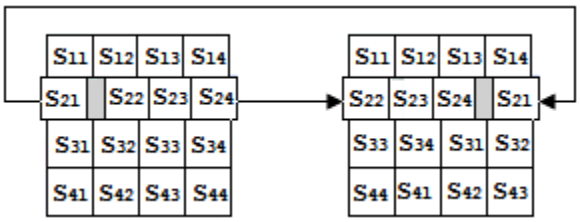

Figure 3 Shift Rows transformation

C. Mix Column

Operates on each column individually as per the equation Eq.(2). Each byte is mapped into a new value which is a function of all 4 bytes in that column.

$$\begin{bmatrix} S_{11}' & S_{12}' & S_{13}' & S_{14}' \\ S_{21}' & S_{22}' & S_{23}' & S_{24}' \\ S_{31}' & S_{32}' & S_{33}' & S_{34}' \\ S_{41}' & S_{42}' & S_{43}' & S_{44}' \end{bmatrix} = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} * \begin{bmatrix} S_{11} & S_{12} & S_{13} & S_{14} \\ S_{21} & S_{22} & S_{23} & S_{24} \\ S_{31} & S_{32} & S_{33} & S_{34} \\ S_{41} & S_{42} & S_{43} & S_{44} \end{bmatrix}$$

---------- Eq.2

D. Add Round Key

The 128 bits of state are bitwise XORed with 128 bits of the spherical key. Every round key is generated within the key enlargement and programming method. Ten rounds of the full AES method are continual for a key length of 128 bit. The spherical keys are generated by a key enlargement method. The expanded key is of 176 bits long.

A Matlab implementation of the cipher a part of AES algorithmic rule was administrated for understanding the varied transformations concerned in changing a block of plain text to cipher text. The diagram shown in Figure 4 illustrates the information flow structure of the secret writing algorithmic rule. AES_Demo is that the main program that initiates the formatting performs 'AES_init' and also the Cipher performs that will the plain text to cipher text conversion.

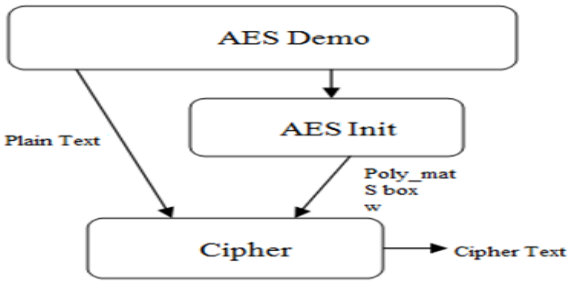

Figure 4 AES Encryption block diagram

E. AES Initialization Function

The initialization performs as represented in Figure 5 returns the swollen key schedule w, the, substitution table s_box and also the polynomial matrix poly_mat. It uses perform s_box_gen that successively calls functions find_inverse and affine_transform for generating the substitution box. Each part within the substitution box is obtained by playacting Associate in making transformation on the inverse of the part within the binary extension field GF (28). To get the key schedule 'w', AES_init perform calls the functions sub_box, rot_word and rcon_gen. The key enlargement perform takes the user equipped 16 bytes long key and utilizes the antecedently created spherical constant matrix rcon and also the substitution table s_box to get a 176 byte long key schedule w, which can be used throughout the encoding processes.

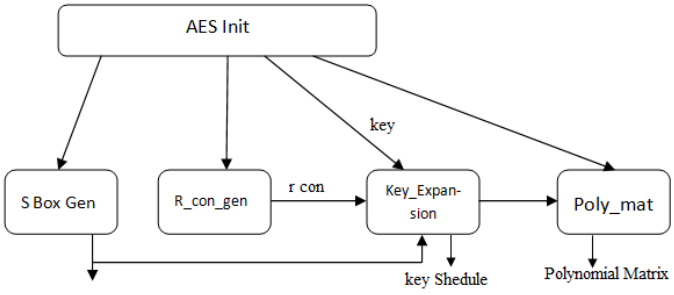

Figure 5 AES Initialization function

F. S –Box generation function

Figure 6 shows the substitution box generation perform diagram. The substitution table, s_box is employed by the enlarged key schedule perform key_expansion and also the coding perform cipher to directly substitute a byte (element of GF(28)) by another byte of identical finite field. The perform s_box_gen creates the S-box by checking out the inverses of all components of GF(28) by the employment of find_inverse and by applying affine transformations to any or all inverses mistreatment aff_trans perform. mod_pol denotes the quality AES standard reduction polynomial and is given as 283d = 100011011b = x8 + x4 + x3 + x + 1. Key enlargement and polynomial generation perform steps square measure carried intent on develop the ultimate diagram of AES rule.

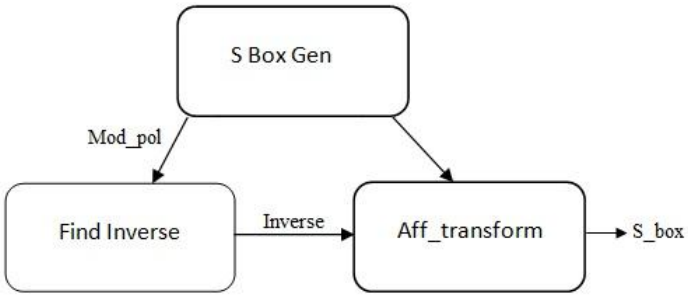

Figure 6 S- Box generation function

The main function of Cipher takes s_box , key schedule and poly_mat generated by the AES_init perform likewise because the sixteen byte plain text and produces the encrypted text. It re-arranges the plain text into a 4x4 byte state matrix and calls functions Add_round_key, Sub_Bytes, shift Row and Mix_Columns so as to come up with cipher text.

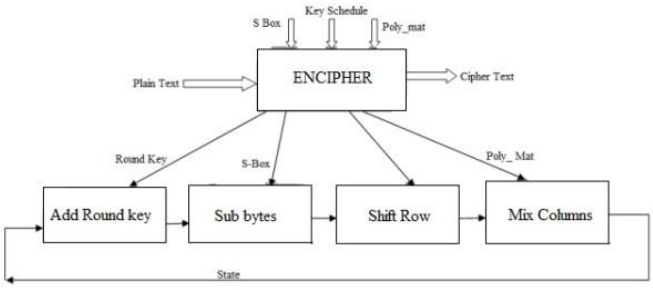

Figure 7 Cipher function for encryption

Figure 7 shows the diagram of 'Cipher' fuction for cryptography. Within the Figure, add_round_key perform performs a bitwise xor of the state matrix and therefore the spherical key matrix. The perform shift_rows cyclically permutes (shifts) the rows of the state matrix to the left. The mix_columns transformation computes the new state matrix S0 by left-multiplying this state matrix S by the polynomial matrix P.

Software modeling of AES cryptography formula exploitation Matlab has been dole out and varied transformations utilized in the formula in changing plain text to cipher text were studied. The software system modeling has been dole out specified the most program calls the low-level formatting perform and therefore the cryptography perform that successively calls alternative sub functions to accomplish the task of cryptography. The low-level formatting perform calls sub functions to come up with S-box, key schedule and polynomial matrix. The cryptography perform makes use of the outputs of those sub functions yet as alternative functions to hold out operations like byte substitution, add spherical key, shift rows and blend columns. The results obtained for software system modeling of AES formula is given for analysis. Comparison of coverage obtained with direct, random and unnatural random stimulant is given showing the connection of purposeful take a look at vector generation.

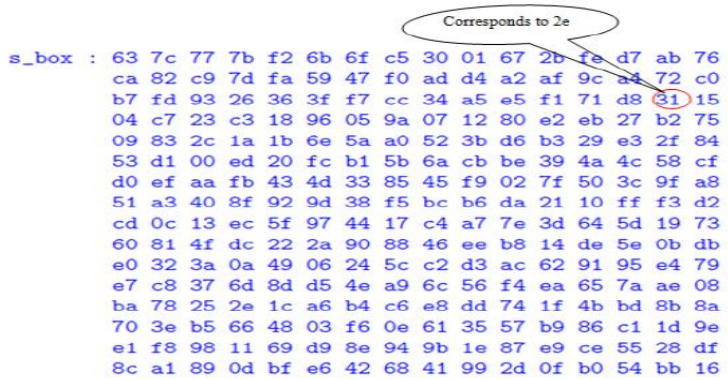

Figure 8 S_box generated

Figure 8 shows s-box generation. The S-box is obtained as a 16 x 16 matrix with row and column numbers ranging from 0 to f.

IV SOFTWARE REFERENCE MODEL FOR RIJNDAEL (AES) ALGORITHM

In this work, a software reference model to analyze the performances of AES algorithm is proposed. The algorithm discussed in Figure 2 is modeled in Matlab. The input operands are expressed in Hexadecimal format, the input operand range is set between 0 to 255 and hence 8 bits are used for representation using hexadecimal number representation format. The plain text or initial state of 128 bits of data is arranged as a 4 x 4 matrix of 16 bytes and a round key of length 128 bits is also generated from the initial key. The input data is transformed using each transformations namely sub_bytes, shift_rows, mix_columns and add round key. Finally the cipher text obtained after 10 such repetitions (rounds) is computed. Figure 9 shows the flow chart for software reference model developed in Matlab.

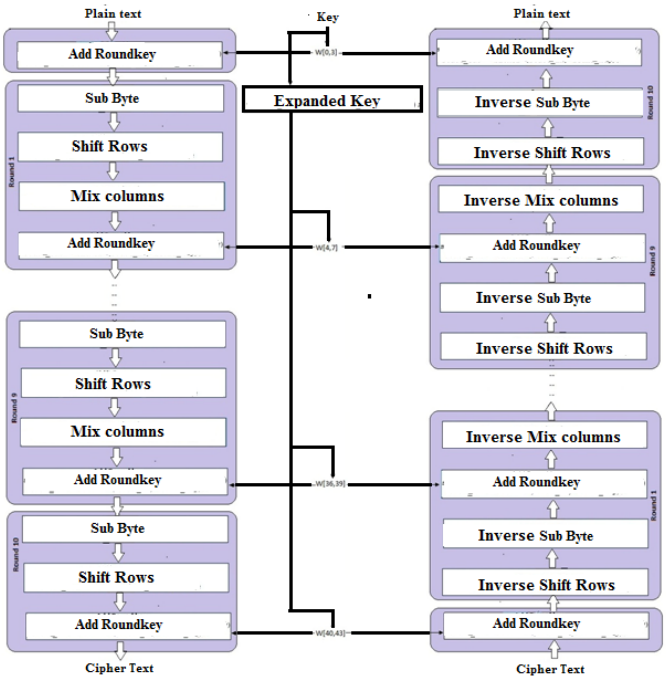

Figure 9 Flow chart for AES encryption and decryption

In this work, various input data such as image and text data is chosen to validate the developed software reference model. The input test vectors have been chosen such that they form the real test vectors to analyze the performances of AES algorithm.

V. RESULTS AND DISCUSSION

In order to validate the software reference model, four sets of check vectors every of 128 bit frame is chosen and is encrypted with exploitation of nine sets of keys. The encrypted information is 128 bits and is more decrypted exploitation nine sets of keys. Figure 10 shows the results of cryptography and decoding exploitation of nine sets of keys. These square measure the results with completely different input plaintexts with exploitation same key for cryptography.

Input		Input Data	key	Key1	Key2	Key3	Key4	Key5	Key6	Key7	Key8	Key9	Round Key	Output Data
I	CIPHER	00 04 08 0c 01 05 09 0d 02 06 0a 0e 03 07 0b 0f	2b 28 ab 09 7e ae f7 cf 15 d2 15 4f 16 a6 88 3c	a0 88 23 2a fa 54 a3 6c fe 2c 39 76 17 b1 39 05	f2 7a 59 73 c2 96 35 59 95 b9 80 f6 f2 43 7a 7f	54 47 1e 6d 80 16 23 7a 47 fe 7e 88 7d 3e 44 3b	d4 7c ca 11 44 52 71 0b a5 5b 25 ad 41 7f 3b 00	d4 7c ca 11 d1 83 f2 f9 c6 9d b0 15 f9 87 bc bc	6d 11 db ca 88 0b f9 00 a3 3e 86 93 7a fd 41 fd	4e 5f 84 4e 54 5f a6 a6 f7 c9 4f dc 0e f3 b2 4f	ea b5 31 7f d2 8d 2b 8d 73 ba f5 29 21 d2 60 2f	ac 19 28 57 77 fa d1 5c 66 dc 29 00 f3 21 41 6e	d0 c9 e1 b6 14 ee 3f 63 f9 25 0c 0c a8 89 c8 a6	50 99 cd 9b fa 6d 09 af 67 32 37 ac cc b6 e9 60
	DECIPHER	50 99 cd 9b fa 6d 09 af 67 32 37 ac cc b6 e9 60	d0 c9 e1 b6 14 ee 3f 63 f9 25 0c 0c a8 89 c8 a6	ac 19 28 57 77 fa d1 5c 66 dc 29 00 f3 21 41 6e	ea b5 31 7f d2 8d 2b 8d 73 ba f5 29 21 d2 60 2f	4e 5f 84 4e 54 5f a6 a6 f7 c9 4f dc 0e f3 b2 4f	fd 11 db ca 88 0b f9 00 a3 3e 86 93 7a fd 41 fd	d4 7c ca 11 d1 83 f2 f9 c6 9d b0 15 f9 87 bc bc	ef a8 b6 db 44 52 71 0b a5 5b 25 ad 41 7f 3b 00	3d 47 1e 6d 80 16 23 7a 47 fe 7e 88 7d 3e 44 3b	f2 7a 59 73 c2 96 35 59 95 b9 80 f6 f2 43 7a 7f	a0 88 23 2a fa 54 a3 6c fe 2c 39 76 17 b1 39 05	2b 28 ab 09 7e ae f7 cf 15 d2 15 4f 16 a6 88 3c	00 04 08 0c 01 05 09 0d 02 06 0a 0e 03 07 0b 0f
II	CIPHER	aa aa cc cc bb ff dd dd cc aa aa aa dd bb bb ff	2b 28 ab 09 7e ae f7 cf 15 d2 15 4f 16 a6 88 3c	a0 88 23 2a fa 54 a3 6c fe 2c 39 76 17 b1 39 05	f2 7a 59 73 c2 96 35 59 95 b9 80 f6 f2 43 7a 7f	54 47 1e 6d 80 16 23 7a 47 fe 7e 88 7d 3e 44 3b	d4 7c ca 11 44 52 71 0b a5 5b 25 ad 41 7f 3b 00	d4 7c ca 11 d1 83 f2 f9 c6 9d b0 15 f9 87 bc bc	6d 11 db ca 88 0b f9 00 a3 3e 86 93 7a fd 41 fd	4e 5f 84 4e 54 5f a6 a6 f7 c9 4f dc 0e f3 b2 4f	ea b5 31 7f d2 8d 2b 8d 73 ba f5 29 21 d2 60 2f	ac 19 28 57 77 fa d1 5c 66 dc 29 00 f3 21 41 6e	d0 c9 e1 b6 14 ee 3f 63 f9 25 0c 0c a8 89 c8 a6	b8 e5 07 38 27 fd dd cf 16 53 97 40 e1 52 b5 25
	DECIPHER	b8 e5 07 38 27 fd dd cf 16 53 97 40 e1 52 b5 25	d0 c9 e1 b6 14 ee 3f 63 f9 25 0c 0c a8 89 c8 a6	ac 19 28 57 77 fa d1 5c 66 dc 29 00 f3 21 41 6e	ea b5 31 7f d2 8d 2b 8d 73 ba f5 29 21 d2 60 2f	4e 5f 84 4e 54 5f a6 a6 f7 c9 4f dc 0e f3 b2 4f	fd 11 db ca 88 0b f9 00 a3 3e 86 93 7a fd 41 fd	d4 7c ca 11 d1 83 f2 f9 c6 9d b0 15 f9 87 bc bc	ef a8 b6 db 44 52 71 0b a5 5b 25 ad 41 7f 3b 00	3d 47 1e 6d 80 16 23 7a 47 fe 7e 88 7d 3e 44 3b	f2 7a 59 73 c2 96 35 59 95 b9 80 f6 f2 43 7a 7f	a0 88 23 2a fa 54 a3 6c fe 2c 39 76 17 b1 39 05	2b 28 ab 09 7e ae f7 cf 15 d2 15 4f 16 a6 88 3c	aa aa cc cc bb ff dd dd cc aa aa aa dd bb bb ff
III	CIPHER	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	2b 28 ab 09 7e ae f7 cf 15 d2 15 4f 16 a6 88 3c	a0 88 23 2a fa 54 a3 6c fe 2c 39 76 17 b1 39 05	f2 7a 59 73 c2 96 35 59 95 b9 80 f6 f2 43 7a 7f	54 47 1e 6d 80 16 23 7a 47 fe 7e 88 7d 3e 44 3b	d4 7c ca 11 44 52 71 0b a5 5b 25 ad 41 7f 3b 00	d4 7c ca 11 d1 83 f2 f9 c6 9d b0 15 f9 87 bc bc	6d 11 db ca 88 0b f9 00 a3 3e 86 93 7a fd 41 fd	4e 5f 84 4e 54 5f a6 a6 f7 c9 4f dc 0e f3 b2 4f	ea b5 31 7f d2 8d 2b 8d 73 ba f5 29 21 d2 60 2f	ac 19 28 57 77 fa d1 5c 66 dc 29 00 f3 21 41 6e	d0 c9 e1 b6 14 ee 3f 63 f9 25 0c 0c a8 89 c8 a6	7d 1a 3e 89 f7 b8 42 1b 6b 99 f0 54 0c b3 47 6f
	DECIPHER	7d 1a 3e 89 f7 b8 42 1b 6b 99 f0 54 0c b3 47 6f	d0 c9 e1 b6 14 ee 3f 63 f9 25 0c 0c a8 89 c8 a6	ac 19 28 57 77 fa d1 5c 66 dc 29 00 f3 21 41 6e	ea b5 31 7f d2 8d 2b 8d 73 ba f5 29 21 d2 60 2f	4e 5f 84 4e 54 5f a6 a6 f7 c9 4f dc 0e f3 b2 4f	fd 11 db ca 88 0b f9 00 a3 3e 86 93 7a fd 41 fd	d4 7c ca 11 d1 83 f2 f9 c6 9d b0 15 f9 87 bc bc	ef a8 b6 db 44 52 71 0b a5 5b 25 ad 41 7f 3b 00	3d 47 1e 6d 80 16 23 7a 47 fe 7e 88 7d 3e 44 3b	f2 7a 59 73 c2 96 35 59 95 b9 80 f6 f2 43 7a 7f	a0 88 23 2a fa 54 a3 6c fe 2c 39 76 17 b1 39 05	2b 28 ab 09 7e ae f7 cf 15 d2 15 4f 16 a6 88 3c	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Figure 10 Results of encryption and decryption

In the following set of test investigation, 128 bit of data is encrypted utilizing different sets of keys. Keeping in mind the end goal to accept the exhibitions of AES calculation, data bits with all '0's and all '1's have been utilized as test vector to complete the investigation. Figure 11 shows the results got. These are the results with same data plaintexts with utilizing distinctive key for encryption.

Input		Input Data	Initial key	Key1	Key2	Key3	Key4	Key5	Key6	Key7	Key8	Key9	Round Key	Output Data
I	CIPHER	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	62 62 62 62 63 63 63 63 63 63 63 63 63 63 63 63	9b f9 9b f9 98 fb 98 fb 98 fb 98 fb c9 aa c9 aa	90 69 f2 0b 97 6c f4 0f 34 cf 57 ac 50 fa 33 99	ee 87 75 7e 06 6a 9e 91 da 15 42 ee 7b 81 b2 2b	7f f8 8d f5 2e 44 da 4b 2b 3e 7c 92 88 09 bb 90	ec 14 99 6a 61 25 ff b4 4b 75 09 9b 85 8c 37 a7	21 35 ac c6 75 50 af 1b 17 62 6b f0 87 0b 3c 9b	0e 3b 97 51 f9 a9 06 1d 03 61 0a fa 33 38 04 9f	b1 8a 1d 4c d4 7d 7b 66 d8 b9 b3 49 a2 da de 41	b4 3e 23 6f ef 92 e9 8f 5b a2 51 18 cb 11 cf 8e	66 ef 88 ca e9 8a 4c 34 4b 2c fa 2b d4 3b 59 2e
	DECIPHER	66 ef 88 ca e9 8a 4c 34 4b 2c fa 2b d4 3b 59 2e	b4 3e 23 6f ef 92 e9 8f 5b a2 51 18 cb 11 cf 8e	b1 8a 1d 4c d4 7d 7b 66 d8 b9 b3 49 a2 da de 41	0e 3b 97 51 f9 a9 06 1d 03 61 0a fa 33 38 04 9f	21 35 ac c6 75 50 af 1b 17 62 6b f0 87 0b 3c 9b	ec 14 99 6a 61 25 ff b4 4b 75 09 9b 85 8c 37 a7	7f f8 8d f5 2e 44 da 4b 2b 3e 7c 92 88 09 bb 90	ee 87 75 7e 06 6a 9e 91 da 15 42 ee 7b 81 b2 2b	90 69 f2 0b 97 6c f4 0f 34 cf 57 ac 50 fa 33 99	9b f9 9b f9 98 fb 98 fb 98 fb 98 fb c9 aa c9 aa	62 62 62 62 63 63 63 63 63 63 63 63 63 63 63 63	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
II	CIPHER	11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11	11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11	92 83 92 83 93 82 93 82 93 82 93 82 93 82 93 82	83 00 92 11 80 02 91 13 80 02 91 13 7f fd 6e ac	fa fa 68 79 fd ff 6e 7d 76 89 a7 9a 4e 4c dd ce	0d f7 9f e6 5d 11 cc 02 01 10 dc da 4b 4b 25 a7	a7 52 cd 2b 01 88 6f f5 ff ef 33 ed c5 8e ab 0c	63 31 fc a7 1c 94 fb 0e 01 88 6f f5 34 ba 11 1d	88 b9 45 92 49 dd 26 28 5b b4 87 6a 3a 80 91 8c	3c 85 c0 52 4b 96 b0 98 3f 8b 0c 66 75 f5 64 e8	61 ef 24 76 78 ee 5e c6 e4 2f 23 45 75 80 e4 0c	e3 07 23 55 16 f8 a6 60 5a 75 56 13 4d cd 29 25	e3 60 8f 98 6e 8b 25 a0 26 8d 56 e0 f5 26 e1 1b
	DECIPHER	e3 60 8f 98 6e 8b 25 a0 26 8d 56 e0 f5 26 e1 1b	a3 07 23 55 16 f8 a6 60 5a 75 56 13 4d cd 29 25	61 ef 24 76 78 ee 5e c6 e4 2f 23 45 75 80 e4 0c	3c 85 c0 52 4b 96 b0 98 3f 8b 0c 66 75 f5 64 e8	88 b9 45 92 49 dd 26 28 5b b4 87 6a 3a 80 91 8c	63 31 fc a7 1c 94 fb 0e ff ef 33 ed 34 ba 11 1d	a7 52 cd 2b 01 88 6f f5 01 10 dc da c5 8e ab 0c	0d f7 9f e6 76 89 a7 9a 5d 11 cc 02 4b 4b 25 a7	fa fa 68 79 fd ff 6e 7d 4e 4c dd ce fd 00 6e 82	83 00 92 11 80 02 91 13 80 02 91 13 7f fd 6e ac	92 83 92 83 93 82 93 82 93 82 93 82 93 82 93 82	11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11	11 11 11 11 11 11 11 11 11 11 11 11 11 11 11 11

Figure 11 Simulation results with same input and different keys

For the results shown in Figure 10 and Figure 11, the last columns show the encrypted output and decrypted output. The decrypted output matches with the input shown in column one. Experimental analyses have conjointly been distributed to demonstrate AES formula to decode victimization 2 completely different keys for cryptography and decoding severally. The input data sets chosen for analysis are encrypted victimization one set of keys and decrypted victimization another set of keys. From the results obtained it's found that the decrypted information doesn't match with the input quantity, therefore proving the effectiveness of cryptography formula. Further during this work, so as to investigate the performance of AES formula, the encrypted information is introduced with noise and is decrypted victimization the keys. The results shown in Figure 12 demonstrates that for the chosen set of check vectors the AES formula isn't ready to reconstruct the right output once the error is introduced. Therefore it's found that the transmitted information over channel once corrupted by noise cannot be decrypted with the keys used for cryptography. These are the results with completely different input plaintexts with victimization same key for cryptography with error obtained at output aspect of cipher. The error bits wherever marked with red colour text.

RESULTS with Error at input Data side of DECIPHER

Input		Input Data	key	Key1	Key2	Key3	Key4	Key5	Key6	Key7	Key8	Key9	Round Key	Obtained Output Data	Desired output
I	CIPHER	aa ee cc cc bb ff dd dd cc aa aa ee dd bb bb ff	3a 18 da 66 4f bc ea 7f 2e ab 1a ac 20 de 55 dc	e9 f1 2b 4d de 62 88 f7 a8 03 19 b5 13 cd 98 44	83 72 59 14 0b 69 e1 16 b3 b0 a9 1c f0 3d a5 e1	c0 b2 eb ff 97 fa 1f 09 4b fb 52 4e 0a 37 92 73	c9 7b 90 6f b8 46 59 50 e4 3f 6d 23 1c 2b b9 ca	8a f1 61 0e 9e d8 81 d1 b0 8f a2 c1 b4 9f 26 ac	94 65 04 0a e6 3e bf 6e 7e f1 13 d2 1f 80 a6 4a	4b 2e 2a 20 53 6d d2 bc a8 59 4a 98 78 f5 5e 14	aa 80 aa 8a 15 78 aa 16 52 0b 41 d9 cf 37 69 7d	f2 72 d8 52 20 58 f2 e4 ad a6 e7 3e b1 86 af 92	ad ff 07 55 92 ca 38 dc a2 44 a3 9d b1 37 d8 4a	d0 b3 f0 1b 43 06 60 84 7e 7b 02 f8 83 86 1f 4f	d1 b3 f0 1b 43 06 60 84 7e 7b 02 f8 83 86 1f 4f
	DECIPHER	d0 b3 f0 1b 43 06 60 84 7e 7b 02 f8 83 86 1f 4f	ad ff 07 55 92 ca 38 dc a2 44 a3 9d b1 37 d8 4a	f2 72 d8 52 20 58 f2 e4 ad a6 e7 3e b1 86 af 92	aa 80 aa 8a 15 78 aa 16 52 0b 41 d9 cf 37 69 7d	4b 2e 2a 20 53 6d d2 bc a8 59 4a 98 78 f5 5e 14	94 65 04 0a e6 3e bf 6e 7e f1 13 d2 1f 80 a6 4a	8a f1 61 0e 9e d8 81 d1 b0 8f a2 c1 b4 9f 26 ac	c9 7b 90 6f b8 46 59 50 e4 3f 6d 23 1c 2b b9 ca	c0 b2 eb ff 97 fa 1f 09 4b fb 52 4e 0a 37 92 73	83 72 59 14 0b 69 e1 16 b3 b0 a9 1c f0 3d a5 e1	e9 f1 2b 4d de 62 88 f7 a8 03 19 b5 13 cd 98 44	3a 18 da 66 4f bc ea 7f 2e ab 1a ac 20 de 55 dc	31 51 02 89 a1 8b ba 2f 15 00 b3 e1 ea d1 b4 e1	aa ee cc cc bb ff dd dd cc aa aa ee dd bb bb ff
II	CIPHER	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	3a 18 da 66 4f bc ea 7f 2e ab 1a ac 20 de 55 dc	e9 f1 2b 4d de 62 88 f7 a8 03 19 b5 13 cd 98 44	83 72 59 14 0b 69 e1 16 b3 b0 a9 1c f0 3d a5 e1	c0 b2 eb ff 97 fa 1f 09 4b fb 52 4e 0a 37 92 73	c9 7b 90 6f b8 46 59 50 e4 3f 6d 23 1c 2b b9 ca	8a f1 61 0e 9e d8 81 d1 b0 8f a2 c1 b4 9f 26 ac	94 65 04 0a e6 3e bf 6e 7e f1 13 d2 1f 80 a6 4a	4b 2e 2a 20 53 6d d2 bc a8 59 4a 98 78 f5 5e 14	aa 80 aa 8a 15 78 aa 16 52 0b 41 d9 cf 37 69 7d	f2 72 d8 52 20 58 f2 e4 ad a6 e7 3e b1 86 af 92	ad ff 07 55 92 ca 38 dc a2 44 a3 9d b1 37 d8 4a	77 7c 48 40 2f 43 48 18 83 20 43 d4 fd 22 81 8a	77 7c 48 40 2f 43 48 18 83 3c 43 d4 fd 22 81 8a
	DECIPHER	77 7c 48 40 2f 43 48 18 83 20 43 d4 fd 22 81 8a	ad ff 07 55 92 ca 38 dc a2 44 a3 9d b1 37 d8 4a	f2 72 d8 52 20 58 f2 e4 ad a6 e7 3e b1 86 af 92	aa 80 aa 8a 15 78 aa 16 52 0b 41 d9 cf 37 69 7d	4b 2e 2a 20 53 6d d2 bc a8 59 4a 98 78 f5 5e 14	94 65 04 0a e6 3e bf 6e 7e f1 13 d2 1f 80 a6 4a	8a f1 61 0e 9e d8 81 d1 b0 8f a2 c1 b4 9f 26 ac	c9 7b 90 6f b8 46 59 50 e4 3f 6d 23 1c 2b b9 ca	c0 b2 eb ff 97 fa 1f 09 4b fb 52 4e 0a 37 92 73	83 72 59 14 0b 69 e1 16 b3 b0 a9 1c f0 3d a5 e1	e9 f1 2b 4d de 62 88 f7 a8 03 19 b5 13 cd 98 44	3a 18 da 66 4f bc ea 7f 2e ab 1a ac 20 de 55 dc	20 94 4b 44 51 83 56 7d 6c b0 81 58 79 76 77 5d	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Figure 12 AES results with channel error

From the examination completed it is observed that the AES calculation expends time as there are a few cycles to be performed, and throughout every cycle the information control is done utilizing a set of keys. At the point when information source is picture which has expansive set of information as far as pixels, encryption of data takes more of a chance, thus it is obliged to pick interchange procedures that might be joined with AES to minimize the handling time. Further mistake in channel undermines the information and it gets troublesome to unscramble from the adulterated data. The calculation created in this work shows the exhibitions of AES.

VI. CONCLUSION

Cryptography is the investigation of mathematics related information security. Data encryption prompts confidentiality, data integrity, entity authentication, and data origin authentication. A few standards for data encryption throughout the last few years, Rijndael or Advanced Encryption Standard (AES) algorithm is the best accessible private key cryptographic algorithm today. Encryption of data sources, for example, picture and text obliges time as AES is an iterative algorithm, encrypted data need to be secured, and channel noise effect need to be examined. In this work, the

software reference model for AES is produced and is accepted utilizing different data sets and the exhibitions of AES algorithm is assessed as far as encryption and decoding ability. The results got exhibit the focal points of AES for encryption of picture and text data. The middle of the road steps in AES might be affixed utilizing suitable algorithms and could be utilized to encode complex input data sources.

REFERENCES

1. Chen-Hsing Wang, Chieh-Lin Chuang, and Cheng-Wen Wu, *An Efficient Multimode Multiplier Supporting AES and Fundamental Operations of Public-Key Cryptosystems*, IEEE Transactions on Very Large Scale Integration Systems (VLSI), Vol.18, No.4, pp.553-563, 2010
2. Satoh A., Morioka S., Takano K., and Munetoh S., *Unified hardware architecture for128-bit block ciphers AES and Camellia*, Proceedings of cryptographic Hardware and Embedded Systems, pp. 304–318, 2003
3. Bruce Schneir, Applied Cryptography, 2nd Edition, John Wiley and Sons Publishers, 1996
4. Herstein I. N., *Abstract Algebra*, Macmillan Publishing Company, 1990
5. William Stallings, Cryptography and Network Security Principles and Practices, 4th edition, Prentice Hall, 2007
6. Tenca A. F. and Koç C. K., *A scalable architecture for modular multiplication based on Montgomery's algorithm*, IEEE Transactions on Computer Science, Vol. 52, No. 9, pp. 1215–1221, 2003
7. Harris D., Krishnamurthy R., Anders M., Mathew S.,, and Hsu S., *An improved unified scalable radix-2 Montgomery multiplier*, Proceedings of 17th IEEE Symposium on Computer Arithmetic, pp. 172–178, 2005
8. A. Satoh and K. Takano, *A scalable dual-field elliptic curve cryptographic Processor*, IEEE Transactions on Computer Science, Vol. 52, No.4, pp.449–460, 2003
9. Wang J., Zeng X.,, and Chen J., *A VLSI implementation of ECC combined with AES,* Proceedings of International Conference on Solid State and Integrated Circuit Technology, pp. 1899–1904, 2006
10. Dominik Engel Thomas stutz,Andreas Uhl,"A survey on JPEF2000 encryption", Multimedia systems[online] SpringerLink Verlag pp.1 -29, ,2008.
11. Shtewi,A.M. "An Efficient Modified Advanced Encryption Standard (MAES) adapted for image cryptosystems" IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.2, pp 226-232 February 2010
12. Shiguo Lian," Quasi-commutative watermarking and encryption for secure media content distribution",[online], Multimedia Tools and Applications Volume 43, Number 1 / May, 2009
13. K. Gaj, P.Chodowiec, "Fast implementation and fair comparison of the final candidates for advanced encryption standard using field programmable gate arrays", in : CT-RSA 2001, pp.84-99
14. A. Hodjat, I. Verbauwhede, "A 21.54 Gbits/s Fully Pipelined AES Processor on FPGA". Proceedings of the 12th Annual IEEE Symposium on Field-Programmable Custom Computing Machines (FCCM'04).
15. K. Janvinen, M. Tominisko, J. Skytta, "A fully pipelined memorlyess 17, 8 Gpbs AES-128 encryptor", in International symposium of Field programmable Gate arrays, 2003, pp.207-215.
16. M. Mclone, J.V. McCanny, "Rijindael FPGA implementations utilizing look-up tables", J.VLSI signal process, syst. 34(3)(2003)261-275.
17. D. Dia, M. Zeghid, M. Atri, B. Bouallegue, M. Machhout and R. Tourki, "DWT-AES Processor for a Reconfigurable Secure Image Coding", Inter-national Journal of Computer Science and Engineering,vol.1,no.2,june 2009.
18. G.Liu, T.Ikenaga, S.Goto and T.Baba, "A Selective Video Encryption Scheme for MPEG Compression Standard", in IEICE Transactions on Fundamentals of Electronics, communications and Computer Sciences, 89 (2006), pp. 194-202.
19. M. Zeghid, M. Machhout, L. Khriji, A. Baganne and R. Tourki, "A Mod-ified AES Based Algorithm for Image Encryption", International Journal of Computer Science and Engineering,1(2007), pp.70-75.
20. Sugreev Kaur and Rajesh Mehra,"High Speed and Area Efficient 2D DWT Processor Based Image Compression", Signal & Image Processing : An International Journal(SIPIJ) Vol.1, No.2, December 2010.
21. Ashwini M. Deshpande, Mangesh S. Deshpande and Devendra N. Kayatanavar, "FPGA implementation of AES Encryption and Decryption", International Conference on Control , Automation, Communication and Energy Conservation -2009, 4th-6th June 2009.
22. A. Mansouri, A. Ahaitouf, and F. Abdi, "An Efficient VLSI Architecture and FPGA implementation of High-Speed and Low Power 2-D DWT for (9, 7) wavelet Filter", IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.3, March 2009.
23. D.Dia, M.Zeghid, M.Atri, B.Bouallegue, M.Machhout and R.Tourki, "DWT-AES Processor for a Reconfigurable Secure Image Coding", Inter-national Journal of Computer Science and Engineering,vol.1,no.2,june 2009.
24. A. E. Rohiem, F. M. Ahmed and A. M. Mustafa "FPGA Implementa-tion of Reconfigurable Parameters AES Algorithm", 13th International Conference on Aerospace Sciences and Aviation Technology, ASAT- 13, May 26 – 28, 2009.

