Hardware Implementation of Multimedia Encryption Techniques Using FPGA

M.A. Mohamed [1], M.E. Abou-Elsoud [2] and W.M. Kamal El-din [3]

[1] Electronics and Communications Engineering Dept., Faculty of Engineering, Mansoura University Mansoura, 35511,Dakahlia, Egypt

[2] Electronics and Communications Engineering Dept., Faculty of Engineering, Mansoura University Mansoura, 35511,Dakahlia, Egypt

[3] Electronics and Communications Engineering Dept., Faculty of Engineering, Mansoura University Mansoura, 35511,Dakahlia, Egypt

Abstract

Multimedia encryption algorithm has gain importance nowadays for copyright protection. Many multimedia encryption Techniques had been designed and tested software base. We will implement a library of hardware realization using FPGA of seven multimedia encryption algorithms. Simulation results had shown that blowfish provided the best result. In addition we proposed new encryption method based on cascaded techniques. This cascaded method provides a great improvement .The discussed techniques were tested on multimedia database.

Keywords: *Multimedia Encryption; Stream Cipher, Block Cipher, FPGA*

1. Introduction

Nowadays, multimedia data are closely related to many aspects of daily life, including education, commerce, and politics. As the multimedia data itself is not protected, and may be stolen during the transmission process. Thus, to maintain security, multimedia data should be protected before transmission or redistribution. Typical protection method is the encryption technique [1, 2]. Generally, multimedia components are divided into: (i) the original multimedia content; (ii) the encrypted multimedia content, (iii) and decrypted multimedia content [1].

Here, the original multimedia content is transformed into encrypted multimedia content with an encryption algorithm under the control of encryption key; Fig.1. Similarly, the encrypted multimedia content is decrypted into the original multimedia content with the decryption algorithm under the control of the decryption key; Fig.1. Additionally, some attacks may be done to break the system and obtain the original multimedia content. Most of the research work focuses on efficient encryption and decryption algorithms that are secure against attacks [2].

This paper has been organized as: (2) presents database; (3) introduces a selected set of evaluation Parameters (4) introduces a selected set of encryption algorithms and proposed technique; (5) gives and discusses the simulation results, and (6) discusses the final conclusion.

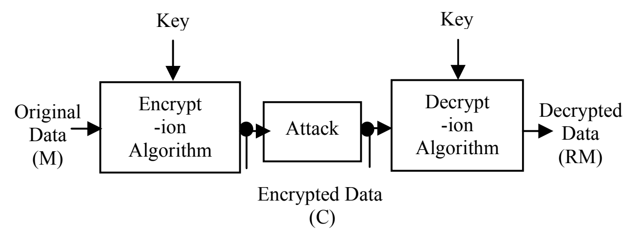

Fig.1 Multimedia Encryption and Decryption Process

2. DATA Collection

In this paper all digital encryption techniques were tested on three multimedia items: (i) machine written English text; (ii) two seconds length mono-type audio, and (iii) greyscale-2D images of joint photographic expert groups (JPEG).

2.1 Text Data

Text data may be taken form keyboard or loaded from any text file in upper case or lower case letters.

2.2 Audio Data

The used digital audio has the following specifications: (i) hands gripped the edges of the table; (ii) sample rate: 48 kHz ;(iii) audio format: wav, and (iv) mono type audio.

2.3 Grayscale Image Database

2D images may be taken from a digital camera or loaded from Matlab gallery of any image format. In this paper two images databases. :The first has the following specifications : (i) JPEG format; (ii) grayscale images; (iii) image size 97×129; (iv) image size: 2819 Bytes; (v) bit depth: 8; (vi) number of quantization levels: 256; (vii) coding method: Huffman, and (viii) coding process: sequential.

3. Evaluation Parameters

In general, the performance of digital encryption techniques can be evaluated using numerous quantitative measures. These parameters can be divided into two categories: (i) quality of reconstruction, and (ii) quality of encryption.

3.1 Quality of Reconstruction

$$R=\frac{\sum_{i=1}^{N}\left(x(i)-\bar{x}\right)\left(x_r(i)-x_r\right)}{\sum_{i=1}^{N}\left(x(i)-\bar{x}\right)^2\sum_{i=1}^{N}\left(x_r(i)-\bar{x}_r\right)^2} \quad (1)$$

$$MSE=\frac{1}{N}\sum_{i=1}^{N}\left(x(i)-x_r(i)\right)^2 \quad (2)$$

where R, and MSE are the correlation coefficient and mean squared error respectively between the original data and the reconstructed data.

3.2 Robustness Parameters

Some of the early literature considered a binary robustness metric that only allows for two different states. However, it makes sense to use a metric that allows for different levels of robustness. The use of bit-correct ratio (BCR) has become recently, as it allows for more detailed scale of values. The BCR is defined as:

$$BCR=\frac{100}{L}\sum_{n=0}^{l-1}\begin{cases}1 & E_n^{'}=E_n\\ 0 & E_n^{'}\neq E_n\end{cases} \quad (3)$$

where L is the data length, E_n is the n^{th} bit of the original data and $E_n^{'}$ is the n^{th} bit of reconstructed data. In this paper the resulting BCR are used as performance metric.

4. Encryption Algorithms

In general, encryption systems can be classified into one of two kinds: symmetric and asymmetric encryption systems. Symmetric encryption uses a single key to encrypt and decrypt the message. It is also called secret key encryption. On the other hand, asymmetric encryption; also known as public-key encryption, uses two different keys; a public key to encrypt the message, and a private key to decrypt it. Public key techniques are much more intensive than purely symmetric algorithms [3].

Encryptions algorithms can be classified: (i) according to the way in which the original data is processed to stream cipher or block cipher (block cipher which split the original data into blocks, stream cipher which operates on original data bit by bit),and (ii) according to the type of operations used for transforming original data to substitution or transposition techniques (substitution which maps each element in the original data into another element, transposition changes the order of the original data elements, but the elements themselves are not necessarily changed) [3].

4.1 RSA Algorithm

RSA is a public key system proposed by three mathematicians; Ron Rivest, Adi Shamir and Len Adleman. To honor them, the method was referred to as the RSA scheme.

Here E is the encryption key, and D is the decryption key [4-5].

- RSA Encoder:
  1.Choose to large prime numbers; P and Q.
  2.Choose the encryption key; E:
  $$1/E<(P-1)(Q-1) \quad (4)$$
  3. Compute the cipher data: C:
  $$C=M^{E}\bmod(P\times Q) \quad (5)$$
- RSA Decoder:
  1. Compute the decryption key; D:
  $$1/E\bmod\{(P-1)(Q-1)\}=D \quad (6)$$
  2. Compute the reconstructed data; RM:
  $$RM=C^{D}\bmod(P\times Q) \quad (7)$$

4.2 RC4 Algorithm

RC4 is a symmetric key algorithm; the same algorithm is used for both encryption and decryption .The original version of RC4 was designed by Ron Rivest in 1987. The encryption/decryption process is shown in Fig.4 [6]:

1. Create two string arrays.
2. Initial one array with numbers from 0 to 255.
3. Fill the other array with the chosen key.
4. Randomize the first array depending on the array of the key.
5. Randomize the first array within itself to generate the final key stream.
6. XOR the final key stream with the plain audio to be encrypted to give cipher audio or with cipher audio to be decrypted to give reconstruct audio.

4.3 DES Algorithm

Data Encryption Standard (DES) is a symmetric block cipher algorithm that ciphers 64-bit blocks of clear data into 64-bit of cipher data that uses 56-bit keys. The encryption/decryption is performed in 16 stages (rounds) [5, 8, 14]. The encryption process is shown in Fig.2, while decryption process is same as encryption except the cipher data is passed through a permutation called the Inverse IP, and the sub keys are applied in reverse order, from c[16] to c[1] ,and d[16] to d[1].

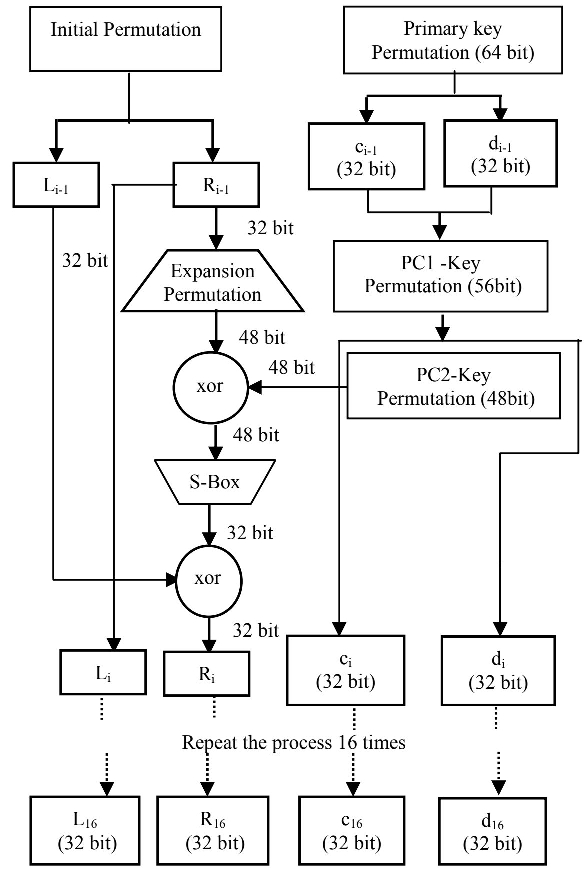

Fig.2. Encryption Process of DES Algorithm

4.4 3DES Algorithm

Triple DES(3DES) encrypted original data three times ; first encrypted it with 56-bit key K_1 by applying DES encryption and then applying DES decryption with 56-bit key K_2 final applying DES 56-bit key K_1 .Decryption process is inverse of encryption process[5].

To encrypt plain audio A to C using K_1 and K_2

$$C = E_{K_1}\left(D_{K_2}\left(E_{K_1}(M)\right)\right) \quad (8)$$

To decrypt cipher audio C to RA using K_1 and K_2

$$RM = D_{K_1}\left(E_{K_2}\left(D_{K_1}(C)\right)\right) \quad (9)$$

4.5 IDEA Algorithm

International Data Encryption Algorithm (IDEA) is a block cipher designed by Xuejia Lai and James Massey. It is 64-bit iterative block with 128-bit key. Each round (R) of encryption /decryption consists of following steps [10-11]:

1. $M_1 \times Z_1^{(R)}$
2. $M_2 + Z_2^{(R)}$
3. $M_3 + Z_3^{(R)}$
4. $M_4 \times Z_4^{(R)}$
5. XOR the result from steps 1and 3.
6. XOR the result from steps 2and 4.
7. Result from step 5 and $Z_5^{(R)}$ are multiplied.
8. Result from step 6 and 7 are added.
9. Result from step 8 and $Z_6^{(R)}$ are multiplied.
10. Result from step 7 and 9 are added.
11. XOR the result from steps 1 and 9.
12. XOR the result from steps 3 and 9.
13. XOR the result from steps 2 and 10.
14. XOR the result from steps 4 and 10.

The swap results from steps 12 and 13.The final values from steps 11-14 form the output of the round. After round 8, the final output transformation is as follows:

1. $M_1 \times Z_1^{out}$ (First sub key of output transformation)
2. $M_2 + Z_2^{out}$
3. $M_3 + Z_3^{out}$
4. $M_4 \times Z_4^{out}$

Different between encryption and decryption is sub keys $Z_1^{(R)} - Z_6^{(R)}$ .Decryption sub keys are generated from encryption sub keys.

4.6 AES Algorithm

The Advanced Encryption Standard (AES) is a block cipher ratified as a standard by National Institute of Standard and Technology of the United States (NIST). Encryption process is as shown in Fig.3 while decryption process is same as encryption process except use inverse sub byte [12-13].

4.7 Blowfish Algorithm

Blowfish is a symmetric block cipher just like DES or IDEA. It takes a variable-length key, from 32 to 448 bits and it is designed as a fast, free alternative to the then existing encryption algorithms. Since Blowfish has been analyzed considerably, and is gaining acceptance as a strong encryption algorithm. The algorithm consists of: (i) key Expansion Part; the P-array consists of eighteen 32-bit sub keys: P_1, P_2... P_{18} and There are four 32-bit S-boxes with 256 entries, (ii) Data encryption part as the following [14]:

1. Divide a 64-bit data into two 32-bit halves: xL, xR
2. xL = xL XOR P_1.
3. xR = F(xL) XOR xR.
4. Swap xL and xR.
5. Repeat steps from1 to 4 sixteen round.
6. Swap xL and xR.
7. xR = xR XOR P_{17}.
8. xL = xL XOR P_{18}.
9. Recombine xL and xR.

Divide xL into four eight-bit quarters: a, b, c, and d; where: F (xL) = (S_1(a)+ S_2(b) mod 2^32) XOR S_3(c)) + S_4(d) mod 2^32. Decryption is exactly the same as encryption, except that P_1, P_2... P_{18} are used in the reverse order.

4.8 Proposed Technique

We proposed cascaded technique which is cascaded between selected stream cipher and block cipher. We cascaded between (i) IDEA algorithm and RSA algorithm (IRCA), (ii) AES algorithm and RSA algorithm (ARCA), and (iii) Blowfish algorithm and RSA algorithm (BRCA).This proposed technique provided security and speed.

5. Results

The above techniques were applied on text, audio and grey scale image data using Matlab R2009b on windows7 which its specifications' are: (i) 64-bit operating system , (ii) processor of 2GHz ,and (iii) 3 GB RAM for software simulation which shown that blowfish given the best result for select technique and cascaded between AES and RSA algorithms (ARCA) for proposed technique based on the resulting of R, MSE and BCR of text, audio ,and grey scale image data are listed in Table 1,Table 2 , and Table 3 receptively and the speed (encryption time (TE), decryption time (TD) and total time (TT)) of text, audio ,and grey scale image data are listed in Table 4,Table 5 , and Table 6 receptively. The original, encrypted and reconstructure text were shown in Fig.4-13. The original, encrypted and reconstructure audio were shown in Fig.14-

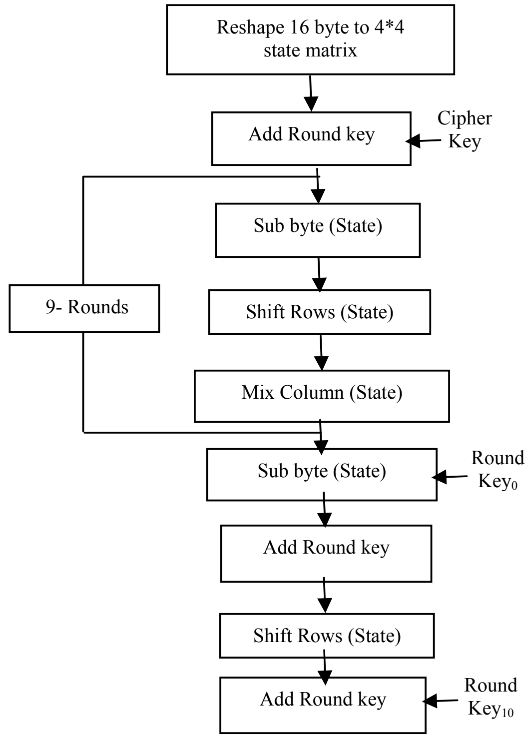

Fig.3 Encryption Process of AES

17. The original, encrypted and reconstructure grey scale image were shown in Fig.18-20.

Implementation of the selected techniques has been done for Virtex-5 FPGA XC5VLX110TFF136 . These techniques were tested initially for behavioral and then for post place & route. The Simulation tools used were ModelSim 6.3a Student Edition with Xilinx ISE 9.2i Simulation download tool. The RTL (Register Transistor Level) results were shown in Fig.21-27 and area reports were listed at Table 7-13 which shown that IDEA is the best depend on area and CLB (Configurable Logic Block) results that shown in Table-14.

Plaintext: Wallaa Mohamed Kamal El-Din Ahmed Ali El-Morshedy

Ciphertext: ??????????? ????????????????????????????????????? ??

Reconstruct text: Wallaa Mohamed Kamal El-Din

Fig.4 Plaintext, Cipher text using RSA and Reconstruct text

Plaintext: Wallaa Mohamed Kamal El-Din Ahmed Ali El-Morshedy

Ciphertext:?? ???????

Reconstruct text: Wallaa Mohamed Kamal El-Din Ahmed Ali El-Morshedy

Fig.5 Plaintext, Cipher text using RC4 and Reconstruct text

IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 3, March 2012
ISSN (Online): 1694-0814
www.IJCSI.org

Plaintext: Wallaa Mohamed Kamal El-Din Ahmed Ali El-Morshedy

Ciphertext: ???2 ???+?E?£©?-û[¾÷°???Ydi??¯â?A?¢O?I%?

Reconstruct text: Wallaa Mohamed Kamal El-Din Ahmed Ali El-Morshedy

Fig.6 Plaintext, Cipher text using DES and Reconstruct text

Plaintext: Wallaa Mohamed Kamal El-Din Ahmed Ali El-Morshedy

Ciphertext: ?²³??×JE¦4??¥???¾$??p????Y??B?¬w?®??J?¨d?y

Reconstruct text: Wallaa Mohamed Kamal El-Din Ahmed Ali El-Morshedy

Fig.7 Plaintext, Cipher text using 3DES and Reconstruct text

Plaintext: Wallaa Mohamed Kamal El-Din Ahmed Ali El-Morshedy

Ciphertext:/2 (??N?»?WZpK 9?9?'6?????¸?b\?T~S8ùc??

Reconstruct text: Wallaa Mohamed Kamal El-Din Ahmed Ali El-Morshedy

Fig.8 Plaintext, Cipher text using IDEA and Reconstruct text

Plaintext: Wallaa Mohamed Kamal El-Din Ahmed Ali El-Morshedy

Cipher text: ô©4¤F`?q k? £?]<OI?Pâ[eê4?[q?}? G=½[D?2IM´

Reconstruct text: Wallaa Mohamed Kamal El-Din Ahmed Ali El-Morshedy

Fig.9 Plaintext, Cipher text using AES and Reconstruct text

Plaintext: Wallaa Mohamed Kamal El-Din Ahmed Ali El-Morshedy

Ciphertext: tl?[¹???????¤?¹? h?J?é??÷??¢v???;³P¥?l?s???

Reconstruct text: Wallaa Mohamed Kamal El-Din Ahmed Ali El- Morshedy

Fig.10 Plaintext, Cipher text using Blowfish and Reconstruct text

Plaintext: Wallaa Mohamed Kamal El-Din Ahmed Ali El-Morshedy

Cipher text: -©Q

Reconstruct text: Wallaa Mohamed Kamal El-Din Ahmed Ali El- Morshedy

Fig.11 Plaintext, Cipher text using IRCA and Reconstruct text

Plaintext: Wallaa Mohamed Kamal El-Din Ahmed Ali El-Morshedy

Cipher text: Q

Reconstruct text: Wallaa Mohamed Kamal El-Din Ahmed Ali El- Morshed

Fig.12 Plaintext, Cipher text using ARCA and Reconstruct text

Plaintext: Wallaa Mohamed Kamal El-Din Ahmed Ali El-Morshedy

Cipher text: Q

Reconstruct text: Wallaa Mohamed Kamal El-Din Ahmed Ali El- Morshed

Fig.13 Plaintext, Cipher text using BRCA and Reconstruct text

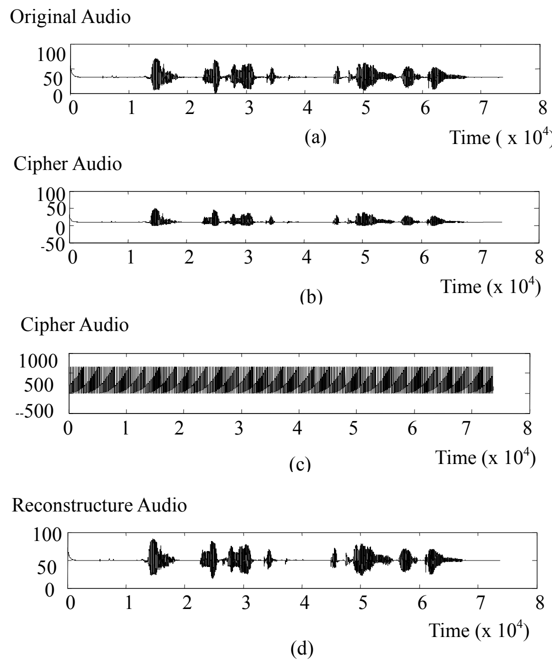

Fig.14 (a) Original Audio, Cipher Audio (b) using RSA, (c) using RC4 ,and(d) Reconstruct Audio

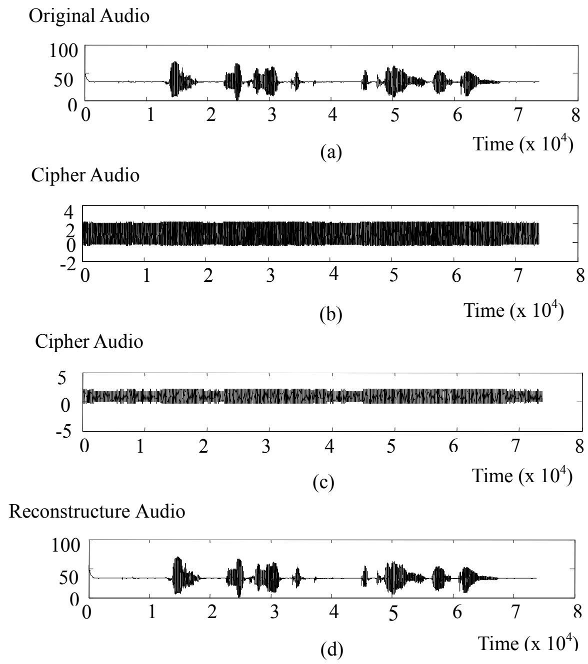

Fig.15 (a) Original Audio, Cipher Audio,(b) using DES ,(c) using 3DES,and (d) Reconstruct Audio

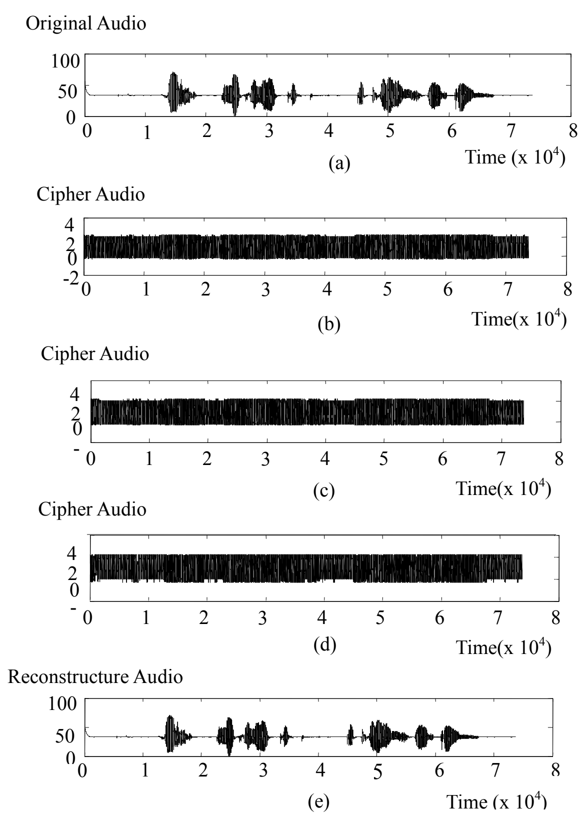

Fig.16 (a) Original Audio, Cipher Audio, (b) using IDEA , (c) using AES ,(d) using Blowfish ,and (e) Reconstruct Audio

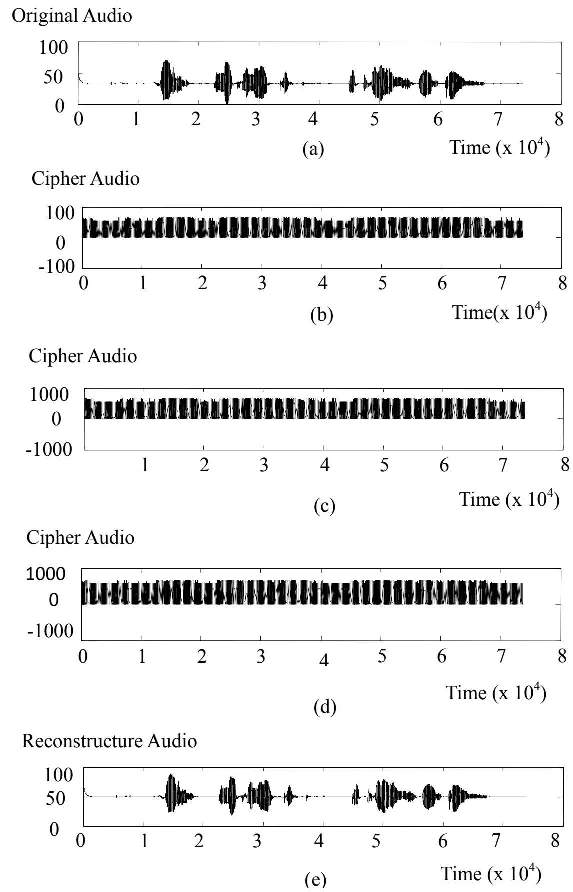

Fig.17 (a) Original Audio, Cipher Audio, (b) using IRCA , (c) using ARCA ,(d) using BRCA ,and (e) Reconstruct Audio

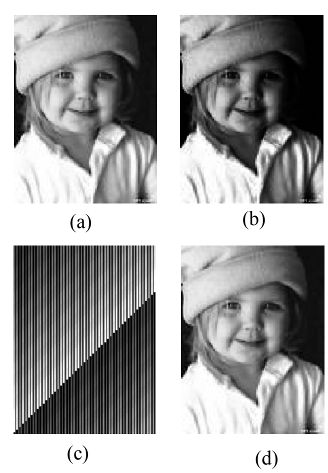

Fig.18 (a) Original Image, Cipher Image (b) using RSA, (c) using RC4, and (d) Reconstruct Image

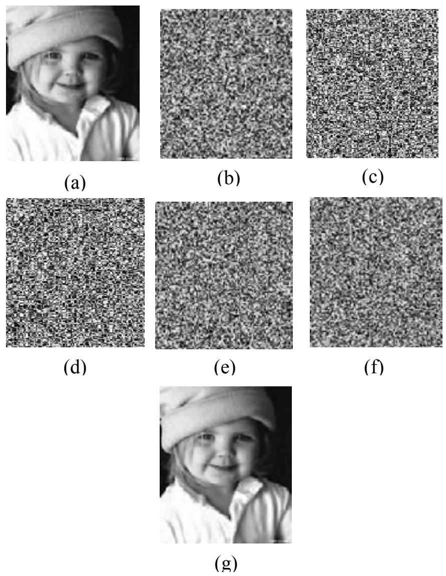

Fig.19 (a) Original Image, Cipher Image, (b) using DES ,(c) using 3DES, (d) using IDEA , (e) using AES ,(f) using Blowfish, and (g) Reconstruct Image

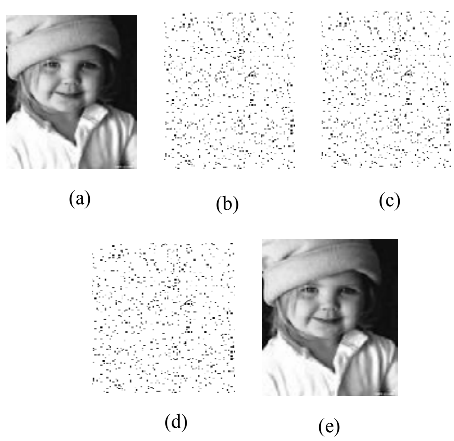

Fig.20 (a) Original Image, (b) Cipher Image using IRCA, (c) using ARCA, (d) using BRCA, and (e) Reconstruct Image

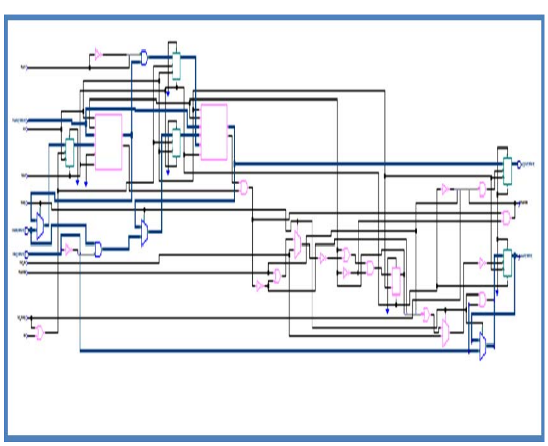

Fig.21 RTL of RSA Algorithm

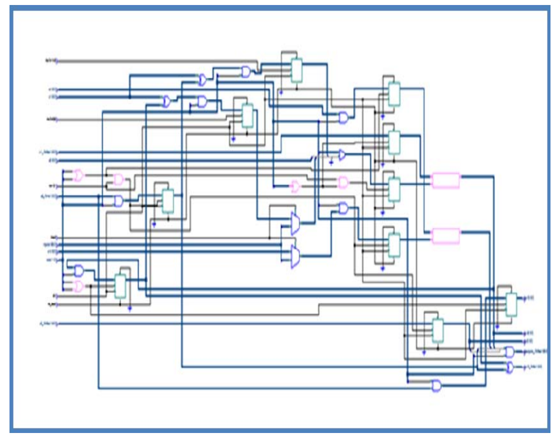

Fig.22 RTL of RC4 Algorithm

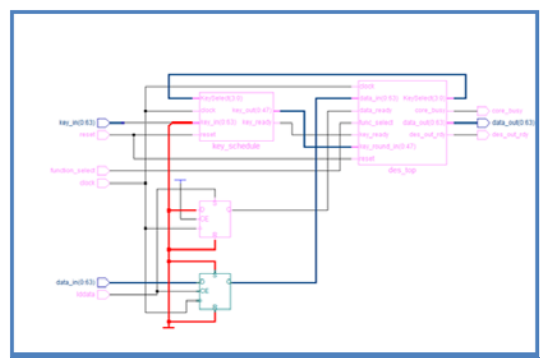

Fig.23 RTL of DES Algorithm

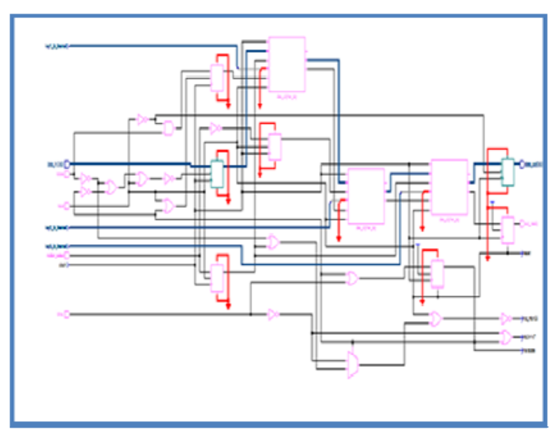

Fig.24 RTL of 3DES Algorithm

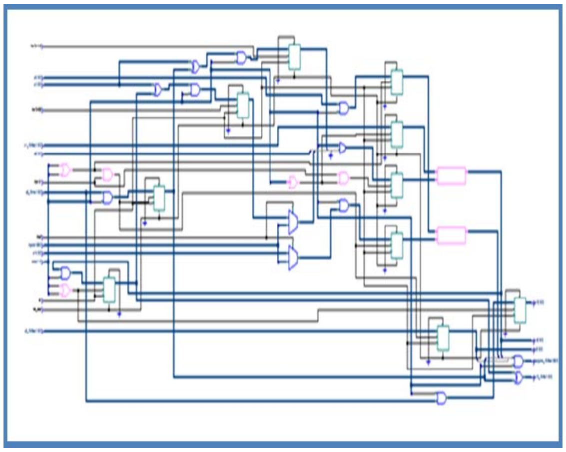

Fig.25 RTL of IDEA Algorithm

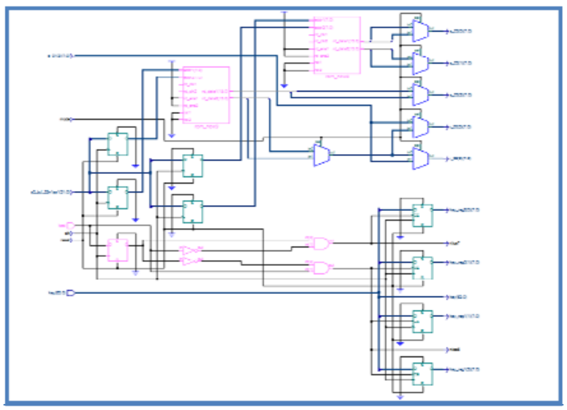

Fig.26 RTL of AES Algorithm

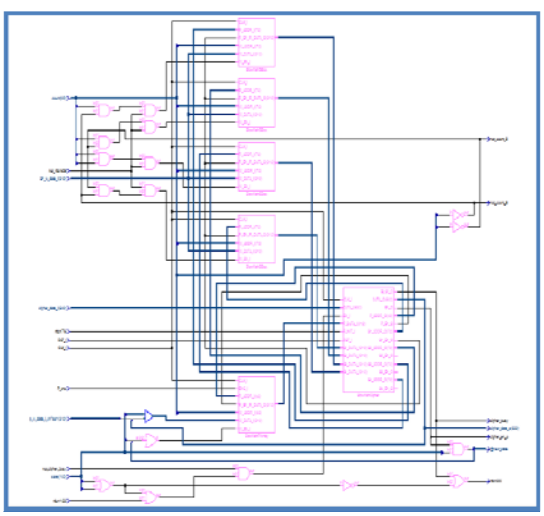

Fig.27 RTL of Blowfish Algorithm

Table 1: R, MSE, AND BCR RESULTS OF TEXT DATA

Algorithm	***R***	***MSE***	***BCR***
RSA	1	0	1
RC4	1	0	1
DES	1	0	1
3DES	1	0	1
IDEA	1	0	1
AES	1	0	1
Blowfish	1	0	1
IRCA	1	0	1
ARCA	0.9059	0.251	0.9898
BRCA	0.8427	0.251	0.9872

Table 2: R, MSE, AND BCR RESULTS OF AUDIO DATA

Algorithm	***R***	***MSE***	***BCR***
RSA	1	0	1
RC4	1	0	1
DES	1	0	1
3DES	1	0	1
IDEA	1	0	1
AES	1	0	1
Blowfish	1	0	1
IRCA	1	0	1
ARCA	1	0	1
BRCA	1	0	1

Table 3: R, MSE, AND BCR RESULTS OF GREY SCALE IMAGE DATA

Algorithm	***R***	***MSE***	***BCR***
RSA	1	0	1
RC4	1	0	1
DES	1	0.1279	1
3DES	0.9998	2.4755	1
IDEA	1	0.2782	1
AES	1	0.0135	1
Blowfish	1	0	1
IRCA	1	0.135	1
ARCA	1	0.251	1
BRCA	0.9999	0.17	0.9999

Table 4: TE, TD, AND TT RESULTS OF TEXT DATA

Algorithm	*TE (Second)*	*TD (Second)*	*TT (Second)*
RSA	0.0244	0.0021	0.0265
RC4	0.0509	0.1655	0.2164
DES	0.0046	0.0044	0.0046
3DES	109.4427	34.1667	143.6094
IDEA	218.8854	68.3334	287.2188
AES	328.3281	102,5001	430.8282
Blowfish	2.5493	2.7037	5.2530
IRCA	0.6449	0.2606	0.3843
ARCA	0.0361	0.0213	0.0148
BRCA	0.0886	0.0483	0.0403

Table 5: TE, TD, AND TT RESULTS OF AUDIO DATA

Algorithm	*TE (Second)*	*TD (Second)*	*TT (Second)*
RSA	5.9498e-004	6.4394e-05	6.5937e-004
RC4	0.0648	0.0045	0.0694
DES	1.5756e-004	8.7441e-05	2.4500e-004
3DES	0.4525	0.1636	0.6161
IDEA	0.9050	0.3272	1.2322
AES	1.3575	0.4908	1.8483
Blowfish	0.1795	0.1021	0.2816
IRCA	0.0151	0.0231	0.0381
ARCA	0.0069	0.0061	0.0129
BRCA	51.3694	65.1785	116.5479

Table6: TE, TD, AND TT RESULTS OF GREY SCALE IMAGE DATA

Algorithm	*TE (Second)*	*TD (Second)*	*TT (Second)*
RSA	0.0018	0.0056	0.0073
RC4	0.0117	0.1481	0.1598
DES	89.4487	31.6038	121.0525
3DES	268.3461	94.88114	381.1575
IDEA	2.2723	2.2844	4.5567
AES	0.0154	0.0226	0.0381
Blowfish	0.0063	0.0062	0.0125
IRCA	11.6396	5.3423	6.2973
ARCA	0.1257	0.0785	0.0472
BRCA	24.2725	9.0788	15.19369

Table7: RESOURCE USED IN THE FPGA IMPLEMENTATION OF DES

ISO	197	640	30.78%
Global Buffers	1	32	3.13%
Function Generators	722	69120	1.04%
CLB Slices	181	17280	1.05%
Dffs or Latches	265	70400	0.38%
Block RAMs	0	148	0.00%
DSP48Es	0	64	0.00%

Table8: RESOURCE USED IN THE FPGA IMPLEMENTATION OF 3DES

ISO	709	640	110.78 %
Global Buffers	1	32	3.13%
Function Generators	2452	69120	3.55%
CLB Slices	613	17280	3.55%
Dffs or Latches	1205	70400	1.71%
Block RAMs	0	148	0.00%
DSP48Es	0	64	0.00%

Table9: RESOURCE USED IN THE FPGA IMPLEMENTATION OF IDEA

ISO	261	640	40.78%
Global Buffers	1	32	3.13%
Function Generators	493	69120	0.71%
CLB Slices	124	17280	0.72%
Dffs or Latches	235	70400	0.62%
Block RAMs	0	148	0.00%
DSP48Es	0	64	0.00%

Table10: RESOURCE USED IN THE FPGA IMPLEMENTATION OF AES

ISO	261	640	40.78%
Global Buffers	1	32	3.13%
Function Generators	2972	69120	4.30%
CLB Slices	743	17280	4.30%
Dffs or Latches	787	70400	1.12%
Block RAMs	0	148	0.00%
DSP48Es	0	64	0.00%

Table11: RESOURCE USED IN THE FPGA IMPLEMENTATION OF BLOWFISH

ISO	584	640	91.25%
Global Buffers	1	32	3.13%
Function Generators	835	69120	1.21%
CLB Slices	209	17280	1.14%
Dffs or Latches	804	70400	1.71%
Block RAMs	0	148	4.05%
DSP48Es	0	64	0.00%

Table12: RESOURCE USED IN THE FPGA IMPLEMENTATION OF RSA

ISO	603	640	94.22%
Global Buffers	1	32	3.13%
Function Generators	3191	69120	4.62
CLB Slices	798	17280	3.00%
Dffs or Latches	2112	70400	20.38%
Block RAMs	0	148	0.00%
DSP48Es	2	64	3.13%

Table13: RESOURCE USED IN THE FPGA IMPLEMENTATION OF RC4

ISO	338	640	52.81%
Global Buffers	1	32	3.13%
Function Generators	295	69120	0.43%
CLB Slices	74	17280	0.43%
Dffs or Latches	115	70400	0.16%
Block RAMs	0	148	0.00%
DSP48Es	0	64	0.00%

Table14: AREA AND CLB RESULTS

Algorithm	***Area***	***CLB***
RSA	94.22%	3.00%
RC4	52.81%	0.43%
DES	30.78%	1.05%
3DES	110.78%	3.55%
IDEA	40.78%	0.72%
AES	40.78%	4.30%
Blowfish	91.25%	1.14%

6. CONCLUSION

Multimedia encryption takes importance this days as multimedia data is needed to protect from unwanted and these encryption algorithms is classified to stream and block cipher or symmetric and asymmetric. We merge RSA which is stream cipher and used asymmetric keys algorithm with IDEA, AES and Blowfish algorithms which are block cipher and used asymmetric and symmetric keys which provided more security and speed.

References

[1] A.J. Menezes, P.C. van-Oorschot, and S.A. Vanstone, "Handbook of Applied Cryptography", University of Waterloo, Ontario, Canada, ISBN: 9780849385230, 4th edition, 2010.

[2] R. A. Mollin, "An Introduction to Cryptography", CRC Press, Inc. Boca Raton, FL, USA, ISBN: 1584881275, 4th edition, 2006.

[3] W. Mao, "Modern Cryptography Theory and Practice",Prentice Hall, ISBN: 9780130669438,2003.

[4]N.Hoffman,"A Simplified IDEA Algorithm ",Journal:Crptologia archive,Vol.31,Taylor &Francis,Inc,Bristol,PA,USA,2007.

[5] B. Furht, E. Muharemagic and D. Socek ,"Multimedia Encryption and Watermarking", Florida Atlantic University Boca Raton FL, USA ,ISBN:0387244255,2005.

[6] A. Mousa and A. Hamad, "Evaluation of the RC4 Algorithm for Data Encryption,",PalTel Company, Nablus, Palestine, International Journal of computer Science and Applications,vol.3,No.2 2006.

[7] B. Schneier, "Applied Cryptography" Prentice Hall, ISBN: 0471128457, 2nd edition 2003.

[8] M. Ciampa, "Security+ Guide to Network Security Fundamentals, Course Technology Ptr Publication,ISBN 13: 9781428340664, 2008.

[9]F. Harold and M. Krause," Information Security Management Handbook, Sixth Edition ",Taylor &Franceis Group,LLC, ISBN: 9780849374951,2007.

[10] H .C.Thomas,E.L.Charles ,E. Leiserson, L. R.Ronald and C. Stein , "Introduction to Algorithms, Second Edition", MIT Press and McGraw-Hill, ISBN: 0262032937, 2001.

[11] N.Hoffman,"A Simplified IDEA Algorithm ",Journal:Crptologia archive,Vol.31,Taylor &Francis,Inc,Bristol,PA,USA,2007.

[12] B. Furht , D. Socek and A. M. Eskicioglu "Fundamentals of Multimedia Encryption Techniques ", Multimedia Security Handbook,ISBN:0849327733,2005.

[13] A .Pommer and A.Uhl ,"Selective Encryption of Wavelet-Packet Encoded Image Data Efficiency and Security ", Journal of Network Security & Its Application (IJNSA), Vol.2, No.1,2010.

[14] T. Nie and T. Zhang,"A Study of DES and Blowfish Encryption Algorithm ",Commun. & Electron. Eng. Inst., Qingdao Technol. Univ., Qingdao, China, ISBN: 9781424445462, 2009.

Mohamed Abdel-Azim received the PhD degree in Electronics and Communications Engineering from the Faculty of Engineering-Mansoura University-Egypt by 2006. After that he worked as an assistant professor at the Electronics & Communications engineering department until now. He has 40 publications in various international journals and conferences. His current research interests are in multimedia processing, wireless communication systems, and Field Programmable Gate Array (FPGA) applications.

W.M. Kamal-Eldin received BSc in Electronics and Communications, Master student