Development AES Algorithm to Encryption Images and Sounds Files

Mohammed C.Y. Al-Zubaidy

College of Computer Sciences and Mathematics
University of Mosul

Received on: 29/05/2011 **Accepted on: 16/08/2011**

ABSTRACT

In this research, the Advanced Encryption Standard (AES) algorithm was developed, the AES is used for encryption and decryption the images and sounds files by expanding the block size of data to reach the maximum size of 512 bit instead 128 bit/cycle, by using the Thread API techniques, which is a break off CPU working for increasing times taken the inline encrypt or decrypt operations. The data entranced from the file by size 512 bits per cycle, is converted to one dimension matrix by block size which is 2048 bit. The method considered 4−lines using 4 AES, which in every line, one AES is working in a distinct system.

Transmission and reception of encoded files could be performed by using Email programs provided that the sent file does not include the encoding key for the purpose of protecting encoded files against unauthorized access.

In addition to the use of the histogram in this research by comparing the block size of images or sounds files through the encrypting or decrypting system by scanning bit to bit operations. The implement algorithm with a sample of histogram was used to ensure that the data is not changed throughout this study.

Keywords: AES Algorithm , Encryption, Images Files, Sounds Files.

تطوير خوارزمية AES لتشفير الصور وملفات الأصوات

محمد الزبيدي

كلية علوم الحاسوب والرياضيات

جامعة الموصل

تاريخ الاستلام: 2011/29/05 **تاريخ القبول: 2011/08/16****الملخص**

تم في هذا البحث تطوير خوارزمية التشفير القياسية AES لغرض تشفير الملفات الصورية والصوتية من خلال توسيع الحجم الكتلي للبيانات ليصل إلى أعلى ما يمكن (512 bit) بدلا من (128 bit) لكل دورة، وذلك باستخدام تقنية التجزئة Threads API والتي تعمل على تجزئة عمل الـ CPU لأجل تقليل الوقت الذي يقضيه بعمليات التشفير وفك التشفير الحسابية، والتي يتم فيها إدخال البيانات الصورية والصوتية بحجم كتلي يصل إلى (512 bit) لكل دورة، إذ يتم تحويلها إلى مصفوفة أحادية بحجم كتلي (2048 bit) باستخدام أربعة خطوط رئيسية (4 AES)، كل خط يكون فيه AES واحدة تعمل بشكل منفصل عن الأخرى.

ويمكن أن تتم عملية الإرسال والاستقبال للملفات المشفرة باستخدام برامج البريد الإلكتروني المعروفة، مع عدم تضمين مفتاح التشفير داخل الملف المرسل لحماية الملفات المشفرة من الاختراق.

تم حساب الأرقام الثنائية للملفات الصورية والصوتية الأصلية والمشفرة من خلال عرض المنحني التكراري(Histogram) بقراءة البيانات (bit to bit) لأجل مطابقة كتل الملفات قبل وبعد تشفيرها للوصول إلى حالة التأكد التام من عدم تغير القيم الثابتة في بيانات الملفات بعد أخذ عينات منها وتطبيق الخوارزمية المقترحة عليها.

الكلمات المفتاحية: خوارزمية AES ، التشفير ، ملفات الصور ، ملفات الأصوات.

1. Introduction to Cryptography

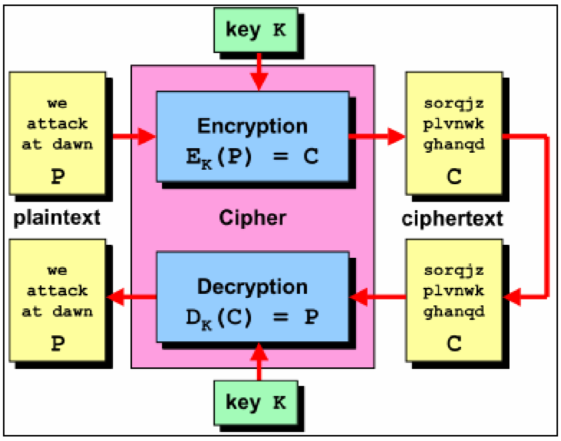
Cryptography is the science of secret codes, enabling the confidentiality of communication through an insecure channel that is protected against unauthorized parties, by preventing unauthorized alteration of use [Vaudenay, 2005].

Generally speaking, it uses a cryptographic system to transform a plaintext into a cipher-text using most of the time a key, figure(1), one has to notice that there exists certain ciphers that do not need a key at all [Steffen, 2005].

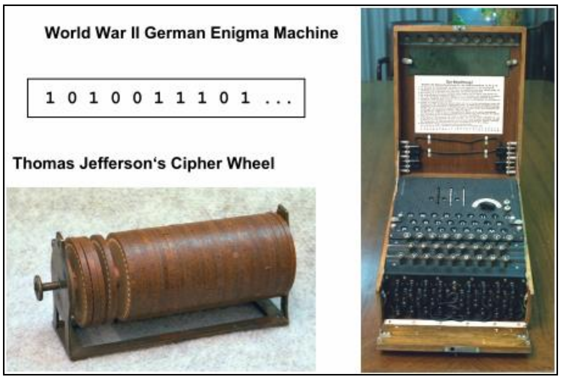
A simple Caesar−cipher that obscures text by replacing each letter with the letter thirteen placed down in the alphabet, since our alphabet has 26 characters, it is enough to encrypt the ciphertext again to retrieve the original message [Vaudenay, 2005].

Briefly, that there is securing public−key ciphers, like the famous and very secures, is commonly called Rivest Shamir Adleman (RSA) algorithm that uses a public key to encrypt a message and a secret key to decrypt it, cryptography is a very important domain in computer science with many applications, where the most famous example of cryptography is certainly the Enigma machine in World War II, figure(2), the legendary cipher machine is used by the German Third Reich to encrypt their messages, whose security breach ultimately led to the defeat of their submarine force, cryptography which has long been of interest to intelligence gathering agencies and law enforcement agencies because of its facilitation of privacy and the diminution of privacy attendant on its prohibition, cryptography is also of considerable interest to civil rights supporters, accordingly, there has been a history of controversial legal issues surrounding cryptography; especially since the advent of inexpensive computers has made possible widespread access to high quality cryptography [Haan, 2007] [Steffen, 2005].

In some countries, even the domestic use of cryptography is, or has been, restricted until 1999, France significantly restricted the use of cryptography domestically, in China, a license is still required to use cryptography, and many countries have tight restrictions on the use of cryptography, among the more restrictive are laws in Belarus, Kazakhstan, Mongolia, Pakistan, Russia, Singapore, Tunisia, Venezuela, and Vietnam [Haan, 2007].



Figure(1): The basic encryptions [Steffen, 2005].


World War II German Enigma Machine
1 0 1 0 0 1 1 1 0 1 ...
Thomas Jefferson's Cipher Wheel

Figure(2): Enigma machine in World War II[Steffen, 2005].

2. Introduction to Advanced Encryption Standard

Advanced Encryption Standard(AES) is a formal encryption method adopted by the National Institute of Standards and Technology of the US Government, and is accepted worldwide[Townsend, 2009].

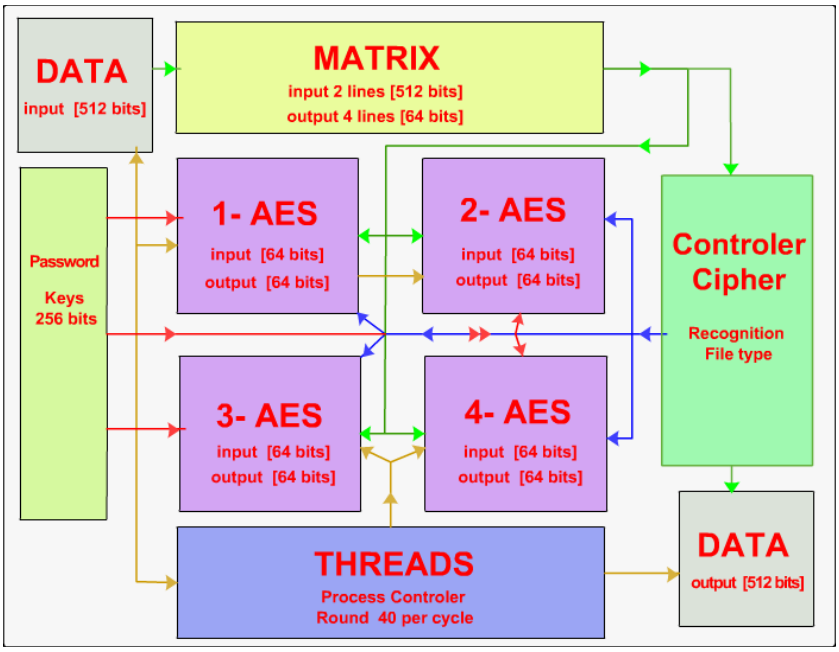
This paper introduces AES and key management, and discusses some important topics related to a good data security strategy.

The AES algorithm is a symmetric block cipher that can encrypt encipher and decrypt decipher, where the information encrypted converts data to an unintelligible form called ciphertext; decrypting the ciphertext converts the data back into its original form called plaintext[US Federal Information, 2001].

It uses 128, 192 and 256 bits block size with a single key as a part of the encryption process are 128, 192 or 256 bits, the term 128−bit encryption refers to the use of a 128−bit encryption key[Roche, 2007].

In AES, both the encryption and the decryption are performed by using the same key, this is called a symmetric encryption algorithm, where the encryption algorithms that use two different keys, a public and a private key, are called asymmetric encryption algorithms[Townsend, 2009].

The standard AES, with maximum sizes 256 bit /cycle is founded as a result of the standard algorithm software in this study, the result was very low in the processed of this data. Finally, increased with low spend a high physical memory in the system used which is more than 4096 bits/cycle. The stands read/write operations which are used in this software, they involve the algorithm in pipe line processing, data processed in the 4 lines that selected in this algorithm, every line takes 64 bits per cycle, with a result of 512 bit/cycle, it still uses the key size 256 bits in this involved, but that means, it's possible to increase the key size in the same way. On the other hand, the key may increase as data processed, AES was developed to enable to uses 512 bits key size, in the center ProtectStar™ Research, they modified the key size up to 512 and the data processed up to max 512 bit /cycle, where the rounded key is 24 cycle[Wikpedia, 2008]. As data increase the time's process decreases times, this means that the data will take a large data to perform a low time processing, and to encrypt files that take data size 1GB, these mixed times will be more sensitive to reach a few minutes sort data a low break off CPU and the highest process called the Threads API Techniques, figure(3).

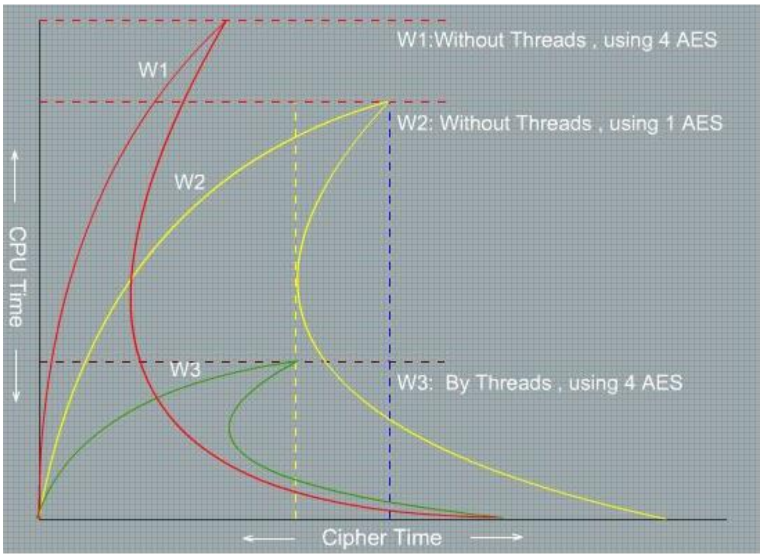


Figure(3): The development by using 4-AES with Threads API technique.

3. The Aim of the Study

In this study, the AES algorithm was developed to encrypt and decrypt the images and sounds files by using Visual C++ v.6 language, where the software package increases data decrypt/encrypt to reach this normal level and makes processed large data in a very limited time with a very low used physical memory, figure(4). This software works on a limited physical memory, it works properly in less than 32 MB to have the action been performed; the data have been selected in very low stores bytes, while the program processed in mode is either encrypted or decrypted.

There are many areas where AES is now in commercial use, including offerings from Checkpoint, Cisco, and Symantec. AES is now commonly found in network appliance, also the voice over IP vendors are using AES for telephone security, and AES has even been added to common file compression programs, such as WinZip, WinRar and 7-Zip.



Figure(4): Histogram of three different stages to the condition of states on CPU/Cipher time using or not the Threads API techniques:

Where W1 refers to the highest level of numbers recorded as a red line by using the algorithm study(4 AES) with non threads applied, the times to cipher are still long too.
W2 refers to the use of one AES standard without Threads and noted here the level is lower than the red level, but this state is still abnormal operation as a yellow line showed, also the times to cipher are still long. But the W3 as a green line showed in this figure as the best level reached to the highest speed, and shortest time elapsed showed by using 4 AES with threads applied to.

4. Review to the Other Literatures

The AES is used by many researchers for encrypt plain text only, it was limited to encrypt a large size files, and it takes a long time to encrypt the large plain text files, in this case on its block data is 64 per cycle. The necessary order developed this algorithm by ProtectStar™ [Wikpedia, 2008].

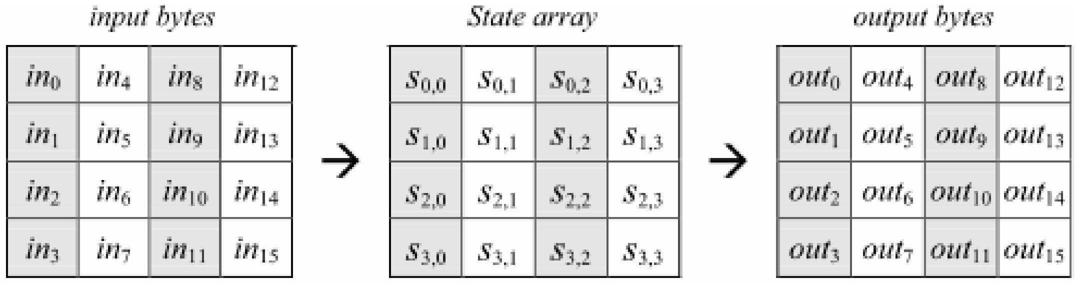
The Researcher patrick Townsend is succeeded in increasing the block size from 64 to 512 per cycle, and increasing the rounds from 12 to 24 by different methods of using keys with the AES, these different methods are called "modes of operation", the National Institute of Standards and Technology (NIST) defines six modes of operation that can be used with AES: Electronic Code Book(ECB), Cipher Block Chaining(CBC), Cipher Feed Back (CFB), Output Feed Back(OFB), Galois Counter Mode(GCM) and Counter (CTR) where CTR is default mode in AES algorithm[Townsend, 2009].

Some researchers changed the name of this algorithm from AES to new name "ProtectStar Extended AES Algorithm", the results increase the time's line process with a high large file length, for example, 1GB takes a few minutes to complete the encryption, unlike the standard AES which take a longer time if compared with the former[Wikpedia, 2008].

5. Description of the AES Algorithm

The original name of the AES algorithm was Rijndael, it was chosen as the algorithm for the Advanced Encryption Standard(AES) in 2001 by Joan Daemen and Vincent Rijmen, Rijndael, it consists of a number of rounds, each round makes a number of transformations on a state, and uses a round key derived from the encryption key, the number of rounds depends on the block and key size, an encryption of a block starts with a transformation AddRoundKey, this is followed by an odd number of regular rounds, and ends with a special final round, the reason of the final round is different which has nothing to do with security, but was done to make it possible to reuse encryption code to do the decryption[Daemen and Rijmen, 1998].

All the transformations used are invertible, which make decryption possible, Rijndael operates on a state that is initialized with a plaintext block, and after encryption this contains the cipher-text, the state can be pictured as an rectangular array of bytes, it consists of four rows and a number of columns defined by the block size in bytes divided by four, a block size of 128 bit would require a state of four rows and(128/8=4*4) columns as shown in figure(5).



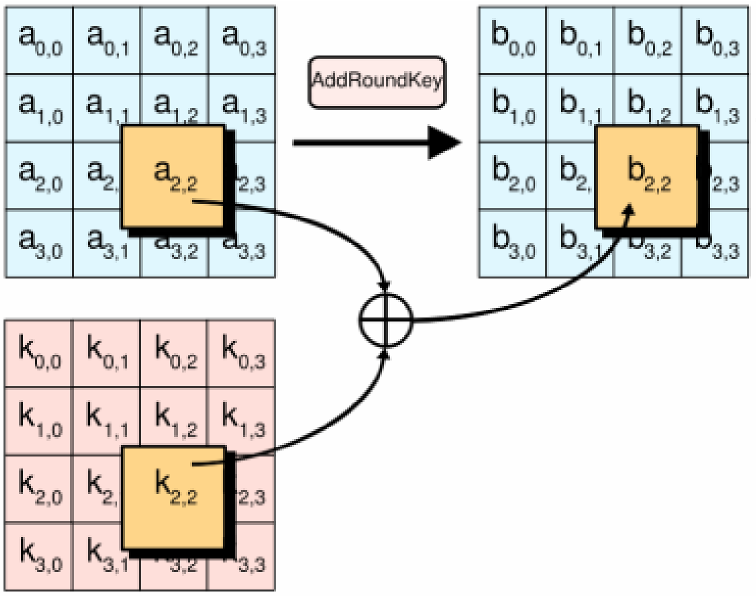
in_0	in_4	in_8	in_{12}
in_1	in_5	in_9	in_{13}
in_2	in_6	in_{10}	in_{14}
in_3	in_7	in_{11}	in_{15}

$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,0}$	$s_{1,1}$	$s_{1,2}$	$s_{1,3}$
$s_{2,0}$	$s_{2,1}$	$s_{2,2}$	$s_{2,3}$
$s_{3,0}$	$s_{3,1}$	$s_{3,2}$	$s_{3,3}$

out_0	out_4	out_8	out_{12}
out_1	out_5	out_9	out_{13}
out_2	out_6	out_{10}	out_{14}
out_3	out_7	out_{11}	out_{15}

Figure(5): State array for impute and output [Winterthur 2002].

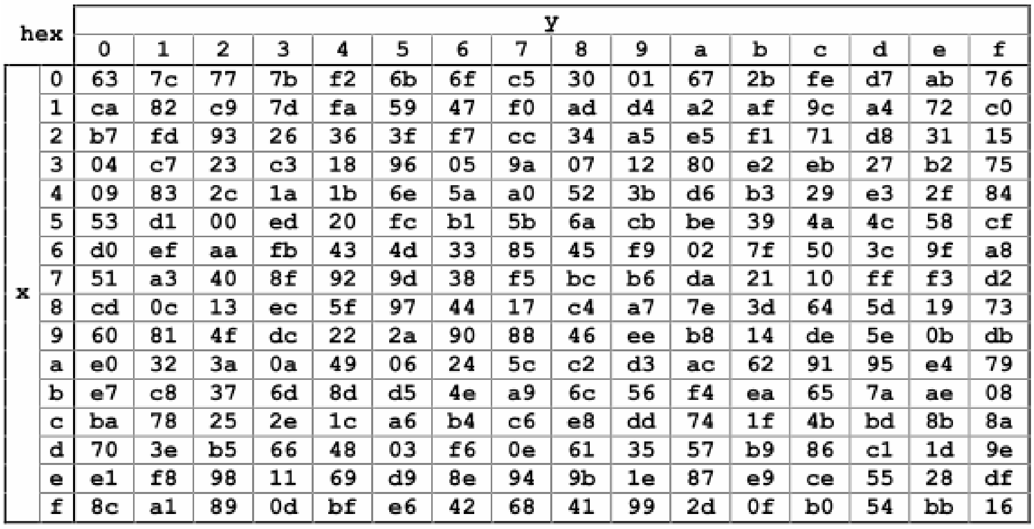
The details of the main part of AES algorithm which flowed in this research are:
5-1 Add Round Key:
It is an XOR between the state and the Roundkey, this transformation is of its own inverse as shown in figure(6).


$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
AddRoundKey
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$
$\oplus$
$k_{0,0}$ $k_{0,1}$ $k_{0,2}$ $k_{0,3}$
$k_{1,0}$ $k_{1,1}$ $k_{1,2}$ $k_{1,3}$
$k_{2,0}$ $k_{2,2}$ $k_{2,3}$
$k_{3,0}$ $k_{3,1}$ $k_{3,2}$ $k_{3,3}$

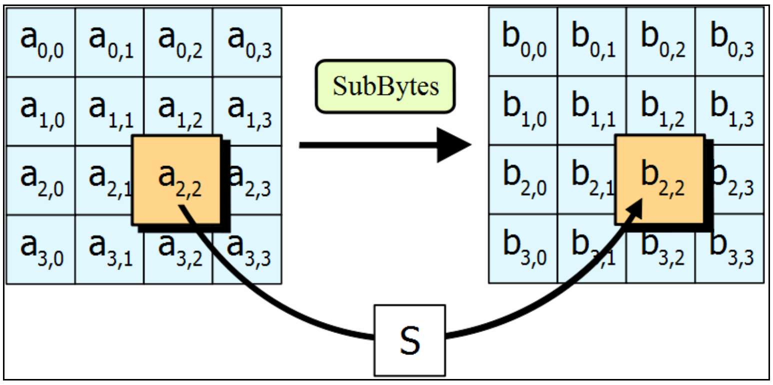
Figure(6): Roundkey combined with the state [Alkharobi, 2007].

5-2 SubBytes:
SubBytes are a substitution of each byte in the block independent of the position in the state, figure(7), this is an S−box as shown in table(1), where the coordinates(x,y) are hexadecimal values that it is a bisection on all possible byte values and therefore invertible, the inverse S−box can easily be constructed from the S−box, this is a non−linear transformation, the S−box used is proved to be optimal with regards to non−linearity [Boesgaard, 2003] [Alkharobi, 2007]. The S−box values are based on the arithmetic complex equations shown in the source [Daemen and Rijmen, 2001].

Table(1): The AES S−box[Daemen and Rijmen, 2001].



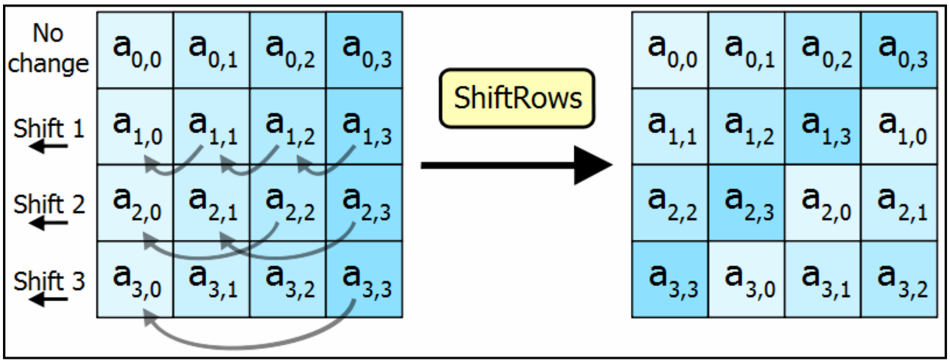
hex		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
	3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
	5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
	6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
	a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
	b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
	c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
	d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16


$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
SubBytes
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,1}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$
S

Figure(7): SubBytes step, each byte in the array is updated by using an 8 bit S−box [Alkharobi, 2007].

5-3 ShiftRows:

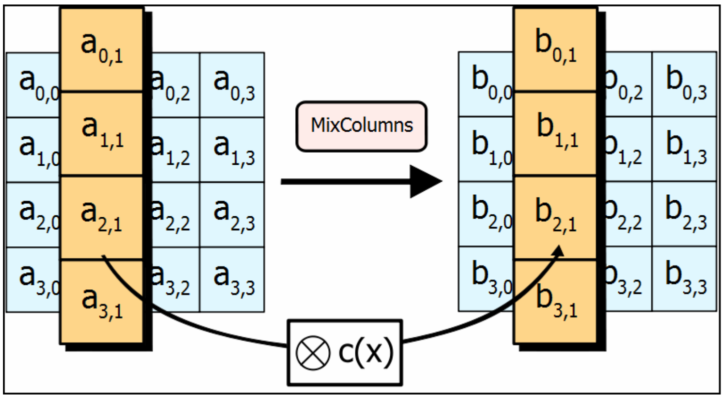
ShiftRows is a cyclic shift of the bytes in the rows of the state and is clearly invertible by a shift in the opposite direction by the same amount, figure(8).


No change
Shift 1
Shift 2
Shift 3
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
ShiftRows
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,1}$ $a_{1,2}$ $a_{1,3}$ $a_{1,0}$
$a_{2,2}$ $a_{2,3}$ $a_{2,0}$ $a_{2,1}$
$a_{3,3}$ $a_{3,0}$ $a_{3,1}$ $a_{3,2}$

Figure(8): The operates on the rows of the state; it cyclically shifts the bytes in each row by a certain offset [Alkharobi, 2007].

5-4 MixColumns:

Each column in the state is considered a polynomial with the byte values as coefficients, the columns are transformed independently by multiplication with a special polynomial c(x), where c(x) is a state illustrated in figure(5), that is used to reverse the multiplication by c(x) as shown in figure(9).



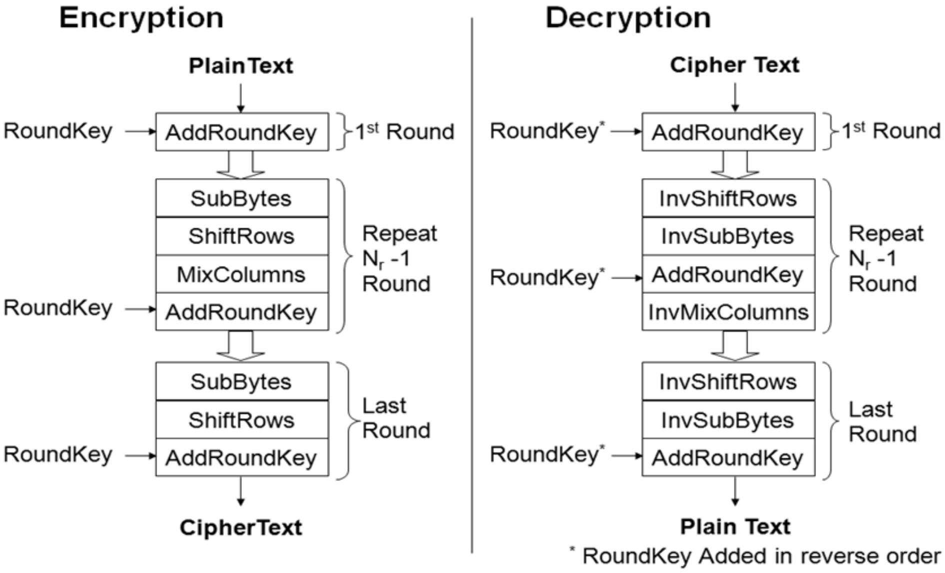
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
MixColumns
$\otimes$ c(x)
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,1}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$

Figure(9): Four bytes of each column of the state are combined by using an invertible linear transformation [Alkharobi, 2007].

Finally, the following functions are used together to obtain the AES algorithm:

```
Round(State, RoundKey)
{
 SubBytes(State);
 ShiftRows(State);
 MixColumns(State);
 AddRoundKey(State, RoundKey);
}
```

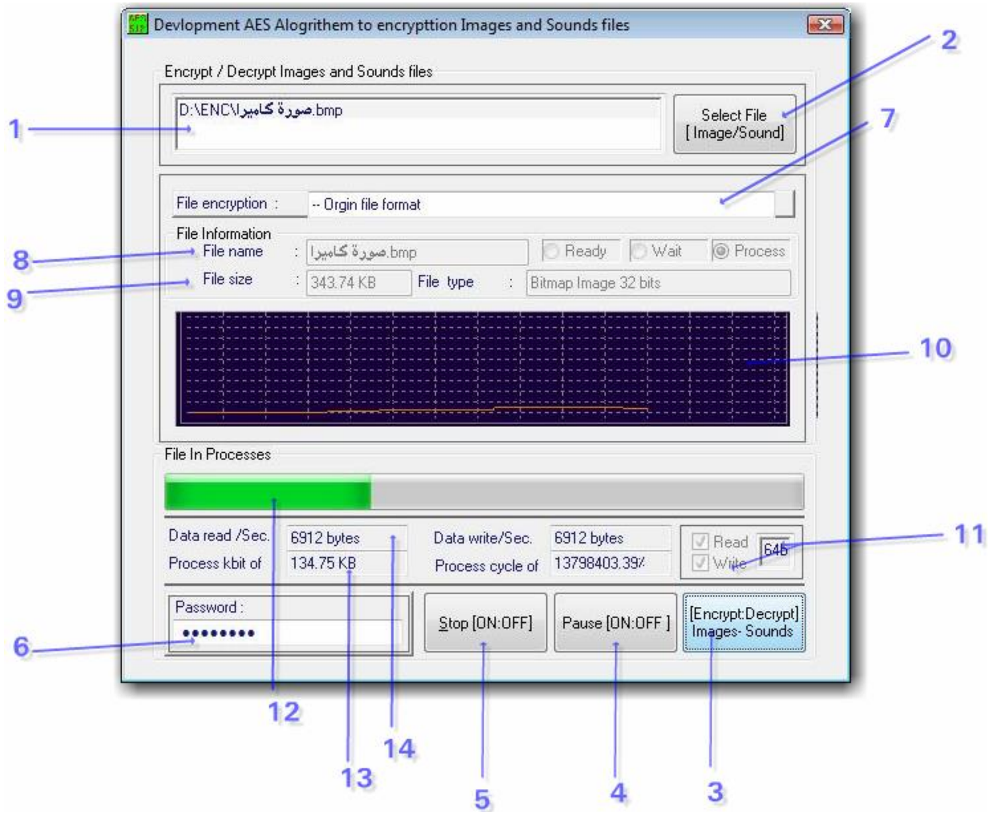
In the final round in the algorithm is like a regular Round function above, but without the MixColumns transformation, where figure(10) illustrates the flowchart of the AES algorithm in the final methods from the Encryption to Cipher-text, and from the Decryption to Plain-text in addition to the RoundKey explained in figure(6) above.



Figure(10): The general AES algorithm at 128 bit/cycle[Roche, 2007].

6. Description of the Software System and Display Packages

The software has a main window with control buttons to apply the proposed algorithm to make the program works easily and understandably, as illustrated in figure(11).



Devlopment AES Alogrithem to encrypttion Images and Sounds files

Encrypt / Decrypt Images and Sounds files

D:\ENC\صورة كاميرا.bmp

File encryption : -- Orgin file format

File Information

File name : صورة كاميرا.bmp

File size : 343.74 KB File type : Bitmap Image 32 bits

File In Processes

Data read /Sec. 6912 bytes Data write/Sec. 6912 bytes

Process kbit of 134.75 KB Process cycle of 13798403.39⁄

Password : ••••••••

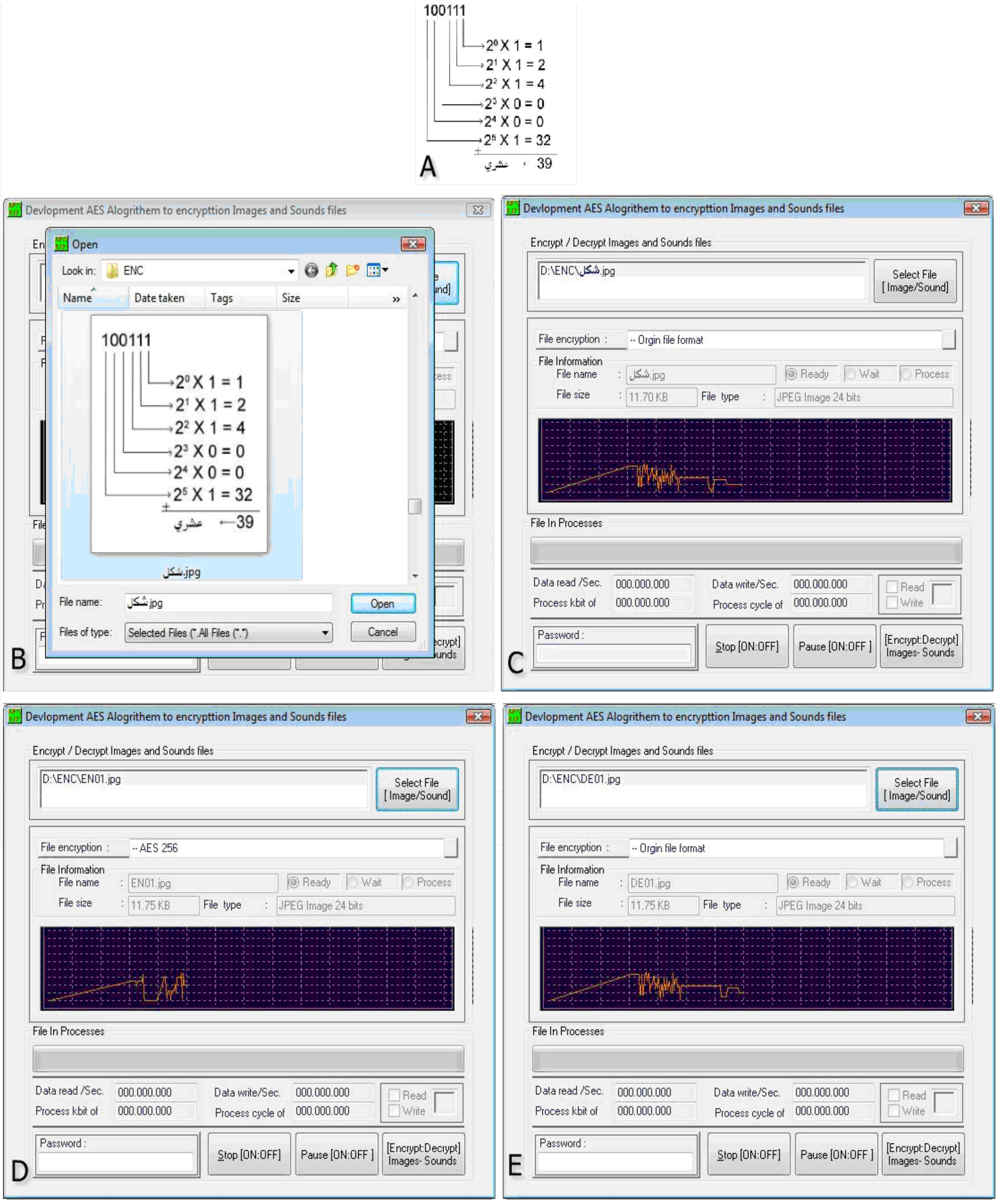
Figure(11): The main window with control buttons in proposed algorithm.

Each number in the figure(11) above gives a special control of program software as the following functions:

1. Display the full−path(directory) of the files that is encrypted or decrypted.
2. Select the files by browsing in the computer through list−files.
3. Begin to encrypt or decrypt the files depends on initiate files.
4. Paused the process during the encryption operation.
5. Canceling the operation during the encryption operation.
6. Allow the user to enter the password to prevent unauthorized persons.
7. Appears the file state if its encrypted or non.
8. Display the current file name.
9. Display the current file size(bytes, kilobytes, megabytes and gigabytes).
10. Display the file histogram by bit to bit technique.
11. Display the synchronization read/write operation.
12. Display the progress file through the process, which depends on the file size and the time−line processing.
13. Display the number of byte/cycle in the data during the processing.
14. Display the synchronization data block read/write operation(kilobytes/sec.).

7. Display the Software System Results

The proposed algorithm is applied to the samples in figures(12, 13, 14 and 15). Each figure contains the file acquisition method and the steps operation. Where, Chart A shows the test input(original) image or sound file. Chart B shows the test input file is already entered to the program system. Chart C shows the histogram of the number of bits which contains the test input file. Chart D shows the histogram after encryption mode. Chart E shows the histogram as the normal state and the test file returns to its original bits after decryption mode in program system.



B:

File name: شكل.jpg

Files of type: Selected Files (*.All Files (*.*)

C:

D:\ENC\شكل.jpg

File encryption : -- Orgin file format

File name : شكل.jpg

File size : 11.70 KB File type : JPEG Image 24 bits

Data read /Sec. 000.000.000 Data write/Sec. 000.000.000

Process kbit of 000.000.000 Process cycle of 000.000.000

D:

D:\ENC\EN01.jpg

File encryption : -- AES 256

File name : EN01.jpg

File size : 11.75 KB File type : JPEG Image 24 bits

Data read /Sec. 000.000.000 Data write/Sec. 000.000.000

Process kbit of 000.000.000 Process cycle of 000.000.000

E:

D:\ENC\DE01.jpg

File encryption : -- Orgin file format

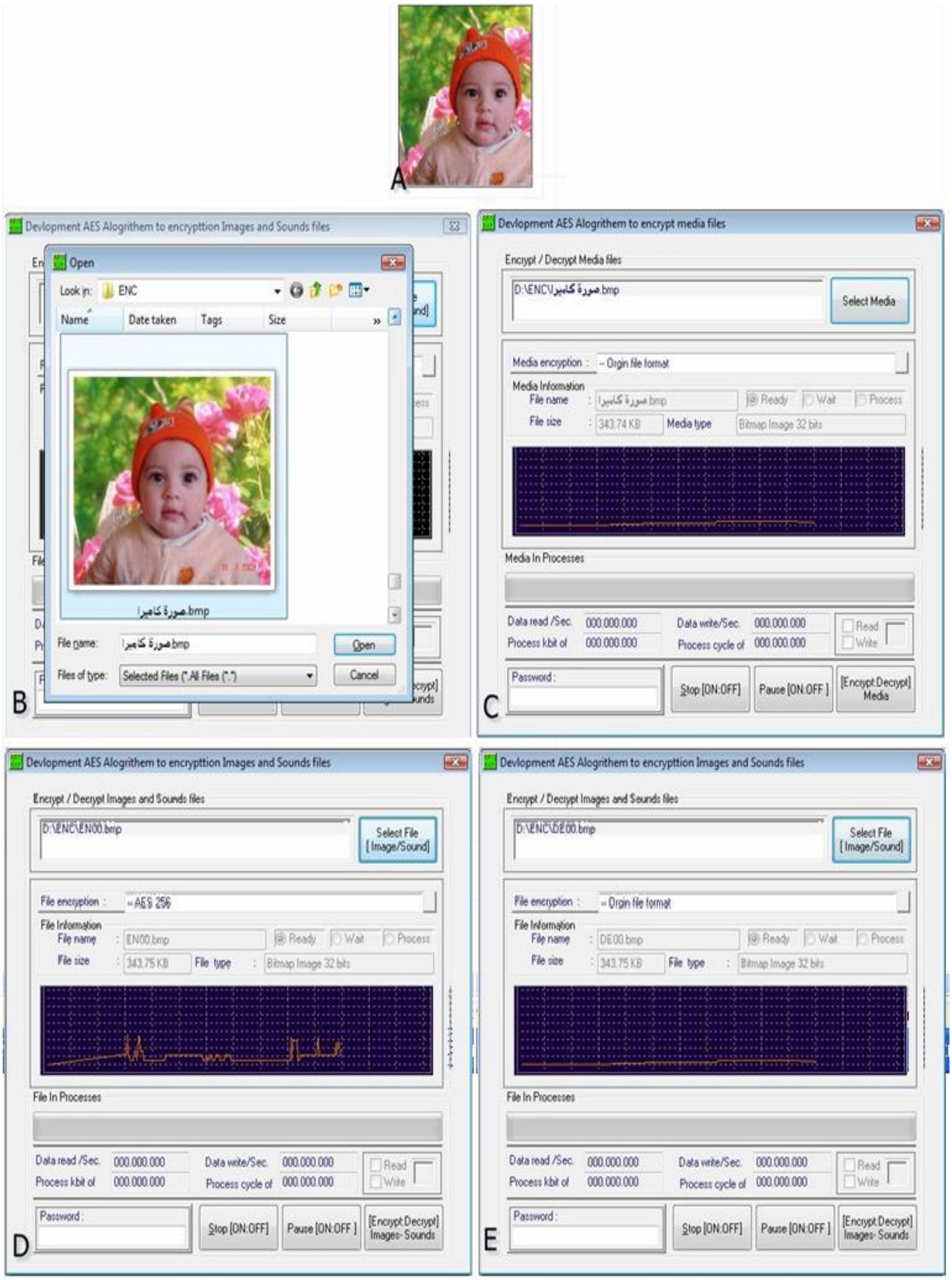
File name : DE01.jpg

File size : 11.75 KB File type : JPEG Image 24 bits

Data read /Sec. 000.000.000 Data write/Sec. 000.000.000

Process kbit of 000.000.000 Process cycle of 000.000.000

Figure (12): Applies the proposed algorithm to gray scale image that takes from the office system.



Devlopment AES Alogrithem to encrypttion Images and Sounds files

Open

Look in: ENC

Name | Date taken | Tags | Size

صورة كاميرا.bmp

File name: صورة كاميرا.bmp

Files of type: Selected Files (*.All Files (*.*)

Open

Cancel

Devlopment AES Alogrithem to encrypt media files

Encrypt / Decrypt Media files

D:\ENC\صورة كاميرا.bmp

Select Media

Media encryption : -- Orgin file format

Media Information

File name : صورة كاميرا.bmp ○ Ready □ Wait □ Process

File size : 343.74 KB Media type Bitmap Image 32 bits

Media In Processes

Data read /Sec. 000.000.000 Data write/Sec. 000.000.000 □ Read

Process kbit of 000.000.000 Process cycle of 000.000.000 □ Write

Password :

Stop [ON:OFF] Pause [ON:OFF] [Encrypt Decrypt] Media

Devlopment AES Alogrithem to encrypttion Images and Sounds files

Encrypt / Decrypt Images and Sounds files

D:\ENC\EN00.bmp

Select File [Image/Sound]

File encryption : -- AES 256

File Information

File name : EN00.bmp ○ Ready □ Wait □ Process

File size : 343.75 KB File type : Bitmap Image 32 bits

File In Processes

Data read /Sec. 000.000.000 Data write/Sec. 000.000.000 □ Read

Process kbit of 000.000.000 Process cycle of 000.000.000 □ Write

Password :

Stop [ON:OFF] Pause [ON:OFF] [Encrypt Decrypt] Images- Sounds

Devlopment AES Alogrithem to encrypttion Images and Sounds files

Encrypt / Decrypt Images and Sounds files

D:\ENC\DE00.bmp

Select File [Image/Sound]

File encryption : -- Orgin file format

File Information

File name : DE00.bmp ○ Ready □ Wait □ Process

File size : 343.75 KB File type : Bitmap Image 32 bits

File In Processes

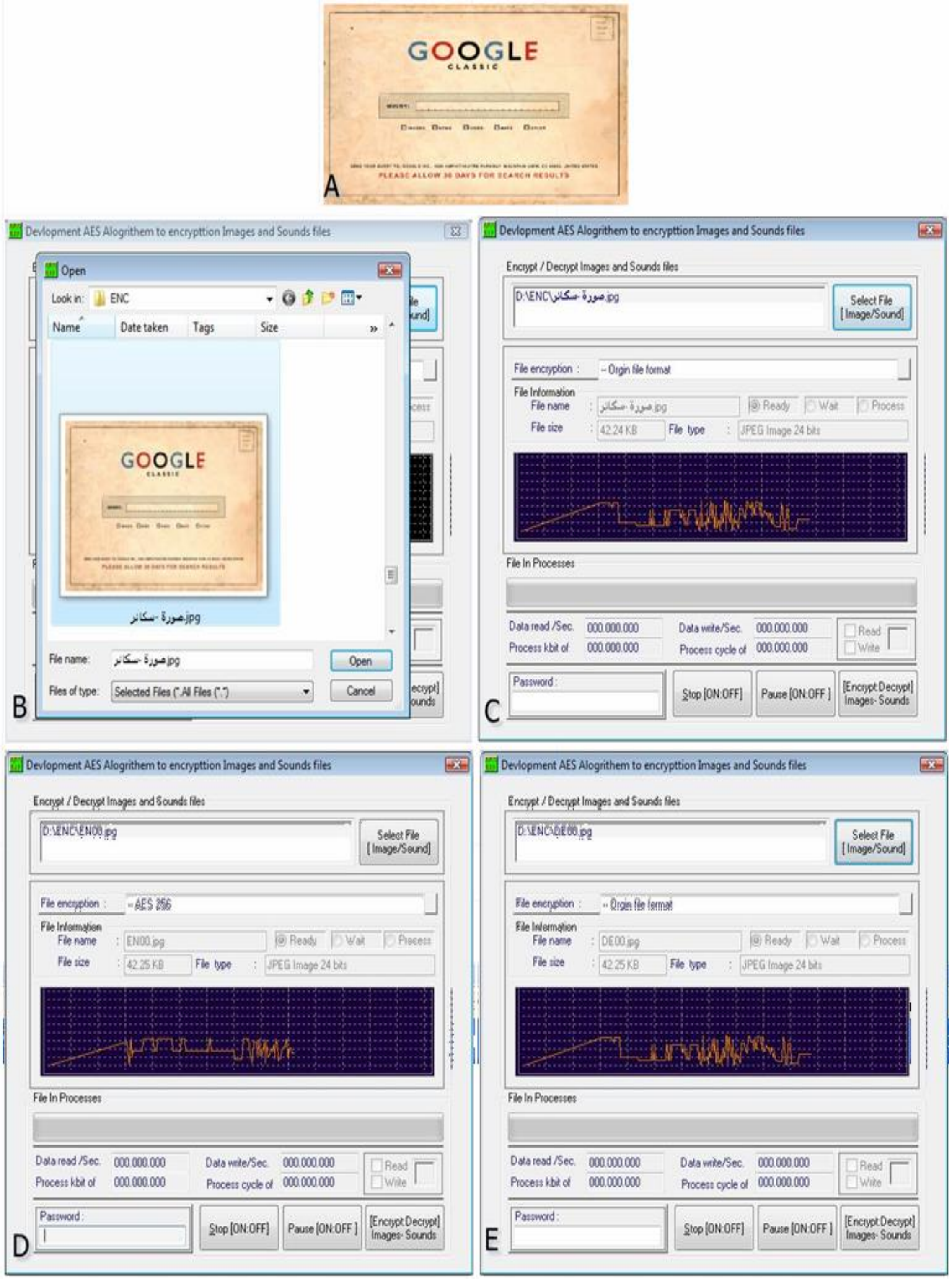
Data read /Sec. 000.000.000 Data write/Sec. 000.000.000 □ Read

Process kbit of 000.000.000 Process cycle of 000.000.000 □ Write

Password :

Stop [ON:OFF] Pause [ON:OFF] [Encrypt Decrypt] Images- Sounds

Figure(13): Applies the proposed algorithm to color RGB image that takes from digital camera.


A
GOOGLE
CLASSIC
PLEASE ALLOW 30 DAYS FOR SEARCH RESULTS
B
C
D
E
Devlopment AES Alogrithem to encrypttion Images and Sounds files
Open
Cancel
Select File [Image/Sound]
Stop [ON:OFF]
Pause [ON:OFF]
[Encrypt Decrypt] Images- Sounds

B

Open

Look in: ENC

Name | Date taken | Tags | Size

صورة- سكانر.jpg

File name: صورة- سكانر.jpg

Files of type: Selected Files (*.All Files (*.*)

C

Encrypt / Decrypt Images and Sounds files

D:\ENC\صورة- سكانر.jpg

File encryption : -- Orgin file format

File Information

File name : صورة- سكانر.jpg ● Ready □ Wait □ Process

File size : 42.24 KB File type : JPEG Image 24 bits

File In Processes

Data read /Sec. 000.000.000 Data write/Sec. 000.000.000 □ Read

Process kbit of 000.000.000 Process cycle of 000.000.000 □ Write

Password :

D

Encrypt / Decrypt Images and Sounds files

D:\ENC\EN00.jpg

File encryption : -- AES 256

File Information

File name : EN00.jpg ● Ready □ Wait □ Process

File size : 42.25 KB File type : JPEG Image 24 bits

File In Processes

Data read /Sec. 000.000.000 Data write/Sec. 000.000.000 □ Read

Process kbit of 000.000.000 Process cycle of 000.000.000 □ Write

Password :

E

Encrypt / Decrypt Images and Sounds files

D:\ENC\DE00.jpg

File encryption : -- Orgin file format

File Information

File name : DE00.jpg ● Ready □ Wait □ Process

File size : 42.25 KB File type : JPEG Image 24 bits

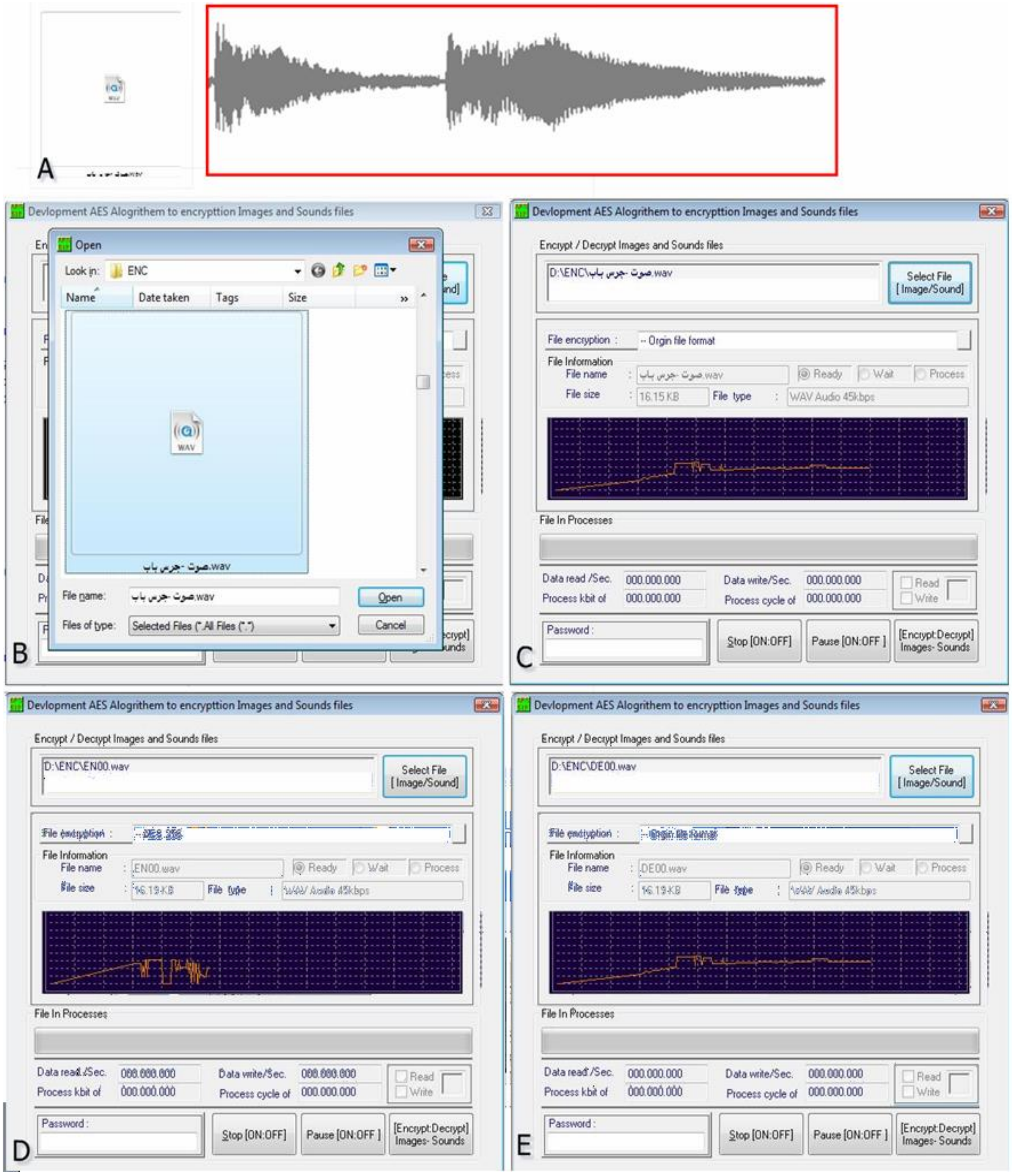
File In Processes

Data read /Sec. 000.000.000 Data write/Sec. 000.000.000 □ Read

Process kbit of 000.000.000 Process cycle of 000.000.000 □ Write

Password :

Figure(14): Applies the proposed algorithm to color indexed image that takes from scanner device.



Devlopment AES Alogrithem to encrypttion Images and Sounds files

Open

Look in: ENC

Name | Date taken | Tags | Size

صوت -جرس باب.wav

File name: صوت -جرس باب.wav

Files of type: Selected Files (*.All Files (*.*)

Open | Cancel

Encrypt / Decrypt Images and Sounds files

D:\ENC\صوت -جرس باب.wav

Select File [Image/Sound]

File encryption : -- Orgin file format

File Information

File name : صوت -جرس باب.wav ◉ Ready ○ Wait ○ Process

File size : 16.15 KB File type : WAV Audio 45kbps

File In Processes

Data read /Sec. 000.000.000 Data write/Sec. 000.000.000 □ Read

Process kbit of 000.000.000 Process cycle of 000.000.000 □ Write

Password :

Stop [ON:OFF] | Pause [ON:OFF] | [Encrypt:Decrypt] Images- Sounds

D:\ENC\EN00.wav

File encryption : -- AES 256

File name : EN00.wav

File size : 16.19 KB File type : WAV Audio 45kbps

D:\ENC\DE00.wav

File encryption : -- Orgin file format

File name : DE00.wav

File size : 16.19 KB File type : WAV Audio 45kbps

Figure(15): Applies the proposed algorithm to sound wave that takes from the windows system.

8. Conclusions

1. When a proposed algorithm had been applied on the earlier computers which have 128 MB physical memory, it has been noted that it can work under any circumstances, but in more physical memory the times and the processing will be increased so far as the file size increases.
2. The results showing the encryption's histogram which determined the difference(in viewing) on both the original and decryption histograms.
3. A comparison between the original and decrypted files kept all data with no changes in any bits in both files, the histogram showing the result has no change

too, this means that the algorithm was successful in continuing the increase of the block’s matrix that was taken as a test .

4. The proposed algorithm failed when applied to file size less than block size(64 byte), because one block data was used while the remaining three blocks data are not used, as illustrated in figure(3).
5. On pressing stop button 5 in the figure(11) during the processing operation, the proposed algorithm will fail to retrieve the data of the tested file, that means the data will be lost.

9. Suggestions

1. Depending this algorithm in most physical protected media files to increase the protected use in different keys generator.
2. It still needs more work to perform full actions to this proposed method, specifically when the block size is 512 bit/cycle, the hope is to perform at least 512 bit/three cycles.
3. Give more possibility to increase more than 4 AES, for example, using 16 AES or 32 AES algorithms, working under any circumstances, this performs to decrease the time in operations used.
4. Hoping to develop this algorithm to encrypt all multimedia files, such as the moves.
5. Hoping to develop this algorithm for encrypt the compression and executable files.
6. Developing proposed algorithm in a way that it would be possible to receive or send the encoded file to the target computer; and the encoding key should be included in a certain location within the encoded file matrix, also the location of the key will be determined by both receiver and transmitter.

REFERENCES

1st: Official Papers:

[1] Roche, W. (2007): "Advanced Encryption Standard", CSC 7002 Computer Security. Website: http://www.ouray.cudenver.edu/~wrroche/Security/Presentation.html

[2] US Federal Information (2001): "Advanced Encryption Standard", Information Processing Standards Publication, FIPS 197, NIST, Computer Security, Public Law 100-235. Website: http//:www.csrc.nist.gov/publications/fips/fips197/fips−197.pdf

2nd: Univ. Thesis:

[3] Alkharobi, Talal (2007) : "Encryption AES", Ph.D. thesis, College of Computer Science & Engineering, King Fahd University of Petroleum & Minerals, Dhahran, Saudi Arabia.

3rd: Articles:

[4] Boesgaard, Ch. (2003): "A Short Introduction to AES", Department of Computer Science, University of Copenhagen, Website: http://www.ijcee.org/papers/141.pdf

[5] Daemen, J. and Rijmen, V. (1998): "AES Submission Document on Rijndael", Rijndael AES Proposal. Website: http//:www.csrc.nist.gov/CryptoToolkit/aes/rijndael/Rijndael−ammended.pdf

[6] Daemen, J. and Rijmen, V. (2001): "Rijndael Homepage". Website: http//:www.esat.kuleuven.ac.be/˜rijmen/rijndael.

[7] Haan, L. (2007): "Advanced Encryption Standard Tutorial". Website: http//:www.progressive-coding.com

[8] Wikpedia (2008): "Wikipedia, the free encyclopedia". Website: http//:www. en.wikipedia.org/wiki/Advanced_Encryption_Standard

4th: Books:

[9] Steffen, A. (2005):"Introduction to Cryptography", Secure Network Communication, Part 1, Zürcher Hochschule Winterthur.

[10] Townsend, P. (2009): "AES Encryption and Related Concepts". Website: http//:www.patownsend.com/cms_uploads/file/WhitePapers/AES_Introduction.pdf

[11] Vaudenay, S. (2006): "A Classical Introduction to Cryptography", Applications for Communications Security, ISBN: 978-0-387-25464-1, Queensland University of Technology, Brisbane, Australia.