Using Random Scrambling in Multi Media Encoding

Ghada Mohammad Tahir Qasim
ghada@uomosul.edu.iq
College of Computer Sciences and Mathematics
University of Mosul, Mosul, Iraq

Received on: 14/10/2012 **Accepted on: 30/01/2013**

ABSTRACT

The research deals with implementation of a new algorithm to encrypt multimedia files this method called random scrambling, to increase the security of the transmitted files, a secret key is used to prevent unauthorized persons from extracting these files.

The encryption applied on image, sound, and video files, Matlab is used to implement the algorithm due to the facilities it provides for dealing with multimedia files as well as GUI.

Finally, experimental results demonstrate the efficiency of the algorithm in the encryption of Multimedia files.

Keywords: multi-media encoding, random number, video encoding, sound encoding

استخدام البعثرة العشوائية في تشفير الوسائط المتعددة

غادة محمد طاهر الدباغ
كلية علوم الحاسوب والرياضيات
جامعة الموصل، الموصل، العراق

تاريخ استلام البحث: 2012/10/14 **تاريخ قبول البحث: 2013/01/30**

الملخص

تم في هذا البحث تنفيذ طريقة جديدة لتشفير ملفات الوسائط المتعددة وهي طريقة البعثرة العشوائية، ولزيادة سرية الملفات المرسلة تم استخدام مفتاح سري إذ لا يمكن استرجاع الملف المشفر دون معرفته أي أن الجهة المخولة التي تعلم المفتاح السري هي التي تستطيع فقط استرجاع الملف.

تم تطبيق التشفير على ملفات صورية وصوتية وفيديوية كما تم استخدام لغة (MATLA 10) في هذا البحث وذلك للتسهيلات التي توفرها في التعامل مع ملفات الوسائط المتعددة فضلا على كونها توفر واجهات للتعامل مع المستخدمين.

وأخيراً فان التجارب العملية أثبتت كفاءة الخوارزمية المقترحة في تشفير ملفات الوسائط المتعددة.

الكلمات المفتاحية: تشفير الوسائط المتعدده، الارقام العشوائية، تشفير الفديو، تشفير الصوت

1- المقدمة

مع التطور الهائل لشبكات نقل المعلومات ومع انتشار الانترنيت اكتسبت سرية المعلومات أهمية كبيرة ولاسيما نقل الصور والملفات الفيديوية.

تجدر الإشارة إلى أن الانترنت لا يوفر أمنية للملفات الفيديوية لذلك ظهرت الحاجة إلى عمليات حساب وتشفير الوسائط المتعددة لذلك فقد ركزت الدراسات الأخيرة على تشفير الملفات الفيديوية بما يضمن السرعة والأمنية العالية لنقل البيانات الخاصة بالملفات الفيديوية.[3]

إن خوارزميات التشفير التقليدية مثل DES (Data Encryption Standard) و(Advanced AES (Encryption Standard وغيرهما من طرائق تشفير النصوص، أصبحت غير ملائمة لتشفير بيانات

الملفات الفيديوية بسبب كبر حجم بيانات الوسائط المتعددة (Multimedia) والتقيد بالزمن الحقيقي لتشفير الملفات الفيديوية[4].

2- الوسائط المتعددة

إن الوسائط المتعددة هي مجموعه من تطبيقات الكومبيوتر التي يمكنها تخزين المعلومات بأشكال متعددة مثل النصوص والأصوات والرسوم والصور الساكنة منها والمتحركة والفيديوية.[9][1]
إن العناصر المهمة لإنشاء تطبيقات الوسائط المتعددة هي: النص، الصور المرسومة، الصور الفوتوغرافية، الصور النقطية، الحركة،الفيديو، الخطوط، الصوت الرقمي، الألوان، سواقة الأحداث. أن ربط هذه العناصر المختلفة في إنتاج موحد ومتماسك يسهل استخدامها. [1]

3- تحديات تشفير ملفات الوسائط المتعددة

إن من أهم التحديات التي تواجه تشفير بيانات الوسائط المتعددة (multimedia) هي الآتي:-

أ- حجم البيانات: إذ أن حجم بيانات الوسائط المتعددة يكون عادة كبيراً جداً (على سبيل المثال ساعتان من فيديو MPEG-1 تأخذ حوالي 1GIGA BYTE).

ب- الوقت الحقيقي: إن بيانات الوسائط المتعددة (multimedia) تحتاج أن تعالج بوقت حقيقي مثلاً نسبة معالجة بيانات (MPEG-1) تتطلب (1.5 mb/sec).

ج- كلفة التشفير: إذ أن نسبة المعلومات في تطبيقات الوسائط المتعددة تكون كبيرة جداً ولكن قيمة المعلومات ضعيفة، إن عملية فك شفرة هذا النوع من التشفير سوف يحتاج إلى كلفة أكبر من كلفة شراء البرنامج.[3]

4- معايير خوارزميات تشفير الوسائط المتعددة:

أ- سرعة الخوارزمية: إذ يجب أن تتوفر السرعة في كل من خوارزمية التشفير وخوارزمية فك التشفير.

ب- سرية الخوارزمية المستخدمة: إذ يجب أن توفر الخوارزمية المستخدمة سرية كبيرة وذلك يأتي من زيادة عدد مفاتيح التشفير (key) المستخدمة.[3]

إن استخدام ألبعثرة العشوائية في أجراء عملية البعثرة يحقق معايير خوارزميات تشفير الوسائط المتعددة من حيث السرعة والسرية إذ أن الوقت المستغرق لإجراء عملية التشفير قليل جدا ولا يتجاوز أجزاء من الثانية، فضلا عن السرية العالية جداً التي تجعل من الصعب على المتطفل الوصول إلى المفتاح المستخدم فضلاً عن التشوه الكبير بعد إجراء عملية البعثرة على ملف الصورة أو الملف الفيديوي المشفر والذي تبين من خلال قياس قيمة (PSNR) وكذلك التشوه الحاصل على الملف الصوتي.

5- الدراسات السابقة

لقد أستخدم كل من Changgui shi & Bharat Bhargava [3] الملفات الفيديوية من نوع MPEG وتجدر الإشارة إلى أن عملية التشفير المستخدمة في هذه الخوارزمية تغير إشارة الـ bits الخاصة بالإشارة لمعاملات الـ DCT (Discrete Cosine Transform) بصورة عشوائية وفقاً للمفتاح السري (secret key) المعطى إذ أن إشارة البت (bit) قد لا تتغير إذا كان البت (bit) المقابل له من المفتاح قيمته تساوي صفراً وقد

تتغير إشارة البت (bit) من الموجب إلى السالب (0 إلى 1) أو قد يتغير بت (bit) الإشارة من السالب إلى الموجب أي (1 إلى 0) كما مبين في المعادلات الآتية:

S=s1:, ……. , s2, …… , s3, ……. , sm …(1)

وعملية تغيير الإشارة الخاصة بالـ bits الخاصة بمعاملات الـ DC وAC كما مبين في المعادلة التالية:

EK(s)=(b1 ⊕ s1)…….(bm ⊕ sm) …(2)

حيث ⊕ هي عملية XOR

S: bitstream of MPEG compressed video
B: bit stream of Encryption key
DC: the average value of the samples sequence
AC: All other transform coefficients

ولقد بينت نتائج هذه الخوارزمية أنه عند تشفير كل معاملات الـ (AC) والـ (DC) تصبح الصورة الناتجة غير مفهومة.

ولقد عرف TANG [6] بعض الطرائق التي تضم عمليتي كبس وتشفير ملفات الـMPEG بخطوة واحده. تعتمد هذه الخوارزمية مبدأ البعثرة (scrambling) وتستخدمه في جزء الكبس إذ تطبق طريقة البعثرة لإجراء تبديل عشوائي لمعاملات الـ DCT في تحويله إلى متجه (1x64 block) بدلا من ترتيب الـ (zig- zag) إن الطرائق التي أستخدمها TANG تقلل نسبة كبس الملف الفيديوي.

إن الخوارزميات التي أقترحها كل من Maples وSteven [8][7] تجرى عملية التشفير بعد إجراء عملية الكبس على الملف من النوع MPEG وعمليات التحليل تتم قبل عملية فك الكبس وهذه الخوارزميات تحتاج لحسابات ضخمة فضلا عن إضافة وقت على زمن وصول الملف في حالة الزمن الحقيقي.

إن الخوارزميات التي أقترحها كل من Tang وMaples وSteven تحتاج إلى حسابات ضخمة وتقلل نسبة الكبس.[3]

لقد برهن **Qiao and Klara** [5] أن خوارزمية Tang تعاني من نقاط الضعف الآتية:

1- خطر معرفة النص الصريح.
2- هجوم النص المشفر فقط.

واقترحوا خوارزمية جديدة تسمى (VEA) (Video Encryption Algorithm) إذ يتم تقسيم كل (chunk) من الإطار (Iframe) إلى نصفين. كلا النصفين تتم بينهما عملية (XOR) وتخزن النتيجة بأحد الإنصاف والنصف الثاني يتم تشفيره بخوارزمية قياسية DES (Data Encryption Standard).

وهذه الخوارزمية توفر سرية جيدة. وعلى كل حال لا تستخدم هذه الخوارزمية في تطبيقات الزمن الحقيقي (real –time).

لقد وسع Zeng and Lie [10] خوارزمية (Tang) وجعلوها تستخدم مقطع من الكتل الصغيرة (segment of macro block) بدلا من استخدام (block) وفي كل مقطع (Segment) يتم تحريك معاملات DCT التي تحمل نفس التردد عشوائيا ضمن نفس المقطع.

ولقد طور **Chen** [11] في خوارزميته الخوارزمية السابقة من مقطع (segment) إلى إطار (frame) حيث يتم في الخوارزمية المطورة تقسيم معاملات الـ DCT (Discrete Cosine Transform) إلى 64 مجموعه (64 group)وفقا لمواقعها ويتم تطبيق خوارزمية البعثرة في كل مجموعة (group) بالإضافة إلى ذلك فإن

الباحثين أبدلوا اتجاه الحركة لكل من P and B frame. لقد أقترح الباحثون C. Narsimha Raju, Ganugula Umadevi, Kannan Srinathan, C.V. Jawahar, [2] خوارزمية تستخدم ملفات الـ (MPEG) إذ تكون قيم الـ (DC) الخاصة بمصفوفة الـDCT (Discrete Cosine Transform) موزعة بين قيم الـ (AC) بالاعتماد على خوارزمية (Shamir 's Secret Sharing) وهذه الخوارزمية توفر سرية وسرعة عالية ونسبة الخطأ مع ازدياد حجم الفيديو نتيجة للعمليات الحسابية. إن البعثرة العشوائية المقترحة في هذا البحث تمتاز بأنها لا تحتاج إلى حسابات ضخمة والوقت المستغرق في عملية التشفير وفك التشفير قليل جدا مع بقاء حجم الملفات الفيديوية والصوتية والصورية ثابت بالإضافة إلى أن البعثرة العشوائية المستخدمة في هذا البحث شملت كل صورة من صور الأطر (frames) الخاصة بالملف الفيديوي مع المعلومات الصوتية لكل (frame) فضلاً عن تطبيقها على ملفات صوتية منفردة وصورية منفردة.

6- دالة توليد الأرقام العشوائية (Random Function)

وهي أحدى الدوال الرياضية المهمة وتقوم هذه الدالة بتوليد الأرقام العشوائية ضمن الفترة المفتوحة (1, 0) ولها صيغ متعددة في لغة MATLAB [1]

1- R = RAND(N)
2- R = RAND(M, N) OR R = RAND([M, N])
3- R = RAND(M, N, P, ...) OR R = RAND([M, N, P, ...])
4- R = RAND(SIZE(A))

ولقد تم استخدام الصيغة الثانية من صيغ دالة توليد الأرقام العشوائية لانجاز عملية البعثرة المنجزة في هذا البحث في هذا البحث.

7- الخوارزمية المقترحة

تضم الخوارزمية المقترحة مجموعة من المراحل وفيما يلي شرح موجز لكل مرحلة من هذه المراحل:-

1- مرحلة قراءة الملف المستخدم

ويتم في هذه المرحلة قراءة الملف المستخدم سواء أكان ملف صورة أو ملفاً فيديوياً أو ملف صوت ومن ثم يتم استخلاص المعلومات (information) الخاصة بذلك الملف ففي حالة الملف الصوري يتم قراءة أبعاد الصورة ونوعها وفي حالة الملف الفيديوي يتم قراءة عدد الأطر المكونة لذلك الملف والمعلومات الخاصة بكل إطار وفي حالة الملف الصوتي يتم استخلاص عدد العينات (Samples) المكونة لذلك الملف والتردد.

2- مرحلة توليد المفتاح العشوائي

وفي هذه المرحلة يتم توليد المفتاح الخاص بعملية التشفير عن طريق استخدام دالة توليد الأرقام العشوائية ونظرا لكون الخوارزمية المقترحة هي من الخوارزميات ذات المفتاح المتماثل فسوف يتم استخدام هذا المفتاح في عملية فك الشفرة أيضا.

3- مرحلة التشفير

وفي هذه المرحلة يتم استخدام المفتاح الذي تم توليده في المرحلة الثانية في عملية التشفير.

4- مرحلة العرض

وفي هذه المرحلة يتم عرض الملف المشفر.

5- مرحلة التحليل وفي هذه المرحلة يتم تحليل الملف المشفر.

8- خطوات الخوارزمية المقترحة للتشفير

1- الخطوة الأولى: إدخال ملف الوسائط المتعددة سواء أكان ملفاً صورياً أم ملفاً فيديوياً أم ملفاً صوتياً، إذا كان الملف لصورة أستمر، إذا كان ملفاً فيديوياً اقفز للخطوة 5، وإذا كان ملفاً صوتاً اقفز للخطوة 11، وفي حالة إدخال ('###') اذهب للخطوة (16).

2- الخطوة الثانية: إذا كان الملف صورياً يتم حساب أبعاد الصورة ومن ثم تحويل بيانات الصورة إلى (unsigned 8-bit integer).

3- الخطوة الثالثة: توليد المفتاح المستخدم لعملية التشفير وفق المعادلة (1)

$$Eke = (w1*rand(1, w1)) \quad \ldots(1)$$

w1: the high of image

4- الخطوة الرابعة: بعثرة بيانات الصورة من خلال استخدام المفتاح الذي تم توليده في الخطوة الثالثة وفق المعادلات الآتية:

$$c = Nimage(i, Ek(i)) \quad \ldots(2)$$

$$Nimage(i, EK(i)) = Nimage(h, i) \quad \ldots(3)$$

$$Nimage(h, i) = c \quad \ldots(4)$$

Where
h: any row
I: current row of image
EK: Encryption Key

ثم عرض الصورة المشفرة والذهاب إلى الخطوة (1).

5- الخطوة الخامسة: قراءة المعلومات الخاصة بالملف الفيديوي وتحويل الأطر (frames) الخاصة بالملف إلى صور مع قراءة المعلومات الخاصة بالصوت إن وجدت في الملف الفيديوي.

6- الخطوة السادسة: حساب أبعاد الصورة الخاصة بكل (frame) ومن ثم تحويل بيانات الصورة إلى (unsigned 8-bit integer) وحساب أبعاد مصفوفة الصوت.

7- الخطوة السابعة: توليد المفتاح المستخدم لعملية تشفير صور الأطر مع توليد المفتاح الخاص بتشفير الصوت وفق المعادلة (5، 6)

$$fke = (f1*rand(1, f1)) \quad \ldots(5)$$

f1: the high of image in frame

$$ske = (s1*rand(1, s1)) \quad \ldots(6)$$

s1: the first dimension of sound array

8- الخطوة الثامنة: بعثرة بيانات الصورة من خلال استخدام المفاتيح التي تم توليدها في الخطوة السابعة وفق المعادلات الآتية:-

$$Fimage(i, fKe(i)) \leftrightarrow Fimage(h, i) \quad \ldots(7)$$

$$SS(SKE(i), h1) \leftrightarrow SS(i, h1) \quad \ldots(8)$$

Where h: any value
Where h1: any value

9- الخطوة التاسعة: إعادة الصور الناتجة إلى الأطر (Frames) المقابلة لها في الملف الفيديوي لإجراء عملية العرض.

10- الخطوة العاشرة: عرض الملف الناتج والذهاب إلى الخطوة (1).

11- الخطوة الحادية عشرة: قراءة معلومات الملف الصوتي.

12- الخطوة الثانية عشرة: حساب أبعاد مصفوفة الصوت.

13- الخطوة الثالثة عشرة: توليد المفتاح المستخدم لعملية تشفير ملف الصوت وفق المعادلة (9)

soke = (so1*rand(1, so1)) …(9)

so1: the first dimention of sound array

14- الخطوة الرابعة عشر: تطبيق البعثرة العشوائية على بيانات الملف الصوتي من خلال استخدام المفتاح الذي تم توليده في الخطوة (13)

SS(SKE(i), h1) ↔ SS(i, h1) …(10)

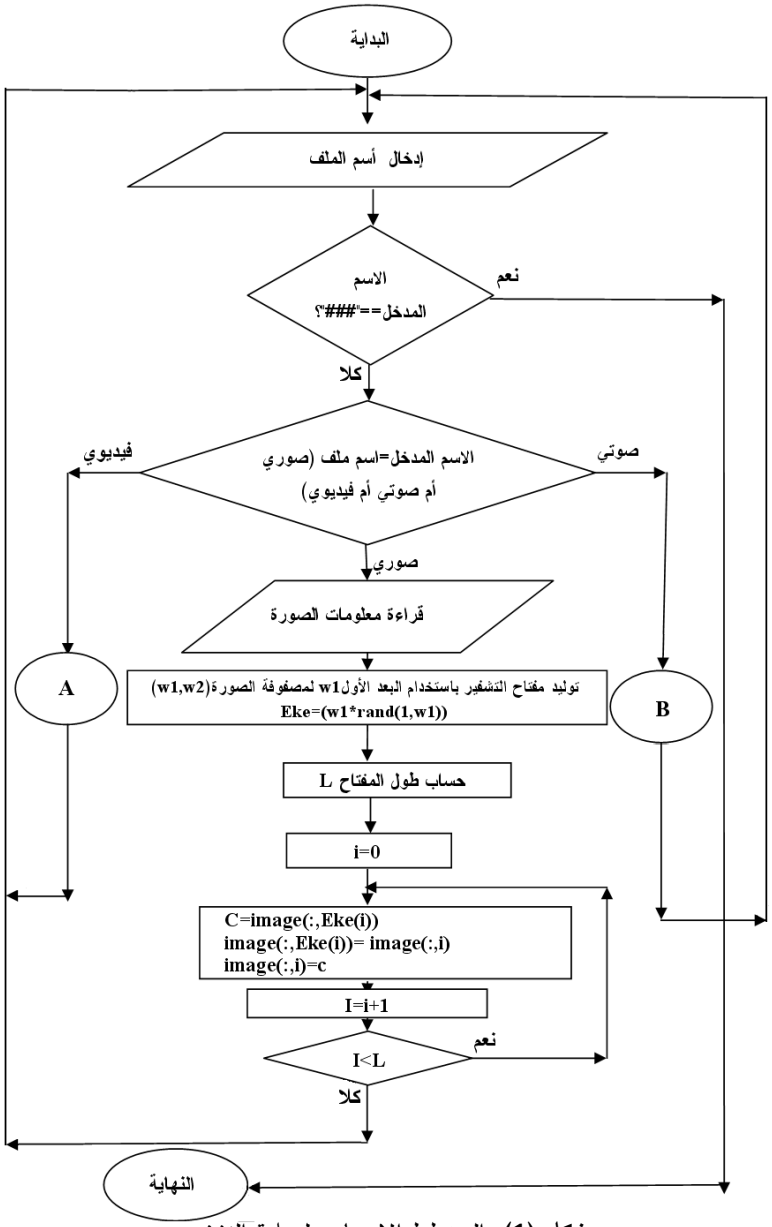
Where SKE : Sound Encryption Key

Where : h1 any value

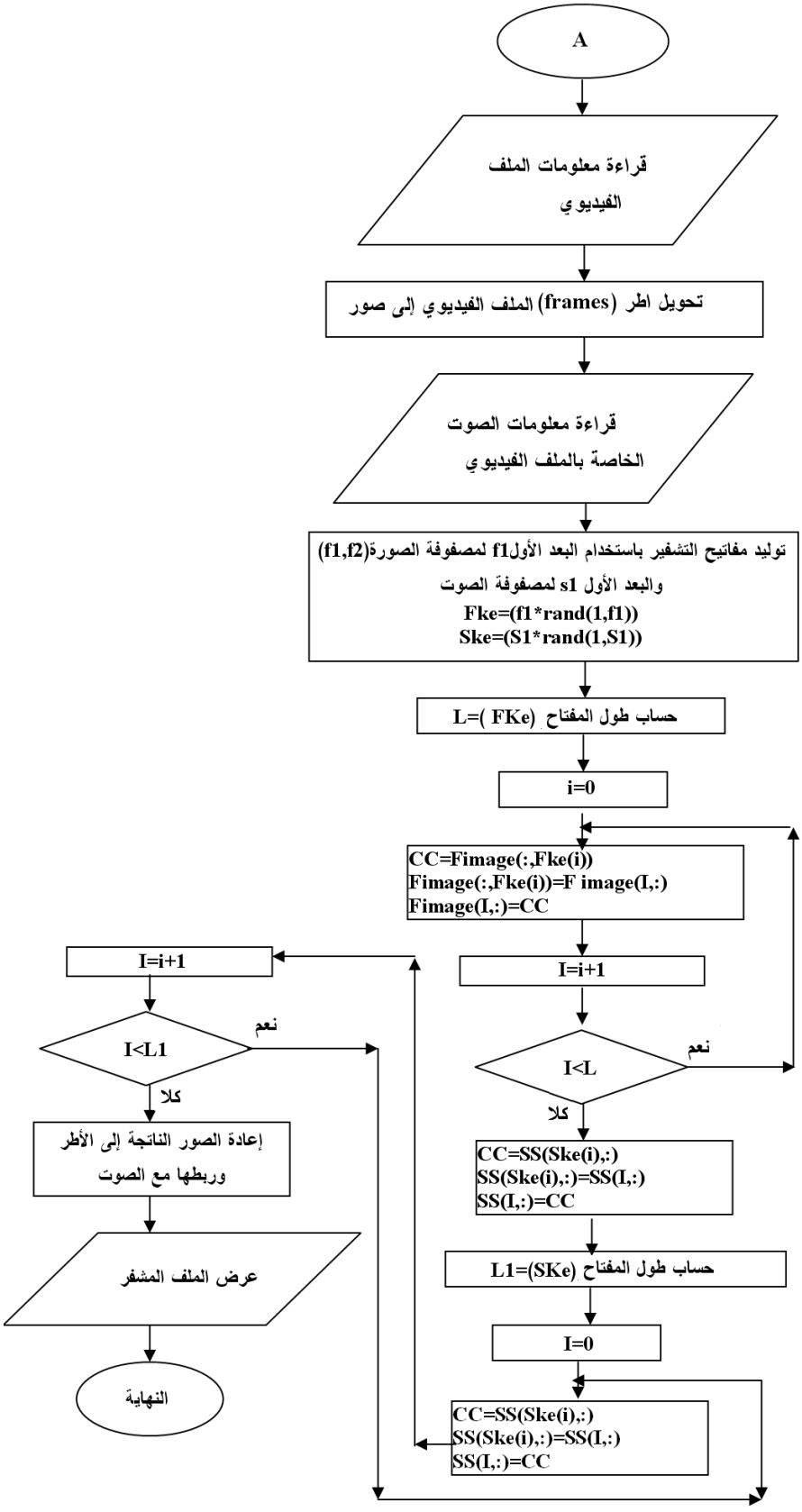
15- الخطوة الخامسة عشر: عرض الملف الناتج والذهاب إلى الخطوة (1).

16- توقف.

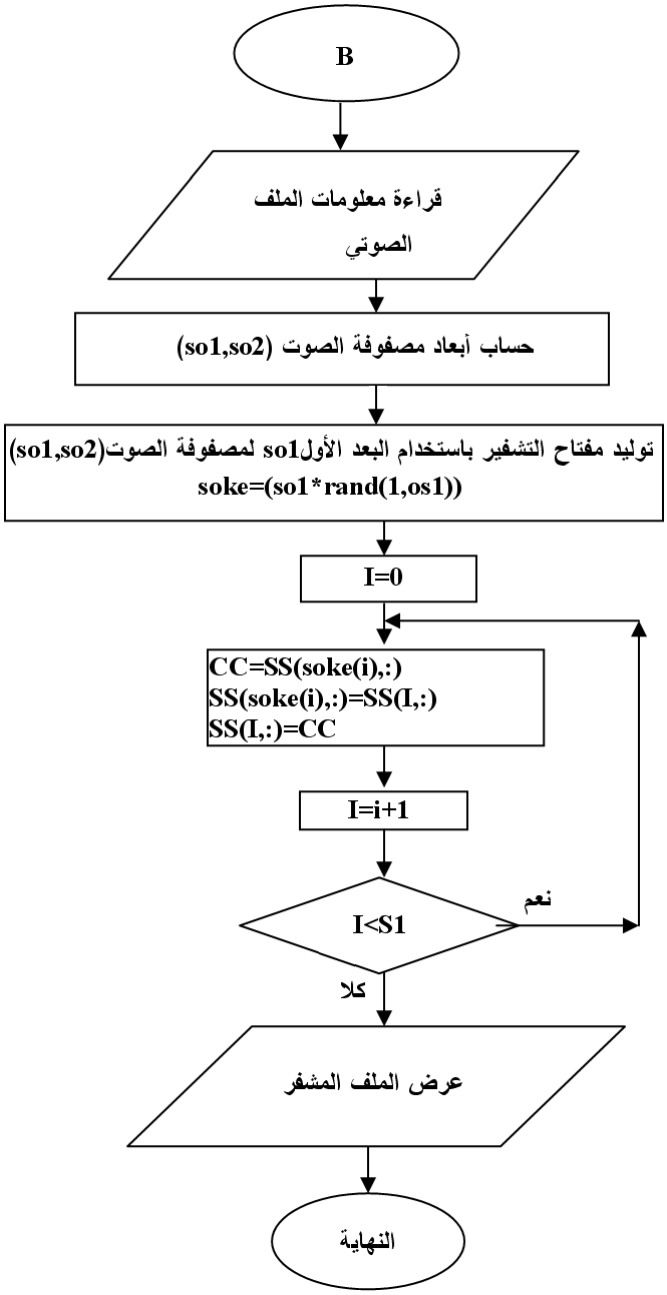
وتبين الأشكال (1، 2، 3) المخططات الانسيابية لعملية التشفير



شكل (1). المخطط الانسيابي لعملية التشفير



شكل(2). المخطط الانسيابي لعملية تشفير الملف الفيديوي



شكل (3). المخطط الانسيابي لعملية تشفير الصوت

9- خطوات الخوارزمية المقترحة لفك التشفير

وفي هذه العملية يتم استرجاع كل من ملف من ملفات الوسائط المتعددة التي يتم إدخالها وفيما يلي عرض لخطوات عملية الاسترجاع

1- الخطوة الأولى: إدخال ملف الوسائط المتعددة سواء أكان ملفاً صورياً أم ملفاً فيديوياً أم ملفاً صوتياً، إذا كان الملف لصورة أستمر، إذا كان ملفاً فيديوياً اقفز للخطوة 5، وإذا كان ملفاً صوتياً اقفز للخطوة 10، وفي حالة إدخال ('###') إذهب للخطوة (14)

2- الخطوة الثانية: إذا كان الملف صورياً يتم حساب أبعاد الصورة ومن ثم تحويل بيانات الصورة إلى (unsigned 8-bit integer).

3- الخطوة الثالثة: أجراء عملية الاسترجاع وذلك من خلال استخدام المفتاح نفسه (Secret key) الذي أستخدم في عملية التشفير وفق المعادلة الآتية:-

$$Nimage(EK(i),i) \leftrightarrow Nimage(I,h) \quad \ldots(11)$$

Where h: any row
EK: Encryption Key

4- الخطوة الرابعة: عرض الصورة المسترجعة والذهاب إلى الخطوة (1).

5- الخطوة الخامسة: قراءة المعلومات الخاصة بالملف الفيديوي وتحويل الأطر (frames) الخاصة بالملف إلى صور مع قراءة المعلومات الخاصة بالصوت إن وجدت في الملف الفيديوي.

6- الخطوة السادسة: حساب أبعاد الصورة الخاصة بكل (frame) ومن ثم تحويل بيانات الصورة إلى (unsigned 8-bit integer) ومن حساب أبعاد مصفوفة الصوت.

7- الخطوة السابعة: أجراء عملية الاسترجاع وذلك من خلال استخدام المفاتيح نفسها التي استخدمت في عملية التشفير

$$Fimage(fKe(i),i) \leftrightarrow Fimage(I,h) \quad \ldots(12)$$

$$SS(h1,SKE(i)) \leftrightarrow SS(h1,i) \quad \ldots(13)$$

Where h:any value of column
h1: any value of row
SKE: sound Encryption key

8- الخطوة الثامنة: إعادة الصور الناتجة إلى الأطر (Frames) المقابلة لها في الملف الفيديوي لإجراء عملية العرض.

9- الخطوة التاسعة: عرض الملف الناتج والذهاب إلى الخطوة (1).

10- الخطوة العاشرة: قراءة معلومات الملف الصوتي.

11- الخطوة الحادية عشرة: حساب أبعاد مصفوفة الصوت.

12- الخطوة الثانية عشرة: أجراء عملية الاسترجاع وذلك من خلال استخدام المفتاح نفسه الذي أستخدم في عملية التشفير

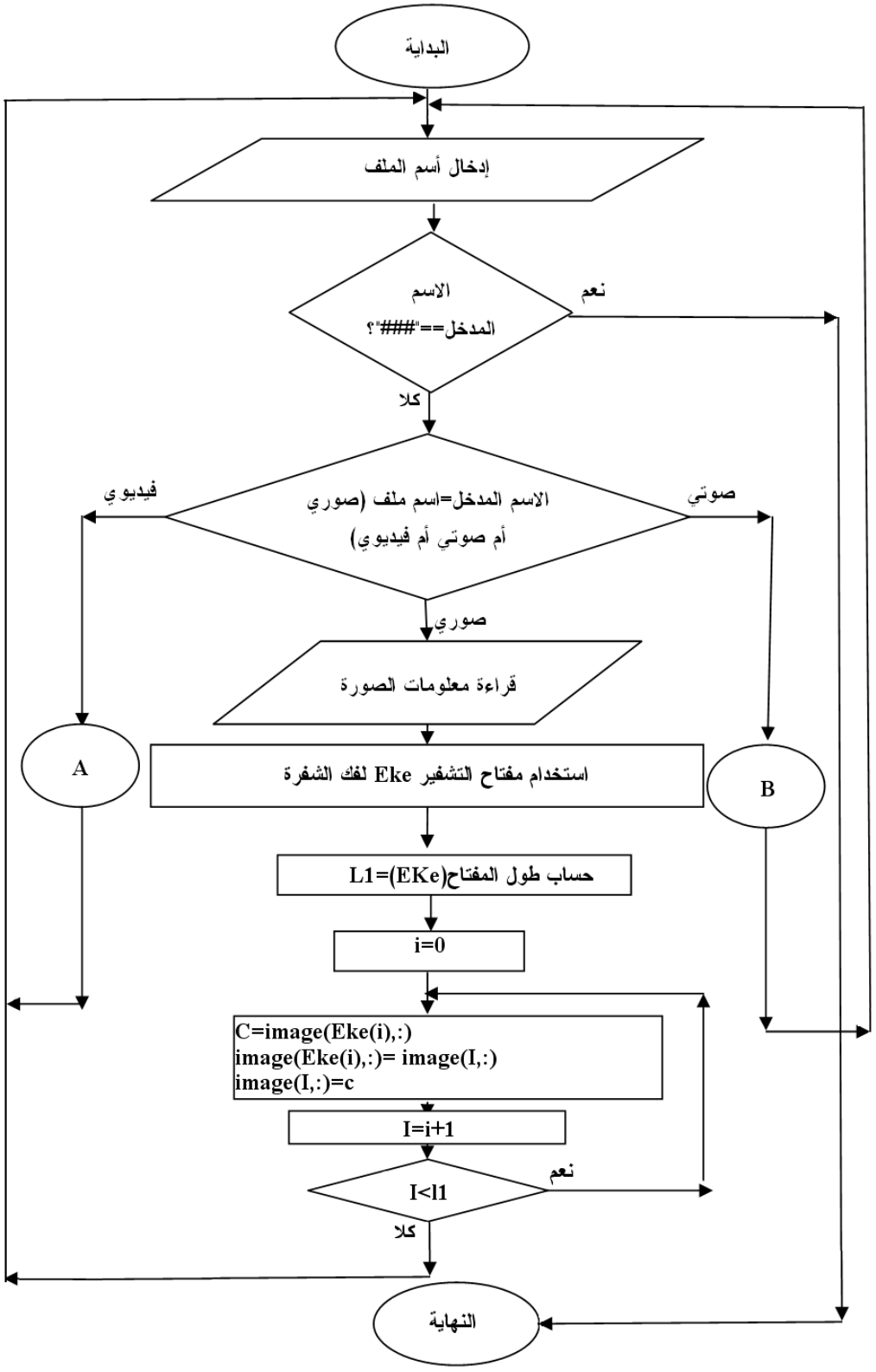
$$SS(h1,SKE(i)) \leftrightarrow SS(h1,i) \quad \ldots(14)$$

Where : h1 any value

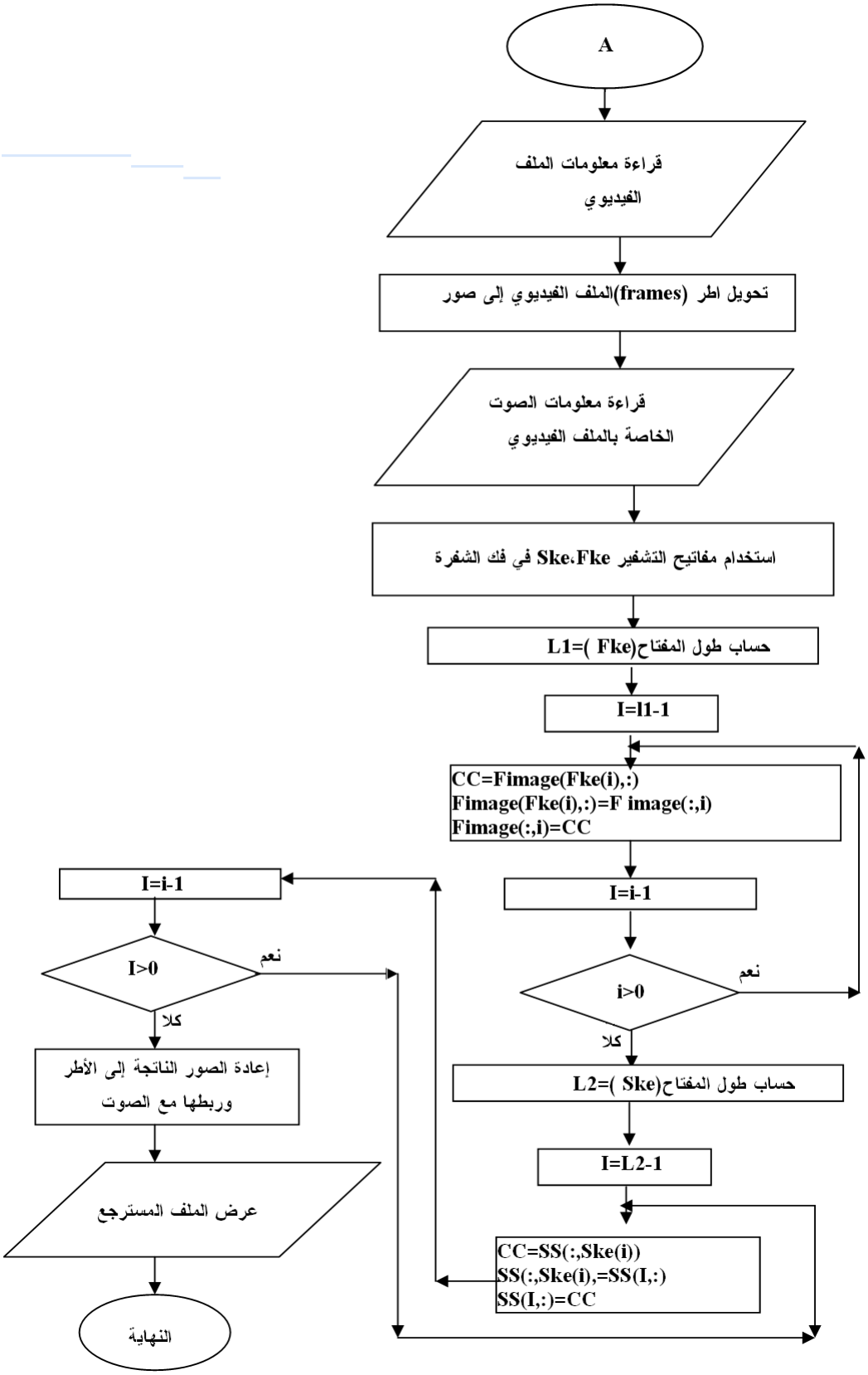
13- الخطوة الثالثة عشر: عرض الملف الناتج والذهاب إلى الخطوة (1).

14- توقف.

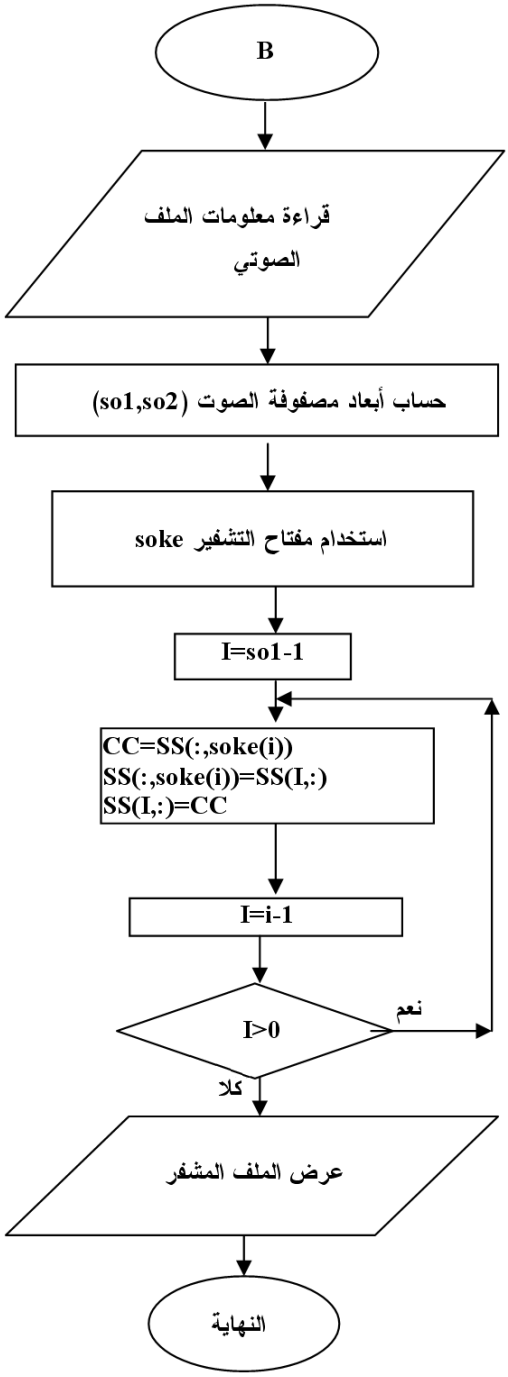
وتوضح الأشكال (4، 5، 6) المخططات الانسيابية لعملية فك الشفرة



شكل (4). المخطط الانسيابي لعملية فك الشفرة



شكل (5). المخطط الانسيابي لعملية استرجاع الملف الفيديوي

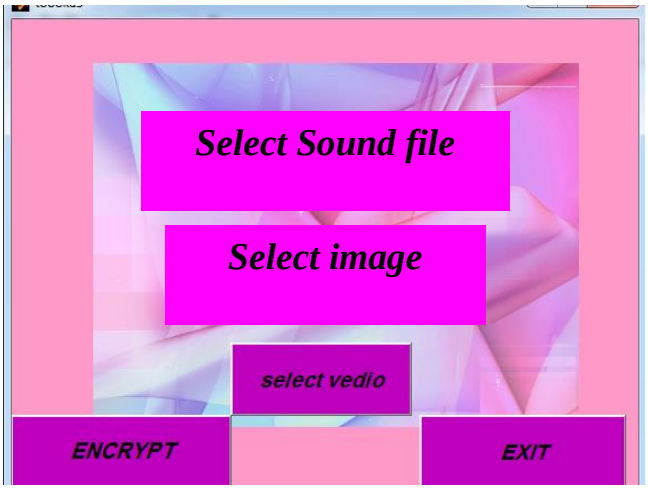


شكل (6). المخطط الانسيابي لعملية استرجاع الصوت

10- النتائج والاستنتاجات

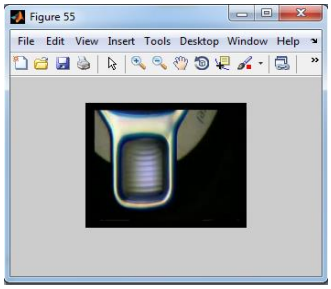
1- النتائج

إن الشاشة الرئيسية للبرنامج المبينة في الشكل (7) تتطلب من المستخدم إدخال الملف المطلوب تشفيره سواء أكان ملفَ صوتٍ أم ملفَ صورة أم ملفاً فيديوياً ، وتجدر الإشارة إلى أنه تم تطبيق الطريقة المقترحة على ملفات صوتية من نوع (.wav) وملفات صورية من نوع(.BMP) وملفات فيديوية من نوع (.AVI) ولقد كانت النتائج جيدة جداً.

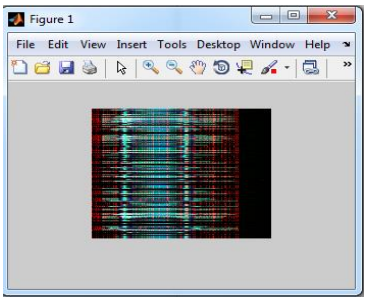


شكل (7). الشاشة الرئيسية

ويبين الشكل (8) واحد من اطر الملف الأصلي المتكون من 54 إطار (frame) ويبين الشكل (9) عملية البعثرة العشوائية على صورة أحد الأطر.

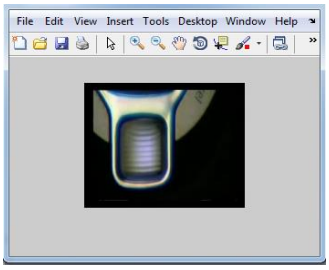


شكل (8). أحد أطر الملف الأصلي



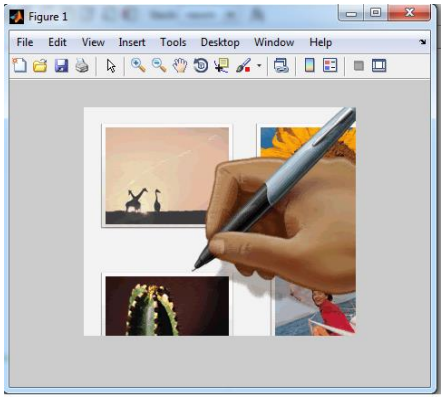
شكل(9). الملف المشفر بطريقة البعثرة العشوائية

وتجدر الإشارة إلى أن الصور أعلاه هي لبيان عملية التشفير لأحد أطر ملف فيديوي يتألف من (54) إطار ولقد تم تشفير الملف كاملا بالطريقة المقترحة وبكفاءة عالية ،كما أن البرنامج الذي أنجز في هذا البحث قد أشتمل على بناء خوارزمية استرجاع إذ يبين الشكل (10) احد اطر الملف المسترجع وهو مطابق للإطار الأصلي.

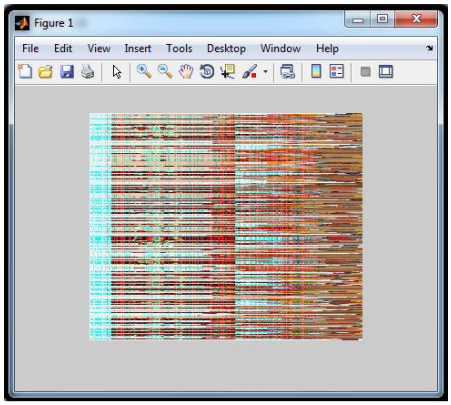


شكل (10). الإطار المسترجع

ولإثبات دقة الخوارزمية المقترحة فلقد تم تطبيقها على عينة أخرى لملف فيديوي يتألف من (59) (frame) إطار ويبين الشكل (11) أحد أطر الملف الأصلي ويبين الشكل (12) ناتج تطبيق عملية البعثرة العشوائية على الإطار الأصلي.

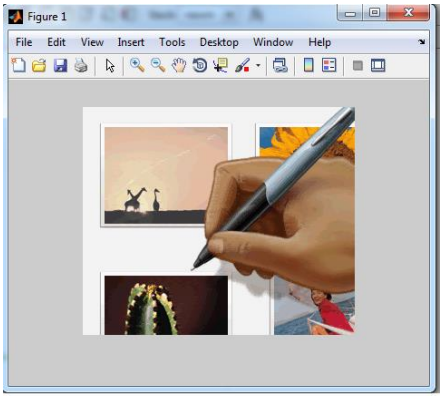


شكل(11). الملف الأصلي



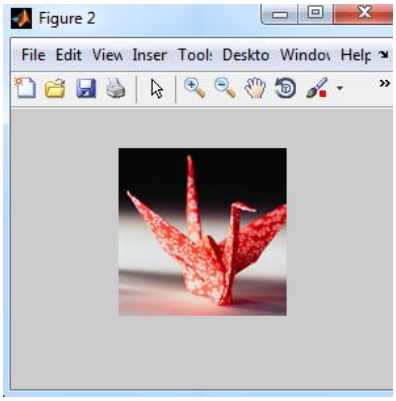
شكل (12). الملف المشفر بطريقة البعثرة العشوائية

ويبين الشكل (13) الملف المسترجع

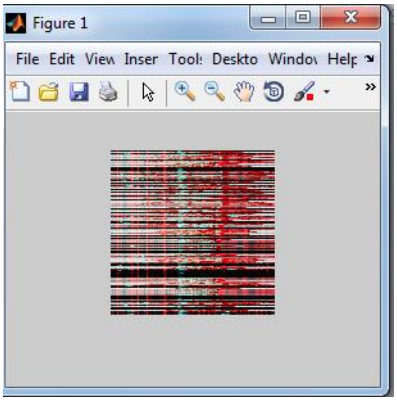


شكل (13). الملف المسترجع

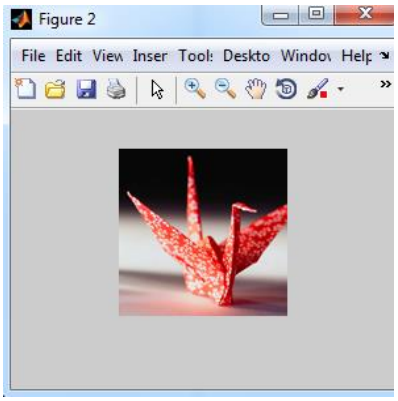
ويبين الشكل (14 و15) ناتج تنفيذ الخوارزمية المقترحة على ملف صوري من نوع (BMP.).



شكل (14). الملف الأصلي



شكل (15). الملف المشفر

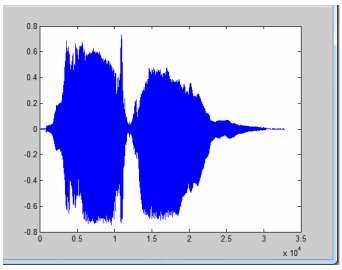


شكل (16). الملف المسترجع

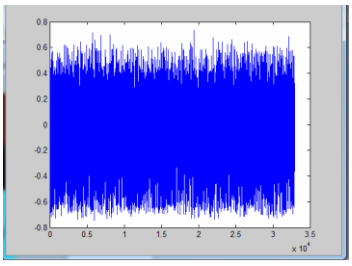
ولقد تم قياس قيمة PSNR مقاسة بل db للملف المشفر ولقد كانت القيمة (53.4967) وقيمة MSE= (0.2674).

وتبين الأشكال (17 و18 و19) ناتج تنفيذ الخوارزمية المقترحة على ملف صوتي من نوع (.wav).

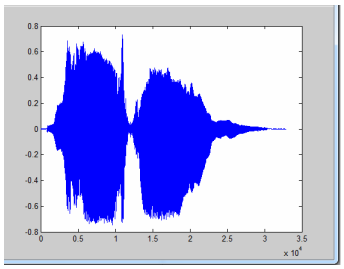
ويبين الشكل (14) التشوه الكبير الحاصل في الملف الصوتي والناتج عن تطبيق الخوارزمية المقترحة.



شكل (17). الملف الأصلي



شكل (18). الملف المشفر



شكل (19). الملف المسترجع

تجدر الإشارة إلى أن عملية التشفير للملف الفيديوي غير المكبوس بالرغم من كونها تحتاج وقت إلى أن الخوارزمية المقترحة في هذا البحث أثبتت سرعة كبيرة وسرية عالية ويبين الجدول (3) الوقت اللازم لعملية تشفير كل من الملفات الفيديوية المستخدمة.

ولقد ساعد استخدام لغة MATLAB10 على السرعة في تنفيذ الخوارزمية المقترحة لما يمتاز به من تسهيلات.

جدول (3). وقت عملية التشفير

أسم الملف	عدد الأطر (frames)	الزمن اللازم لتشفير الملف	حجم الملف
b	59	0.000003 ثانية	1.52MB
Bbb	54	0.00002 ثانية	148KB

ولقد كانت قيمة الـ PSNR للملف الأول db (94.6629) وقيمة MSE=0.004 وقيمة الـ PSNR للملف الثاني db (90.9202) وقيمة MSE=0.009.

ويبين الجدول (4) الوقت اللازم لعملية تشفير الملفات الصورية والصوتية المستخدمة.

جدول (4). الوقت اللازم لعملية تشفير الملفات الصورية والصوتية المستخدمة

أسم الملف	نوع الملف	الزمن اللازم لتشفير الملف	حجم الملف
rr	BMP	0.000001ثانية	48kb
RED	WAV	0.00002ثانية	63.3KB

2- الاستنتاجات

1- إن عملية التشفير باستخدام طريقة البعثرة العشوائية أثبتت كفاءة وسرعة عالية وذلك من خلال الوقت القليل جدا اللازم لعملية التشفير فضلاً على التشوه الكبير في الملفات الصورية والملفات الفيديوية والملفات الصوتية التي تم تطبيق الخوارزمية عليها.

2- الخوارزمية المقترحة أثبتت كفاءة وذلك لسرعتها وعدم تأثيرها على حجم الملف إذ بقي حجم الملف ثابتاً بعد التحليل.

3- الخوارزمية المقترحة حققت المعايير المهمة لتشفير الوسائط المتعددة.

المصادر

[1] احترف ماتلاب 7، الطبعة الأولى 2007، سوريا/حلب–دار الشعاع للنشر والعلوم/ترجمة وإعداد المهندس ظافر محمود.

[2] C. Narsimha Raju, Ganugula Umadevi, Kannan Srinathan, C.V. jawahar, (2008), "A Novel Video Encryption Technique Based on Secret Sharing", IEEE, 978-1-4244, 2008.

[3] Changgui Shi,Bharat Bhargara, (1998). "Fast MPEG Video Encryption Algorthim", Department of computer Sciences, Purdue University.

[4] Douglas R. Stinson., (1995), "Cryptography theory and Practice", CRC Press, Inc, NewYork.

[5] L.Qiao and Klara Nahrstedt,(1997),"A new algorithm for MPEG video encryption,"in Proc.of first International Conference on Imaging Science System and Technology,pp.21-29.

[6] Lei Tang., (1996), "Methods for Encryption and Decryption MPEG Video Data Efficiently. In Processing ACM Multimedia, pages 219-229, Boston, MA., November.

[7] Steven McCanne and Van jacobson. (1995). vic: A Flexible Framework for Packet Video. In Proc. of ACM Multimedia'95, pages 511-522, San Francisco, California Nov. 1995.

[8] T.B. Maples and G.A. Spanos. "performance Study of a Selective Encryprtion Schemefor Security of Networed,real-time Video", (2008), In Proceedings of The 4th International Conference on Vomputer Communications and Nework, September.

[9] Tanya E. Seidel, Daniel Sock, Michal Sramka, (2010), "Cryptanalysis of Video Encryption Algorithm", Florida Atlantic University, USA.

[10] Wenjun Zeng and shawmin lei, (2002), "Efficient frequency domain selective scrambling of digital video", in Proc. Of the IEEE Transaction on Multimedia, pp.118-129.

[11] Zhenyong chen, Zhang Xiong, and Long Tang, (2006), "A novel Scrambling Scheme for digital video encryption", in Proc. of Pacific-Rim Symposium on Image and Video Technology (PSIVT), pp. 997-1006.