Design Hybrid Algorithm for Video Encoding

Ghada Mohammad Tahir Qasim Toqa Zuhair Sahar Saleh Amena Emad
ghada@uomosul.edu.iq
College of Computer Sciences and Mathematics
University of Mosul, Mosul, Iraq

Received on: 25/04/2012 Accepted on: 18/09/2012

ABSTRACT

The most of the related studies and researches have focused on encrypting video files on speed and accuracy in the process of encryption. Some of them have focused on reducing the time required for the calculations. Some of them have focused on increasing the privacy of the process of encryption, regardless the processes of calculations.

Due to the fact that all the studies and researches that have been found were focused on the use of some of the ways of encrypting the texts like data encryption standard (DES) in encrypting video files ,and the fact that all the weakness points were related to the calculations, so in this research, many of these methods were connected with modification required to reduce the calculations and to obtain the speed of encrypting video files and give them a high privacy.

The research has been completed in five stages, four of which are used to provide four levels of protection with levels of internal protection to ensure high privacy. The fifth stage is to conduct the process of analyzing the code of the files that has been encrypted in the previous stages as show below:

The first stage :using the style of scrambling by using a developed style by using a proposed function ,but not by using the style of texts, to ensure speed of performing this method.

The second stage: Using the style of changing some color values to ensure high privacy.

The third stage; Using the style of scrambling (column scrambling) to ensure a stage of higher privacy.

The fourth stage: Using the scrambling method of the color values that bear higher frequency.

The fifth stage :Analyzing the video files resulting from the process of encryption.

As well as achieving an external protection for the program via checking the user ID and the used keys.

It should be pointed out that the results of this research has been achieved by using MATLAB 7 and MATLAB10 languages.

Keywords: video encoding , multi media encoding, encoding algorithm

تصميم خوارزمية هجينة لتشفير ملف فيديوي

غادة محمد طاهر قاسم الدباغ تقى زهير سحر صالح آمنة عماد
كلية علوم الحاسوب والرياضيات، جامعة الموصل

تاريخ استلام البحث: 2012\04\25 تاريخ قبول البحث: 2012\09\18

الملخص

لقد ركزت معظم الدراسات والبحوث الخاصة بتشفير الملفات الفيديوية على السرعة والدقة في عملية التشفير.

فلقد ركز البعض على اختصار الوقت اللازم للحسابات والبعض الآخر ركز على زيادة سرية عملية التشفير بغض النظر عن العمليات الحسابية.

ونظراً لكون جميع الدراسات والبحوث التي تم الإطلاع عليها كانت تركز على استخدام بعض من طرائق تشفير النصوص مثل DES (Data Encryption Standard) في تشفير الملفات الفيديوية ولكون جميع نقاط الضعف كانت تتعلق بالحسابات لذلك تم في هذا البحث أنجاز خوارزمية جديدة تشمل العديد من ميزات هذه الطرائق بالإضافة إلى تقليل الحسابات مما أدى إلى سرعة في تشفير الملفات الفيديوية واكسبها سرية عالية. لقد تم إنجاز البحث على خمس مراحل أربع منها استخدمت لتوفير أربعة مستويات من الحماية مع مستويات حماية داخلية لضمان سرية عالية أما المرحلة الخامسة فكانت لإجراء عملية تحليل شفرة الملف الذي تم تشفيره في المراحل السابقة وكما يأتي:

المرحلة الأولى: استخدام طريقة البعثرة ولكن ليس باستخدام أسلوب خوارزمية (DES) النصوص وإنما بأسلوب مطور من خلال استخدام دالة مقترحة بما يضمن السرعة لأداء هذه الطريقة.

المرحلة الثانية: استخدام أسلوب تغيير بعض القيم اللونية مما يضمن سرية عالية.

المرحلة الثالثة: استخدام أسلوب البعثرة (Column Scrambling) لضمان مرحلة أعلى من السرية.

المرحلة الرابعة: استخدام طريقة البعثرة للقيم اللونية التي تحمل أعلى تردد.

المرحلة الخامسة :تحليل الملف الفيديوي الناتج من عملية التشفير.

فضلا عن أنجاز حماية خارجية للبرنامج من خلال فحص رمز المستخدم والمفاتيح المستخدمة ولقد كانت نتائج الخوارزمية المطورة في هذا البحث جيدة جداً، وتجدر الإشارة إلى أنه تم إنجاز هذا البحث باستخدام لغة ماتلاب (MATLAB 7 MATLAB 10).

الكلمات المفتاحية: تشفير الفديو، تشفير الوسائط المتعدده، خوارزميات التشفير

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 .[8].

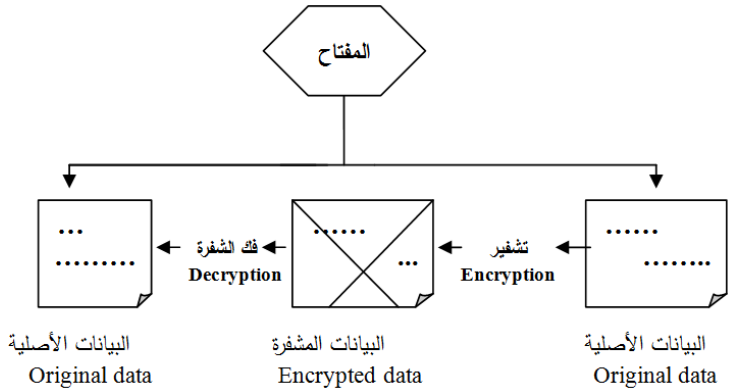
إن خوارزميات التشفير التقليدية مثل DES (Data Encryption Standard) و(Advanced AES (Encryption Standard وغيرهما من طرائق تشفير النصوص، أصبحت غير ملائمة لتشفير بيانات الملفات الفيديوية بسبب كبر حجم بيانات الوسائط المتعددة (Multimedia) والتقيد بالزمن الحقيقي لتشفير الملفات الفيديوية[8].

لقد اقترحت عدة طرائق لتشفير الملفات الفيديوية البعض منها ركز على تقليص الحسابات المطلوبة في عملية التشفير لتقليل الوقت اللازم لتشفير الملفات الفيديوية والبعض الآخر حاول استخدام طرائق البعثرة والتي سيتم التطرق لها لاحقاً.

2- خوارزميات المفتاح المتماثل وغير المتماثل

في **خوارزمية المفتاح المتماثل**، المفتاح المستخدم في التشفير هو نفسه في فك الشفرة ويبقى سريا بين المرسل والمستلم، والمفتاح في الأنظمة التي تستخدم هذه الخوارزمية يتبادل بين الأطراف بطريقة فيها بعض السرية (عن طريق قناة سرية (secret channel)). ويصبح المفتاح بدون معنى عند زيادة عدد المشتركين، أو عندما

تكون القناة السرية غير متوفرة لتبديل المفتاح. وعمليا، المفتاح المنفصل مطلوب لكل زوج من الأطراف، وهذا النوع من النظام يدعى عادة بنظام تشفير المفتاح الخاص(Private Key)، أو المفتاح السري (secret Key)، أو المفتاح التقليدي(conventional Key)، وهذا النوع من الخوارزميات يكون سريعا ومناسبا إذا كانت البيانات لا تحتاج إلى اشتراك(تشفير قرص صلب، أو تشفير ملف بيانات حساس في الحاسبة الشخصية) كما في الشكل (1).[4]

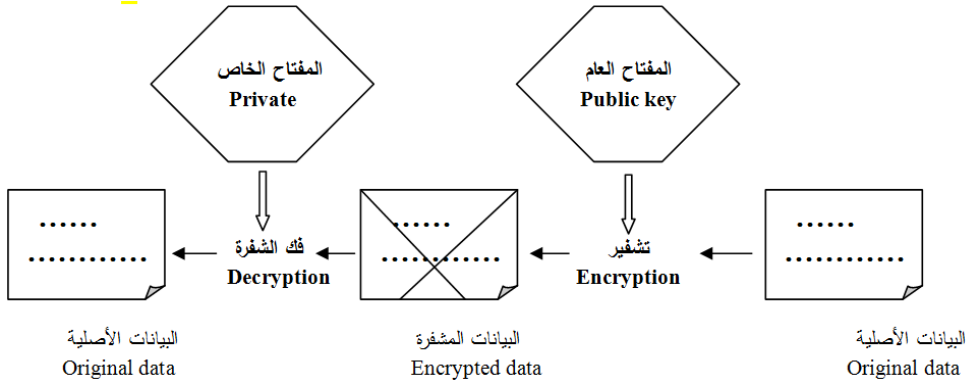


شكل (1) التشفير باستخدام المفتاح المتماثل[4]

من الخوارزميات المتماثلة المعروفة، خوارزمية تشفير البيانات القياسية (Data Encryption Standard (DES)) وهي من أكثر الخوارزميات استخداما في العالم وتستخدم مفتاحا للتشفير يتكون من 56 رقما ثنائيا، وبسبب كسرها فقط طورت إلى (Triple DES). ومنها أيضا خوارزمية تشفير البيانات العالمية ((IDEA) International Data Encryption Algorithm) وتعد من الخوارزميات الأسرع من (Data Encryption Standard) DES والأكثر سرية الموجودة حاليا، تستخدم مفتاحا مكوناً من 128 رقما ثنائيا. [4]

أما خوارزميات المفتاح غير المتماثل، فيوجد فيها زوج من المفاتيح التي تكون مترابطة رياضيا، الأول يستخدم في التشفير والثاني لفك الشفرة. وبعض الخوارزميات التي تستخدم هذا المفتاح وليس جميعها لها خواص إضافية التي تجعل المفتاح الأول عاما أما الثاني فلا يكون عاما ويستنتج من المفتاح العام (Public key) ويكون سريا ويسمى المفتاح الخاص (Private key) وتعرف الخوارزمية من هذا النوع بخوارزمية المفتاح العام/المفتاح الخاص .[4]

في هذا النوع يوجد زوج من المفاتيح لكل مستلم (مهما كان عدد المرسلين) ، امتلاك مفتاح عام لا يفشي سرية الخوارزمية مادام لم يعرف المفتاح الخاص الذي يقابله من أي مهاجم كما في الشكل (2).



شكل (2) التشفير باستخدام المفتاح غير المتماثل[4]

3- الوسائط المتعددة

مجموعة من تطبيقات الكومبيوتر التي يمكنها تخزين المعلومات بأشكال متعددة مثل النصوص والأصوات والرسوم والصور الساكنة منها والمتحركة والفيديو، وعرض هذه المعلومات بطريقة تفاعلية "Interactive" وفقا لمسارات يتحكم فيها المستخدم.[15][5]

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. [10][9]

4- أنواع الملفات الفيديوية (صيغ الملفات الفديوية)

توجد عدة أنواع للملفات الفيديوية وعدة صيغ ويبين الجدول (1) صيغ الملفات الفيديوية مع بعض المعلومات عنها.

الجدول (1) صيغ الملفات الفيديوية

صيغة الملف الفيديوي	المعلومات عن الصيغة
صيغة ملف AVI (Audio Video Interleave)	طورّت هذه الصيغة في جميع الملفات الفيديوية من قبل شركة (Microsoft) وتم دعم صيغة AVI من قبل كل الحاسبات التي تنفذ الويندوز (Windows) ومن قبل أكثر متصفحات الانترنت شيوعاً. تجدر الإشارة إلى أن صيغة الـ AVI هي صيغة ملائمة جداً على الانترنت، لكن ليس بالإمكان تشغيلها على الحاسبات التي لا تستخدم الويندوز (Windows).
صيغة ملف MPEG(Moving Picture Expert Group)	لها ثلاث صيغ للملفات الفيديوية وهي (MPEG-1،MPEG-2،MPEG-4)
MPEG-1	هي أكثر الصيغ شيوعاً في الاستخدام على الأنترنت. الملفات الفيديوية التي تخزن بصيغة MPEG يكون امتدادها أو mpe. تعتبر الـ MPEG-1 أقدم صيغة جُهزّت بكافة متطلبات العرض الجيد بأبعاد عرض على الأقل أكثر من (240×352) وهي كفاءة معقولة وصيغة جيدة للويب (web).
MPEG-2	وتوفر أمكانية كبس أفضل وأبعاد عرض (720x480). وتستخدم هذه الصيغة في (الفيديو الرقمي) Digital Video Disk)DVD) والـ SVCD (Super Video Compact Disk)
MPEG-4	مجموعة من الشفرات البعض منها مفتوح والآخر خاص بملكية شركة مايكروسوفت (Microsoft).
صيغة ملف MJPEG (motion JPEG)	هي صيغة تتألف من سلسلة من صور الـ JPEG وتكون هذه الصيغة ملائمة للملفات الفيديوية التي يتم الحصول عليها من الكاميرات الرقمية وتعتبر صيغة مقبولة للتعامل مع الملفات الفيديوية ولكن تكون غير مكبوسة بشكل جيد ولذلك تكون غير جيدة بالنسبة للتوزيع على الانترنيت.
صيغة الوسائط الحقيقية RM(Real Media)	هي صيغة تم تطويرها من قبل مصممي الشبكات الحقيقية لغرض الحصول على سلسلة من الفيديو والصوت

ونظراً لكون لغة ماتلاب (Matlab) هي اللغة التي تم إنجاز البحث بها، آثرنا أن نعطي نبذة عن كيفية

تعامل هذه اللغة مع الملفات الفيديوية والصوت والصور،وفيما يلي شرح موجز عن كل فقرة.

5- الفيديو في لغة ماتلاب (MATLAB)

الفيديو هو مجموعة صور متحركة "Moving Image" دون رؤية متقطعة للحركة بسبب سرعة تغيير الصورة.[2][12]

يؤمِّن التابعان (getframe و movie) الأدوات اللازمة لإلتقاط اطر الملفات الفيديوية وتشغيلها، إذ يقوم الأمر (getframe) بالتقاط صورة للشكل الحالي في حين يقوم الأمر (movie) بتشغيل تتالي الإطارات بعد أن تم إلتقاطها، خرج التابع (getframe) هو بنية تتضمن كافة المعلومات اللازمة للتابع (movie) وإلتقاط عدة إطارات هو مجرد إضافة عناصر جديدة إلى البنية. أما المعطيات اللونية الموجودة في المصفوفة (cdata) تشكل صورة نقطية بألوان حقيقية أو (RGB) .[1].

5-1 ملف الـ AVI في لغة ماتلاب (MATLAB) :

بصورة عامة، ملفات الـ AVI تحتوي على العديد من الاطر ولأنواع مختلفة من البيانات، لكن اغلب ملفات الـ AVI تستخدم أطر الفيديو والصوت، ومن الممكن ان تستخدم بيانات فيديو فقط وبدون الحاجة لأطر صوت. [5]

ونظرا لكون نوعية الملفات الفيديوية التي تم استخدامها في البحث هي من نوع AVI لذلك يبين الجدول(1) الايعازات التي تتعامل مع ملف ال AVI

جدول(2) الايعازات التي تتعامل مع ملف الAVI

الأيعاز في ماتلاب7 (MATLAB 7)	المهمة التي يقوم بها	الصيغة العامة
Avifile	ينشئ ملف فيلم من الصيغة avi.	aviobj = avifile(filename)
Aviread	يقرأ ملف فيلم من الصيغة avi.	mov = aviread(filename)
Aviinfo	يستخلص معلومات عن ملف الفيلم من صيغة avi.	fileinfo= aviinfo(filename)
Addframe	يضيف اطارا الى ملف فيلم من الصيغة avi.	aviobj=addframe(aviobj،frame)
Close	يغلق ملف الفيلم ذا الصيغة avi.	Close
الإيعاز في ماتلاب10 (MATLAB 10)	**المهمة التي يقوم بها**	**الصيغة العامة**
mmReader	يقرأ ملف فيلم	Obj = mmReader (filename)
mmFileInfo	يستخلص معلومات من ملف الفيديو	Info = mmFileInfo (filename)
Video.Multimedia FileReader	والـ Videoيجهز معلومات إضافية عن الـ Audioالخاص بالملف الفيديوي	Hmfr = video.Multimedia FileReader ('filename' , 'Audio Outputport' , true)

6- تشفير الملفات الفيديوية

لقد اهتمت الدراسات الأخيرة بتشفير تطبيقات الوسائط المتعددة ومنها الملفات الفيديوية ونظراً لكون عملية تشفير الملفات الفيديوية هو موضوع بحثنا لهذا سوف يتم التطرق إلى أهم التحديات الخاصة بتشفير الملفات الفيديوية و المعايير الخاصة بخوارزميات تشفير بيانات الملفات الفيديوية وأهم الخوارزميات التي تم التعرف عليها

من خلال البحوث التي تم الحصول عليها.

6-1- تحديات تشفير ملفات الوسائط المتعددة

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

أ- حجم البيانات: حيث 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: حيث أن نسبة المعلومات في تطبيقات الوسائط المتعددة تكون كبيرة جداًولكن قيمة المعلومات ضعيفة، إن عملية فك شفرة هذا النوع من التشفير سوف يحتاج إلى كلفة أكبر من كلفة شراء البرنامج.[7]

6-2- 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.[7]

7- الدراسات السابقة

إن جميع الخوارزميات التي تم التعرف عليها من خلال البحوث المستحصلة كانت تتعامل مع ملفات الـ MPEG لما تمتاز به هذه الملفات من نسبة كبس مما يجعل عملية التشفير سريعة. وكانت معظم هذه الخوارزميات تركز على طريقة الـ DCT (Discrete Cosine Transform) التى تستخدم في كبس الصور وكانت عمليات التشفير تركز على التعامل مع معاملات الـ DCT من حيث البعثرة أو التغيير باستخدام بعض طرق تشفير النصوص مثل الـ (DES) (Data Encryption Standered) وكانت معظم المشاكل التي تعاني منها هذه الطرق هو كثرة الحسابات.

لقد أستخدم كل من Changgui shi&Bharat Bhargavaالملفات الفيديوية من نوع MPEG و تجدر 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 الـ (bit) قد لا تتغير إذا كان الـ (bit) المقابل له من المفتاح قيمته تساوي صفراً وقد تتغير إشارة الـ (bit) من الموجب إلى السالب (0 إلى 1) أو قد يتغير بت الإشارة من السالب إلى الموجب أي (1 إلى 0) كما مبين في المعادلات التالية:

S=s1:,…….,s2,……,s3,…….,sm ……..(1)

وعملية تغيير الإشارة الخاصة بالـ bits الخاصة بمعاملات الـ DC و AC كما مبين في المعادلة الاتية:

$EK(s)=(b1 \oplus s1).....(bm \oplus sm)$ .....(2)

حيث $\oplus$ هي عملية XOR

ولقد بينت نتائج هذه الخوارزمية أنه عند تشفير كل معاملات الـ (AC) و الـ (DC) تصبح الصورة الناتجة غير مفهومة.[7]

ولقد عرف TANG بعض الطرائق التي تضم عمليتي كبس وتشفير ملفات الMPEG بخطوه واحد.تعتمد هذه الخوارزمية مبدأ البعثرة (scrambhzling) وتستخدمه في جزء الكبس حيث تطبق طريقة البعثرة لإجراء تبديل عشوائي لمعاملات الـ DCT في تحويله إلى متجه (1x64 block) بدلا من ترتيب الـ (zig- zag). إن الطرق التي أستخدمها TANG تقلل نسبة كبس الملف الفيديوي.[11]

إن الخوارزميات التي أقترحها كل من Maples وSteven 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.[13][14]

إن الخوارزميات التي أقترحها كل من Tang وMaples وSteven تحتاج إلى حسابات ضخمة وتقلل نسبة الكبس.[7]

لقد برهن **خوارزميةَ Qiao and Klara** أن خوارزمية Tang تعاني من

1- خطر معرفة النص الصريح (known – plain text)

2- هجوم النص المشفر فقط (Cipher text only attack)

واقترحوا خوارزمية جديدة تسمى (VEA) (Video Encryption Algorithm) حيث يتم تقسيم كل (chunk) من ال(Iframe) الى نصفين.كلا النصفين تتم بينهما عملية (XOR) وتخزن النتيجة بأحد الإنصاف والنصف الثاني يتم تشفيره بخوارزمية قياسية (DES (Data Encryption Standered وهذه الخوارزمية توفر سرية جيدة. وعلى كل حال لا تستخدم هذه الخوارزمية في تطبيقات الزمن الحقيقي (real –time)[10]

إن الخوارزمية المقترحة في هذا البحث تمتاز بأنها لا تحتاج إلى حسابات ضخمة والوقت المستغرق في عملية التشفير وفك التشفير قليل جدا مع بقاء حجم الملف ثابت

لقد وسع Zeng and Lie في خوارزميتهم خوارزمية (Tang) وجعلوها تستخدم مقطع من الكتل الصغيرة (segment of macro block) بدلا من استخدام (block) وفي كل مقطع (Segment) يتم تحريك معاملات الDCT التي تحمل التردد نفسه عشوائيا ضمن نفس المقطع.[16].

ولقد طور **Chen** 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 أبدلو اتجاه الحركة لكل من الP and B frame.[17] إن البعثرة لوحدها لا توفر سرية عالية في عمليات تشفير الوسائط المتعددة[4].

تجدر الإشارة إلى أن البعثرة المستخدمة في خوارزميتنا المقترحة في هذا البحث لم تقتصر على الأطر (frames) وإنما شملت الأعمدة المكونة لكل صورة من صور الأطر مع تغيير القيم اللونية مما أكسب عملية التشفير سرية عالية.

لقد أقترح الباحثان C.Narsimha Raju,Ganugula Umadevi, Kannan Srinathan, C.V.Jawahar, خوارزمية تستخدم ملفات الـ (MPEG) حيث تكون قيم الـ (DC) الخاصة بمصفوفة الDCT (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[6]

تجدر الإشارة إلى أن الخوارزمية المقترحة في هذا البحث قد بنيت على استخدام المفاهيم المستخدمة في بعض هذه الخوارزميات مع تطوير هذه المفاهيم بما يخدم عملية التشفير وفك الشفرة كما إن الخوارزمية المستخدمة

في هذا البحث تعد الأولى في التعامل مع ملفات الـ AVI (Audio Video Interleave) وكانت ملفات AVI المستخدمة في التشفير غير مكبوسة وقد أثبتت الخوارزمية المستخدمة سرعة عالية ودقة سوف يتم ملاحظتها من خلال النتائج المستحصلة التي سيتم مناقشتها بالرغم من كون الملفات المستخدمة غير مكبوسة.

8- الخوارزمية المطورة للتشفير

يتم في هذه الخوارزمية تحقيق العديد من معايير خوارزمية التشفير الجيدة إذ يتم في هذه الخوارزمية استخدام أربعة مفاتيح سرية مما يضمن سرية عالية لهذه الخوارزمية وتجدر الإشارة إلى أن عدد المفاتيح المستخدمة لا يؤثر على سرعة الخوارزمية المقترحة.

توفر الخوارزمية المقترحة أربعة مستويات من الحماية للملف الفيديوي من خلال استخدام أربعة مفاتيح تشفير مختلفة (secret keys) إذ يختلف المفتاح المستخدم في كل مستوى عن المفتاح المستخدم في المستوى الذي يسبقه وعن المستوى الذي يليه وضمن بعض المستويات مثل مستوى بعثرة القيم ذات التردد العالي يتم ملاحظة استخدام مفتاح key آخر إضافي في هذا المستوى إذ يتم تشفير جزء من الملف ضمن المفتاح المدخل أما تشفير الجزء الثاني من الملف يتم تشفيره بواسطة مفتاح ثاني يتم توليده ذاتياً داخل المستوى مما يجعل من الصعب على الشخص المتطفل حتى في حالة اكتشاف المفتاح الخارجي اكتشاف المفتاح الداخلي.

تجدر الإشارة إلى أن الخوارزمية المطورة لا تقتصر على إجراء عملية التشفير فقط وإنما تم أيضاً في هذا البحث أنجاز خوارزمية استرجاع الملف المشفر.

12- خطوات الخوارزمية المطورة

1- الخطوة الأولى: إدخال ملف الفيديو من نوع AVI (Audio Video Interleave) ثم أدخل الرمز (code) الخاص بالمستخدم لزيادة السرية عند عملية الإرسال ثم أدخل مفاتيح التشفير (EK4 EK3, EK2, EK1,) للسماح بدخول المستخدم إلى البرنامج.

2- الخطوة الثانية: إذا كان رمز المستخدم غير صحيح أو أي مفتاح تشفير لا يحقق الوثوقية، اذهب إلى الخطوة (19) وإذا كانت القيم صحيحة يتم الانتقال أستمر.

3- الخطوة الثالثة: قراءة المعلومات الخاصة بالملف الفيديوي وحساب عدد الأطر (Frames) الخاصة بالملف الفيديوي.

4- الخطوة الرابعة: تطبيق خوارزمية البعثرة على الأطر (Frames) الخاصة بالملف الفيديوي وفق مفتاح التشفير الأول (EK1) كما موضح بالمعادلة الآتية

```
For j=1:no of frames
Ij+EK1
End
```

5- الخطوة الخامسة: تحويل أطر الملف الفيديوي إلى صور.

6- الخطوة السادسة: حساب تردد القيم اللونية لكل صورة (الهستوكرام) من صور أطر (Frames) الملف الفيديوي من خلال مصفوفة الألوان الخاصة لكل صورة (cmap) كما موضح فيما يأتي

```
For i=1:256
For i1=1:image size1
For j1=1:image size2
If  x(i1,j1)==cmap(i)
```

```
d(i)=d(i)+1;
end ; end ; end ; end
```

حيث x(i,j) هي مصفوفة الصورة، Cmap(i) هي مصفوفة ألوان الصور,d(i) هي مصفوفة تردد الألوان في كل صورة من صور الأطر (Frames) الخاصة بالملف الفيديوي.

7- الخطوة السابعة: حساب أكبر تردد للألون (py) Py=max(d);

8- الخطوة الثامنة: تغيير القيم اللونية التي تحمل أعلى تردد بقيم أخرى وفق المفتاح EK2 وفق المعادلة التالية:

```
If x(i,j)=py
x(i,j) ↔ x(i,j)+EK2;
end
```

9- الخطوة التاسعة: إعادة الصورة إلى الإطار (Frame).

10- الخطوة العاشرة: تحويل الأطر (Frames) الخاصة بالملف الفيديوي إلى صور.

11- الخطوة الحادية عشرة: تحديد قيم الأعمدة التي سيتم إجراء البعثرة عليها باستخدام مفتاح داخلي (key) بالاعتماد على قيمة مفتاح التشفير الثالث (EK3). كما في المعادلة التالية:

```
if EK3=SK
```

$x(i,j_{nkey(i1)}) \leftrightarrow x(i,j_{nkey(i1)})$

حيث nkey هي مصفوفة المفتاح (key) الداخلي المستخدم، x(i,j) هي مصفوفة الصورة الناتجة.

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

13- الخطوة الثالثة عشر: تحويل أطر الملف الفيديوي (Frames) إلى صور.

14- الخطوة الرابعة عشر: حساب الترددات للقيم اللونية لكل صورة وفقاً لمصفوفة الألوان الخاصة (cmap).

15- الخطوة الخامسة عشر: تغير القيم اللونية لكل صورة حسب عدد الأطر (frames) المكونة للملف الفيديوي.

```
For i=1:256
For i1=1:image size1
For j1=1:image size2
If  x(i1,j1)==cmap(i)
d(i)=d(i)+1;
end ; end ; end ; end
```

16- الخطوة السادسة عشر: إجراء عملية البعثرة للقيم التي تحمل أعلى تردد وفقاً لمفتاح التشفير الأخير كما في المعادلة التالية:

$x(i,j)=x(i,j_{scn})$

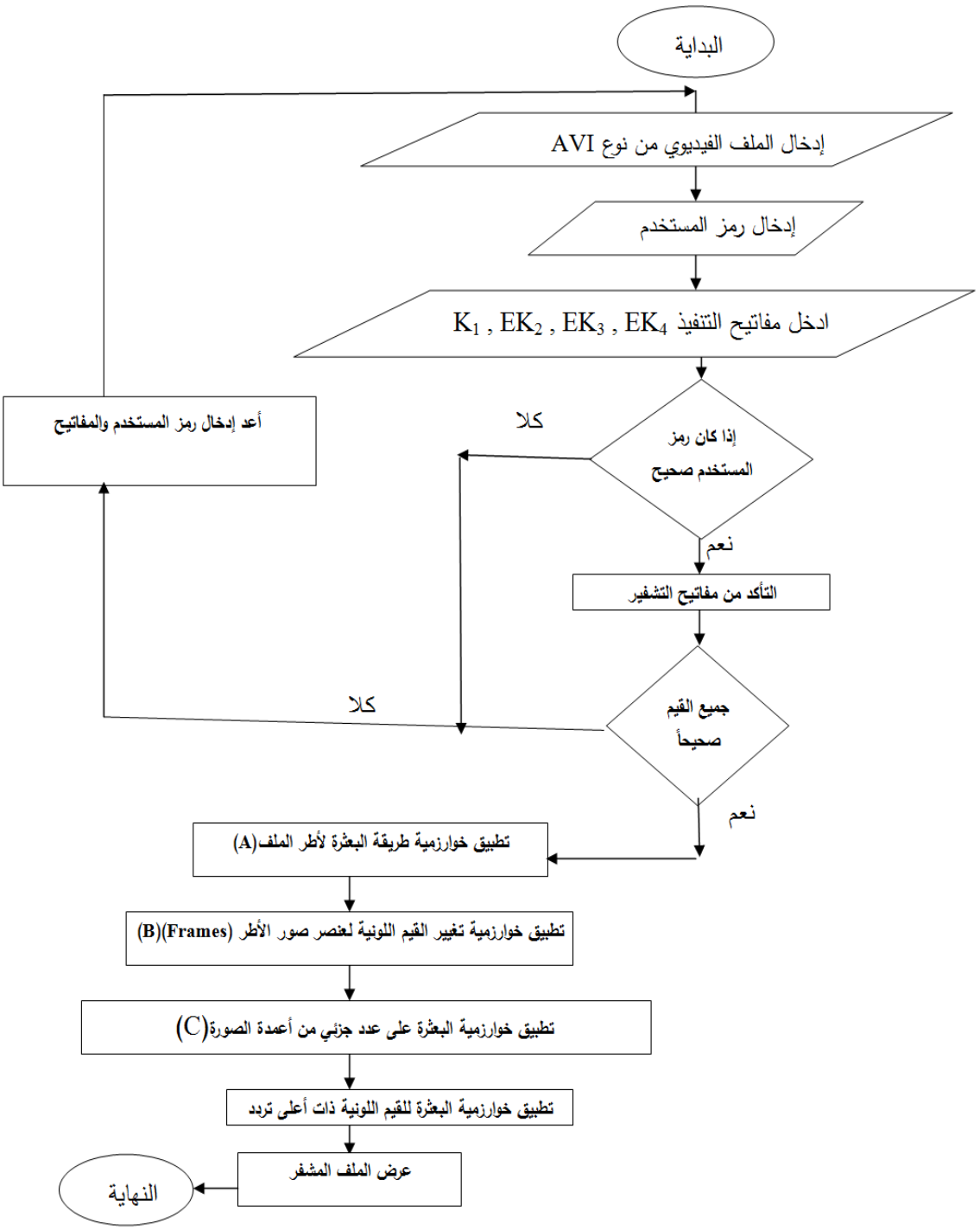
حيث x(i,j) هي مصفوفة الصورة، scn هو مفتاح التشفير الداخلي EK4.

17- الخطوة السابعة عشر: إعادة الصورة الناتجة إلى أطر الملف الفيديوي (Frames)

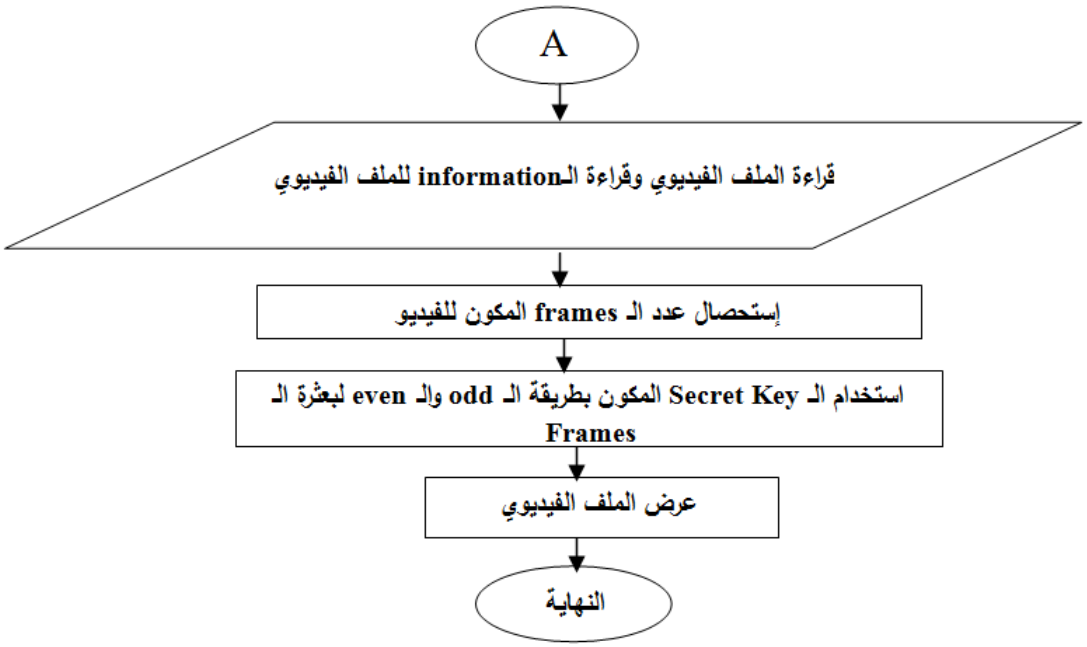
18- الخطوة الثامنة عشر: عرض الملف المشفر النهائي.

19- الخطوة التاسعة عشر: أعد إدخال مفاتيح التشفير ورمز المستخدم وأذهب إلى الخطوة (1).

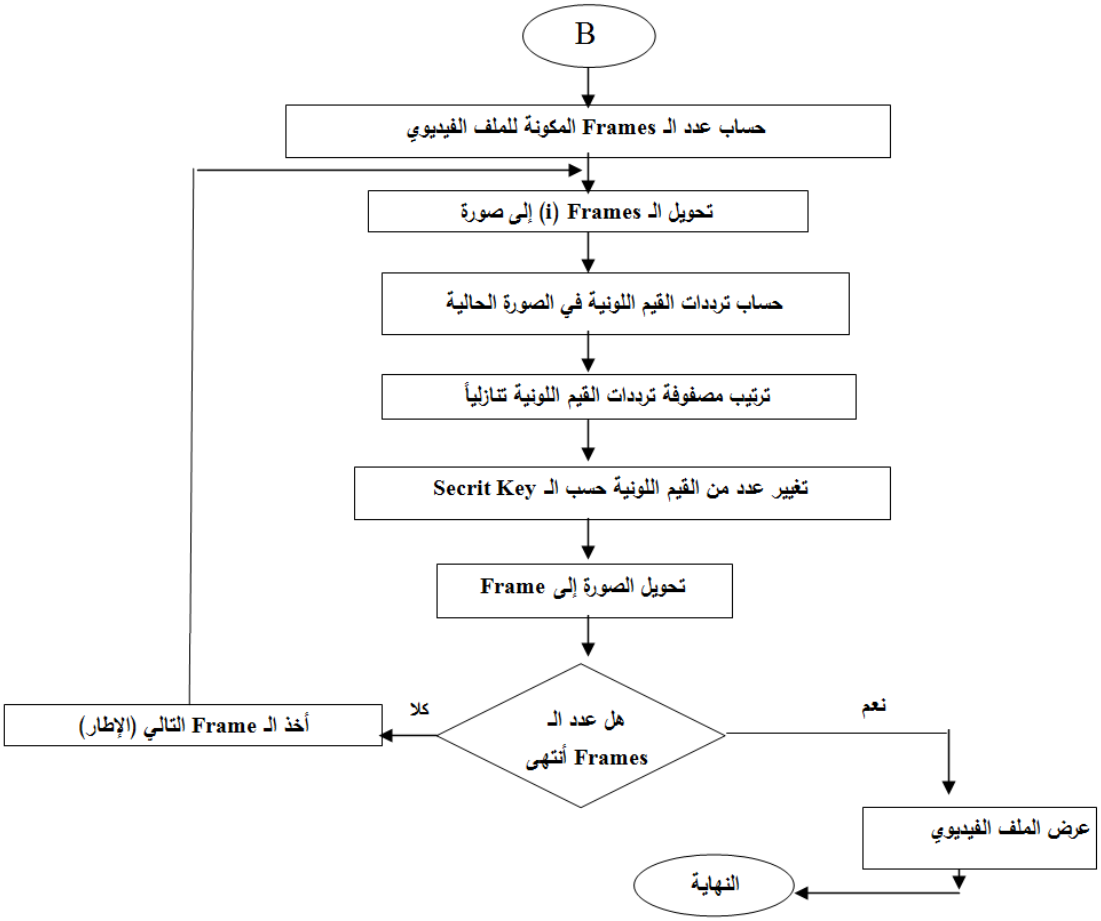
ويبين الشكل (3،4،5،6) المخطط الانسيابي للخوارزمية المطورة



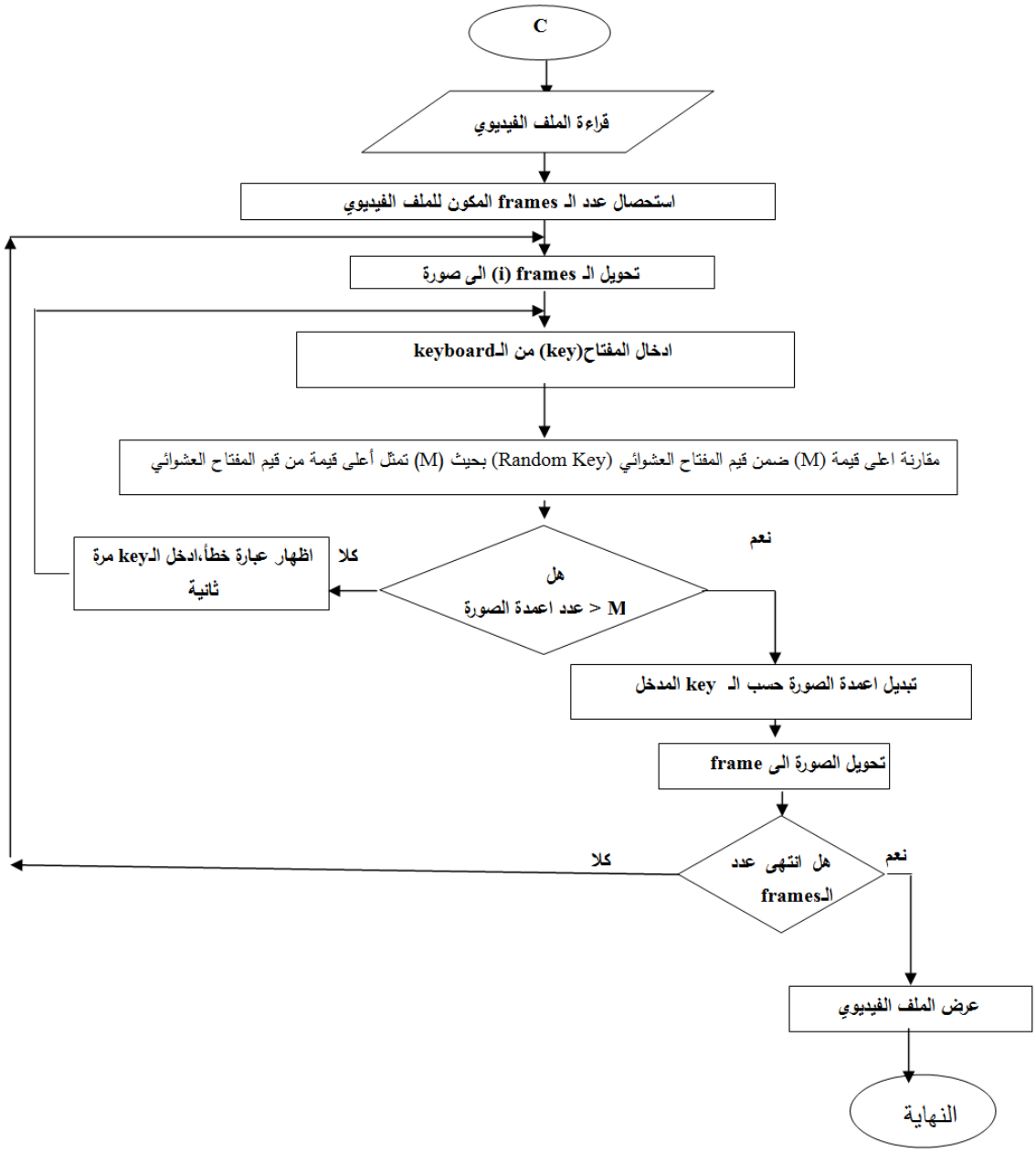
الشكل (3) المخطط الانسيابي لخوارزمية التشفير الجديدة



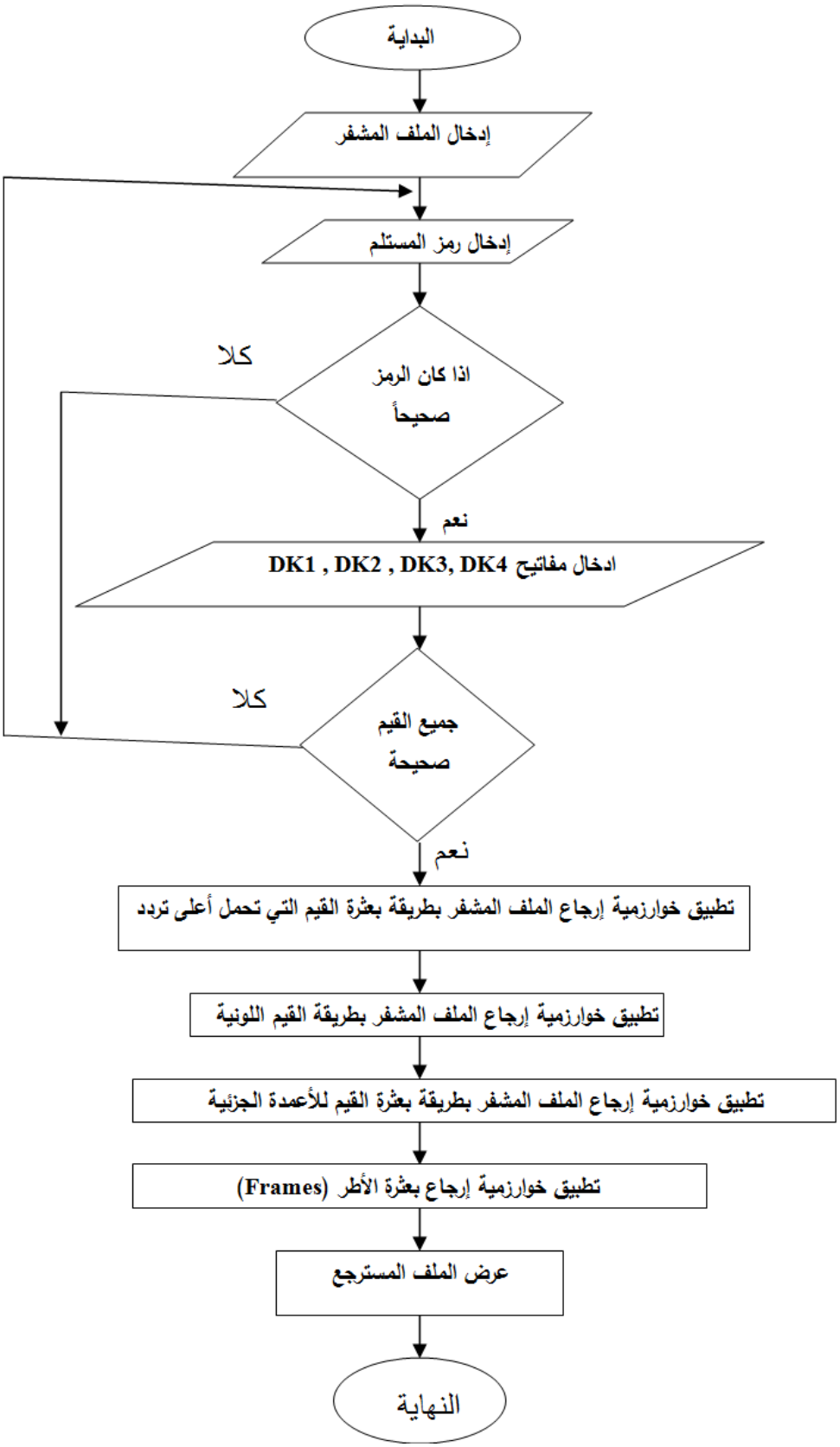
شكل (4) المخطط العام لطريقة البعثرة (A)



الشكل (5) المخطط العام لطريقة تغيير القيم اللونية (B)



الشكل (6) مخطط عام لبعثرة الأعمدة المكونة للصورة حسب مفتاح مدخل(C)

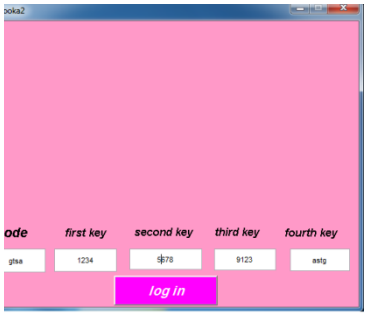


الشكل (7) المخطط العام لعملية التحليل

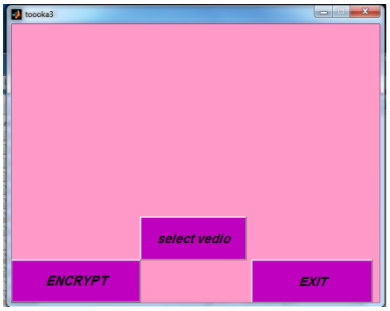
13- النتائج والاستنتاجات

1- النتائج

إن الشاشة الرئيسية للبرنامج المبينة في الشكل (8) تتطلب من المستخدم إدخال رمز المستخدم وإدخال المفاتيح الخاصة بعملية التشفير فإذا كان الإدخال صحيحاً تظهر شاشة اختيار الملف الفيديوي المبينة في الشكل (9) وتضم عملية اختيار الملف الفيديوي وتشفيره.

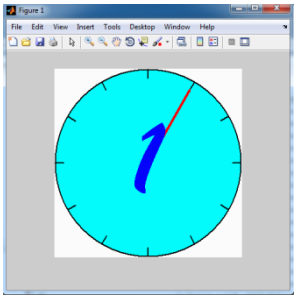


شكل (8) الشاشة الرئيسية

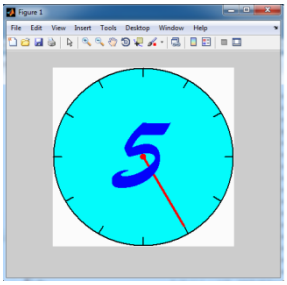


شكل (9) شاشة أختيار الملف الفيديوي

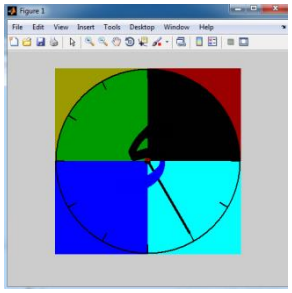
ويبين الشكل (10) واحداً من اطر الملف الأصلي المتكون من 12 إطار(frame) ويبين الشكل (11) عملية البعثرة للأطر إذ ظهر الإطار الخامس بدل الإطار الأول ويبين الشكل (12) ناتج تغيير القيم اللونية.



شكل (10) أحد أطر الملف الأصلي

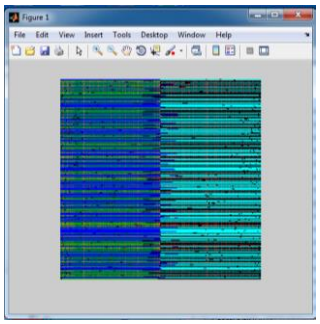


شكل(11) عملية البعثرة



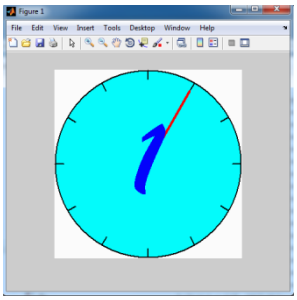
شكل (12) عملية تغيير القيم اللونية

ويبين الشكل (13) النتيجة النهائية لعملية التشفير بعد إجراء عملية بعثرة الصفوف والأعمدة.



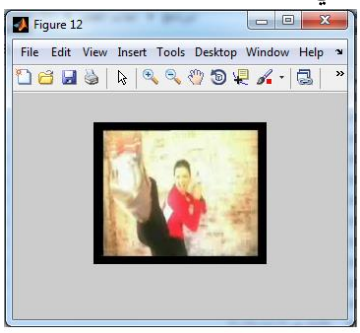
شكل(13) الملف المشفر

وتجدر الإشارة إلى أن الصور أعلاه هي لبيان تسلسل مراحل عملية التشفير لأحد أطر ملف فيديوي يتألف من (12) ولقد تم تشفير الملف كاملا بالطريقة المطورة وبكفاءة عالية إذ تم حساب PSNR لمعرفة نسبة التشوه وكانت تساوي(3.318 db) وهذه النسبة جيدة بالنسبة لعملية التشفير، كما أن النظام الذي أنجز في هذا البحث قد أشتمل على بناء خوارزمية استرجاع إذ يبين الشكل (14) احد اطر الملف المسترجع وهو مطابق للإطار الأصلي.



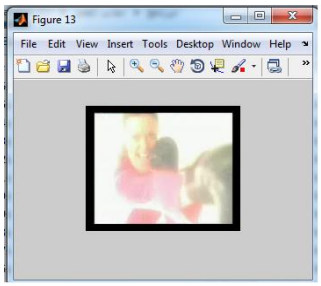
شكل (14) الإطار المسترجع

ولإثبات دقة الخوارزمية المطورة فلقد تم تطبيقها على عينة أخرى لملف فيديوي يتألف من (54)(frame) ويبين الشكل (15) أحد أطر الملف الأصلي.

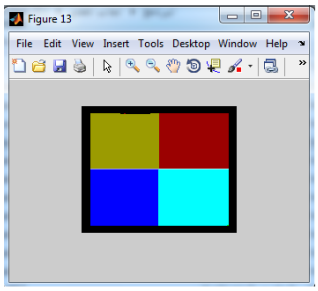


شكل (15) الملف الأصلي

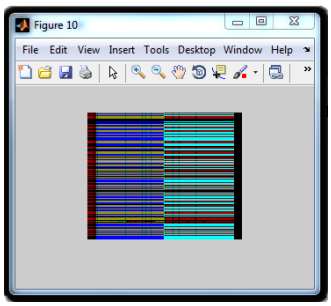
وتبين الأشكال (16،17،18) كل من عمليات البعثرة للأطر وتغيير القيم اللونية والمرحلة النهائية التي تضم عملية البعثرة للصفوف والأعمدة ويبين الشكل (19) الملف الملف المسترجع



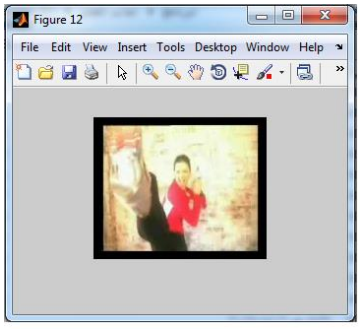
شكل (16) عملية البعثرة



شكل (17) تغيير القيم اللونية



شكل (18) الملف المشفر



شكل (19) الملف المسترجع

تجدر الإشارة إلى أن عملية التشفير للملف غير المكبوس بالرغم من كونها تحتاج وقتا إلى أن الخوارزمية المقترحة في هذا البحث أثبتت سرعة كبيرة وسرية عالية ولقد كانت قيمة ال PSNR للملف المشفر(8.3518) وهي نسبة جيدة ويبين الجدول (3)الوقت اللازم لعملية تشفير كل من الملفات المستخدمة

ولقد ساعد استخدام لغة MATLAB10على السرعة في تنفيذ الخوارزمية وذلك لسرعة هذا الإصدار ولوجود العديد من الايعازات التي تسهل التعامل مع الفيديو من نوع AVI بصورة موسعة.

جدول (3) وقت عملية التشفير

أسم الملف	عدد الأطر (frames)	الزمن اللازم لتشفير كل (frame)	عدد الأطر التي تعالج في الثانية (frame per second fps)	حجم الملف
Clock	12	2 ثانية	0.5	84kb
bbb	54	1.11 ثانية	0.90009	148kb
المعدل			0.700045	

2- الاستنتاجات

1- عملية التشفير باستخدام طرائق البعثرة أكثر سرعة من عملية تغيير القيم اللونية ولكنها أقل سرية.

2- إن عملية التشفير باستخدام أكثر من مفتاح وفرت سرية كبيرة.

3- إن عملية استخدام مفتاحين سريين ضمن نفس مستوى الحماية وفرت سرية عالية ولم تؤثر على سرعة التنفيذ حيث تم استخدام أربعة مفاتيح سرية للتشفير في بداية البرنامج وذلك لزيادة السرية.

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

المصادر

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

[2] صالح، نادية طارق، حزيران 2000، "المعالجة الفيديوية في الوسائط المتعددة"، أطروحة ماجستير، قسم علوم الحاسبات، كلية علوم الحاسبات والرياضيات، جامعة الموصل.

[3] حليم، علياء موفق عبد المجيد ،2003، "تشفير إشارة الكلام بطريقة البعثرة"، أطروحة ماجستير، علوم حاسبات، كلية علوم الحاسبات والرياضيات، جامعة الموصل.

[4] B.Furht and D.Kirovski,(2004),"Multimedia Security Handbook", CRC Press LLC,.

[5] C.Kotro Panlos and I.Patas,(2001),"Nonliner Model based image/video processing and analysis",Awiley-Enter science publication, John Wiley & Sons, inc,USA.

[6] 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.

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

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

[9] Kaplan, R.M., (1997) " Intelligent Multimedia Systems "Wiley Computer publishing.

[10] 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.

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

[12] Minasi, M., (1996), "The Complete PC Up Grade & Maintenance Guide", Sybex-inc.

[13] 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.

[14] 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.

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

[16] 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.

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