Journal of Education and Science
Vol. 27, No.3, 2018, pp. 99-117
ISSN 1812-125X
http://edusj.mosuljournals.com

إخفاء نص في القنوات الصوتية ضمن ملفات الصوت والفيديو

حسن ماهر أحمد النعمة

كلية علوم الحاسوب والرياضيات / جامعة الموصل

تاريخ الاستلام 2012/01/5 *تاريخ التسليم 2012/06/10*

Abstract

The aim of research and studies in the field of steganography to hide data inside other data are not aware, as the world witnessed during the recent period significant development in this area, and that the goal of this research is to hide the text data in secret within the media audio (wav), also been working on concealment within the channel audio in the video, and through access to the audio channels for each frame of video frames and include the data inside.

When we hide in the channel audio video clip of the type (Avi), all within a framework of frameworks The video has audio channels belonging to him can been forced in any one of the audio channels for each frame of frames the video, so it is very hard to detect sites of concealment where the view of the capacity high for the video, it is possible to hide a very large amount of information without a clear change in the video, where the results of concealment in audio channel of digital video is fully compatible with the goal of the research.

المستخلص

تهدف البحوث والدراسات في مجال إخفاء المعلومات إلى إخفاء بيانات داخل بيانات أخرى بشكل غير مدرك، حيث شهد العالم خلال الفترة الأخيرة تطورا ملحوظا في هذا المجال، وان الهدف من هذا البحث هو العمل على إخفاء البيانات النصية بشكل سري داخل وسائط صوتية (wav)، كما تم العمل على الإخفاء داخل القناة الصوتية في الأطر الفيديوية، وذلك من خلال الوصول إلى القنوات الصوتية لكل إطار من اطر الفيديو وتضمين البيانات بداخلها.

عند الإخفاء في القناة الصوتية لمقطع فيديو من نوع (Avi) فإن كل إطار من اطر الفيديو له قناة صوتية تابعة له ويمكن الإخفاء في أي واحدة من القنوات الصوتية لكل إطار من اطر

الفيديو، وبذلك فإنه من الصعب جدا اكتشاف مواقع الإخفاء فيها ونظراً للسعة الخزنية العالية للفيديو فانه من الممكن إخفاء كمية كبيرة جدا من المعلومات دون حدوث تغيير واضح في الفيديو، حيث كانت نتائج الإخفاء في القناة الصوتية من الفيديو الرقمي متوافقة تماما مع هدف البحث.

المقدمة

الإخفاء هو علم من أمن المعلومات، يستطيع طرفان من خلاله تبادل معلومات مهمة وسرية دون علم الطرف الثالث (الخصم) بهما [2][3]، هذا المفهوم تم استخدامه وتطبيقه منذ مئات السنين، فعند ظهور نهضة الحاسبات والتكنولوجيا دخل فن الإخفاء إلى عصر جديد يمكن أن يطلق عليه بالعصر الرقمي، وفي يومنا هذا تشهد صناعة أجهزة الحاسوب تطورات كبيرة من حيث لغات البرمجة والبرامج التطبيقية وغيرها، كما أن استخدام أجهزة الحاسوب دخل في عدة مجالات منها التجارية والمصرفية وغيرها من المجالات، كل هذه المجالات تحتاج إلى حماية بياناتها من التجسس والتطفل وهذا أدى إلى ضرورة استخدام تقنيات الإخفاء[3][4]، حيث أنه في الوقت الحاضر قد ازدادت أهميتها في إخفاء البيانات في نص (Text) أو وسط رقمي (Digital Media) مثل صورة (Image) أو صوت (Audio) وذلك لان الدول والحكومات بدأت تفقد السيطرة على الرسائل المشفرة المتبادلة بين المؤسسات والشركات واحتمال احتواء هذه النصوص المشفرة على معلومات قد تكون مخلة بالأمن والمصلحة العامة، لذلك لجأت بعض الحكومات لمنع استخدام التشفير في الاتصالات لمستخدمي الشبكات للأغراض الشخصية.[3][9][10]

من هنا برزت الحاجة الملحة لإيجاد تقنيات جديدة بديلة عن التشفير لتجاوز نقاط الضعف هذه، فنشأت تقنيات إخفاء المعلومات (والتي تقوم على مبدأ مغاير لفكرة التشفير وهو أن الرسالة المرسلة تكون غير مرئية لأي شخص بواسطة إخفاءها داخل إحدى وسائل الاتصال (الصوت , الصورة والنص, الفيديو))، حيث يتم طمر المعلومات (Information Embedding) داخل وسائط أخرى حاملة لها وجعلها غير مدركة (Imperceptible) من قبل المتطفلين والمهاجمين وهكذا تكون المعلومات مشاعة لمستخدمي الشبكة، بينما يبقى محتواها حكرا على الجهات ذات العلاقة التي لوحدها تعرف كيفية استخراج محتواها، ومن المواضيع الفرعية المهمة لإخفاء المعلومات هو الكتابة المخفية (Steganography)، فعندما تكون الغاية من التشفير هو حماية محتوى الرسالة فأن الكتابة المخفية هي لإخفاء وجود الرسالة.[2][3]

إن الغاية من إخفاء المعلومات ليست منع الآخرين من معرفة المعلومات المخفية، بل لإزالة الشك أصلا في وجود معلومات مخفية، والشيء المميز في تقنيات إخفاء المعلومات أنها

تواكب التقنيات الحديثة، ويمكن استخدامها في جميع الوسائط الحاسوبية من صور، نصوص، صوت، فيديو وحزم الشبكة.[3][4]

لقد حاول الباحثون إيجاد تقنيات إخفاء متطورة تواكب التطور السريع في تقنيات الإخفاء، ففي عام 2002 قدم الباحث Ahsan بحثاً تضمن تقنيتين لتصميم القنوات المخفية، الأولى هي إخفاء البيانات في ترويسة البروتوكولات IP و TCP، والثانية هي إعادة ترتيب حزم الشبكة باستخدام بروتوكول IPSec.[6]

وفي عام 2003 قدم الباحثان Selvaraj و Balasubramaniam بحثا لدمج تقنيات الإخفاء مع تقنيات الذكاء الاصطناعي لإخفاء بيانات سرية في صورة، فاستخدما شبكة عصبية من نوع (Backpropagation) يكون مدخلها الصورة والرسالة المراد إخفاؤها، وبذلك يتم إخفاء الرسالة السرية بصورة غير مباشرة في بيانات الصورة اعتمادا على مخرج الشبكة الذي يحشر في الخلية الثنائية الأقل أهمية لبيانات الصورة. [14]

وفي عام 2006 قدم الباحثون Zander وSebastian و Armitage بحثاً للإخفاء في بروتوكولات TCP/IP وذلك بالاستفادة من الخلايا الثنائية غير المستخدمة في ترويسة البروتوكول IP في الحقل TOS، والخلايا الثنائية محجوزة في بروتوكول النقل TCP في حقل محجوز (reversed)، فتمكنا من إرسال حرف واحد في كل حزمة شبكة. [18]

وفي عام 2010 قدم الباحثون Kekre و Athawale و Rao و Athawale بحثا تم فيه عملية إخفاء البيانات داخل إشارة الصوت حيث تم استخدام خوارزمية LSB وذلك من خلال عمل XOR بين البيانات المدخلة وإشارة الصوت. [12]

وفي عام 2011 قدم كل من Venkateswaran و Director بحثا تم فيه عملية إخفاء نص داخل إشارة صوتية وذلك من خلال تشفير النص باستخدام تقنية E-Cipher ثم تضمين البيانات المشفرة داخل الإشارة الصوتية. [16]

وفي عام 2011 أيضا قدمت إيمان بحثا تم فيه إخفاء نص في ملف الصوت WAV وذلك من خلال تطبيق نظام التغطية داخل ملف الصوت والطريقة هي تغيير الخلية الثنائية الأقل أهمية [1].

1-الهدف من البحث

إن الهدف من هذا البحث هو العمل على إخفاء البيانات النصية بشكل سري داخل وسائط صوتية (Audio)، حيث تم استخدام الملفات الصوتية من نوع wav، كما تم العمل على الإخفاء داخل القناة الصوتية في الفيديو الرقمي، حيث تم العمل على محورين:

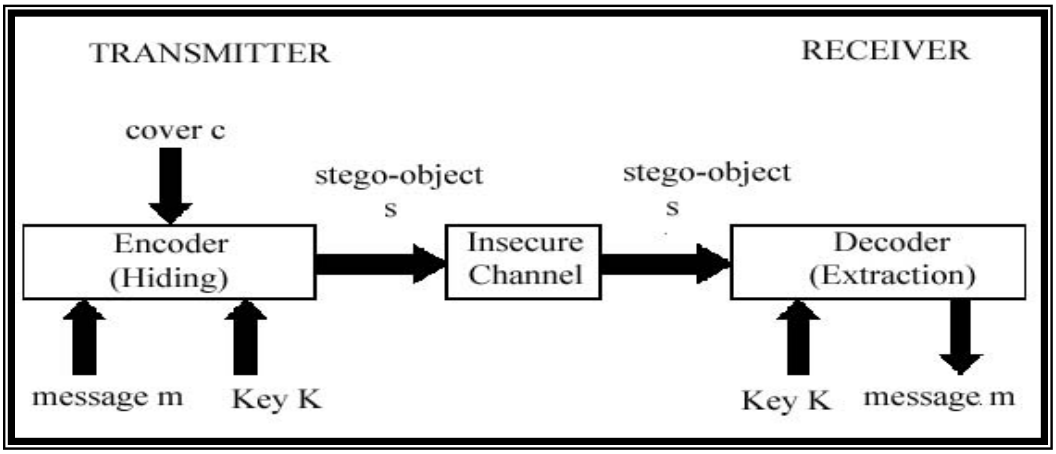
المحور الأول: بعد أن يتم قراءة النص المراد إخفاءه (من ملف txt) يتم تحويله إلى الصيغة الثنائية ثم تشفير البيانات باستخدام تقنية XOR (وعن طريق مفتاح سري) ثم إخفاء البيانات المشفرة في البت الأقل أهمية من الملف الصوتي (الغطاء)، بعدها تم العمل على الإخفاء في البتان 2) (Bits الأقل أهمية وكانت النتيجة متوافقة، وهكذا إلى أن تم الإخفاء في الخمسة بتات الأقل أهمية دون تأثير ملموس على الغطاء (الملفات الصوتية والفيديوية) وكانت النتائج متوافقة مع هدف البحث.

المحور الثاني: تم تطوير العمل وذلك من خلال الوصول إلى القنوات الصوتية داخل الملفات الفيديوية الرقمية من نوع AVI (حيث أن الصوت الخاص بملف الفيديو (AVI) مكون من قناتين صوتيتين (stereo))، حيث تم الوصول إلى المقاطع الصوتية الخاصة بكل إطار (Frame) من ملف الفيديو الرقمي وتضمين البيانات بداخلها.

ذلك أنه عند الإخفاء في القناة الصوتية لمقطع فيديو من نوع (Avi) فإن كل إطار من اطر الفيديو له قناة صوتية تابعة له ويمكن الإخفاء في أي واحدة من القنوات الصوتية لكل إطار من اطر الفيديو، وبذلك فإنه من الصعب جدا اكتشاف مواقع الإخفاء فيها ونظراً للسعة الخزنية العالية للفيديو فانه من الممكن إخفاء كمية كبيرة جدا من المعلومات دون حدوث تغيير واضح في الفيديو، حيث كانت نتائج الإخفاء في القناة الصوتية من الفيديو الرقمي متوافقة تماما مع هدف البحث.

2-نظام التغطية:

يمكن تعريف نظام التغطية على انه فن وعلم إخفاء المعلومات باستخدام ملف حامل لها (Host) بهدف منع أي متطفل خارجي من الشك بوجود رسالة مخفية داخل الملف الحامل، وهي وسيلة من وسائل الاتصال السري بأسلوب يخفي وجود الاتصال، والشكل (1) يمثل النموذج العام لنظام التغطية.[2][4][5]

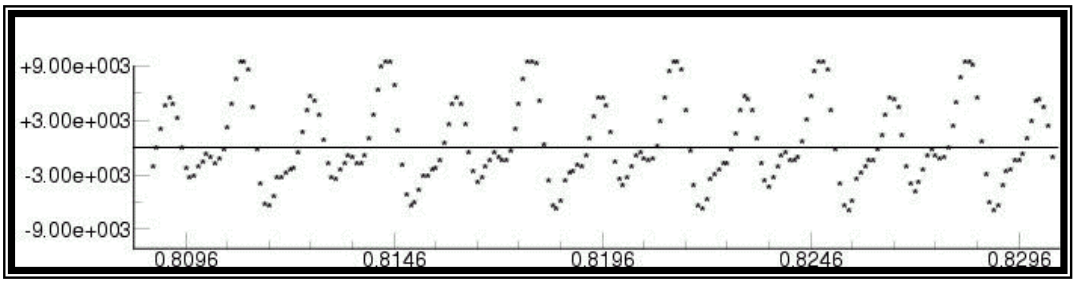


الشكل(1): المخطط العام لنظام التغطية

ويمكن تعريف الإخفاء على انه علم الاتصال بطريقة تخفي وجود الرسالة ولا تسمح لأي متطفل باكتشاف وجود رسالة ثانية داخل الرسالة الحالية، إذ لا يتغير شكل الرسالة الحاملة، ذلك أن علم الإخفاء يهتم بسرية محتويات الرسالة إضافة إلى تحقيق سرية الاتصال، وعندما يشك المتطفل بوجود معلومات مخفية فانه يحاول أن يفك أو يدمر أو يغير الرسالة، ثم يرسلها إلى المستلم الذي يعلم كيف يفسرها، واحتمالية معرفة الشخص غير المعني بوجود معلومات والقدرة على تفسير الرسالة احتمالية ضعيفة.[4][7][8]

3- الإخفاء في الملفات الصوتية (Hiding in Sound File):

يتكون الصوت من موجات مضغوطة تتحرك خلال وسط قابل للانضغاط، وتعتمد دقة الصوت على المادة التي ينتقل من خلالها، وفي يومنا هذا ظهرت العديد من تطبيقات الصوت الرقمي في الحاسبات وشبكات الاتصالات، لذا كان من الضروري تحويل الإشارة التناظرية إلى إشارة رقمية، والإشارة الرقمية تتكون من سلسلة من الأرقام (Digital) أي أن المعلومات داخل الإشارة تكون بشكل رقمي[3][13]، والشكل (2) يوضح الإشارة الرقمية، والسبب في استخدام الإشارة الرقمية هو لغرض معالجة البيانات باستخدام أجهزة الحاسوب وذلك لاختزال الضوضاء أثناء النقل خلال شبكات الاتصال.



الشكل (2) الاشارة الرقمية

إن عملية إخفاء البيانات في إشارة الصوت يعد تحديا خاصا لان نظام السماعية البشري HAS(Human Auditory System) يعمل بشكل ديناميكي واسع المدى من الترددات التي تقع بين (20Hz–20000Hz) , لذا فان هذا النظام يكون حساس جدا لإضافة ضوضاء عشوائية. [10]ومع ذلك فان هناك بعض الفجوات التي يمكن استغلالها في عملية الإخفاء وهي أنه ذو مدى تمايزي محدود وصغير ونتيجة لذلك فان الأصوات العالية تحجب الأصوات الواطئة أو الهادئة. يتم تمثيل كل عينة صوتية ببايت واحد (1 Byte/sample) والشائع هو عملية الإخفاء في البت الأول من اليمين من كل بايت إذ يعتبر هذا البت ذا تأثير محدود جدا، ويكاد يكون التبديل فيه غير مسموع من قبل الأذن البشرية.[12][17]

إن تكميم العينة هو عدد ألبايتات (Bytes) المستخدمة في تمثيل العينة الصوتية وهو من العوامل المهمة جدا في المحافظة على دقة الصوت عند تحويله إلى الصيغة الرقمية، فكلما زاد عدد البايتات المستخدمة في التمثيل كانت مواصفات الصوت قريبة جدا من القيمة الحقيقية للعينات الصوتية، وهنالك نوعان قياسيان للتكميم: النوع الأول يستخدم بايت واحد (1Byte) لتمثيل العينة الصوتية (8 bit/sample)، أما النوع الثاني فيستخدم بايتين (16bit/sample).[12][17]

4-الإخفاء في الملفات الفيديوية من نوع (Avi):

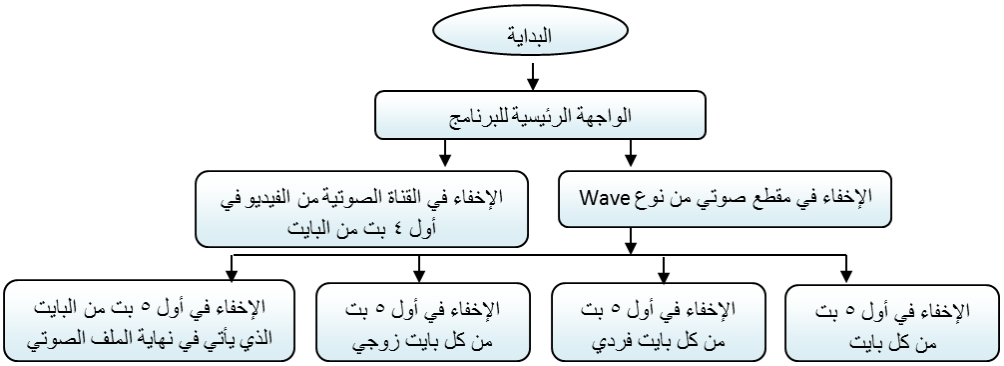
إن الـ Avi هو اختصار لتداخل الفيديو والصوت "Audio/Video Interleaved" وهو حالة خاصة من الـ "RIFF:Resource Interchange File Format" المعرفة من قبل شركة (Microsoft) ويعد الصيغة الأكثر شيوعا لبيانات الفيديو والصوت العاملة على أجهزة الحاسوب الشخصية.[13] إن صيغة ملف الـ Avi هي تمثيل لملف الـ RIFF التي تستخدم مع التطبيقات التي تقوم بعمليات الالتقاط "Capture" التحرير "Edit" التشغيل "Playback" لتتابع الفيديو والصوت "Sequence".[17]

بصورة عامة فان الملفات ذات الامتداد (Avi) تحتوي على العديد من التيارات ولأنواع مختلفة من البيانات، ذلك أن ملف الـ Avi يتألف من تتابع مجموعة من الأطر (Frames)

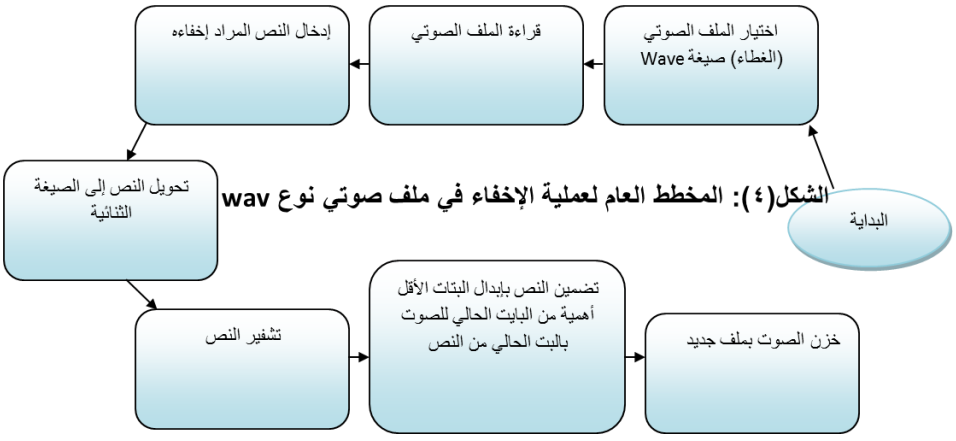
حيث أن كل إطار هو عبارة عن صورة يرتبط بها جزء يكون خاص بها من القناة الصوتية للفيديو، لكن اغلب تتابعات الـ AVI تستخدم تيارات الفيديو والصوت ومن الممكن أن تستخدم تيارات فيديو فقط وبدون الحاجة لتيار صوت [15][17].

6-المخطط العام للبحث:

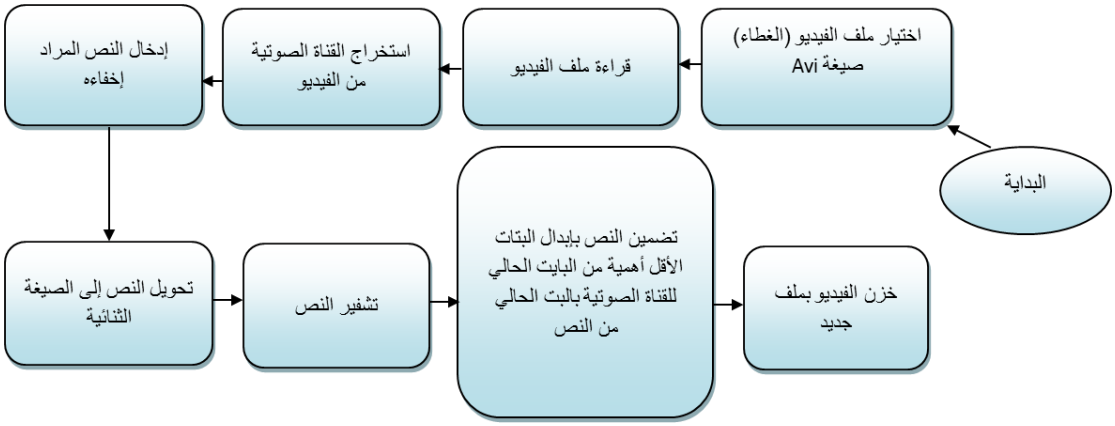
تم اعتماد خطوات متتابعة لغرض تنفيذ عملية الإخفاء، وذلك بتحديد الملف الصوتي (الغطاء) والنص المراد إخفاؤه ثم يتم تشفير النص، بعد ذلك يتم تضمين النص المشفر بإبدال البتات الأقل أهمية من بايتات الصوت، وبعد الانتهاء من عملية التضمين يتم خزن المقطع الصوتي (الغطاء) بملف جديد، ثم تم العمل أيضا على تضمين وإخفاء النص المشفر في القنوات الصوتية في الملفات الفيديوية، ويمكن تمثيل المراحل التي سوف تعتمد في الخوارزمية في الأشكال (3) (4) (5).



الشكل(3): المخطط العام للبحث



الشكل(٤): المخطط العام لعملية الإخفاء في ملف صوتي نوع wav



الشكل(5): المخطط العام لعملية الإخفاء في القناة الصوتية لملف فيديو نوع AVI

6-1 خوارزمية الإخفاء في الملف الصوتي من نوع Wave:

تتضمن عملية الإخفاء في الملف الصوتي من نوع Wave مجموعة من الخطوات، والتي من خلالها لا يمكن التمييز بين الملف الصوتي قبل وبعد عملية الإخفاء، كما في الشكل(6)، والخطوات الآتية توضح عمل الخوارزمية:

1- اختيار الملف الصوتي (الغطاء) صيغة Wave.
2- قراءة الملف الصوتي وخزنه في المصفوفة w والتي تمثل البايتات الصوتية.
3- تحويل قيم موجة الصوت من (1،1−) إلى (255،0) لكي لا يحصل ضياع فيها عند التضمين.
4- قراءة النص المراد إخفاءه وخزنه في مصفوفة ولتكن (a).
5- تحويل النص إلى الصيغة الثنائية.
6- تشفير النص باستخدام (Xor)، ومن ثم خزنه في مصفوفة ولتكن (t).
7- خزن عدد أحرف النص في البايت الأول من الصوت ((w(1)) ليتم الاستفادة منه في عملية الاسترجاع.
8- إعطاء قيمة k=1 ليمثل العداد للمصفوفة t.
9- لكل i=2:length(w) نفذ الخطوات التالية.
10- وضع العداد m=1:5 ليمثل موقع البت المراد استبداله في عملية التضمين.
11- إذا كان k اقل من أو يساوي طول النص length(t) نفذ الخطوات التالية وإذا كان اكبر من طول النص اذهب إلى الخطوة 13.
12- استبدال البت الحالي من الصوت w(i) بالبت الحالي من النص t(k) والذي يشير إليه العداد m باستخدام الإيعاز bitset، k=k+1.

13- إرجاع قيم الصوت الأصلية بين (1،1−).

14- خزن الصوت بملف جديد.

6-2 خوارزمية الاسترجاع من الملف الصوتي من نوع Wave

1- اختيار الملف الصوتي الحاوي على النص المخفي.

2- قراءة الملف الصوتي وخزنه في المصفوفة wr والتي تمثل البايتات الصوتية.

3- تحويل قيم موجة الصوت من (1،1−) إلى (255،0).

4- اخذ قيمة البايت الأول الذي يحتوي على عدد أحرف النص المضمن وخزنها في المتغير n.

5- إعطاء k=1 ليمثل العداد للمصفوفة w2 التي سيتم فيها خزن البتات المخفية.

6- لكل i=2:n*8 حيث أن i يمثل العداد للمصفوفة wr و n هو عدد أحرف النص مضروباً في 8 لان كل بايت متكون من 8 بت، نفذ الخطوات التالية.

7- وضع m=1:5 ليمثل موقع البت من البايت الصوتي.

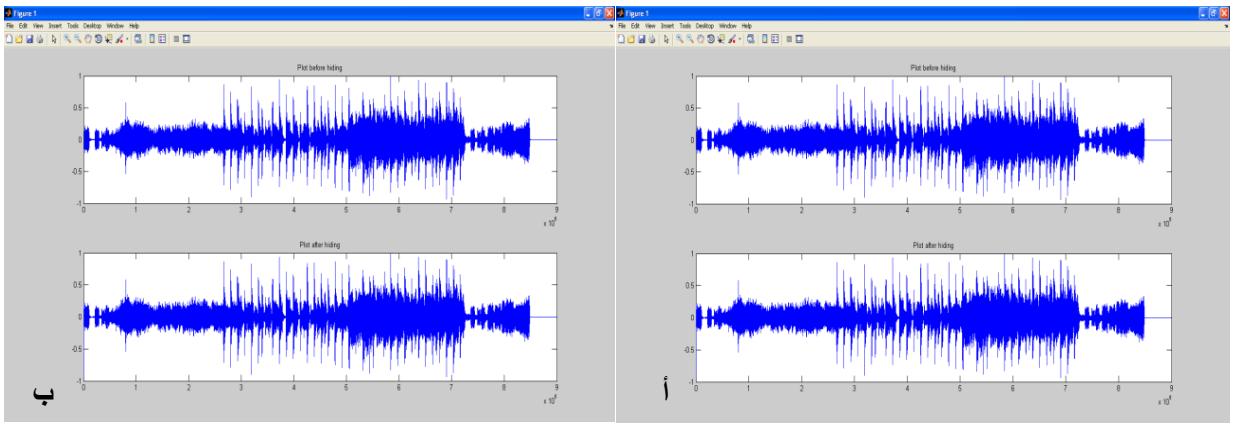
8- استرجاع البت الذي يشير إليه العداد m والذي يحتوي على بتات النص المضمنة داخله باستخدام الإيعاز bitget.

9- k=k+1.

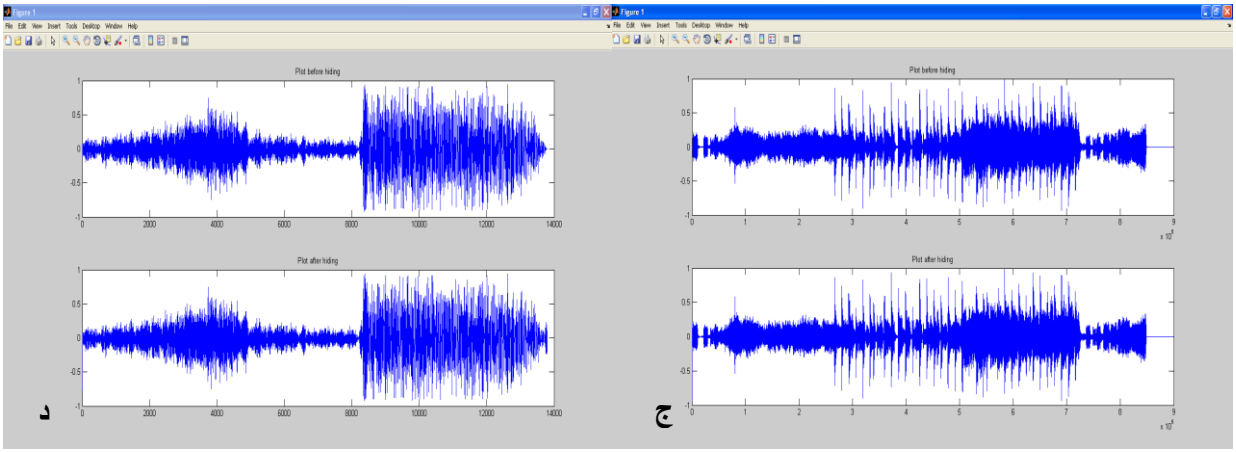
10- إذا كان i < n*8 أي أن النص لم ينتهي اذهب إلى الخطوة 7، وإذا كان i=n*8 اذهب إلى الخطوة التالية.

11- فك تشفير النص باستخدام (Xor) مع نفس العدد الذي استخدمناه في عملية التشفير وخزنه في المصفوفة t.

12- تحويل النص من الصيغة الثنائية إلى قيمه الأصلية ثم خزنه النص بملف نصي جديد.



ب أ



الشكل(6): أ- شكل الموجة للصوت قبل وبعد الإخفاء في أول خمسة بتات من البايت ب- شكل الموجة للصوت قبل وبعد الإخفاء في أول خمسة بتات من البايت الفردي ج- شكل الموجة للصوت قبل وبعد الإخفاء في أول خمسة بتات من البايت الزوجي د- شكل الموجة للصوت قبل وبعد الإخفاء في البايتات التي تأتي في نهاية الملف الصوتي

3-6 خوارزمية الإخفاء في القناة الصوتية من الفيديو الرقمي:

تتضمن عملية الإخفاء في القناة الصوتية من الفيديو الرقمي مجموعة من الخطوات، والتي من خلالها لا يمكن التمييز بين القناة الصوتية قبل وبعد عملية الإخفاء، كما في الشكل (7)، والخطوات الآتية توضح عمل الخوارزمية:

1- اختيار ملف الفيديو (الغطاء) صيغة Avi.

2- قراءة ملف الفيديو.

3- إدخال النص المراد إخفاءه، ثم تحويل النص إلى الصيغة الثنائية وخزنه في المصفوفة (t).

4- تشفير النص باستخدام (Xor) مع العدد المدخل.

5- حساب عدد الأطر (Frames) للفيديو.

6- اخذ قيمة المؤشر للإطار (Frame) الوسطية وخزنه في المتغير (midframe) أي أن (Midframe=noframes/2-5).

7- إنشاء سجل (Structure) وليكن s يتكون من حقلين حقل يضم جزء الأطر (Frames) للفيديو وليكن b أما الحقل الثاني يضم القناة الصوتية للفيديو وليكن a.

8- لكل i = 1 : noframes نفذ الخطوات التالية.

9- استخراج القناة الصوتية من الفيديو التابعة للإطار الحالي Frame(i) وخزنها في s(i).a أما الإطار Frame(i) فيتم خزنه في s(i).b.

10- إذا كان i اكبر أو يساوي الإطار الوسطي (midframe)، نفذ الخطوات التالية وإذا لم يحقق الشرط عد إلى الخطوة 9.

11-خزن عدد أحرف النص L في البايت الأول من القناة الصوتية للإطار Frame(i) وذلك للاستفادة منه في عملية الاسترجاع.

12- وضع k=1 ليمثل العداد لمصفوفة النص t.

13- وضع h=1 ليمثل العداد للمصفوفة b والتي ستمثل مخزن وسطي للبايتات الصوتية عند تحويل قيمها إلى (uint8) لكي يتم التعامل مع البايت الصوتي بـ (8 bits) عند الإخفاء.

14- إعطاء j = 2 : L*2+1 ليمثل العداد للبايتات الصوتية المخزونة في الحقل a من السجل (s)، وينتهي العداد بالقيمة (L*2+1)، لكي يتم الإخفاء في أول 4 بت من البايت الصوتي، حيث أن كل حرف يحتاج لـ 2 بايت وبذلك تم تحديد العداد بالقيمة L*2 حيث L تمثل عدد أحرف النص.

15- إعطاء m = 1 : 4 ليمثل موقع البت المراد استبداله بالبتات التابعة للنص.

16- استبدال البت الحالي من الصوت b(h) بالبت الحالي من النص t(k) والذي يشير إليه العداد m باستعمال الإيعاز bitset، k=k+1، h=h+1.

17- تجميع البيانات الناتجة ثم خزن الفيديو بملف جديد.

6-4 خوارزمية الاسترجاع من القناة الصوتية من الفيديو:

1- اختيار ملف الفيديو الحاوي على النص، ثم قراءته.

2- حساب عدد الأطر (Frames) للفيديو وخزنه في المتغير noframes.

3- اخذ قيمة المؤشر للإطار الوسطي وخزنه في المتغير (midframe) أي أن midframe=noframes/2-5.

4- إنشاء سجل Structure وليكن s يتكون من حقلين حقل يضم جزء الأطر (Frames) للفيديو وليكن b أما الحقل الثاني فيضم القناة الصوتية للفيديو وليكن a.

5- لكل i=1:noframes نفذ الخطوات التالية.

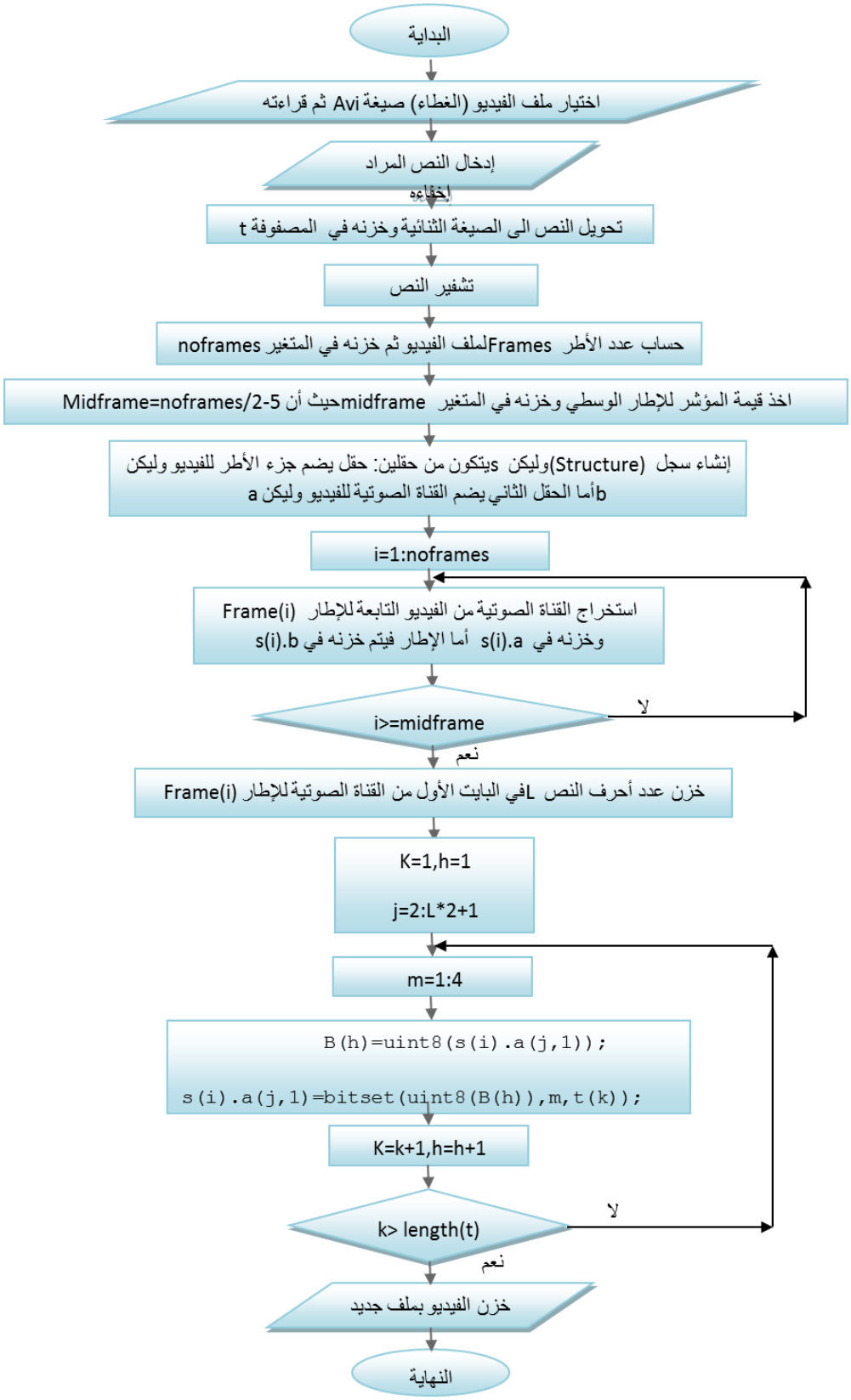
6- استخراج القناة الصوتية من الفيديو التابعة للإطار Frame(i) وخزنها في s(i).a أما الإطار Frame(i) يتم خزنه في s(i).b.

7- اخذ عدد أحرف النص L ووضعها في البايت الأول من القناة الصوتية للإطار Frame(i).

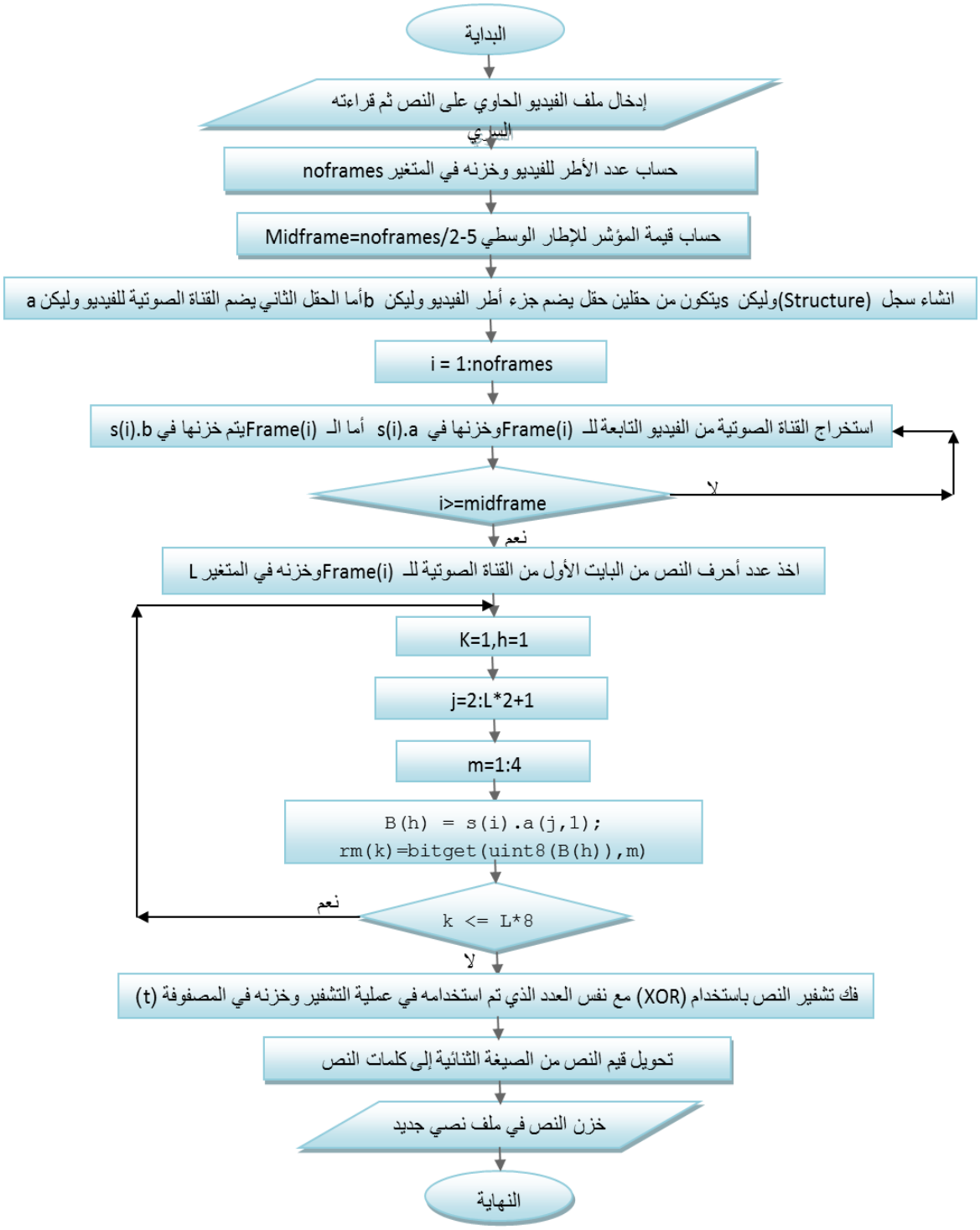
8- وضع k=1 ليمثل العداد للمصفوفة rm والتي سوف يتم فيها استرجاع النص، أي العداد لبتات النص.

9- وضع h=1 ليمثل العداد للمصفوفة b والتي ستمثل مخزن وسطي للبايتات الصوتية.

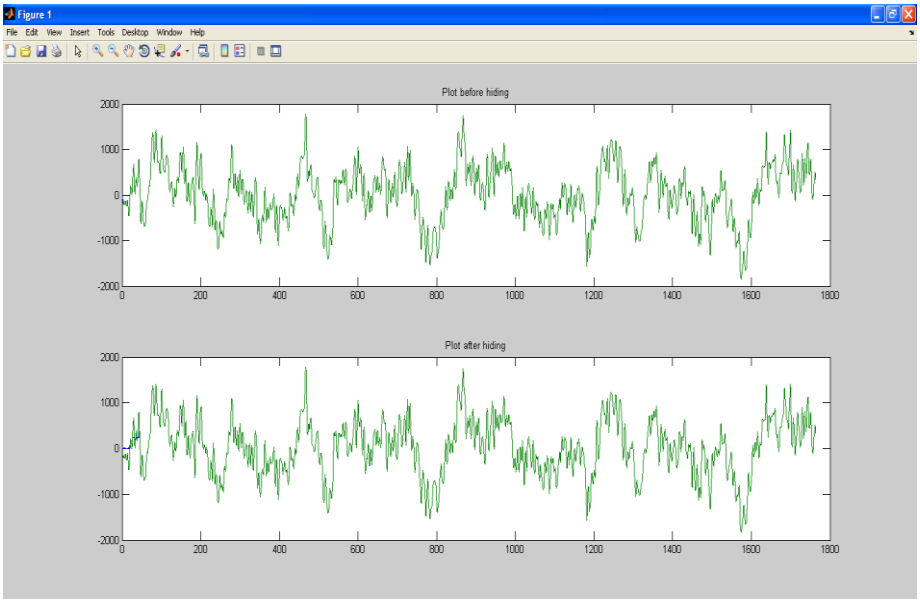
10- وضع j=2:L*2+1 ليمثل العداد للبايتات الصوتية المخزونة في الحقل a من السجل (s)، وينتهي العداد بالقيمة (L*2+1).
11- استرجاع البت الذي يشير إليه العداد m والذي يحتوي على بتات النص المضمنة داخله.
12- إذا كان k أكبر من L*8 اذهب إلى الخطوات التالية.
13- فك تشفير النص باستخدام (Xor) مع نفس العدد الذي تم استخدامه في عملية التشفير وخزنه في المصفوفة t.
14- تحويل النص من الصيغة الثنائية إلى قيمه الأصلية.
15- خزن النص بملف نصي جديد.



المخطط الانسيابي(1): خوارزمية الإخفاء في القناة الصوتية من الفيديو الرقمي



المخطط الانسيابي(2): خوارزمية الاسترجاع من القناة الصوتية من الفيديو



الشكل (7): شكل الموجة للقناة الصوتية للفيديو قبل وبعد الإخفاء

7-الاختبارات الإحصائية:

بعد أن تم تطبيق جميع الخوارزميات والحصول على نتائجها، تم تقييم طرق الإخفاء بوساطة الاختبارات الإحصائية، حيث انه في الاختبارات الإحصائية تستخدم طرق رياضية، وتوجد عدة أنواع من الاختبارات الإحصائية أهمها: [1]

1- إيجاد اقل قيمة لمربع الخطأ (Minimum Squared Error) بين إشارة الإدخال والإخراج كما موضح في المعادلة (1).

$$MSE = (\sum_{MN}[I_i(m,n)-I_{21}(m,n)]^2) / (M*N) \quad \text{..... (1)}$$

حيث تمثل M و N عدد الأعمدة والأسطر للإشارة، وتمثل $I_i(m,n)$ و $I_{21}(m,n)$ إشارة الإدخال والإخراج.

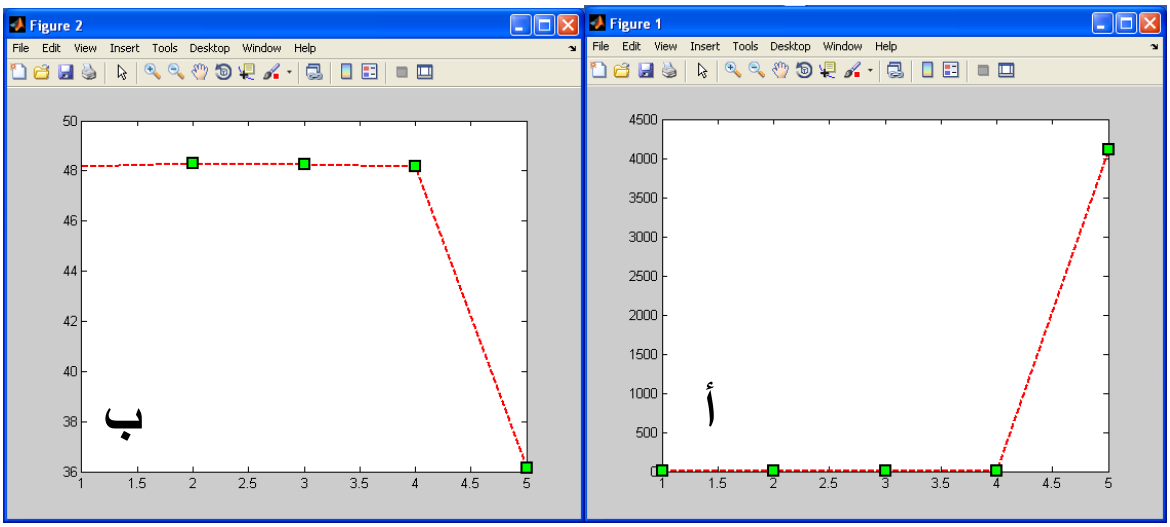
2- قياس نسبة الضوضاء (Peak Signal-to-noise ratio)

$$PSNR = 10\log_{10}[R^2/MSE] \quad \text{.....(2)}$$

حيث تمثل R^2 قيم البيانات إذا كانت Floating Point أو Unsigned integer. [1]

جدول (1): يمثل قيم الاختبارات الإحصائية

Algorithm	SNR	MSE	PSNR
Hide in 5 Bits (WAV)	63.7638 +31.4159i	1.5275e-005	48.1602
Hide in odd Bytes (WAV)	63.7690 +31.4159i	1.4834e-005	48.2873
Hide in even Bytes (WAV)	63.6736 +31.4159i	1.4974e-005	48.2466
Hide in end Bytes (WAV)	63.8276 +31.4159i	1.5188e-005	48.1851
Hide in sound of video (AVI)	36.9383	4.1070e+003	36.1353



الشكل (8): الاختبارات الإحصائية

أ- قياس الحد الأدنى لمربع الخطأ MSE ب- قياس نسبة الضوضاء PSNR

بعد تطبيق المعادلة (1) والمعادلة (2) على عينات صوتية وفيديوية وباستخدام جميع الخوارزميات لإيجاد الحد الأدنى لمربع الخطأ (MSE) وإيجاد نسبة الضوضاء (PSNR) كما موضح في الشكل(8)، يتبين أن نسبة الخطأ كانت متقاربة بالنسبة لجميع خوارزميات الإخفاء المطبقة في البحث (علما انه تم حساب نسبة الخطأ ونسبة الضوضاء بالاعتماد على القناة الصوتية لملف الفيديو)، وبذلك تكون النتائج متوافقة مع أهداف البحث.

8-الاستنتاجات :

من خلال ما تقدم يمكن القول بان العمل مع القنوات الصوتية (وخاصة ضمن ملفات الفيديو الرقمي) أكثر صعوبة من التعامل مع بقية أجزاء الوسائط المتعددة لما يحتويه من ترددات غير محسوسة، ومن خلال التطبيق العملي تم التوصل إلى ما يلي:

1. عند استخدام المقطع الصوتي من نوع (Wave) في الإخفاء ذو التردد الواقع بين [1,1-] فيجب تحويل القيم إلى قيم ذات مدى أعلى عند إبدال تلك القيم بأحرف النص المراد إخفاءه لكي لا يحدث ضياع كبير في قيم الصوت، فقد تم إخفاء أحرف النص بعد تحويلها إلى النظام الثنائي وتم تجربة إخفاء أكثر من 250 حرف دون أن يحدث تأثير واضح في الصوت.
2. عند الإخفاء في القناة الصوتية لمقطع فيديو من نوع (Avi) فإن كل إطار من اطر الفيديو له قناة صوتية تابعة له ويمكن الإخفاء في أي واحدة من القنوات الصوتية لكل إطار من اطر الفيديو، وبذلك فإنه من الصعب جدا اكتشاف مواقع الإخفاء فيها ونظراً للسعة الخزنية العالية للفيديو فانه من الممكن إخفاء كمية كبيرة جدا من المعلومات دون حدوث تغيير واضح في الفيديو، حيث كانت نتائج الإخفاء في القناة الصوتية من الفيديو الرقمي متوافقة تماما مع هدف البحث.
3. إن الخوارزميات المستخدمة في البحث كانت متوافقة مع الأهداف المطلوبة من البحث، وان استخدام خوارزميات التشفير كانت متوافقة مع ما يحتاج اليه البحث من سرية.
4. عند الإخفاء في القناة الصوتية لمقطع فيديو من نوع (Avi) فإن كل إطار من اطر الفيديو له قناة صوتية تابعة له ويمكن الإخفاء في أي واحدة من القنوات الصوتية لكل إطار من اطر الفيديو، وبذلك فإنه من الصعب جدا اكتشاف مواقع الإخفاء فيها ونظراً للسعة الخزنية العالية للفيديو فانه من الممكن إخفاء كمية كبيرة جدا من المعلومات دون حدوث تغيير واضح في الفيديو، حيث كانت نتائج الإخفاء في القناة الصوتية من الفيديو الرقمي متوافقة تماما مع هدف البحث.

9-التوصيات:

1. يمكن استخدام خوارزميات أخرى أكثر كفاءة في عمليات الإخفاء (مثل إجراء عملية التهجين بين الطرق التقليدية والطرق الذكائية).
2. يمكن استغلال المساحات الغير المستخدمة من ترويسة (Header) الملفات المستخدمة للإخفاء في داخلها.
3. يمكن استخدام ملفات فيديوية أخرى تكون ذات سعة خزنية اقل من الملفات المستخدمة في هذا العمل.
4. يمكن استخدام تقنيات أخرى للتشفير ذات كفاءة أعلى (مثل التقنيات المعتمدة على مجموعة من المفاتيح السرية العامة والخاصة).

المصادر

1- أحمد، إيمان فتحي، 2011، "إخفاء نص في ملف الصوت WAV"، مجلة التربية والعلم، المجلد (24) العدد (4)، قسم الحاسوب، كلية التربية، جامعة الموصل.

2- الحمامي، علاء حسين و الحمامي، محمد علاء (2008)، "إخفاء المعلومات: الكتابة المخفية والعلامة المائية "، إثراء للنشر والتوزيع، الشارقة، الإمارات.

3- سلو، اميرة بيبو، (2009)، "تقنيات إخفاء المعلومات باستخدام الشبكات العصبية وبروتوكولات الشبكة"، رسالة ماجستير غير منشورة، قسم علوم الحاسبات، كلية علوم الحاسوب والرياضيات، جامعة الموصل، العراق.

4- الصميدعي، عامر تحسين سهيل، 2002، "تطبيق نظام التغطية" ، بحث ماجستير، قسم علوم الحاسوب، كلية علوم الحاسوب والرضيات، جامعة الموصل، العراق.

5- Abed F. Salman, Mustafa Nada Abdul Aziz, 2010, "A proposed Technique for Information Hiding Based on DCT", International Journal of Advancements in Computing Technology Volume 2, Number 5, *E-Mail: Fad1234567826@Yahoo.com*

6- Ahsan, Kamran (2002), "Covert channel analysis and data hiding in TCP/IP", Unpublished M. Sc. Thesis, University of Toronto, Canada.

7- Alrouh B., Adel A., Gheorghita G., 2011, " Information Hiding in SOAP Messages: A Steganographic Method for Web Services", International Journal for Information Security Research (IJISR), Volume 1, Issue 1, bachar.alrouh@brunel.ac.uk

8- Hui-fen Huang, 2011, "Swift LSB Information Hiding Algorithm to RS Attacks", Journal of Convergence Information Technology(JCIT) Volume6, Number10, *Shan Dong YingCai University, E-MAIL:shouyu1976@163.com*.

9- Jalil Zunera, 2010, "Copyright Protection of Plain Text using Digital Watermarking", A thesis submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy to the FAST National University of Computer and Emerging Sciences, Islamabad, Pakistan.
10- Jayaram P, Ranganatha H R, Anupama H S, 2011, "INFORMATION HIDING USING AUDIO STEGANOGRAPHY–A SURVEY", The International Journal of Multimedia & Its Applications (IJMA) Vol.3, No.3, Bangalore, INDIA.
11- Kekre H. B., Athawale A., Rao S., Athawale U., 2010, "Information Hiding in Audio Signals", International Journal of Computer Applications (0975 – 8887),Volume 7– No.9.
12- Le T. Van, 1999, "COVERT CRYPTOGRAPHY", A Thesis Submitted in Partial Fulfillment of the Requirements for the degree of Master of Science in Computer Science, The University of Wisconsin_Milwaukee.
13- Peter Bayer, 2002, "Information Hiding – Steganographic Content in Streaming Media", Master Thesis, software Engineering, Bleking Institute of technology, Ronneby, Sweden.
14- Selvaraj, J. and Balasubramaniam, R., (2003), "Neural Network Based Camouflaging in Still Image", University of Tamilnadu, India, selvarajjayapal@yahoo.com.
15- Tadiparthi G. Reddy, Sueyoshi Toshiyuki, 2006, "StegAnim-A Novel Information Hiding Technique using Animations", Advance online publication.
16- Venkateswaran R., Director V. S., 2011, "Implementation of ISS - IHAS (Information Security System – Information Hiding in Audio Signal) model with reference to proposed e-cipher Method", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No. 6.
17- Wu M., 2001, "MULTIMEDIA DATA HIDING", a dissertation presented to the faculty of princeton university in candidacy for the degree of doctor of philosophy.
18- Zander, Sebastian , Armitage, Grenville and Branch, Philip (2006), "Covert Channels in the IP Time To Live Field", Swinburne University of Technology Australia.