Hiding Techniques using Mp3

Shyma Sh. Mohammed shymshak@uomosul.edu.iq
Ahmed S. Nori ahmed.s.nori@uomosul.edu.iq
College of Computer Science and Mathematics
University of Mosul

Received on: 19/9/2010 **Accepted on: 10/11/2010**

ABSTRACT

In last years, Steganography techniques involving audio file formats appear to be increasing in popularity. This may be attributed to the fact that current steganalysis tools available to the general public fall short when applied to audio files. Another factor that may be contributing to the increasing popularity is the widespread popularity of the MP3 file format and its ubiquitous presence on the Internet.

In this paper, an introductory look at steganography and the important methods for hiding data in audio is shown, as well as the strengths and weaknesses of each method. An overview about sound and their file formats especially MP3 file format and its attribute and features.

Here, some steganography techniques on sound (Low Bit Encoding, Phase Coding) has been used to apply them on MP3 file format which had been chosen as a cover for data transmission.

Keywords- Steganography, Steganalysis, MP3, Phase coding.

تقنيات الإخفاء باستخدام MP3

شيماء شكيب **أحمد سامي نوري**
كلية علوم الحاسبات والرياضيات
جامعة الموصل

الملخص

في السنوات الأخيرة ازدادت شعبية تقنيات نظام التغطية التي تستخدم ملف الصوت كغطاء لنقل المعلومات، وهذا يعود إلى حقيقة أن أدوات التحليل المتوفرة حالياً غير مناسبة للعمل مع ملفات الصوت، فضلاً عن الشعبية المتزايدة لبعض الملفات الصوتية وخاصة ملف MP3 الذي احتل حضوراً كبيراً على الانترنيت.

في هذا البحث تم إعطاء نظرة عامة عن نظام التغطية، وشرح أهم تقنيات الإخفاء داخل الصوت وعوامل القوة والضعف لها. مع إعطاء نظرة عامة عن الصوت واهم ملفاته وخاصة ملف MP3 وأهم خصائصه ومميزاته.

هنا، بعض تقنيات نظام التغطية (الإخفاء في الخلية الأقل أهمية، تبديل الطور) التي تم تطبيقها على ملف الصوت MP3 الذي تم اختياره كغطاء لعملية تراسل المعلومات.

الكلمات المفتاحية: التغطية، التحليل، MP3، تبديل الطور.

1. مدخل إلى نظام التغطية Steganography

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.

أما كلمة Steganography فيرجع اصلها إلى اللغة اليونانية ويتكون من المقطعين Steganos وتعني المغطاة Graphy أي الكتابة أو الرسم والمعنى الحرفي لها الكتابة المغطاة Covered Writing. [2][1]

هناك ثلاث طرائق مستخدمة لإجراء عملية التغطية هي:

- **التغطية النقية Pure Steganography**

يتم إجراء عملية الإخفاء دون الحاجة إلى استخدام أي مفتاح سري.

- **التغطية باستخدام المفتاح السري Secret _key Steganography**

يتم في هذا النوع اعتماد مفتاح سري متبادل بين الطرفين Stego_key.

- **التغطية باستخدام مفتاح عام Public_key Steganography**

تشبه مفهوم التشفير بالمفتاح العام، إذ يستخدم مفتاح عام Public key في الإخفاء ومفتاح خاص Private key لفك رموز الرسالة Decoding Process.[3]

2. إخفاء البيانات داخل الصوت Hiding data in Audio

يعد الإخفاء داخل ملف الصوت تحدياً كبيراً بسبب المدى الواسع لنظام السمع البشري (Human Audio System (HAS)، إذ أن الأذن البشرية لها قدرة إدراك الأصوات بنسبة عالية جدا مما يجعل هناك صعوبة بإضافة أو حذف بيانات من الملف الأصلي والتي يتم إدراكها مباشرة كضوضاء Noise، ولكن وجود بعض الفجوات في نظام السمع البشري والتي يمكن استغلالها، جعلت ذلك ممكنا مثلا أن الأذن البشرية لاتفرق بين نبرتي صوت مختلفتين والأصوات العالية تحجب الأصوات الواطئة. [4]

3. دراسات سابقة

- في العام (2000)، قدم العلماء Bender وزملائه مسحاً شاملاً لتقنيات الاخفاء موزعة حسب اماكن استخدامها. [1]
- اما في العام (2004)، استطاع العالم Cvejic من تقديم اكثر من خوارزمية للاخفاء في ملفات Audio ولكلا المجالين الاخفاء وحقوق الملكية.[2] وفي العام نفسه، تم عرض عدد اخر من التقنيات التي تتعامل مع الاخفاء وحقوق الملكية من قبل العلماء Cummins وآخرون. [3]
- اما الاعوام التي تلت ذلك، فقد شهدت ظهور الكثير من التعاملات مع انظمة الاخفاء وبالاخصِ Audio، حيث تمكن العلماء Yan وزملائه في العام (2008) من انتاج تقدم جديد في التعامل مع الاخفاء في Audio عن طريق تقنيتهم الجديدة. [4]

- وكان الاهتمام واضحاً بملف الصوت المميز ذو الامتداد MP3 ضمن اعمال العلماء Diqun وزملائه والذي قدم كخوارزمية جديدة للاخفاء في MP3 عام (2009).[5] وهذا ما حصل مع العالمين Yan و Wang في العام نفسه، حين تمكنا من تقديم عملهم كتقنية جديدة للتعامل مع الاخفاء ضمن ملفات الصوت MP3. [6]
- وجاء العام (2010)، الذي استطاع فيه العالم Al-Rababah من عرض فكرته للتعامل مع ملف الصوت MP3 والذي يعمل كجزء خاص من اجزاء الفيديو MPEG.[7]

4. الصوت ومفهوم MP3

1.4. الصوت: يمكن إعطاء تعريف مبسط للصوت على انه موجات ناتجة عن تغير في ضغط الهواء، وعلى الرغم من كون هذا التغير لا يتعدى (±1)، لكن عند ملامسته للأذن الداخلية فأنه يحرك طبلة الأذن ويُدرك كترددات صوتية مختلفة.[4]

2.4. طرائق خزن الصوت: يتم خزن الصوت داخل ملفات مختلفة بالاعتماد على هيئات الخزن المتنوعة ومن أشهر هذه الملفات هو ملف MP3:

I. MP3 (Moving Picture Expert Group Layer III)

يعد ملف MP3. من أشهر ملفات الصوت وأكثرها انتشارا وخاصة على الانترنيت، يرجع تاريخ نشوئه إلى عام 1987 في معهد فرانهوفر Frannhofer Institute في ألمانيا نتيجة مشروع يهدف إلى بناء ميكانيكية لكبس ملفات الصوت لتكوين ملف ذو حجم صغير دون التأثير على نوعية الصوت فكان الناتج هو MPEG 1 layer 3 الذي اختصر فيما بعد إلى ما يسمى MP3. بالنسبة لملف MP3 فأنه يعد عُشر حجم الملف الأصلي مما يساعد على تحميل الملف خلال دقائق بدلا من ساعات كما يمكن خزن المئات من ملفات الصوت دون اشغال مساحة خزنية كبيرة. [7][5].

II. التكوين الداخلي لملف MP3

يتكون ملف MP3 من مجموعة مقاطع (Frames) تكون متفاعلة مع بعضها البعض، كل مقطع يتكون من بادئة Header يبلغ طولها 32bit تحوي معلومات عن البيانات الموجودة في ذلك المقطع، ومن الجدير بالذكر أن ملف MP3 لا يحوي على بادئة موحدة لكل الملف وانما كل مقطع له بادئة خاصة به. أما مكونات بادئة كل مقطع فلاحظها في الجدول (1).

من أهم المعلومات الخاصة بملف MP3 هي:

a. **مقياس سرعة البيانات Bit Rate**

وهي عدد البتات لكل ثانية التي تخصص لخزن ملف الصوت، كلما زاد عدد البتات المستخدمة أدى ذلك إلى زيادة دقة الصوت (Audio Resolution) وبالتالي زيادة حجم ملف الصوت الناتج، أما قلة عدد البتات فسوف يعني ملف صوت ذا نوعية واطئة.

وحجم ملف MP3 يدعم صيغتين لمقياس سرعة البيانات:

- **ثابتة Constant Bit Rate (CBR)**

كل مقاطع الملف من البداية حتى النهاية لها نسبة ثابتة.

- **متغيرة Variable Bit Rate (VBR)**

لكل مقطع من مقاطع الملف له نسبة خاصة به تختلف عن بقية المقاطع، إن هذه الصيغة لها عدد من المساوئ.

b. نسبة التعيان Sampling Rate

إن دقة إشارة الصوت Resolution تعتمد بشكل كبير على عدد العينات لكل ثانية، وتعني قياس التردد الذي خزنت به الإشارة (Hz).

c. ID3 Tags

يحوي ملف MP3 نصاً تفسيرياً مطموراً، يشمل العنوان واسم المؤلف ومعلومات أخرى، ويدعى (ID3 tag). **[6][8].**

III. تكوين MP3 MP3 Encoder

في البدء، بعض المعلومات كمقدمة:

a. مدى الترددات التي يسمعها الإنسان هي (20 kHz–20 Hz).

b. عند وجود إشارتين متشابهتين بالتردد فان أي شخص يجد صعوبة في تحسس إحداهما وهذه الخاصية تدعى الحجب ألتزامني (Simultaneous(Auditory)Masking).

c. إن العقل البشري له مشاكل في سماع الأصوات المختلفة عند حدوثها في وقت متقارب وتدعى الحجب الزمني (Temporal Masking).

تمر عملية تكوين MP3 بعدة مراحل :

a. تقسيم الإشارة الداخلة إلى مجموعة من المقاطع الصغيرة frames، وكل مقطع يحوي أجزاء من الثانية، وهي تشبه إلى حد كبير مقاطع الفلم.

b. حساب مقياس سرعة البيانات Bit Rate المناسب لكل مقطع .

c. تحليل البيانات الموجودة داخل كل مقطع ومقارنته مع النموذج السابق (Human Psychcoaustice) المخزونة كمرجع والتي يتم من خلالها تحديد أي الترددات سوف تهمل وأي منها سوف تبقى.

d. إدخال البيانات على ترميز هوفمان (Huffman Coding)، إذ يتم كبس البيانات الناتجة من الخطوة السابقة لتقليل حجم الملف إلى أقل حد ممكن.

e. تجميع مجموعة المقاطع في سلسلة متتالية مع بادئة Header تسبق كل مقطع والذي يحوي معلومات عن ذلك المقطع. [8][7][6]

جدول (1) مكونات البادئة التابعة لكل مقطع لملف MP3

Sign	Length (bit)	Description
A	11	Frame sync (all bits set)
B	2	MPEG audio version (MPEG 1, 2, etc)
C	2	MPEG layer description (layer I, II, III)
D	1	Protection (if on, then check sum follows header)
E	4	Bit-rate index (lookup table used to specify bit-rate for this MPEG version and layer)
F	2	Sampling rate frequency(lookup table)
G	1	Padding bit (on or off, compensates for unfilled frames)
H	1	Privet bit (on or off, allows for application specific triggers)
I	2	Channel mode (stereo, joint stereo, dual channel, single

		channel)
J	2	Mode extension (used only with joint stereo to conjoin channel data)
K	1	Copyright (on or off)
L	1	Original (off if copy of original, on if original)
M	2	Emphasis (respects emphasis bit in the original recording :now largely obsolete)

5. تحليل ملف الصوت نوع MP3

أن هيكلية ملف MP3 متكونة من عدد من المقاطع تدعى Frames وكل مقطع له بادئة خاصة به بطول 32Bit تحوي معلومات حول البيانات الموجودة في ذلك المقطع واهم هذه المعلومات التي نحتاجها لتحليل ملف MP3 هي:

I. مقياس سرعة البيانات (Bit Rate): وهي بطول 4 bit تمثل مدخل إلى جدول يحوي القيم الحقيقية المقابلة للقيمة السابقة وهذا ما يوضحه الجدول (2).

جدول (2) يوضح جدول تواجدات Bit Rate

Bits Value	Bit Rate	Bits Value	Bit rate	Bits Value	Bit rate
0001	32	0110	80	1011	192
0010	40	0111	96	1100	224
0011	48	1000	112	1101	256
0100	56	1001	128	1110	320
0101	64	1010	160	1111	Bad

II. نسبة التعيان (Sampling Rate): تكون بطول 2 bit وهي مدخل إلى جدول يحوي القيم الحقيقية لنسب التعيان المستخدمة مع هذا النوع من الملفات الصوتية وكما يوضح الجدول (3).

جدول (3) قيم نسب التعيان

Bits Value	Sample Rate
00	44100
01	48000
10	32000
11	Reserved

III. Padding Bit: وهي بطول بت واحدة ولها قيمتان فقط

0:Frame is not padded

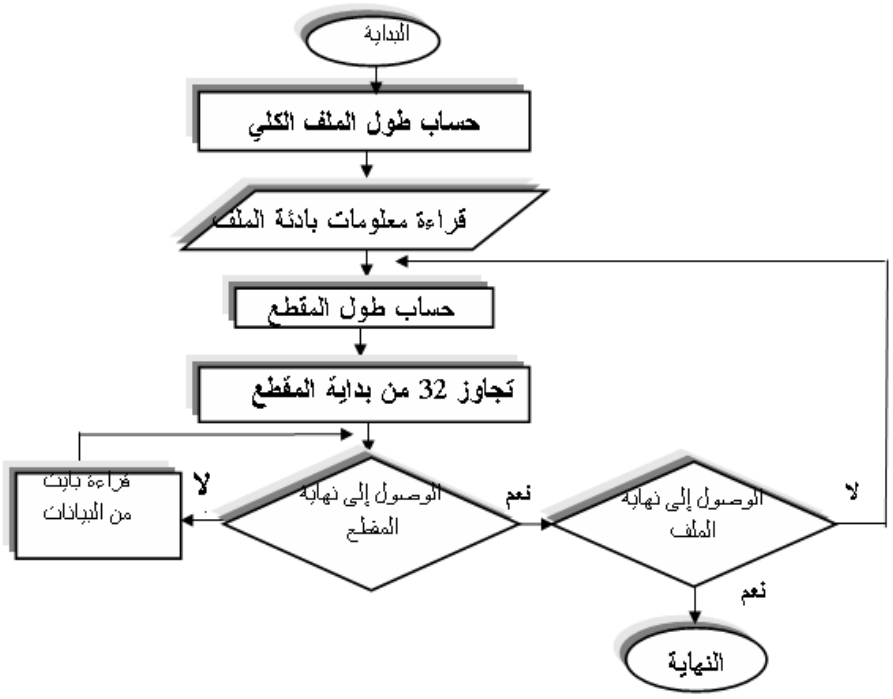
1: Frame is padded with extra slot

المعلومات السابقة نستفاد منها لحساب طول كل مقطع وحسب المعادلة الآتية:

Frame Length in Byte = 144*Bitrate /Sample Rate +Padding

ويقاس الطول بالـ slote والذي يعادل byte بالنسبة MP3 . [1][7]

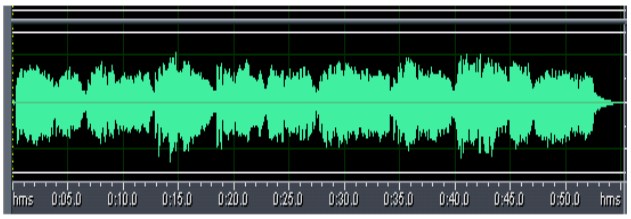
والشكل (1) يوضح عملية قراءة بيانات ملف MP3.



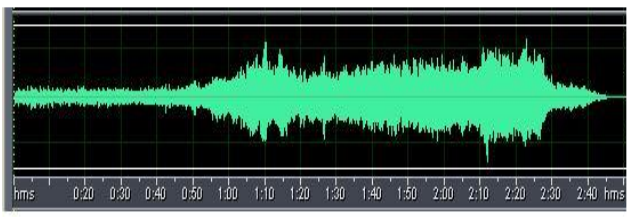
شكل (1) : مخطط انسيابي لقراءة بيانات ملف MP3

6. الملفات المنتخبة للاختبار

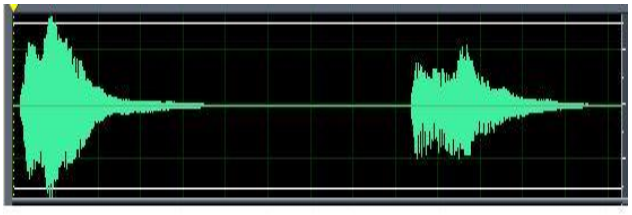
نذكر هنا الملفات الصوتية نوع MP3 المنتخبة ذات الخصائص المختلفة لغرض التطبيق:



الشكل (2) الإشارة لملف MP3 (تلاوة لصورة الفاتحة). بنسبة تعيان 44.1 kHz وسرعة البيانات 96 Kb.

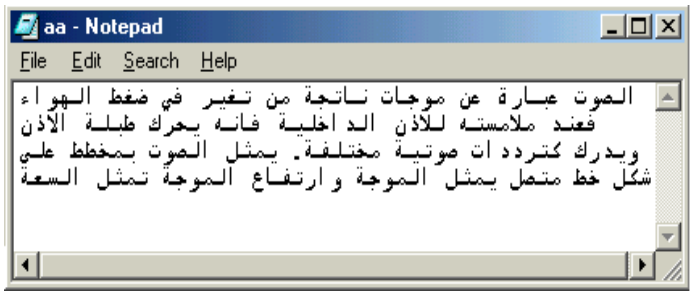


الشكل (3) الإشارة لملف MP3 (ملف موسيقي). بنسبة تعيان 48 kHz وسرعة البيانات 256 Kb.



الشكل (4) الإشارة لملف MP3 (فترات صوتية مستوية). بنسبة تعيان 44.1 kHz وسرعة البيانات 48 Kb.

كما تم اختيار الملفات الاتيه لعملية الإخفاء (رسائل سرية).

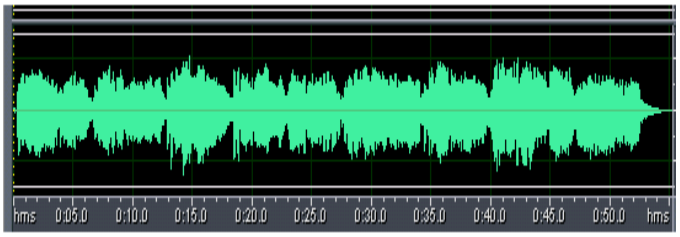


الشكل (5)

ملف نصي نوع TXT

الشكل (6)

ملف صوره نوع BMP

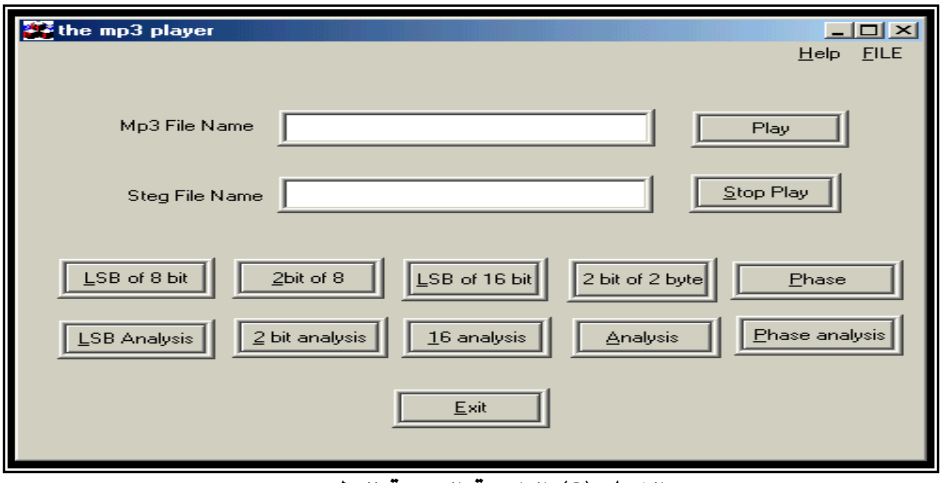


الشكل (7)

ملف صوت نوع WAV

7. الواجهة الرئيسة للتطبيق

مع بداية تطبيق الخوارزمية تظهر الواجهة الآتية:



الشكل (8) الواجهة الرئيسة للتطبيق

ولغرض توضيح ماتحويه الواجهة الرئيسية من اختيارات، يمكن اتباع مايلي:

I. فتح ملف الغطاء نوع MP3

يتم اختيار ملف الغطاء من القائمة file…open ويعرض بالخانة النصية الأولى.

II. فتح الملف المراد إخفاءه

يتم اختيار الملف المراد إخفاءه من القائمه السابقة ويعرض في الخانه النصيه الثانيه.

III. تشغيل ملف الصوت من نوع MP3

تم تكوين دالة التشغيل بالاعتماد على بعض الخصائص الموجودة في لغة Visual C++ ،أما الصيغة العامة لهذه الدالة كالأتي:

PlayMP3 (char filename, int volume, int loop, priority).

واهم المتغيرات الظاهرة أعلاه:

- اسم الملف Filename : ويتضمن اسم وموقع ملف الصوت.
- سعة الصوت Volume: وتكون قيمتها مابين 0-225.
- التكرار Loop: وتكون قيمته إما True أو False.
- الأسبقية Priority: قيمتها True كون هذا الملف له أسبقية بالتشغيل على ملف ثاني يعمل ايضاً.

IV. إيقاف التشغيل Stop Play :

يتم إيقاف تشغيل MP3 باستدعاء الدالة الآتية: Close ();

8. الإخفاء داخل ملف الصوت من نوع MP3

تم تطبيق طريقتين من طرائق الإخفاء داخل ملف MP3، لابد من الإشارة إلى أن عملية الإخفاء سوف تكون داخل البيانات الصوتية دون استخدام بادئة الملف في عملية الإخفاء، وذلك لأنها تكون أكثر عرضة للشك والاكتشاف.

أما أهم التقنيات المستخدمة لاخفاء البيانات داخل ملف الصوت فهي :

❖ **الإخفاء في الخلية الثنائية الأقل أهمية Low Bit Encoding**

تتم عملية الإخفاء بواسطة تبديل أول خليه bit من كل عينة.

❖ **تبديل الطور Phase Coding**

يتم باستبدال الطور للإشارة مع الطور للبيانات المراد إخفاؤها وتتم بتقسيم الملف إلى مجموعة من المقاطع وحساب الطور لها واستبداله مع البيانات المراد إخفاؤها، وهي اكفأ من الطريقة السابقة وتعد من الطرائق الفعالة لتقليل نسبة الضوضاء Noise.

9. الإخفاء بتغيير الخلية الثنائية الأقل أهمية Low Bit Encoding

تنص هذه الخوارزمية على تغيير أول بت Least Significant Bit (LSB) من كل عينة بقيمة البيانات المراد إخفاؤها. في هذا البحث تم اتباع أسلوبين لهذه الطريقة :

1.9. إجراء التغيير لكل بايت Byte

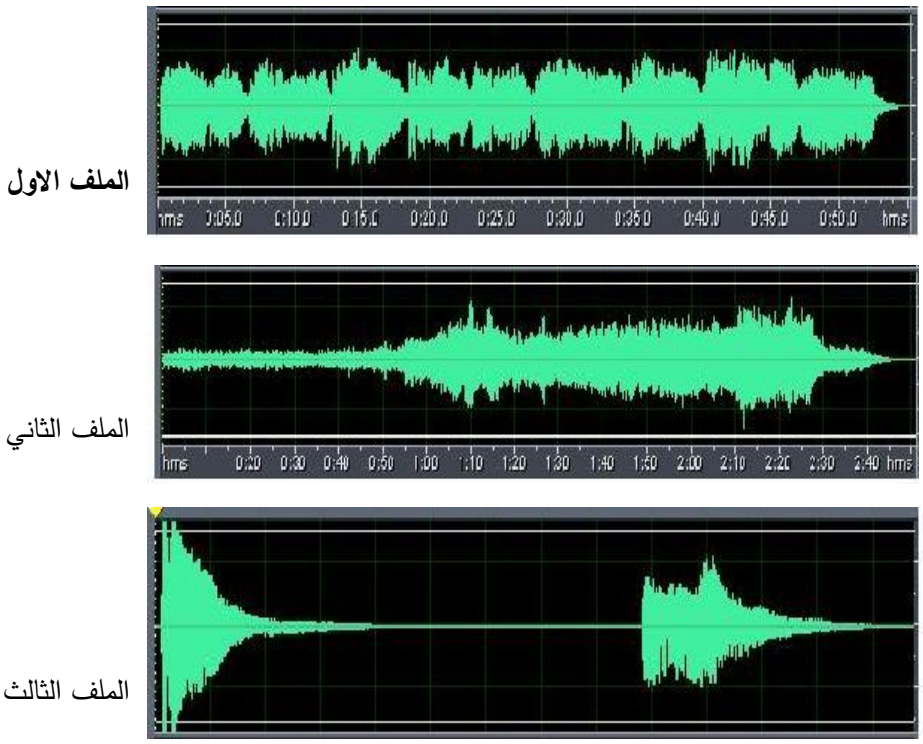
a. تغيير أول بت LSB لكل بايت Byte

تم بناء خوارزمية لتغيير اول bit من كل Byte، تبدأ الخطوات بفحص شرط قبول الحجم للرسالة المخفية وحسب المعادلة الآتية:

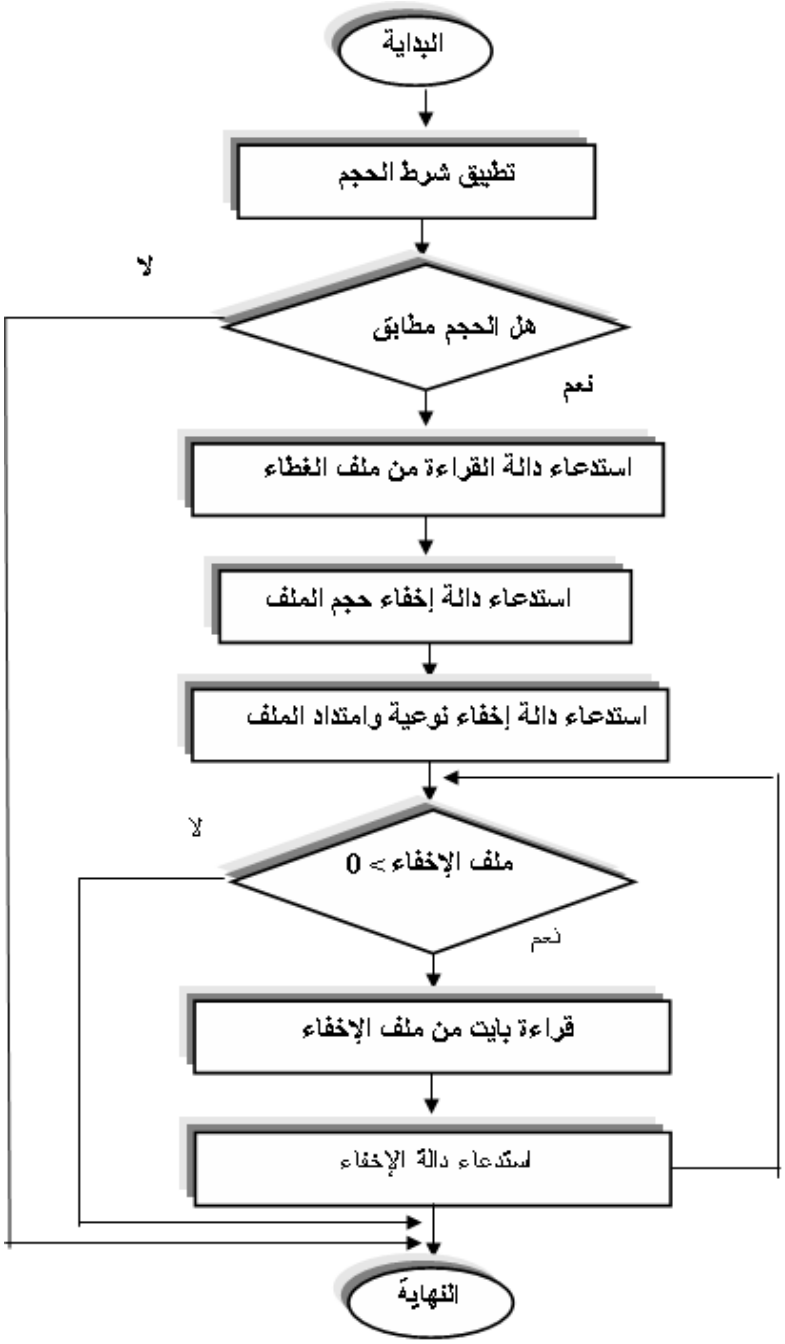
[حجم ملف الإخفاء + 32(طول الملف المخفي) + 8(نوع الملف) +8] ≥

[حجم الغطاء − (عدد المقاطع * 4(طول بادئة المقطع)) ÷ 8]

في حالة عدم مطابقة شرط الحجم السابق يتم الخروج من الخوارزمية لكبر حجم الملف المخفي بالنسبة إلى ملف الغطاء، أما في حالة تحقق الشرط يتم إجراء عملية الإخفاء. الشكل (9) يوضح نتائج تطبيق هذه الخوارزمية على الملفات المختارة. والشكل (10) يمثل المخطط الانسيابي لعملية الإخفاء.



الشكل (9) النتائج بعد تغيير بت لكل بايت



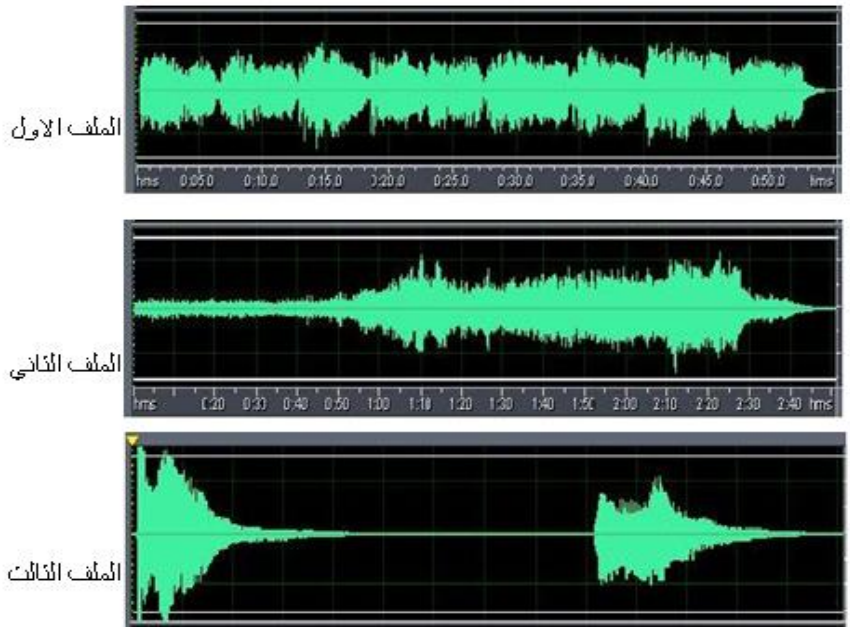
الشكل (10) مخطط انسيابي لعملية الإخفاء بتغيير بت من كل بايت

b. تغيير أول 2LSB Bit من كل بايت

هنا يتم تغيير أول 2bits من كل بايت، وهي تشبه الطريقة السابقة ماعدا اختلاف شرط مطابقة الحجم، إذ تكون كمية البيانات الممكن إخفاؤها هنا اكبر وحسب المعادلة الآتية:

[حجم ملف الإخفاء +16+4+ 4 ≥ حجم الغطاء – (عدد المقاطع*(4) ÷ 4]

ونتائج تطبيق هذه الطريقة على الملفات المعدة للاختبار في الشكل (11).



الشكل (11) النتائج بعد تغيير 2LSB من كل بايت

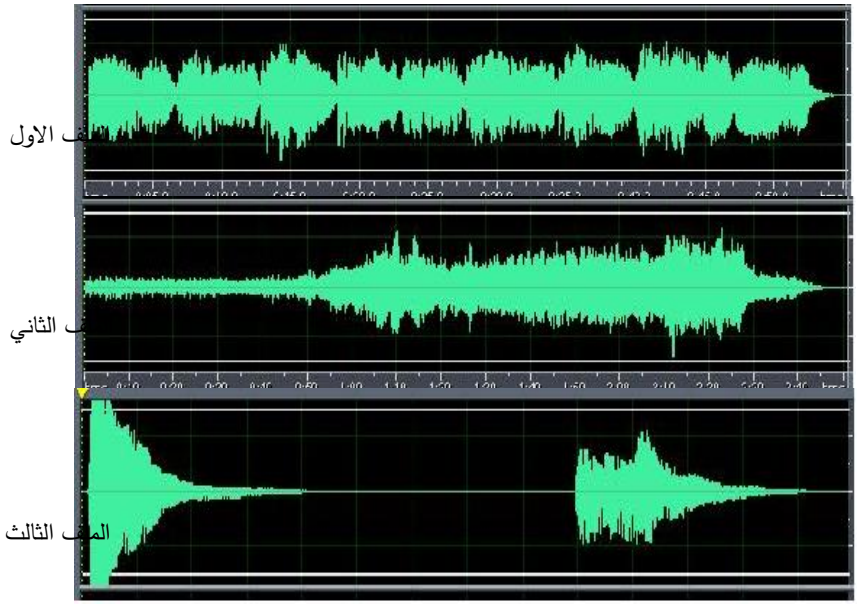
2.9. إجراء التغيير كل 2 byte

a. تغيير أول بت LSB لكل 2 Bytes

يتم تغيير أول بت من كل بايتين (2Bits)، هذه الطريقة اكفأ من السابقة، إذ أن نسبة الضوضاء الناتجة اقل ولكن كمية البيانات المخفية اقل، اما شرط مطابقة الحجم فحسب المعادلة الآتية:

[حجم ملف الإخفاء+32*2+16+16 ≥ حجم الغطاء–(عدد المقاطع*4)÷16]

وبعد تطبيق الخوارزمية على الملفات السابقة كانت النتائج في الشكل (12).



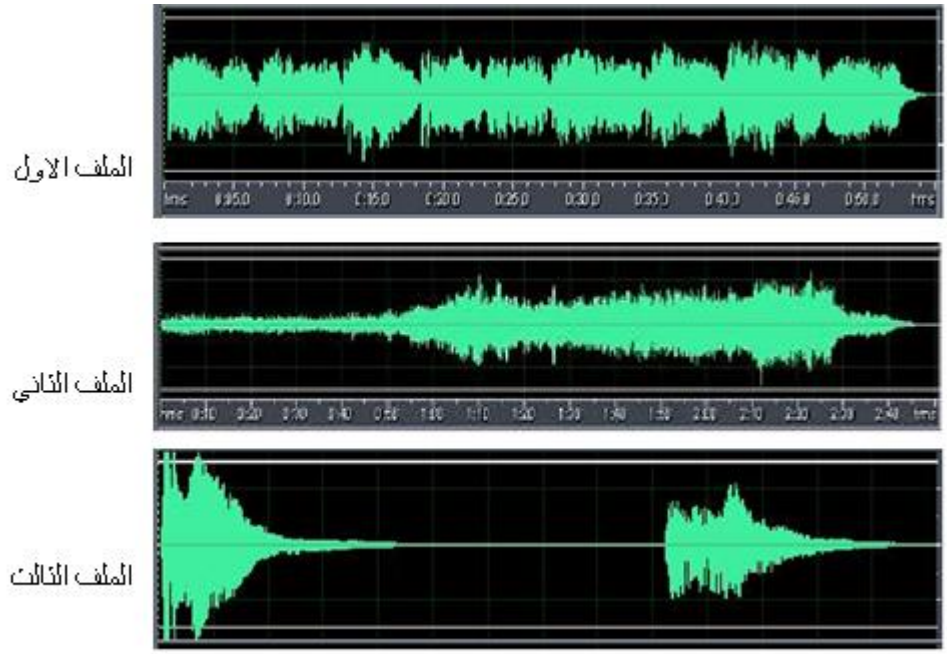
الشكل (12) النتائج بعد تغيير bit من كل 2byte

b. تغيير أول 2LSB من كل 2Bytes

هنا يتم تغيير أول بت من كل بايتين (2bits)، وبنفس الأسلوب ماعدا تغيير شرط الحجم، وحسب المعادلة الآتية:

[حجم ملف الإخفاء+32+8+8 ≥ حجم الغطاء−(عدد المقاطع*4)÷8]

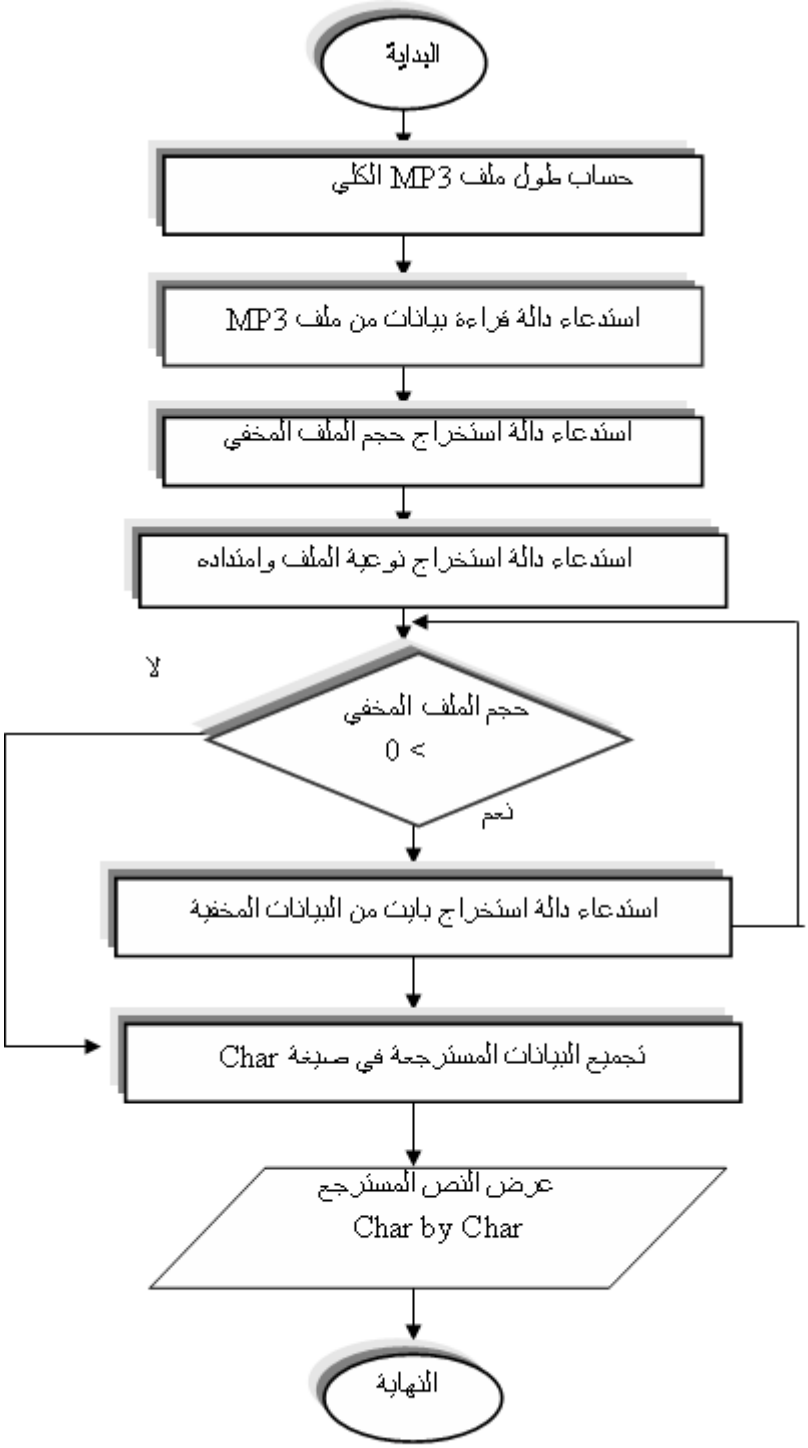
والشكل (13) يوضح النتيجة بعد إجراء التغيير على الملفات السابقة.



الشكل (13) النتائج بعد تغيير 2bits من كل 2byte

3.9. استعادة الرسالة المخفية

عملية فك الإخفاء تتم باستعادة حجم الملف المخفي ثم نوعية الملف وامتداده وبعدها تتم استعادة الرسالة، الشكل (14) يوضح الطريقة العامة لفك الإخفاء للطرائق السابقة:



الشكل (14) عملية استعادة البيانات المخفية

10. الإخفاء باستبدال الطور Phase Coding

هذه الطريقة تعمل على استبدال الطور للإشارة الأصلية بطور يمثل البيانات المخفية وتعتمد على مبدأ أن الأذن البشرية تكون اقل حساسية للتغيير في الطور للإشارة الصوتية، أما خطوات الخوارزمية فهي كآلاتي: [8][1]

a. تقسيم الإشارة الصوتية إلى سلسلة من المقاطع الصغيرة Segmentation .

b. اختيار نقاط من كل مقطع وتطبيق معادلة فوريير المتقطع Discrete Fourier Transform وحسب المعادلة:

$$F(u)=1/N \sum_{x=0}^{n-1} f(x)e^{-j2\pi ux/n} \quad \ldots (1)$$

وبعدها يتم حساب الطور Phase والقيمة Magnitude لكل نقطة وحسب المعادلات:

$$\phi(u) = \tan^{-1}\frac{imaj}{real} \quad \ldots (2)$$

$$\left|F(u)\right| = \sqrt{real^2 + imaj^2} \quad \ldots (3)$$

c. إيجاد الفرق بين أطوار كل مقطعين متتابعين ومتجاورين وحسب المعادلة:

$$\Delta\phi(n+1) = \phi(n+1) - \phi(n) \quad \ldots (4)$$

d. تمثيل البيانات المخفية كقيم طور وكالأتي:

$$0 \longrightarrow \frac{\pi}{2} \quad , \quad 1 \longrightarrow -\frac{\pi}{2}$$

إذ أن:

$$\varphi(n) = \varphi(data) \quad \ldots(5)$$

e. استبدال قيم الطور للإشارة الأصلية بالقيم المقابلة لها التي تمثل قيم الطور للبيانات المخفية مضافة إلى قيمة الفرق بين أطوار المقاطع المتجاورة.

$$\varphi(n) = \varphi(n-1) + \Delta\phi(n) \quad \ldots(6)$$

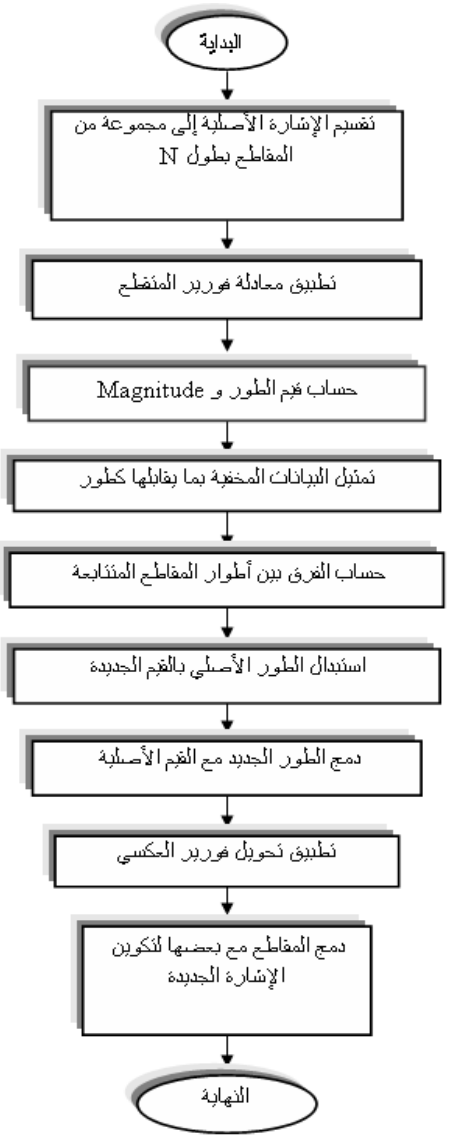
f. دمج قيم الطور الجديدة New Phase والقيمة الأصلية Original Magnitude ويتم تطبيق معادلة فوريير العكسية Inverse Fourier Transform وحسب المعادلة:

$$f(x)= \sum_{u=0}^{n-1} F(u)e^{j2\pi ux/n} \quad \ldots(7)$$

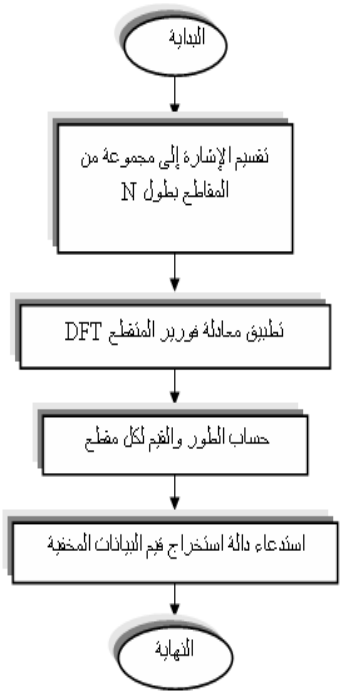
g. إعادة دمج المقاطع مع بعضها لتكوين الإشارة الجديدة .

والأشكال (15)(16) توضح خطوات خوارزمية الإخفاء وفك الإخفاء.

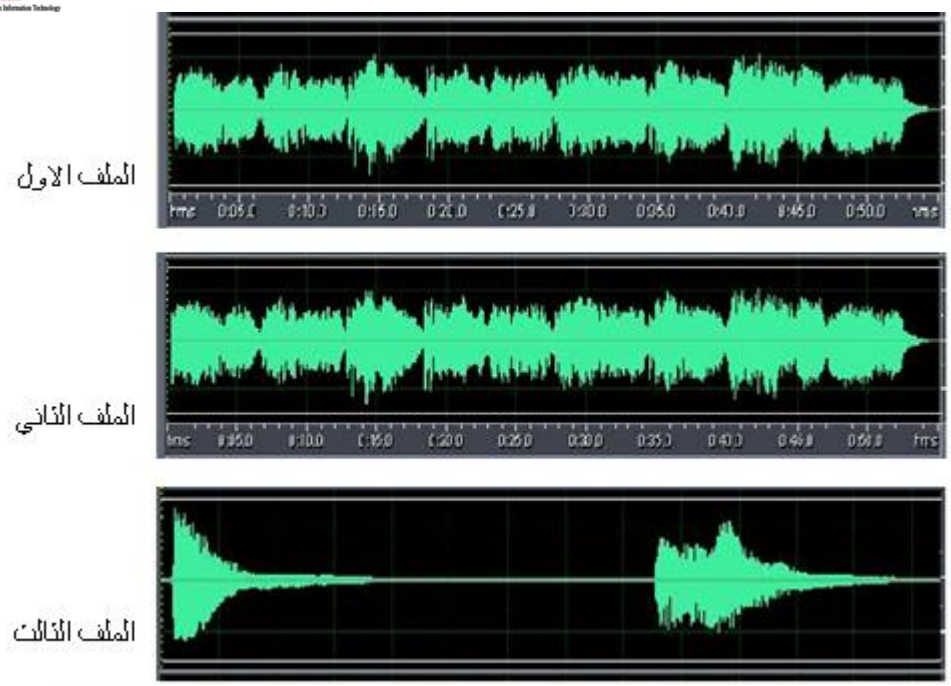
ونتائج تطبيق هذه الخوارزمية على الملفات المختارة فحسب الشكل (17).



الشكل (15) مخطط انسيابي لطريقة استبدال الطور



الشكل (16) مخطط انسيابي لعملية فك الإخفاء بطريقة استبدال الطور



الشكل (17) النتائج بعد الإخفاء باستبدال الطور

11. الاستنتاجات

من خلال ما تقدم يمكن القول بان العمل مع ملفات الصوت اكثر صعوبة من التعامل مع بقية أجزاء الوسائط المتعددة لما يحتويه من ترددات غير محسوسة، هذا بالإضافة إلى أن ملف الصوت MP3 والهيئة الخاصة به معقدة جداً وليست سهلة كما تبدو. كما تم استنتاج مايلي:

- تستفاد تقنيات التغطية من خصائص نظام الإدراك البشري وتعمل على استغلال نقاط الضعف لهذا النظام.
- إن اختلاف نسب التعيان Sample Rate ومقياس سرعة البيانات Bit Rate ليس لها تأثير كبير في عملية الإخفاء .
- تعد تقنية استبدال الطور افضل من طريقة تغيير الخلية الثنائية الأقل أهمية بسبب أن الأذن البشرية لا تستطيع تمييز الفرق بالطور.
- تعد طريقة استبدال الطور اكثر سرية من طريقة تغيير الخلية الثنائية الأقل أهمية وذلك لحاجة المستلم إلى معرفة طول كل مقطع والنقاط المختارة منه لعملية الإخفاء.
- يفضل استخدام الملفات الصوتية كثيرة التردد وتجنب الملفات الصوتية التي تحوي فترات صوتية مستوية لأنها اكثر عرضة للتأثر بالتغيير الحاصل بعد عملية الإخفاء.
- توزيع البيانات المخفية على طول ملف الغطاء لضمان عدم ظهور شك لدى المتطفل.
- تم قياس كفاءة الطرائق المستخدمة وتثبيت النتائج كما في الجدول.(4)

جدول (4) اختبار نسبة التمييز للطرائق المستخدمة

الطريقة	نوع ملف الاخفاء	نسبة التمييز
LSB (1Bit, 2Bits)	ملف نص (TXT)	99 %
	ملف صورة (BMP)	98 %
	ملف صوت (WAV)	95 %
استبدال الطور	ملف نص (TXT)	97 %
	ملف صورة (BMP)	96 %
	ملف صوت (WAV)	95 %

المصادر

[1]. Bender, W., et. al., (2000), "Applications for Data Hiding", IBM SYSTEMS JOURNAL, VOL 39, NOS 3&4.

[2]. Cvejic, N., (2004), "Algorithms For Audio Watermarking And Steganography", Department of Electrical and Information Engineering, Information Processing Laboratory, University of Oulu.

[3]. Cummins, J., et. al., (2004), "Steganography And Digital Watermarking", School of Computer Science, The University of Birmingham.

[4]. Yan, D. and Wang, R., (2008), "Reversible Data Hiding for Audio Based on Prediction Error Expansion", International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IEEE, pp.249-252.

[5]. Diqun, Y., et. al., (2009), "Quantization Step Parity-based Steganography for MP3 Audio", Fundamenta Informaticae archive, Volume 97, Issue 1-2 (January), Pp:1-14 .

[6]. Yan, D. and Wang, R., (2009), "Huffman Table Swapping-Based Steganography For Mp3 Audio", Springer Sciences+Business Media.

[7]. Al-Rababah, O. A., (2010), "A Steganography Method Based on Hiding secrete data in MPEG/Audio Layer III", International Journal of Computer Science and Network Security, VOL.10 No.7, July.

[8]. http://en.wikipedia.org/wiki/Mp3