**المجلة العراقية للعلوم الإحصائية (25) 2013**
**عدد خاص بوقائع المؤتمر العلمي السادس لكلية علوم الحاسوب والرياضيات**
**ص ص[415-429]**

# الإخفاء في الصوت باستخدام تقنية M8MA

د.أحمد سامي نوري* مصطفى باسم محمود** محمد عبد الكريم محمد**
حنين عبد الغفور جاسم***

**الخلاصة**

مؤخراً بعد ازدياد استخدام تقنيات الاخفاء ازداد الاهتمام بالملفات الصوتية و يعزى ذلك الى ان الادوات المتوفرة لتحليل الصوت تفشل عند تطبيقها .

و السبب الاخر هو شعبية ملفات الـ(MP3) و الـ(WAV) خصوصاً في الانترنيت، في هذا البحث يتم تسليط الضوء على احدى احدث تقنيات الاخفاء وهي M8MA التي تستخدم لإخفاء البيانات داخل الملفات الصوتية .

و كذلك التعرف بعمق على الصيغ الصوتية التي تم استخدامها كغطاء للبيانات و دراسة بعض خصائصها ومميزاتها ،حيث تم تطبيق التقنية المذكورة اعلاه باستخدام لغة الـ(C#) لكتابة الجزء العملي و بناء الواجهات التطبيقية للبرنامج على الملفات الصوتية من نوع WAV و MP3 ، و بحمد الله تم التوصل الى نتائج مرضية .

## Audio Steganography Using M8MA Technique

**Abstract**

In recent years , The use of concealment techniques that include audio files has been increased due to the fact that the tools available to analyze sound fail when applied .

Another reason is the popularity of MP3 and WAV files , especially on the Internet, the purpose of this research is to shed light on one of the latest of these techniques which is M16MA that is used to hide data within the Audio Files .

As well as give a general view on the audio formats that have been used as a cover for the data and identify some of the characteristics and advantages of those formats, the purpose of this research is to apply the algorithm above to the audio files of type WAV and MP3.

*أستاذ مساعد / قسم علوم الحاسوب / كلية علوم الحاسوب والرياضيات / جامعة الموصل

**باحث / قسم علوم الحاسوب / كلية علوم الحاسوب والرياضيات / جامعة الموصل

***باحثة / قسم علوم الحاسوب / كلية علوم الحاسوب والرياضيات / جامعة الموصل

**تاريخ استلام البحث** 2013/10/10 ـــــــــــــــــــ **تأريخ القبول** 2013/11/21

C #is used as the programming language to apply the practical part and building project interfaces.

**1- المقدمة**

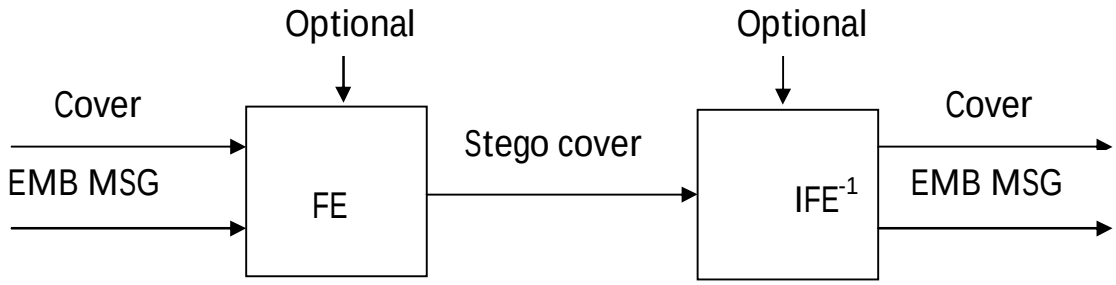
كانتو لا تزال سرية المعلومات احدى أهم عوامل تقنية المعلومات والاتصالات وخاصةً مع تقدم و ازدياد استخدام الحاسوب، فالاحتمالات المتزايدة لأجهزة الاتصالات الحديثة وتطبيقات الوسائط المتعددة على شبكات الاتصال أدى إلى زيادة الحاجة لتوفير طرائق كفؤة تعمل على حماية البيانات، من هنا ظهرت الحاجة إلى توفير وسائل أمنية البيانات لذا ظهر علم خاص بها يسمى علم التشفير (Cryptography) كتقنية لتأمين سرية البيانات و تناقل المعلومات، لكن هذه الطرائق لم تكن كافية ولا مضمونة لإبقاء هذه البيانات سرية، فمن المهم ابقائها بشكل سري امام المتطفلين، والتقنية المستخدمة لتطبيق ذلك تسمى الاخفاء (Steganography).

الإخفاء (Steganography) هو علم الاتصال الخفي، و يتم ذلك عن طريق إخفاء بيانات في بيانات اخرى. كلمة (Stganography) مشتقة من كلمات يونانية الأصل حيث أن كلمة "Stegos" تعني "Cover " او "غطاء" و كلمة "Grafia " تعني "Writing " او " كتابة "، حيث تعرف الكلمة بالشكل التالي "Cover Writing" او "الكتابة المغطاة"[1].

وهنالك اختلاف كبير بين علم الإخفاء (Steganography) وعلم التشفير (Cryptography)، حيث أن التشفير يعمل على ترميز و ابقاء البيانات بشكل سري غير مفهوم من قبل المتطفلين، أما الاخفاء يعمل على اخفاء ملف في ملف آخر دون الشك فيه [2].

يمكن تعريف نظام التغطية على انه علم إخفاء المعلومات باستخدام ملف حامل لها (Host) بهدف منع أي متطفل خارجي من الشك بوجود بيانات مخفية داخل الملف الحامل، وهي وسيلة من وسائل الاتصال السري بأسلوب يخفي وجود الاتصال.

ان النموذج الأساسي في نظم الإخفاء يكون كما موضح في الشكل (1) ادناه.




**الشكل (1) عملية الإخفاء**

| | |
|---|---|
| 1- FE | Steganography function "Embedding |
| 2- IFE | Steganography function "Extracting |
| 3- Cover | Cover data in which EMB MSG will be hidden |
| 4- EMB MSG | Message to be embedded |
| 5- optional key | Parameter of FE and IFE |
| 6- Stego cover | Cover data with embedded message |

## 2- الدراسات السابقة

- طبقت الباحثة شيماء محمد شكيب نظرية للاخفاء في مقطع MP3 باستخدام خوارزمية البت الاقل أهمية، 2004، وحصلت على نتائج تجاوزت 85% [3].
- طبقت الباحثة علياء موفق مع مجموعة من خريجي المرحلة الرابعة كبحث تخرج نظرية أخفاء نص في ملف صوتي بأستخدام خوارزمية ASCII Code و خوارزمية RSA،2007، علماً بأن النتائج كانت جيدة [4].
- اخفاء بيانات داخل مقطع MP3 بأستخدام خوارزمية Quantized Spectrum من قبل BEIXING DENG و آخرون، 2007، وتوصلوا إلى نتائج 80% [5].
- استخدم العالم Diqun وزملائه تقنية Quantization Step للاخفاء في مقطع MP3 ، 2009، علماً بأن النتائج كانت مشجعة [6].
- قدم الباحث نكتل مؤيد اللهيبي مع مجموعة من خريجي المرحلة الرابعة كبحث تخرج أخفاء نص في ملف صوتي من نوع WAV بأستخدام خوارزمية البت الاقل أهمية، 2012، وحققوا نتائج جيدة[7].

## 3- الصوت

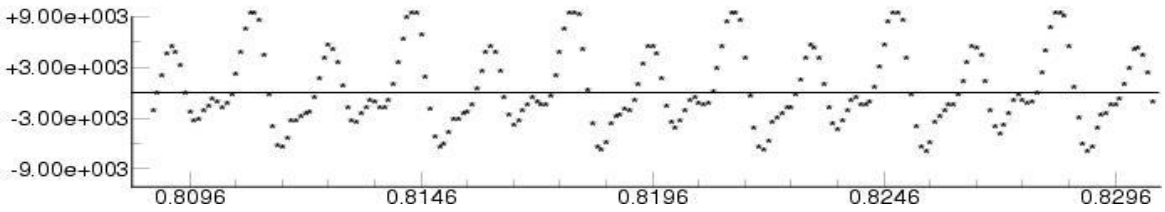
الصوت هو التردد الناتج عن تغير في ضغط الهواء، و على الرغم من كون هذا التغير لا يتعدى (1±)، لكن عند ملامسته للأذن الداخلية فأنه يحرك طبلة الأذن و يُدرك كترددات

صوتية مختلفة، تكون قادرة على التحرك في عدة أوساط مادية مثل الأجسام الصلبة، السوائل، و الغازات،ولا ينتشر في الفراغ.

يُمثل الصوت بمخطط على شكل خط متصل يُعرف الموجة و ارتفاع الموجة تمثل سعة الصوت (Volume) وهذه الصيغة تدعى بالإشارة التناظرية (Analog Signal) كما


**الشكل (2) الإشارة التناظرية المستمرة**

عند تسجيل الصوت يتم تحويل الإشارة التناظرية الى أشاره رقمية (Digital Signal) التي تتم عن طريق محول يدعى (A-D Converter). أول خطوة في عملية التحويل تتم بأخذ عينات من الإشارة التناظرية و خزن قيمتها المقابلة لوقت معين، وعندما يتم أخذ نسبة كافية من العينات لكل وحدة زمن من الصوت الأصلي فإن الإشارة الناتجة تكون قريبة جداً من الاشارة الاصلية أي بمعنى آخر أن الإشارة الرقمية تحوي معظم المعلومات الموجودة في الإشارة الأصلية [8][9]، الشكل (3) يوضح الإشارة الرقمية المقابلة للإشارة التناظرية في الشكل السابق




**الشكل (3) الإشارة الرقمية**

**4-العوامل المؤثرة على جودة الصوت**

1. **نسبة التعيـــان Sampling Rate** : كلما زادت نسبة التعيان والتي تمثل عدد العينات المأخوذة في الثانية الواحدة كلما اصبح الصوت اقرب إلى الحقيقة لكنه يؤدي الى زيادة حجم ملف الصوت الناتج .

2. **عدد البت المستخدمة لتمثيل العينةBit Per Sample** : غالباً يستخدم لتمثيل العينة الواحدة اما (8 bit) او (16 bit)، و كلما زاد عدد البت المستخدمة لتمثيل العينة زادت جودة و نوعية و حجم ملف الصوت [3].
3. **عدد القنوات المستخدمة Number of Channel** : عند استخدام قناتين للتسجيل (Stereo) فإن حجم الملف الصوتي سيكون بضعف الحجم الناتج للملف نفسه لو تم تسجيله باستخدام قناة واحدة (Mono)، وقد وفرت طرائق التسجيل الرقمية الحالية عدداً مختلفاً من قنوات التسجيل فيمكن التسجيل بقناة واحدة أو قناتين أو اكثر[3].

**5- أنواع الملفات الصوتية المستخدمة في البحث كغطاء لإخفاء البيانات**

**1- الملفات السماعية ذات الامتداد ( WAV )**

الملفات الصوتية ذات الامتداد (WAV.) شائعة الاستخدام تحت بيئة نظام (Windows)المنتج من قبل شركة Microsoft، وتعرف هيئة الملف العامة بـ RIFF (Resource Interchange File Format) التي ضمت بشكل مقاطع متداخلة مع بعضها البعض، إن الملفات السماعية من نوع WAV لاتحوي فقط القيمة الرقمية للعينة وإنما تحوي معلومات توصف وتعرف صيغة البيانات السمعية، قبل فتح الملف لتشغليه يقوم النظام بمعرفة بعض البيانات الخاصة بالملف، منها نسبة التعيان ونوع القناة المستخدمة سواء كانت (Mono) او (Stereo) وكذلك عدد الأرقام الثنائية المستخدمة لتمثيل العينة الصوتية.

الملفات من نوع WAV هي نوع خاص من ملف الـ RIFF الذي يتكون من أربعة مقاطع، كل مقطع يبدأ بأ بعة رموز أو كتل ثمانية وهي ( "data" List "fmt" RIFF ) ثم يليه حجم المقطع ، جميع ملفات الـ WAV تمثل بمقطع الـ RIFF الذي يكون ذا حجم كبير يظهر بعد الـ RIFF Chid المقطع Cksize والذي يحوي قيمة تساوي حجم الملف مطروح منها 8-bytes التي تمثل قيمة الـ RIFF Chid مع .Chsize إن المقاطع التالية تعرف بـ sub chunk، تكون موجودة داخل الـ RIFF Chunk هي :

أ- "fmt" ويحوي معلومات عن صيغة الـ PCMو هي سلسلة من النبضات التي ترمز برمز ثنائي.

ب- "data" الذي يمثل الجزء الأكبر من الملف والذي يحوي جميع الصيغ الرقمية للبيانات، مع نهاية هذا المقطع يتم تمثيل نهاية الـ RIFF Chunk .إن مقطع الـ RIFF Chunk يساوي الرقم الكلي لمجموع الـ bytes المكونة للمقطع الجزئي "fmt"و المقطع "data" . بعض ملفات الـRIFF تحوي المقطع List الذي يحوي معلومات أخرى مثل

ملاحظات عن النسخة الأصلية للملف وتعريف بيانات المستخدم التي تصف المحتويات الرقمية لمقطع الـ "data"والجدول (1) يوضح الصيغة القياسية المعتمدة لبداية الملف، ونلاحظ أن جميع ملفات الـ WAV تكون مشتركة في الحقول (1-11)[13].

**جدول (1) مكونات الملف RIFF ذو الصيغة القياسية**

| Filed | Size/b | Offset | Contains | Description |
|---|---|---|---|---|
| 1 | 4 | 0 | "RIFF" | Signature For Resource Interchange File Format |
| 2 | 4 | 4 | Size | Total File SIZE -8 |
| 3 | 4 | 8 | "wave" | Signature for audio RIFF |
| 4 | 4 | 12 | " fmt" | After it the Information about the sound |
| 5 | 4 | 16 | 16/18 | Size of info after this local |
| 6 | 2 | 20 | Compr. Code | Usually 1=PCM : 0 not Compressed |
| 7 | 2 | 22 | No. of Channels | 1 mono, 2 stereo |
| 8 | 4 | 24 | Samples/Sec | The file sampling rate |
| 9 | 4 | 28 | Byte/sec | Number of bytes/second |
| 10 | 2 | 32 | Sample size in bytes | Size of sample in bytes |
| 11 | 2 | 34 | Sample size in bits | Size of sample in bits |
| 12 | 2 | 36 | Reserved | This location is exist if offset 16 contain 18 |
| 13 | 4 | 36/38 | "Data" | Chunk type data |
| 14 | 4 | 40/42 | Length of Sound Data | The length of the sound data in bytes |
| 15 | Length of Data | N | Signal | Actual sound samples |

**2- الملفات السماعية ذات الامتداد ( MP3 )**

يعد ملف MP3 من أشهر ملفات الصوت وأكثرها انتشارا، يرجع تاريخ نشوئه إلى عام ١٩٨٧ في معهد فرانهوفر Frannhofer Institute في ألمانيا نتيجة مشروع يهدف إلى بناء ميكانيكية لكبس ملفات الصوت فكان الناتج هو MPEG 1 layer 3 الذي اختصر فيما بعد إلى مايسمى MP3 .

يعد ملف MP3 عشر حجم الملف الأصلي مما يساعد على تحميل الملف خلال دقائق بدلا من ساعات[10][11] . يتكون ملف الMP3 من مجموعة من المقاطع (Frames) تكون متفاعلة مع بعضها البعض، كل مقطع يتكون من بادئة (Header) يبلغ طولها 32Bit تحوي معلومات عن البيانات الموجودة في ذلك المقطع .

يحوي ملف الMP3 نصاً تفسيرياً ، يشمل العنوان و أسم المؤلف و معلومات أخرى ، يدعى (ID3 tag) ، يبلغ طول هذه المعلومات كحد أقصى 256 Byte.[12]

حجم ملف الMP3 يدعم صيغتين لمقياس سرعة البيانات (Bit Rate)، الاولى ثابتة وتسمى(Constant Bit Rate (CBRحيث ان كل مقاطع الملف من البداية الى النهاية لها نسبة ثابتة، و الاخرى متغيرة تسمى(Variable Bit Rate (VBR لكل مقطع من مقاطع الملف له نسبة خاصة به تختلف عن بقية المقاطع.

تفاصيل البادئة التابعة لكل مقطع لملف الMP3

**AAAAAAAA AAABBCCD EEEEFFGH IIJJKLMM**

**جدول (2)** مكونات البادئة التابعة لكل مقطع لملفMP3

| 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) |

جدول (3) يوضح جدول تواجداتBit Rate

| Bits Value | Bit Rate |
|---|---|
| 0001 | 32 |
| 0010 | 40 |
| 0011 | 48 |
| 0100 | 56 |
| 0101 | 64 |

| Bits Value | Bit Rate |
|---|---|
| 0110 | 80 |
| 0111 | 96 |
| 1000 | 112 |
| 1001 | 128 |
| 1010 | 160 |

| Bits Value | Bit Rate |
|---|---|
| 1011 | 192 |
| 1100 | 224 |
| 1101 | 256 |
| 1110 | 320 |
| 1111 | Bad |

جدول (4) قيم نسب التعيان Sample Rate

| Bits Value | Sample Rate |
|---|---|
| 00 | 44100 |
| 01 | 48000 |

| | |
|---|---|
| 10 | 32000 |
| 11 | Reserved |

المعلومات السابقة يتم الاستفادة منها لحساب طول كل مقطع وحسب المعادلة الآتية:

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

ويقاس الطول بالByte بالنسبة للـ [12]MP3.

## 6- خوارزمية العمل ( M8MA )

هي طريقة جديدة لإخفاء البيانات في الملفات الصوتية (MP3,WAV)، هذه الطريقة تعتمد على باقي القسمة على8(M8M – Mod8 Method) و التي تم تصميمها في البداية للتعامل مع الصور و من ثم طورت لتشمل الإخفاء في المقاطع الصوتية ( Mode 8 Method for Audio – M8MA) بالإضافة إلى استخدام طريقة لتوليد مواقع الإخفاء و ذلك لتجنب الإخفاء في مواقع تسلسلية و مما يساعد على تجنب تشوه جودة الصوت .

البيانات المراد إخفائها ممكن ان تكون بأي شكل رقمي و تعامل عادةً كسيل من البتات (Bit stream)، ويتم توليد مواقع الإخفاء حسب دالة رياضية تعتمد على القيم الرقمية للملف الصوتي .

فكرة الخوارزمية مبنية على الإخفاء بتضمين 3bit من البيانات المراد إخفائها في كل عينة من المقطع الصوتي، بالاعتماد على باقي قسمة العينة الواحدة على 8،فبذلك يتم ضمان جودة المقطع الناتج مع مساحة تضمين اكبر داخل الملف الحامل . عملية الاسترجاع تبدأ بتحديد المواقع التي تم التضمين فيها ثم الاسترجاع بعمليات محددة للحصول على البيانات الاصلية (خوارزمية الاسترجاع).

### الخوارزمية الحاسوبية

هنالك جزئين، الأول يتم تطبيق عند الطرف المرسل والأخر عند المستقبل .

**الطرف المرسل**

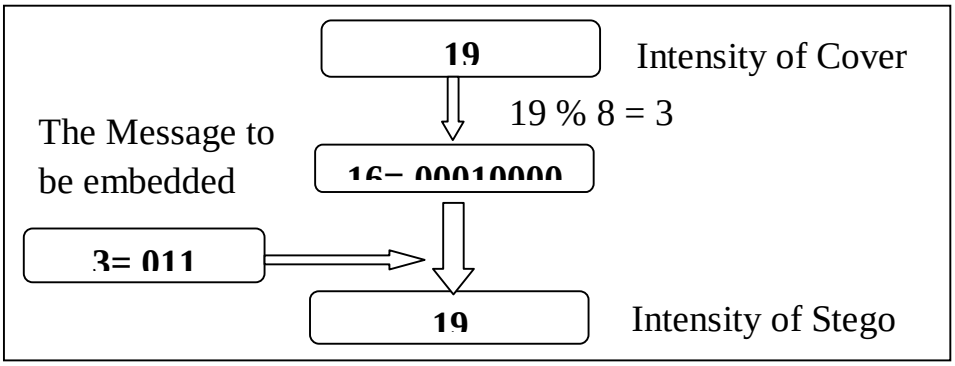
- اختيار المقطع الصوتي الذي يمثل الغطاء .
- اختيار البيانات المراد إخفائها .
- يتم اخفاء البيانات داخل الغطاء باستخدام الخوارزمية المقترحة لإنتاج المقطع الصوتي الذي يحوي البينات المخفية (Stego Audio).

**الطرف المستقبل**

- يتم اختيار المقطع الصوتي الذي يحوي على البيانات المخفية (Stego Audio) .
- استخراج البيانات المخفية باستخدام الخوارزمية المقترحة (M8MA) بطريقة الاستخراج.
- عرض البيانات الاصلية المستخرجة من المقطع الصوتي

### طريقة تضمين البيانات Data Embedding Method

- Input: Audio File.
- Input: secret Data.
- Matrix(sampels)=Get sampels from Input Audio.
- Matrix(secret)= Convert the secret Data to the binary stream .
- Let size = the size of matrix(secret) mode 3.
- If size equal "1" then extend the matrix(secret) by two locations and give it "0" value.
- Else If size equal "2" then extend the matrix(secret) by one location and give it "0" value.
- Initialize m = val = inc = count = 1.
- Begin for loop start with i=0 , increment by 3 ,till size of matrix(secret).
- Let cvr = contains the value of sampels(m) .
- If cvr is negative then sgn = -1. else sgn=1.
- Let dcm = the decimal of the concatenation three bits(secret[i+2], secret[i+1], secret[i],).
- Let r be the remainder after dividing cvr by 8 .
- cvr=cvr – e + dcm.
- If sgn=-1 then cvr = cvr * -1.
- Set the value of cvr at the sampels(m).
- Val = inc mod 8.
- If val less than 8 then m = m + val + 1.
- Increment inc by one .
- End for loop.

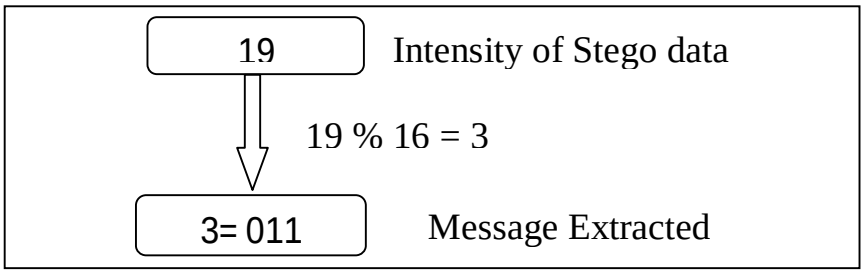



**الشكل (4) مثال توضيحي لعملية تضمين البيانات .**

### طريقة استخراج البيانات Data Extraction Method

- Input: Stego Audio Data vector(stego),v= samples from stego , Message size
- Initialize m = x = count =1;binmsg1="";vector(bytes)
- Begin for loop starting with i=0, incrementing 3 till entire message is retrieved
- let r be the remainder after dividing v by 8;
- v = value of stego(m)
- if(r == BI) where BI varies from 0 to 7 then
- convert r to 3 bit binary and add the each bis to vector(bytes).
- End if

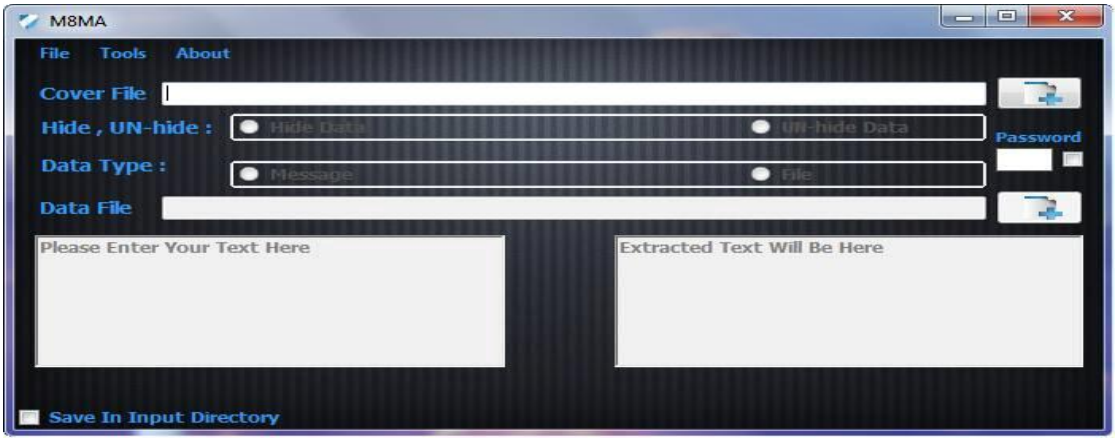
- Let r be the remainder after dividing x by 3;
- If r = val then m = m + r+1; where val = 0, 1 and 2 ;
- x = x + 1;
- End For Loop
- Initialize msgx=msg1='';k=0;
- Begin for Loop with i=1, incrementing 1 and till
- Message size
- Begin for Loop with j=1, incrementing 1 and till 8
- Increment k by 1;
- msgx(j)= character equivalent of (binmsg1(k));
- End For loop
- End For Loop
- Begin for loop starting with k=0, increment by 8 .
- convert each 8 bits to 1 byte and assign it to a location in vector(bytes) .
- end loop.




**الشكل (5) مثال توضيحي لعملية استخراج البيانات .**

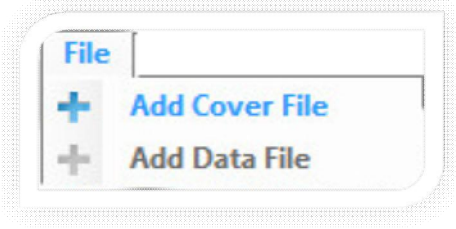
**7- واجهة النظام للاخفاء في MP3 او WAV**

فيما يلي بعض الواجهات الرئيسية للنظام كما في الاشكال (6) (7) (8) (9) (10)




**الشكل (6) الواجهة الرئيسية للتطبيق**

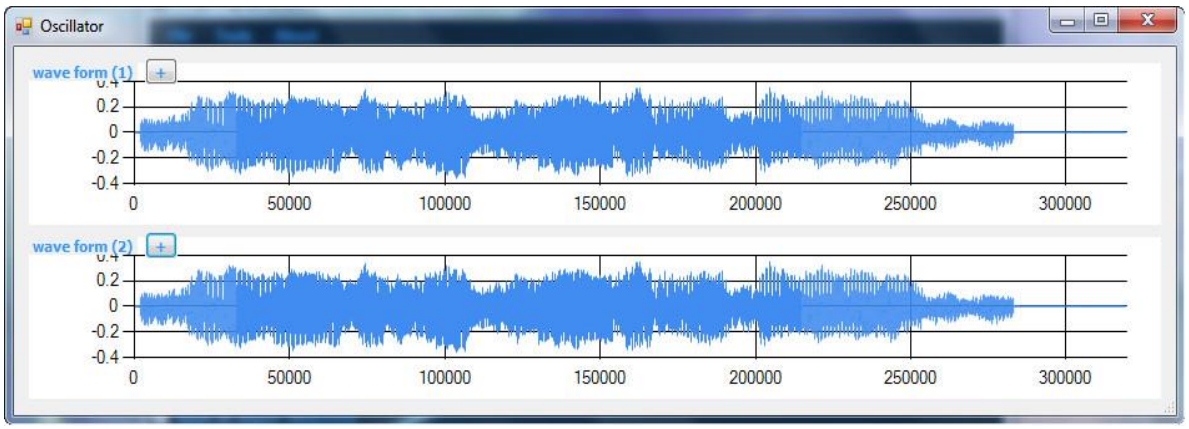
.1




شكل(7) قائمة File

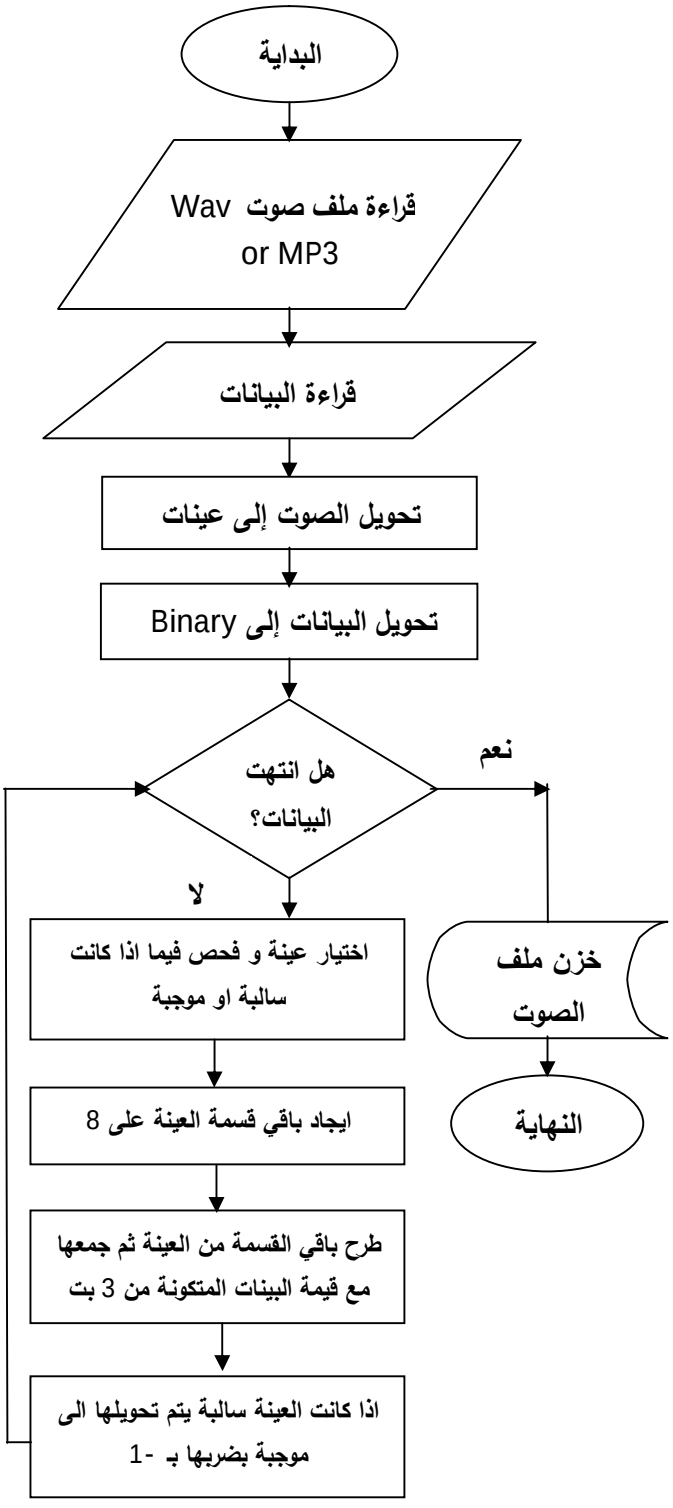

شكل (8) قائمة Tools


شكل (9) واجهة مسجل الصوت

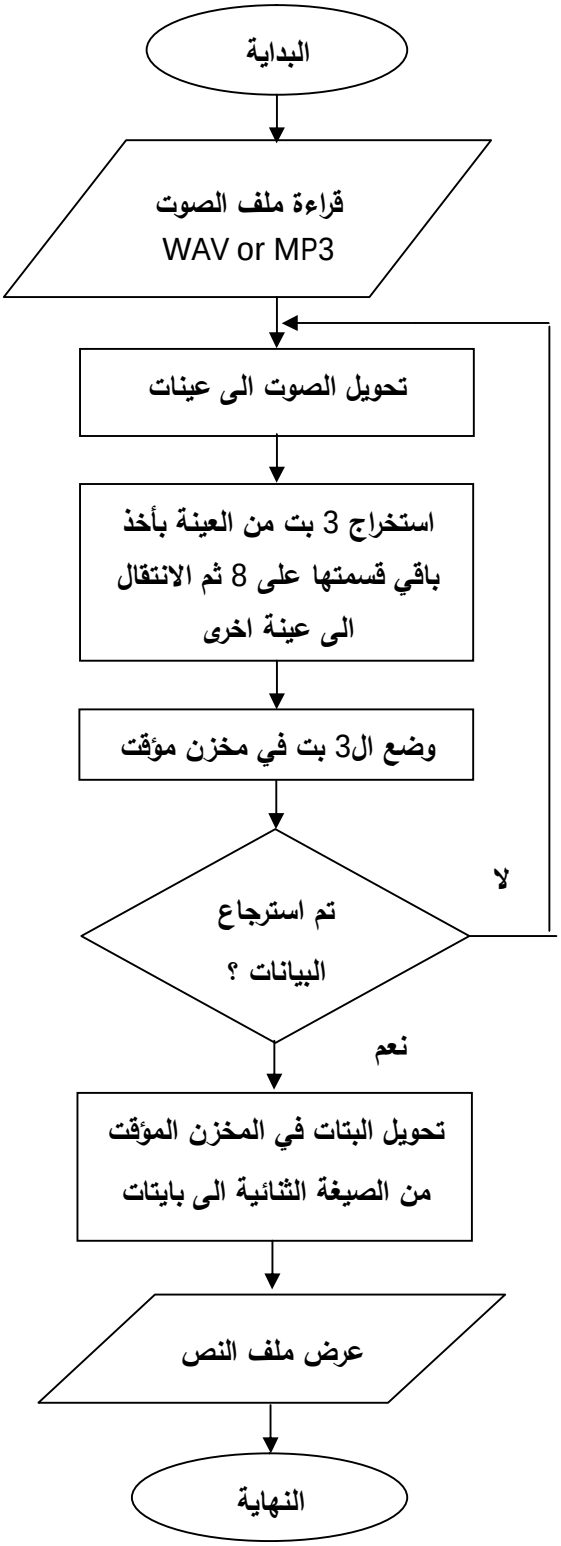



شكل (10) واجهة عارض الموج.

**8- المخطط الانسيابي لخوارزميتي الإخفاء و الاسترجاع**




الشكل (14) خوارزمية الإخفاء




الشكل (15) عملية الاسترجاع

**9- الاختبارات الشيئية**

تم تقييم الإخفاء بواسطة الاختبارات الشيئية التي تستخدم طرائق رياضية (الجداول 5 و 6)، حيث توجد عدة أنواع من الاختبارات الشيئية أهمها:[3]

**أولا:** إيجاد معدل مربع الخطأ (Mean Squared Error) بين إشارة الإدخال وإشارة الإخراج، المعادلة (1).

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

حيث تمثل M و N عدد الأعمدة والأسطر للإشارة

**ثانيا:** قياس نسبة الضوضاء إلى نسبة الإشارة الأصلية (Peak Signal-to-Noise Ratio) ، المعادلة (2).

$$PSNR = 10\log_{1o}[\frac{R^2}{MSE}] \quad \text{..... (2)}$$

**جدول(5) قيم الاختبارات الشيئية**

| Audio File | Audio Length | Measure | Data Size 10 KB | Data Size 100 KB | Data Size 500 KB |
|---|---|---|---|---|---|
| بسملة.wav | 00:00:04 | MSE<br>PSNR | 2.6001e-09<br>76.7408 | 65.6286 | N.A |
| Speech.wav | 00:01:01 | MSE<br>PSNR | 1.4882e-10<br>80.0531 | 1.2445e-09<br>70.8300 | N.A |
| Calcul.wav | 00:03:02 | MSE<br>PSNR | 6.3761e-11<br>97.2187 | 4.1455e-10<br>89.0884 | 2.3807e-09<br>81.4971 |

**جدول(6) مقارنة تقنيتي M8MA و LSB**

| Audio File | M8MA | | LSB | |
|---|---|---|---|---|
| | Data Size 100 KB | Data Size 500 KB | Data Size 100 KB | Data Size 500 KB |
| بسملة.wav | 65.6286 | 59.6291 | 63.1045 | 57.3481 |
| Speech.wav | 70.8300 | 63.7102 | 66.2773 | 59.1220 |
| Calcul.wav | 89.0884 | 81.4971 | 82.2610 | 74.9821 |

**10- الاستنتاجات**

من خلال ما تقدم يمكن القول بان العمل مع ملفات الصوت اكثر صعوبة من التعامل مع بقية أجزاء الوسائط المتعددة ، هذا بالإضافة الى أن ملف الصوت MP3 والهيئة الخاصة به تعد حديثة العهد. بالاضافة إلى:

1. يمكن استخدام تقنيات التغطية لإخفاء اي نوع من انواع الملفات المتمثلة بصيغة Bit Stream .
2. ان التعامل مع ملفات الصوت Wav أسهل من التعامل مع MP3 كون الاخيرة تعتبر خلاصة الصوت.
3. كلما زاد حجم العينة اصبح الصوت الناتج من عملية الاخفاء اكثر كفاءة .
4. يمكن توزيع البيانات المخفية على طول ملف الغطاء لضمان عدم ظهور شك لدى اي متطفل.

**11- المصادر**


[1] Jayaram P and others," INFORMATION HIDING USING AUDIO STEGANOGRAPHY – A SURVEY", August 2011, College of Engineering, Bangalore, INDIA. www.ivsl.org .

[2] Wang, H & Wang, S, **"Cyber warfare: Steganography vs. Steganalysis"**, Communications of the ACM, October 2004.

[3] شيماء شكيب محمد ،" **تطبيق نظرية الاخفاء في مقطع MP3 بأستخدام خوارزمية البت الاقل أهمية** "، 2004، بحث ماجستير، قسم علوم الحاسوب، كلية علوم الحاسوب والرياضيات، جامعة الموصل.

[4] أخفاء نص في ملف صوتي بأستخدام خوارزمية ASCII Code و خوارزمية RSA، للباحثة علياء موفق مع مجموعة من خريجي المرحلة الرابعة كبحث تخرج، 2007

[5] اخفاء بيانات داخل مقطع MP3 بأستخدام خوارزمية Quantized Spectrum من قبل BEIXING DENG وآخرون، 2007، دائرة الهندسة الالكترونية، جامعة تسينغهوا، بكين ، الصين

[6] استخدام تقنية Quantization Step من قبل العالم Diqun و زملائه للاخفاء في مقطع MP3 ، 2009

[7] أخفاء نص في ملف صوتي من نوع WAV بأستخدام خوارزمية البت الاقل أهمية للباحث نكتل مؤيد اللهيبي مع مجموعة من خريجي المرحلة الرابعة كبحث تخرج، 2012

[8] Geoff Martin, B.Mus., M. Mus., **"Introduction to Sound Recording "**, October 23, 2011www.tonmeister.ca/main/textbook/

[9] Mcglougline, Stephen, 2001**, "Multimedia Concepts and practice"**, Prentice Hall, Inc.,upper saddle River, New Jersey, 073458.

[10] 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 .

[11] 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.

[12] Mohammed Salem Atoum And others**," MP3 Steganography: Review"**, November 2012, UniversitiTeknologi Malaysia www.ivsl.org .

[13] أيمان فتحي، 2011، "**إخفاء مستند نص وصورة في مقطع صوت wav**"، مشروع تخرج، علوم الحاسوب، كلية التربية، جامعة الموصل.