Suggested Method for Audio File Steganography

Saja J. Mohammed *Sj_alkado@uomosul.edu.iq*
Faris E. Mohammed *FarisEM@hotmail.com*
College of Computer Science and Mathematics
University of Mosul, Mosul, Iraq

Received on: 15/10/2012 **Accepted on: 30 /01/2013**

ABSTRACT

The world is tend now a lot of development in communication field specially in internet , therefore it is very important to find security methods for files that is send from one place to another. One of these security approaches is steganography which have characteristic of transfer massages within transmission media (files) without notice from any obtrusive. This paper provide anew suggested method for hiding text in audio file (wav file), first the text file will be read to extract the massage which is hidden, for more security this massage will be encrypted (or coded) before hiding it inside sound media (in time domain) . This algorithm was applied on more than one example and good results were obtained without missing the text massage or notice any noise in the cover file.

Keywords: audio file, text steganography, wav file .

طريقة مقترحة للإخفاء داخل ملفات الصوت

سجى جاسم محمد **فارس إدريس محمد**
كلية علوم الحاسوب والرياضيات
جامعة الموصل، الموصل، العراق

تاريخ استلام البحث: 2012/10/15 **تاريخ قبول البحث: 2013/01/30**

الملخص

نظراً لما يشهده العالم من تطور في مجال الاتصالات وخاصة عبر شبكة الانترنت أصبحت الحاجة ملحة إلى وجود طرق حماية للملفات التي يتم إرسالها من مكان إلى آخر. ومن بين أساليب هذه الحماية برز فن الإخفاء الذي يتميز بنقل الرسائل عبر وسائط النقل (الملفات) دون ملاحظة عملية النقل هذه من قبل أي متطفل.

يقدم البحث فكرة مقترحة لإخفاء النصوص داخل الملف الصوتي من نوع wav، إذ يتم أولاً قراءة ملف النص لاستخراج الرسالة المطلوب إخفاؤها ثم تشفير (ترميز) تلك الرسالة وإخفاؤها في ملف الصوت الغطاء وفي حيز الزمن، تم تطبيق الخوارزمية على أكثر من ملف صوتي وحققت نسبة استرجاع جيدة لبيانات الرسالة النصية ودون إحداث أي تشويه ملحوظ في الملف الغطاء.

الكلمات المفتاحية: الملف الصوتي، اخفاء النص ، ملف .wav

1- المقدمة:

مع نشوء وتطور علم الحاسوب والاتصالات ظهرت الحاجة الماسة إلى إيجاد وسائل أمنية تمنع قراصنة المعلومات أو ما يسمى بالـ (Hackers) من السطو على المعلومات المهمة والأمنية بشكل خاص مما يسبب نشرها أو التلاعب بمضمونها أو حتى حذفها، ومن الأمثلة على ذلك التلاعب بالأرصدة في بنوك الدولة وسرقتها،

وسرقة المعلومات العسكرية أثناء الحروب، فكان لابد من إيجاد وسائل أمنية ذو كفاءة عالية لغرض حماية المعلومات وخاصة على الانترنت فظهر نتيجة لذلك نظام حماية يعرف بإخفاء المعلومات (Information Hiding). [1][2]

من المعروف أن الحاسوب يقوم بتمثيل جميع البيانات ومنها الوسائط المتعددة (Multimedia) بالقيم الرقمية الثنائية، هذه التمثيلات غالباً ما تكون فيها مستويات رقمية ومناطق التغيير الطفيف في قيمها غير مدرك أو محسوس من قبل وسائل الإنسان الحسية كالسمع والبصر، وهكذا تتم الاستفادة من هذه الخصائص لإخفاء البيانات في الوسائط المتعددة وذلك بتبديل قيم هذه المواقع بقيم البيانات المراد إخفاؤها، مع مراعاة الحدود المقبولة لعملية التبديل وعدم تجاوزها لمنع حصول حالة الانحلال (Degradation) للوسائط الحاوية لها بطريقة يصبح فيها التغيير مدركاً ومحسوساً من قبل الإنسان.[3]

2- علم الإخفاء:

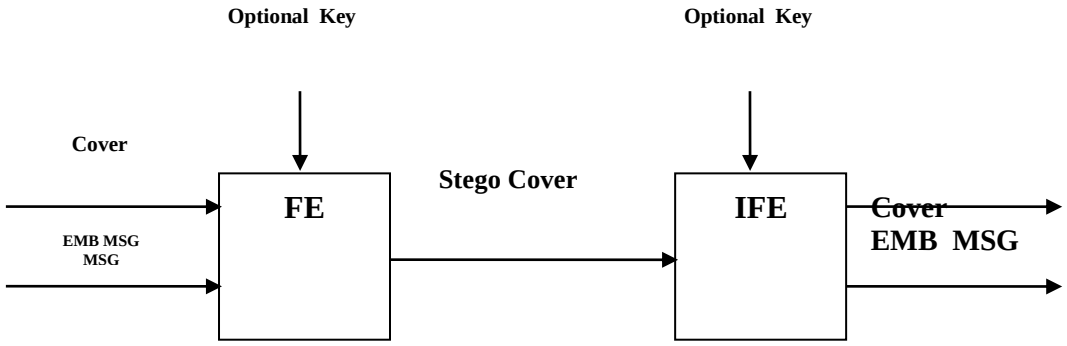
الإخفاء هو حجب البيانات عبر شبكات الاتصال باستخدام طرق تقي لهذا الغرض وهو يعمل على حجب البيانات ضمن غطاء كبير نسبيا كأن تكون صورة أو ملف صوتي أو فيديوي بحيث يكون غير مدرك كن قبل المتطفلين وهذا هو الفرق الأساسي بينه وبين التشفير الذي يقوم بتغير معالم الرسالة نفسها. يكمن هدف الإخفاء في تقليل احتمالية كشف احتواء الملف على رسالة سرية وكذلك تقليل الفرق بين بيانات الغطاء الأصلية وبياناته بعد عملية الإخفاء بالمقابل يجب أن تكون هناك زيادة في حجم الرسالة المنقولة عبر الغطاء [4][5].

يهتم علم الإخفاء 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. لذلك فإن علم الإخفاء يستخدم لعدة أسباب، والسبب الرئيسي هو لحماية الكتابة والمحافظة على خصوصية المعلومات، والسبب الثانوي هو لحفظ البيانات من محاولات سرقتها وذلك بإخفائها في وسط آخر [1][6].

وهناك أربعة عناصر في الإخفاء وهي [6] [7] [8]:-

1. **الناقل (carrier):** ويسمى غطاء "cover" ويمثل حامل الرسالة المخفية وهو أحد الوسائط المتاحة عديمة الأهمية، ويشار إليه بالحرف c.
2. **الرسالة السرية (secret message):** وهي الرسالة المراد إخفاؤها ويشار إليها بالحرف m.
3. **مفتاح الإخفاء (stego-key):** يستخدم كمستوى إضافي من السرية ويشار إليه بالحرف k، إن مفتاح الإخفاء لا يعتبر أساسي في نظام الإخفاء وإنما يستخدم لزيادة درجة السرية.
4. **وسط الإخفاء (stego-media):** ناتج عملية الإخفاء هذه الحصول على وسط الإخفاء الذي يضم الرسالة السرية ويشار إليه بالحرف s ويمكن تمثيل نظام التغطية بالمعادلة (1)[5] ويوضح الشكل (1) خطوات عملية الإخفاء بصورة عامة [8][9]:

$$c + m + k = s \quad \ldots(1)$$



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**

الشكل (1). خطوات عملية الإخفاء

وهناك بعض النقاط التي يجب توافرها في تقنية الإخفاء وهي [9]:

1. سلامة البيانات المخفية بعد أن يتم طمرها داخل الغطاء الناقل إذ يجب أن تكون صحيحة بعد استرجاعها.
2. الوسط الناقل للبيانات المخفية (الغطاء) يجب أن يبقى بدون أي تغيير ملحوظ.
3. بالنسبة للعلامة المائية فان أي تغيير في الغطاء يجب أن لا يؤثر على سلامة العلامة المائية.
4. يجب أن يؤخذ بنظر الاعتبار دائما أن المهاجم يعلم انه هناك بيانات مخفية داخل الغطاء.

أما الأوساط الرقمية التي تصلح أن تكون غطاء لإخفاء الرسائل فهي [10]:

- Plain Text.
- Digital Image.
- Audio.
- Video.
- IP Datagram.

3- الإخفاء في ملف الصوت:-

إن عملية إخفاء البيانات في إشارة الصوت يعد تحدياً خاصاً لأن نظام السمع البشري (HAS: Human Auditory System) يعمل بشكل ديناميكي واسع المدى من الترددات التي تقع بين (20Hz-20000Hz)، لذا فإن هذا النظام يكون حساس جدا لإضافة ضوضاء عشوائية، ومع ذلك فان هناك بعض الفجوات التي يمكن استغلالها في عملية الإخفاء وهي [3][11][12]:

1. الصوت ذو مدى تمايزي محدود وصغير ونتيجة لذلك فان الأصوات العالية تحجب الأصوات الواطئة أو الهادئة.
2. المسافات الصوتية المستوية تكون أكثر حساسية للتغير من المناطق عالية التردد.
3. النماذج الصوتية ذات القيمة العالية تحجب النماذج المتجاورة ذات القيمة الواطئة والمنخفضة.

هناك عدد من التقنيات التي يمكن أن تستخدم لإخفاء البيانات داخل ملفات الصوت منها [5][8][11]:

1. **LSB CODING** .
2. **PARITY CODING**.
3. **PHASE CODING**.
4. **SPREAD SPECTRUM**.
5. **ECHO HIDING**.

3-1- الإخفاء في الـbit الأقل أهمية (LSB CODING)

وهي طريقة مشهورة جدا وتعتمد مبدأ إلغاء قيمة الـbit الأقل أهمية في الملف الغطاء لإخفاء سلسلة من الـbits التي تكون الرسالة المخفية. في العمليات الحسابية فان قيمة الـbit الأخير من كل (byte) يعطي قيمة واحدة فقط (إما 1 أو 0) فهو يحدد ما إذا كان العدد هو فردي أو زوجي وأي اختلاف في قيمة هذا الـbit يولد فرق مقداره 1[5] .

ويتم إخفاء البيانات بالاعتماد على نوع الوسط ففي الوسائط الصورية والسمعية غالبا ما يتم تبديل الخلية الثنائية الأقل أهمية (Least Significant Bit) LSB أو الخليتين الأقل أهمية بخلية ثنائية لحرف من حروف الرسالة المراد إخفاؤها بعد تحويلها إلى كتل ثمانية من الـ (Bits)، أو يمكن إنجاز عملية الإخفاء للوسطين باحتواء المعلومات المخفية في موقع غير مستخدم مثل بادئة الملف ولكنها تعتبر من الطرائق الضعيفة لإمكانية تمييزها وصغر حجمها يتم الإخفاء في الصور حسب عمل نظام الرؤية البشري (Human Visual System) HVS فيتم حشر الرقم الثنائي (bit) عن المعلومات في مواقع تكون اقل ملاحظة، أو أن يتم توزيع الأرقام الثنائية (bit) من هذه المعلومات بصورة عشوائية داخل الصورة. أما في الملف الصوتي فيتم احتواء المعلومات المخفية في مستويات صغيرة قليلة الإدراك مثل الضوضاء (noise). [3]

4- الخوارزمية المقترحة للإخفاء:

تعتمد خوارزمية الإخفاء المقترحة على فكرة وجود الملف الصوتي الأصلي (الغطاء) لدى المرسل والمستلم للرسالة في الطرف الآخر، وهي تعتمد أيضا فكرة إبدال الـbit الأقل أهمية (LSB) لكن بأسلوب جديد وهو استخدام بوابة xor المنطقية مع الـ bit الأقل أهمية واعتماد نواتجها بدلا من إبدال bit من الغطاء مع bit الرسالة المخفية (أي عملية التعويض).

تتكون الخوارزمية المقترحة للإخفاء من مرحلتين:

1. تضمين الرسالة النصية داخل الغطاء.
2. استرجاع الرسالة.

4-1- المرحلة الأولى (تضمين الرسالة):

في هذه المرحلة يتم تضمين الرسالة النصية داخل الغطاء (الملف الصوتي) وهذه المرحلة تتكون من عدة خطوات يمكن تفصيلها بما يلي:

4-1-1- تهيئة الغطاء:-

وتضم:

أ. قراءة الملف الصوتي.

ب. خزنه في مصفوفة أحادية والتي تضم قيم العينات الصوتية ممثلة بنظام (double).

ت. إيجاد طول الملف الصوتي (عدد عينات الصوت) وليكن L.

ث. إيجاد الجذر التربيعي للعدد L وليكن n.

ج. تكوين مصفوفة مربعة ثنائية الأبعاد (n*n) من مصفوفة الصوت الأحادية الناتجة من الخطوة (ب)، كما موضح في الشكل (2)، فلو كان طول الملف الصوتي (45600) عينة (sample) ستكون أبعاد المصفوفة الناتجة (213 × 213) لكون العدد (213) هو ناتج إيجاد الجذر التربيعي للعدد (45600).

وفي كثير من الأحيان يكون هناك قيم متبقية من مصفوفة الصوت يتم الاحتفاظ بها لإعادتها إلى الملف الناتج بعد إتمام عملية الإخفاء، حسب المثال السابق سيكون المتبقي من ملف الصوت هو(231) عينة وهو الناتج من طرح ناتج تربيع n من L.

0	0	0
-0.3438	-0.2813	-0.1641
-0.1953	-0.2891	-0.3047
0.0703	0.0156	-0.0078
0.2188	0.1172	0.0234
0.1953	0.2188	0.2734
-0.0547	-0.1094	-0.1406
0.1016	0.1094	0.0156
-0.3281	-0.0625	0.0938

شكل (2). يمثل شكل العينات الصوتية ممثلة بنظام double بعد تحويلها إلى مصفوفة مربعة

4-1-2- تهيئة الرسالة النصية:-

لغرض زيادة سرية الخوارزمية المقترحة تم عمل شفرة خاصة للنص وذلك بإجراء العمليات الآتية لترميز النص المرسل قبل عملية الإخفاء:-

أ. قراءة الرسالة النصية من ملف نصي (.txt)، ولتكن الرسالة على سبيل المثال

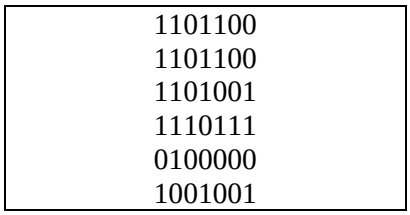
"I will be there"

ب. تحويل النص إلى Binary كما في الشكل (3) وستتكون من هذه الخطوة مصفوفة ثنائية أبعادها x*8 إذ أن x يمثل عدد أحرف الرسالة و8 هو عدد الـ(bits) التي تمثل كل حرف

message =
1001001
0100000
1110111
1101001
1101100
1101100

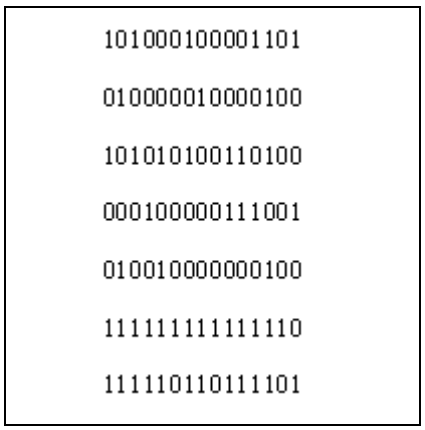
شكل (3). جزء من النص بعد تحويله إلى مصفوفة Binary

ج. قلب المصفوفة أعلى أسفل (up-down) بحيث يتم تبديل آخر سطر مع أول سطر والسطر ما قبل الأخير مع الثاني وهكذا، كما في الشكل (4).



شكل (4). جزء مصفوفة Binary بعد قلبها (أعلى أسفل)

د. تدوير المصفوفة الناتجة من الخطوة ج بزاوية قدرها 90^o كما موضح في الشكل (5)، ومن البديهي أن تكون أبعاد المصفوفة الناتجة هي8*x



شكل (5). جزء من مصفوفة Binary بعد تدويرها بـ 90^o.

هـ. تحويل المصفوفة الناتجة إلى مصفوفة أحادية لتكون هي عبارة عن سلسلة الـ (bits) التي سيتم إخفاؤها في الملف الصوتي وهو موضح في الشكل (6).

10100110100111101001100010110010111000001010100110100011000001000110110011011100101111101110000010100100 1

شكل (6). الرمز الناتج للرسالة النصية والذي سيتم إخفاؤه داخل ملف الصوت

4-1-3- عملية التضمين:-

بعد عملية تهيئة كل من الغطاء والرسالة المنقولة تبدأ عملية التضمين والتي تعتمد على فكرة الإخفاء داخل عينات المثلث السفلي فقط ضمن مصفوفة الصوت المربعة والناتجة من مرحلة تهيئة الغطاء، تتضمن عملية التضمين الخطوات الآتية:-

أ. قراءة bit من الرسالة المشفرة.
ب. قراءة عينة من ضمن العينات الواقعة في المثلث السفلي من المصفوفة الثنائية الأبعاد للوسط الناقل.
ج. تحويل هذه الصيغة إلى النظام الثنائي بسعة bit 16 لكل عينة.
د. إجراء عملية (xor) بين الـ (bit) الذي تم الحصول عليه من الرسالة وبين الـ (bit) ذي التسلسل الأخير ضمن المواقع المعتمدة من المصفوفة (وهي المثلث السفلي فقط منها).
ه. إعادة الخطوات (أ، ب، ج، د) إلى حين انتهاء الرسالة المنقولة.
و. تحويل المصفوفة الناتجة من مصفوفة ثنائية مربعة إلى مصفوفة أحادية، ومن ثم إعادة الجزء المتبقي من الملف الصوتي (إن وجد) إلى نهاية المصفوفة الناتجة.

ز. إيجاد عدد حروف الرسالة المخفية (بضمنها الفراغ) وإخفاءها في آخر 8 عينات من الملف الصوتي (على فرض انه أكثر عدد ممكن لأحرف الرسالة هو256 حرف) أما أسلوب الإخفاء المتبع فهو التعويض في الـ(bit) الأقل أهمية وكما يلي:

1. تحويل طول النص إلى الرمز الثنائي.
2. اعتماد العينة ذي التسلسل L (والذي يمثل طول الملف الصوتي).
3. تحويلها إلى التمثيل الثنائي.
4. إبدال الـ(bit) الأخير منها بالـ(bit) ذي التسلسل b من الرمز الثنائي لعدد أحرف الرسالة، إذ يمثل b أول bit من العدد.
5. إعادة العينة إلى الرمز العشري.
6. زيادة b بمقدار 1 ونقصان L بمقدار 1
7. تكرار الخطوات (2 –5) إلى أن تصبح قيمة b =8.

4-2- المرحلة الثانية (استرجاع الرسالة): وتتضمن:

أ. قراءة الملف الصوتي وتحويله إلى مصفوفة أحادية البعد.

ب. استرجاع عدد حروف الرسالة من آخر 8 عينات من الملف الغطاء بنفس الخطوات التي تم ذكرها سابقا لخزن عدد حروف النص مع تغيير بسيط هو استرجاع الـ(bit) الأخير من العينة بدلا من إبداله بقيمة أخرى.

ج. تحويل العدد الناتج من الاسترجاع إلى الرمز العشري ليتم معرفة عدد حروف النص.

د. إيجاد طول الملف الصوتي المرسل (L) واستخراج الجذر التربيعي له (n).

ه. تحويل مصفوفة الملف الصوتي المرسل إلى مصفوفة ثنائية الأبعاد مربعة بالأبعاد (n*n).

و. اعتماد ملف الصوت الأصلي الموجود لدى المستقبل وتحويله أيضا إلى مصفوفة مربعة وبنفس الأبعاد (n*n)، مع الأخذ بنظر الاعتبار احتمال وجود بقية في ملف الصوت ومعالجتها بنفس الأسلوب المتبع للإخفاء.

ز. إجراء عملية xor بين ملف الغطاء والملف الأصلي لجميع القيم الموجودة في المثلث السفلي بعد تحويله إلى النظام الثنائي.

ح. استخراج الرسالة من الملف الغطاء باعتماد نواتج استخدام الدالة المنطقية xor.

ط. تكرار عملية الاسترجاع حسب طول الرسالة المخفية وتكوين سلسلة من الـ(Bits) وحسب المثال المعطى ستكون سلسلة الـbit الناتجة كما هي موضحة بالشكل (7).

10100110100111101001100010110010111000001010100110100011000001000110110011011100101111101110000010100100 1

شكل (7). سلسلة الـ Bits الناتجة من عملية الاسترجاع

ي. تحويل سلسلة الـbits الناتجة إلى مصفوفة ثنائية البعد بحيث يكون فيها عدد الأسطر 8 (عدد الـbits التي تمثل كل حرف) وعدد الأعمدة بعدد أحرف النص المخفي والتي تم استرجاعها من نهاية الملف بالخطوة (ب) وكما موضح بالشكل (8).

1010001000011101
0100000100000100
1010101001101100
0001000000111001
0100100000000100
1111111111111110
1111101101111101

شكل (8). مصفوفة الرسالة المخفية بعد تحويلها إلى مصفوفة ثنائية

ك. إجراء الخطوات المعاكسة لعملية الترميز (التدوير بزاوية مقدارها 90 وقلب الناتج (أعلى وأسفل) وكما موضح في الشكل (9) .

1001001	1101100
0100000	1101100
1110111	1101001
1101001	1110111
1101100	0100000
1101100	1001001
ب	أ

الشكل (9). أ. المصفوفة بعد تدويرها بمقدار 90[5] ب. المصفوفة بعد قلبها أعلى وأسفل

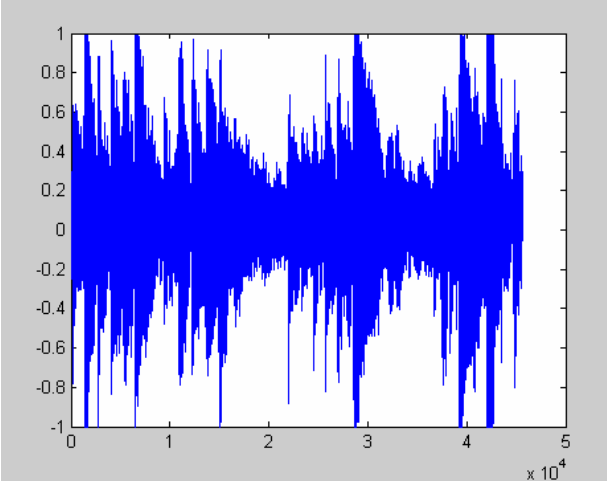
ل. تحويل كل سطر من المصفوفة الناتجة إلى حرف نصي وبالتالي استرجاع الرسالة المخفية كاملة وهي "I will be there"

5- النتائج:

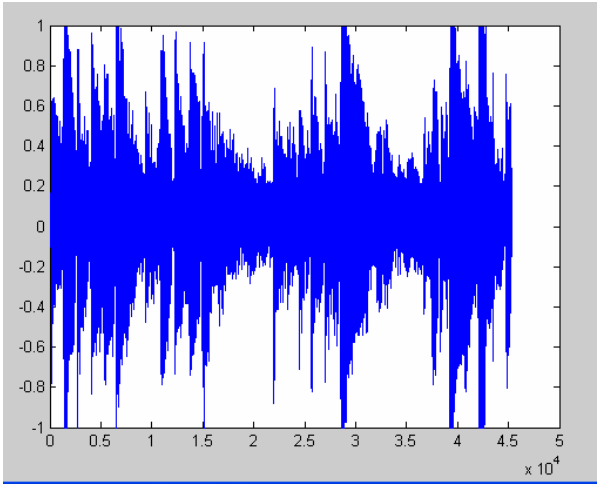
تم تطبيق الخوارزمية المقترحة على أكثر من ملف صوتي من نوع (wav) وبأحجام مختلفة واستخدمت مقاييس عديدة منها mse مربع نسبة الخطأ (mean squared error) وcor عامل الارتباط (correlation) وBER (bit error rate) و mae (mean absolute error) وكانت النتائج كما موضحة في الجدول (1) إذ لم يكن هناك أي تشويه واضح في الملف الصوتي وكذلك تم استرجاع الرسالة النصية كاملة، وكما في الأشكال الموضحة أدناه إذ يبين الشكل (10) شكل إشارة الملف الصوتي قبل الإخفاء بينما يوضح الشكل (11) شكل هذه الإشارة بعد عملية الإخفاء، وكذلك بالنسبة للشكلين (12) و(13) اللذان يمثلان إشارة صوت لملف صوتي آخر قبل وبعد الإخفاء على الترتيب.

جدول (1). نتائج تطبيق الخوارزمية المقترحة على ملفات صوتية مختلفة

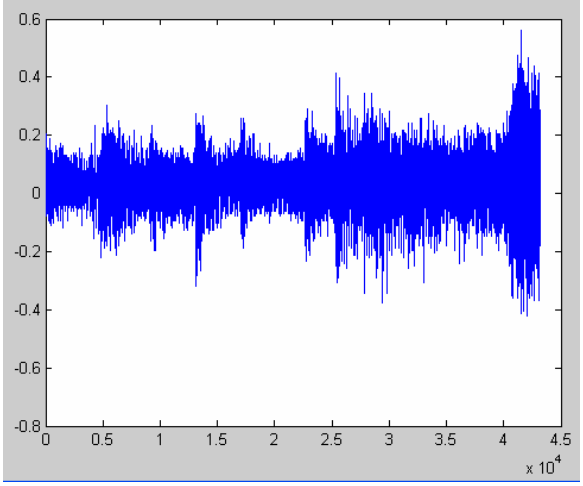
اسم الملف	حجمه	Mse	cor	Mae	BER
P31	42.2KB	2.8586e-001	1	1.9493e-007	zero
A1	31.2KB	3.8706e-008	1	3.6204e-005	zero
P32	44.5KB	1.6961e-010	1	4.1300e-007	zero
A2	46.9KB	2.3372e-008	1	2.1143e-005	zero



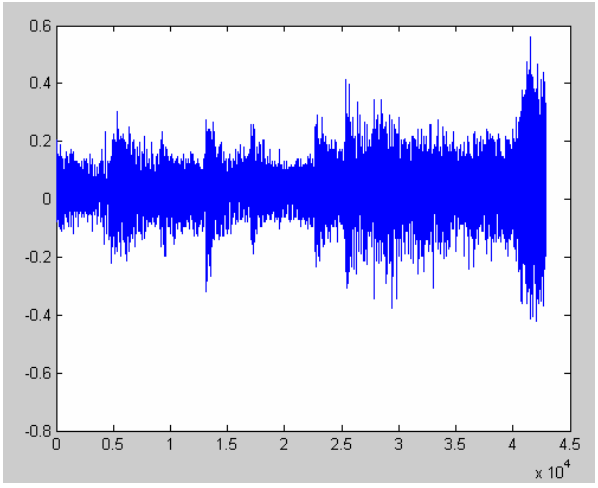
شكل (10). يوضح إشارة الصوت للملف(P31) قبل الإخفاء



شكل(11). يوضح إشارة الصوت للملف (P31) بعد الإخفاء



شكل (12). يوضح إشارة الصوت للملف (P32) قبل الإخفاء



شكل (13). يوضح إشارة الصوت للملف (P32) بعد الإخفاء

من الأشكال والجدول أعلاه نلاحظ أن الخوارزمية المقترحة تحافظ على سلامة البيانات المنقولة لكون قيمة نسبة الخطأ في الـbits هي صفر وهي تحافظ أيضا على بقاء الإخفاء في الملف الصوتي غير مدرك بالعين أو الإذن البشرية وهذا يتضح من قيم نسب مربع الخطأ (mse, mae) وبقاء معامل الارتباط بين الغطاء الأصلي قبل الإخفاء والغطاء بعد الإخفاء أعلى ما يمكن (قيمته 1)، وهذا ما يبين كفاءة الخوارزمية المعتمدة.

المصادر

[1] سلو، اميريبيد، (2009)، "تقنيات إخفاء المعلومات باستخدام الشبكات العصبية وبروتوكولات الشبكة"، بحث ماجستير في علوم الحاسوب.

[2] Cacciaguerra Stefano and Ferretti Stefano, (2000), "Data hiding steganography and copyright marking", university of Bologna. Italy.

[3] Stefan Katzenbeisser Fabin A.P. Petitcolas, "Information Hidding Techniques for Steganography and Watermarking".

[4] Bhavana.S and K.L.Sudha,(2012)"TEXT STEGANOGRAPHY USING LSB INSERTION METHOD ALONG WITH CHAOS THEORY", arXiv, IVSL.

[5] Athawale , A.,etal. ,(2010),"Information Hiding in Audio Signals", *International Journal of Computer Applications (0975 – 8887), Volume 7– No.9,IVSL.*

[6] الصميدعي، عامر تحسين سهيل، (2002)، "تطبيق نظام التغطية"، بحث ماجستير قسم علوم الحاسوب والرياضيات– جامعة الموصل– العراق.

[7] lyenyar, V., (2003), "Hiding messages in Images & Test: Risk Associated with the Technology of steganography", InfoBytes Journal.

[8] Jayaram. P, etal. H.S., (2011), "Information Hiding Using Audio Steganography – A Survey", The International Journal of Multimedia & Its Applications (IJMA) Vol.3, No.3, IVSL.

[9] Channalli, S., etal., (2009), "Steganography An Art of Hiding Data", International Journal on Computer Science and Engineering Vol.1(3), 137-141, IVSL.

[10] Borgohain, R., (2012), "Data Hiding Techniques using number decompositions, 2012, IVSL.

[11] الحمامي، علاء حسين والحمامي محمد علاء، (2008)، "إخفاء المعلومات ، الكتابة المخفية والعلامة المائية، أثراء للنشر والتوزيع.

[12] الجواهري، شيماء شكيب محمد يحيى، (2004)، "الإخفاء في ملف مكبوس"، بحث ماجستير، قسم علوم الحاسوب– كلية علوم الحاسوب والرياضيات– جامعة الموصل.