إخفاء نص في ملف الصوت WAV

إيمان فتحي احمد
قسم الحاسوب / كلية التربية
جامعة الموصل

الاستلام	القبول
٠٩ / ٠١ / ٢٠١١	٢٨ / ٠٦ / ٢٠١١

Abstract

Digital communications and information security has become one of the key issues to send data, there are two techniques available to achieve this goal: Encryption And concealment of information, the goal of this research is the application of technical system coverage within the audio file and the way is to change the cell bilateral least important (Low Bit Encoding) file that has been chosen here is the file named WAV used as a cover for the transfer of data, using three algorithms for this purpose, followed by a Testing Statistical and so on methods of measuring the minimum square error, in addition to measuring the proportion of noise to the original signal, was to illustrate the results within the practical side of using the MATLAB version of 10, tests showed that the concealment algorithm using the secret key to give the best results

المستخلص

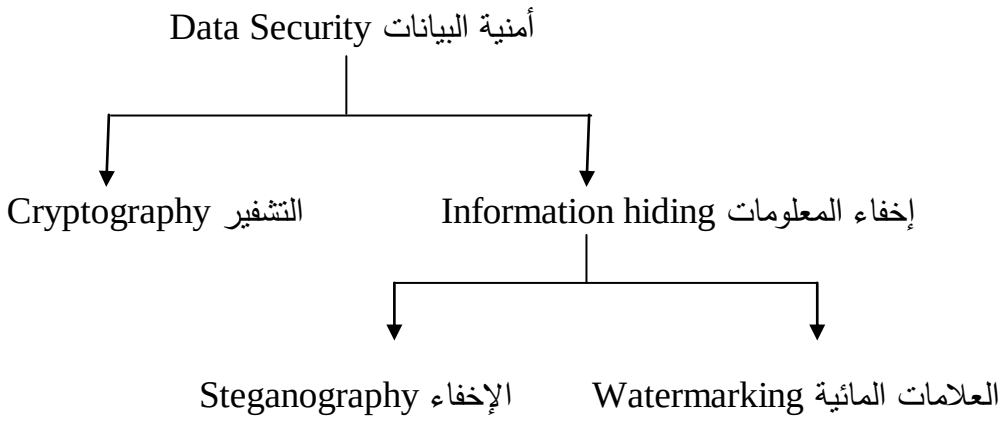
الاتصالات الرقمية وأمنية المعلومات أصبحت من المسائل الأساسية لإرسال البيانات ، يوجد اثنين من التقنيات المتاحة لتحقيق هذا الهدف : التشفير وإخفاء المعلومات ، الهدف من هذا البحث هو تطبيق تقنية نظام التغطية داخل ملف الصوت والطريقة هي تغيير الخلية الثنائية الأقل أهمية (Low Bit Encoding)، الملف الذي تم اختياره هنا هو الملف المسمى WAV الذي استخدم كغطاء لنقل البيانات، استخدمت ثلاثة خوارزميات لهذا الغرض، تلا ذلك إجراء الاختبارات الإحصائية وذلك عن طرق قياس الحد الأدنى لمربع الخطأ، بالإضافة إلى قياس نسبة الضوضاء إلى الإشارة الأصلية، تم توضيح النتائج ضمن الجانب العملي باستخدام ماتلاب الإصدار العاشر ، أظهرت الاختبارات ان خوارزمية الإخفاء باستخدام المفتاح السري تعطي أفضل النتائج.

١- المقدمة

الاحتمالات المتزايدة لأجهزة الاتصالات الحديثة وتطبيقات الوسائط المتعددة على شبكات الاتصال أدى إلى زيا دة الحاجة لتوفير طرائق كفوءة تعمل على حماية البيانات، لذلك كان لابد من ظهور وسائل تعمل على توفير أمن لهذه الوسائط لحمايتها من السراق و المتطفلين من العبث بها وتحريفها أو سرقتها و نشر المعلومات الحساسة منها، من هنا ظهرت الحاجة إلى توفير وسائل أمنية البيانات لذا ظهر علم خاص بها يسمى علم التشفير وبالرغم من كونه طريقة جيدة لحفظ المعلومات إلا انه سهل الاكتشاف ويمكن لأي متطفل التلاعب به فكانت الحاجة إلى تقنية أكثر تطورا وأكثر سرية حفاظا على المعلومات وخصوصا مع ظهور وتطور شبكة الانترنيت فتم اللجوء إلى نظام التغطية الذي يعتمد على مبدأ ان الرسالة المرسلة تكون غير مرئية لأي شخص بواسطة إخفاءها داخل إحدى وسائل الاتصال (الصوت ، الصورة والنص ، الفيديو)[8][4].

٢- تقنية أمنية البيانات (Data Security Technique):

تعتبر أمنية البيانات (Data Security) من الاحتياجات المهمة في أن ظمة الحاسبات وهي نتيجة مباشرة للاستخدام المتزايد للحاسبة ، تصنف أمنية البيانات وكما موضح في الشكل (١) إلى صنفين [5]:



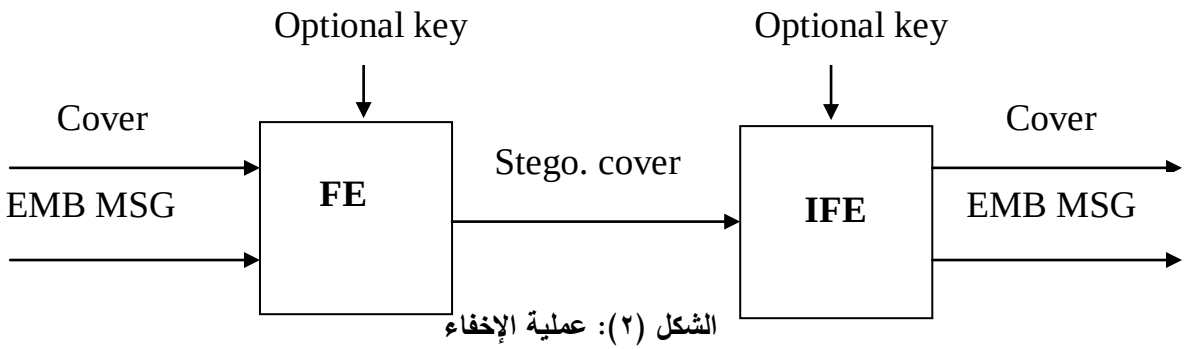
الشكل (١): يوضح التقسيم العام لتقنية أمنية البيانات

٢-١ التشفير Cryptography

علم التشفير (Cryptography) هو العلم الذي يعنى بالطرق التي تجهزنا بحماية خزن المعلومات ونقلها في مجال واسع، وهذه الطرق تعتمد على مفتاح سري يستخدم لتشفير البيانات [2][10].

٢-٢ الإخفاء (Steganography) أو نظام التغطية (Cover Writing):

وهو فن إخفاء ونقل البيانات خلال بيانات أخرى كمضيف (host) أو حامل (carrier) بطريقة غير مؤذية للجمل المخفية، حيث تعمل على إخفاء وجود أية اتصالات سرية وبذلك تمنع أي عدو أو مراقب من اكتشاف وجود بيانات سرية ومخفية . إن النموذج الأساسي في نظم الإخفاء يكون كما في الشكل (٢) الذي يوضح عملية الإخفاء.



الشكل (٢): 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**

ان الدالة الحاملة (cover) قد تكون (صورة، صوت، فديو، نص) والذي سيقوم باحتواء المعلومات المراد إخفاءها (EMB MSG)، أما المعلومات المراد إخفاءها (EMB MSG) من الممكن إن تكون نصا مشفرا أو صورة أو أي شيء يمكن إدخاله إلى سيل البتات، إن المعلومات المخفية تحتاج إلى مفتاح إخفاء والذي هو عبارة عن معلومات سرية إضافية مثل كلمة العبور والتي تكون محتاجة لعملية إدخال المعلومات[7][6][5] .

3- برمجة ملف WAV مع نظام التغطية

إن الملفات السماعية من نوع WAV هي من صيغ الصوت المستخدمة من قبل شركة Microsoft تحت بيئة النظام Windows وهي من الصيغ الشائعة و الأكثر استخداما ، وتعرف هيئة الملف العامة RIFF (Resource Interchange File Format) التي نظمت بشكل مقاطع متداخلة مع بعضها البعض . إن الملفات السماعية من نوع WAV لا تحوي فقط القيمة الرقمية للعينة وإنما تحوي معلومات توصف وتعرف صيغة البيانات السمعية .لاستعادة هذا النوع من الملفات تقوم أنظمة الوسائط المتعددة بفتح الملف ومن ثم قراءته وتفسيره عن طريق المعلومات الموجودة في بداية الملف ، ثم تحمل البيانات السمعية على الذاكرة بعدها يتم فتح الجهاز السماعي وتشغيل الملف الصوتي ، ويتم غلقه باستخدا م نفس الجهاز . قبل فتح الملف

يجب معرفة بعض البيانات الخاصة بالملف ، منها نسبة التعيان ، ونوع القناة المستخدمة سواء كانت (Mono Or 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 بأربعة رموز أو كتل ثمانية وهي ("fmt" List " data") (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" الذي يحوي معلومات عن صيغة الـ PCM حيث أن PCM هو 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 Chunkيساوي الرقم الكلي لمجموع الـ bytes المكونة للمقطع الجزئي "fmt" و المقطع "data". بعض ملفات الـ RIFF تحوي المقطع List الذي يحوي معلومات أخرى مثل ملاحظات عن النسخة الأصلية للملف وتعريف بيانات المستخدم التي تصف المحتويات كما مبين الجدول(١)[1][3] [11].

جدول(١): هيكلية ملف WAV

Size Information In byte	Offset	Contains	Description
4	0	"RIFF"	Signature for resource interchange file format
4	4	size	Total file size- 8
4	8	"WAVE"	Signature for audio RIFF file
4	12	"fmt ∇ "	After it information about the sound
4	16	16/18	Size of info after this location
2	20	Compression code	Usually 1=PCM:0 not compressed
2	22	Number of channels	1 mono, 2 stereo
4	24	Samples per second	The sampling rate of the file
4	28	Bytes per second	Number of bytes per second
2	32	Sample size in bytes	Size of sample in bytes
2	34	Sample size in bits	Size of sample in bits
2	36	Reserved	This location is exist if offset 16 contain 18
4	36/38	"data"	Chunk type data
4	40/42	Length of sound data	The length of the sound data in bytes
Length of data	N	Signal	Actual sound samples

4- طرائق إخفاء البيانات:

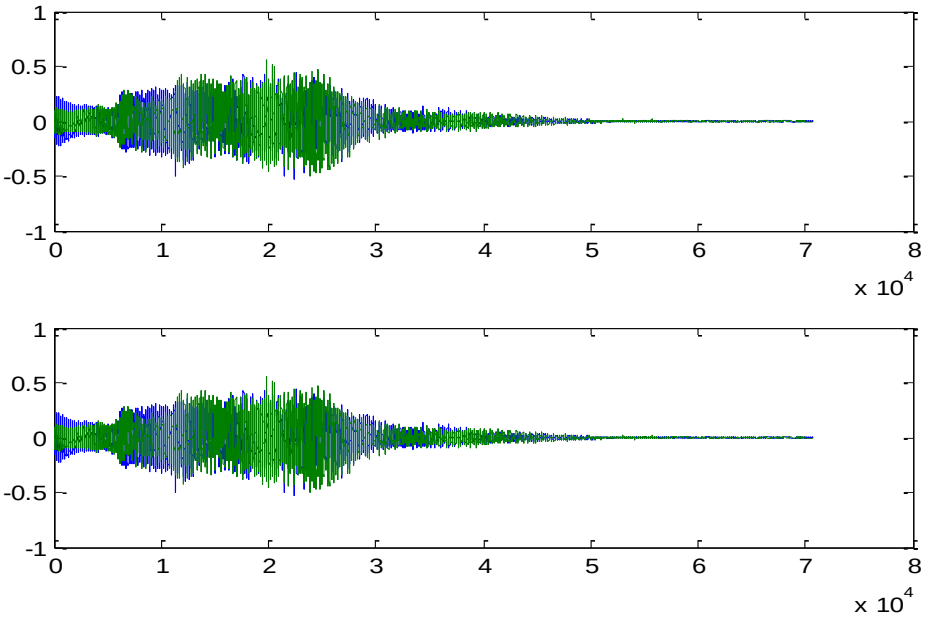
يتم إخفاء البيانات بالاعتما د على نوع الوسط . ففي الوسائط الصورية والسمعية غالبا ما يتم تبديل الخلية الثنائية الأقل أهمية (Least Significant Bit) LSB أو الخليتين الأقل أهمية 2LSB بخلية ثنائية لحرف من حروف الرسالة المراد إخفاؤها بعد تحويلها إلى كتل ثمانية من البتات، أو يمكن إنجاز عملية الإخفاء للوسطين باحتواء المعلومات المخفية في موقع غير مستخدم مثل بادئة الملف ولكنها تعتبر من الطرائق الضعيفة لإمكانية تمييزها وصغر حجمها يتم الإخفاء في الصور حسب عامل 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 (bits) من هذه المعلومات بصورة عشوائية داخل الصورة .أما في الملف الصوتي فيتم احتواء المعلومات المخفية في مستويات صغيرة قليلة الأدراك مثل الضوضاء (noise). على العكس من ذلك الإخفاء في النص الذي عادة ما يحوي معلومات إضافية قليلة ، هذه المعلومات يتم استخدامها في الاتصالات السرية لذلك يتم إخفاء البيانات التي غالبا ما تكون رسالة نصية عن طريق استغلال الفراغات بين الكلمات والجمل للنص الحامل حيث تمثل (0) بفراغ واحد و (1) بفراغين ، وغالبا ما يتم اكتشاف الإ خفاء في هذا النوع نتيجة التغييرات الحاصلة بالنص الحامل مقارنة مع النص الأصلي .هناك طريقة أخرى للإخفاء هي مناطق القرص عن طريق إيجاد مواقع غير مستخدمة أو غير منظورة من قبل المتطفل ، أو استخدام مواقع محجوزة تحمل معلومات عن الغطاء لإخفاء معلومات فيها دون تأثير ملموس على الملف الحامل [٩] [١٥][12].

٤-١ خوارزمية الإخفاء بتغيير الخلية الأقل أهمية باستخدام مفتاح سري.

في هذه الخوارزمية تم بناء نظام لتغيير كل بت Bit من كل بايت Byte، تبدأ خطوات الخوارزمية بفحص شرط قبول الحجم للرسالة المخفية بالنسبة لحجم ملف ال غطاء، في حالة عدم مطابقة شرط الحجم يتم الخروج من الخوارزمية بسبب كبر حجم الملف بالنسبة الى ملف الغطاء . اما في حالة تحقق الشرط يتم إجراء عملية الإخفاء ، حيث تم استخدام ملفات من نوعً WAV لتطبيق الخوارزمية كما في الشكل (٤،٥)[13].

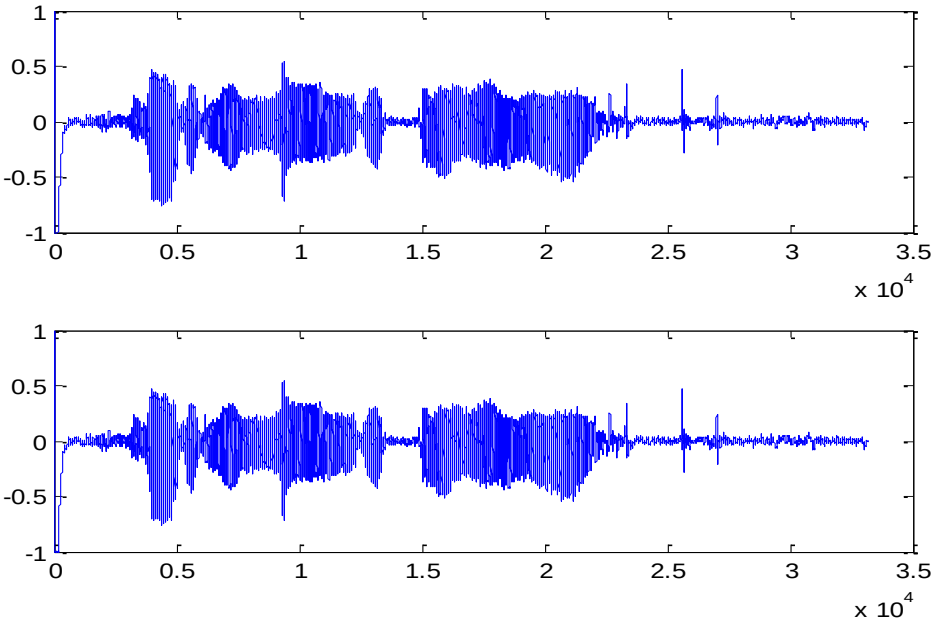
استدعاء دالة قراءة من ملف الغطاء

١. ملف صوت WAV يمثل مقطع موسيقى، بنسبة تعيان 22050 kHz وبتمثيل 16 bits، وبمقياس، حجم الملف 70641 KByte،



شكل(٤): يمثل تغيير بت لكل بايت

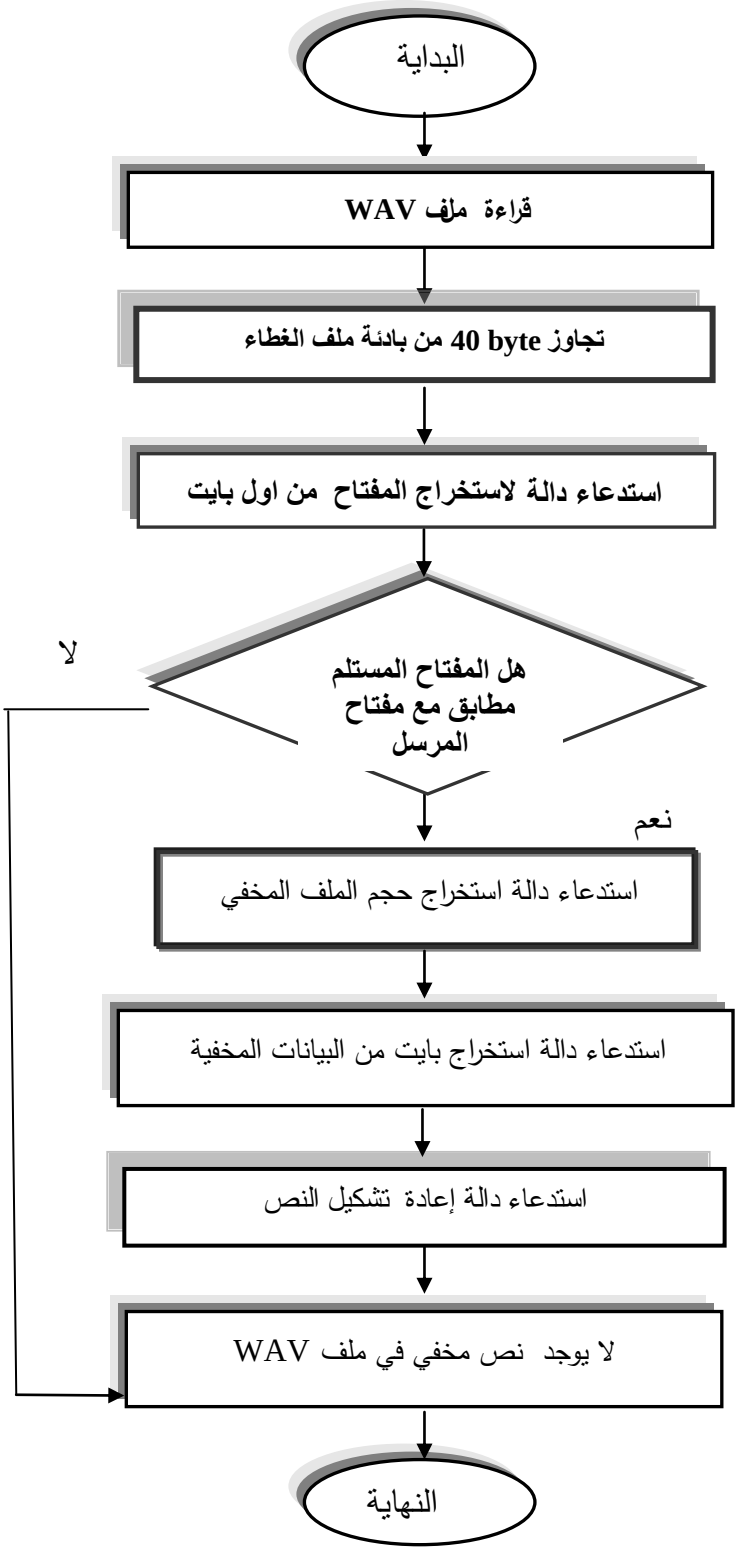
٢. ملف صوت WAV يمثل كلمة بسم الله الرحمن الرحيم، بنسبة تعيان 11025kHz وبتمثيل 16 bits، حجم الملف 33215 KByte،



شكل(٥): بت لكل بايت

٤-١-٢ استعادة الرسالة المخفية

عملية فك الإخفاء تتم باستعادة حجم الملف المخفي ومن ثم قراءة اول بايت الذي يمثل قيمة المفتاح المحدد من قبل الطرفين المرسل والمستقبل ثم تتم استعادة حروف الرسالة . المخطط (٦) الآتي يوضح الطريقة العامة لفك الإخفاء.

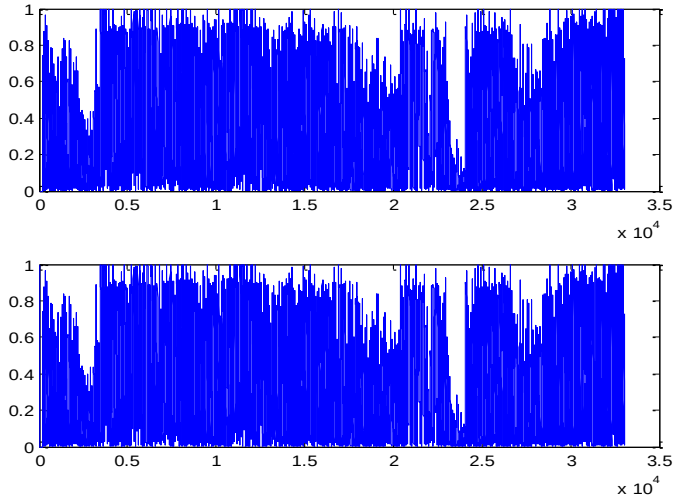


شكل(٦): يمثل مخطط انسيابي لعملية فك لاخفاء

٤-٢ خوارزمية الإخفاء بتغيير الخلية الأقل أهمية في أول بايت من الجزء الحقيقي لملف الصوت.

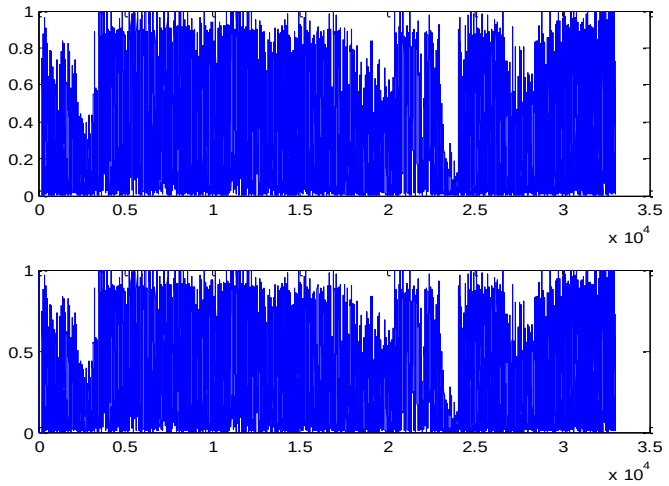
في هذه الخوارزمية تم بناء نظام لتغيير كل بت Bit من أول بايت Byte في الجزء الحقيقي من ملف الصوت ، تبدأ خطوات الخوارزمية بفحص شرط قبول الحجم للرسالة المخفية بالنسبة لحجم ملف الغطاء ، في حالة عدم مطابقة شرط الحجم يتم الخروج من الخوارزمية بسبب كبر حجم الملف بالنسبة الى ملف الغطاء . اما في حالة تحقق الشرط يتم إجراء عملية الإخفاء. كما مبين في الأشكال (٧،٨).

١ – ملف صوت WAV يمثل مقطع من ملف اغنية ، بنسبة تعيان 8000kHz وبتمثيل 16 bits، حجم الملف 33075 Kbyte.



شكل(٧): يمثل قبل وبعد الإخفاء في LSB

٢ – ملف صوت WAV يمثل مقطع من ملف اغنية، بنسبة تعيان 8000kHz وبتمثيل 16 bits، حجم الملف 33075 Kbyte.

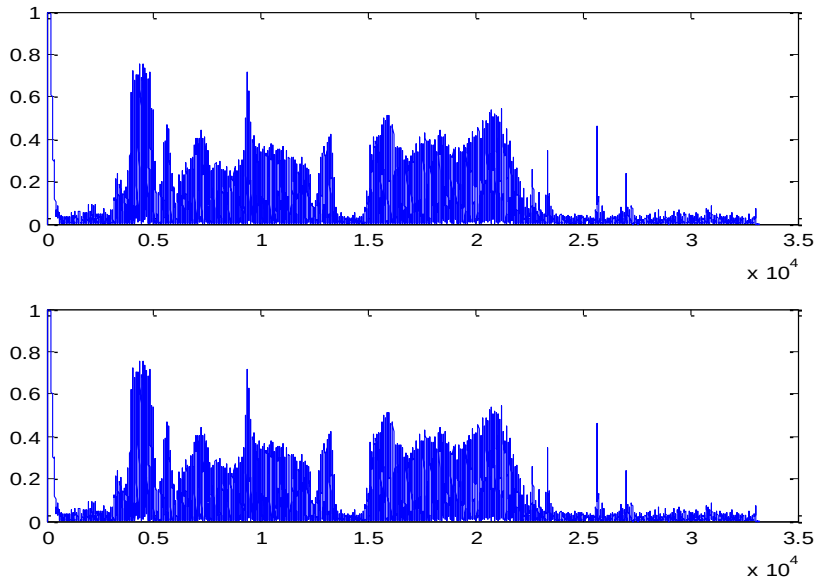


شكل (٨) :

٤-٣ خوارزمية الإخفاء بتغيير الخليتين الأقل أهمية 2LSB في الجزء الحقيقي من ملف الصوت.

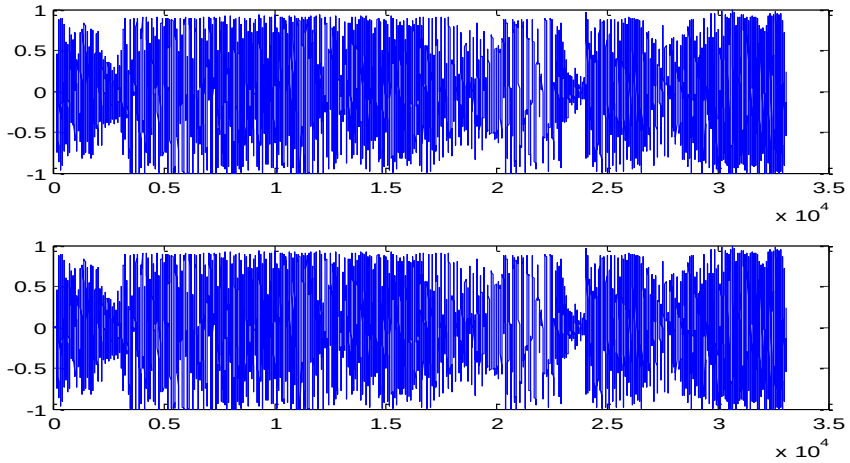
في هذه الخوارزمية تم بناء نظام لتغيير كل بت 2Bit من كل بايت Byte،هنا عملية الاخفاء مشابهة للطريقة السابقة ماعدا مطابقة شرط الحجم كما في الاشكال (٩،١٠).

١ – ملف صوت WAV يمثل كلمة الحمد لله رب العالمين ، بنسبة تعيان 11025kHz وبتمثيل 16 bits، حجم الملف 33215 Kbyte



شكل(٩) : يمثل قبل وبعد الاخفاء في 2LSB

٢ -ملف صوت WAV يمثل كلمة الحمد لله رب العالمين ، بنسبة تعيان 11025kHz وبتمثيل 16 bits، حجم الملف 33215 KByte



شكل(10) : يمثل قبل وبعد الاخفاء في ٢LSB

٥- الاختبارات الإحصائية

تم تقييم طرق الاخفاء بوساطة الاختبارات الاخصائية ، فـي الاختبارات الاحصائية تستخدم طرق رياضية . توجد عدة انواع من الاختبارات الاحصائية اهمها[13]:

أولاً: ايجاد اقل قيمة لمربع الخطأ (Minimum Squared Error) بين اشارة الادخال وبين اشارة الاخراج كما موضح في المعادلة (١)

$$\mathrm{MSE} = \frac{\sum_{MN} \left[I_i(m,n) - I_{21}(m,n) \right]^2}{M * N} \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

حيث تمثل M و N عدد الاعمدة والاسطر لاشارة ، ويمثل $I_i(m,n)$ و $I_{21}(m,n)$ اشارة الادخال والاخراج.

ثانياً: قياس نسبة الضوضاء **peak signal-to-noise ratio**

$$PSNR = 10\log_{1o}\left[\frac{R^2}{MSE}\right] \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2)$$

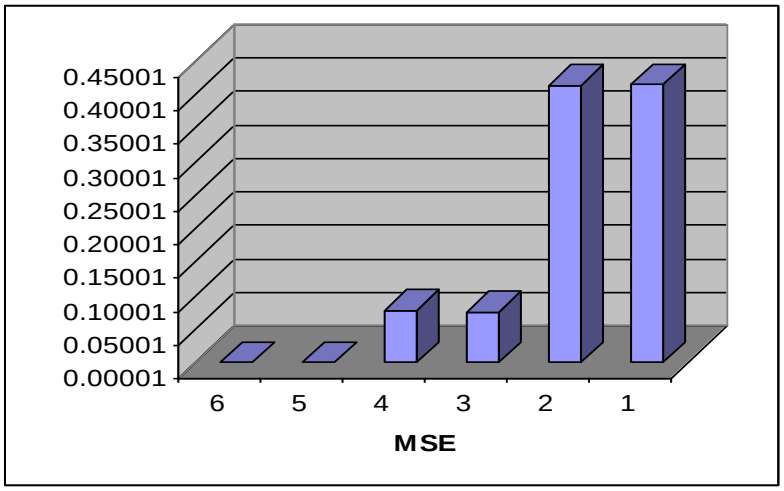
حيث تمثل R^2 قيم البيانات اذا كانت Floating point او Unsigned integer

جدول(٢): يمثل قيم الاختبارات الاحصائية

algorithm	SNR	MSE	PSNR
LSB by using key algorithm (1)	150.7858	1.8919e-012	117.2310
	35.0342	7.4304-e012	111.2892
LSB algorithm (2)	55.7563	0.4153	3.8160
	63.8656	0.4149	3.8206
2LSB algorithm (3)	5.2575	0.750	11.2488
	25.2432	0.0774	11.1142

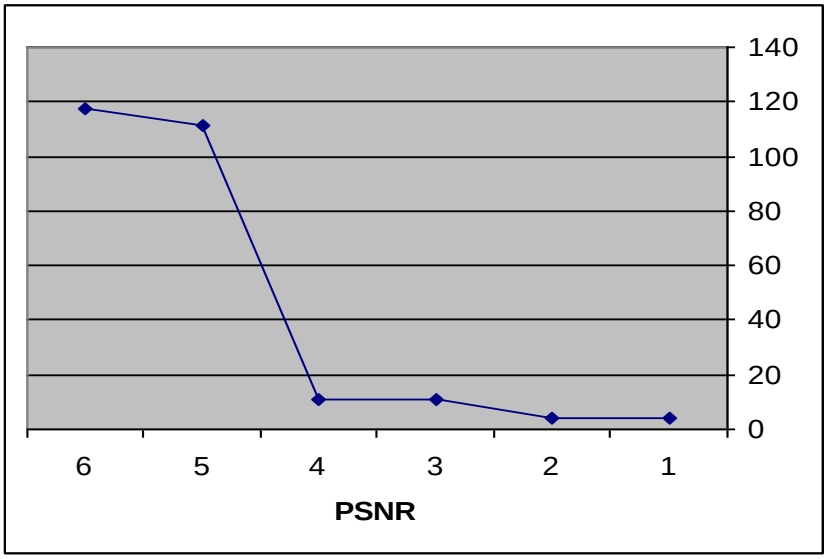
٦- مناقشة النتائج Discussion of result

أولاً: تم تطبيق المعادلة (١) على عدد من العينات الصوتية وباستخدام الخوارزميات الثلاثة لإيجاد الحد الأدنى لمربع الخطأ كما في الشكل التالي:



شكل (١١): قياس الحد الأدنى لمربع الخطأ

ثانياً : تم تطبيق المعادلة (٢) على عدد من العينات الصوتية وباستخدام الخوارزميات الثلاثة لإيجاد نسبة الضوضاء نسبة إلى الإشارة الأصلية كما في الشكل التالي:



شكل(١٢) : قياس نسبة الضوضاء نسبة إلى الإشارة الأصلية

يتبين من خلال الأشكال السابقة ان نسبة الخطأ كانت كبيرة عند استخدام الخوارزمية الثانية والثالثة بينما قلت في الخوارومية الأولى، هذا بالإضافة ان قيم PSNR حققت اعلى قيم لها في الخوارزمية الأولى.

٧- الاستنتاجات

من خلال ما تقدم يمكن القول بان العمل مع ملفات الصوت أكثر صعوبة من التعامل مع بقية أجزاء الوسائط المتعددة لما يحتويه من ترددات غير محسوسة.

من خلال التطبيق العملي تم التوصل إلى ما يلي :

١. طريقة الاخفاء باستخدام المفتاح السري أعطى سرية اكبر للاتصال
٢. الدمج بين تقنيات الإخفاء وعملية التشفير اعطى زيادة سرية الرسالة المخفية.
٣. طريقة الاخفاء باستخدام المفتاح السري في الخوارزمية الأولى أعطت نتائج جيدة من ناحية معدل الخطأ ونسبة الضوضاء من خلال استخدام الاختبارات الاحصائية.
٤. يمكن استخدام تقنيات التغطية لاخفاء أي نوع من أنواع الملفات المتمثلة بصيغة Bit Stream.
٥. تستفاد تقنيات التغطية من خصائص نظام الإدراك البشري وتعمل على استغلال نقاط الضعف لهذا النظام.
٦. إن اختلاف نسب التعيان Sample Rate ومقياس سرعة البيانات Bit Rate ليس لها تأثير كبير في عملية الإخفاء .
٧. يفضل استخدام الملفات الصوتية كثيرة التردد وتجنب الملفات الصوتية التي تحوي فترات صوتية مستوية لأنها اكثر عرضة للتأثر بالتغيير الحاصل بعد عملية الإخفاء وكما هو موضح بالجانب العملي.
٨. يمكن توزيع البيانات المخفية على طول ملف الغطاء لضمان عدم ظهور شك لدى أي متطفل.
٩. المسافات الصوتية المستوية تكون اكثر حساسية للتغيير من المناطق كثيرة التردد.
١٠. حجم البيانات المراد اخفائها في اول 2LSB من كل بايت تكون اكبر من حجم البياتات المخفية في LSB منكل بايت..

٨- التوصيات

١ - يمكن الاستفادة من تقنيات الإخفاء الأخرى داخل ملف الصوت مثل طريقة نشر الطيف وطريقة قياس العمق الصوتي.

٢ - يمكن الاخفاء من خلال اختيار Byte ذات طول مثلا ٢٥٥ فقط لغرض الإخفاء متجاهل بقية البايتات،

٩- دراسات سابقة

- "تصميم نظام حماية هجين وتطبيقه على النصوص "، تناول هذا البحث عملية الدمج بين نظام التشفير مع نظام التغطية باستخدام مفتاح سري لاخفاء المعلومات المشفرة داخل صورة ذات تدرجات رمادية من نوع BMP. [٢]

- "إخفاء نص في صورة" تم استخدام نظام الإخفاء لنص في صورة ولكن حسب قيم ا لجدول اللوني palette حيث يقارن قيمة الحرف مع قيمة الجدول اللوني ان وجدت ويخزن الموقع في الجدول[6].
- "تصميم اطار جديد لحماية البيانات المخفية داخل الفيديو" تم في هذا البحث تصميم نظام يدمج بين التشفير ونظام التغطية باستخدام مفتاح سري لاخفاء البيانات داخل فيدي و، مما اعطى قدرة على خزن كمية كبيرة من البيانات في الصور داخل الفيديو [15].
- "استخدام خوارزمية SLSB لتحسين اداء خوارزمية LSB" تم استخدام خوارزمية جديدة حسنت من اداء الخوارزمية LSB حيث تم خزن البيانات في الخلية الأقل أهمية في احد الألوان الصور متجاهل بقية الألوان في البكسل الواحدة. [9]

١٠- المصادر

١) الجوهري ، شيماء شكيب محمد ،(٢٠٠٤)، "الإخفاء في ملف صوت مكبوس "، بحث ماجستير، كلية علوم الحاسبات والرياضيات، جامعة الموصل، العراق.

٢) الغريري ، شهد عبد الرحمن ،(٢٠٠٣)، "تصميم نظام حماية هجين وتطبيقه على النصوص "، بحث ماج ستير، كلية علوم الحاسبات والرياضيات، جامعة الموصل، العراق.

٣) الصميدعي عامر تحسين سهيل ، (2002)، "تطبيق نظام التغطية "، بحث ماجستير ، كلية علوم الحاسبات والرياضيات، جامعة الموصل، العراق.

٤) قدو ، سجى جاسم محمد ،(٢٠٠٤)، "كبس اشارة الكلام بواسطة استخلاص الخواص " بحث ماجستير، كلية علوم الحاسبات والرياضيات، جامعة الموصل، العراق.

٥) محمود، فرح طارق ،(٢٠٠٤)، "حماية استنساخ الكتابة باستخدام انتشار الطيف "؛ بحث ماجستير، كلية علوم الحاسبات والرياضيات، جامعة الموصل، العراق.

٦) يوسف، هلال محمد وإبراهيم، عروبة إسماعيل، ٢٠٠٢، "إخفاء نص في صورة"، مجلة كلية الرافدين الجامعة للعلوم، العدد ٩ الندوة العلمية الأولى لتقانات إخفاء المعلومات.

7) Alain C., (2003), Brainos II East Carolina University, "Study Stegnaography and The Art of Hiding of information" .

8) Johnson N. F., Duric Z., Jajodia S., (2001), “Information Hiding: Steganography And Watermarking–Attack And Countermeasures”, published by kluwer academic.

9) Juan J., (2008), "SLSB Improving The steganographic Algorithm LSB", World Academy of Science, Engineering and Technology.

10) Jonthan Watkins, (2001), "Steganography – Messages hiddens in Bits", Multimedia System Coursework, Department of Electronics and Computer Science, University of Southampton, S017 1BJ,UK.

11) Lee, Y., Chen, L., (2000), "High Capacity image Steganographic model", IEE Proceedings on Vision, Image and Signal Processing.

12) Mamta J. & Parvinder S., (2009), "Application of LSB based steganographic technique for 8-bit color images", world academy of science, engineering and technology.

13) R.sridevi & Dr. Adamodaram, (2009), "Efficient Method of image steganography by modified LSB algorithm and strong encryption key with enhanced security" Journal of theoretical and applied information Technology

14) Sharp, T., (2001), "An implementation of key-based digital steganography', proc. international workshop on information hiding. Spring LNCS, vol. 2137, pp.13-26 .

15) Sherly A. & Amrtha P., (2010), "A compressed video steganography using TPVD", international Journal of Database Management system, vol.2, No.3.