الباب الأول

مقدمة

1.1 المقدمة

مع تطور علم الحاسوب والإتصالات ظهرت الحاجة الماسة إلى إيجاد وسائل أمنية تمنع قراصنة المعلومات من السطو على المعلومات المهمة والأمنية بشكل خاص مما يسبب نشرها أو التلاعب بمضمونها أو حتى حذفها، فكان لابد من إيجاد وسائل أمنية ذات كفاءة عالية لغرض حماية المعلومات وخاصة على الانترنت.

من المعروف أن الحاسوب يقوم بتمثيل جميع البيانات ومنها الوسائط المتعددة بالقيم الرقمية الثنائية، هذه التمثيلات غالباً ما تكون فيها مستويات رقمية ومناطق التغيير الطفيف في قيمها غير مدرك أو محسوس من قبل حواس الإنسان كالسمع والبصر، وهكذا تتم الاستفادة من هذه الخصائص لإخفاء البيانات في الوسائط المتعددة .

علم الإخفاء هو من الطرق التي إستخدمها الإنسان قديما في مجال إخفاء البيانات، وتعود هذه الطريقة إلى أصول يونانية، حيث تعني كلمة (Stegano) مغطى أو محجوب، وكلمة (Graphy) تعني رسالة أو كتابة، أي إمكانية إخفاء البيانات داخل غطاء معين، وقد ساعد ظهور الحواسيب وسرعة نقل البيانات داخل الشبكات وإمكانية نقل أنواع مختلفة من البيانات، على إمكانية إخفاء نوع معين من البيانات داخل نوع آخر، وبالتالي أعطت درجة حماية أعلى[4].

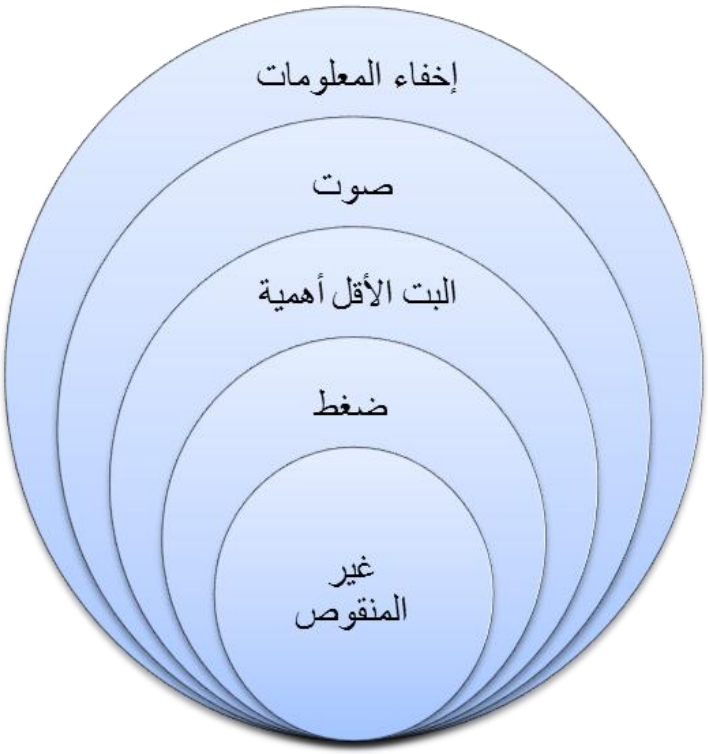
و يمكن تعريف نظام الإخفاء على انه فن وعلم إخفاء المعلومات (او الرسالة) باستخدام ملف حامل لها بهدف منع أي متطفل خارجي من الشك بوجود رسالة مخفية داخل الملف الحامل ، وهي وسيلة من وسائل الاتصال السري بحيث يخفي وجود الاتصال. ومن التقنيات الحديثة في إخفاء المعلومات هي إخفاء الملف النصي داخل الملف الصوتي ، يخطئ كثير من الناس عندما يعتبرون أن التشفير وإخفاء الكتابة هما نفس الشيء ; فبأخذ نظرة دقيقة وتقنية نرى أن التشفير هو دراسة لطرق إرسال الرسالة بصورة أخرى لا يستطيع فك رموزها إلا المرسل والمستقبل ، وهذا يختلف عن فن الإخفاء حيث أن التشفير يغير من هيئة محتوى الرسالة لكنه لا يخفي وجودها ، أما إخفاء الكتابة فيخفي وجود الرسالة من الأساس[4].

و من أهم مميزات الإخفاء في الصوت هو وجود بعض الفجوات في النظام السمعي البشري التي يمكن إستغلالها ، فمثلا الاذن البشرية لا تفرق بين نبرتي صوت مختلفتين والاصوات العالية تحجب الاصوات المنخفضة ، و أيضا مقارنة الإخفاء في الصوت بالإخفاء في الصورة هو أن الصوت يوجد بأحجام كبيرة مقارنة بالصورة مما يمكن من تخزين معلومات كبيرة في ملفات الصوت [4].

و أسباب إخفاء المعلومات كثيرة, منها لغرض تبادل بيانات سرية بين شركات معينة أو بين دوائر حكومية او عسكرية معينة على سبيل المثال.

2.1 حدود المشروع

هذا المشروع يهتم بإخفاء البيانات داخل ملف صوتي بإستخدام خوارزمية ال (LSB) و كتطوير للخوارزمية تم إضافة مفهوم ضغط البيانات بإستخدام طريقة الضغط غير المنقوص ،وأيضاً يمكن إستخدام المشروع فقط في الشركات التي يتعامل موظفيها مع ملفات الوسائط المتعددة و بالتحديد ملف صوتي بصيغة wav. و أن تكون الرسالة المراد إخفاءها رسالة نصية.



الشكل 1.1 يوضح تدرج التقنيات المستخدمة في المشروع

3.1 مشكلة المشروع

من المهم والشائع اليوم في أي منظمة تبادل المعلومات بين أفراد هذه المنظمة في داخلها أو خارجها ، و قد تتعرض هذه المعلومات أثناء نقلها عبر الشبكة لخروقات أو تعديلات عليها ، يهدف هذا المشروع إلي تصميم برنامج يمكن بواسطته إخفاء المعلومات في ملف صوتي حيث لا يمكن للإنسان تميز ما إذا كان هذه الملف يحتوي علي معلومات أم لا، فيصبح في إمكان المنظمة نقل المعلومات بصورة آمنة و أيضاً حل المشكلات الأتية:

- مشكلة التوفيق بين حجم الملف الصوتي و الملف النصي الذي سيتم إخفاءه فيه.
- التشويش الناتج في الملف الصوتي بعد عملية تضمين الملف النصي بداخله.

4.1 أهداف المشروع

الأهداف الرئيسية التي سيتم تحقيقها:

1. من أهم أهداف هذا المشروع هو تقليل نسبة التشويش الذي يحدث بسبب عملية الإخفاء، و التي تقلل من نسبة الشك من قبل المتطفل.
2. إخفاء المعلومات لحماية الخصوصية .
3. إخفاء أكبر قدر ممكن من المعلومات في ملف صوتي .
4. حماية المعلومات من التعديل بواسطة أفراد غير مصرح لهم .

5.1 المنهجية المتبعة و الأدوات

1. قمنا في هذا المشروع بتناول مجموعة من الدراسات السابقة وقياس نقاط ضعفها وقوتها .
2. تم تطوير خوارزمية ال(LSB) وإضافة مفهوم ضغط البيانات كتحسين لهذه الخوارزمية .
3. ومن ثم إجراء مجموعة من التجارب التي توضح التشويش الناتج من تضمين مختلف أحجام الملفات النصية و قياس جودة الملف الصوتي الناتج.
4. وتم استخدام لغة البرمجة (java) في تطوير هذا النظام و هي عبارة عن لغة برمجة ابتكرها جيمس جوسلينج (James Gosling) في عام 1992 أثناء عمله في مختبرات شركة صن Sun (Microsystems) وذلك لاستخدامها بمثابة العقل المفكر المستخدم لتشغيل الأجهزة التطبيقية الذكية مثل التلفاز التفاعلي.

   في المشروع محل الدراسة قمنا بإستخدام هذه اللغة لأنها تدعم الكثير من المكتبات التي تساعدنا في تطبيق النظام بصورة أكثر كفاءة.
5. و إستخدام ال MATLAB في قياس جودة ملف الصوت الناتج.

6.1 تنظيم المشروع

يحوي هذا المشروع خمسة أبواب:

الباب الأول عبارة عن مقدمة المشروع التي تتناول مقدمة عن مفهوم إخفاء المعلومات و فوائد إخفاء المعلومات في الصوت و الجهات المستفيدة منه و مشكلة المشروع و أهميته و المنهجية المتبعة في العمل و مدى المشروع .

ويتناول الباب الثاني أهم المفاهيم التي يجب الإلمام بها لمعرفة كيفية عمل النظام و كما يحوي أيضا الدراسات السابقة في مجال عمل المشروع والتي تم الإستفادة منها في تطوير النظام الحالي بالإستفادة من الأخطاء و العيوب التي كانت في الأنظمة السابقة.

ويشمل الباب الثالث توضيح للكيفية التي يعمل بها النظام كما يوضح تفصيل العمليات في النظام وكذلك يشمل مجموعة من التجارب في النظام. والباب الرابع النتائج المتحصل عليها من إجراء المشروع إضافة إلى تحليل هذه النتائج.

و صولاً إلى الباب الخامس الذي يحوي التوصيات والمراجع التي تعنى بتطوير هذا النظام فيما بعد.

الباب الثاني

الإطار النظري

الفصل الأول: أدبيات البحث

الفصل الثاني: الدراسات السابقة

الـفـــــصـــل الأول

أدبيات البحث

1.1.2 المقدمة

في هذا الفصل سيتم التطرق لمفاهيم عامة في مجال أمن المعلومات تم الإستفادة منها في فهم طريقة عمل المشروع، حيث سيتم سرد هذه المفاهيم حتى يتسنى للقارئ فهم أبعاد البحث و معرفة التقنيات التي تم إستخدامها في إكمال العمل على هذا المشروع.

2.1.2 مفاهيم أمن المعلومات

هناك طرق عديدة وكثيرة تلعب دور مهم فيما يخص أمن المعلومات، ومنها الطريقة الأكثر شيوعاً والمعروفة ‘‘بالتشفير’’ وذلك بتشفير البيانات لتصبح غير مقروءة. من ناحية أخرى هناك فن آخر يهتم بإخفاء البيانات كلياً للتواصل مابين جهتين لتصبح هذة البيانات أو هذا الإتصال غير ظاهر من الأساس لجهة ثالثة وهذا مايعرف بال (Steganography)[11].

كلمة (Steganography) في الأساس مشتقة من كلمة يونانية تعني ‘‘الكتابة المخفية’’، و هي طريقة و فكرة قديمة ولها قصة تاريخية بدأت أيام الإمبراطورية اليونانية القديمة عندما كانت تكتب رسائل على رؤوس العبيد أنذاك. كان يحلق شعر العبد ويكتب على رأسه رسالة سرية معينة، وعندما يعود شعره للنمو مرة أخرى تختبئ الرسالة السرية تحت شعره الكثيف وعندها يتم إرساله للشخص المعني الذي بدوره يقوم بحلق رأس العبد مرة أخرى حتى يستطيع قراءة الرسالة، وهكذا كانت بدايات إستخدام هذة الطريقة لإخفاء رسالة أو معلومة ما تحت غطاء أو شيء ما حتى لا يكون هناك علم أن أي إتصال سري يتم مابين إثنين أو أكثر[12].

إخفاء المعلومات هي طريقة أو تقنية لحجب و إخفاء المعلومات داخل وسيط رقمي ، حتى يتم إخفاء أن هناك إتصال أوتبادل معلومات يتم في الخفاء، ولا يكون على علم بهذا الإتصال إلا الأشخاص المعنيين[12].

علم الإخفاء يستخدم لعدة أسباب، والسبب الرئيسي هو لحماية البيانات والمحافظة على خصوصية المعلومات، والسبب الثانوي هو لحفظ البيانات من محاولات سرقتها وذلك بإخفائها في وسط آخر [12].

الكثير من الناس لديه خلفية بمصطلح التشفير والذي يعني بإختصار تشفير المعلومة لتصبح غير مفهومة وغير قابلة للقراءة إلا من قبل الشخص الذي يمتلك مفتاح التشفير لفك الشفرة.

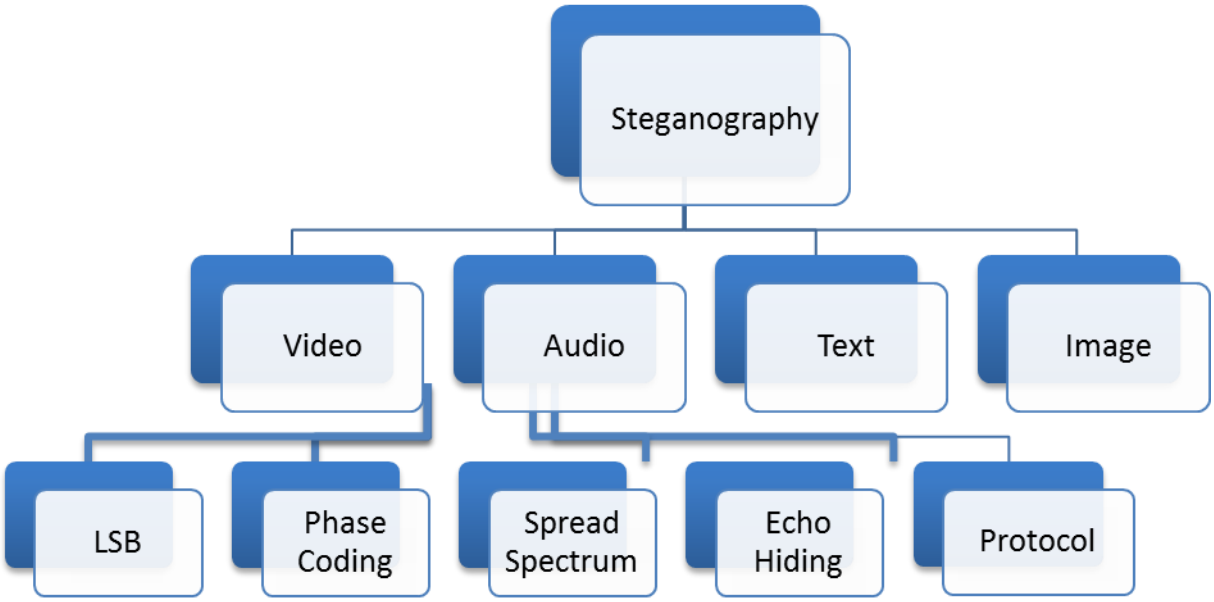
إخفاء المعلومات يختلف عن التشفير بالرغم من وجود الكثير من التشابه بينهما، هنا إخفاء المعلومات يعني تخبئتها داخل وسيط أو تحت غطاء معين حتى لا يتسنى لأي شخص معرفة أن هناك معلومات مخفية من الأساس, و مثلاً من الوسائط التي تستخدم لغرض إخفاء المعلومات الصور ، النصوص ، و الملفات الصوتية[12].

إذا نستطيع القول أن الفرق الأساسي بين التشفير و إخفاء المعلومات هو أن عند تشفير معلومة ما يستطيع الطرف الثالث معرفة أن هناك إتصال يتم مابين شخصين أو مجموعتين لكنه لا يستطيع فهم المعلومات لأنها مشفرة.

بينما في إخفاء المعلومات لا يكون هناك علم لأي طرف ثالث بأن هناك شيء مخفي أو أن هناك إتصال بين إثنين.

3.1.2 أساليب الإخفاء

يتم إخفاء الرسالة عن طريق إدخالها ضمن الغطاء والذي غالبا ما يكون ملف نصي أو صورة أو ملفات صوت أو فيديو ثم إرسالها إلى الأطراف المعنية.



الشكل 1.1.2 طرق الإخفاء وأنواع الإخفاء في الملفات الصوتية

1.3.1.2 الإخفاء في ملف نصي

وذلك عن طريق إخفاء الرسالة المراد إرسالها باستخدام النصوص. وتتم هذه الطريقة إما بطريقة نصية، مثلاً: يكون أول حرف من كل كلمة يمثل حرف من الرسالة المخفية. أو بطريقة نحوية أو لفظية. ويعتبر هذا النوع من الإخفاء من أصعب أنواع الإخفاء . و تتم عن طريق إستخدام الحرف الأول من كل كلمة وتعتبر هذه الطريقة من أوائل طرق الإخفاء النصي، و يمكن تطبيقها على اللغة العربية والإنجليزية. في هذه الطريقة، يتوجب بناء قطعه

نصية مفهومة بحيث عندما يقوم المستقبل بجمع الأحرف الأولى أو الأخيرة مثلا من كل كلمة يحصل على الرسالة السرية. في ما يلي مثال مبسط لهذه الطريقة :

Bring us your invoice by Monday و التي قد تعني BUY IBM .

2.3.1.2 الإخفاء في صورة

وذلك عن طريق إخفاء الرسالة المراد إرسالها في صورة، ويعد هذا النوع من الإخفاء من أكثر الأنواع شيوعاً في الإستخدام لما تتميز به الصور من صفات تجعلها الوسط المثالي للإخفاء. ويتم تطبيق هذه النوع من الإخفاء باستخدام أحد الطرق التالية: الإخفاء باستخدام التحويل الزاوي المتقطع (Discrete Cosine Transform)، الإخفاء باستخدام التحويل الموجي والإخفاء باستخدام الإدخال في البت الأقل أهمية (LSB). وتعد طريقة الإدخال في البت الأقل أهمية من أكثر الطرق شيوعاً.

3.3.1.2 الإخفاء في فيديو

يعتبر الإخفاء بإستخدام ملفات الفيديو جزءاً مشتقاً من الإخفاء بإستخدام الصور، وذلك لأن ملفات الفيديو عبارة عن صور مجتمعة.

ومن أشهر الطرق المستخدمة في هذا النوع طريقة الإخفاء بإستخدام التحويل الزاوي المتقطع .(Discrete Cosine Transform) وتقوم هذه الطريقة بإخفاء جزء من المعلومات في جزء معين من الصور التي يتكون منها الفيديو، وتمتاز هذه الطريقة بأنها غالبا لا يتم اكتشاف البيانات المخفية بالفيديو بواسطة العين البشرية. لكن يجب ملاحظة أنه كلما ازداد حجم البيانات المخفية كلما كان كشفها أسهل في جميع الطرق المستخدمة للإخفاء.

4.3.1.2 الإخفاء في صوت :

يتم في هذه الطريقة إخفاء الرسالة المراد إرسالها داخل إشارة صوتية .

5.3.1.2 الإخفاء في بروتوكول

يستخدم في هذه الطريقة قنوات الخزن المخفية لإخفاء معلومات نصية أو صورة مخفى فيها معلومات سرية في بروتوكولات طبقة الإنترنت TCP/IP .

4.1.2 الإخفاء في صوت

إن عملية إخفاء المعلومات في إشارة الصوت تعد تحدياً كبيراً لأن النظام السمعي البشري (HAS) يعمل بشكل ديناميكي واسع المدى في ترددات تقع بين 20 Hz – 20000Hz ، إذ أن الاذن البشرية لها القدرة على إدراك الأصوات بنسبة عالية جداً مما يجعل هنالك صعوبة بإضافة بيانات إلى الملف الأصلي أو حذفها منه والتي يتم إدراكها مباشرةً بوصفها ضوضاء لذا فإن هذا النظام يكون حساساً جداً لأي تغيرات شاذة في العينات، ولكن وجود بعض الفجوات في نظام السمع البشري والتي يمكن إستغلالها، جعلت عملية الإخفاء والتلاعب ببيانات الملف الأصلي ممكنة ، فمثلا الأذن البشرية لا تفرق بين نبرتي صوت[1].

الضعف في ال (HAS) يأتي من محاولة التمييز بين الأصوات (الأصوات العالية تحجب الأصوات الهادئة) وهذا هو ما يجب إستغلاله لإخفاء رسائل سرية في الصوت دون أن يتم اكتشافها ، و من أنواع الإخفاء في الصوت :

1.4.1.2 البت الأقل أهمية

هي أبسط طريقة لإخفاء البيانات السرية في الوسائط. عن طريق إستبدال ال bit أقصى اليمين في byte ملف الوسائط ب bit من الملف السري ، وهي تسمح بإخفاء كمية كبيرة من البيانات ، لإستخراج الرسالة من ملف الوسائط يجب على المستخدم إجراء نفس العملية في الملف المعدل عن طريق إستخراج الكلمات من ال (LSB) . و أيضا نلاحظ أن هناك فرصة 50% أن يكون الbit المراد تمثيله هو نفس الbit الموجود في ملف الصوت ، أي بعبارة اخرى أن في نصف عملية الإخفاء لا يتم تغيير ال bit مما يقلل من تهدور الجودة في الملف الصوتي و ظهور تشويش فيه[9].

2.4.1.2 الترميز الطوري

تعتمد هذه الطريقة على توقع الأذن البشرية للضوضاء أكثر من توقعها للأصوات الحقيقية في الملف الصوتي وتعتمد على دمج الرسالة بشكل Bits في مواضع إنقلاب الطور بالموجة الصوتية[1].

3.4.1.2 الأثير المنتشر

تعتمد هذه الطريقة على نشر موجات ضمن نطاق واسع من الترددات لا يمكن تمييزها عن الضوضاء (Noise) وتحتوي بداخلها على البيانات المراد إرسالها. المشكلة التي تعترض هذه الطريقة هي إندماجها مع اشارة اخرى. وقد استخدمت هذه الطريقة لاول مرة على يد القوات الامريكية في سنة 1941 ولها طرق عديدة فهناك الدمج ضمن الوقت او ضمن التردد وتستخدم ايضا مع ملفات الصوت[5] .

5.4.1.2 الإخفاء بالصدى

تقوم هذه الطريقة على توليد صدى للصوت بمسافة زمنية قصيرة لا يمكن للاذن البشرية التمييز بين الصوتين ويتم التشفير بواسطة إختلاف المسافات الزمنية بين الصدى والصوت الأصلي[5].

5.1.2 من أنواع الإخفاء في البت الأقل اهمية :

1.5.1.2 البت الأقل أهمية العادية

يتم تخزين البيانات المراد إخفاءها بتعديل ال bits أقصى اليمين. هذه الbits تستبدل بالbits المكونة للرسالة المراد إخفاؤها ،ومن الخارج لا يتم التعديل على الملف بشكل ملحوظ هذا يَسْمحُ للشخص بإخْفاء المعلوماتِ في الملفِ ويَتأكّدُ من أنه لا يمكن لأي إنسانَ أَنْ يَكتشفَ التغيّرْ في الملفِ. ال LSB عادة لا تَزِيدُ حجمَ الملفَ[5].

2.5.1.2 البت الأقل أهمية العشوائية

يتم في هذه الطريقة إخفاء البيانات عشوائياً داخل ملف الصوت بإستخدام مفتاح في عملية الإخفاء يعرف هذا المفتاح ب(stego key) ومن ثم يتم إستخدام مفتاح الإخفاء لتحديد المناطق العشوائية وأيضا يمكن إستخدام خوارزمية لتحديد المناطق العشوائية مثل خوارزمية الFibonacci[5].

Edge Least significant bit 3.5.1.2

هذه الطريقة يتم إستخدامها مع الصور بصورة كبيرة ولا يحبذ إستخدامها في الملفات الصوتية أو ملفات الفيديو ، تقوم فكرة هذه الطريقة علي تحديد مجموعة من الpixels المتتالية التي تسمى edge ويتم تحديدها بإستخدام خوارزمية Canny Edge detection method ومن ثم إخفاء البيانات فيه[5].

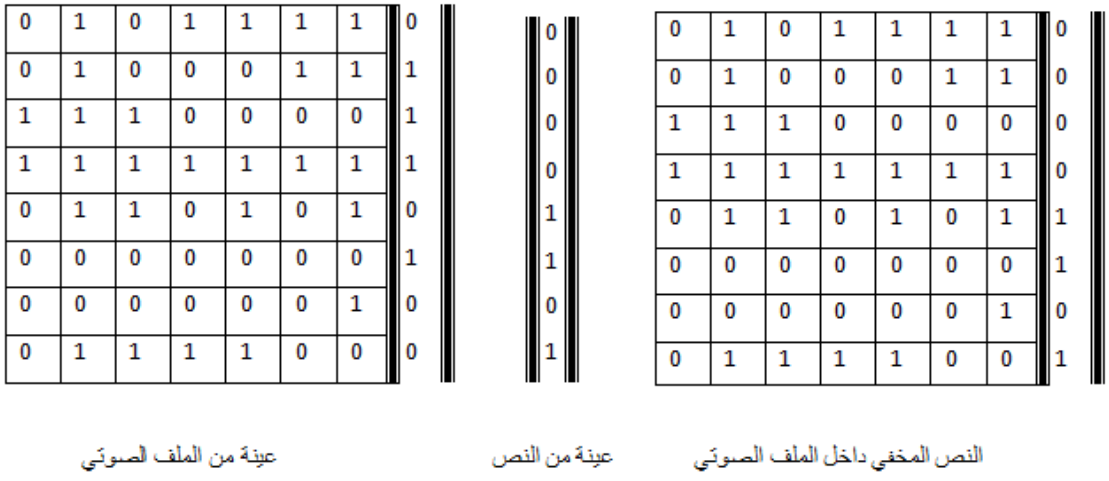
6.1.2 الإخفاء في البت الأقل أهمية (LSB)

وهي طريقة مشهورة جدا وتعتمد على مبدأ تبديل قيمة الbit الأقل أهمية في الملف الغطاء لإخفاء سلسلة من الbits التي تكون الرسالة المخفية، ويتم فيها إستبدال البت الأخير من المف الصوتي لbyte معينة بأخري من الملف النصي المراد إخفائه ، و يوجد أربعة أنواع معترف بها عالمياً .

هنالك عدد من الطرق لتطبيق عملية الإخفاء في البت الأقل أهمية و تم إختيار هذه الخوارزمية للتمكن من تطبيق الخوارزمية المقترحة بأبسط طريقة، ويتم في هذه الطريقة تحويل كل من الملف الصوتي والملف النصي إلي الترميز الثنائي وذلك بعد ضغط الملف النصي وتختلف طرق التطبيق[9] وهي كالتالي :

1.6.1.2 البت الأقل أهمية رقم واحد(1 LSB)

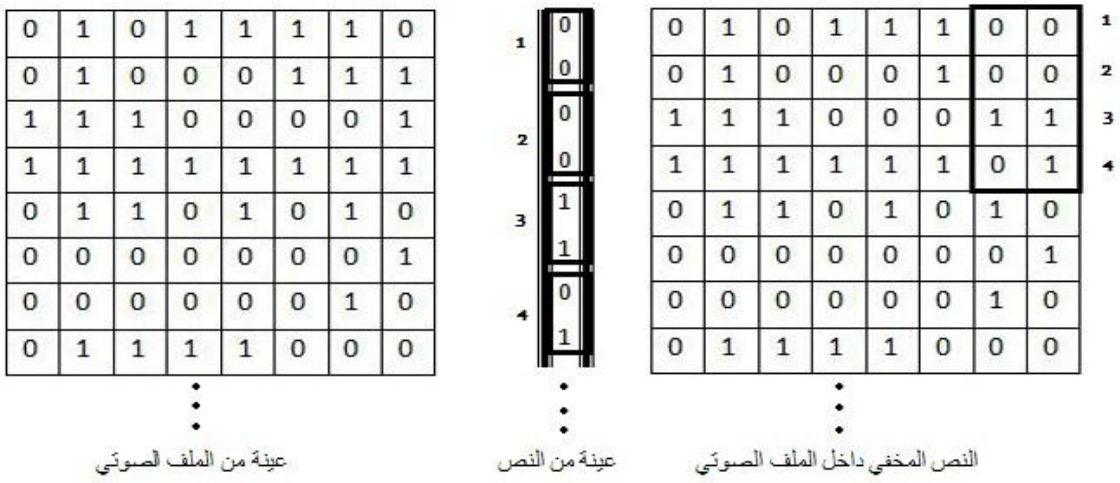
يتم في هذه الطريقة إستبدال الخانة الأخيرة من ال(byte) في الملف الصوتي بخانة من الملف النصي كما هو موضح بالشكل (3.1) :



الشكل 2.1.2 يوضح طريقة تنفيذ خوارزمية ال1 LSB

2.6.1.2 البت الأقل أهمية رقم إثنان (2 LSB)

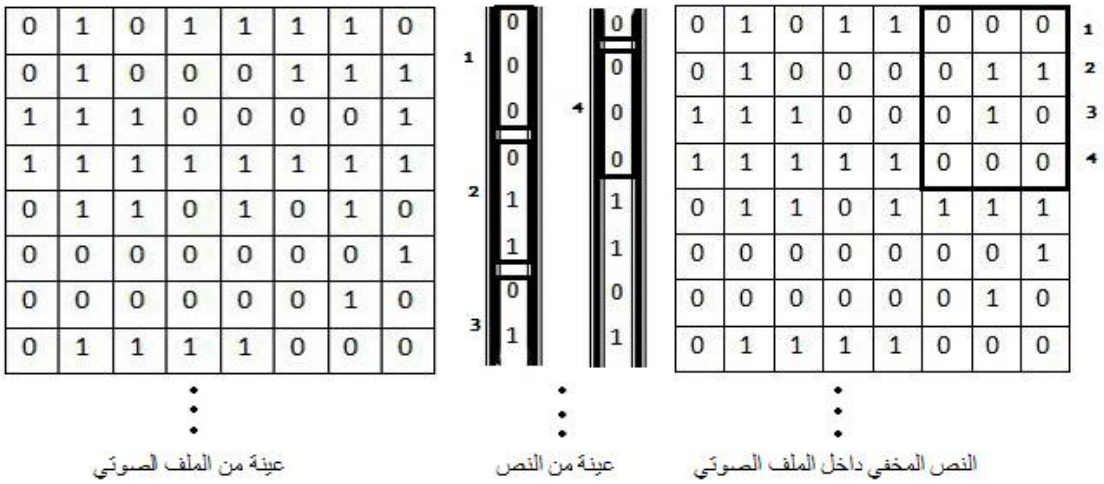
ويتم في هذه الطريقة إستبدال الخانة السابعة و السادسة من ال(byte) في الملف الصوتي بخانتين من الملف النصي كما هو موضح بالشكل (3.2) :



الشكل 3.1.2 يوضح طريقة تنفيذ خوارزمية الLSB 2

3.6.1.2 البت الأقل أهمية رقم ثلاثة (3 LSB)

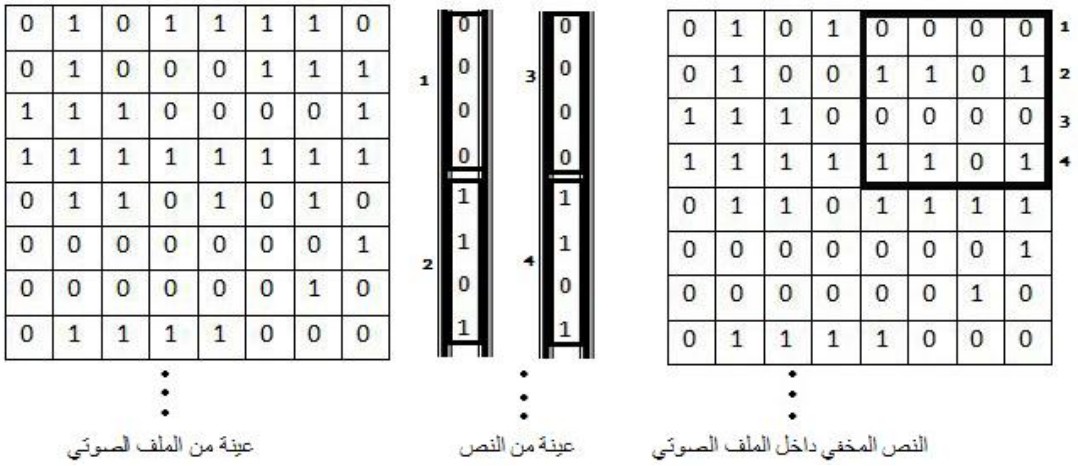
ويتم في هذه الطريقة إستبدال الخانة السابعة و السادسة و الخامسة من ال(byte) في الملف الصوتي بثلاث خانات من الملف النصي كما هو موضح بالشكل (3.3) :



الشكل 4.1.2 يوضح طريقة تنفيذ خوارزمية ال LSB 3

4.6.1.2 البت الأقل أهمية رقم أربعة (4 LSB)

ويتم في هذه الطريقة إستبدال الخانة السابعة و السادسة و الخامسة و الرابعة من ال(byte) في الملف الصوتي بأربع خانات من الملف النصي كما هو موضح بالشكل (3.4) :



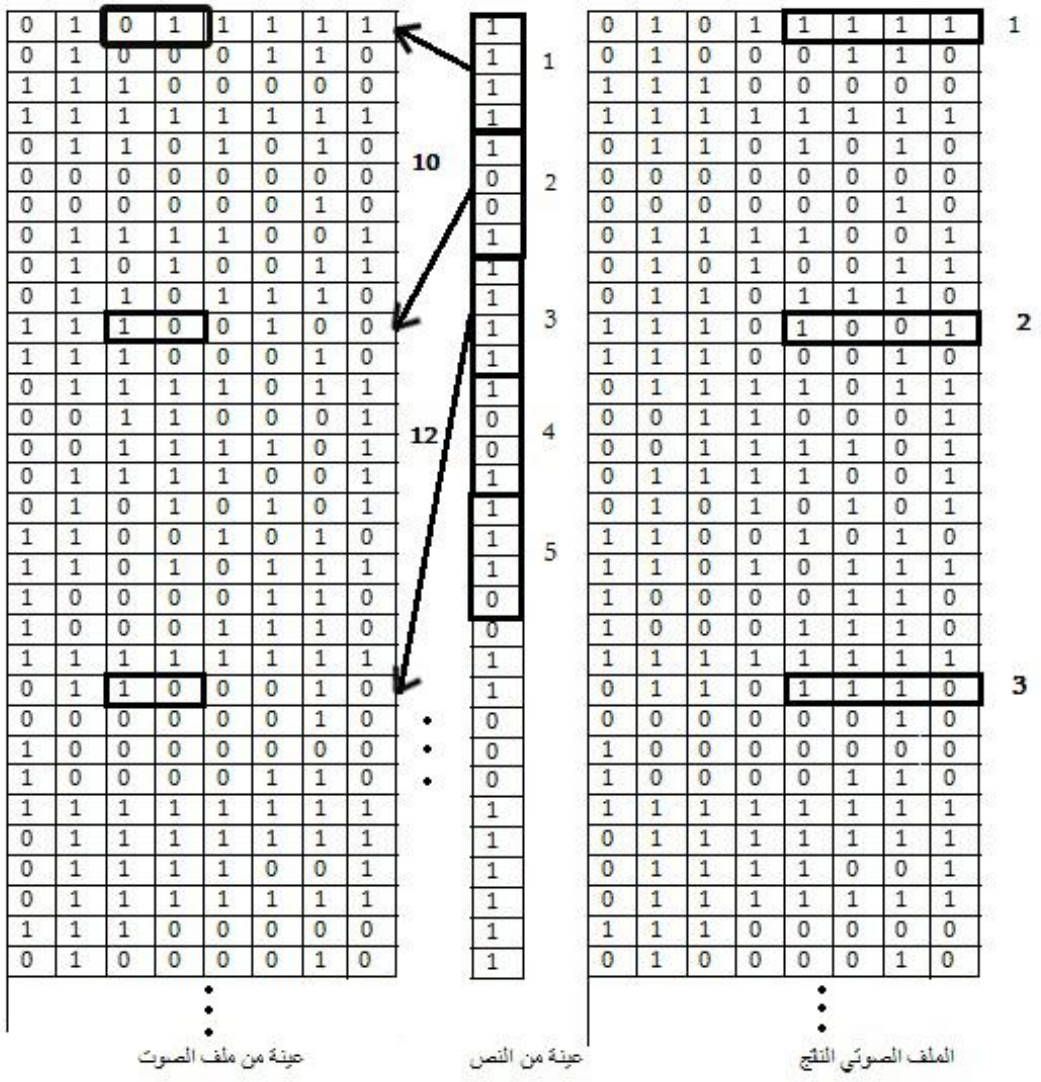
الشكل 5.1.2 يوضح طريقة تنفيذ خوارزمية ال4 LSB

5.6.1.2 الخوارزمية المقترحة

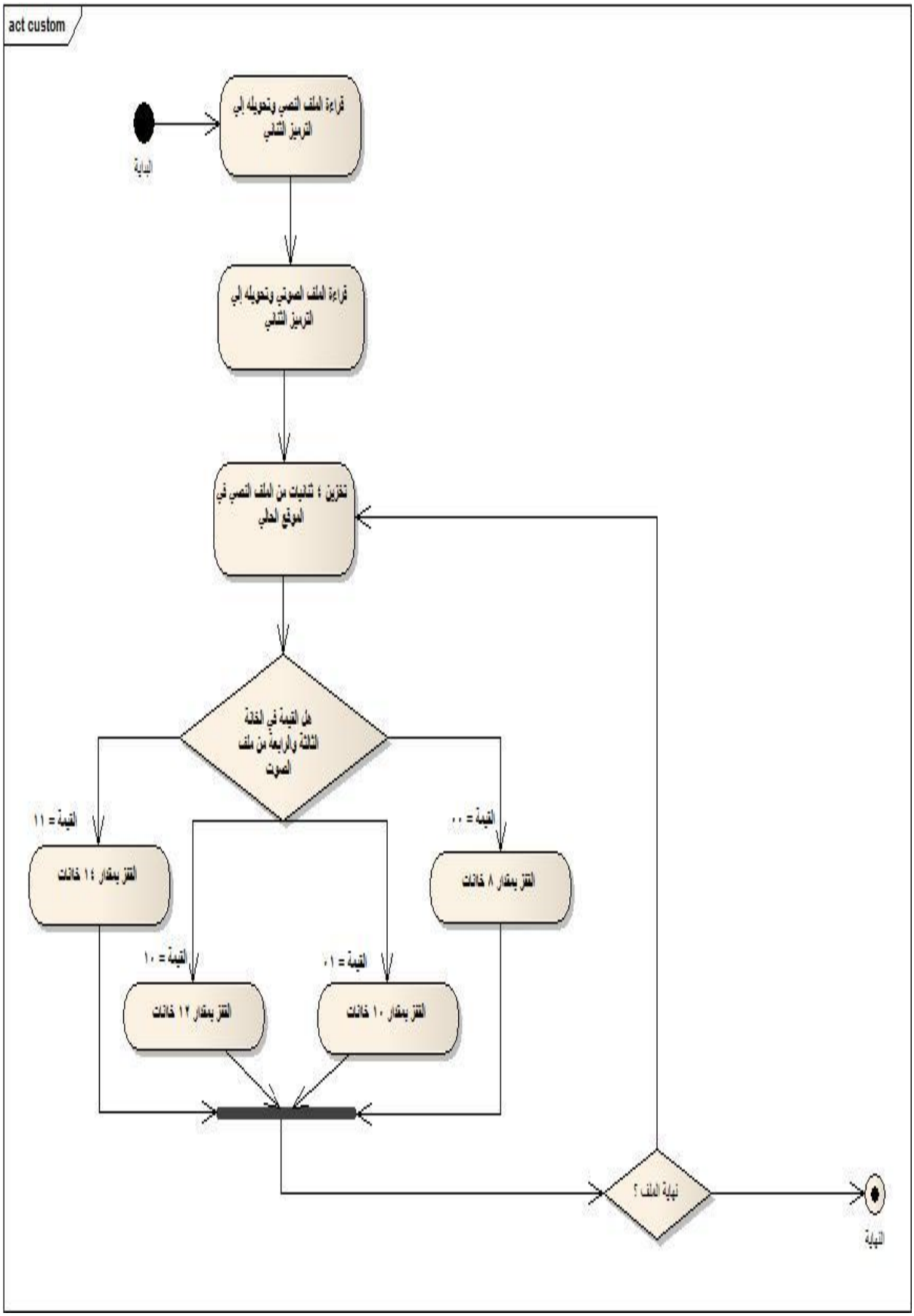
يتم في الخورزمية المقترحة إستخدام البت الأقل أهمية رقم أربعة (4 LSB) و يتم أيضا ضغط الملف النصي وتحويله إلي الترميز الثنائي وتحويل الملف الصوتي أيضا إلي الترميز الثنائي .

تعمل الخوارزمية المقترحة بإستبدال أربع خانات من ال(byte) في الملف الصوتي بأربع خانات من ال(byte) في الملف النصي و تستخدم تقنية تعرف بتقنية القفز وهذه التقنية تسمح بتقليل التشويش في الملف الصوتي الناتج ، وتعمل هذه التقنية هذه على إختبار الخانة الثالثة و الخانة الرابعة في الملف الصوتي و من ثم تحديد مقدار القفزة إعتماداً على قيمها كما هو موضح الجدول أدناه :

القيمة الثنائية للخانتين	مقدار القفزة
00	8
01	10
10	12
11	14



الشكل 6.1.2 يوضح طريقة تنفيذ الخوارزمية المقترحة



الشكل 7.1.2 المخطط الإنسيابي لطريقة عمل الخوارزمية المقترحة

7.1.2 أنواع الملفات الصوتية :

قبل التطرق إلي عملية الإخفاء في الصوت سنتاول عدد من صيغ الملفات الصوتية أهمها :

1.7.1.2 ملف ذو إمتداد (MP3)

تعتبر من أشهر الصيغ المستخدمة في الملفات الصوتية و ذلك بسبب أنها تحفظ المعلومات الصوتية في ملفات أصغر حجما و أيضاً لقابلية تشغيلها على العديد من الأجهزة مثل الـmp3 players[13].

2.7.1.2 ملف ذو إمتداد (RM, RA, RAM)

نوع من الملفات الصوتية تابع لشركة RealNetworks،وهو يستخدم لبث الموسيقى عبر تقنية البث الحي (Streaming)[13].

3.7.1.2 ملف ذو إمتداد (AIFF)

هو ملف صوتي قامت بإبتكاره شركة Apple لتسجيل و تشغيل هذا النوع من الأصوات على حواسيبها الخاصة، وهو يحمل إما امتداد AIFF أو AIF[6].

4.7.1.2 ملف ذو إمتداد (WAV)

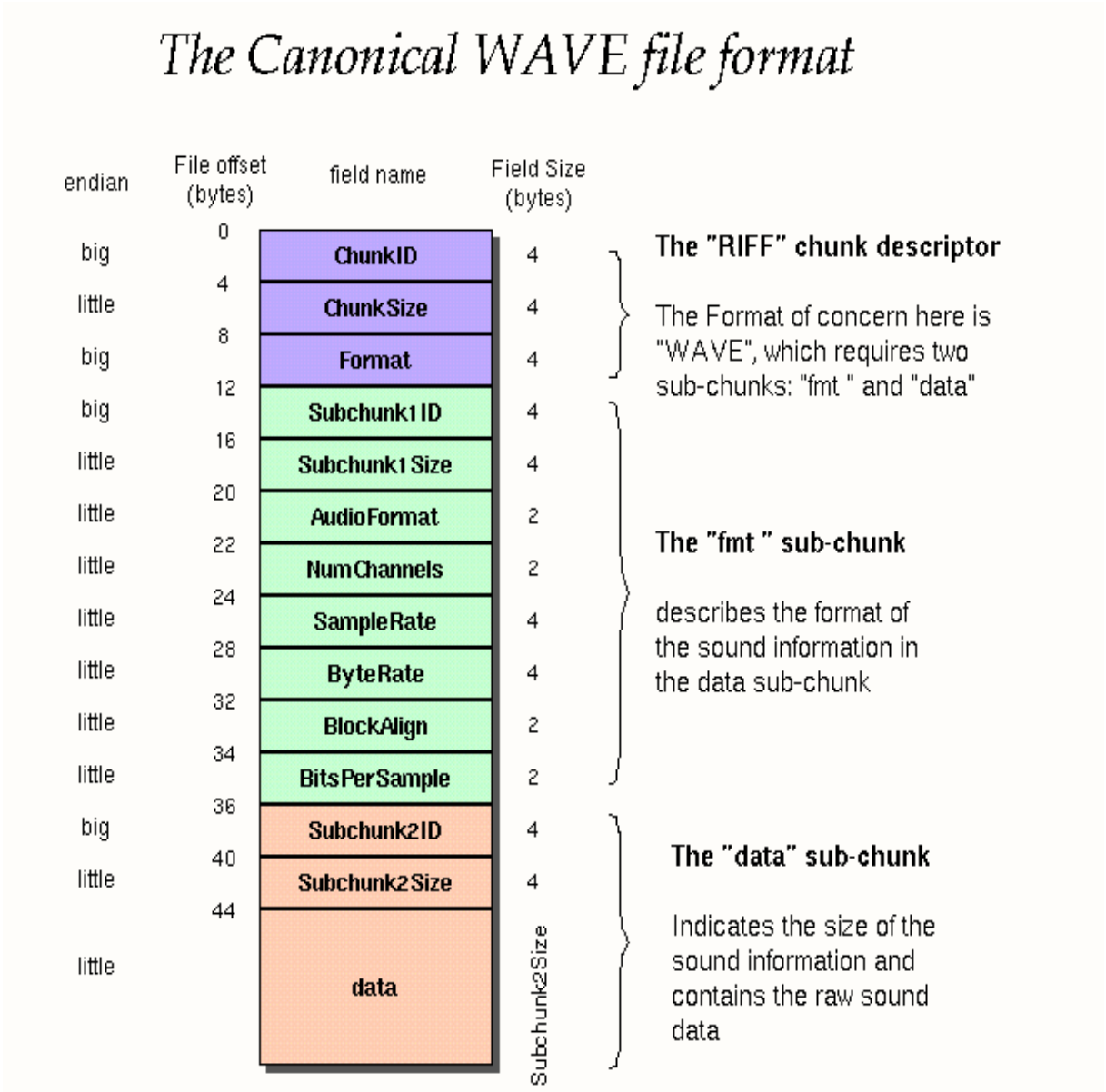
أنتجته شركة Microsoft ، ويتميز الملف الذي يحمل هذا الامتداد بجودة صوت نقية و عالية ، إلا أن حجمه يكون كبيرا إذا كانت مدة الصوت أطول[6].

8.1.2 ملف الصوت ذو الإمتداد (wav)

يوصف الملف ذو الإمتداد WAV بصيغة (PCM) بأنه شائع الإستخدام من قبل شركة Microsoft تحت بيئة التشغيل (Windows) لذلك يعد من الصيغ الأكثر استخداماً، حيث تعرف Microsoft هيئة الملف العامة ب (RIFF) حيث يمثل ال(WAV)نوعا خاصاً منه وقد نُظم الملف فيه على شكل مقاطع متداخلة ومترابطة تدعى بال(Chunks) وأبسط صيغة لملف ال(WAV) يجب أن تحتوي على مقطع الصيغة (Format Chunks "fmt") الذي يحتوي على معلومات مهمة عن الملف،ويجب أيضاً أن

يحتوي على مقطع البيانات (Data Chunk) ، أما المقاطع الأخرى فتعد إختيارية(list , disp) ، كل مقطع في ملف ال(WAV) يبدأ بتعريف يتألف من أربعة [6].

Bytes وهي (RIFF , fmt , list , disp , data) يليها حجم ذلك المقطع، كما موضح في الشكل 2.1 المبين أدناه [7]:



الشكل 8.1.2 المقاطع المتداخلة لملف الصوت من نوع RIFF

الجدول 1.1.2 يوضح معاني المصطلحات في الشكل 8.1.2

المحتوى	التوضيح
ChunkID	يحتوي على الكلمة RIFF ممثلة في شكل ASCII
ChunkSize	يحتوي على حجم الملف الكلي منقوص منه 8 بايت لل ChunkID و ChunkSize
Format	تحتوي على الحروف wave
Subchunk1ID	يحتوي على الحروف fmt
Subchunk1Size	يحتوي على الحجم المتبقى لل subchunk
AudioFormat	يحتوي على قيمة ، إذا كانت غير الواحد تعني أن الملف قد تم ضغطه
NumChannels	يحتوي على نوع القناة (Mono = 1 , Stereo = 2)
SampleRate	8000،44100..الخ
ByteRate	SampleRate * NumChannels * BitsPerSample/8 يتم حسابها من المعادلة
BlockAlign	SampleRate * BitsPerSample/8 يتم حسابها من المعادلة
BitsPerSample	8 bits = 8, 16 bits = 16
Subchunk2ID	تحتوي على الحروف data
Subchunk2Size	يحتوي على عدد ال bytes في البيانات
Data	تحتوي على البيانات الفعلية للصوت

9.1.2 ضغط البيانات (Data compression)

هي عملية تقليص البيانات إلى حجم معين، عملية التقليص هي عملية الإختصار (الترميز) و الإستغناء عن البيانات الإضافية أو المكررة، يقصد بالحجم المعين الحد الأدنى الذي يمكن أن تقلص له البيانات دون أن تفقد كمية المعلومات التي تحتويها وهي التي تحدد كفاءة الخوارزمية من ناحية الضغط و الجودة , ويوجد العديد من البرامج التي تقوم بضغط البيانات[3]. وهنالك نوعين لضغط البيانات :

1.9.1.2 ضغط البيانات المنقوص

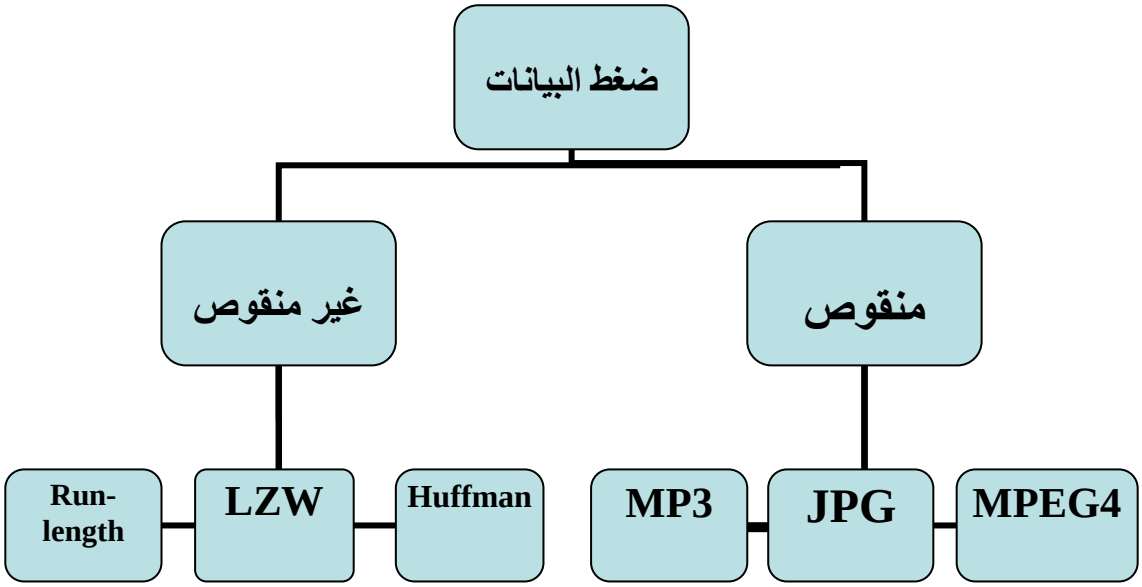
هي طريقة تضغط الملف من خلال تجاهل أي بيانات غير ضرورية. يستعمل الضغط المنقوص لتقليص ملفات الأصوات أو الصور إذا كانت الدقة المطلقة غير مطلوبة وإذا كانت خسارة بعض البيانات ليست ذات أهمية.

أي أن الملف المضغوط عند فك ضغطه لن نحصل منه علي نسخة تكون مطابقة للملف الأصلي تماماً و لكن سنحصل مثلاً علي 90% أو 80% منه بحيث يكون لدينا المعلومات المهمة عنه فقط أي أننا سنحصل علي ملف مشابه للملف الأصلي ولكن جودته تكون أقل من جودة الملف الأصلي.

ويتم إستخدام هذا الأسلوب عند الرغبة في الحصول علي نسبة ضغط عالية جداً وليست هناك حاجة ضرورية لأن يكون الملف الناتج بعد عملية الضغط مطابق تماماً للملف الأصلي[3].

2.9.1.2 ضغط البيانات غير المنقوص

لا تؤدي طريقة الضغط هذه إلى خسارة أي بيانات أصلية عند إلغاء الضغط. يتم إستعمال هذا النوع من الضغط مع ملفات البرامج و المستندات ، حيث لا يمكن تحمل خسارة أي بيانات. أي أن الملف الناتج من عملية الضغط يكون نسخة طبق الملف الأصلي قبل الضغط[3].



الشكل 9.1.2 يوضح أنواع ضغط البيانات

10.1.2 أنواع ضغط البيانات الغير منقوص

1.10.1.2 خوارزمية آبراهام ليمبيل و يعقوب زيف 1997

تقوم هذه الخوارزمية بإستبدال العناصر المكررة في البيانات بالإشارة إليها في شكل زوج من الأرقام يوضح الرقم الأول المكان الذي ستبدأ منه الحروف التي سيتم إستبدالها و الرقم الثاني يمثل رقم اخر حرف سيتم وضعه ، مثال:

لدينا كلمة "hamza" نريد أن نشير إلى الثلاث الحروف الأولى "ham" سنكتب [1,3] يعني من الحرف 1 إلى الحرف رقم 3 إذن فلنجرب ضغط "hamzahamtaro" "hamza[1,3]taro".

2.10.1.2 ترميز طول التشغيل

هو نموذج بسيط جداً من عمليات ضغط البيانات وكلمة(طول) (تعني تكرار أحد المعطيات بشكل متتابع في العناصر المعطاة) يتم تخزين هذه القيمة المكررة على شكل قيمة واحدة بجانبها عدد مرات التكرار. وهذا الترميز مفيد جداً عند وجود نص يوجد به الكثير من التكرارات ، على سبيل المثال

WWWWWWWWWWWWBWWWWWWWWWWWWBBBWWWWWWW
WWWWWWWWWWWWWWWWWBWWWWWWWWWWWWWW

إذا طبقنا ترميز (RLE) نحصل على ما يلي:

12W1B12W3B24W1B14W

3.10.1.2 خوارزمية ليمبيل زيف فيليش

خوارزمية مشهورة لضغط البيانات بدون ضياع أي جزء منها، تم إنشاؤها من قبل آبراهام ليمبيل ,جاكوب زيف ,وتيري فيلش.

تم نشرها من قبل فيلش عام 1984 كتحسين لخوارزمية lz77/78 المنشورة من قبل ليمبيل وزيف عام 1978. الخوارزمية مصممة لتكون سريعة لكنها عادةً لا تصل للحالة المثالية لضغط البيانات لأنها تقوم بتحليل محدود للبيانات.

تستخدم هذه الخوارزمية ضمن عدة تقنيات وعمليات, كضغط النصوص و كمرحلة من مراحل ضغط الصور.

4.10.1.2 خوارزمية هوفمان

تقوم هذه الخوارزمية على فكرة إعطاء الحرف الأكثر تكراراً في الملف أقل عدد ممكن من ال bits لتمثيله و الحرف الأقل تكراراً عدد أكبر من الbits لتمثيله [2].

11.1.2 خوارزمية هوفمان (Huffman Algorithm)

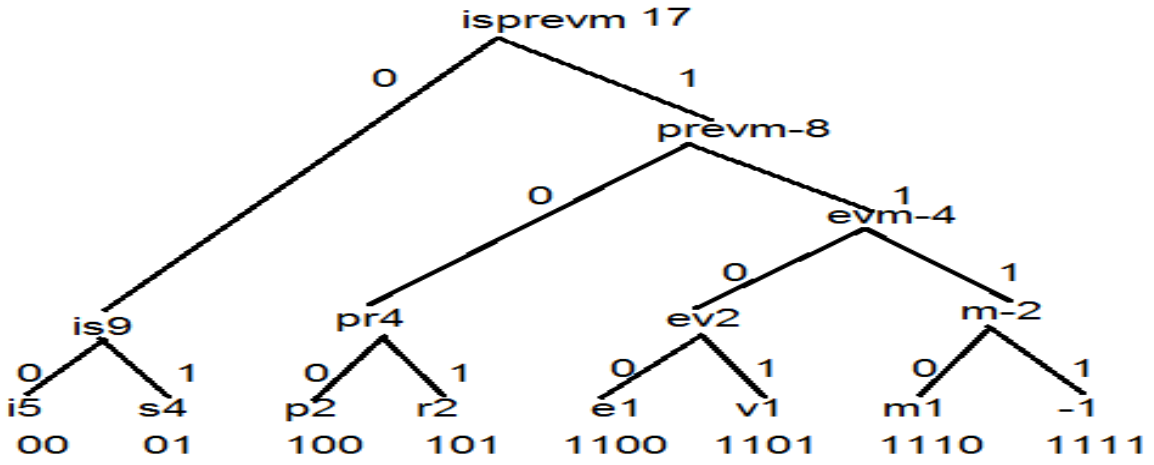
تقوم هذه الخوارزمية على فكرة إعطاء الحرف الأكثر تكراراً في الملف أقل عدد ممكن من ال bits لتمثيله و الحرف الأقل تكراراً عدد أكبر من الbits لتمثيله .

تبدأ خوارزمية هوفمان إستناداً إلى قائمة الحروف التي يتم ترتيبها تنازلياً حسب عدد مرات ورودها في الملف المراد ترميزه. ثم يتم إنشاء شجرة مع رمز في كل ورقة (leaf node). يتم بناء الشجرة من أسفل إلي أعلى ، وذلك بإختيار الورقتان اللتان يحتويان على الحرفين الأقل تكراراً ويكونا عقدة جديدة تمثل الأب لهما (parent) وحاصل جمع تكرار الأولى إلى الثانية يمثل قمية العقدة الجديدة ، يتم ترقيم المسار(edge) من الأب إلي الابن الايسر (leftchild) بالرقم (0) و الإبن الأيمن(rightchild) بالرقم (1)، يتم تكرار العملية إلى أن نصل إلي جذر الشجرة (root)الذي تكون قيمته حاصل جمع كل التكرارات. وأخيراً يتم تعيين رمز(code) لكل ورقة يعتمد على المسار من العقدة الجذر(root) إلى الحروف في اوراق الشجرة [2]. مثلا : Mississippi River

الجدول 2.1.2 يوضح عدد تكرارات الحروف في كلمة Mississippi River

الحرف	التكرار
I	5
S	4
P	2
R	2
M	1
E	1
V	1
Space(-)	1

في جملة Mississippi River عدد الحروف هو 17 حرف و كل حرف يمثل 8bits في الحاسوب (ASCII) ، أي نحتاج الي 136 bit s (8*17) لهذه الجملة .



الشكل 10.1.2 يوضح شجرة ترميز هوفمان

الجدول 3.1.2 يوضح التشفير لكل حرف من حروف كلمة Mississippi River

الحرف	الكود
I	00
S	01
P	100
R	101
E	1100
V	1101
M	1110
Space(-)	1111

أما جملة Mississippi River بواسطة هوفمان نحتاج الي 46bits فقط لتمثيل هذه الجملة :

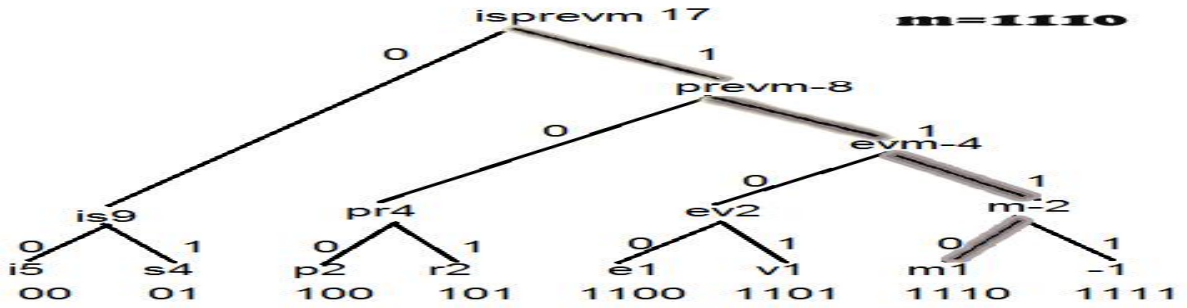
1110000101000101001001000011111010011011100101=46bits

و لإستخراج النص الاصلي من النص المضغوط نبدا من جذر الشجرة (root)و نأخذ اول bit من النص المضغوط اذا كانت (0) تعني الذهاب لل (left child) له اما اذا كانت (1) تعني الذهاب إلى ال (right child) له ، ثم نختبر هل الابن (child) هو ورقة (leaf node) في الشجرة ام لا، اذا كان كذلك نكتب الحرف الموجود فيها و ناخذ ال bit التي تليها و نبدا من جذر الشجرة و نبحث عن الحرف التالي عن طريق المسار من الجذر الي اوراق الشجرة التي تحتوي على الحروف اما اذا كانت ليست ورقة (leaf node) ناخذ ال bit التي ليها و نختبر هل هي تقود الي الابن الايسر او الايمن و نواصل المرور على الشجرة حتي نصل الي ورقة ، و هكذا الي أن نكمل النص كله

مثلا مناخذ المثال السابق للجملة Mississippi River النص المضغوط لها هو :

1110000101000101001001000011111010011011100101

لانستخراج اول حرف من النص المضغوط نأخذ مثلاً اول (4 bits) من النص وهي (1110)



الشكل 11.1.2 يوضح مسار علمية الإسختراج في ترميز هوفمان

الـفـــصــل الثاني

الدراسات السابقة

1.2.2 المقدمة

قدم عدد كبير من الباحثين دراسات في مجال الإخفاء وكذلك في مجال ضغط البيانات ولكن قليلاً منهم تطرق إلى إخفاء البيانات المضغوطة حيث إن الملف الغطاء عادة يكون أكبر بكثير من الرسالة المراد إخفاءها لذا لا تحتاج إلى ضغط البيانات وهنا تأتي أهمية البحث في معالجة البيانات وتقليل حجمها بواسطة خوارزمية هوفمان ثم إخفائها في ملف الصوت وسبب إختيار طريقة هوفمان بالذات لأنها تقوم بترميز البيانات ليس فقط للتقليل من حجمها ولكن أيضا لزيادة سريتها عن طريق الضغط حيث إن الشخص غير المخول له لن يستطيع الوصول إلى النص السري بسبب ترميز البيانات المطبق قبل إخفائها .بالإضافة إلى ذلك زيادة حجم البيانات المخفية داخل ملف الصوت[14].

2.2.2 الدراسات السابقة

شهدت الأعوم السابقة ظهور الكثير من التعاملات مع أنظمة الإخفاء وبالأخص الملفات الصوتية حيث تمكن العالم Yan وزملائه من إنتاج تقدم جديد في التعامل مع الإخفاء في الملف الصوتي ، وكان الإهتمام واضح بملف الصوت ذو الإمتداد mp3 ضمن أعمال العالم diqun والذي قدم خوارزمية جديدة للإخفاءفي ملف mp3 في عام 2009 ، وهذا ما حصل في العام نفسه مع العالمين Wang & Yan حيث تمكنا من تقديم عملهم كتقنية جديدة للتعامل مع الإخفاء ضمن ملفات الصوت ذات الإمتداد mp3 ، وجاء العام 2010 الذي استطاع فيه العالم AL-RABABAH من عرض فكرته للتعامل مع ملفات الصوت ذات الإمتداد MP3 والذي يعمل كجزء خاص من أجزاء الفيديو MPEG [14].

وقامت شهد عبد الرحمن من جامعة الموصل بإقتراح خوارزمية جديدة لضغط البيانات بطريقة هوفمان ثم إخفائها في ملف صوت باستخدام مفتاح لتوزيع البيانات المرمزة داخله وبطريقة LSB المعروفة ،و من ثم يتم خزن الناتج في ملف صوت جديد ، وفي مرحلة الاسترجاع يتم استرجاع القيم المرمزة وفك ترميزها بنفس طريقة الترميز[14].

ولكن تتمثل مشكلة هذه الدراسة ظهور التشويش بصورة واضحة في الملف الصوتي الناتج .

تم الإستفادة من هذه الدراسة بإستخدام طريقة هوفمان للضغط المعلومات للتمكن من تخزين أكبر قدر ممكن من المعلومات وكذلك تم إستخدام خوارزمية الإخفاء في البت الأقل أهمية .

قام عادل صبري ورضوان يوسف في عام 2007 بتصميم نظام إخفاء يعمل على تقليل التشويش الحاصل عند الإخفاء والتخلص منه وذلك بإستخدام تقنية القفز بعدد من البتات عند كل عملية إخفاء ، وقد تم الإعتماد على الأذن البشرية لمجموعة من الأشخاص لقياس تقليل التشويش في الملف الحامل للرسالة، وفي حالة التمثيل الثماني تم إستخدام البت الاول من كل بايت في عملية الاخفاء .

وإستنتج أن أي تشويش حاصل يختفي تماماً عند القفز ب 10 بايت في كل عملية إخفاء، وإستنتج أيضاً أن التشويش قد إختفى تماماً عند القفز 30 بايت عندما إستخدم البت الأول والثاني من كل بايت في عملية الإخفاء.

وفي التمثيل السداسي عشر تم التوصل إلى إلغاء التشويش تماما عند القفز ب 10 بايت مهما كان عدد البتات المستخدمة في النصف الأول من كل بايت[1].

ولكن مشكلة هذه الدراسة تتمثل في عجز النظام المصمم عن إخفاء أحجام كبيرة من الملفات النصية .

تم إستخدام تقنية القفز المستخدمة في الدراسة أعلاه للإستفادة منها في تقليل التشويش في الملف الصوتي الناتج .

البـــاب الثالث

تصميم النظام

الفصل الأول: تصميم النظـــام

الفصل الثاني:التجـــارب علـي النظـــام

الـفـــــصـــل الأول

تصميم النظـــــام

1.1.3 المقدمـــــة

يختص هذا الفصل بوصف المنهجية المتبعة و توضيح واجهات البرنامج و الخطوات التي يتم إتباعها في عملية تضمين الملف النصي و في عملية إستخراجه من الملف الصوتي.

2.1.3 المنـهجية المتبعة

1. تضمين الرسالة في ملف الصوت

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

- قراءة الملف الصوتي.
- قراءة الرسالة النصية من ملف نصي.
- تحويل كل منهما إلي ثنائي وتتم عملية تحويل الملف النصي إلي ثنائي بعد عملية الضغط بإستخدام خوارزمية (Huffman).
- إخفاء الملف النصي داخل الملف الصوتي.
- ومن ثم إرسال الرسالة إلي الطرف الأخر(المستقبل).

2. إسترجاع الرسالة

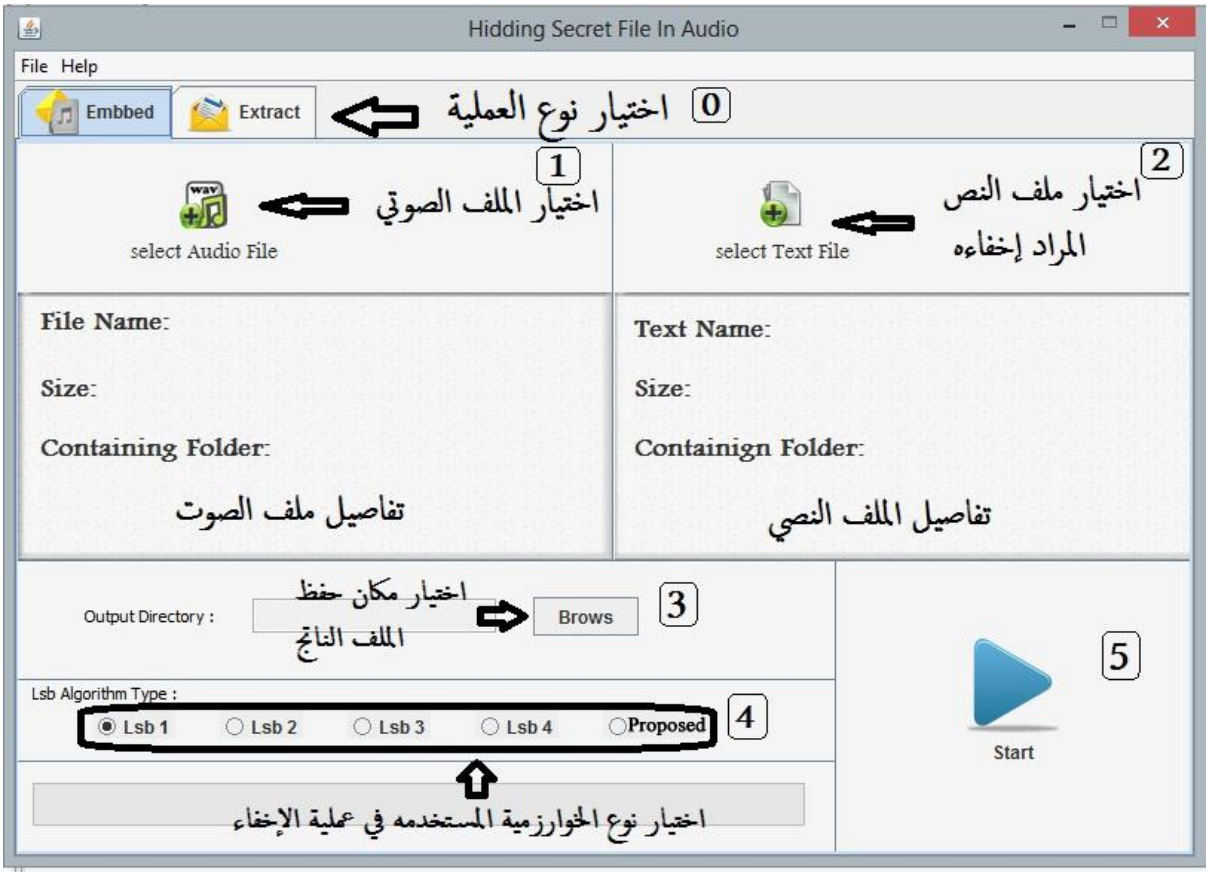
يقوم مستقبل الرسالة بالأتي :

- إستقبال الرسالة من الطرف المرسل وإستخراج جميع ال bits في خانات ال (LSB).
- ومن ثم فك ضغط الرسالة و إستخراجها .
- تحويل الbits من ثنائية إلي نص ،وبذلك يصبح لديه الرسالة المرسلة من قبل المرسل.

3.1.3 تصميم النظام

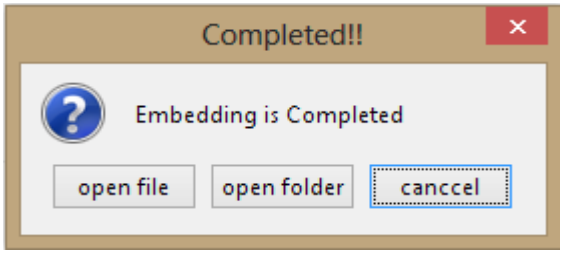
ينقسم النظام إلي قسمين، قسم يشرح عملية التضمين للملف النصي داخل الملف الصوتي بإستخدام إحدي طرق تطبيق خوارزمية البت الأقل أهمية، وعند بدأ عملية تنفيذ النظام يظهر للمستخدم لوحة يختار منها إما أن يقوم بعملية التضمين للملف النصي داخل الملف الصوتي أو إستخراج الملف النصي من الملف الصوتي.

في عملية تضمين الملف يتم إختيار طريقة تطبيق عملية التضمين ومن ثم إختيار الملف الصوتي المراد تضمين النص به وإختيار ملف النص المراد تضمينه ومن ثم إختيار المسار لحفظ الملف الصوتي الجديد (الملف الذي يحوي البيانات المخفية بداخله) ومن ثم الضغط علي زر البدء في عملية التضمين كما هو موضح بالشكل (1.3) :



الشكل 1.3 يوضح كيفية إجراء عملية التضمين

بعد الإنتهاء من عملية التضمين تظهر رسالة للمستخدم تفيد بذلك كما هو موضح في الشكل (2.3) :

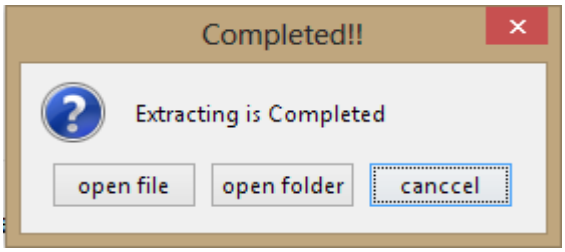


الشكل 2.3 يوضح الرسالة التي تظهر بعد عملية التضمين

أما في عملية الإستخراج يتم إختيار الملف الصوتي الذي يحتوي على المعلومات المضمنة بداخله ومن ثم تحديد مسار إستخراج الملف النصي المضمن ومن ثم الضغط علي زر البدء في عملية الإستخراج كما هو موضح بالشكل (3.3) :

الشكل 3.3 يوضح كيفية إجراء عملية الإستخراج

بعد الإنتهاء من عملية الإستخراج تظهر رسالة للمستخدم تفيد بذلك كما هو موضح في الشكل (4.3) :



الشكل 4.3 يوضح الرسالة التي تظهر بعد عملية الإستخراج

الـفـــصــل الثاني

التجـــارب على النظـــام

1.2.3 المقدمـــــة

يختص هذا الفصل بتوضيح مجموعة من التجارب التي تمت علي النظام، حيث تم تطبيق مجموعة من التجارب علي عملية تضمين الملف النصي داخل الملف الصوتي وذلك بإستخدام مجموعة من الملفات الصوتية والنصية مختلفة الأحجام المضغوطة أو غير المضغوطة لكل طريقة من طرق خوارزمية البت الأقل أهمية لقياس مدي تأثير كل طريقة علي جودة الملف الصوتي الناتج .

2.2.3 التجـــــارب

لمقارنة الخوارزمية المقترحة مع الخوارزميات الأساسية قمنا بإجراء عدة تجارب إستخدمنا فيها ثلاث ملفات للصوت بأحجام مختلفة وثلاث ملفات للنص بأحجام مختلفة أيضاً .

تم أخذ ثلاث أحجام مختلفة للملف الصوتي تتدرج من ملف صوتي ذو حجم صغير إلي ملف صوتي ذو حجم كبير كما هو موضح بالجدول أدناه :

الجدول 1.2.3 يوضح أسماء الملفات الصوتية المستخدمة وأحجامها

إسم الملف الصوتي	حجم الملف الصوت بال(KB)
Audio 1	1,730
Audio 2	3,586
Audio 3	10,177

وتم أيضا إختيار أحجام مختلفة من الملفات النصية تتدرج أحجامها كما هو موضح بالجدول أدناه :

الجدول 2.2.3 يوضح أسماء الملفات الصوتية المستخدمة وأحجامها

إسم الملف الصوتي	حجم الملف النصي بال(KB)
Text 1	84
Text 2	132
Text 3	444

ومن ثم تم قياس جودة الصوت بإستخدام مقياسين هما PSNR , MSE لكل طريقة من الطرق الخمس(LSB 1, LSB 2,LSB 3,LSB 4,Propsed LSB) وتم إنشاء جداول مختلفة من النتائج التي تم التوصل إليها.

لكل طريقة من طرق الإخفاء بإستخدام خوارزمية البت الأقل أهمية يوجد جدولين الجدول الأول يوضح قيم معادلة الPSNR وجدول يوضح قيم معادلة الMSE .

وأيضا يوضح كل جدول حالة الملف النصي وذلك بتوضيح ما إذا كان الملف النصي مضغوطاً أم لا .

البـــاب الرابع

النتائج

1.4 المـــقـــدمـــــة

يخضع ملف الصوت لأنواع كثيرة من التشوهات خلال المراحل التي قد تمر به مثل تخزين ومعالجة وضغط وهذه التشوهات تؤثر على جودة الصوت ،و هناك عدة مقاييس تسخدم لتقييم جودة الصوت مثل MSE , RMSE , PSNRو هي من أكثر المقاييس اتستخداماَو شيوعاَ.

لتقييم أداء كل خوارزمية من خوارزميات الLSB والخوارزمية المقترحة ومعرفة أي الخوارزميات تعطي تنائج أفضل و يتم ذلك بقياس جودة الصوت النتاتج من كل خوارزمية ، و تم إستخدام MSE , PSNR كمقاييس لجودة الصوت .

2.4 مقياس (PSNR)

عبارة عن مصطلح هندسي للنسبة بين أعلى درجة للإشارة و الضوضاء التي تؤثر على دقة الإشارة , تم إستخدام هذا المقياس في حساب جودة الملف الصوتي قبل عملية التضمين و حساب جودة الملف الصوتي الناتج بعد عملية التضمين.

$$PSNR = 10 * log10 \left(\frac{MAX_i^2}{MSE}\right)$$

MAX ≡ اعلى قيمة للإشارة الصوتية في العينة المستخدمة, يتم حسابها كما يلي

$$MAX_I = 2^B - 1$$

B ≡ عدد ال bits في العينة المستخدمة (Bits per sample) .

مثلا اذا كانت قيمة ال B تساوي 8 تكون قيمة ال PSNR بين 30 و 50 , و اذا كانت تساوي 16 تكون قيمة ال PSNR بين 60 و 80 و هكذا .

MSE ≡ هي معادلة لقياس متوسط مربعات الأخطاء في العينة المستخدمة .

3.4 مقياس (MSE)

هو مربع متوسط الفرق بين ملف الصوت الاصلي والملف المعدل

$$MSE = \frac{1}{M * N} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - K(i,j)]^2$$

4.4 الـنـــتـــائج

تم إجراء مجموعة من التجارب علي كل ملف صوتي وذلك بتضمين مختلف أحجام الملفات النصية ومن ثم قياس جودة الملف الصوتي الناتج من كل تجربة وذلك بحساب أعلى نسبة للإشارة إلى الضوضاء (PSNR) و متوسط مربعات الأخطاء (MSE) لكل خوارزمية وتم تدوين النتائج في الجداول التالية :

الجدول 1.4 يوضح نتائج ال PSNR لخوارزمية LSB 1

الملفات وأحجامها	LSB 1 With Compression			LSB 1 Without Compression		
	Audio 1 (1,730KB)	Audio 2 (3,586KB)	Audio 3 (10,177KB)	Audio 1 (1,730KB)	Audio 2 (3,586KB)	Audio 3 (10,177KB)
Text 1 (84 KB)	75.4718	77.0534	79.3846	74.2984	75.8522	77.7806
Text 2 (132 KB)	74.4793	76.0690	78.3881	73.3137	74.8797	76.9339
Text 3 (444 KB)	73.7421	73.5179	75.7738	72.4786	72.2709	74.4685

الجدول 2.4 يوضح نتائج ال MSE لخوارزمية LSB 1

الملفات وأحجامها	LSB 1 With Compression			LSB 1 Without Compression		
	Audio 1 (1,730KB)	Audio 2 (3,586KB)	Audio 3 (10,177KB)	Audio 1 (1,730KB)	Audio 2 (3,586KB)	Audio 3 (10,177KB)
Text 1 (84 KB)	0.000003	0.000002	0.000001	0.000006	0.000003	0.000001
Text 2 (132 KB)	0.000005	0.000003	0.000001	0.000009	0.000005	0.000002
Text 3 (444 KB)	0.000008	0.000008	0.000003	0.000014	0.000015	0.000005

الجدول 3.4 يوضح نتائج ال PSNR لخوارزمية LSB 2

الملفات وأحجامها	LSB 2 With Compression			LSB 2 Without Compression		
	Audio 1 (1,730KB)	Audio 2 (3,586KB)	Audio 3 (10,177KB)	Audio 1 (1,730KB)	Audio 2 (3,586KB)	Audio 3 (10,177KB)
Text 1 (84 KB)	71.7438	73.5448	75.1828	70.8978	72.6773	74.0800
Text 2 (132 KB)	70.8393	72.5669	74.2579	69.9887	71.6913	73.3730
Text 3 (444 KB)	70.1495	70.0496	72.0676	69.1942	69.0629	71.1416

الجدول 4.4 يوضح نتائج ال MSE لخوارزمية LSB 2

الملفات وأحجامها	LSB 2 With Compression			LSB 2 Without Compression		
	Audio 1 (1,730KB)	Audio 2 (3,586KB)	Audio 3 (10,177KB)	Audio 1 (1,730KB)	Audio 2 (3,586KB)	Audio 3 (10,177KB)
Text 1 (84 KB)	0.000019	0.000008	0.000004	0.000028	0.000013	0.000007
Text 2 (132 KB)	0.000029	0.000013	0.000006	0.000043	0.000020	0.000009
Text 3 (444 KB)	0.000040	0.000042	0.000017	0.000062	0.000066	0.000025

الجدول 5.4 يوضح نتائج ال PSNR لخوارزمية LSB 3

الملفات وأحجامها	LSB 3 With Compression			LSB 3 Without Compression		
	Audio 1 (1,730KB)	Audio 2 (3,586KB)	Audio 3 (10,177KB)	Audio 1 (1,730KB)	Audio 2 (3,586KB)	Audio 3 (10,177KB)
Text 1 (84 KB)	69.6391	71.5957	73.0165	68.9412	70.6378	73.2153
Text 2 (132 KB)	68.8083	70.6459	72.0222	68.0490	69.7143	72.1059
Text 3 (444 KB)	68.1656	68.1987	69.9940	67.2538	67.1157	69.4278

الجدول 6.4 يوضح نتائج ال MSE لخوارزمية LSB 3

الملفات وأحجامها	LSB 3 With Compression			LSB 3 Without Compression		
	Audio 1 (1,730KB)	Audio 2 (3,586KB)	Audio 3 (10,177KB)	Audio 1 (1,730KB)	Audio 2 (3,586KB)	Audio 3 (10,177KB)
Text 1 (84 KB)	0.000051	0.000021	0.000011	0.000070	0.000032	0.000010
Text 2 (132 KB)	0.000074	0.000032	0.000017	0.000105	0.000049	0.000016
Text 3 (444 KB)	0.000100	0.000098	0.000043	0.000152	0.000162	0.000056

الجدول 7.4 يوضح نتائج ال PSNR لخوارزمية LSB 4

الملفات وأحجامها	LSB 4 With Compression			LSB 4 Without Compression		
	Audio 1 (1,730KB)	Audio 2 (3,586KB)	Audio 3 (10,177KB)	Audio 1 (1,730KB)	Audio 2 (3,586KB)	Audio 3 (10,177KB)
Text 1 (84 KB)	66.5134	68.6577	69.9879	65.3169	67.1572	69.0281
Text 2 (132 KB)	65.7634	67.7721	69.0009	64.4959	66.2543	67.9277
Text 3 (444 KB)	65.1993	65.3944	66.8457	63.6753	63.6174	65.7011

الجدول 8.4 يوضح نتائج ال PSNR لخوارزمية LSB 4

الملفات وأحجامها	LSB 4 With Compression			LSB 4 Without Compression		
	Audio 1 (1,730KB)	Audio 2 (3,586KB)	Audio 3 (10,177KB)	Audio 1 (1,730KB)	Audio 2 (3,586KB)	Audio 3 (10,177KB)
Text 1 (84 KB)	0.000204	0.000080	0.000043	0.000371	0.000159	0.000067
Text 2 (132 KB)	0.000302	0.000120	0.000068	0.000542	0.000241	0.000112
Text 3 (444 KB)	0.000392	0.000358	0.000184	0.000790	0.000812	0.000311

الجدول 9.4 يوضح نتائج ال PSNR للخوارزمية المقترحة

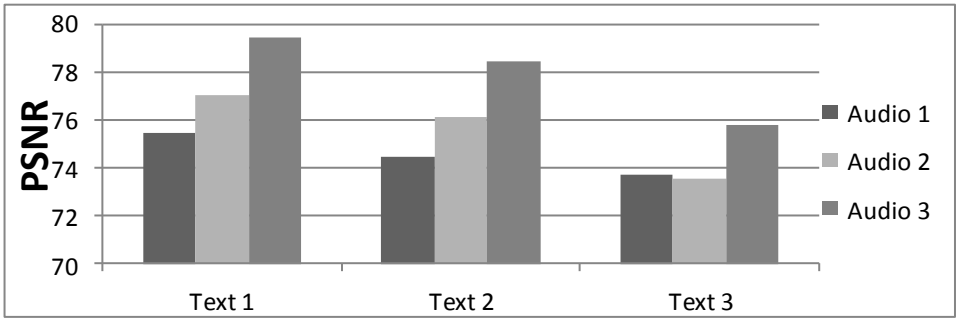
الملفات وأحجامها	Proposed With Compression			Proposed Without Compression		
	Audio 1 (1,730KB)	Audio 2 (3,586KB)	Audio 3 (10,177KB)	Audio 1 (1,730KB)	Audio 2 (3,586KB)	Audio 3 (10,177KB)
Text 1 (84 KB)	79.5287	79.8120	79.7965	79.3471	79.7217	79.5398
Text 2 (132 KB)	79.4667	79.6635	79.6389	78.7768	79.5076	79.3869
Text 3 (300 KB)	79.1193	79.4381	79.2750	79.0011	79.0233	79.2350

الجدول 10.4 يوضح نتائج ال MSE للخوارزمية المقترحة

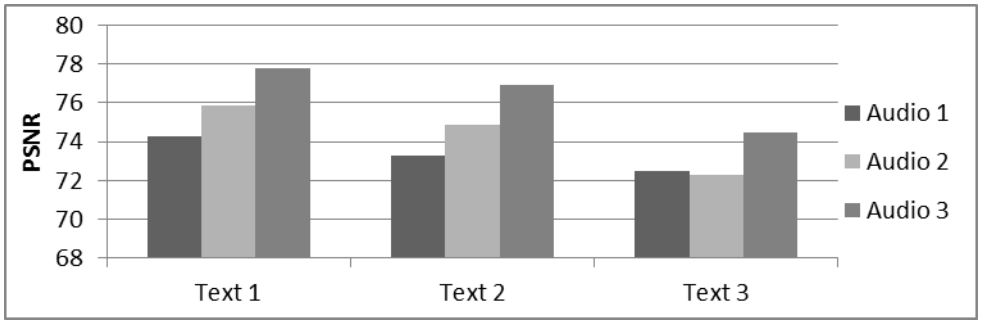
الملفات وأحجامها	Proposed With Compression			Proposed Without Compression		
	Audio 1 (1,730KB)	Audio 2 (3,586KB)	Audio 3 (10,177KB)	Audio 1 (1,730KB)	Audio 2 (3,586KB)	Audio 3 (10,177KB)
Text 1 (84 KB)	0.00000001	0.0000002	0.00000001	0.00000014	0.00000011	0.00000018
Text 2 (132 KB)	0.00000010	0.0000003	0.00000002	0.00000020	0.00000016	0.00000020
Text 3 (300 KB)	0.00000012	0.0000004	0.00000003	0.00000033	0.00000024	0.00000021

5.4 مخططات لتوضيح التباين في النتائج

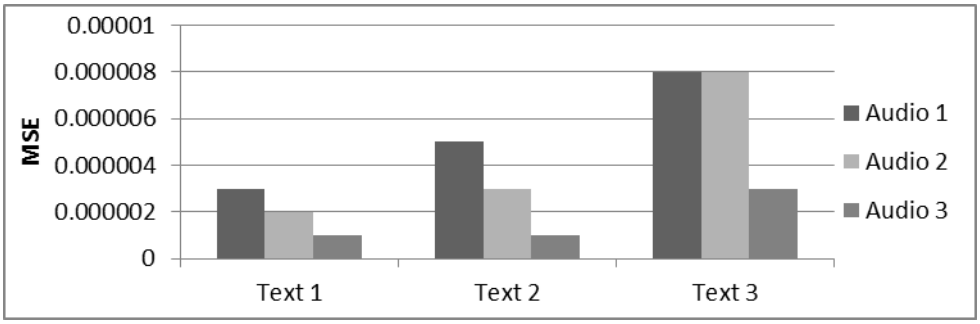
في ما يلي مجموعة من المخططات التي تم تكوينها إعتماداً على الجداول السابقة:



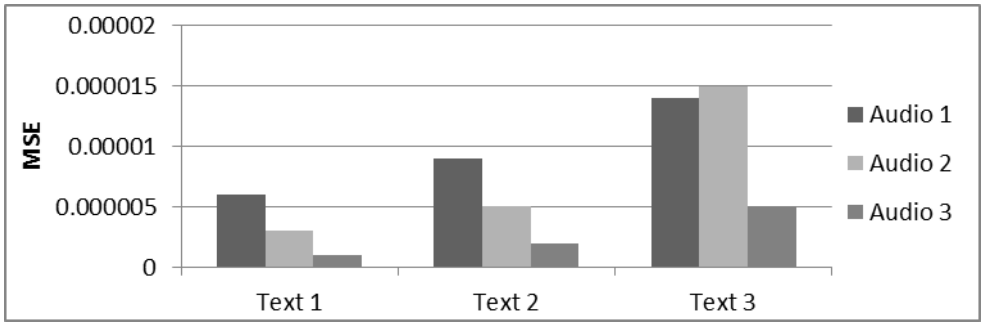
الشكل 1.4 يوضح نتائج ال PSNR لخوارزمية LSB 1 مع ضغط للبيانات



الشكل 2.4 يوضح نتائج ال PSNR لخوارزمية LSB 1 بدون ضغط للبيانات

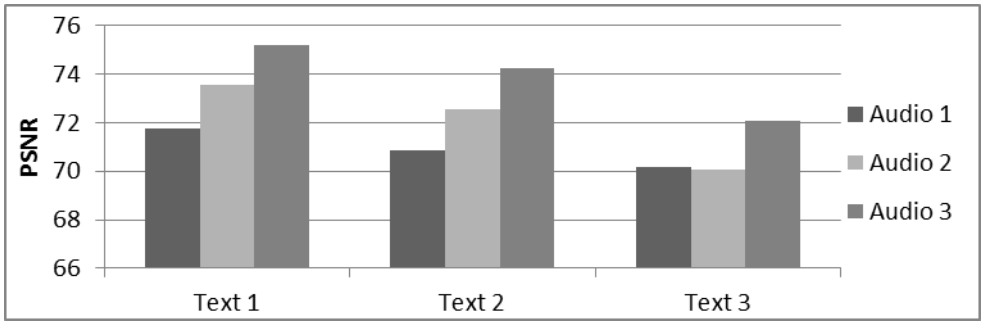


الشكل 3.4 يوضح نتائج ال MSE لخوارزمية LSB 1 مع ضغط للبيانات

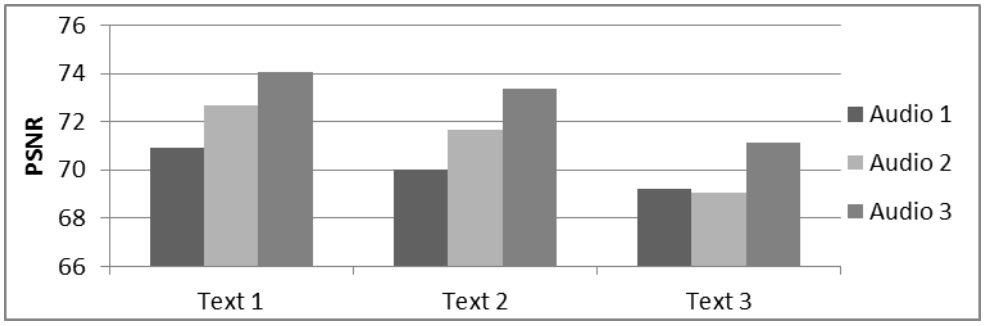


الشكل 4.4 يوضح نتائج ال MSE لخوارزمية LSB 1 بدون ضغط للبيانات

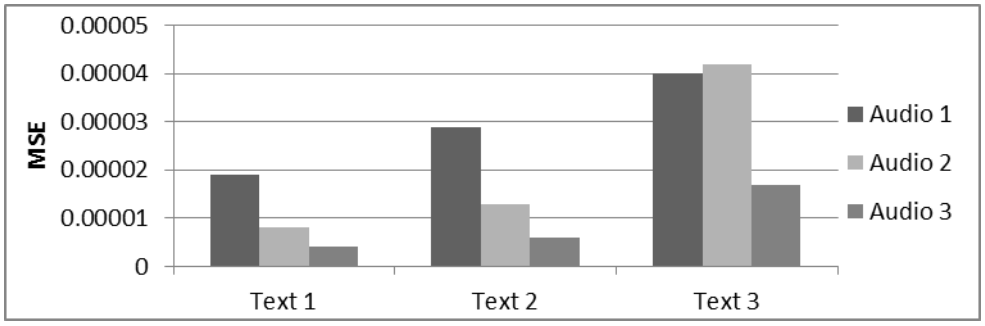
1- من الملاحظ من الأشكال أعلاه أن جودة الصوت تكون عالية في خوارزمية LSB 1 و لكن تخزين بت واحد في كل بايت يقلل من المساحة التخزينية للملف الصوتي وأيضاَ الإختلاف في محتوي الملف الصوتي الأصلي والملف الصوتي الناتج يزيد كلما زاد حجم الملف النصي المخفي بداخل الملف الصوتي الناتج (MSE) .



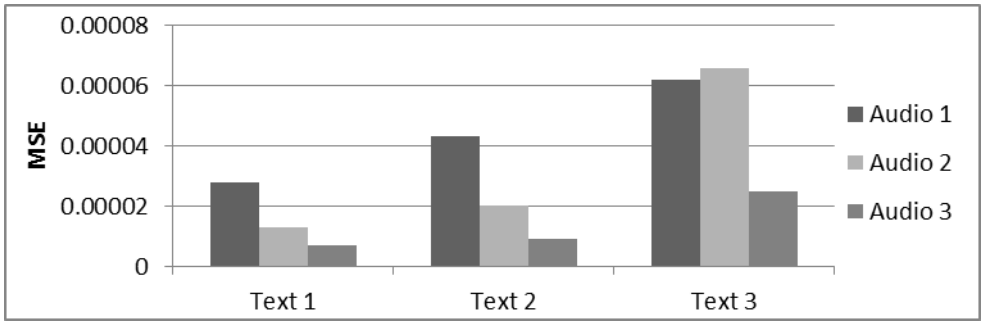
الشكل 5.4 يوضح نتائج ال PSNR لخوارزمية LSB 2 مع ضغط للبيانات



الشكل 6.4 يوضح نتائج ال PSNR لخوارزمية LSB 2 بدون ضغط للبيانات

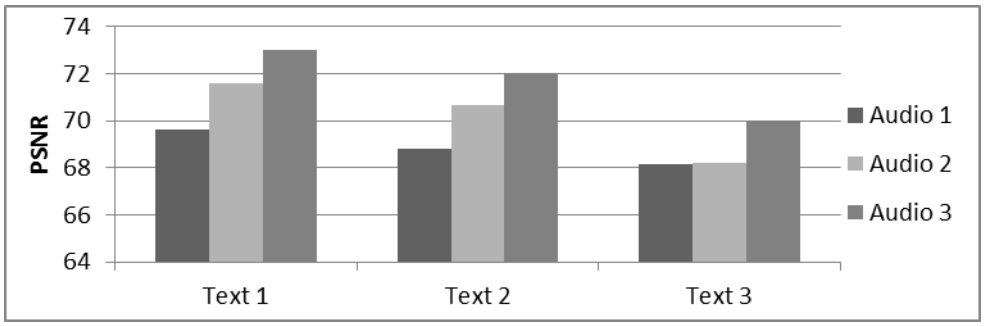


الشكل 7.4 يوضح نتائج ال MSE لخوارزمية LSB 2 مع ضغط للبيانات

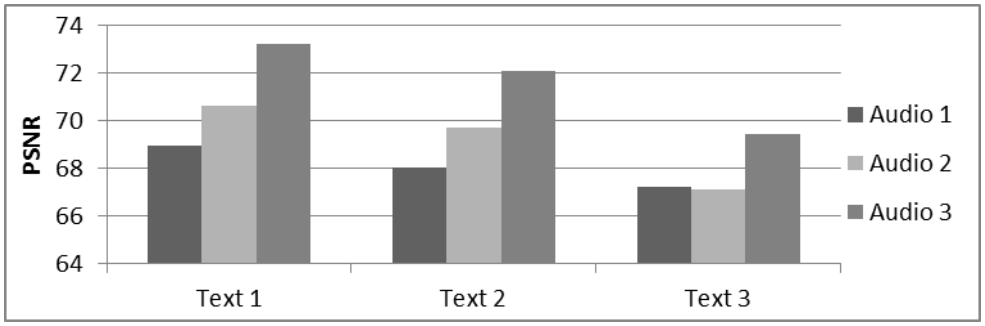


الشكل 8.4 يوضح نتائج ال MSE لخوارزمية LSB 2 بدون ضغط للبيانات

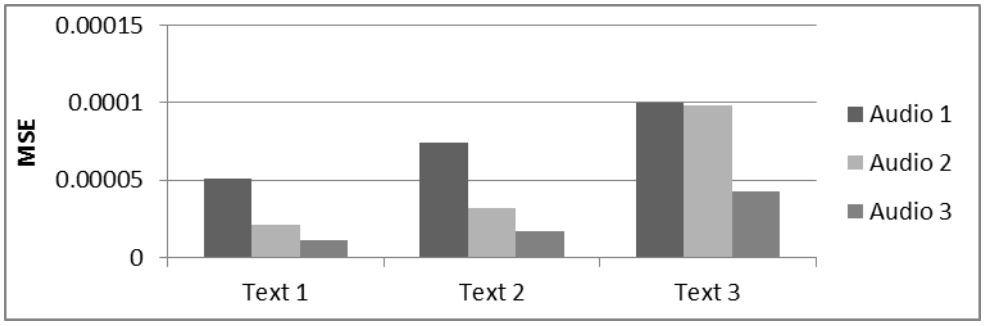
2- من الملاحظ من المخططات أعلاه أن جودة الصوت قد قلت لأن التعديل يشمل خانتين بدلاً من خانة واحدة ، وأن المعلومات المخزنة بطريقة ال LSB 2.يمكنها تخزين قدر مضاعف من الملف النصي بالمقرنة مع الملف النصي المخزن بإستخدام طريقة ال LSB 1 مما يقلل نسبة الإختلاف بين الملفين.



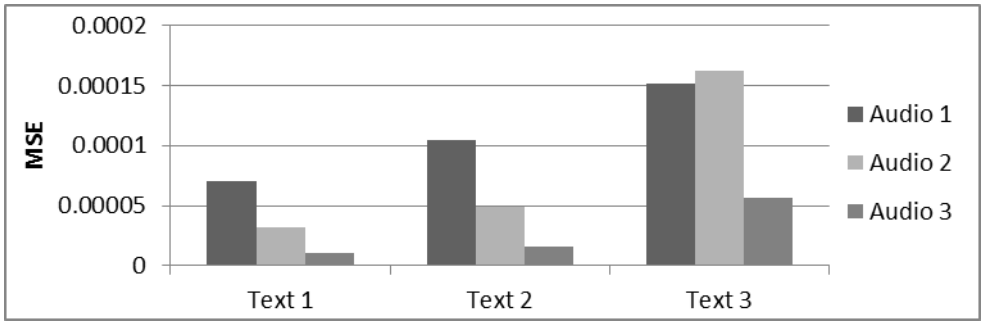
الشكل 9.4 يوضح نتائج ال PSNR لخوارزمية LSB 3 مع ضغط للبيانات



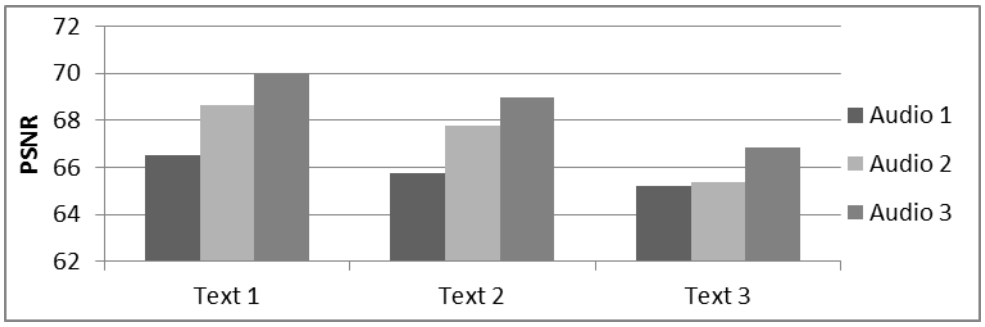
الشكل 10.4 يوضح نتائج ال PSNR لخوارزمية LSB 3 بدون ضغط للبيانات



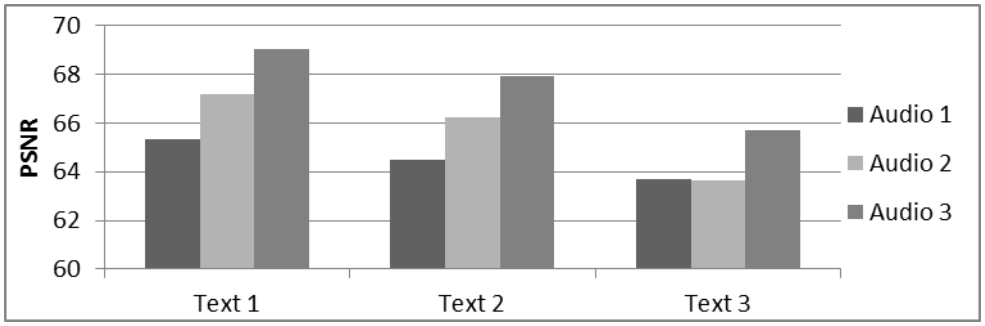
الشكل 11.4 يوضح نتائج ال MSE لخوارزمية LSB 3 مع ضغط للبيانات



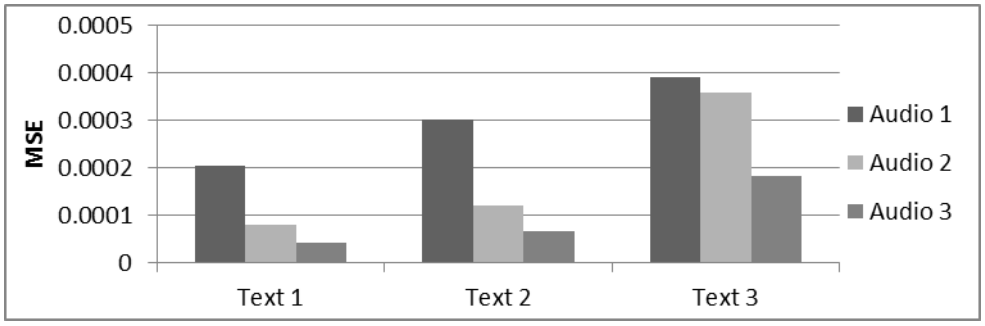
الشكل 12.4 يوضح نتائج ال MSE لخوارزمية LSB 3 بدون ضغط للبيانات



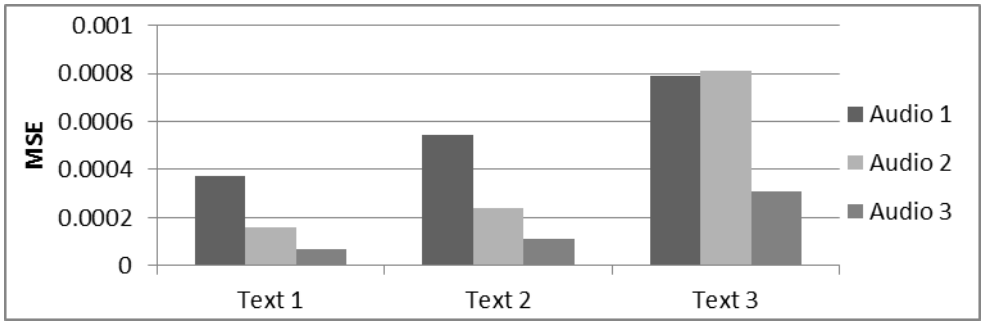
الشكل 13.4 يوضح نتائج ال PSNR لخوارزمية LSB 4 مع ضغط للبيانات



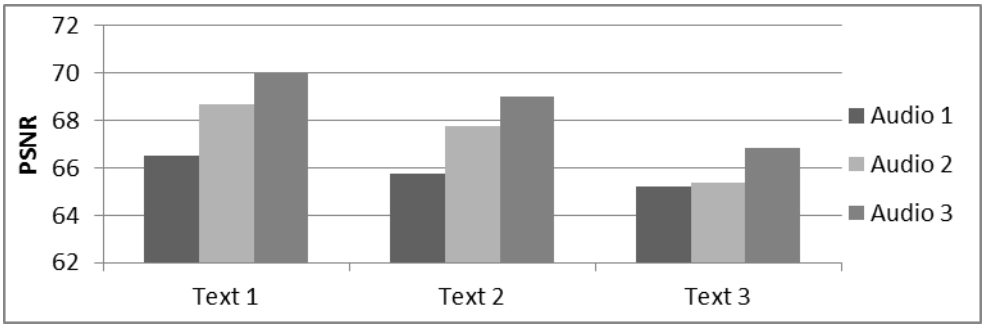
الشكل 14.4 يوضح نتائج ال PSNR لخوارزمية LSB 4 بدون ضغط للبيانات



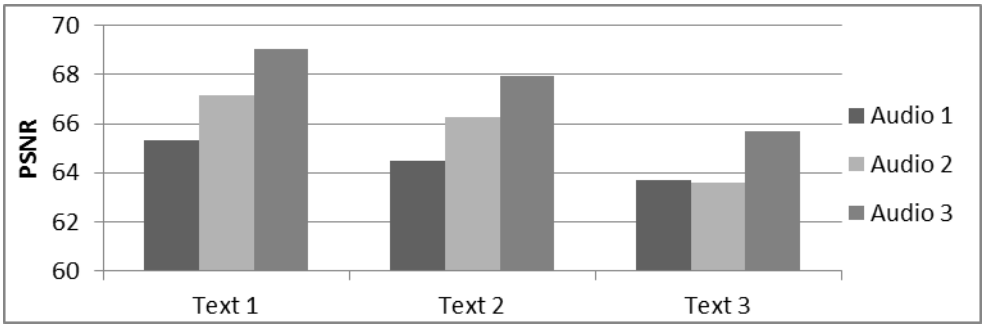
الشكل 15.4 يوضح نتائج ال MSE لخوارزمية LSB 4 مع ضغط للبيانات



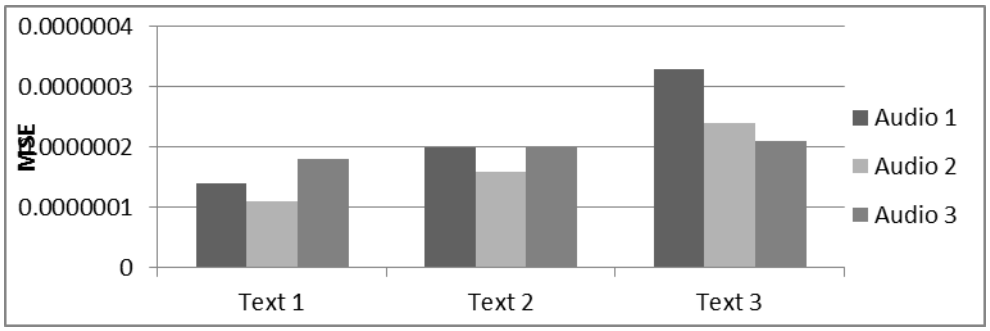
الشكل 16.4 يوضح نتائج ال MSE لخوارزمية LSB 4 بدون ضغط للبيانات



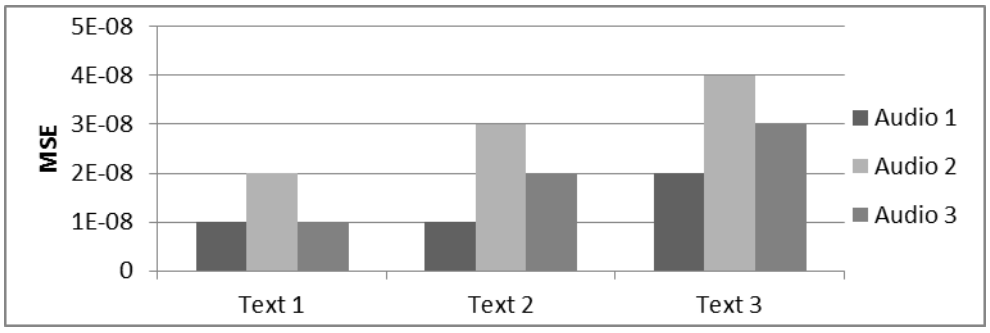
الشكل 17.4 يوضح نتائج ال PSNR الخوارزمية المقترحة مع ضغط للبيانات



الشكل 18.4 يوضح نتائج ال PSNR للخوارزمية المقترحة بدون ضغط للبيانات



الشكل 19.4 يوضح نتائج ال MSE للخوارزمية المقترحة مع ضغط للبيانات



الشكل 20.4 يوضح نتائج ال MSE للخوارزمية المقترحة بدون ضغط للبيانات

3- من الملاحظ من الأشكال أعلاه أن جودة الملف الصوتي الناتج من الخوارزمية المقترحة أعلى من الخوارزميات السابقة , و ذلك لأن تأثير التعديل يقل بسبب طريقة الإخفاء المستخدمة (Jumping technique) في هذه الخوارزمية بغض النظر عن حجم المعلومات المخفية.

4- و أيضا من الملاحظ في الخوارزمية المقترحة أنه بالرغم من أختفاء التشويش يمكن تخزين احجام كبيرة للملفات النصية و ذلك بسبب إستخدام طريقة ال LSB 4 في عملية التضمين.

5- وأيضا الإختلاف بين محتوى الملف الصوتي الأصلي والملف الصوتي الناتج من إخفاء النص بإستخدام الخوارزمية المقترحة يقل بنسبة كبيرة مقارنة بطرق التضمين الأخرى.

البـــاب الخامس

التـــوصيـات والمراجـــع

1.5 التوصيات

حتى يكتمل البرنامج و يعمل بفعالية أكثر نوصي بإضافة مميزات و خصائص جديدة لم نتمكن من تضمينها في هذا المشروع نسبة لضيق الوقت و من أهم التوصيات ما يلي:

1. يمكن الدمج بين تقنيات الاخفاء وعملية التشفير لزيادة سرية الرسالة المخفية.
2. تجريب الخوارزمية المفترحة علي ملفات الفيديو والأفلام وذلك لكبر حجمها.
3. إضافة إمتدادت صوتية جديدة للبرنامج .

2.5الخاتمة

تم بحمد الله وتوفيقه إتمام هذا المشروع حسب المتطلبات لإنشاء تطبيق يقوم بتوفير الحماية اللازمة لتناقل آمن بين مستخدمي الوسائط المتعددة الصوتيه للحفاظ على السرية بينهم .

فالحمد لله الذي بنعمته تتم الصالحات و صلى الله و سلم على خير خلقه و خاتم رسله سيدنا محمد و على آله و صحبه ، و من إستن بسنته إلى يوم الدين .

المراجع

[1] www.iasj.net/iasj?func=fulltext&aId=8115
مقدمة عن تقليل التشويش الملازم عند الإخفاء في ملف صوتي 3:00م 2014/7/20
[2] http://en.wikipedia.org/wiki/Huffman_coding
مقدمة عن ترميز هوفمان 11:00ص 2014/7/21
[3] http://en.wikipedia.org/wiki/Data_compression
مقدمة عن ضغط البيانات 1:00م 2014/7/21
[4] http://en.wikipedia.org/wiki/Steganography
مقدمة عن علم الإخفاء 8:00م 2014/7/18
[5] ijcsi.org/papers/IJCSI-9-1-1-30-37.pdf
دراسة ميداينية عن علم الإخفاء 8:30م 2014/7/18
[6] http://en.wikipedia.org/wiki/WAV
مقدمة عن إمتداد الصوت wav 3:00م 2014/7/23
[7] http://mathmatrix.narod.ru/Wavefmt.html
التقسيم الداخلي للملف ذو الإمتداد wav 3:10م 2014/7/23
[8] arxiv.org/pdf/0912.2319
مقدمة عن علم الإخفاء و فن إخفاء البيانات 4:00م 2014/7/18
[9] www.ijetae.com/files/Volume3Issue6/IJETAE_0613_25.pdf
الإخفاء بإستخدام تقينة البت الأقل أهمية 6:00م 2014/7/20
[10] www.airccse.org/journal/jma/3311ijma08.pdf
مقدمة عن إخفاء البيانات في ملف الصوت 1:20م 2014/7/19
[11]أمن المعلومات http://ar.wikipedia.org/wiki/
أمن المعلومات 12:00م 2014/3/12
[12] http://www.scincear.com/إخفاء-المعلومات-steganography-2/
إخفاء المعلومات 1:00م 2014/2/13
[13] http://ar.wikipedia.org/wiki/صيغة_الملفات_الصوتية
صيغة الملفات الصوتية 11:00 ص 2014/3/15
[14] www.iasj.net/iasj?func=fulltext&aId=71743
إخفاء النصوص المكبوسة في ملف صوتي 3:00م 2014/5/21