# إخفاء صوت داخل صورة ملونة

**رسالة مقدمة**
إلى مجلس كلية العلوم - جامعة بابل
كجزء من متطلبات نيل درجة الماجستير في علوم
الحاسبات

من

**شيماء عبد الحمزه محمد الكرعاوي**

آذار –٢٠٠٦ م صفر-١٤٢٧هـ

# Speech In Image Steganography

**A Thesis**
**Submitted to the Council of College of Science**
**University of Babylon**
**In partial fulfillment of the Requirements for the degree of**
**Master of Science in computer science**

By

**Shaymaa Abdul Hamza Mohemmed Al-Garawi**

Sufer -١٤٢٧ March–٢٠٠٦

# إخفاء صوت داخل صورة ملونة

**رسالة مقدمة**
إلى مجلس كلية العلوم - جامعة بابل
كجزء من متطلبات نيل درجة الماجستير في علوم
الحاسبات

من

**شيماء عبد الحمزه محمد الكرعاوي**


آذار –٢٠٠٦ م صفر-١٤٢٧هـ

# Speech In Image Steganography

**A Thesis**
**Submitted to the Council of College of Science**
**University of Babylon**
**In partial fulfillment of the Requirements for the degree of**
**Master of Science in computer science**

By

**Shaymaa Abdul Hamza Mohemmed Al-Garawi**

March–٢٠٠٦ Sufer -١٤٢٧

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

قَالَ رَبِّ اجْعَل لِّيَ آيَةً قَالَ آيَتُكَ أَلاَّ تُكَلِّمَ النَّاسَ ثَلاَثَةَ أَيَّامٍ إِلاَّ رَمْزاً وَاذْكُر رَّبَّكَ كَثِيراً
وَسَبِّحْ بِالْعَشِيِّ وَالإِبْكَارِ

صدق الله العظيم

سورة آل عمران/ ٤١/

# شكر وتقدير

لا يسعني إلا أن اشكر الله سبحانه وتعالى على ما آتاني من فضله وعلمه وأمدني من الصبر والقوة والعزم لإكمال رسالتي .

* * *

أود أن أعرب عن خالص شكري وامتناني لأستاذي المشرف ، الأستاذ الدكتور نبيل هاشم كاغد ألا عرجي على تواصله المستمر في إبداء توجيهاته السديدة و آرائه القيّمة للمضي قدما في إنجاز البحث ، واشكر أستاذي

المشرف ، الدكتور توفيق عبد الخالق الأسدي على تفانيه في تقديم يد المساعدة وتوفير المصادر اللازمة لإنجاز البحث ، فجزاهما الله عني خير جزاء وسدد خطاهما .

* * *

أشكر زملائي وزميلاتي و منتسبي قسم علوم الحاسبات في جامعة بابل لتعاونهم في إرساء خطاي وتثبيت عزيمتي لإكمال الرسالة ، وأشكر جميع من شد من أزري وألهمني الصبر ، وأتقدم بالشكر الجزيل للآنسة نجلاء المياحي، الآنسة هبه الخفاجي والآنسة هدى المعموري لتعاونهنّ الشديد .

* * *

أشكر جميع أساتذتي في السنة التحضيرية ، وأخص بالذكر منهم من لم يتسنَ لي أن اشكره ، لإنسانيته وعدالته وعلمه الرفيع الأستاذ الدكتور محمد الشربيني (رحمه الله) .

* * *

الإهداء

إلى أمي وأبي..

وإلى أسرتي ..

# مع كل الحب والامتنان

## إقرار الأستاذ المشرف

اشهد بأن هذه الرسالة الموسومة بـ(إخفاء صوت داخل صورة ملونة) قد جرى تحت إشرافي في قسم علوم الحاسبات – كلية العلوم – جامعة بابل ، وهي جزء من متطلبات نيل درجة ماجستير في علوم الحاسبات .

التوقيع :

اسم المشرف : أ.د.نبيل هاشم كاغد ألاعرجي

المرتبة العلمية : أستاذ

التاريخ : / /٢٠٠٦

التوقيع :

اسم المشرف : د.توفيق عبد الخالق عباس ألاسدي

المرتبة العلمية : أستاذ مساعد

التاريخ : / /٢٠٠٦

## توصية رئيس القسم

**إشارة إلى التوصية أعلاه المقدمة من الأستاذ المشرف أحيل هذه الرسالة إلى لجنة المناقشة لدراستها وبيان الرأي فيها .**

**التوقيع :**
**اسم رئيس القسم : د.عباس محسن البكري**
**المرتبة العلمية : أستاذ مساعد**

التاريخ : / /٢٠٠٦

قرار لجنة المناقشة

**نحن أعضاء لجنة المناقشة ، نشهد بأننا قد اطلعنا على الرسالة الموسومة بـ (إخفاء صوت داخل صورة ملونة) . وقد ناقشنا الطالبة (شيماء عبد الحمزه محمد) في محتوياتها وفيما له علاقة بها وذلك بتاريخ ٢٠٠٦/٨/١٠ ووجدنا أنها جديرة بالقبول بدرجة (جيد جداً) لنيل درجة ماجستير في علوم الحاسبات .**

**التوقيع :**
**عضو اللجنة: د.فاضل عبد العباس**
**المرتبة العلمية : أستاذ مساعد**
**العنوان : المعهد التقني/كوفة**
التاريخ : / /٢٠٠٦

**التوقيع :**
**عضو اللجنة:د.عباس محسن البكري**
**المرتبة العلمية : أستاذ مساعد**
**العنوان : كلية العلوم/جامعة بابل**
التاريخ : / /٢٠٠٦

التاريخ : / /٢٠٠٦

**التوقيع :**
**عضو اللجنة : د.توفيق عبد الخالق الاسدي**
**المرتبة العلمية : أستاذ مساعد**
**العنوان :كلية العلوم/جامعة بابل**

**التوقيع :**
**عضو اللجنة: د.نبيل هاشم ألاعرجي**
**المرتبة العلمية : أستاذ**
**العنوان :رئاسة جامعة بابل**

التاريخ : / /٢٠٠٦ التاريخ : / /٢٠٠٦

## مصادقة عماده كلية العلوم

**أصادق على ما جاء في قرار اللجنة في أعلاه .**

**التوقيع :**
**الاسم :د.عودة مزعل الزاملي**
**المرتبة العلمية : أستاذ مساعد**
**العنوان : عمادة كلية العلوم**

التاريخ : / /٢٠٠٦

# الخلاصة


يهدف النظام المقترح إلى إخفاء ملف صوتي كبير نسبيا مسجل من مصادر مختلفة : مستوى لوني وبحجم (٢٥٦)أقراص مضغوطة ولاقطة حاسبة ، داخل صورة ملونة ذات (١٢٨).

يتألف النظام المقترح من مرحلتين : المرحلة الأولى هي مرحلة الإخفاء وتتكون من : تقنية تحويل المويجة المتقطعة(DWT) ، تحويل معاملات الصوت ، تقنية تشفير طول السلسلة(RLE) ، تقنية القطاعات المتشابهة وتوليد المفتاح .

مخرجات مرحلة الإخفاء هي: ملف الصورة الحاملة(stego_image) وملف سلسلة المفتاح . يرسل الملفان عبر وسائط الاتصال المختلفة إلى المستلم.

**المرحلة الثانية هي مرحلة الاستخراج:ويستخدم فيها المفتاح كدليل لاستخراج**
**معاملات الصوت من الصورة الحاملة، تليها عملية فك ضغط تشفير طول السلسلة ، معكوس تحويل المعاملات ، معكوس تحويل المويجة المتقطع ، بعدها يتم سماع**
**الرسالة الصوتية.**

استخدمت المنظومة البرمجية الماتلاب الإصدار(٦.٥) (Matlab version ٦.٥) في تنفيذ النظام المقترح.

**Abstract**

The proposed system aims to embed a great sound file that is recorded from different references: compact disks and computer microphone inside color image with (٢٥٦) color level with size (١٢٨).

The system consists of two stages: The first one is the embedding stage which contains: Discrete Wavelet Transform technique, sound coefficients transformations, Run Length Encoding technique, Similar Blocks technique and key generation. The outputs of embedding stage are: stego_image and key sequence file. The two files are transmitted by multi media communications to receiver.

The second stage is the extracting: The key sequence has been used as an index to extract the sound coefficients from the stego_image, inverse Run Length Encoding, inverse sound coefficients transformations, inverse Discrete Wavelet Transform. Then the sound message can be heard.

Matlab version (٦.٥) was used in execution the proposed system.

المحتويات

# الفصل الأول : مقدمة عامة

١



# الفصل الثاني : تقنيات الإخفاء

١٠

# الفصل الثالث : النظام المقترح



# الفصل الرابع : النتائج

## ١.١ مقدمة

في العقود القليلة الماضية ، شهد العالم ثورة في المعلومات والتكنولوجيا، والعامل الرئيس لتلك الثورة هو الحاسبة. إن الحاسبات تجعل الحياة اسهل بكثير لملايين الناس في كل أرجاء العالم. وبوجود الإنترنت نستطيع أن نعلم ما يجري في الشارع حتى لو كنا على بعد آلاف الأميال. وقد يستطيع مستخدم الشبكة القيام بالبيع والشراء وهو مستلق على سريره ، لكن لتحقيق مثل هكذا استقرار في العالم عندما تعقد كثير من الصفقات التجارية فإن بلايين الدولارات تكون في خطر لذا يجب أن يكون هناك نوع من الأمنية لتنظيم حركة المعلومات بين ملايين الحاسبات المربوطة.وحتى لو كانت تقنيات أمنية الحاسبة كفوءة فهناك تهديدات لأمنية الحاسبة لمستخدم الإنترنت.

أصبحت أمنية المعلومات(Information Security) مهمة جدا بسبب تقنيات الاتصالات ، و أمنية المعلومات هو اسم عام لمجموعة أدوات مصممة لحماية البيانات وإحباط المتطفلين . ومن المهم أن تتحقق الأمنية لحماية البيانات أثناء انتقالها . وعندما تكون هناك خدمات أمنية لمجموعة حاسبات في شبكة فإن انتقال المعلومات يحدث بثقة تامة والأشخاص المخولين فقط هم الذين يستطيعون قراءة البيانات ولا يمكن لأي مجموعة أخرى الوصول أليها(٢٠٠١) [١].

**تزود اليوم تقنيات الحاسبات والشبكات قنوات اتصال سهلة الاستخدام للمعلومات المخفية (٢٠٠٣) [٢] . والمعلومات المخفية(Steganography) هي فن تغطية المعلومات والغرض منها هو ستر الاتصال من خلال إخفاء وجود**

**الرسالة عن فريق أو جماعة ثالثة(٢٠٠٤)[٣] . تخفى معلومات الإخفاء في وسط غطاء(Cover Media) ، وإن بعض أوساط الغطاء تكون انسب لإخفاء المعلومات من الأخرى(٢٠٠٤)[٤]. وتعد اليوم ملفات الصوت والصورة هي الأغطية الأكثر شيوعا(٢٠٠٤)[٣]. وإن واحداً من أهم المستلزمات الرئيسة لإخفاء المعلومات في الصوت أو الصورة الرقمية هو الفيض(redundant) وهو عبارة عن معلومات متكررة ويستخدم هذا الجزء من الصوت أو الصورة لإخفاء المعلومات السرية(٢٠٠٢)[٥].**

نظام الإخفاء الجيد يجب أن يحقق المتطلبات نفسها الموجودة في نظام التشفير الجيد. هذا يعني أنَ أمنية النظام يجب أن تؤسس على فرضيات إن العدو يملك معرفة كاملة بتصميم وتفاصيل إنجاز نظام الإخفاء . المعلومات المفقودة بالنسبة للعدو هي المفتاح فقط ، والمفتاح هو سلسلة قصيرة من الأرقام العشوائية قابلة للتغيير بسهولة ، وبدون المفتاح فإن العدو سوف لن يعرف إن الاتصال المخفي قد حدث(٢٠٠٤)[٦].

توجد تقنيات أساسية استخدمت في أمنية المعلومات هي: التشفير(Cryptography) ، المعلومات المخفية(Steganography) و الطريق الرئيس لحماية البيانات المنتقلة هو إخفاء الرسالة (٢٠٠١)[١].

## ١. ٢ التشفير(Cryptography) والمعلومات المخفية(Steganography)

يعد علما المعلومات المخفية(steganograpy) والتشفير(Cryptography) ذوا قرابة في أسرة حرفة التجسس (٢٠٠٢)[٧] ،الغرض من الاثنين لتوفير اتصال سري(Secret Communication) ، يخفي التشفير محتوى الرسالة السرية من المهاجم ، بينما الإخفاء يخبئ وجود الرسالة ، لذا فان وصف كسر النظام يكون مختلفاً. ففي نظام التشفير يكسر النظام عندما يستطيع المهاجم قراءة الرسالة السرية. بينما كسر نظام الإخفاء يتكون من مرحلتين (١٩٩٨)[٨] :

١ ـ على المهاجم أن يستطيع الكشف من إن الإخفاء قد استخدم.
٢ ـ أن يكون قادراً على قراءة الرسالة المخفية.

استخدمت المعلومات المخفية(Steganography) بسبب إن بعض الشركات لا تسمح بتشفير الرسائل والصور ، وبعض الحكومات المحلية لا تسمح بذلك أيضا، تعد المعلومات المخفية (Steganography) حالة صحيحة في بعض الدول التي يعاني مواطنوها ظلم أسلوب حكم السلطات فيها(١٩٩٨) [٩] .

## ١. ٣ الخلفية التاريخية للمعلومات المخفية (Historical Background for Steganography)

**الكلمة اليونانية (στεγανό-γραφ-ειν) تعني المعلومات المخفية [١٠,١١](١٩٩٩,٢٠٠٠) . أي إن(steganography) مشتقة من كلمتان يونانيتان :"steganos" تعني المغطاة و "graphica" تعني الكتابة (٢٠٠٢) [١٢]. تعد المعلومات المخفية(steganography) فن إرسال الرسائل غير المرئية أو المخفية(٢٠٠٤)[٤].**

**دوَن المؤرخ اليوناني هيرودوتس الذي يعود تاريخه إلى العصور اليونانية، في سجلاته البدايات المبكرة لليونان في المعلومات المخفية(Steganography) .وقد كان وسط الكتابة في ذلك الزمن هو النصوص. وقد ذكر إن رجلا اسمه هاربوكوس قد قتل أرنباً بريا أخفى رسالة في بطنه ثم أرسل الأرنب مع أحد الصيادين. هناك طرق أخرى لإخفاء البيانات شرحت في اليونان القديم.**

**عندما امسك الملك الطاغية داريوس بهستيوس كسجين في القرن الخامس قبل الميلاد ، عندها أرسل هستيوس رسالة إلى صهره ارسطوكوراس حيث حلق راس العبد ووشم الرسالة على فروة رأسه وعندما نمى شعر رأس العبد أرسل إلى الهدف وحلق رأسه لكشف الرسالة.**

**هناك وقائع أخرى مثل قصة ديمترويس عندما انذر سبارتا أن اكسريكس نوى غزو اليونان ، ولتجنب ذلك حفر شمع الألواح (رقعة الكتابة) وكتب رسالة اسفل الخشب وغطى الألواح بالشمع من جديد إذ إن الألواح كانت تغطى بالشمع في ذلك الزمن لكتابة الرسائل عليها. وقد بدت الألواح فارغة وغير مستعملة بحيث اجتازت تفتيش الحراس بنجاح.**

هناك طريقة أخرى تعد الأكثر شيوعا وجاذبية وشعبية لإخفاء الرسائل وهي استخدام الحبر السري(Invisible Ink) ، استخدم الرومان الكتابة بالحبر السري ما بين السطور بالاعتماد على خلاصة عصير الفاكهة ، البول والحليب. ولكسر الرسالة تعرض إلى حرارة بحيث تغمق ألوان الأحرف ومن ثمَّ سيعود ظهور النص. هناك طريقة أخرى لإعادة فك الرسالة وذلك بإضافة نسبة من الهباب أو الكربون الأسود إلى الورقة حيث سيلتصق بالكربون. وهذه الطرق تطورت بتطور علم الكيمياء.

استمرت المعلومات المخفية(Steganography) بالتطور خلال القرنين السادس عشر والسابع عشر بسبب سخط بعض الأحزاب القومية بحيث أخفى مؤلفو الكتب أسماءَهم في أعمالهم. مثال على ذلك اشتبه كثير من الأدباء في تأليف مسرحيات شكسبير على أنها نسبت إلى فرانسس باكون ، لكن ملاحظة كاتب اليزابيث اكتشف نصوصاً مخفية في تلك المسرحيات التي تحتوي اسم باكون وقد احتوت تلك الأعمال على مصادر لإخفاء النص نفسه (٢٠٠٤) [١٣,١٤] .

وعندما اكتشف التصوير الشمسي بحيث يسمح بتقليل حجم الصورة كما حدث في حرب فرنسا مع روسيا ، وعندما حوصرت مدينة باريس التقط الناس صوراً شمسيةً لرسائلهم وصغروا حجم الصور إلى

انج بنصف انج الفلم ثم ربطت حول أرجل الحمام وأرسلت محلقة خارج المدينة.وبتقدم التصوير في عمل العدسات ومعالجة الفلم اصبح بالإمكان تغيير حجم الصور إلى النقطة (dot)،وتلك النقطة تملك وضوح صفحات الكتابة المطبوعة(١٩٩٨)[١٥].

وهذه المعالجة سميت بتقنية النقطة المصغرة(Microdot) وقد طور هذه التقنية مخترع ألماني .

وبسبب صغر حجم هذه الصور المايكرويه (Microdot Photograph) فانها تسمح بانتقال نسبة كبيرة من البيانات المتضمنة صوراً ومخططاتِ رسوماتٍ(١٩٩٨)[٩]. باستخدام هذه التقنية ، الرسالة المخفية لا تلفت الأنظار نحوها لصغر حجمها وبنفس الوقت تخزن معلومات هائلة متضمنة صور ورسومات.

وفي القرن العشرين وسمت الحرب العالمية الثانية تجارب إخفاء قوية.وفي بداية الحرب كانت اغلب تقنيات الإخفاء مؤلفة من الحبر السري(Invisible Ink) بصورة تامة. التقنية البديلة لإخفاء البيانات كانت تقنية فتح الشفرات .تقنية فتح الشفرات كانت تستخدم شفرات كلمات فقد استخدم الجواسيس الألمان عملية تزييف قوائم البضائع التي تشير إلى كميات البضائع مكتوبة عليها بحيث إذا كانت القائمة تطلب ٤,٠٠٠) (pens من لندن فهذا يعني انه يوجد أربع سفن عدوة في ذلك المكان(٢٠٠٤)[١٣].

**على الرغم من أن استخدام المعلومات المخفية قد بدأ منذ قرون كثيرة ماضية، لكن حديثا هذا المجال اصبح يأخذ مساحة مهمة ومفيدة للأفراد والحكومات بسبب التكنولوجيا، فالناس ينقلون معلومات مهمة بسبب زيادة الربط الناشئ عن الحاسبات والإنترنت. إن هذا التطور اليوم يمثل العمود الفقري للمعلومات المخفية . إذن المعلومات المخفية الحديثة (Modern Steganography) هي فن إخفاء المعلومات في وثيقة أو ملف غطاء . اصبح الآن الإخفاء تام وكامل في العالم الرقمي باستخدام خوارزميات رياضية هذه الخوارزمية تخلق مفتاحاً يستخدم لاحقا لتحويل البيانات المشفرة إلى الشكل الأصلي بحيث يستطيع المستلم فهم الرسالة (٢٠٠٢)[٥].**

**تتعامل المعلومات المخفية الحديثة مع الأوساط الإلكترونية بدلا عن الأجسام الفيزيائية و النصوص . وهذا يعطينا إدراك بوجود عدد من الأسباب، وهي آلاتية (٢٠٠٤)[٤] :**

١- لان حجم المعلومات صغير بالمقارنة مع البيانات المراد الإخفاء فيها(الغطاء) تكون الأوساط الإلكترونية اسهل بكثير في المعالجة لإخفاء البيانات واستخراج الرسائل.

٢- عندما تكون البيانات إلكترونية فإن استرجاع نفسها يعالج ذاتيا وآليا، لان الحاسبات تعالج البيانات بكفاءة وتنفذ الخوارزميات الضرورية لاسترجاع الرسائل .

٣- بسبب توفر المعلومات الإلكترونية بشكل كبير وتوفر وسائط الغطاء لإخفاء المعلومات فيها.

٤- تضمن البيانات الإلكترونية على فيض غير ضروري . وفراغ بياني غير مفيد يمكن معالجته لإخفاء الرسائل.

حاولت المعلومات المخفية الحديثة(modern steganography) أن تكون قابلة للكشف فقط إذا كانت المعلومات السرية معرفة كمفتاح سري(١٩٩٩)[١٦]. وهذا يشابه مبادئ (Kerckhoff) في التشفير الذي اعتبر إن سرية أنظمة التشفير يجب عليها أن تعتمد على أداة المفتاح فقط لا غير لأنظمة التشفير ذات المفتاح السري.

لكي تبقى المعلومات المخفية (steganography ) دون كشفها ، فإن وسط الغطاء غير المحدث يجب أن يحفظ بسرية ، لأنه إذا كشف أو عرض فإن المقارنة بين الغطاء ووسط الإخفاء ( steganography medium) يؤدي حالا إلى إفشاء التغييرات(٢٠٠٣)[٢].

كثير من المعلومات المخفية الحديثة(modern steganography) تركز على الصور والإشارات الصوتية (٢٠٠٤)[٤] ، وتعد ملفات الصوت والصورة الأوساط الحاملة الأسهل والأكثر شيوعا في الإنترنت بسبب إن ملفات الأغطية موجودة بشكل عادي ويمكن أن تخلق بسهولة كذلك فإن برمجيات الإخفاء سهلة الوصول عند استخدام الإنترنت(٢٠٠٤)[٦].

## ١. ٤ الإخفاء بالصورة(Image Steganography)

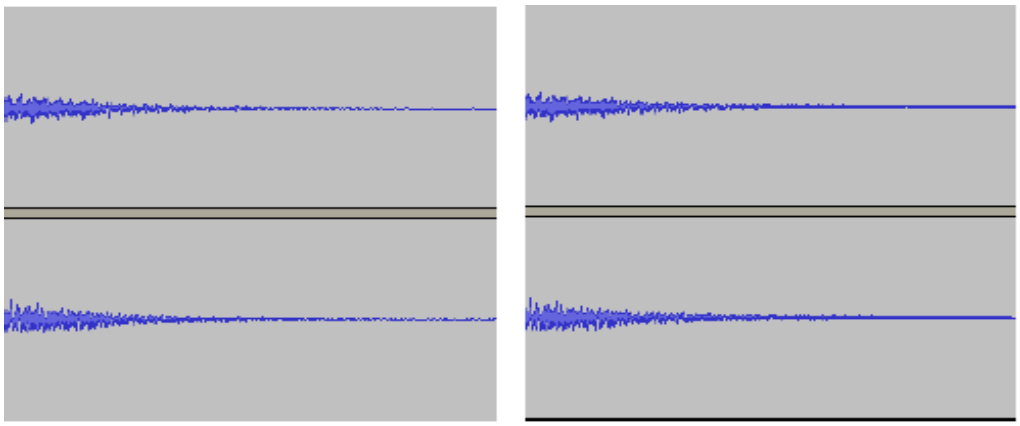
**إن الإخفاء باستخدام الصورة قد حصل على شعبية اكبر في السنين الأخيرة من أنواع الإخفاء الأخرى، بسبب غمر الصور الإلكترونية بمجيء الكاميرات الرقمية وسرعة توزيع الإنترنت للصور. اغلب أنواع المعلومات تحتوي بعض أنواع الضوضاء ، وهذه الضوضاء يمكن أن توصف كتشويه غير مرغوب فيه للمعلومات ترد خلال الإشارة.**

وبصورة عامة فإن الضوضاء تشير إلى نقص يلازم عملية تحويل صورة تناظرية إلى صورة رقمية، على سبيل التمثيل قيم لوحة الألوان(Palette) للصورة الرقمية سوف لن تكون بالضبط الألوان نفسها في الصورة الحقيقية، كذلك توزيع هذه الألوان سوف لن يكون مكتملا

**(٢٠٠٤)[٤].**
**إن القياس اللحظي للفوتونات يتم باستخدام الكاميرا الرقمية للحصول على العشوائية الملازمة لها. وهذا يقود إلى مجموعة مساحات غير مكتملة وهذه المساحات تعدل لتصبح صورة رقمية(٢٠٠٢)[١٧].**

## ١. ٥ الإخفاء بالصوت(Audio Steganography)

**إن إخفاء الرسائل باستخدام الصوت الحاوي على "الضوضاء" ( والترددات التي لا يستطيع الإنسان سماعها ) هي مساحة أخرى لإخفاء المعلومات وتعتمد على استخدام المصدر الموجود كفراغ لإخفاء المعلومات. قد يعاني الإخفاء باستخدام الصوت مشاكل ، لان الموسيقيين ومهندسي الصوت سخّروا ليكونوا قادرين على كشف "أنين درجة الصوت العالي" المرافق لمعلومات الترددات العالية جدا المشفرة في الرسائل. وهذا يؤدي إلى خزن المعلومات بالترددات غير المسموعة(Non-Audible Frequency) أو تشويه الإشارة المسموعة لتضمنها على ضوضاء إضافية.**
**في الشكل (١.١) عينة قصيرة ، ناتجة من إخفاء ملف صوت بحجم(١٣ k) بآخر ذي حجم (١٦٨ k) بهيئة(wav) باستخدام المعلومات المخفية (steganography) (٢٠٠٤) [١٨]. صوت الملف المخفي سيصدر رنيناً بصورة مشوشة ، مثل الراديو الذي يشتغل بصورة غير جيدة(ملف الصوت الأصلي يكون صافياً بشكل تام). يكون تمثيل الموجه ولاسيما نهاية الموجة صامتاً(silence) ورغم إن كلا الصورتين متشابهتان إلا أننا لو تفحصنا تمثيل الإخفاء لوجدنا ضوضاء إضافية(وهذه تعمل خطأ إضافياً في نهاية الإشارة الواقعة في جهة اليمين أكثف من الإشارة في جهة اليسار).**



Clean .wav file (cover object)  stego . Wav file

شكل رقم ١.١١ يبين ملف صوت خالي من الرسالة وملف

بينما الإشارة الأصلية تبقى قابلة التمييز في الجسم المخفي(stego –object) فالتغييرات قابلة للكشف من المصغي. بينما يقع خلال مدى نوع الضوضاء المسموع في محطات الراديو أو خلال التداخل ، إن ورود مثل هذه الضوضاء بشكل غير متوقع في السياق مُمَكِن لأنْ تثار الشكوك عن ملف الصوت نفسه (٢٠٠٤)[٤].

## ١. ٦ تطبيقات المعلومات المخفية(Steganography Applications)

تزود المعلومات المخفية(steganography) فائدة كبيرة ، وتجاريا تعطي وظائف مهمة في العالم الرقمي ، لا سيما العلامة المائية الرقمية(Digital Watermarking) . حيث يستطيع الكاتب أن يخفي رسالة في ملف بحيث يؤكد ملكية حقوق النسخ. مثلا الفنان ، يستطيع أن يرسل عملاً فنياً أصلياً على موقع الإنترنت . فإذا قام شخص ما "بسرقة" الملف وتبنى العمل على أساس انه يمتلكه ، فإن الفنان يستطيع أن يثبت ملكيته وذلك لأنه يستطيع استرداد العلامة المائية(Watermarking) (٢٠٠٤,٢٠٠١,٢٠٠٣) [٣,١٩,٢٠].

يمتلك الإخفاء عدداً من التطبيقات الشريرة ،اغلب سجلات الإخفاء الشهيرة لها نشاطات غير قانونية ، مثل عمليات النصب المصرفي ، والاتصال بين مجموعة أعضاء مجرمين أو منظمات إرهابية (٢٠٠٤,٢٠٠٣) [٢١] [٣] . بحيث إن التقدم في تحليل الإخفاء(steganalysis) قد تطور بسبب تنامي استخدام المعلومات المخفية(steganography) (٢٠٠٤)[٦].

## ١. ٧ الأدبيات السابقة

اقترح (A.Tumas) (١٩٩٦) [٢٢] خوارزمية لإخفاء ثنائية مختارة من صورة رقمية . الفكرة الأساسية هي استخدام التبديل العشوائي(pseudorandom permutation) لثنائية الغطاء .

قدم (D.paul and S.Michael) (١٩٩٦) [٢٣] طرق إخفاء لحشر المعلومات السرية في ملف الصورة . هذه الطريقة استخدمت تقنيات ضغط الصورة الجزئية في إنتاج ملفات صورة الإخفاء ، تسمح الطريقة للمستخدم أن يخصص مفتاحاً مرئياً عندما يخفي المعلومات السرية . المفتاح المرئي يجب أن يستخدم لاحقا عند استرجاع البيانات المخفية .

عرّف (S.Joshua and C.Barrett) (١٩٩٦) [٢٤] بعض طرق إخفاء-بيانات الطيف المنتشر(Spread Spectrum) . استخدمت هذه التقنيات بيانات الرسالة لتضمين الإشارة الحاملة ، والتي ستركب لاحقا مع صورة الغطاء في جزء المقاطع غير المتداخلة . تستخرج الرسالة خلال علاقة التقاطع بين صورة الإخفاء والإشارة الحاملة المعاد توليدها ، بعد التنفيذ صورة الغطاء تصبح غير ضرورية ، بعدها تنجز عملية التعتيب(Threshold operation) على علاقة التقاطع الناتجة لتحدد القيمة الثنائية لثنائيات بيانات الإخفاء .

قدّم (W.Andreas and W. Gritta) (١٩٩٨) [٢٥] نظام الإخفاء الذي يخفي الرسالة السرية في نظام الفيديو . يحول مسار الإشارة بتحويلات الجيب تمام المتقطع (DCT). تكون النتيجة تحويلاً تقنياً لخوارزمية إخفاء والتي تؤسَس أمنيّتها بالاعتماد على مبدأ اللاحتمية خلال مسار الإشارة .

أقترح(A.Ross at.el) (١٩٩٨) [٢٦] نظام إخفاء ملف . صممت ميكانيكية الخزن هذه لتعطي المستخدم مستوى عالٍ من الحماية لكي لا تؤدي إلى كشف محتويات الملف . وهذه سوف تحرر الملف لأي مستخدم الذي يعرف اسمه وكلمة السر ، لكن المهاجم الذي لا يملك هذه المعلومات ولا يستطيع تخمينها ، لا يستطيع الحصول على أي معلومة فيما إذا قدم له الملف .

استخدم (G.Daniel and B.Walter)(١٩٩٨) [٢٧] طريقة سميت (patcwork) ، وهي طريقة إحصائية . تخفي في الصورة المضيفة بصورة غير مدركة حسيا صورة إحصائية معينة تمتلك توزيع كاوس .

قدّم (L.Avedissian) (٢٠٠٠)[٢٨] ، طريقة إخفاء صورة صغيرة ذات تدرج رمادي داخل صورة أكبر ذات تدرج رمادي أيضا أو صورة ملونة ، تتضمن هذه الطريقة استبدال بعض ثمانيات الصورة

الأصلية بثمانيات جديدة من الصورة المراد إخفاؤها ، وهي مؤلفة من ست مراحل : مرحلة اختبار التغييرات ، مرحلة التحويل ، مرحلة البحث الأمثل ، مرحلة التعويض ، مرحلة إخفاء المواقع ومرحلة إخفاء المفتاح .

قدّم (S.B.Abdulah) (٢٠٠١)[٢٩] طريقة لإخفاء نصوص عربية بنوعين من الأغطية : الغطاء الأول هو نص عربي آخر ، وحيث إن الإخفاء يعتمد على الخصائص الطبيعية للنص العربي . الغطاء الثاني هو صورة ، وقد استخدمت العملية ثلاثة طرق : الإخفاء بوحدة قياس ٢ من قطعة الثنائيات الأقل أهمية ، الإخفاء بوحدة قياس ٢ باستخدام التشفير والإخفاء في قناة من العينات .

قدّم [A. M. Jafar] (٢٠٠٢)[٣٠] طريقة لإخفاء صورة داخل صورة ، وهذه الطريقة تتضمن تقنيات تحويل المويجة .

أنجزت (H.Al Kafaji) (٢٠٠٣)[٦٧] طريقة لإخفاء صورة بمستويات لونية مختلف ( صورة طبيعية ، ملونة ٢٥٦ ،رمادية ) داخل صورة أخرى بالحجم نفسه باستخدام خمسة طرق مختلفة : طريقة (Image Downgrading) ، حشر الثنائيات الأقل أهمية ، ميكانيكية التعديل ، الطريقة الهجينة وطريقة القطع المتشابهة .

أنجزت (Najla'a A.M.Al-Mayahee) (٢٠٠٥)[٣١] طريقة لإخفاء صورة ملونة صغيرة داخل صورة ملونة أكبر باستخدام طريقة القطاعات المتشابهة ، وقد تضمنت هذه الطريقة استخدام تقنية(DCT) لزيادة الحصانة ضد التغييرات التي تجرى على الصورة الغطاء .

## ١. ٨ الهدف من البحث :-

يهدف البحث إلى تصميم منظومة برمجية لإخفاء ملف صوتي داخل صورة ملونة صغيرة نسبيا إلى حجم ملف الصوت . دون إحداث تشويه ظاهر على الغطاء لتجنب إحداث شكوك لدى المهاجم . يتضمن النظام المقترح عمليات تحويل وضغط لملف الصوت قبل عملية الإخفاء وقد استخدمت تحويلات المويجة المتقطعة (DWT) وتشفير طول السلسلة (RLE) .

## ١. ٩ الهيكل العام للبحث:-

**الفصل الأول :-** يتضمن مقدمة عن أمنية المعلومات واستخدام تقنيات المعلومات المخفية

لتحقيق هذه الأمنية ، كذلك مميزات المعلومات المخفية ومساوئ التشفير
، وتضمنه نظرة تاريخية عن المعلومات المخفية والطرق القديمة المستخدمة في الإخفاء وفرقها عن الإخفاء الحديث ، كذلك مقارنة بين
الإخفاء والعلامة المائية وأخيرا تطبيقات المعلومات المخفية .

**الفصل الثاني :-** تضمن الخلفية النظرية للمعلومات المخفية ، كذلك متطلبات ، أنواع
وتقنيات المعلومات المخفية كذلك تقنيات التحويل والضغط : تحويل
المويجة المتقطع (DWT) وتشفير طول السلسلة (RLE) وتقنية كذلك الخلفية النظرية لاستخدام مقاييس الدقة أو النوعية .

**الفصل الثالث :-** يتضمن نظام المعلومات المخفية المقترح المكون من جزئيه جزء الإخفاء
وجزء الاسترجاع .

**الفصل الرابع :-** يتعامل مع نتائج النظام المقترح .
**الفصل الخامس:-** يتضمن الاستنتاجات وبعض التوصيات والأعمال المستقبلية .

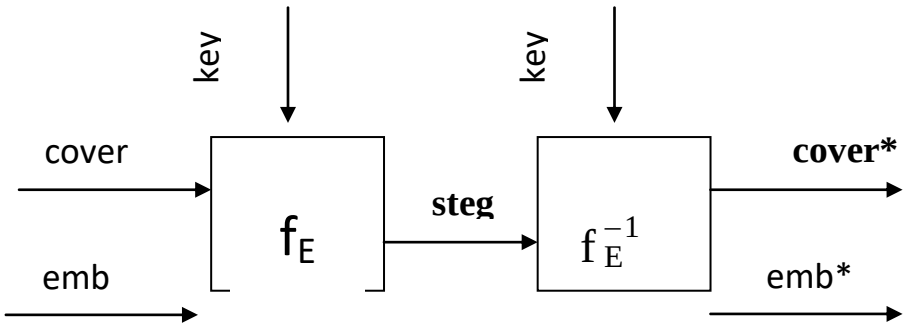
## ٢. ١ المقدمة

تعد المعلومات المخفية(Steganography) فن إخفاء المعلومات بطرق تمنع الكشف عن الرسائل المخفية(٢٠٠١)[٣٢] وهي تتضمن أنظمة واسعة من طرق الاتصال السري بحيث تخفي وجود الرسالة بشكل فعلي(٢٠٠٢)[٧]
تمتلك المعلومات المخفية مكانة أمنية وهي لا تعني استبدال التشفير(Cryptography) بل إلحاقه بها . وهي تقلل فرص كشف الرسالة السرية .

**وإذا كانت الرسالة مشفرة فإنها تزودنا بمستوى آخر من الحماية(٢٠٠٣)[٣٣] . لذلك فإن بعض طرق المعلومات المخفية تجمع بين التشفير التقليدي والمعلومات المخفية ، بحيث يشفر المرسل الرسالة السرية في كل عملية اتصال ، وذلك لجعلها اكثر صعوبة للمهاجم الذي ينوي كشف النص المشفر المخفي في الغطاء . وكنتيجة طبيعية فإن أنظمة المعلومات المخفية القوية لا تحتاج إلى مرحلة تشفير سابق(٢٠٠٠)[٢٨].**

## ٢. ٢ النموذج الأساسي لنظام المعلومات المخفية

يعرف الشكل(٢.١) نموذج المعلومات المخفية الذي يعتمد على نتائج مناقشات تمت في جامعة كامبرج(١٩٩٦) [٣٤] . يسمى هذا النموذج بنموذج المعلومات المخفية (١٩٩٧) [٣٦,٣٥].




الشكل(٢.١) يبين نموذج المعلومات المخفية النموذجي

حيث ان :

$f_E$ : **دالة المعلومات المخفية " الإخفاء" .**

$f_E^{-1}$ **: دالة المعلومات المخفية "الاستخراج".**

cover : بيانات الغطاء التي يراد إخفاء المعلومات فيها.

emb : الرسالة المراد إخفاؤها .

key : المفتاح المستخدم .

stego : بيانات الغطاء مع الرسالة المخفية .

## ٢. ٣ متطلبات نظام المعلومات المخفية

**توجد مجموعة من الصفات أو المتطلبات التي يجب توافرها في أي نظام معلومات مخفية هي (١٩٩٨,٢٠٠٠)[٣٨,٣٧] :**

### ١. التحصين (Robustness):

تشير القوة أو التحصين إلى قدرة المعلومات المخفية على البقاء سليمة(١٩٩٩)[٣٢]

عند إجراء تعديلات على بيانات الغطاء وعدم التأثر أو التشويه بعد التمييز . على سبيل التمثيل ، المرشحات الخطية و اللاخطية(Linear and Nonlinear Filter) (مثل مرشحات الحدة والوسيط) ، الضغط الحاوي على فقدان للبيانات (Lossy Compression) ، التقييس(Scaling) ، التدوير (Rotation) ،إضافة الضوضاء(Noise Adding) وتكميم اللون(Color Quantization) وغيرها(١٩٩٨)[٣٨] .

### ٢. عدم القدرة على الاكتشاف(Undetectablity) :

تمثل هذه الخاصية المطلب المثالي لأي نظام اتصال أمين . حيث إن المعلومات المخفية لا يمكن اكتشافها إذا كانت تشكل مع معلومات الغطاء نموذجا متماسكا(متلائما) . على سبيل التمثيل ، إذا استعملت مكونات الضوضاء للصورة الرقمية لاخفاء المعلومات المهمة فإن هذا لا يؤدي إلى تغيير كبير ومهم في الخصائص الإحصائية للصورة لذا فإن مفهوم عدم القدرة على القدرة على الاكتشاف(Undetectability) يرتبط مع النموذج الإحصائي لمصدر الصورة . فإذا كان للمهاجم معرفة تفصيلية بمصدر الصورة فإنه سوف يكتشف وجود رسالة مخفية فيها . ولكن قدرة اكتشاف وجود الرسالة لا يعني إمكانية قراءة الرسالة(١٩٩٨)[٣٨].

عدم القدرة على الاكتشاف تتأثر بصورة مباشرة بحجم الرسالة السرية وهيأة محتوى بيانات الغطاء(٢٠٠١)[٢٩] .

## ٣. عدم الرؤيا (Invisibility)

**يعتمد هذا المفهوم على خصائص نظام الرؤيا أو السمع البشري(Human Visual or Audio system) . تكون المعلومات غير محسوسة(مدركة) إذا كان معدل الأشخاص (Human Subject Average) غير قادر على التمييز بين الأوساط الحاملة الأصلية التي تحتوي على معلومات مخفية . الطريقة الشائعة هي ما تعرف بـ (Blind Test) التي تستعمل في(Psycho-Visual Experiment) وتعتمد على التمثيل العشوائي لعدد كبير من الصور الحاملة لمعلومات مخفية وأخرى لا تحتوي على معلومات مخفية . وكانت نسبة النجاح قريبة من ٥٠٪ ، أثبتت إن هؤلاء الأشخاص غير قادرين على التمييز بين الصور الأصلية والحاوية على معلومات مخفية (١٩٩٨)[٣٨] .**

### ٤. السرية(Security)

إن خوارزمية المعلومات المخفية تكون أمينة إذا كانت المعلومات المخفية غير قابلة للإزالة (الحذف) بعد اكتشافها من المهاجم اعتمادا على المعرفة الكاملة بخوارزمية المعلومات المخفية والمفتاح السري(١٩٩٨)[٣٨] .

### ٥. السعة(Capacity)

تتنافس المتطلبات المذكورة آنفا بالتبادل ولكنها لا تستطيع الوصول إلى الحالة الأمثل بالوقت نفسه . فلإخفاء رسالة كبيرة داخل أي غطاء فإننا لا نشترط الحصانة الكبيرة وعدم الاكتشاف المطلق . أي إن الاتفاق المعقول هو بحسب الحاجة أو الضرورة فالحاجة إلى التحصين تعني إن الرسالة يجب أن تكون صغيرة حتى لا تؤدي إلى تشوه وسط الغطاء(١٩٩٨)[٣٨] .تشير فكرة السعة في إخفاء البيانات إلى الرقم الكلي للثنائيات المخفية وتسترجع بنجاح بواسطة نظام الإخفاء (١٩٩٩)[٣٩] .

## ٢. ٤ أنواع المعلومات المخفية(Steganography types)

تقسم المعلومات المخفية إلى ثلاثة أنواع . وقد وصفت هذه الأنواع كالآتي :

## ٢. ٤. ١ المعلومات المخفية الصرفة(Pure Steganography) :

يدعى نظام المعلومات المخفية الذي لا يحتاج إلى تغيير مسبق ببعض المعلومات السرية (مثل معلومات الإخفاء) بالمعلومات المخفية الصرفة . وبشكل أساسي يمكن أن توصف عملية المعلومات المخفية تفصيليا C CxM: E حيث إن C هي مجموعة الأغطية الممكنة ، و M هو مجموعة الرسائل الممكنة . عملية الاستخراج مؤلفة من M C:D ، استخراج الرسالة السرية خارج الغطاء . وبشكل أوضح ، من الضروري أن يكون |M|=<|C| بحيث إن كلا المرسل والمستلم يجب أن يمتلكا وصولاً إلى الإخفاء وخوارزمية الاسترجاع ، لكن يجب أن تكون الخوارزمية غير معلنة (٢٠٠٠)[٤٠] .

## ٢. ٤. ٢ المعلومات المخفية ذات المفتاح السري (Secret Key Seganography):

يكون نظام المعلومات المخفية ذات المفتاح السري مماثلاً للتشفير. يختار المرسل الغطاء C ، ويخفي الرسالة السرية بالغطاء C ، باستخدام المفتاح السري K . إذا استخدم المفتاح في عملية الإخفاء فيجب أن يكون معرّفاً للمستلم ، بحيث يستطيع قلب العملية واستخراج الرسالة المخفية . ان الغطاء C ووسط الإخفاء(stego _object) يجب أن يكونا متشابهين حسيا . يمكن أن توصف عملية المعلومات المخفية تفصيليا C CxMxK: $E_k$ وعملية الاستخراج M CxK: $D_k$ . حيث إن K هي مجموعة المفاتيح السرية الممكنة(١٩٩٦)[٤١] .

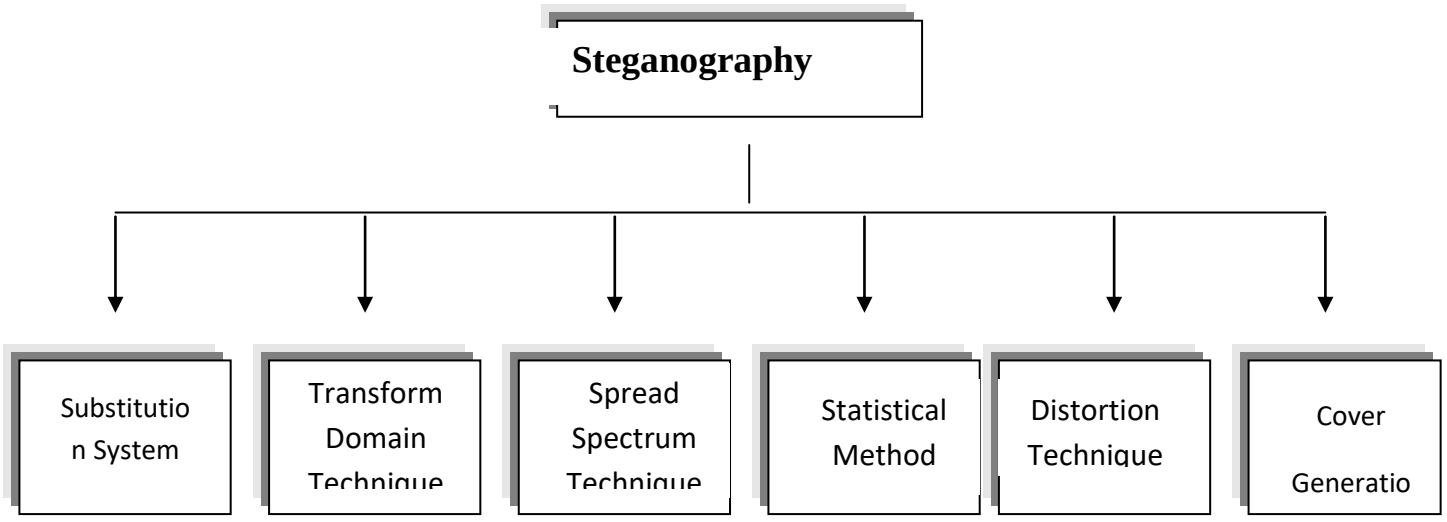
## ٢. ٤. ٣ المعلومات المخفية ذات المفتاح المعلن (Public Key Steganography) :

يتضمن هذا النظام مفتاحين الأول سري(Secret) والآخر(Public) وهو مشابه لنظام التشفير ذي المفتاح المعلن (Public Key Cryptography) . يستعمل المفتاح المعلن في عملية المعلومات المخفية ويخزن في قاعدة بيانات معلنة على حين يستعمل المفتاح السري في عملية استرجاع الرسالة السرية .

تعدُ طريقة استعمال نظام التشفير ذي المفتاح المعلن إحدى طرائق بناء نظام المعلومات المخفية ذات المفتاح المعلن ، إذ يستعمل نظام المعلومات المخفية ذي المفتاح المعلن الدالة D لاسترجاع الرسالة السرية التي تكون عبارة عن عناصر عشوائية M وهذا ما يعرف بالعشوائية الطبيعية(Natural Randomness) للغطاء . لبناء نظام معلومات مخفية أمين يخفى النص المشفر بدلا من النص(الرسالة) الواضح (٢٠٠٠)[٤٠] .

## ٢. ٥ تقنيات المعلومات المخفية(Steganography Techniques)

يمكن أن تصنف تقنيات المعلومات المخفية إلى ست مجاميع كما مبين في الشكل (٢.٢) (٢٠٠٠)[٤٠].



الشكل (٢.٢) يبين تصنيف تقنيات الإخفاء

١- **النظام الإبدالي(substitution system):** تعوَض أجزاء الفيض الموجودة في الغطاء بالرسالة السرية .
٢- **تقنيات مجال التحويل(Transform Domain Techniques):** تخفى المعلومات السرية في فضاء تحويل الإشارة (مثل مجال التردد) .
٣- **تقنيات الطيف المنتشر (spread spectrum Techniques):** هذه التقنيات تبنت أفكار اتصال الطيف المنتشر .
٤- **تقنيات التشويه(Distortion Techniques):** تخزن المعلومات بمناطق تشوه الإشارة وتقيس الزيغ أو الانحراف (deviation) من الغطاء الأصلي في مرحلة الاسترجاع .
٥- **الطرق الإحصائية(statistical Methods):** وهي تشفر المعلومات بتغيير الخصائص الإحصائية للغطاء وتستخدم اختبارات افتراضية في عملية الاسترجاع .
٦- **طرق توليد الغطاء(Cover Generation Methods):** وهي تشفر المعلومات بالطريقة التي تجعل الغطاء يخلق للاتصال السري (٢٠٠٠)[٢٨] .

## ٢. ٥. ١ الأنظمة الإبدالية (Substitution Systems)

أنظمة الإبدال الأولية تحاول أن تشفر المعلومات السرية بإبدال الأجزاء غير المهمة من الغطاء بثنائيات الرسالة السرية . يستطيع المستلم أن يستخرج المعلومات إذا كانت لديه معرفة بالمواقع التي اختفت فيها المعلومات السرية . وبسبب أن هناك تحويرات بسيطة قد عملت في عملية الإخفاء ، فإن المستلم سيفترض إن المهاجم سوف لن يلاحظ ذلك . وهذه الأنظمة مؤلفة من عدة تقنيات وهي كآلاتي .

### أ- إبدال الثنائيات الأقل أهمية ((Least Significant Bits Substitution (LSB)

تعتمد عملية الإخفاء على اختيار مجموعة جزئية $\{j_1 \ldots j_{l(m)}\}$ من عناصر الغطاء وإنجاز عملية الإبدال $m_i$ $C_{ji}$ عليها ، من خلال استبدال البت الأقل أهمية لـ $C_{ji}$ بواسطة $m_i$ (والذي يمثل مفردات الرسالة ويمكن أن تكون ٠ أو ١ ) . عند الاسترجاع تستخرج عناصر البتات الأقل أهمية من الغطاء لاعادة إنشاء الرسالة السرية . لكي نكون قادرين على فك الرسالة السرية ، فالمستلم يجب أن يكون قادر على الوصول إلى سلسلة العناصر الدالة المستخدمة في عملية الإخفاء . إن المرسل يستخدم جميع عناصر الغطاء لنقل المعلومات بدءا من أول عنصر . وبسبب إن الرسالة السرية تمتلك ثنائيات أقل بصورة عادية من طول عناصر الغطاء ((L ( c) ، فإن عملية الإخفاء ستنتهي قبل انتهاء الغطاء ، على أية حال ،

المرسل يستطيع أن يترك جميع العناصر التي لم تغير . وهذا يمكن أن يقود إلى مشكلة أمنية حقيقية ; فالجزء الأول من الغطاء سيمتلك خصائص إحصائية مختلفة اكثر من الجزء الثاني ، الذي لا توجد فيه تغييرات(٢٠٠١)[٢٩] .

## ب- التباديل شبه العشوائية (Psedorandam Permutation)

إذا كانت جميع ثنائيات الغطاء يمكن الوصول أليها في عملية الإخفاء ، فيسمى الغطاء بغطاء الوصول العشوائي ، وثنائيات الرسالة السرية يمكن أن توزع بصورة عشوائية على كل الغطاء . إن هذه التقنية تزيد من التعقيد بالنسبة للمهاجم ، بسبب ان ثنائيات الرسالة اللاحقة لا تحقق الإخفاء بنفس الترتيب .

عملية الإخفاء تبدأ بخلق مولد رقم عشوائي ابتدائي ، وسلسلة العناصر($j_{l(m)}$,... $j_1$) تشير وتخزن kth من ثنائيات الرسالة في العنصر بالفهرس $j_k$ .من الملاحظ إن الفهرس يمكن أن يظهر أكثر من مرة في السلسلة ، بحيث إن التعارض سيرد . وإذا كانت الرسالة قصيرة بالمقارنة مع عناصر الغطاء ، فإن احتمالية التعارض يمكن إهمالها ، والثنائيات المتعارضة يمكن أن يعاد إنشائها باستخدام شفرة تصحيح الخطأ (٢٠٠٠,٢٠٠١)[٢٨,٢٩] .

## ج- قنوات الغطاء وتشويه الصور(Image downgrading and Cover Channels)

وهي حالة خاصة من الأنظمة ألابدالية ، تستعمل لاخفاء صورة داخل صورة أخرى وبالحجم نفسه ، حيث تستعمل الثنائيات الأربع الأقل أهمية من صورة الغطاء ( رمادية التدرج أو الملونة ) بالثنائيات الأربع الأكثر أهمية من الصورة السرية . ولاسترجاع الصورة السرية ، تستخلص الثنائيات الأقل أهمية من الصورة الحاملة للصورة السرية (stego-Image) . في الكثير من الحالات ، نجد أن إرسال أربع ثنائيات فقط من الصورة السرية كافية تقريبا .
في هذه الطريقة يكون تشوه الغطاء كبيراً بالرغم من انه نظريا غير ملحوظ ولكنه في التطبيق العملي يكون غير ذلك(٢٠٠٠,٢٠٠٣)[٤٠,٦٧] .

## د- مناطق الغطاء وثنائيات التطابق(Cover Regions and Parity Bits)

يمكن أن نعرف أي مجموعة جزئية غير فارغة {$c_1$...$c_{l(c)}$} بمنطقة الغطاء(Cover Region) . يقسم الغطاء على عدة مناطق مختلفة ثم تخفى ثنائية واحدة من المعلومات السرية في كل منطقة بدلاً من كل عنصر ، إذ تستعمل ثنائية التطابق(Parity Bit) من كل منطقة في عملية الإخفاء . يمكن حساب ثنائية التطابق كما يأتي :

$$b(I) = \sum_{j \in I}(I) = LSB(Cj) \bmod 2 \qquad \ldots\ldots (1\text{-}6)$$

في عملية الإخفاء تُختار مناطق الغطاء $I_i$ بحيث تكون (١<=I<=I(m)) ويمثل I(m) طول الثنائيات المراد إخفاؤها ، حيث تخفى الثنائية السرية $m_i$ في ثنائية المطابقة $b(I_i)$ فإذا كانت الأخيرة لا تتطابق مع

الثنائية السرية تستبدل بالـ $m_i$ أما في عملية الاسترجاع فتستخلص ثنائيات التطابق لكل منطقة مختارة لإعادة تكوين الرسالة .

ويمكن أيضا استعمال طريقة شبه عشوائية في اختيار مناطق الغطاء وبالاعتماد على مفتاح سري (٢٠٠٣)[٦٧] .

## هـ- الصور المعتمدة على لوحة الألوان(Palette-Based Images)

توجد طريقتان لإخفاء المعلومات في قاعدة لوحة ألوان الصورة ، أما في لوحة الألوان أو بيانات الصورة التي يمكن التلاعب بها .الثنائيات الدنيا التي لها معنى LSB لمتجهات الألوان يمكن أن تستخدم لتحويل المعلومات ، مثل طرق الإبدال التي قدمت سابقا .

وحيث إن لوحة الألوان لا تحتاج أن تفرز ، المعلومات يمكن أن تخفى بطريقة تجعل الألوان تخزن في لوحة الألوان . يوجد !N من الطرق المختلفة لترتيب لوحة الألوان لـ N من الألوان . وتوجد سعة كافية لإخفاء رسالة صغيرة . ومع ذلك فإن كل الطرق التي تستخدم ترتيب لوحة الألوان لخزن المعلومات تعد غير حصينة(robust) أو قوية ، السبب يعود إلى إن المهاجم يستطيع ببساطة أن يفرز المداخل بطرق مختلفة ويحطم الرسالة السرية(٢٠٠٥)[٣١].

## و- التكمية والإهتياج (Quantization and Dithering)

تستعمل عمليات التكمية والاهتياج لاخفاء المعلومات السرية في الصور الرقمية . تعمل بعض أنظمة الإخفاء على الصور المكماة(Quantized Image) ، حيث يُحسب الفرق $e_i$ بين العناصر المتجاورة $x_i$ و $x_{i+1}$ ثم يدخل إلى المكمم Q (Quantizer) لينتج تقريبات متقطعة $\Delta i$ لإشارة الفرق (Deference Signal) ، $x_i-x_{i-1}$ .

لغرض الإخفاء ، يستعمل خطأ التكمية(Quantization Error) في مقطع الترميز التنبؤي PCS (Predictive Coding Scheme) ولا سيما عند تعديل إشارة الفرق $\Delta i$ لإرسال معلومات إضافية ، حيث يتكون مفتاح الإخفاء(stego-key) من جدول يسند ثنائية خاصة لكل قيمة ممكنة $\Delta i$ .

لاجل إخفاء ثنائية الرسالة i-th في إشارة الغطاء ، تُحسب إشارة الفرق المكممة $\Delta i$ فإذا كانت لا تتطابق (تبعا الى الجدول السري) مع الثنائية السرية المراد إخفاؤها ، حيث يبدل $\Delta i$ بأقرب $\Delta i$ ، تكون الثنائية المرافقة له مساوية إلى ثنائية الرسالة السرية والقيم الناتجة $\Delta i$ تدخل إلى (Entropy Coder) . على الجانب الآخر فإن المستلم يستطيع استرجاع الرسالة عن طريق حساب إشارة الفرق $\Delta i$ ومفتاح الإخفاء(Stego-Key) (٢٠٠٣)[٦٧] .

## ز- إخفاء المعلومات في الصور الثنائية (Information Hiding in Binary Image)

تحتوي الصور الثنائية(Binary Image) على تكرارات من العناصر البيضاء والسوداء . وعلى الرغم من إمكانية تطبيق عملية الإبدال البسيطة عليها إلا إنها تتأثر بصورة كبيرة بأخطاء الإرسال لذلك تكون غير حصينة .

تقسم الصور الثنائية إلى قطاعات(Blocks) مستطيلة $B_{ij}$ لتكن $P_0(B_i)$ هي النسبة المئوية للعناصر السوداء في قطاع الصورة $B_{ij}$ و$P_1(B_i)$ هي النسبة المئوية للعناصر البيضاء. بصورة عامة يتم إخفاء ١ في قطاع واحد إذا كانت($P_1(B_i)>0.50$ ) و٠ إذا كانت($P_0(B_i)>0.50$ ) . تتغير ألوان بعض العناصر للحصول على العلاقة المطلوبة تنجز تغيرات على العناصر التي لجيرانها لون معاكس(مغاير) . في الصور الثنائية ذات التباين الحاد تنجز التغيرات على حدود العناصر البيضاء والسوداء لكي تكون غير محسوسة (٢٠٠٣)[٦٧] .

## ح- الفضاء غير المستعمل أو الاحتياطي في أنظمة الحاسبات (Unused or Reserved Space in Computer System)

يمكن الإفادة من المساحات غير المستعملة أو الاحتياطية لإخفاء المعلومات من دون أن يسبب تشويه في الوسط الحامل(الغطاء) . فعلى سبيل التمثيل ، طريقة خزن الملفات في نظام التشغيل تكون في المساحات غير المستعملة ليمثل عنوان الملف .

هناك طريقة أخرى لإخفاء المعلومات في نظام الملف(File System) هو خلق أجزاء مخفية ، حيث تكون غير مرئية إذا كان النظام يعمل بصورة طبيعية (٢٠٠٣)[٦٧].

## ٢. ٥. ٢ تقنيات مجال التحويل(Transform Domain Techniques)

توجد مجموعة من الطرق التي تعتمد في عملية الإخفاء على مجال التحويل (Transform Domain) حيث تُخفى الرسالة في منطقة مهمة من صورة الغطاء . مما يجعلها اكثر قوة ضد الهجوم(Attacks) مثل الضغط(Compression) وبعض معالجات الصور نسبة الى طرائق(LSB) .

على أية حال فهي اكثر مقاومة لأنواع مختلفة من معالجات الإشارة زيادة على أن نظام الرؤيا البشري(HVS) لا يمكنه الشعور بوجودها . توجد مجموعة من طرائق التحويل المختلفة منها تحويل جيب التمام المتقطع(DCT) والتحويل الموجي(WT) ولكن يجب أن تكون هناك موازنة بين كمية المعلومات المضافة إلى الصورة (المعلومات المخفية) والتحصين الذي يتم الحصول عليه ، كما إن بعض طرائق مجال التحويل لا تعتمد على هيأة الصورة(Image Format) (٢٠٠٣)[٦٧].

## ٢. ٥. ٣ الطيف المنتشر وإخفاء المعلومات (Spread Spectrum and Information Hiding

طورت تكنولوجيا الطيف المنتشرSS (Space Spectrum) منذ عام ١٩٥٠ كمحاولة

لتوفير وسائل الاتصالات باحتمالية واطئة للجزء المحصور وغير المضغوط . يمكن تعريف تقنيات الطيف المنتشر بأنها وسائل إرسال بحيث تكون الإشارة محصورة بمدى يتجاوز الحد الأدنى الضروري(المقبول) لإرسال المعلومات ، انتشار الحزمة يتم الحصول عليه بوسائل الشفرة التي تكون مستقلة عن البيانات ، ويتزامن مع الشفرة في الاستلام التي استعملت من اجل تجميع سلسلة البيانات المسترجعة . على الرغم من ان طاقة الإشارة المرسلة تكون كبيرة فإن نسبة الإشارة إلى الضوضاء SNR (The Signal to-Noise ratio) في كل مدى ترددي تكون صغيرة . حتى في حالة حذف أجزاء من الإشارة في بعض المجالات(النطاقات) الترددية . فإن المعلومات الموجودة في النطاقات الأخرى تكون كافية لاسترجاع الإشارة ، وهذا مشابه لنظام الإخفاء الذي يحاول نشر الرسالة السرية على كل الغطاء لتبدو غير محسوسة ، وبما إن نشر ( توزيع) الإشارات يكاد يكون صعب الحذف(الإزالة) فإن عملية الإخفاء التي تعتمد على (SS) تعطي مستوى عالياً من التحصين .

يوجد نوعان مختلفان من الـ SS يستعملان في إخفاء المعلومات : السلسلة المباشرة

(Direct Sequence) والوثب الترددي(Frequency-hopping) . في السلسلة المباشرة ، تنشر ( توزَع) الرسالة السرية بوساطة ثابت يسمى معدل القطعة(Chip Rate) ، لنمذجة الإشارة شبه العشوائية وتضاف إلى الغطاء . أما في الوثب الترددي فإن تردد الإشارة الحاملة يتغير بطريقة قفز سريع من تردد إلى آخر. يستعمل الـ SS بصورة واسعة في سياق العلامة المائية(Contex of Watermarking) (٢٠٠٣)[٦٧].

## ٢. ٥. ٤ المعلومات المخفية الإحصائية(Statistical Steganography)

تستعمل تقنيات المعلومات المخفية الإحصائية(bit ١) لإخفاء ثنائية واحدة من المعلومات في الحامل الرقمي ، وذلك بتغيير الخصائص الإحصائية للغطاء إذا تم إرسال "١"وإلا فإن الغطاء يبقى بدون تغيير ، وإن المستلم يجب أن يكون قادرا على التمييز بين الأجزاء المعدلة والأجزاء التي لم يطرأ عليها تعديل .

ولتركيب (بناء ) نظام إخفاء l(m) من الثنائيات من تعدد أنظمة إخفاء(bit ١) ، تقسم الغطاء إلى l(m) من القطاعات المختلفة $\{B_{١},....,B_{l(m)}\}$ . ولحشر الثنائية السرية $m_i$ في القطاع

i-th يتم إحلال "١" في $B_i$ إذا كانت ($m_i$=١) وإلا فإن القطاع يبقى من دون تغيير . ولاسترجاع الثنائية السرية تستعمل دالة اختبار(Test Function) لتمييز القطاعات المعدلة عن القطاعات غير المعدلة .

$$f(B_i)=\begin{cases}1 & \text{block } B_i \text{ was modified in embeded process}\\ 0 & \text{otherwise}\end{cases}\}.....(1-8)$$

تعدّ الدالة f دالة اختبار الفرضية(Hypothesis-Testing Function) لاختبار

فرضية العدم(Null-Hypothesis) "القطاع لم يتغير" وإلا فإن القطاع تم تغييره ، وعلى المستلم أن يطبق الدالة f على كل قطاعات الغطاء $(B_i)$ من اجل استرجاع كل ثنائية من الرسالة السرية .

هناك عدة حالات ، تكون هذه التقنية فيها صعبة التطبيق هي : يجب أن يوجد أفضل اختبار إحصائي للتمييز بين قطاعات الغطاء المعدلة وغير المعدلة ، زيادة على إن التوزيع يجب أن يكون طبيعياً ، وتعد مهمة تحقيق هذه الشروط عملية صعبة الحصول(٢٠٠٣)[٦٧].

## ٢. ٥. ٥ تقنيات التشويه(Distortion Techniques)

تختلف تقنيات التشويه عن تقنيات الإبدال بأنها تتطلب وجود الغطاء الأصلي (Original Cover) في عملية الاسترجاع ، تتضمن عملية الإخفاء سلسلة من التغيرات التي تنجز على الغطاء وهذه التغيرات تمثل (تقابل) الرسالة السرية المراد إرسالها . أما في عملية الاسترجاع فإن المستلم يحسب الفرق بين الوسط الحامل (الغطاء) للرسالة والغطاء الأصلي من اجل استرجاع سلسلة التغيرات التي طبقت من المرسل والتي تقابل (تمثل )الرسالة السرية . في الكثير من التطبيقات نجد أن مثل هذه الأنظمة غير مفيدة ، لأن المستلم يجب ان يعرف الغطاء الأصلي ليستطيع استرجاع الرسالة .فإذا استطاع المهاجم أن يصل إليها . فإنه سوف يكتشف التغيرات التي طرأت على الغطاء وبعد ذلك يحصل على الرسالة السرية .

كذلك في حالة كون دوال الإخفاء والاسترجاع Embedding and Extraction)

Function) معلنة(Public) ولا تعتمد على مفتاح سري(Stego-Key) فإنها تكون سهلة الكسر من المهاجم وبعد ذلك يستطيع استرجاع الرسالة السرية بصورة كلية(٢٠٠٣)[٦٧].

## ٢. ٥. ٦ تقنيات توليد الغطاء(Cover Generation Techniques)

تختلف هذه التقنيات عن كل الطرق السابقة ، ومن أجل إضافة معلومات سرية إلى

غطاء خاص ، فإنه تطبق خوارزمية إخفاء تقوم ببعض تطبيقات الإخفاء بتوليد كيان(غطاء-وسط) رقمي(Digital Object) لغرض جعله غطاء لإخفاء المعلومات (٢٠٠٣)[٦٧] .

## ٢. ٦ طريقة القطاعات المتشابهة:

اقترحت طريقة جديدة لإخفاء صورة داخل صورة توفر إمكانات في عملية الإخفاء .
حيث إنها تعد أكثر الطرائق أمنية وحصانة وذلك لأنها تعتمد على معلومات سرية ترسل بصورة مستقلة وهذه المعلومات تمثل حجم القطاع ومواقع القطاع ، ومن دون هذه المواقع لن يستطيع المستلم استرجاع الصورة المخفية زيادة على إن هذه الطريقة هي الأكثر مقاومة ضد التغيرات والمعالجات التي تنجز على الصورة الحاملة للصورة المخفية .

تعتمد هذه الطريقة على إيجاد القطاعات المتشابهة بين الصورة المراد إخفاؤها وصورة الغطاء وهي تتضمن خمس مراحل : ففي المرحلة الأولى تختبر صورة الغطاء لمعرفة مدى ملاءمتها لتكون غطاء مناسب للصورة المراد إخفاؤها وقد استعمل مقياسان هما التشابه(Similarity) والاختلاف(Dissimilarity) بالاعتماد على حساب المدرج التكراري(Histogram) الذي يعطي خصائص إحصائية للصورة( من خلال عد عناصر الصورة التي تمتلك الشدة اللونية نفسها ) وكما في المعادلتين (١٩٩٩)[٤٢] .

$$S\{H(E),\ H(C)\} = \frac{\sum_{j=1}^{n} \min\{h_j(E), h_j(C)\}}{Nc \times Mc} \quad .....(2-3)$$

$$D\{H(E),\ H(C)\} = \sum_{j=1}^{n} \left| \frac{h_j(E)}{Ne \times Me} - \frac{h_j(C)}{Nc \times Mc} \right| \quad .....(2-4)$$

حيث تستعمل المعادلة (٣-٢) لقياس التشابه بين المدرج التكراري للصورة المخفية(E) وصورة الغطاء(C) . و$h_j(E)$ هي عدد العناصر ذات اللون (j) في الصورة (E) و$h_j(C)$ هي عدد العناصر ذات اللون (j) في الصورة (C) وMcxNc هو حجم صورة الغطاء و min{} تمثل اصغر قيمة . أما المعادلة

(٤-٢) فتستعمل لقياس الاختلاف بين (E) و( C) ، حيث Me×Ne يمثل حجم الصورة المخفية (E) و || || تمثل القيمة المطلقة .

كما استعملت معادلة حسن المطابقة (Goodness of Fit) في عملية اختبار التوافق بين صورتي الغطاء والمخفية وكما في المعادلة (١٩٨٥)[٤٣] :

$$S = \frac{\sum_{i=1}^{n} (C_i - E_i)^2}{C_i} \quad .....(2-5)$$

حيث إن $E_i$ تمثل الصورة المخفية و $C_i$ تمثل صورة الغطاء .

بعد اختيار الغطاء المناسب تأتي مرحلة الإخفاء وفيها يتم تقسيم كلا من الصورة المراد إخفاؤها والغطاء إلى قطاعات (Blocks) ، ثم تبدأ عملية البحث عن القطاعات المتشابهة . تعتمد عملية البحث على خاصية (صفة) تستخلص من كل قطاع من قطاعات الصورة المراد إخفاؤها (بعد أن يتم تقلص عدد القطاعات بحيث يخفى قطاع واحد من القطاعات المتشابهة) مع جميع قطاعات صورة الغطاء لإيجاد القطاع المشابه له أو القريب أليه ليُستبدَل مع ذلك القطاع .

إن تمثيل الصورة بمركبة أو عدد قليل من المركبات تحمل معلومات كافية للتمييز أي تحويل مستوى واطئ من تمثيل بيانات الصورة ( عناصر الصورة ) إلى مستوى عال من تمثيل البيانات ( عدد قليل من القيم الرقمية ) وهذه القيم يشار اليها بمصطلح " خصائص " التي يتم إدخالها مباشرة للتعرف على الأنماط ، حيث إنها تحتفظ بمعلومات كافية تتمكن من تصنيف الصور أو أجزاء منها .

وقد استعملت معادلة الارتباط المشترك المعدل(Normalized Cross-Correlation) لقياس التشابه(الارتباط) بين صورتي الغطاء والمخفية ( إذ تعد صفة مستخلصة عن كل قطاع ) وكما في المعادلة (٢٠٠١)[٣٢] :

$$Ncc(w1, w2) = \frac{(w1 - \bar{w1}) \bullet (w2 - \bar{w2})}{\left\| w1 - \bar{w1} \right\| \bullet \left\| w2 - \bar{w2} \right\|} \quad .....(2-6)$$

**إذ إن w١,w٢ يمثلان متجهين (قطاعين) أحدهما للصورة المخفية والآخر لصورة الغطاء و $\bar{w1}, \bar{w2}$ يمثل معدل القطاعين و || || يمثل المعيار (Norm) . إن المعادلة (٦-٢) لم تحقق نجاحا كبيرا في عملية المقارنة بين القطاعات .**

وقد استعملت معادلة حسن المطابقة (Goodness Fit) في عملية الموازنة حيث إن $E_i$ يمثل قطاع من الصورة المخفية و $C_i$ يمثل قطاع من صورة الغطاء . وقد حققت هذه المعادلة نجاحا كبيرا وذلك لان عملية الموازنة تكون بموازنة كل عنصر من عناصر قطاع الصورة المراد إخفاؤها مع العنصر المقابل له في قطاع صورة الغطاء .

تتطلب هذه الطريقة حفظ مواقع الإخفاء (أرقام القطاعات) . أما في عملية الاسترجاع ، فيتم استرجاع كل قطاع من قطاعات الصورة المخفية وذلك من معرفة موقع ذلك القطاع داخل الصورة الناتجة بعد الإخفاء(Stego-image) . إن هذه المواقع ترسل بصورة مستقلة عن صورة (Stego-image) ومن دونها لن يستطيع المستلم استعادة الصورة المخفية ( أي إن رقم كل قطاع من قطاعات الصورة المخفية يقابله رقم قطاع في صورة الغطاء ومن هذا الرقم يستطيع استرجاع عناصر القطاع ) .

كذلك طُبقَت خصائص أخرى مثل متوسط الانحراف المطلق الذي يمثل مقياسا لشدة التباين بين القيم اللونية(intensity) للصور ، فالتباين الكبير يعطي دلالة على إن الصورة تمتلك اختلافات عالية وبالعكس وكما في المعادلة (١٩٨٤)[٤٤] .

$$M = \frac{\sum_{i=1}^{N} \left| x_i - \bar{x}i \right|}{N} .....(2-7)$$

حيث إن $x_i$ يمثل قطاع من الصورة و $\bar{x_i}$ يمثل معدل القطاع و N تمثل حجم القطاع و

$/ \bar{x_i} - x_i /$ يمثل الفرق المطلق لـ $x_i$ ، $\bar{x_i}$ .

ويجب أن يكون اختيارنا للصورة بشكل جيد بحيث لا تحتوي على مساحات كبيرة من الألوان الجامدة . بسبب إن أي تغيير طفيف ناتج عن المعلومات المخفية سوف يكون واضحاً في صورة الإخفاء(٢٠٠٢)[٧] . كما إن الحجم الكبير لصورة الغطاء يكون غير طبيعي وقد يثير شكوك المتطفلين ، كما يكون مربكاً في عمليتي الإرسال والاستلام (٢٠٠٣)[٦٧].

## ٢. ٧ نظام المويجة (Wavelet System)

**تحليل قاعدة المويجة هي أداة حل مشكلة مثيرة جديدة للمختصين بالرياضيات،والعلماء والمهندسين. وهي تناسب الحاسبة الرقمية بصورة طبيعية بدوالها الأساسية الموصوفة المحددة بواسطة عمليات الجمع وليس بالتكاملات أو الاشتقاقات وهي لا تشبه أغلب أنظمة التوسع التقليدية،الدوال الرئيسة لتحليل المويجات ليست معادلات تفاضلية ، إنها أولا أداة جديدة حقيقية ظهرت في السنين الحديثة .**

في عام ١٩٠٩ ظهرت المويجة في ملحق أطروحة (A.Haar) (١٩٩٢)[٤٥]. الخاصية الأهم لمويجة(Haar) إنها تملك دعماً محكماً ، وهذا يعني إنها تختفي(تتلاشى) خارج الفترة المنتهية. في عام

١٩٣٠ بضع مجاميع عملت بحوث مستقلة لتمثيل دالة باستخدام دالة قاعدة الاختلاف-التقييس.لسوء الحظ إن هذه القواعد تمتلك نقاط ضعف.على سبيل التمثيل (Philip Franklin) وهو بروفيسور في (MIT) (١٩٩٦)[٤٦]. يملك فكرة خلق قواعد متعامدة باستخدام القواعد السابقة . ضعف قاعدة (Franklin) هو إنها لا تملك تركيباً خوارزميَاً بسيطاً (١٩٩٦,١٩٩٥,١٩٩٣)[٤٦,٤٧,٤٨].دالة (Franklin) لا تشبه قاعدة مويجة (Haar) لأنها ليست مشتقة من دالة ثابتة($\varphi(t)$) بتحويلات صحيحة وتقسيم ثنائي . إن هذا القصور جعل نظام (Franklin) مقيداً ومنسيَاً اكثر من ٤٥ سنة . وبين عام ١٩٦٠ و ١٩٨٠ ، درس الرياضيان(Guido Weiss) و(Ronalld Coifman) ابسط عناصر مجال الدالة ، وقد سميت بالذرات . كانت موضوعيتهم هي إيجاد ذرات لدالة شائعة وإيجاد قواعد تسمح بإعادة إنشاء جميع عناصر الدالة باستخدام هذه الذرات.

في عام ١٩٨٠ قام الفيزيائي(Grossman) والمهندس(Morlet) بتعريف المويجة في سياق فيزياء الكم(١٩٩٦)[٤٩].في عام ١٩٨٥ أعطى(Stephane Mallet) (١٩٩٤)[٥٠] المويجة قفزة إضافية خلال عمله في معالجة الإشارة . حيث اكتشف بعض العلاقات بين مرشحات المرور وأساسيات المويجة المتعامدة(orthonormal) (١٩٩٥,١٩٩١)[٥١,٥٢].

أنشأ(Meyer) أول مويجات لا تشبه مويجة(Haar) وهي مختلفة بصورة مستمرة ، وعلى أية حال فهما لا يمتلكان دعماً محكماً (١٩٩٥)[٥٢]. في السنتين اللاحقتين استخدم(Ingrid Daubechies) عمل (Mallet) لإنشاء مجموعة دوال قواعد المويجة المتعامدة(orthonormal) (١٩٩٣)[٥٣,٥٤] ، التي تزود تحليل وتركيب فعال أكثر بكثير من الذي نحصل عليه بواسطة نظام(Haar) (١٩٩٩)[٥٥].

الهدف الرئيس لأكثر امتدادات الدالة أو الإشارة هو للحصول على معاملات الامتداد التي تعطي معلومات مفيدة عن الإشارة بالمقارنة مع المعلومات الواضحة المباشرة من الإشارة نفسها. الهدف الثاني هو للحصول على المعاملات أكثرها تكون صفراً أو صغيرة جدا. وهذا ما يسمى بالتمثيل اليسير(Spare Representation) وهو مهم للغاية في تطبيقات التخمين الإحصائي والكشف (Statistical Estimation and Detection)،ضغط البيانات(Data Compression) ، إزالة الضوضاء اللاخطية (Nonlinear Noise Reduction)، والخوارزميات السريعة(Fast Algorithm) على الرغم من ان هذا الامتداد سمي بتحويل المويجة المتقطع (Discrete Wavelet Transform)،فمن الممكن أن تسمى بمتسلسلة المويجة (Wavelet Series) بسبب إنها

امتداد أو توسع متسلسل يحول دالة المتغيرات المستمرة إلى سلسلة من المعاملات بطريقة سلسلة فورير نفسها (Fourier Series). توجد كثير من أنظمة المويجة المختلفة التي يمكن أن تستخدم بصورة كفوءة. لكنها جميعا تملك الخصائص العامة الثلاث الآتية:-

١- نظام المويجة(wavelet system) هو مجموعة قطع مبنية إلى تركيب أو تمثيل إشارة أو دالة . وهي إشارة ذات بعدين . بعبارة أخرى ، إذا مجموعة المويجة أعطيت $\psi_{j,k}(t)$ تشير $j, k= ١, ٢, ...$ إلى امتداد خطي فإنها ستكون $f(t)= \sum_k \sum_j a_{j,k} \psi_{j,k}(t)$ لبعض مجموعة معاملات $a_{j,k}$ .

٢- امتداد المويجة يعطي تمركز الوقت-التردد للإشارة. وهذا يعني اغلب طاقة الإشارة

تمثل جيدا ببعض امتداد معاملات $a_{j,k}$ .

٣- حساب المعاملات من الإشارة يمكن أن يعمل بصورة كفوءة. وهذا يعود إلى إن كثيراً

من تحويلات المويجة (مجموعة معاملات الامتداد) يمكن أن تحسب بعمليات O(n).

وهذا يعني إن عدد عمليات الضرب والجمع الحقيقية تتزايد خطيا مع طول الإشارة. إن أكثر تحويلات الموجة العامة تحتاج $O(N \log(N))$ من العمليات كما في تحويلات فورير(FFT).

في الواقع جميع أنظمة المويجة تمتلك هذه الخصائص العامة.بحيث إن سلسلة فورير تحول دالة البعد الواحد للمتغيرات المستمرة إلى سلسلة البعد الواحد من المعاملات بينما امتداد المويجة (wavelet) يحولها إلى مصفوفة ذات بعدين من المعاملات. سوف ترى إن التمثيل ذوي البعدين يسمح بتمركز الإشارة لكلا الوقت و التردد .

## خصائص محلية المويجات يسمح بالحدث الوقتي لامتداد المويجة أن يمثل بعدد قليل من المعاملات. وهذا أعطى نتيجة مفيدة في التطبيقات.

امتداد سلسلة فورير تمركزت بالتردد في ذلك إذا امتداد سلسلة فورير للإشارة نفسها يعطي تمركزاً بالوقت. فالإشارة هي نبضة بسيطة ، موقع تلك النبضة متمركز بالوقت . تمثيل الموجة سيعطي موقعاً في كلا الوقت والتردد بصورة متزامنة.

في الحقيقة ، تمثيل المويجة يشبه الإشارة الموسيقية بحيث إن موقع النغمات يخبرنا أين يرد الصوت وما هي ترددات (١٩٩٨)[٥٦].

## ٢. ٧. ١ الترشيح والتنقيص ( Filtering and Down-Sampling)

في نظام معالجة الإشارة الرقمية ، ينجز الترشيح(filtering)عملية طي سلسلة الأرقام

(الإشارة المدخلة) بمجموعة من الأرقام تدعى بمعاملات المرشح(Filter Coefficient) ، أوزان(Weights) أو استجابة النبضة(Impulse Response). توجد لسلسلة الإدخال x(n) و معاملات المرشح h(n) ، سلسلة إخراج وتساوي y(n) كما مبين في المعادلة الآتية (١٩٩٥)[٤٧]:

$$y(n)=\sum_{k=0}^{N-1} h(k)\, x(n-k) \quad \ldots(2.25)$$

إذا كان عدد معاملات المرشح(N)يساوي عدد منتهى ، فإن المرشح يسمى باستجابة النبضة المنتهية(Finite Impulse Response) مختصرها(FIR).وإذا كان العدد غير منتهي فيسمى باستجابة النبضة غير المنتهية(Infinite Impulse Response) ومختصرها(IIR).

مشكلة التصميم هي في اختيار h(n) للحصول بعض التأثيرات المرغوبة ، وغالبا تستخدم لإزالة الضوضاء(noise) أو فصل الإشارات.

في المرشحات الرقمية المتعددة النسب توجد علاقة مفترضة بين الفهرس الصحيح (n) في الإشارة x(n) والوقت. وغالبا سلسلة الأرقام فصلت بشكل تام بعينات من دوال الوقت .

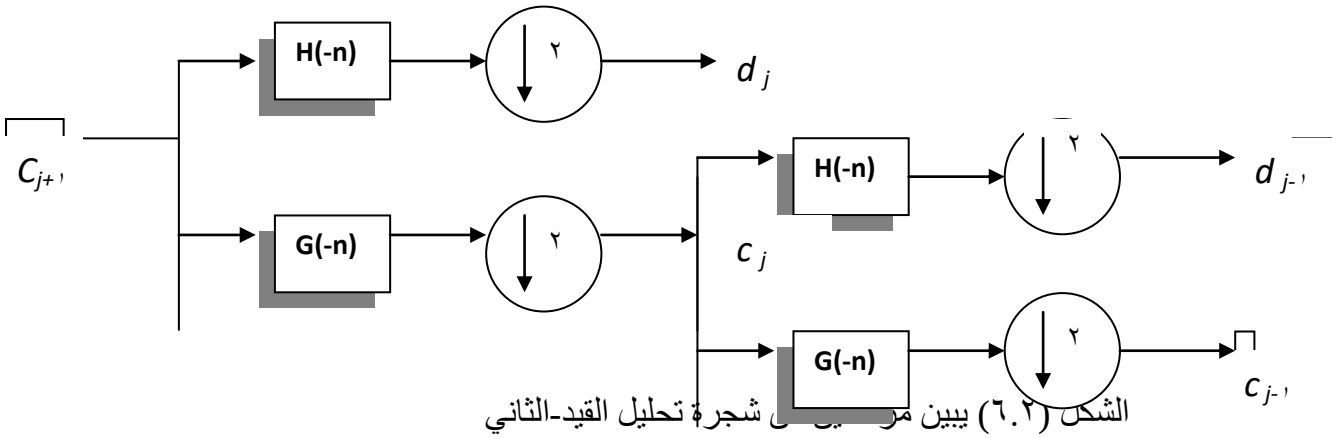
توجد عمليتان أساسيتان في مرشحات النسب المتعددة وهما التنقيص(Down-sampling) والزيادة(up-sampling).ويسمى التنقيص أحيانا بالممثل(sampler) .

$$c_j(k) = \sum_m h(m-2k)\, c_{j+1}(m) \ldots..2.23$$

$$d_j(k) = \sum_m g(m-2k)\, c_{j+1}(m) \ldots..2.24$$

**تبين المعادلتان (٢.٢٣) و(٢.٢٤) إن معاملات التقييس ومعاملات المويجة يمكن الحصول عليها عند المستويات المختلفة وذلك بطي المعاملات عند المستوى( j ) بمعاملات تكرار معكوس-الوقت h(-n) و g(-n) ثم التنقيص لتعطي**

**معاملات امتداد في المستوي اللاحق (j-١) ، بعبارة أخرى ، معاملات التقييس j ) ( رشحت بمرشحين رقميين (FIRS) بمعاملات h(-n)، g(-n) اللذان أعطيا بعد التنقيص معاملات تقييس ومعاملات المويجة. إنجاز المعادلات (٢.٢٣) و(٢.٢٤) موضح بالشكل (٦.٢)[٥٦] ، بحيث إن أسهم نقاط التنقيص(down-pointing) ترمز إلى التنقيص باثنين والصناديق الأخرى ترمز إلى مرشحات(FIRS) أو الطي باستخدام h(-n)، g(-n) . مرشح (FIRS) أنجز بواسطة h(-n) –مرشح المرور الواطئ(Low pass filter)-و آخر أنجز بواسطة g(-n) – مرشح المرور العالي(high pass filter)- ،إن هذا الانقسام الترشيح والتنقيص يمكن أن يكرر على معاملات التقييس ليعطي تركيب قياس-ثان كما في (٦.٢)[٥٦].**

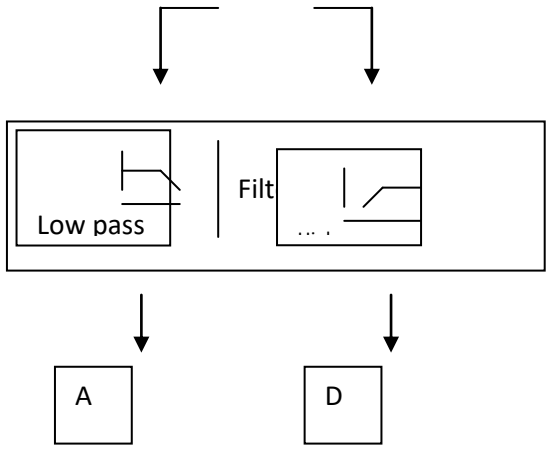



الشكل (٦.٢) يبين مرشحات شجرة تحليل القيد-الثاني

تكرار هذه العملية على المعاملات يسمى ببنك مرشح التكرار(Iteration Filter Bank).إن تكرار جسر المرشح (filter bank) مرة أخرى يعطينا تركيب قياس ثلاثي .

المرحلة الأولى للجسرين(banks) تقسم طيف ($c_{j+1}(k)$) إلى حزمة الامرار الواطئ(low pass band) وحزمة الامرار العالي(high pass band) منتجة معاملات التقييس ومعاملات المويجة عند النتاج الأدنى $c_j(k)$ و $d_j(k)$ . في المرحلة الثانية تقسم حزمة الامرار الواطئ (low pass band) إلى حزمة امرار واطئة أدنى وحزمة امرار أعلى كما في الشكل(٦.٢) (١٩٩٨)[٥٦] .

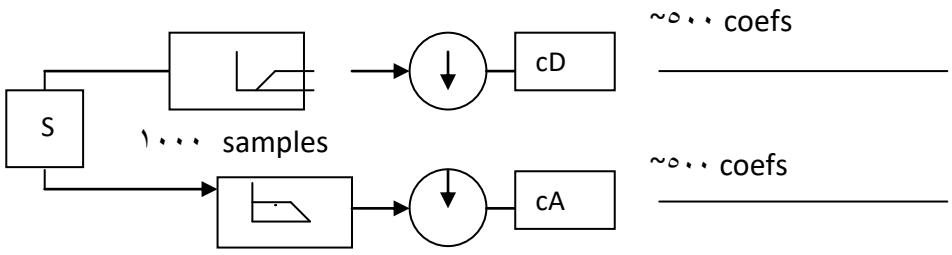
يعد محتوى التردد الواطئ (low frequency) هو الجزء الأكثر أهمية وهذا المحتوى يعطي للإشارة كيانها . من جهة أخرى محتوى التردد العالي(high frequency) يعطي للإشارة خصوصية أو فارقاً دقيقاً ، فمثلا في صوت الإنسان إذا أزلنا محتوى التردد العالي(high frequency) فإن الصوت الناتج سيكون مختلفاً لكن نستطيع إن نخبر الآخرين بما سمعنا ، أما إذا أزلنا كمية كافية من التردد الواطئ(low frequency) فإننا سوف نسمع ثرثرة غير مفهومة(gibberish) .ولهذا السبب بتحليل المويجة (Wavelet analysis) ، فإننا غالبا ما نتحدث عن التقريبات (Approximations) والتفاصيل(Details) . تقيس التقريبات(Approximations) الترددات الواطئة ( Low Frequencies) للإشارة أما التفاصيل(Details ) فتقيس الترددات العالية(high frequencies) .




الشكل(٧.٢) إشارة تمر خلال مرشحات

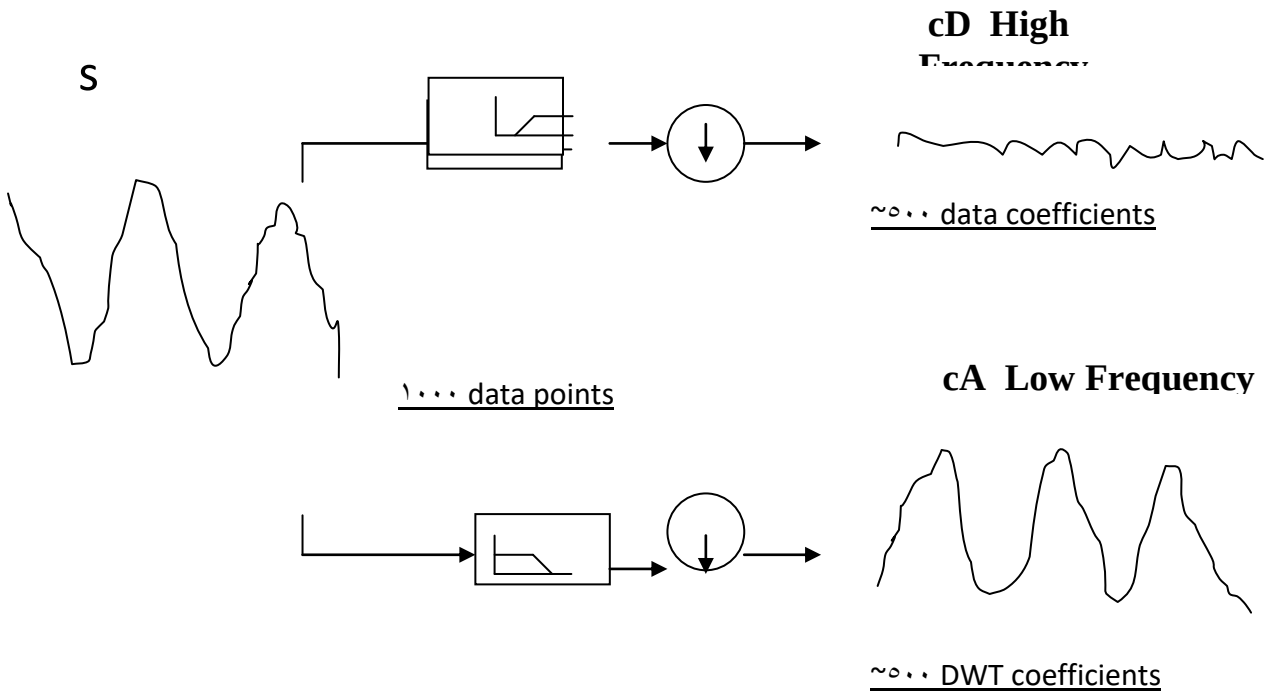
الإشارة الأصلية S تمر خلال مرشحات (filters) مكملة وتفصل إلى إشارتين . لسوء الحظ إذا أنجزت هذه العملية فإننا سنحصل على بيانات مضاعفة أي إذا كانت لكل من التقريبات والتفاصيل قيم عددها (١٠٠٠) عينة فإن العدد الكلي سيكون (٢٠٠٠) عينة كما موضح في الشكل(٧.٢)[٥٧]

لتصحيح تلك المشكلة نجري عملية التنقيص(downsampling) كما مبين في الشكل (٨.٢)[٥٧] :



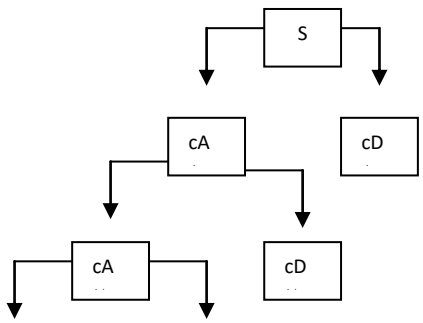

الشكل(٨.٢) يبين عملية التنقيص

وهذه العملية سوف تنتج معاملات تحويل المويجه ، ونلاحظ إن معاملات التفصيلات مؤلفة بشكل عام من ضوضاء ذي تردد عالي . بينما معاملات التقريبات اقل ضوضاء بالمقارنة نسبيا مع الإشارة الأصلية كما مبين في الشكل(٩.٢)[٥٧].




الشكل(٩.٢) يبين الضوضاء المرافقة لكل من معاملات التقريبات والتفاصيل

يمكن لعملية التفكيك (decomposition) أن تكرر عدة مرات بحيث إن التقريبات تحلل من جديد ولهذا السبب فإن الإشارة الواحدة ممكن لها أنْ تحلل إلى عدة مستويات وهذا ما يسمى بشجرة تحليل المويجه كما مبين في الشكل(١٠.٢)[٥٧].



الشكل(٢.١٠) يبين شجرة تحليل المويجه (Wavelet Analysis)

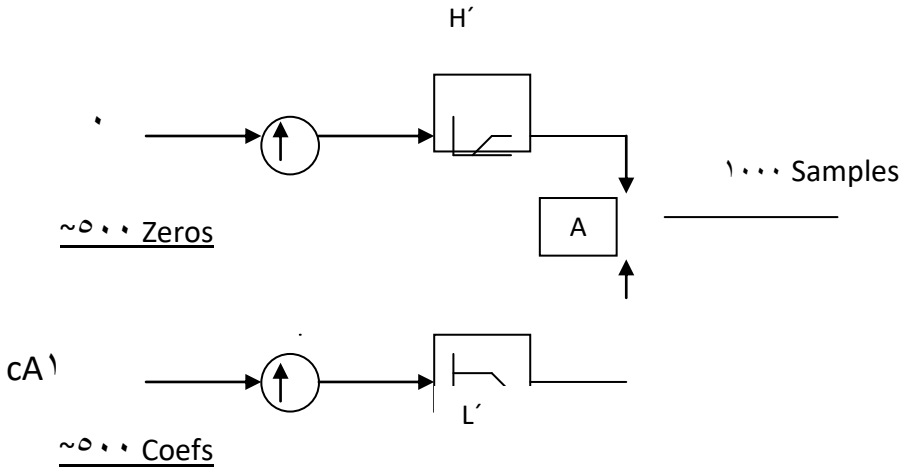
**إن عملية التحليل هي عملية تكرارية ويمكن لها أنْ تستمر بصورة غير منتهية. وفي الحقيقة ينتهي التكرار متى ما أصبحت قيمة التفاصيل مؤلفة من عينه واحدة ، أما اختيار عدد المستويات(levels) فيعتمد على طبيعة الإشارة ، أو المعيار المناسب مثل الانتروبي (Entropy)(١٩٩٧) [٥٧].**

## ٢. ٧. ٢ استخدام معكوس تحويل المويجة المتقطع(IDWT)

وهي تمثل العملية العكسية لتحويل المويجة المتقطع (Inverse Discrete Wavelet Transform)

### أ- إعادة إنشاء التقريبات والتفاصيل (Reconstructing Approximations and Details)

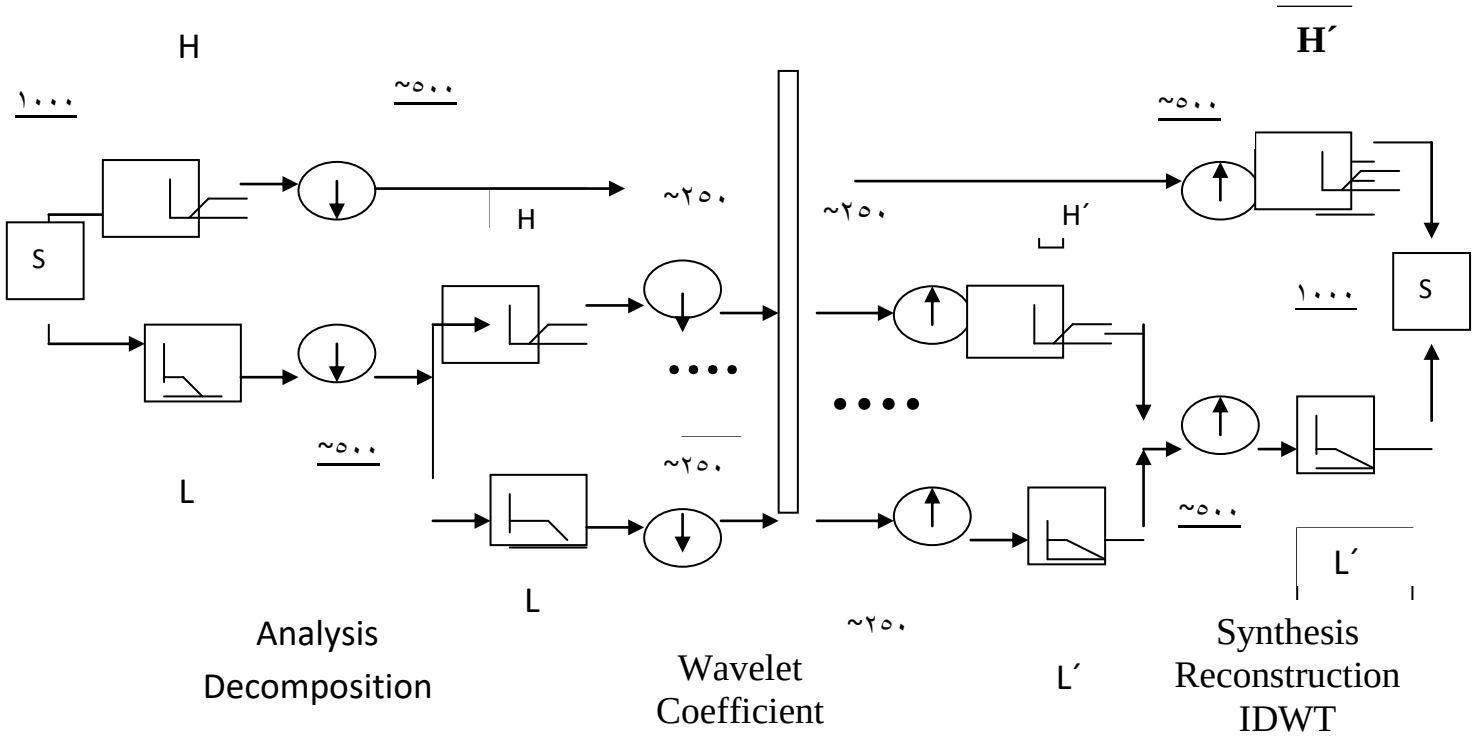
من الممكن إعادة إنشاء الإشارة الأصلية من معاملات التقريبات والتفاصيل من متجهات معاملاتها . على سبيل التمثيل ، عندما نريد إعادة إنشاء المستوي الأول (First-level) من التقريبات من متجه معاملات cA١ . سنمرر متجه معامل cA١ خلال العملية نفسها المستخدمة في إعادة إنشاء الإشارة الأصلية وبدلا من دمجها مع المستوي الأول لـcD١ فإننا سنغذي متجه من الأصفار بدلا من التفاصيل ، كما مبين في الشكل(٢.١١)[٥٧].



الشكل(١١.٢) يبين إعادة إنشاء الإشارة لمستوي واحد

## ب- خطوات متعددة لتفكيك وإعادة إنشاء الإشارة (Multistep Decomposition and Reconstruction)

الخطوات المتعددة لتحليل-و إعادة الإنشاء ممكن إن تلخص بالشكل(١٢.٢)[٥٧].




الشكل(١٢.٢) يبين إعادة إنشاء الإشارة لعدة مستويات

هذه المعالجة تتضمن ثلاثة جوانب :

١- كسر الإشارة للحصول على معاملات المويجه.
٢- تحديث معاملات المويجه.
٣- إعادة تجميع الإشارة من المويجه (١٩٩٧)[٥٧] .

## ٢. ٨ الضغط (Compression) :

أصبحت عملية ضغط الصورة في مقدمة مجالات معالجة الصورة . وجاء هذا نتيجة التنامي السريع في قدرات الحاسبة وهذا يطابق التنامي الحاصل في الأسواق ذات الأوساط المتعددة ، وتقدم الشبكة الواسعة العالمية(World Wide Web) ، التي تجعل من الإنترنت قابلاً للوصول بسهولة من أي شخص . فضلاً عن ذلك فإن التقدم في تقنية الفيديو قد خلق طلب لخوارزميات ضغط أسرع وافضل واحدث ، بدأ تطور خوارزمية الضغط على تطبيقات صور ذات بعدين ، بسبب إن إشارات الفيديو والتلفزيون مؤلفة من بيانات صور متعاقبة ذات بعدين.

يتضمن ضغط الصورة تقليل حجم ملفات بيانات الصورة ، وفي الوقت نفسه الحفاظ على المعلومات الضرورية . يسمى الملف الناتج بالملف المضغوط(Compressed File) ، ويستخدم لإعادة إنشاء الصورة ، منتجا الصورة المفكوكة الضغط(Decompressed) ، تدعى الصورة قبل الضغط بالصورة غير المضغوطة (Uncompressed Image) وتسمى نسبة الصورة الأصلية (غير المضغوطة) إلى الملف المضغوط بنسبة الضغط ويرمز لها كالآتي(١٩٩٨)[٥٨]:

$$\text{CompressedRatio} = \frac{\text{Uncompressed File Size}}{\text{CompressdFile Size}} = \frac{\text{Size}_U}{\text{Size}_C}$$

يأتي مفتاح الضغط الناجح النموذجي من الجزء الثاني من التعريف-إرجاع المعلومات الضرورية- وهذا يستوجب التمييز أو التفرقة بين البيانات والمعلومات .

ففي الصور الرقمية تشير البيانات لقيم مستوى التدرج الرمادي لعناصر الصورة(pixel) والتي تشير إلى مدى إضاءة عنصر الصورة(pixel) عند نقطة الفراغ . بينما تشير المعلومات إلى ترجمة البيانات بصورة ذات معنى . تستخدم البيانات للتعبير عن المعلومات كما يحدث عندما تستخدم الأبجدية للتعبير عن المعلومات من خلال الكلمات ، مفهوم المعلومات هو مفهوم محيّر ، على سبيل التمثيل الصورة الثنائية التي تحتوي على نص فقط فالمعلومات الضرورية يمكن فقط أن تبقي النص المقروء فقط ، بينما في الصور الطبية يمكن أن تكون كل التفاصيل الدقيقة في الصورة الأصلية .

يوجد نوعان أساسيان من طرق ضغط الصورة – بعضها تحفظ البيانات دون فقدان والأخرى تؤدي إلى خسارة ببعض البيانات النوع الأول تسمى طرائق الضغط دون فقدان(Lossless Methods) بحيث

لا تفقد أياً من البيانات ويمكن استرجاع الصورة بالضبط كما كانت قبل الضغط من خلال البيانات المضغوطة .

**في الصور المعقدة حددت هذه الطرائق لضغط ملف الصورة إلى حوالي اثنين إلى واحد وثلاثة إلى واحد (٢:١ to ٣:١) من الحجم الأصلي؛غالبا ما يكون الضغط المنجز أقل بكثير .**

في الصور البسيطة مثل صور النص طرق الضغط دون فقدان قد تنجز ضغطاً أعلى . النوع الثاني من الطرائق يسمى الضغط بفقدان لأنها تسمح بفقدان بيانات الصورة الحقيقية ، لذا فإن الصورة الأصلية غير المضغوطة لا يمكن أن تخلق بالضبط من الملف المضغوط .

في الصور المعقدة هذه التقنيات يمكن أن تنجز نسب ضغط من ١٠ الى ٢٠ وترجع معلومات بنسب مرئية عالية الجودة .

أما الصور البسيطة ، تكون نسب الضغط فيها كبيرة ويمكن لها أن تحرز نسب ضغط من ١٠٠ إلى ٢٠٠ (١٩٩٨)[٥٨].

## ٢. ٨. ١ طرائق الضغط بفقدان(Lossy Compression Methods)

لإنجاز نسب ضغط عالٍ للصور المعقدة ، فإننا نحتاج إلى طرائق الضغط بفقدان . حيث يزود الضغط بفقدان موازنة بين نوعية الصورة ودرجة الضغط .

في بعض الطرائق المقدمة ، يمكن للصور أن تضغط من ١٠ إلى ٢٠ مرة بدون خسارة للمعلومات المرئية ، ومن ٣٠ إلى ٥٠ مرة بأقل انحطاط للصورة . إن تقنيات تحسين الصورة وتقنيات إعادة الخزن يمكن أن تدمجا مع طرائق الضغط بفقدان لإصلاح الصورة بعد فك الضغط منها .

تمثل طرائق الضغط بفقدان الأدوات المتوفرة لتطوير خوارزمية الضغط وتزود تنوع واسع لنسب الضغط ونوعية الصورة . إن كثيراً من الطرائق تملك معلمات معدلة لتسمح للمستفيد باختيار نسبة الضغط المرغوبة(Desired Compression Ratio) ودقة الصورة(Image Fidelity) .وبصورة عامة فإن نسبة الضغط العالية تنتج صورة أضعف ، لكن النتائج تخدمنا بشكل كبير . كذلك فإن التقنية التي تعمل جيدا على تطبيق ما قد لا تتلاءم مع تطبيق آخر(١٩٩٨)[٥٨] .

## ٢. ٨. ٢ تشفير طول السلسلة (Run Length Encoding)

تعد طريقة تشفير طول السلسلة واحدة من طرق الضغط التي تعمل بحساب عدد العينات التي تملك نفس مستوى الشدة اللونية أو القيمة ، هذا الحساب يسمى بطول السلسلة(Run Length) ويرمّز لاحقا ثم تخزن القيمة وعداد التكرار(١٩٩٨)[٥٨].

الفكرة التي تقف خلف هذه الطريقة لضغط البيانات هي : إذا كان عنصر البيانات ( d ) يتكرر( n ) من المرات المتعاقبة في السلسلة المدخلة ، فنستبدل الـ ( n ) من قيم d الواردة بزوج مفرد يكون بشكل (d,n). إن ظهور ( n ) المتعاقب لعنصر البيانات يدعى بطول سلسلة ( n ) وهذه الطريقة لضغط البيانات تدعى بتشفير طول السلسلة(Run Length Encoding) ومختصرها(RLE). إن أحد مساوئ الضغط بتشفير طول السلسلة(RLE) هي إن مخرجات نتيجة الضغط قد تكون أكبر من البيانات الأصلية (١٩٩٨)[٥٩].

## ٢. ٩ درجة الدقة (Fidelity Criteria):

يمكن تصنيف درجة الدقة إلى صنفين : الاول هو قياس الدقة الهدف (objective fidelity criteria) . والثاني هو قياس الدقة الشخصي (subjective fidelity criteria) ، النوع الأول اقتبس من معالجة الإشارة الرقمية ونظرية المعلومات وزودنا بمعادلات استخدمت لقياس نسبة الخطأ في الصور المنشأة ( مفكوكة الضغط) . أما النوع الثاني فتتطلب تعريف المقياس النوعي لتقيم نوعية الصورة . هذا المقياس يمكن أن يستخدم من الإنسان بشكل شخصي ليحدد النوعية.

إن التقييم بالمقياس الشخصي(subjective) يتطلب اختيار أشخاص الاختبار باهتمام وتصميم تجارب الاختبار بدقة . وبصورة شائعة استخدمت مقاييس الهدف(objective) مثل حساب الجذر التربيعي لمعدل مربع الخطأ(RMSE) ، حساب نسبة الإشارة إلى الضوضاء($SNR_{RMS}$) و حساب قمة نسبة الإشارة إلى الضوضاء(PSNR) ونستطيع أن نعرف الخطأ بين قيم الثمانيات غير المضغوطة (الأصلية) وقيم الثمانيات المفكوكة الضغط .

$$error(r,c)=\hat{I}(r,c)-I(r,c) \quad .....2.25$$

عندما :

$I(r,c)$ : الصورة الأصلية

$\hat{I}(r,c)$ : الصورة المفكوكة الضغط.

$$Totalerror=\sum_{r=0}^{N-1}\sum_{c=0}^{N-1}[\hat{I}(r,c)-I(r,c)] \quad ...2.26$$

ويُستخرَج الجذر التربيعي لمعدل مربع الخطأ(RMSE) بحساب الجذر التربيعي للخطأ مقسوم على العدد الكلي لثمانيات الصورة ويمثل المعدل "mean" .

$$e_{RMS} = \sqrt{\frac{1}{N^2}\sum_{r=0}^{N-1}\sum_{c=0}^{N-1}[\hat{I}(r,c) - I(r,c)]^2} \quad ....2.27$$

أما مقياس نسبة الإشارة إلى الضوضاء$(SNR_{RMS})$ فيعدُ الصورة المفكوكة الضغط $\hat{I}(r,c)$ هي الإشارة والخطأ (error) هو الضوضاء "Noise" لذا نستطيع تعريف نسبة الإشارة الى الضوضاء كما يلي :

$$SNR_{RMS} = \sqrt{\frac{\sum_{r=0}^{N-1}\sum_{c=0}^{N-1}[\hat{I}(r,c)]^2}{\sum_{r=0}^{N-1}\sum_{c=0}^{N-1}[\hat{I}(r,c) - I(r,c)]^2}} \quad .....2.28$$

أما مقياس قمة نسبة الإشارة إلى الضوضاء$(SNR_{Peak})$ فيعرف كما يلي :

$$SNR_{PEAK} = 10\log_{10}\frac{(L-1)^2}{\sqrt{\frac{1}{N^2}\sum_{r=0}^{N-1}\sum_{c=0}^{N-1}[\hat{I}(r,c) - I(r,c)]^2}} \quad .....2.29$$

حيث :

L : هو عدد درجات المستوى الرمادي .

N : بعد مصفوفة الصورة .

إن المقاييس الهدف(objective) غالبا ما تستخدم في البحوث بسبب سهولة توليدها وكونها غير متحيزة (١٩٩٨)[٥٨] .

## ٢. ١٠ الإشارات(Signals)

يمكن أن ترد المعلومات على شكل بيانات رقمية مثل الصوت ، الصورة أو أشكال أخرى ولنقل تلك المعلومات يجب أن تحول إلى إشارات إلكترونية . والإشارات يمكن أن تكون تناظرية أو رقمية . الإشارات التناظرية يمكن أن تأخذ أي قيمة في المدى ، بينما الإشارات الرقمية تأخذ أرقاماً محددة من القيم . تصنف الإشارات التناظرية إلى بسيطة ومعقدة .

الإشارة التناظرية البسيطة ، أو الموجة الجيبية ، لا يمكن أن تفك إلى إشارات ابسط . أما الإشارة التناظرية المعقدة فتنشأ من موجات جيبيه متعددة .

يمكن ان توصف الموجات الجيبيه بثلاث خصائص : هي سعة الإشارة (signal amplitude) وتمثل قيمة الإشارة في أي نقطة على الموجة , الفترة(period) فتشير إلى نسبة الوقت بالثواني والإشارة تحتاج إلى دورة(cycle) واحدة كاملة ، لذا فإن الفترة(period) هي نسبة الوقت الذي تأخذه الإشارة لإكمال دورة واحدة , التردد(frequency) فيمثل عدد الدورات لكل ثانية .وتمثل العلاقة رياضيا بين التردد(frequency) والفترة(period) هي إن أحدهما تعاكس الأخرى فإذا أعطيت أحدهما الاخرى .

**Frequency=١/Period , Period=١/Frequency**

واخيرا الطور(Phase) فهو موقع شكل الموجة المتعلق بوقت البداية عندما يساوي الوقت صفراً (١٩٩٨)[٦٠] .

## ٢. ١٠. ١ الموجات الصوتية

**يختلف البشر في قدرتهم على سماع الأصوات .ونحن نعلم جميعا إن سمع بعض الناس قد يضعف لسبب من الأسباب ، وبذلك تقل حساسية آذانهم بدرجة كبيرة عن حساسية إذن الشخص ذي السمع العادي . ومع ذلك يتفق معظم الناس إلى درجة كبيرة في شدة الصوت الذي يمكن سماعه بالكاد ، وكذلك في جهر الصوت المسبب للألم . ومن ثم يمكننا وضع حدود متوسطة للقدرة السمعية للإذن البشرية .**

وتعتمد استجابة الإذن للصوت على تردده بالإضافة إلى شدته . فالإذن اكثر حساسية لبعض الترددات من البعض الآخر . وقد أثبتت الدراسات إن معظم الناس لا يستطيعون سماع الموجات الصوتية التي يزيد ترددها عن حوالي ٢٠,٠٠٠ Hz .وتسمى الموجات التي يزيد ترددها عن هذه القيمة **بالموجات فوق السمعية** .بمعنى الصوت "الأعلى" أو "الأكبر"من ناحية التردد . بالمثل لا يستطيع معظم الناس إن يسمعوا الأصوات التي يقل ترددها عن حوالي ٢٠ Hz (٢٠٠١)[٦٨].

أهم الخصائص التي يعتمدها السامع لتمييز الأصوات المختلفة هي شدة الصوت ودرجة الصوت ونوعية الصوت . شدة موجة الصوت هي الوحدة لقياس الطاقة المنتشرة خلال وحدة المساحة ، وتعرف درجة الصوت بأنها ذلك الإحساس الذاتي الذي يتوقف على تردد الصوت المسموع ، أي إنها حدة نغمة الصوت كما تشعره الإذن البشرية . ولذلك تعد درجة الصوت مرادفا لتردده ، وتزداد درجة الصوت بزيادة الشده عند الترددات ما فوق ٣٠٠٠ Hz حتى بثبوت التردد ، لكن عندما يكون التردد اقل من ٢٠٠٠ Hz فإن درجة الصوت سوف تقل بزيادة الشدة . من الممكن التمييز بين صوتين لهما الدرجة نفسها وذلك بسبب الاختلاف في نوعية الصوت . إن نوعية الصوت هي التي تمكننا من التمييز بين صوتين لهما العلو والدرجة نفسها ولكنهما صادران من مصدرين مختلفين ، وهذا يعزى إلى الاختلاف في عدد وترتيب وشدة التوافقيات التي يتالف منها كل صوت . إذا كانت أشكال الموجة(Wave Forms )

للصوت هي دورية (Periodic) تقريبا فإن الصوت الناتج سوف يكون لطيفا (إذا كانت شدته ليست عالية جدا) بينما إذا كانت أشكال الموجة ليست دوريه فإن الصوت الناتج يكون أشبه بضوضاء(Noise) ، يمكن إن تمثل الضوضاء بوصفها موجات دورية مركبة .

لو كانت جميع الأصوات هي عبارة عن موجات جيبيه نقية (Sine Waves) ، لاصبح الكثير من الأصوات متشابها تقريبا . وهذا السبب الذي يجعل صفة الصوت (النوعية) تلعب دورا مهما في تمييز الأصوات .فمن خلال علو ودرجة الصوت يمكن التعرف على إن هذا الصوت لرجل ، أو امرأة أو لطفل ، أما نوعية الصوت فتساعد على التعرف على الشخص وتمييزه (٢٠٠١)[٦٩].

الموجات الصوتية هي موجات طولية تنتقل في أي مادة تقريبا ، سواء كانت هذه المادة صلبة أم سائلة أم غازية . وتنشأ هذه الموجات بواسطة أي آلة لتوليد الموجات التضاغطية في الوسط المحيط . والصوت لا ينتقل في الفراغ لعدم وجود المادة التي يمكنها نقل التضاغطات الموجية . والتجربة الشهيرة لإثبات ذلك هي إننا لا نسمع صوت جرس يرن داخل غرفة مفرغة من الهواء ، فبالرغم من إن الجرس يهتز ، فليس هناك مادة محيطة به يمكنها أن تحمل الاهتزاز إلى آذاننا .

إن اهتمامنا ينصب أساسا على انتشار الموجات الصوتية في الهواء لأن هذا هو أساس حاسة السمع لدينا . ومع ذلك فإن الصوت ينتقل بسرعة أكبر وفقد اقل للطاقة في السوائل والجوامد منه في الهواء . وهذا هو السبب في إننا إذا وضعنا أذننا على قضيب السكة الحديد يمكننا بهذه الطريقة سماع صوت اقتراب القطار قبل أن نسمعه في الهواء بوقت طويل . وبالرغم من أن الصوت يعرف عادة بأنه تلك الموجات التي نستطيع سماعها بآذاننا ، فإن ترددات الصوت يمكن أن تكون أكبر كثيرا أو أقل كثيرا من الترددات التي تحس بها الأذن (٢٠٠١) [٦٨].

**٢. ١٠. ٢ الشدة ومستوى الشدة**

إن المصدر الذي يرسل موجة على وتر يرسل الطاقة أيضا مع الموجة . والواقع إن جميع الموجات تحمل طاقة معها ، وليست الموجات الصوتية استثناء من هذه القاعدة .

تعرف شدة الموجة بدلالة الطاقة التي تحملها هذه الموجة . وهكذا يمكننا تعريف شدة الموجة I بأنها الطاقة التي تحملها الموجة عبر وحدة المساحة هذه في الثانية . وحيث إن القدرة هي الطاقة المنتجة في الثانية ،إذن :

شدة الصوت هي القدرة المارة عبر وحدة مساحة عمودية على اتجاه انتشار الموجة.

ووحدات شدة الصوت في النظام (SI) هي الواط لكل متر مربع (٢٠٠١) [٦٨].

**٢. ١٠. ٣ درجة الصوت ونوعية الصوت**

درجة الصوت هي إدراكنا الكيفي لما إذا كان صوت موسيقى معيناً ( أي نغمة موسيقية عاليا حادا(كصوت مغني الأوبرا السوبرانو) ، أو منخفضا غليضا (كصوت مغني الأوبرا الباس) . وتعد درجة الصوت مرادفا لتردد الصوت تقريبا . والعكس صحيح كذلك ، فإذا أنخفض التردد تنخفض درجة الصوت بالتبعية .

ومع ذلك فإن الموجات الصوتية وحيدة التردد ليست شائعة بين الأصوات التي نسمعها عادة . فإذا نقر أحد أوتار الكمان مثلا باليد أو بالقوس فلن تكون الموجة الصوتية الصادرة منه موجة جيبيه قوية . ويستطيع أي شخص أن يتحقق من ذلك بسهولة عندما يقارن النغمة التي يحصل عليها عازف كمان ماهر بالنغمة التي يحصل عليها عازف مبتدئ . ففي الحالة الأولى تكون النغمة تامة وشجية ، بينما قد يحصل العازف المبتدئ على أصوات خشنة ذات صريف ومثيرة للأعصاب من الوتر نفسه. ويقال عندئذ عن نوعية النغمة مختلفة في الحالتين.

ويمكننا أن نلاحظ إن وتر البيانو يعطي عددا اكبر من التوافقيات بالمقارنة بوتر الكمان . وربما يكون ذلك راجعا إلى الطريقة المستخدمة في هز الوتر . ففي حالة الكمان يمرر العازف القوس على الوتر ببطء ونعومة ، بينما يثار اهتزاز وتر البيانو بواسطة ضربة من المطرقة .

يستنتج مما سبق أن نوعية الصوت تعتمد على عدد التوافقيات المكونة له والسعة النسبية لمختلف هذه التوافقيات . وإذا كانت جميع الأصوات موجات جيبيه نقية فإن هذا سوف يفقد الأصوات قدرا كبيرا من تنوعها . وعندئذ ستكون نغمة جميع الأصوات البشرية واحدة ، وعندئذ سوف يمكن تمييز صوت الشخص بالتردد المميز في مقام الصوت أو ارتفاعه فقط . كذلك فإن الموسيقى سوف تفقد قدرا كبيرا من جمالها لو كانت نوعية جميع الأصوات واحدة .

ليس من السهل دائما تحديد درجة الصوت ، ولا سيما إذا كان الصوت معقدا كصوت البيانو آو الكلارينت . ذلك إن درجة الصوت في مثل هذه الحالات ليست مرادفا لتردده ، لأن الصوت يحتوي على عدة موجات مختلفة في التردد ومتساوية تقريبا في السعة . ويوجد بعض الناس من يعانون ضعفا غير عادي في السمع وقد لا يعلمون هم أنفسهم بذلك – إذ لا يستطيع هؤلاء سماع أي صوت يزيد تردد عن حوالي (٦٠٠٠ Hz) . وحيث إن معظم الأصوات التي نسمعها تتكون ، جزئيا على الأقل ، من ترددات أقل من هذه القيمة فإن هؤلاء يمكنهم سماع الأصوات المسموعة لغيرهم . مع ذلك فإن نوعية الأصوات التي يسمعونها تختلف تماما عن نوعية الأصوات التي يسمعها شخص ذو سمع عادي . ويتضح لنا من ذلك إذن إن نوعية الصوت ودرجة الصوت خاصِيتان معقدتان وغير موضوعيتين إلى حد كبير (٢٠٠١) [٦٨].

## ٣. ١ المقدمة

يتكون النظام المقترح بشكل عام من مرحلتين رئيستين ، **مرحلة الإخفاء ومرحلة الاسترجاع** ، في **مرحلة الإخفاء** تم إخفاء صوت داخل صورة ملونة ، أما **مرحلة الاسترجاع** فقد تم استخراج الصوت من الصورة الحاملة لذلك الصوت .

مدخلات مرحلة الإخفاء هي الصوت المراد إخفاءه وصورة ملونة تستخدم كغطاء ، تتضمن **مرحلة الإخفاء** ثلاث مراحل فرعية ، **تسجيل الصوت** ، **قراءة وضغط الصوت** ، **إخفاء الصوت داخل الصورة** .

في **مرحلة تسجيل الصوت** تم تسجيل الصوت باستخدام برنامج (Cool Edit Pro version ٢.٠) ، أما مرحلة **ضغط الصوت** فقد تم باستخدام تقنيات تحويل المويجة المتقطعة (Discrete Wavelet Transform) (DWT) وتشفير طول السلسلة (Run Length Encoding) (RLE) لإغراض التقوية ، حيث تم ضغط عينة بيانات الصوت وزيادة الأمنية . أما مرحلة **إخفاء الصوت داخل الصورة** فقد تم إخفاء بيانات الصوت داخل صورة ملونة مختارة وفق معايير وذلك باستخدام تقنية القطاعات المتشابهة حيث يتم استبدال كل قطعة (Block) من بيانات الصوت بالقطعة (Block) الأكثر شبها بها أو المطابقة لها تماما إن وجدت من بيانات الصورة بدلا من استبدال بت واحد أو بايت كما هو الحال في اكثر طرق الإخفاء . مخرجات مرحلة الإخفاء هي صورة ملونة حاملة للصوت وسلسلة مفتاح بصورة مستقلة .

مدخلات مرحلة الاسترجاع هي صورة ملونة حاملة للصوت وسلسلة المفتاح ( مخرجات مرحلة الإخفاء ) ويتم في هذه المرحلة استخراج الصوت المخفي من الصورة الحاملة بواسطة استخدام سلسلة المفتاح كدليل للوصول إلى مواقع القطع (Blocks) التي تم فيها الإخفاء ، مخرجات هذه المرحلة هي معاملات الصوت الأصلي بعد الضغط حيث يكون الضغط بفقدان (lossy compression) .استخدمت المنظومة البرمجية الماتلاب الإصدار(٦.٥) (Matlab version ٦.٥) في تنفيذ النظام المقترح. والشكل(١.٣) يبين المخطط الكتلي التفصيلي للنظام المقترح .

## ٣. ٢ مرحلة الإخفاء

تتكون هذه المرحلة الرئيسة كما ذكرنا آنفا من ثلاث مراحل فرعية : **تسجيل الصوت ، قراءة وضغط الصوت ، إخفاء الصوت داخل صورة** وسنأتي على ذكرها تفصيليا .

### ٣. ٢. ١ تسجيل الصوت

سجلت العديد من الكلمات القصيرة والجمل باستخدام (Cool Edit Pro version ٢.٠)

وكما موضح في الجدول (٣-١):

الجدول (٣-١) يبين خصائص بعض الجمل أو الآيات المسجلة المختارة

| ت | الآية أو الجملة | السعة | الوقت | شكل الصوت |
|---|---|---|---|---|
| ١ | بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ | (٢٤٢٥٥) عينة | ٠:٠٢.٢٠٠ ثا | pcm ,١١٠٢٥ Hz ,١٦ bit, Mono |
| ٢ | اقرأ وربك الأكرم | (٢١٨٢٨) عينة | ٠:٠١.٩٧٩ ثا | pcm ,١١٠٢٥ Hz ,١٦ bit, Mono |
| ٣ | وانك لعلى خلق عظيم | (٢٨٣٨٣) عينة | ٠:٠٢.٥٧٤ ثا | pcm ,١١٠٢٥ Hz ,١٦ bit, Mono |
| ٤ | علم القرآن | (١٦٥٣٨) عينة | ٠:٠١.٥٠٠ ثا | pcm ,١١٠٢٥ Hz ,١٦ bit, Mono |
| ٥ | غلبت الروم | (١٥٤٣٥) عينة | ٠:٠١.٤٠٠ ثا | pcm ,١١٠٢٥ Hz ,١٦ bit, Mono |
| ٦ | قل هو الله أحد | (١٦٢٧٠) عينة | ٠:٠١.٤٧٥ ثا | pcm ,١١٠٢٥ Hz ,١٦ bit, Mono |

ودرست إمكانية الضغط لهذه التسجيلات الصوتية وعند تحليل الصوت بالـ(wavelet) بعضها نزل إلى مستوي واحد أو إلى اثنين وذلك للأسباب الآتية :

١-الضوضاء وظروف التسجيل .

٢- طبيعة الصوت للأشخاص لم تتم من خلال مخارج الحروف الذي يعطي وضوح كامل للكلمة المنطوقة .

٣- ومن ثم فإن عملية الضغط ستكون محدودة ، ولا يخفى إن حجم الملف الصوتي كبير جدا بالنسبة للسعة الاستيعابية للصورة ولأجل الوصول إلى حالة متوازنة بين الملف الصوتي من خلال زيادة الضغط وحجم الصورة الغطاء التجأنا إلى استخدام التسجيلات الصوتية التي يكون هنالك وضوح في مخارج حروف الكلمة لتحقيق الهدف أعلاه لذا تم الاعتماد على مرتلين معروفين لهذا الصدد.

في النظام المقترح تم اختيار الصوت من أقراص على شكل آيات مرتلة من القرآن الكريم بأصوات مقرئين لامتلاك أصواتهم خصائص مميزه تم ذكرها ، ووضوح مخارج الأحرف عند تلفظ الكلمات ، وقد تم اختيار الآية (بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ) (١٩٨٨)[٧١] ، وذلك لعدم وجود فواصل زمنية بين كل كلمة وأخرى عند القراءة ، إذ إن هذه الفواصل الزمنية تؤدي إلى زيادة طول التمثيل الموجي للصوت ومن ثمَ زيادة بيانات الصوت الدالة على ذلك التمثيل إذ إن العلاقة بينهما هي علاقة طردية.

عولجت الآية باستخدام برنامج (Cool Edit Pro version ٢.٠) ، خزن الصوت على ملف الموجه ذي امتداد (wav) بسبب إن الموجه بهيأة (wav) وهو شكل من أشكال الصوت يستخدم في Microsoft) (Windows وهو واحد من اكثر أشكال الصوت شعبية ، كما إن هذا الشكل من الأصوات يوصى باستخدامه.

شكل الملف (Windows pcm) لأن اغلب ملفات الموجه بهيأة (wav) تستخدم بيانات صوت (pcm) البسيطة(١٩٩٨)[٦١][٦٢] .

وقد لوحظ لاحقا في مرحلة استخدام تحويل المويجة المتقطع(DWT) إن العلاقة بين نسبة العينة(sample rate) ومستوى تحليل المويجة (Wavelet Analysis Level) تتناسب تناسبا طرديا إذ كلما زادت نسبة العينة(sample rate) كلما زادت إمكانية تحليل المويجة (Wavelet Analysis) إلى مستويات أعلى .

## ٣. ٣ قراءة وضغط الصوت

وتعد هذه المرحلة هي المرحلة الفرعية من مرحلة الإخفاء وتتكون من عدة خطوات : **قراءة ملف الصوت ، استخدام (DWT) ، تحويل معاملات الصوت ، ضغط معاملات الصوت باستخدام RLE**.

### ٣. ٣. ١ قراءة ملف الصوت

تعد ملفات الموجه بهيأة (wav) نوع خاص من ملفات (RIFF) ، و تمثل القطعة الخارجية لذلك الملف محتويات (RIFF) مع نوع محتويات الموجه بهيأة (wav) واغلب ملفات الموجه (wav) تحتوي على قطعة الشكل (fmt chunk) وقطعة البيانات (data chunk) والشكل (٣.٣) يبين شكل قطعة (RIFF) .


الشكل (٢.٣) يبين شكل قطعة (RIFF ) ( RIFF Chunk Format )

وبسبب إن كثيراً من ملفات الموجه بهيأة (wav) تمتلك نفس هذا الهيكل الأساسي ، فإن كثيراً من البرامج البسيطة تعامل ملفات الموجه بهيأة (wav) على أنها تملك ترويسة ثابتة (fixed header) وكما موضح في الجدول (٣-٢) (١٩٩٨)[٦١] :

الجدول (٣-٢) يبين شكل ملف الموجه بهيئة ( wav)

| Size | Description |
|---|---|
| ٤ | Chunk type : RIFF |
| ٤ | Total file size minus ٨ |
| ٤ | RIFF container type |
| ٤ | Chunk type : fmt |
| ٤ | Format chunk data length : usually ١٦ |
| ١٦ | Format chunk data |
| ٤ | Chunk type : data |
| ٤ | Length of sound data |
| N | Actual sound samples |

قُرئت بيانات ملف الموجه (wave file) بالإيعاز (wavread) حيث يؤمن هذا الإيعاز

الوصول مباشرة إلى بيانات الصوت بدلا عن تجاوز الترويسه (header) برمجيا والمكونة من ٤٤ bytes كما مبين في الجدول (٣-١)، علما أنَ قيم بيانات ملف الموجه (wave file) محصورة بين ١-] ١ ,[ وهذا بعد اجراء عملية التطبيع(normalized) .

## ٣. ٣. ٢ استخدام تحويل المويجه المتقطع(DWT)

ضُغِطَت بيانات الصوت وزيادة الأمنية باستخدام تحويل المويجة المتقطع (DWT) باستخدام مويجة (Haar) أو(DB١) ولثلاثة مستويات كما هي موضحة في المعادلات آلاتية(١٩٩٨)[٦٣].

$$\varphi(t) = \sqrt{2}\left[ {}^{1}\!/_{\sqrt{2}}\,\varphi(2t) + {}^{1}\!/_{\sqrt{2}}\,\varphi(2t-1) \right] \ldots\ldots\ldots\ldots\ldots (2.19)$$

$$\psi(t) = \sqrt{2}\left[ {}^{1}\!/_{\sqrt{2}}\,\varphi(2t) - {}^{1}\!/_{\sqrt{2}}\,\varphi(2t-1) \right] \ldots\ldots\ldots\ldots\ldots (2.20)$$

تم تطبيق تحويل المويجة المتقطع على بيانات الصوت الأصلي ليقسم الإشارة بالتساوي إلى التقريبات(Approximations) والتفاصيل(Details) لنحصل على المستوي الأول من التقريبات وهو الجزء المهم من الإشارة إذ إن التفاصيل تمثل الجزء الأقل أهمية حيث تعطي للإشارة خصوصية ، لذا يتم تحليل تقريبات المستوي الأول فقط من جديد لنحصل على تقريبات وتفاصيل المستوي الثاني ، وهكذا تجرى العملية نفسها على تقريبات المستوي الثاني لنحصل في النهاية على تقريبات وتفاصيل المستوي الثالث ويعتمد اختيار عدد المستويات على طبيعة الإشارة حيث لوحظ من خلال التجربة إن تقريبات الإشارة في المستوي الثالث قد تعرضت إلى كثير من الفقدان لدرجة إن إمكانية فهم الصوت عند الاسترجاع بالكاد تكون مفهومه للبعض ، وإن التحليل للمستوي الرابع فما فوق سيؤدي إلى فقدان طاقة الإشارة مما يسبب عدم القدرة على تمييز الصوت عند الاسترجاع . وكلما زادت نقاوة الصوت وزاد وضوحه كلما زادت إمكانية التحليل لمستويات أعلى قد تصل إلى المستوي الخامس أو اكثر ومن ثمَ زيادة كفاءة نتائج تحويل المويجة المتقطع من حيث ضغط البيانات.

## ٣. ٣. ٣ تحويل معاملات الصوت

بعد تطبيق تحويلات المويجه المتقطعة (DWT) للمستوي الثالث على بيانات الصوت الأصلية ، نحصل على معاملات الصوت . لقد أشرنا سابقا إلى أن قيم بيانات الصوت تتراوح ضمن المدى [١ , ١-] وتختلف قيم معاملات الصوت عن بيانات الصوت الأصلي إذ إنها تقع ضمن مدى غير معلوم قد يكون اقل من (١-) واكبر من (١) ، وبما إن هذه المعاملات يراد إخفاؤها في صورة ملونه ذات ثمانيَة واحدة لكل عينه أي قيمها تتراوح بين ٠-٢٥٥ ، لذا يجب تحويل هذه المعاملات بنفس مدى قيم بيانات الصورة ، ولإجراء ذلك يجب:

١-التخلص من مشكلة القيم السالبة بإيجاد القيمة الصغرى (minimum value) من معاملات الصوت وتخزن في متغير min.

٢-إضافة القيمة المطلقة للقيمة الصغرى لجميع قيم معاملات الصوت لنحصل على قيم موجبة للمعاملات

٣-أيجاد القيمة العظمى (maximum value) للقيم الموجبة للمعاملات وتخزن في متغير max ونضرب هذه القيم بمعامل ويساوي(٢٥٥/max) بحيث تصبح أعلى قيمه موجبة للمعاملات تأخذ ٢٥٥ واقل قيمه تأخذ صفراً .

القيم الناتجة ستكون قيماً حقيقيةً وبما إن قيم بيانات الصورة صحيحة لذا تقرب القيم الناتجة لتصبح قيماً صحيحة.

والخوارزمية (١.٣) تبين تحويل معاملات الصوت .

**Sound Coefficients Transformation Algorithm**

Input: Sound Coefficients Array (a٣)

Output: Sound Coefficients Array (a)(Real Positive Values)

Step١: Calculate the Minimum value for coefficients and put in (Min) .

Min ⟵ a٣[١]

For i⟵١ to Length(a٣) do

Begin

If a٣[I] < Min

Min ⟵ a٣[i]

End

Step٢: Add the Absolute value of(Min) to all Coefficients to

Remove the minus sign problem and to get positive Coefficients.

For i ⟵ ١ to Length(a٣) do

## ٣. ٣. ٤ ضغط معاملات الصوت بطريقة تشفير طول السلسلة(RLE)

بعد تحويل معاملات الصوت ضمن المدى ٠...٢٥٥ في المرحلة السابقة ، لوحظ من خلال التجربة إن القيم الناتجة تمتلك خصائص أهمها تطابق أو تقارب القيم المتجاورة من حيث المقدار وبالاستفادة من هذه الخاصية يمكن ضغط هذه القيم باستخدام تقنية تشفير طول السلسلة (RLE) لتقليل تمثيل هذه المعاملات بعدد اقل من القيم ، وتجري هذه العملية على مرحلتين:

**المرحلة الأولى** يجري فيها حساب مجموع تكرار القيم المتطابقة المتجاورة وتمثل هذه المجموعة بقيمة واحدة يقابلها التكرار الكلي( مجموع تكرار القيمة) . **المرحلة الثانية** نختار قيمة تمثل العتبة(Threshold) من خلالها يتم الضغط على ألا يزيد الفرق بين القيمة السابقة واللاحقة عن العتبة(Threshold) وتخزن القيمة ذات التكرار الأعلى ويتم ضغط المعاملات بتعميم القيمة التي تملك أعلى تكراراً .علما إن العتبة(Threshold) يتم اختيارها بالتجربة أو بحساب التباين(Variance) ،حيث إن معاملات الصوت التي تملك أعلى تبايناً(Variance) تتحمل ضغطاً اكثر أي إمكانية زيادة قيمة العتبة(Threshold) ، إذ كلما زاد تباين قيم معاملات الصوت كلما زادت إمكانية تعظيم قيمة العتبة(Threshold) .

والخوارزمية (٢.٣) تبين ضغط معاملات الصوت بطريقة تشفير طول السلسلة(RLE).

**RLE Algorithm**

Input: Coefficients of sound as an array (a) with one dimension.

Output: array with one dimension (RLE_ARRAY) contains RLE values.

Step١: Put the first value of data Coefficients (a) in value column of Array(b١). Put Zero in occurrence column of array (b١).

Step٢: Compare array(b١) with array of Coefficients(a).

والخوارزمية (٣.٣) تبين ضغط معاملات الصوت باستخدام العتبة(Threshold).

**Sound Coefficients Values Compression Algorithm**

Input: array with two dimension (b١) contains value column and Occurrence column.

Output: array with two dimension (RLE) contains value column and Occurrence column.

Step١: Select a Threshold to Compress the Result array values from RLE Compression from the Last Algorithm to get more Compression for sound Coefficients.

Step٢: If the deference between previous and next value less than

## ٣. ٤ إخفاء معاملات الصوت داخل الصورة

وتتضمن **قراءة ملف الصورة ، اختبار التوافق بين معاملات الصوت والصورة ، استخدام طريقة القطاعات المتشابهة (Similar Blocks)للإخفاء .**

### ٣. ٤. ١ قراءة ملف الصورة (Image File Reading)

تعتمد عملية قراءة ملف الصورة على هيأة ملف الصورة المستعمل ، حيث تتوافر العديد من الهيئات المستعملة لتمثيل الصور ، ولقد وقع الاختيار على هيأة BMP (Bitmap Format) الذي يعد من اشهر الأنواع وأهمها ويرجع السبب في ذلك إلى سهولة التعامل مع هذه الملفات زيادة على إنها تمتاز بإمكانية تخزين الرسوم أو الصور من أي نظام عرض وبإمكانية عرض الرسوم أو الصور من أي نظام عرض(١٩٩٧) [٧٠].

يتألف ملف BMP من الترويسة(header) ومنطقة جدول الألوان الاختياري ، ومنطقة بيانات النقاط (pixel) . الفائدة الرئيسة تقع في نمط الصور الملونة نوع RGB غير المضغوطة ذات (٢٤ bit) لكل

نقطة ، بايت ازرق ، بايت اخضر و بايت احمر حسب الترتيب. العمل من اليسار إلى اليمين متجها إلى الأمام سطر تلو الآخر . نقاط البيانات تبدأ عند الموقع المنطقي وتستمر إلى نهاية ملف BMP (٢٠٠٤)[٦٤].

الصورة المنظمة(mapped image) أو صورة لوحة الألوان(palette image) تخزن الألوان بصورة غير مباشرة . صور لوحة الألوان(palette image) تكون فيها الألوان محصورة على شكل مجموعة مرقمة من الألوان ، تسمى 'palette' . كل لون في اللوحة 'palette' يعرف بثلاثة أرقام تعطي الشدة أو الكثافة اللونية الابتدائية . لون النقطة على الشاشة (pixel) تعرف بتعيين رقم اللون بالـ 'palette' . فوائد هذه الطريقة هي تقليل نسبة الذاكرة اللازمة لخزن الصورة (٢٠٠٣)[٦٥].

يعتمد حجم لوحة الألوان على عدد الثنائيات لكل عنصر (Bit Per Pixel) فإذا كان عدد الثنائيات يساوي ثمانيّة واحدة فإن حجم لوحة الألوان يكون (٠-٢٥٥) وكل عنصر في الصورة يمثل فهرس يشير إلى أحد مداخل لوحة الألوان ، ويمثل الجزء الأخير بيانات الصورة (٢٠٠٠)[٦٦].

وبسبب الخصائص التي تملكها ملفات ذات هيأة BMP فقد تم اختيار صور من الإنترنت ذوات الهيأة JPEG والتي تملك خصائص معينة وتحويلها إلى هيأة BMP وتغيير خصائصها إلى خصائص جديدة باستخدام برمجيات **(CorelDraw ١٠)** و**(PhotoShop Suite)** و**(Ulead Photo Express)** بحيث اصبح حجم الصورة يساوي ١٢٨×١٢٨ وطول النقطة(pixel) يساوي ثمانية واحدة .

علما إن زيادة حجم الصورة يعقد من عملية الإخفاء والاسترجاع إذ كلما زاد حجم الصورة كلما زاد الوقت المستغرق في إخفاء بيانات الصوت واسترجاعها لذا تم اختيار الصورة بحجم ١٢٨×١٢٨ ليتناسب مع عمليات الحساب والبحث لتقنية إخفاء بيانات الصوت بالصورة.

## ٣. ٤. ٢ اختبار التوافق بين معاملات الصوت والصورة

بعد أن قرئت بيانات الصورة لابد من اختبار كون هذه الصورة هي الغطاء المناسب لمعاملات الصوت المضغوط ، ولاختبار مدى التوافق بين معاملات الصوت والصورة يجب عمل مدرج تكراري (Histogram) لكل منهما بحيث نحسب تكرار كل عنصر من عناصر الصورة على حدة وتكرار كل عنصر من عناصر الصوت على حدة أخرى.

## ٣. ٤. ٣ استخدام طريقة القطاعات المتشابهة(Similar Blocks)

لقد ذكرنا سابقا في مرحلة ضغط معاملات الصوت باستخدام (RLE) إن مخرجات هذه المرحلة هي مصفوفة تتكون من عمودين الأول يمثل عمود القيمة والعمود المقابل هو عمود التكرار لكل قيمة ، يتميز عمود القيمة بأن اغلب قيمه كبيرة أما عمود التكرار فيحتوي على قيم اغلبها صغيرة نسبيا وبسبب تجانس

قيم عمود القيمة وتجانس عمود التكرار كل على حدة بصورة نسبية لذا يجب الفصل بينها وذلك بتحويل المصفوفة ذات البعدين إلى مصفوفة ذات بعد واحد متكونة من جزأين الجزء الأول يمثل أرقام القيمة والجزء الثاني أرقام التكرار وذلك لنزيد من كفاءة نتائج الإخفاء بالقطاعات المتشابهة .

والخوارزمية (٤.٣) تبين عملية تجانس قيم بيانات الصوت.

**Sound Coefficients Values Homogeneity Algorithm**

Input: Array of (RLE) with value column and the facing occurrence Column to each value.

Output: array with one dimension(speech).

Step١: Put all values column of array(RLE)in the first part of array (speech) .

Step٢: Put all occurrence column of array(RLE)in the second part of array (speech) by:

k ← ١

تُقسَيم بيانات الصورة إلى قطع متساوية تماما (Blocks) اما (٨x٨) أو (١٦x١٦) ، وبما إن الصور ذات حجم (١٢٨x١٢٨) كما مر ذكره في مرحلة قراءة ملف الصورة وذلك لأن زيادة حجم الصورة سيعقد عملية إخفاء قطع بيانات الصوت (Blocks) في تلك الصورة من الناحية الحسابية ومن ناحية الوقت اللازم في إيجاد القطعة المناسبة من بيانات الصورة لإخفاء قطعة بيانات الصوت فيها.

تقسم معاملات الصوت إلى قطع متساوية (Block) بنفس حجم قطع بيانات الصورة غير إن القطعة الأخيرة لمعاملات الصوت تحتوي فضلى قيم معاملات الصوت وتعالج هذه الفضلى قبل عملية الإخفاء وسنأتي على ذكرها تفصيليا .

نأخذ أول قطعة من معاملات الصوت بحجم حدد سابقا فإذا كان (٨x٨) (أي أول ٦٤ قيمة من مصفوفة RLE ) وتخزن على شكل مصفوفة ذات بعدين ((block١(i,j)) ونأخذ أول قطعة من بيانات الصورة وبنفس الحجم (٨x٨) وتخزن أيضا على شكل مصفوفة ذات بعدين ((block٢(i,j)) ثم نحسب مجموع الفرق المطلق بين كل نقطة من مصفوفة الصوت ((block١(i,j)) مع النقطة المقابلة لها من مصفوفة الصورة ((block٢(i,j)) وصولا لآخر نقطة للمصفوفتين كما مبين :

$$s = \frac{\sum_{i=1}^{N} |xi - yi|}{N} \quad \text{.....(1.3)}$$

N: تمثل حجم قطعة البيانات.

xi: تمثل معاملات الصوت.

yi: تمثل بيانات الصورة.

s : تمثل معدل مجموع الفرق المطلق.

نقسم مجموع الفروقات المطلقة على حجم المصفوفة (٨x٨) لنحصل على المعدل فإذا كان المعدل يساوي صفراً نخزن رقم قطعة (Block) بيانات الصورة على اعتبار كونها أنسب قطعة لإحلال (إخفاء) معاملات الصوت فيها ، لأنها تمثل القطعة المطابقة تماما لمعاملات الصوت ، وإلا نختبر المعدل مع متغير (Minblock) ويحتوي هذا المتغير على قيمة ابتدائية وتساوي ( ٢٥٥) وهي اكبر قيمة يمكن إن نحصل عليها إن وجدت تمثل معدل مجموع الفرق المطلق بين مصفوفة الصوت ((block١(i,j)) ومصفوفة الصورة ((block٢(i,j)) فإذا كانت النتيجة اقل من المتغير (Minblock) ، سيتم إحلال النتيجة بالمتغير (Minblock) إذ كلما قل الفرق بين معاملات الصوت والصورة كلما زادت كفاءة الإخفاء وقل تحسس العين بوجود تشوهات في الصورة لذا يخزن رقم قطعة بيانات الصورة وبعدها يتم القفز إلى قطعة (Block) بيانات الصورة اللاحقة وتجرى العملية نفسها من جديد.

وعند انتهاء مقارنة قطعة معاملات الصوت مع جميع قطع بيانات الصورة نحصل في النهاية على رقم يمثل أنسب قطعة بيانات صورة واكثر شبها بقطعة معاملات الصوت أو المطابقة لها إن وجدت بصورة نادرة ، علما إن رقم هذه القطعة سوف يستثنى من المقارنة في العمليات اللاحقة لتجنب ضياع المعاملات .

بعدها يتم البحث في الصورة عن موقع بداية تلك القطعة بالاستفادة من رقم قطعة بيانات الصورة ليتم إحلال قيم مصفوفة معاملات الصوت التي سبق وإن تم خزنها ((block١(i,j)) في تلك القطعة ابتداء من موقع البداية .

تكرر هذه العملية على جميع قطع معاملات الصوت وعند الوصول إلى القطعة الأخيرة التي تمت معالجتها وذلك بتقسيم معاملات الصوت إلى قطع فإذا كان حجم القطعة الواحدة يساوي (٨x٨) والجزء الباقي (الفضلى) من المعاملات يكون حجمه اصغر من القطعة الواحدة ، لذا يجب أن نضيف إليه (أصفار) حتى يصل حجمه إلى حجم يساوي حجم القطعة الواحدة (٨x٨) وبذلك نحصل على تقسيم منتظم .

وأضيفت (أصفار) للقطعة الأخيرة من معاملات الصوت وهذا لا يؤثر على معاملات الصوت لأن وجود الصفر يمثل حالة قليلة التكرار. وهذا يفيدنا في عملية الاسترجاع إذ إن معاملات الصوت سيتم استرجاعها باستثناء الأصفار التي أضيفت في هذه المرحلة .

وفي نهاية هذه المرحلة سنحصل على صورة جديدة حاملة للصوت وسلسلة من الأرقام تمثل أرقام قطع بيانات الصورة التي تم فيها إحلال (إخفاء) معاملات الصوت وهذه السلسلة تمثل سلسلة المفتاح الذي من خلاله سيتم الاسترجاع ، تخزن الصورة الناتجة الحاملة للصوت على شكل ملف بهيأة (BMP) وسلسلة المفتاح على ملف آخر منفصل وترسل للمستلم لاحقا عبر الإنترنت بالبريد الإلكتروني .

والخوارزمية (٥.٣) تبين عملية أيجاد التطابق للإخفاء بالقطاعات المتشابهة.

Matching Algorithm

Input: The embedded Sound Coefficients and Cover Image Consist of

Step١: Compare between block of embedded sound with blocks of cover Image by:

For i←١ to embeded block No do

Get Subblock[i]

For j←١ to Cover block No do

If Length(Index Matrix)>٠

For k ←١ to Length(Index Matrix)

If block number[j]==Index Matrix[k]

## ٣. ٥ مرحلة الاسترجاع

تتكون هذه المرحلة الرئيسة من ثلاث مراحل فرعية : **استخراج معاملات الصوت من الصورة وفك الضغط ومعكوس تحويل معاملات الصوت واستخدام معكوس تحويل المويجة المتقطع(IDWT) .**

### ٣. ٥. ١ استخراج معاملات الصوت من الصورة

نقسم الصورة الحاملة لمعاملات الصوت إلى قطع (Blocks) بنفس تقسيم الصورة الأصلية ونعمل عداداً تقارن قيمة هذا العداد مع أول قيمة من قيم مصفوفة سلسلة المفتاح والتي تمثل رقم أول قطعة لقيم بيانات الصورة الحاملة لمعاملات الصوت ، فإذا تحقق شرط المساواة سيتم إحلال قيم معاملات الصوت المخفية في تلك القطعة في مصفوفة ذات بعد واحد وهي تشابه مصفوفة (RLE) بعدما حولت إلى مصفوفة ذات بعد واحد في مرحلة استخدام القطاعات المتشابهة ، وإنْ إذا لم يتحقق شرط التساوي نقفز إلى القطعة اللاحقة من بيانات الصورة لإجراء نفس الاختبار وصولا إلى القطعة الحاملة للصوت (أي شرط المساواة)، تكرر هذه العملية لحين انتهاء سلسلة المفتاح.

مخرجات هذه المرحلة هي مصفوفة ذات بعد واحد تحتوي على معاملات الصوت ولابد من الإشارة إلى أنَ وجود مجموعة من الأصفار في نهاية هذه المصفوفة قد جاء من القطعة الأخيرة لمعاملات الصوت التي عولجت بتلك الأصفار كما أشرنا سابقا .

والخوارزمية (٦.٣) تبين عملية استخراج معاملات الصوت من الصورة الحاملة.

**Extracting Algorithm**

Input: File of Stgo_Image , File of Key Sequence .

Output: array of Sound Coefficients with one Dimension (INV_RLC)

Step١: Open Key Sequence File and Stgo_Image File.

Step٢: Put Key Sequence File in Array with one Dimension to present Facilitation in use .

Step٣: Compare between Key Sequence with blocks of Stego_Image.

For i ⟵ ١ to Length(Key) do

## ٣. ٥. ٢ معكوس تحويل معاملات الصوت

تُنسَخ قيم المصفوفة إلى أخرى جديدة باستثناء القيم الصفرية لنحصل على الحجم الأصلي للمصفوفة دون الأصفار ، بعدها يتم إرجاع عمود القيم وعمود التكرار المقابل لكل قيمة وذلك بقسمة الطول الكلي للمصفوفة على اثنين بحيث يصبح النصف الأول من المصفوفة يمثل عمود القيمة و النصف الثاني يمثل عمود التكرار .

ثم يُفَك الضغط وذلك بتكرار كل عنصر من عمود القيمة بقدر عدد مرات التكرار المقابل لتلك القيمة لنحصل في النهاية على قيم جديدة لمعاملات الصوت لا تشبه القيم الأصلية لأنها تعرضت إلى الضغط بفقدان (Lossy Compression) . ولتحويل قيم معاملات الصوت إلى المدى الأصلي نضرب قيم المعاملات الموجبة بمعامل ويساوي (max/٢٥٥) لترجع قيم المعاملات ضمن مداها الأصلي ، ثم تطرح القيمة المطلقة للقيمة الصغرى(Minimum Value) والتي رمزها (min) لجميع معاملات الصوت لإرجاع الإشارة السالبة للقيم كما كانت قبل التحويل ، علما إن القيمة العظمى (Maximum value) والقيمة الصغرى(Minimum Value) (min , max) على الترتيب يرسلان مع المفتاح .

والخوارزمية (٧.٣) تبين معكوس تحويل معاملات الصوت.

| **INVERSE of Sound Coefficients Transformation Algorithm**<br>Input: Array of Sound Coefficients with one Dimension (INV_RLC).<br>Output: Array with one Dimension (na٣) of Sound Coefficients |
|---|
| after decompress.<br><br>Step١: Extract Sound Coefficients excepting Zero values from the last block to get the Original values.<br>For i◄—— ١ to Length(INV_RLE) do<br>Begin |

Step٣: Decompress An Array IRLE .

S ◄—— ١

IRLC ◄—— IRLE

While (i<Length(INVERSE_RLC/٢) do

Begin

j◄—— ١

While (j<=RLC[i,٢]) do

Begin

IRLE [s,١]=IRLC[i,٢]

s ◄—— s+١

j ◄—— j+١

End

i ◄—— i+١

End

Step٤: Multiply the positive Coefficients values with factor (Max/٢٥٥) to make values in its original range

من الملاحظ إن القيم الناتجة لمعاملات الصوت بعد الاسترجاع تختلف عن القيم الأصلية قبل عملية الإخفاء لأنها عانت الكثير من الفقدان في مرحلة تحويل المويجة المتقطعة والضغط بتشفير طول السلسلة والضغط بالعتبة .

## ٣. ٥. ٣ استخدام معكوس تحويل المويجة المتقطعIDWT

بعد استخلاص معاملات الصوت وفك الضغط من الخطوة السابقة والتي تساوي القيم التقريبية لمعاملات الصوت للمستوي الثالث(cA٣) لأنها عانت الضغط بفقدان . أُعيد إنشاء (Reconstruct) معاملات المستوي الثاني (cA٢) بإضافة سيل من الأصفار بقدر عدد معاملات(cA٣) بدلا من قيم تفاصيل المستوي الثالث(cD٣) الأصلية ، ولإعادة إنشاء (Reconstruct) معاملات تقريبات المستوي الاول (cA١) يضاف سيل من الأصفار بقدر عدد معاملات المستوي الثاني (cA٢) بدلا عن قيم تفاصيل المستوي الثاني (cD٢) الأصلية و بالطريقة نفسها يعاد إنشاء بيانات الصوت حيث تضاف أصفار بقدر معاملات المستوي الأول(cA١) بدلا من قيم تفاصيل المستوي الأول (cD١) الأصلية لنحصل في النهاية على بيانات الصوت ، غير أَنَ البيانات الجديدة قد تعرضت للكثير من الفقدان لذا فهي تختلف عن بيانات الصوت الأصلية ويمكن تمييز ذلك بشكل واضح من خلال السمع.

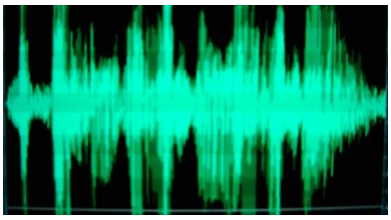
لذا تعالج الإشارة الناتجة بإزالة الضوضاء منها باستخدام برنامج (Cool Edit Pro Version ٢.٠) لتحسين الصوت الناتج. والشكل (١٢.٢) يبين إعادة إنشاء الإشارة لعدة مستويات

## ١.٤ نتائج النظام المقترح:

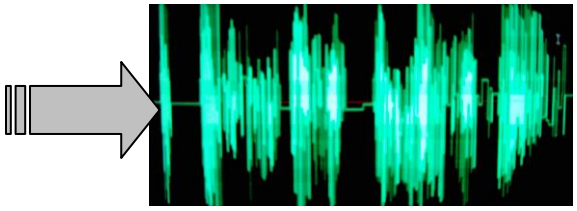
تبين التجارب اللاحقة مجموعة من الأصوات المخفية وصور الغطاء ، والصور الحاملة الناتجة من عملية الإخفاء ، والصوت المسترجع الناتج من عملية استخراجه من الصورة المخفية الحاملة والذي يختبر في النظام المقترح .

**تجربة ١ :**

في **المرحلة الأولى** ضُغِطَ ملف الصوت الأصلي الذي يساوي (٢٣٦٠١) عينة وهذا الحجم كبير بالنسبة لحجم الصورة الغطاء (١٢٨x١٢٨) بحوالي مرة ونصف وبعد تطبيق تحويل المويجة المتقطع(DWT) للمستوي الثالث أصبح ملف الصوت يساوي (٢٩٥١) عينة وبعد تطبيق تشفير طول السلسلة أصبح حجم ملف الصوت يساوي (١٩١٠) عينة بحيث إن نسبة الضغط أكبر من ١٢ وتساوي ١٢.٣٥٦ .



ملف الصوت الأصلي



ملف الصوت بعد الضغط

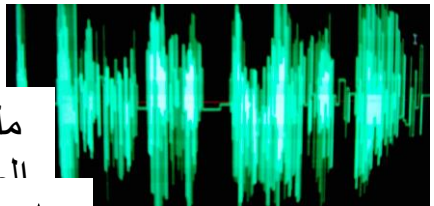
في **المرحلة الثانية** أُختيرت الصورة الغطاء لإجراء الإخفاء ، حجم القطعة

يساوي(١٦x١٦)

**تجربة ٢ :**

في **المرحلة الأولى** أُتبعَت الخطوات السابقة نفسها في تجربة ١ وأعطت نفس نتائج الضغط لنفس ملف الصوت.

في **المرحلة الثانية** أُختيرت الصورة الغطاء لإجراء الإخفاء ،حجم القطعة

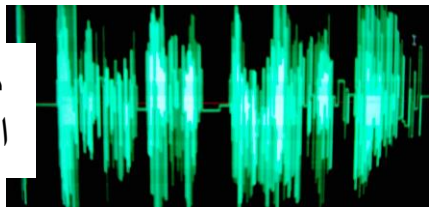


ملف

**الصورة الحاملة**

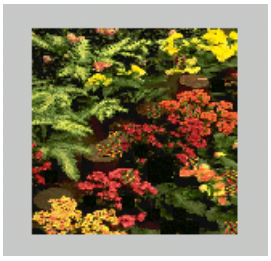
يساوي(٨x٨)

الصورة الحاملة

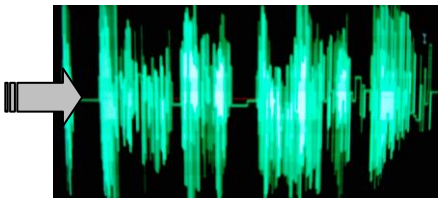


ملف الصو

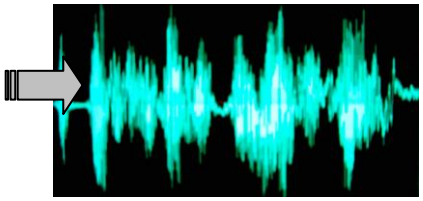
في **المرحلة الثالثة** استُرجِع الصوت من الصورة الحاملة وأُزيلَت الضوضاء منه باستخدام(CPE) .



الصورة الحاملة



الصوت بعد الاسترجـ



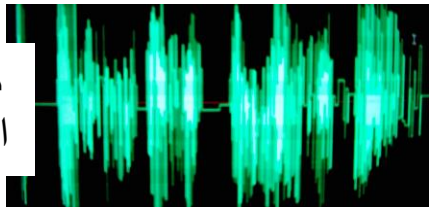
الصوت بعد إزالة الضوضاء

**<u>تجربة ٣ :</u>**

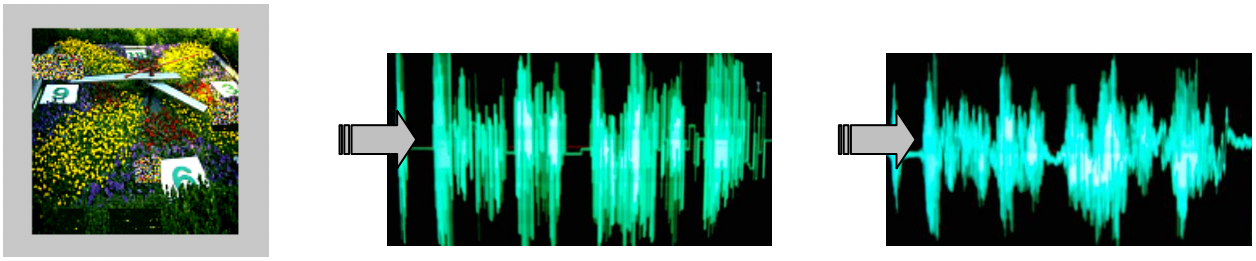
في **المرحلة الأولى** اتُبِعَت الخطوات السابقة نفسها في تجربة(١,٢) وأعطت نفس نتائج الضغط لنفس ملف الصوت.

في **المرحلة الثانية** أُختيرَت الصورة الغطاء لإجراء الإخفاء ،حجم القطعة يساوي(١٦X١٦)


الصورة الحاملة




في **المرحلة الثالثة** استُرجِع الصوت من الصورة الحاملة وأُزيلَت الضوضاء منه باستخدام(CPE) .



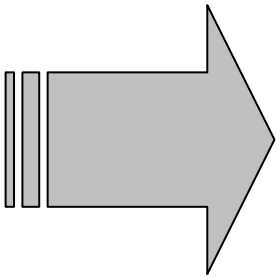
الصوت بعد إزالة الضوضاء الصوت بعد الاستر الصورة الحاملة

**<u>تجربة ٤ :</u>**

في **المرحلة الأولى** اتُبِعَت الخطوات السابقة نفسها في تجربة(١,٢,٣) وأعطت نفس نتائج الضغط لنفس ملف الصوت.

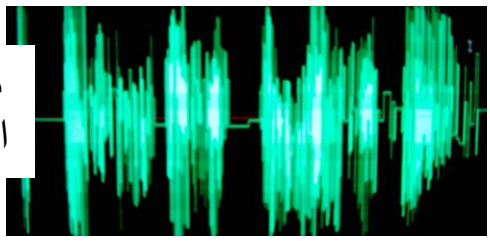
في **المرحلة الثانية** أُختيرَت الصورة الغطاء لإجراء الإخفاء ،حجم القطعة يساوي(٨x٨)

الصو

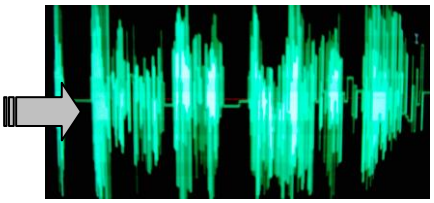


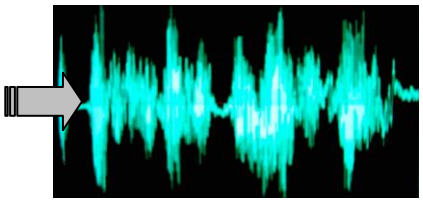
**الصورة الحاملة**

ملف الصو



في **المرحلة الثالثة** استُرجِع الصوت من الصورة الحاملة وأُزيلَت الضوضاء منه باستخدام(CPE) .



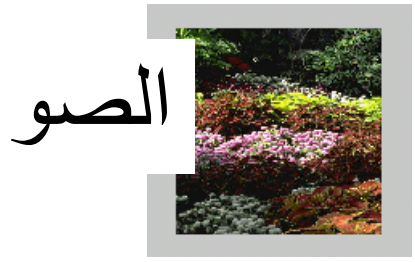


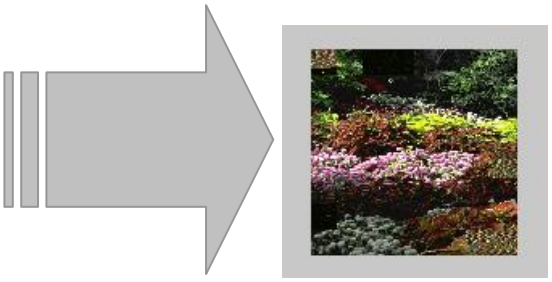
الصوت بعد إزالة الضوضاء الصوت بعد الاسترج الصورة الحاملة

**<u>تجربة ٥ :</u>**

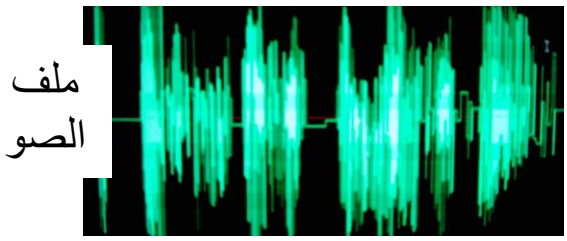
في **المرحلة الأولى** اتُبِعَت الخطوات السابقة نفسها في تجربة(١,٢,٣,٤) وأعطت نفس نتائج الضغط لنفس ملف الصوت.

في **المرحلة الثانية** أُختيرَت الصورة الغطاء لإجراء الإخفاء ،حجم القطعة يساوي(١٦x١٦)

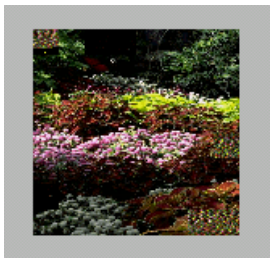


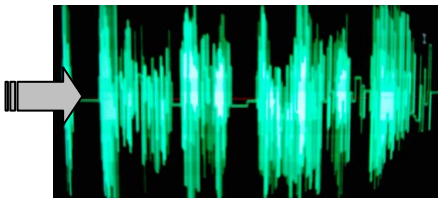



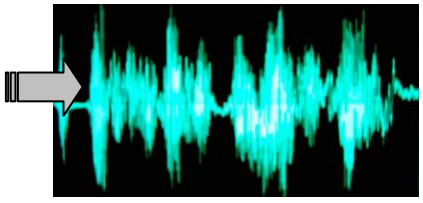
الصورة الحاملة




في **المرحلة الثالثة** استُرجِع الصوت من الصورة الحاملة وأُزيلَت الضوضاء منه باستخدام(CPE) .







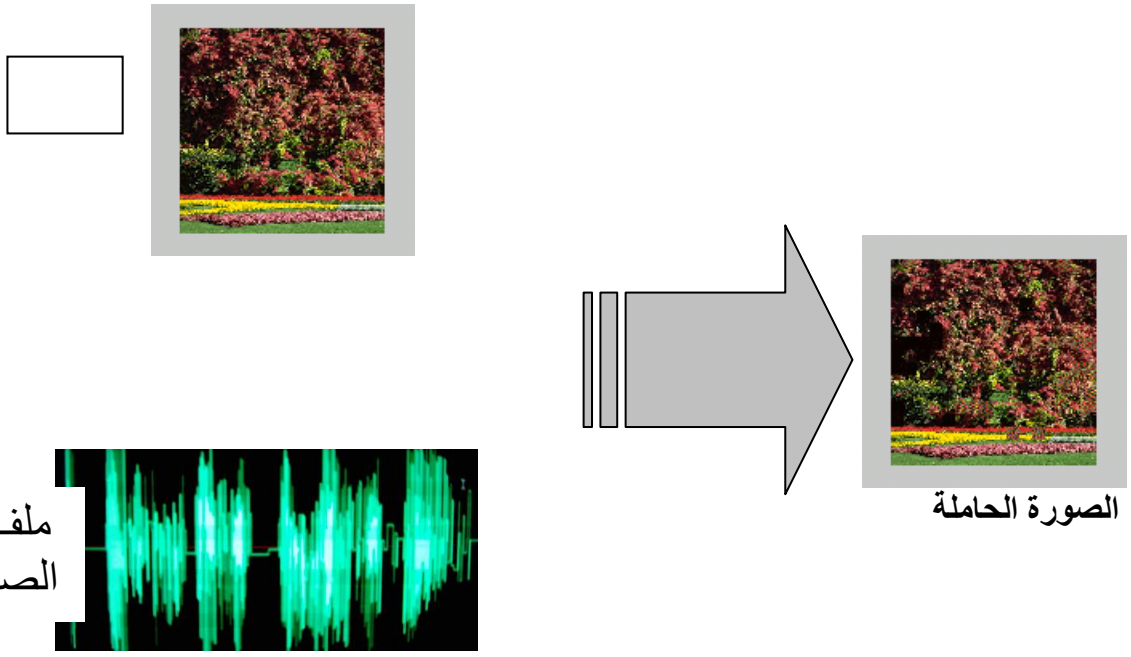
الصوت بعد إزالة الضوضاء الصوت بعد الاسترجِ الصورة الحاملة

**<u>تجربة ٦ :</u>**

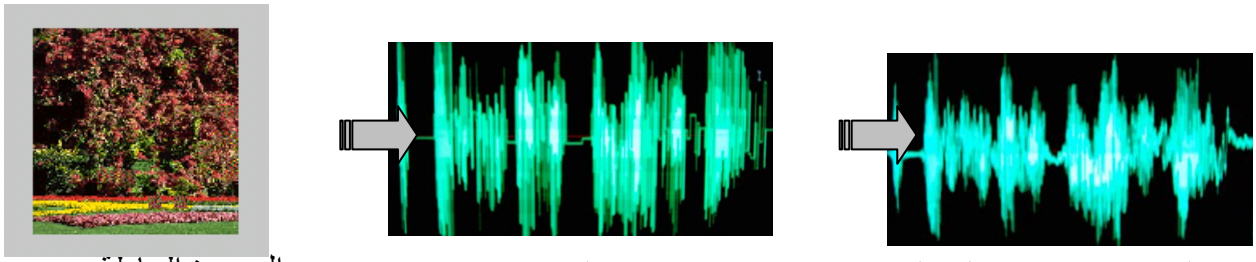
في **المرحلة الأولى** اتُبِعَت الخطوات نفسها في التجارب الخمس السابقة وأعطت نفس نتائج الضغط لنفس ملف الصوت.

في **المرحلة الثانية** أُختيرَت الصورة الغطاء لإجراء الإخفاء ،حجم القطعة يساوي(٨x٨)

الصو




في **المرحلة الثالثة** استُرجِع الصوت من الصورة الحاملة وأُزيلَت الضوضاء منه باستخدام(CPE) .

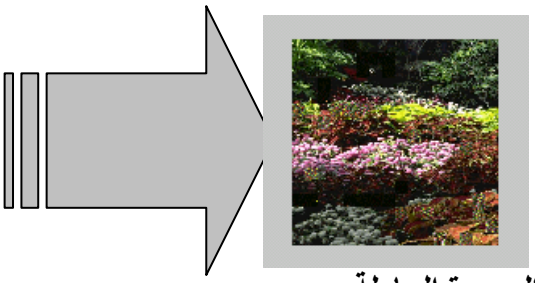



**تجربة ٧ :**

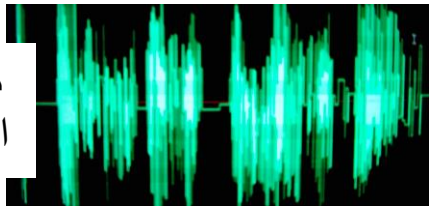
في **المرحلة الأولى** اتُبِعَت الخطوات نفسها في التجارب الست السابقة وأعطت نفس نتائج الضغط لنفس ملف الصوت.

في **المرحلة الثانية** أُختيرَت الصورة الغطاء لإجراء الإخفاء ،حجم القطعة يساوي(٨x٨)

الصو

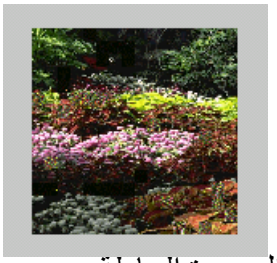


الصورة الحاملة

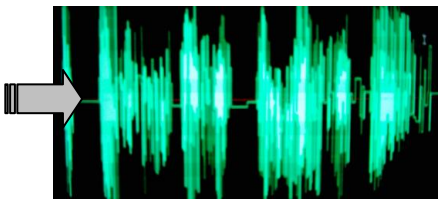


ملف الصو

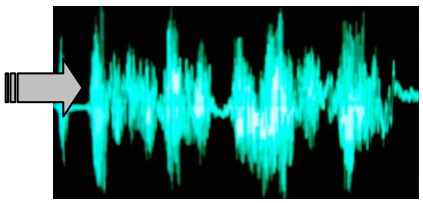
في **المرحلة الثالثة** استُرجِع الصوت من الصورة الحاملة وأُزيلَت الضوضاء منه باستخدام(CPE) .



الصورة الحاملة



الصوت بعد الاسترج



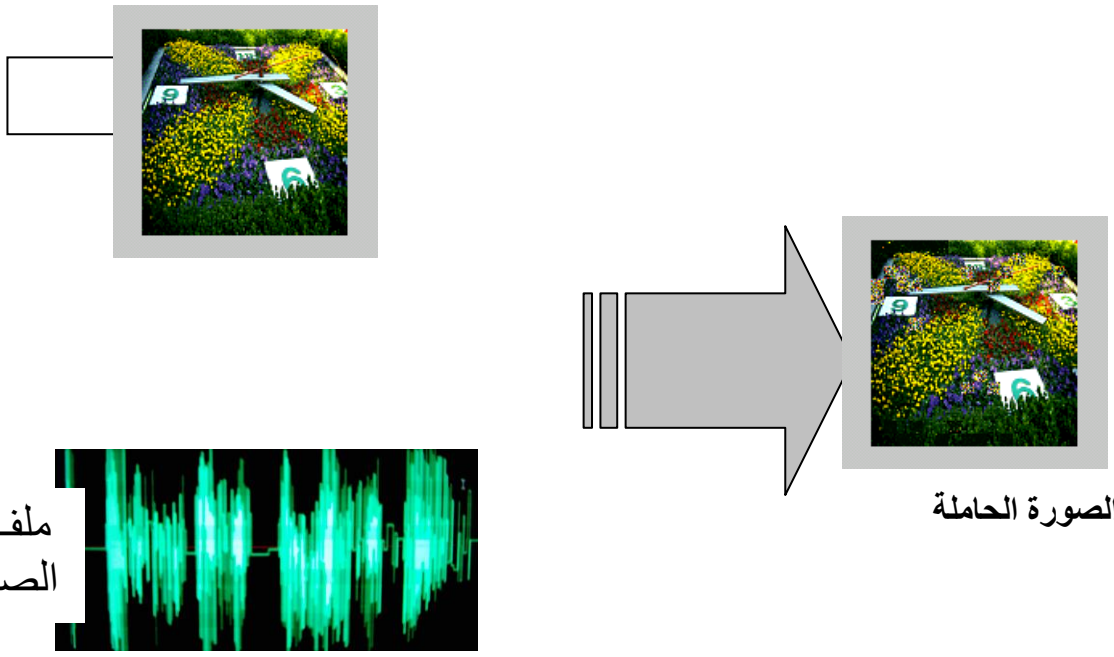
الصوت بعد إزالة الضوضاء

**<u>تجربة ٨ :</u>**

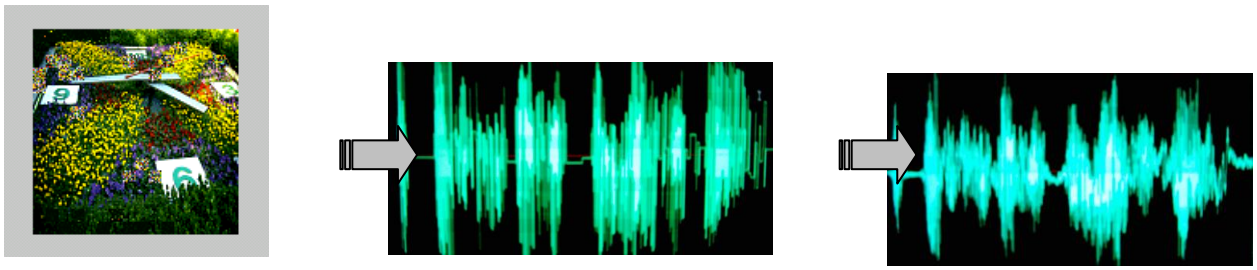
في **المرحلة الأولى** اتُبِعَت الخطوات نفسها في التجارب السبع السابقة وأعطت نفس نتائج الضغط لنفس ملف الصوت.

في **المرحلة الثانية** أُختيرَت الصورة الغطاء لإجراء الإخفاء ،حجم القطعة يساوي(٨x٨)

الصو




في **المرحلة الثالثة** استُرجِع الصوت من الصورة الحاملة وأُزيلَت الضوضاء منه باستخدام(CPE) .




## ٥. ١ الاستنتاجات:

١-تزداد كفاءة التحليل إلى مستويات أعلى باستخدام تحويل المويجة المتقطع كلما زادت نقاوة الصوت ووضوحه بحيث يمكن الوصول إلى المستوي الرابع أو اكثر ومن ثمَ زيادة كفاءة نتائج تحويل المويجة المتقطع من حيث ضغط البيانات إلى معاملات اقل.

٢- كلما ازدادت قيمة التردد المسجل به الصوت كلما ازدادت إمكانية التحليل إلى مستويات أعلى هذا من جهة ، ومن جهة أخرى ازداد عدد بيانات الصوت حيث

إن العلاقة بين التردد وعدد المستويات يتناسب تناسبا طرديا ، والعلاقة بين التردد وبيانات الصوت يتناسب تناسبا طرديا أيضا .

٣- في مرحلة تحويل معاملات الصوت من القيم الحقيقية إلى قيم صحيحة كانت القيم الناتجة مقاربة إلى بيانات الصورة نسبيا ، حيث إن المعاملات المتجاورة متطابقة أو متقاربة من حيث المقدار أو القيمة حسب مقياس تطابق القطاعات.

٤- إن بيانات الصوت الناتج عن معكوس تحويل المويجة المتقطع تكون اكثر عددا من بيانات الصوت الأصلي كما في تجربة ١ ، وذلك لان عملية تحويل المويجة المتقطع(DWT) تعالج البيانات التي عدد عيناتها فرديا بإضافة(٠) ولثلاثة مستويات لذا فإن الاسترجاع أدى إلى زيادة بيانات الصوت لتصل إلى(٢٣٦٠٨) عينة بدلا عن بيانات الصوت الأصلي والتي تساوي(٢٣٦٠١) عينة.

٥- في مرحلة ضغط معاملات الصوت بطريقة تشفير طول السلسلة(RLE) أنتج الضغط سلاسل قصيرة بسبب وجود تشابه قليل في القيم بحيث ضاعف أو زاد من عدد معاملات الصوت لذا فقد تلت طريقة ضغط معاملات الصوت بطريقة تشفير طول السلسلة(RLE) استخدام الضغط بالعتبة(Threshold).

٦- إن معاملات الصوت الناتجة عن استخراج القيم من الصورة تساوي نفس عدد معاملات الصوت قبل الإخفاء كما في تجربة ١ ، حيث تم استثناء القيم الصفرية لذا فإن الاسترجاع أدى إلى إعادة بيانات الصوت .

٧- تزداد كفاءة الإخفاء بالقطاعات المتشابهة كلما قل حجم القطعة التي يتم فيها الإخفاء حسب مقياس قمة نسبة الإشارة إلى الضوضاء(PSNR) حيث يقل تحسس العين للتشوهات الموجودة على الغطاء ولكن على حساب طول سلسلة المفتاح إذ كلما قل حجم القطعة كلما زاد طول سلسلة المفتاح وهذه حالة غير مقبولة ، لذا يجب أن تكون هناك موازنة بين حجم القطعة بحيث لا تظهر فيها التشوهات وطول سلسلة المفتاح .

٨- كلما ازداد تعقيد الصورة الغطاء وتقاربت بياناتها من معاملات الصوت المراد إخفاءه فيها كلما اصبح بالإمكان زيادة حجم القطعة اللازمة للإخفاء ومن ثمَ قصر طول سلسلة المفتاح الناتجة.

٩- من خلال التجارب السابقة لوحظ إن قيمة نسبة قمة الإشارة إلى الضوضاء بين صورتي الغطاء والصورة الناتجة(الحاملة) تتراوح بين(٣٤.٢٢٣ - ٣٦.٢٢٣) وتعد هذه النتائج جيدة جدا بالمقارنة مع أغلب نتائج البحوث السابقة التي تم التوصل إليها عند إخفاء صورة ملونة داخل صورة ملونة أخرى بـ(٢٥٦) تدرج لوني وباستخدام تقنية القطاعات المتشابهة(٢٠٠٣,٢٠٠٥)[٦٧,٣١]. علما إن طبيعة معاملات الصوت تختلف عن بيانات الصورة ويصعب إيجاد التوافق بين معاملات الصوت وبيانات الصورة ولا سيما بعد الضغط بتشفير طول السلسلة والضغط بالعتبة.

١٠- إن قيمة نسبة قمة الإشارة إلى الضوضاء بين الصوت الأصلي والصوت الناتج عن استخراجه من الصورة تساوي (٢٩.٩٠٧) و الجذر التربيعي لمعدل مربع الخطأ يساوي (٦٦.٤٢٦) .

٥. ٢ الأعمال المستقبلية:
من الممكن تطوير العمل من خلال الأوجه آلاتية:-

١- استخدام اكثر من جملة (كلام).

٢- إخفاء كلام عبر الهاتف يحتوي على نسبة عالية من الضوضاء.

٣- تهجين تقنيات تمييز المتكلم واثبات المتكلم مع تقنيات الإخفاء.

## ٤. ٢ أداء النظام المقترح:

**لمعرفة أداء النظام المقترح ، أُعتُمِدَت مجموعة من الصور المختلفة الخصائص وبحجم ١٢٨×١٢٨ كأمثلة تجريبية لبيان كفاءة النظام وفقاً للمقاييس آلاتية :**

١- حساب نسبة قمة الإشارة إلى الضوضاء (PSNR) بين صورة الغطاء والصورة الحاملة.

٢- حساب نسبة الإشارة إلى الضوضاء (SNR) بين صورة الغطاء والصورة الحاملة.

٣- حساب الجذر التربيعي لمعدل مربع الخطأ (RMSE) بين صورة الغطاء والصورة الحاملة.

تجربة ١

في التجربة الأولى كانت نسبة قمة الإشارة إلى الضوضاء (PSNR) بين صورة الغطاء (Cover Image) والصورة الحاملة(Stego Image) تساوي(٣٤.٢٢٣) ، أما نسبة الإشارة إلى الضوضاء (SNR) تساوي (٥.٠٣٧٧) ، أما الجذر التربيعي لمعدل مربع الخطأ (RMSE) فيساوي (٢٤.٥٩) ، وكانت عدد عناصر سلسلة المفتاح تساوي(٨) عناصر علما إن كل عنصر يتكون من ثنائيتين كحد أعلى إذ كلما ازداد حجم القطعة الواحدة عند الإخفاء كلما قصر طول سلسلة المفتاح وتعتبر هذه النتيجة حالة إيجابية.

تجربة ٢

في التجربة الثانية كانت نسبة قمة الإشارة إلى الضوضاء (PSNR) بين صورة الغطاء (Cover Image) والصورة الحاملة(Stego Image) تساوي(٣٥.٩٤٤) ، أما نسبة الإشارة إلى الضوضاء(SNR) فكانت تساوي (٧.٣٦٦٤) ، والجذر التربيعي لمعدل مربع الخطأ (RMSE) يساوي (١٦.٥٤٥) ، وكان عدد عناصر سلسلة المفتاح تساوي(٣٠) عنصراً علما إن كل عنصر يتكون من ثلاث ثنائيات كحد أعلى إذ كلما قل حجم القطعة الواحدة عند الإخفاء كلما ازداد طول سلسلة المفتاح وتعتبر هذه النتيجة اقل من الأولى.

تجربة ٣

في التجربة الثالثة كانت نسبة قمة الإشارة إلى الضوضاء (PSNR) بين صورة الغطاء (Cover Image) والصورة الحاملة(Stego Image) تساوي(٣٤.٩٢٤) ، أما نسبة الإشارة إلى الضوضاء(SNR) فكانت تساوي (٤.٥٢٩) ، والجذر التربيعي لمعدل مربع الخطأ (RMSE) يساوي

(٢٠.٩٢٨)وكـان عـدد عناصـر سلسـلة المفتـاح تسـاوي(٨) عناصـر علمـا إن كـل عنصـر يتكـون مـن ثنائيتين كحد أعلى.

## تجربة ٤

في التجربة الرابعة كانت نسبة قمة الإشارة إلى الضوضاء (PSNR) بين صورة الغطاء (Cover Image) والصـورة الحاملـة(Stego Image) تسـاوي(٣٦.٢٢٢) ، أمـا نسـبة الإشـارة إلـى الضوضـاء(SNR) فكانـت تسـاوي (٨.٥٨٧٢ ) ، والجـذر التربيعـي لمعـدل مربـع الخطـأ (RMSE) يساوي (١٥.٥١٩ ) وكان عدد عناصر سلسلة المفتاح تساوي(٣٠) عنصراً علما إن كل عنصر يتكون من ثلاث ثنائيات كحد أعلى.

## تجربة ٥

في التجربة الخامسة كانت نسبة قمة الإشارة إلى الضوضاء (PSNR) بين صورة الغطاء (Cover Image) والصـورة الحاملـة(Stego Image) تسـاوي(٣٤.٥٠١) ، أمـا نسـبة الإشـارة إلـى الضوضاء(SNR) فكانت تساوي (٥.٠٩٦٣) ، والجذر التربيعي لمعدل مربع الخطأ (RMSE) يساوي (٢٣.٠٦٩)وكـان عـدد عناصـر سلسـلة المفتـاح تسـاوي(٨) عناصـر علمـا إن كـل عنصـر يتكـون مـن ثنائيتين كحد أعلى.

## تجربة ٦

في التجربة السادسة كانت نسبة قمة الإشارة إلى الضوضاء (PSNR) بين صورة الغطاء (Cover Image) والصـورة الحاملـة(Stego Image) تسـاوي(٣٥.٤٧٨) ، أمـا نسـبة الإشـارة إلـى الضوضـاء(SNR) فكانـت تسـاوي (٦.٥٨٩٤ ) ، والجـذر التربيعـي لمعـدل مربـع الخطـأ (RMSE) يساوي (١٨.٨١٧) وكان عدد عناصر سلسلة المفتاح تساوي(٣٠) عنصراً علما إن كل عنصر يتكون من ثلاث ثنائيات كحد أعلى.

## تجربة ٧

في التجربة السابعة كانت نسبة قمة الإشارة إلى الضوضاء (PSNR) بين صورة الغطاء (Cover Image) والصـورة الحاملـة(Stego Image) تسـاوي(٣٥.٨٣٩) ، أمـا نسـبة الإشـارة إلـى الضوضاء(SNR) فكانت تساوي (٦.٩٩٦٨) ،والجذر التربيعي لمعدل مربع الخطأ (RMSE) يساوي (١٦.٩٥) وكان عدد عناصر سلسلة المفتاح تساوي(٣٠) عنصراً علما إن كل عنصر يتكون من ثلاث ثنائيات كحد أعلى.

## تجربة ٨

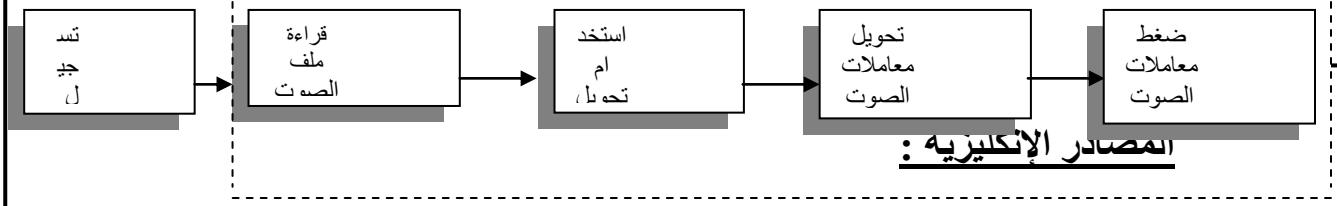
في التجربة الثامنة كانت نسبة قمة الإشارة إلـى الضوضـاء (PSNR) بـين صـورة الغطـاء (Cover Image) والصـورة الحاملـة(Stego Image) تسـاوي(٣٥.٧١٢) ، أمـا نسـبة الإشـارة إلـى الضوضاء(SNR) فكانت تساوي (٥.٣٩٥٤) ، والجذر التربيعي لمعدل مربع الخطأ (RMSE) يساوي (١٧.٤٥٤)وكـان عـدد عناصـر سلسـلة المفتـاح تسـاوي(٣٠) عنصـراً علمـا إن كـل عنصـر يتكـون مـن ثلاث ثنائيات كحد أعلى.

والجدول (٤-١) يبين نتائج ثلاث اختبارات بين الصورة الغطاء والصورة الحاملة

| رقم التجربة | PSNR بين صورة الغطاء والصورة الحاملة | SNR بين صورة الغطاء والصورة الحاملة | RMS بين صورة الغطاء والصورة الحاملة | عدد عناصر الحد الأعلى سلسلة المفتاح | لطول المفتاح |
|---|---|---|---|---|---|
| ١ | ٣٤.٢٢٣ | ٥.٠٣٧٧ | ٢٤.٥٩ | ٨ عناصر | ثنائيتان |
| ٢ | ٣٥.٩٤٤ | ٧.٣٦٦٤ | ١٦.٥٤٥ | ٣٠ عنصر | ٣ ثنائيات |
| ٣ | ٣٤.٩٢٤ | ٤.٥٢٩ | ٢٠.٩٢٨ | ٨ عناصر | ثنائيتان |
| ٤ | ٣٦.٢٢٢ | ٨.٥٨٧٢ | ١٥.٥١٩ | ٣٠ عنصر | ٣ ثنائيات |
| ٥ | ٣٤.٥٠١ | ٥.٠٩٦٣ | ٢٣.٠٦٩ | ٨ عناصر | ثنائيتان |
| ٦ | ٣٥.٤٧٨ | ٦.٥٨٩٤ | ١٨.٨١٧ | ٣٠ عنصر | ٣ ثنائيات |
| ٧ | ٣٥.٨٣٩ | ٦.٩٩٦٨ | ١٦.٩٥ | ٣٠ عنصر | ٣ ثنائيات |
| ٨ | ٣٥.٧١٢ | ٥.٣٩٥٤ | ١٧.٤٥٤ | ٣٠ عنصر | ٣ ثنائيات |

من خلال التجارب السابقة نلاحظ إن قيمة نسبة قمة الإشارة إلى الضوضاء بين صورتي الغطاء والصورة الناتجة(المراد تتراوح بين ٣٦.٢٢٣ ٣٦.٢٢٣١٠٠٠٠ ٣٦.٢٢٣) والجذر التربيعي لمعدل مربع الخطأ يتراوح بين(٩ **مرحلة الإخفاء** ارة إلى الضوضاء تتراوح بين (٥.٠٣٧٧ – ٨.٥٨٧٢) وكانت التجربه رقم (٤) الافضل من حيث قيمة قمة نسبة الإشارة إلى الضوضاء ، ويمكن مراجعة الملحق(١) الذي يحتوي على ملفات صوتية أخرى للإخفاء داخل صور غطاء وبنفس الأسلوب.

**قراءة وضغط الصوت**




**المصادر الإنكليزية :**


[١] O. Rahmouni, **Computer security**, Indiana State University, April ٢٣, ٢٠٠١.

**إخفاء الصوت داخل الصورة**

[٢] N. Provos, P. Honeyman**, Hide and Seek : An Introduction to Steganography**, University of Michigan ity, ٢٠٠٣

[٣] C **erview r the C sics Ex** garyke

[٤] CERIAS Tech Report ٢٠٠٤-١١ , **Linguistic Steganography** , Center For Education and Research in Information Assurance and Security, Department of linguistics purdue University west lafayette, In ٤٧٩٠٦, kbennett@cerias.purdue.edu.

[٥] K. Korhorn, **Steganography uses and Effects On Society,** http://www.cpsr.Org/essays/٢٠٠٢/٢rr٣.html. http://public.lunl.gov/mfisk/papers/iho٢.pdf.Dove

[٦] J.Kremer, **Steganography**, http://www.com **استرجاع الصوت من الصورة** ugust ١٣, ٢٠٠٤.

[٧] J. Neil and S. Jajodia, **Exploring Steg: Seeing the Unsee** /~nichmon/pub/ ٢٠٢٦.pdf. George Mas Apr. edu

[٨] .Westfeld Fede pfitz , **Steganography**, proc. ٢nd Workshop on Information Hiding , April **Modeling the Security of**





**مرحلة الاسترجاع**

الشكل (١.٣) يبين المخطط الكتلي التفصيلي للنظام المقترح

١٩٩٨, portland, LNCS ١٥٢٥, Springer-Verlag, ١٩٩٨, ٣٤٥-٣٥٥. [٩] J.,N.f and S.Jajodia, **Exploring Steganography Seeing the Unseen. Computer** , ٣١:٢٦-٣٤,١٩٩٨.

[١٠] petitcolas, A.P. Fabien, **Information Hiding-Asurvey.** Proceedings of the IEEE ٨٧:٧.١٠٦٢-١٠٧٨.١٩٩٩.

[١١] petitcolas, A.P. Fabien, **Introduction to Information hiding .In Information hiding: Techniques for Steganography and Digital Watermarking**., Stfan Katzenbeisser and Fabien A.P.Petitcolas (eds.).Bosten,:ArtechHouse. ١-١٤.٢٠٠٠.

[١٢] J. Kassim , **Hiding in plain Sight: Steganography in Today s Digital Environment,**software Engineering ٤c٠٣ Research project , March ٢٠٠٢.

[١٣] K. Rabah, **Steganography. The Art of Hiding Data** , Department of physics, Eastern Mediterranean University ,gazimagusa,North Cyprus, via Mersin ١٠, Turkey,Information Technology journal ٣(٣):٢٤٥-٢٦٩, ٢٠٠٤, ISSN ١٦٨٢-٦٠٢٧,©٢٠٠٤ Asian Network for Scientific Information.

[١٤] Bishop, John, Master of Trinity College, Cambridge. http://www.petitcolas.net/fabien/steganography/history.html , ١٩٩٧-٢٠٠٥ by a.p. Fabien, petitcolas.

[١٥] N. f. Johnson, **Steganography**. www: http:// www.jjtc.com/stegdoc/.George Mason University Berkowitz,Michael,"priacy on the net-steganography: .١٢. http://www.tomas.com/privacy/steganoen.htm .

[١٦] F.A.P. Petitcolas,R.J.Anderson,and M.G.Kuhn**, Information Hiding -A survey** ,proc. IEEE,vol.٨٧,no. ٧,١٩٩٩,pp.١٠٦٢-١٠٧٨.

[١٧] Wayner, Peter, **Disappearing Cryptography:Information Hiding: Steganography and Watermarking**, san Francisco: Morgan Kaufman.٢٠٠٢ (٢nd edition).

[١٨] Steganos GmbH**, Steganos Security Suit.٦,** http://www.steganos.com franKfurt am Main: ٢٠٠٤ .

[١٩] M.Arnold, M.Schmucker,& SD. Wolthusen, ,**Techniqus & Applications of Digital Watermarking & Content protection** , Norwood (AM):Artech House,٢٠٠٣.

[٢٠] M. Barni, C.I. Podikhuk., F. Bartolini, and, E.S. Delp**, Watermark Embedding: hiding a signal within a cover Image** . , IEEE Communications Mag., August٢٠٠١

[٢١] C. Hosmer and C.Hyde**, Discovering Covert Digital Evidence**, Digital Forensic Research Workshop (DFRWS) ٢٠٠٣, August ٢٠٠٣. URL.http//www.dfrws.org/dfrws ٢٠٠٣/presentations/paper-hosmer- digitalevidence.pdf.last accessed: ٢٠٠٤-٠١-٠٤.

[٢٢] A.Tumoas, **Practical invisibility In digital communication**, Information Hiding: First International workshop, proceedings, Vol. ١١٧٤ of Lecture Notes In Computer Science pringer, ١٩٩٦, pp.٣٩-٤٨.

[٢٣] D.Paul and S. Michael, Fractal Based Image Steganography, **Information Hiding: first** pringer, **International Workshop**, Proceedings, vol. ١١٧٤ of lecture Notes in Computer Science ١٩٩٦, pp.٢٧٩-٢٩٤.

[٢٤] S.Jashua and C. Barrett**, Modulation and Information Hiding In Images**, Information Hiding: First International Workshop, Proceedings, vol. ١١٧٤ of lecture notes in computer Science, pp.٢٠٧-٢٢٦, springer, ١٩٩٦.

[٢٥] W.Andreas & W.Gritta, **steganography In A Vidio Conferencing** Workshop,proceedings,vol. ١٥٢٥ of lecture notes In **System**, Information hiding:Second International computer Science , pp.٣٢-٤٧,Springer, ١٩٩٨.

[٢٦] A. Ross, J. Needham and S. Adi, **The Steganography File system**, Information Hiding: Second International Workshop,proceeding, vol ١٥٢٥ of lecture notes In computer science ,pp,٧٣-٨٢, Springer, ١٩٩٨.

[٢٧] G. Daniel & B. Wlater, **Information hiding to fail the Casual Counter feiter**, Information hiding: workshop, Proceedings, vol. ١٥٢٥ of lecture notes In computer second International science, pp. ١-١٥, Springer, ١٩٩٨.

[٢٨] L.Z Aredissian, **Image In Image Steganography System**, ph.D. , Thesis, University of Technology, ٢٠٠٠.

[٢٩] S. B. Abdulah, **Arabic Text Information Hiding, M.Sc**. Thesis, Iraqi Commission for Computer and Information/Informatics Institute for Postgraduate Studies, ٢٠٠١.

[٣٠] A.M. jafer**, Image steganography Using wavelet Transform Techniques**, M.Sc. Thesis, University of Baghdad, ٢٠٠٢.

[٣١] N. A. H. M. Al-Mayahee, **New Robust Information Hiding Technique**, M.Sc. Thesis, University of Technology, ٢٠٠٥.

[٣٢] N. F. Jhnson , S. jajodia and Z. Dnric, **Information Hiding steganography and Watermarking Attacks and Countermeasures ,center for Securee Information Systems** ,George Mason University,

Boston/Dordrecht/London, ٢٠٠١.

[٣٣] D. Sellars, **An Introduction to Steganography**, http://ww.cs.uct.ac.za/courses/cs٤٠٠ wnis/papers ٩٩/dsellars/stego- html, ٢٠٠٣.

[٣٤] B. Pifitzmann , **Informatin hiding Terminology**,In R.Anderson, Informatin Hiding first in computer science;vol. ١١٤٧)Berlin ,springer, ١٩٩٦. international workshop ,proceedings (lecture

[٣٥] J.Zollner, H.federrath, A.pfitzmann, A.Westfeld, G.Wicke, G.Wolf, **Uber die Modellierung steganographischer Systeme,** In G.Muller, K.Rannenberg, M.Reitenspieb, H.Stiegler,Verlabliche IT -System. Zwischen Key-Escrow und elektronischem Geld,Friedr . Vieeeg &Sohn Verlagsgesellschaft mbH,Braunschweig/ Wiesbaden, pp.٢١١-٢٢٣, ١٩٩٧.

[٣٦] H. klimanth, R. Piotraschke, **Informations theoretische Bewertung steganographischer Kozelationssyteme ,** In G. Muller, K.Rannenberg, M.Reitenspieb,H. Stiegler:Verlabliche IT-System. Zwischen Key-Escrow und elektronischem Geld,Friedr .Vieeeg &Sohn Verlagsgesellschaft mbH,Braunschweig/ Wiesbaden, pp.٢٢٥-٢٣٢, ١٩٩٧.

[٣٧] Y. Lee and L. Chen, **A Secure Robust Image**, Steganographic Model, Automatic Information Processing Laboratory CIS, NCTU, Hualiean, Taiwan, ٢٠٠٠.

[٣٨] J. Fridrich, **application of Data hiding in digital Images**, Tutuorial for the ISPACS'٩٨ conference in Melbourne, Australia, (١٩٩٨).

[٣٩] E. T. Lin and E.J Delph, **A Review of Data Hiding In Digital Images**, PICS٩٩, Ed., Apr. ١٩٩٩.

[٤٠] S. Katzenbisser and F.A. Pettcolas, **Information hiding Techniques for Steganography and digital Watermarking,** Artech House, USA, ٢٠٠٠.

[٤١] J. Wiley and sons, **Applied Cryptography**, second edition, Protocols algorithms and source code in C, Newyork ,Chichester,brisbone ,Toranto Singapoe, ١٩٩٦.

[٤٢] T. Y. Kim and J. Han**, partial Image Matching by Measures from Connected Color Regions**, Technical Report supported by Minstry of Education of Korea, ١٩٩٩.

[٤٣] R. Johnson and G. Bhattacharyya**, Statistics Principles and Methods**, John Wiley and Sons,INC, ١٩٨٥.

[٤٤] S. N. Chandhry**, Introduction to statistical Theory ,Kutubkhana**, Lahore,Pakistan, ١٩٨٤.

[٤٥] I. Daubechies, **Ten Lecture On Wavelets**, society for industrial and applied Mathematics Philadelphia, ١٩٩٢.

[٤٦] Daubeehies,I., **What do Wavelets come from .Personal Point of**

**View** ,Proceeding of the IEEE,Vol.٨٤,no.٤,pp.٥١٠-٥١٣,April ١٩٩٦.

[٤٧] A. graps, **An Introduction to Wavelet**, IEEE Computational science and Engineering,Vol .٢, no. ٢,pp.١-١٩,١٩٩٥.

[٤٨] M.Vererly,P. Dunhal, P. Flandrain, and Nishitani, Guest Editor **Introduction Wavelet and signal Processing** ,IEEE transaction on signal processing , Vol.٤١,no.١٢,pp.٣٢١٣-٣٢١٥ December ١٩٩٣.

[٤٩] Swildens,W.,**Wavelets What Next ?** , Proceeding of the IEEE ,vol. ٨٤, no.٤,pp.٦٨٠-٦٨٥,April ١٩٩٦{special issue on Wavelet}.

[٥٠] P. M. Bently, J. T. E. Mcdonnel, **Wavelet Transform An Introduction**, Electronic and communication agazine,pp.١٧٥- ١٨٦,August ١٩٩٤.

[٥١] O. Rioul, M. Vetterli, **Wavelet and Signal processing Magazine** ,IEEE ISSN ١٠٥٣-٥٨٨٨,vol.٨,no. ٤,pp.١٤-.٣٧,October ١٩٩١.

[٥٢] C. J. Zarowski, **Notes on orthnormal Wavelets and Wavelet packets** of ,Report of Department Electrical and Computer Engineering , Queen's University Canada k٧L ٣N٦,٣ November ١٩٩٥.

[٥٣] L. Jameson, **On the Differentiation Matrix for daubechies-based Wavelet on an Interval**, NASA Contractor Report ١٩١٥٨٢ ICASE Report ٩٣-٩٤ ,pp.١-٣٤,December,١٩٩٣.

[٥٤] L. Jameson, **On the Daubechies-based Wavelet Differential Matrix**, NASA Contractor Report ١٩١٥٨٣ ICASE Report ,no.٩٣- ٩٥,pp.١-٥٣, Decemper ١٩٩٣.

[٥٥] I. W. Selesnick, **Interpolation Multiwavelet Bases and the Sampling Theorem**, IEEE transaction on signal processing ,vol.٤٧,pp.١٦١٥-

[٥٦] C. S. burrus, R. A. Gopinath and H. Guo, **Introduction to Wavelets and Wavelet Transform**, prentice.Hall Inc, ١٩٩٨.

[٥٧] M. Misiti, Y. Misiti, G. Oppenheim, J. Poggi,**Wavelet Toolbox**, ١٩٩٧.

[٥٨] E. Scott Umbaugh**, Computer Vision image Processing**, prentice Hall PTR, ١٩٩٨

[٥٩] D. Salamon, **Data Compression**, Springer-Verlag New York, ١٩٩٨.

[٦٠] B. Foronzan, **Introduction to data Communications and Networking**, ١٩٩٨.

[٦١] Kientzie ,Tim .**Guide to Sound** ,Library of Congress cataloging-in- publication data, ١٩٩٨.

[٦٢] R. Conboy, **Importing Audio Into Adobe Premiere using Cool Edit pro**, Interactive Media Center , http://Library.albany.edu/ime/٥١٨ ٤٤٢-٣٦٠٨.

[٦٣] L. R. H. Al-Kattab, **Image Identification Using Dsp Techniques,** Ph.d. Thesis, University of Technology, ٢٠٠٢.

[٦٤] M.J.Dallwityz, **An Introduction to Computer Image**,٢ August ٢٠٠٤.

[٦٥] D. Lancaster, **Exploring the.BMP File format,** ٢٠٠٣.http://www.tinaji.com

[٦٦] E.H. Obead, **Parallel Structure for Image Compression using Neural Network**, M.Sc thesis, Babylon University, ٢٠٠٠.

## المصادر العربية:

[٦٧] جعفر، هبه محمد، **نظام لإخفاء صورة ملونة داخل صورة ملونة** ، رسالة ماجستير مقدمه إلى جامعة بابل ، كلية العلوم ،٢٠٠٣.

[٦٨] بوش-جيرد ، **أساسيات الفيزياء** ، الدار الدولية للاستثمارات الثقافية ، الطبعة العربية الأولى ، ٢٠٠١.

[٦٩] المعموري، هدى ناجي نواف، **تمييز اصوات المحركات الصاروخية باستخدام محول المويجة** ، رسالة ماجستير مقدمة إلى جامعة بابل ، كلية العلوم ، ٢٠٠١.

[٧٠] د. الششتاوي، احمد أمين، **برمجة ومعالجة الصور** ، مكتبة الدار العربية للكتاب، ط١ ،١٩٩٧.

[٧١] الخوئي، السيد أبو القاسم الموسوي، **البيان في تفسير القرآن**، منشورات دار العلم للإمام السيد الخوئي، مطبعة العمال المركزية،ص٤٤٩، ١٩٨٨.

# المصطلحات

| | |
|---|---|
| الفيض | (redundant) |
| أمنية الحاسبة | (computer security) |
| التشفير | (cryptography) |
| المعلومات المخفية | (steganography) |
| اتصال سري | (secret communication) |
| الحبر السري | (Invisible Ink) |
| النقطة المصغرة | (Microdot) |
| الصور المايكروية | (Microdot photograph) |
| الكتابة المخفية الحديثة | (Modern steganography) |
| وسط الإخفاء | (steganography medium) |
| لوحة الألوان | (palette) |
| الضوضاء | (noise) |
| الترددات الغير مسموعة | (Non-Audible Frequency) |
| عينة | (sample) |
| مشوش | (Fuzzy) |
| الجسم المخفي | (stego-object) |
| العلامة المائية | (Watermarking) |
| تحليل الإخفاء | (stganalysis) |
| المرشحات الخطية واللاخطية | (linear & nonlinear filters) |
| الضغط بفقدان | (Lossy compression) |
| تكميم اللون | (color quantization) |
| عدم الرؤيا | (Invisibility) |

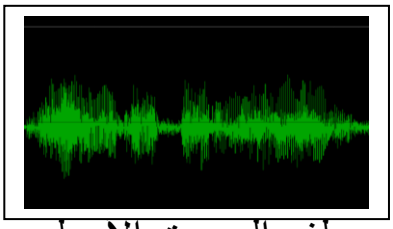
| | |
|---|---|
| نظام الرؤيا البشري | (Human visual system) |
| نظام السمع البشري | (Human Audio system) |

| | |
|---|---|
| تقنيات مجال التحويل | (Transformation Domain Techniques) |
| تقنيات الطيف المنتشر | (spread spectrum techniques) |
| تقنيات التشويه | (Distortion Technique) |
| طرق توليد الغطاء | (Cover Generation Method) |
| إبدال الثنائية الأقل أهمية | (Least significant bit substitution) |
| التباديل شبه العشوائية | (psedorandom permutation) |
| التنقيص | (Down-sampling) |
| حزمة مرور عالي | (high pass filter) |
| حزمة مرور واطئ | (Low-pass filter) |
| تشفير طول السلسلة | (Run Length Encoding) |
| المدرج التكراري | (Histogram) |
| درجة الدقة | (Fidelity Criteria) |
| الجذر التربيعي لمعدل مربع الخطأ | (Root Mean Square Error) |
| نسبة الإشارة إلى الضوضاء | (signal to noise ratio) |
| نسبة قمة الإشارة إلى الضوضاء | (Peak signal to noise ratio) |
| مقياس الموثوقية الشخصي | (Subjective Fidelity Criteria) |
| مقياس الموثوقية الهدف | (objective Fidelity Criteria) |

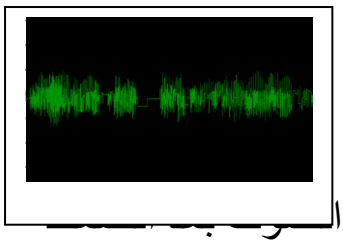
**تجربة ٩ :**

تبين التجربة اللاحقة الصوت المخفي الآية(غلبت الروم) والصورة الغطاء ، والصورة الحاملة الناتجة من عملية الإخفاء، والصوت المسترجع الناتج من عملية استخراجه من الصورة المخفية الحاملة والذي يختبر في النظام المقترح .

في **المرحلة الأولى** ضُغِطَ ملف الصوت الأصلي وذلك بعد تطبيق تحويل المويجة المتقطع(DWT) للمستوي الثالث وبعدها طبق تشفير طول السلسلة .



ملف الصوت الأصلي



ملف الصوت بعد الضغط

في **المرحلة الثانية** أُختيرت الصورة الغطاء لإجراء الإخفاء ، حجم القطعة

الصو

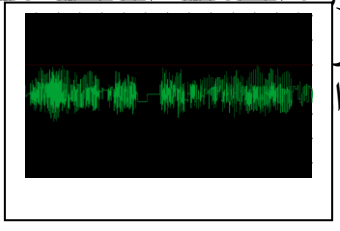
يساوي(١٦x١٦)

**تجربة ١٠**

تبين الصوت المخفي الآية(قل هو الله أحد)

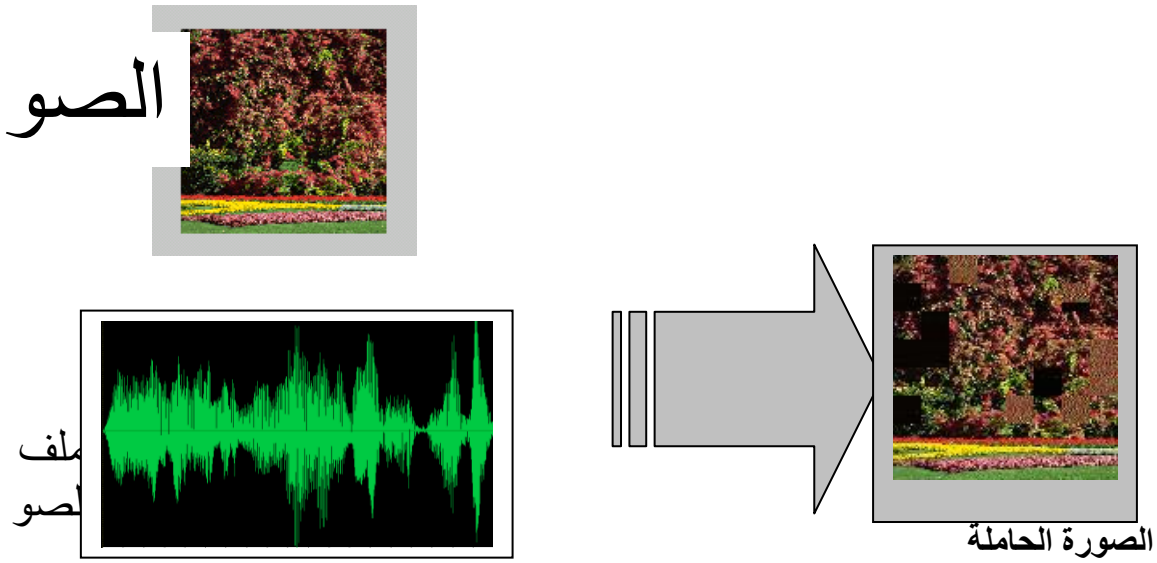
عملية الإخفاء، والصوت المسترجع الناتج من

استخ **الصورة الحاملة** رة المخفية الحاملة والذي يختبر في ا

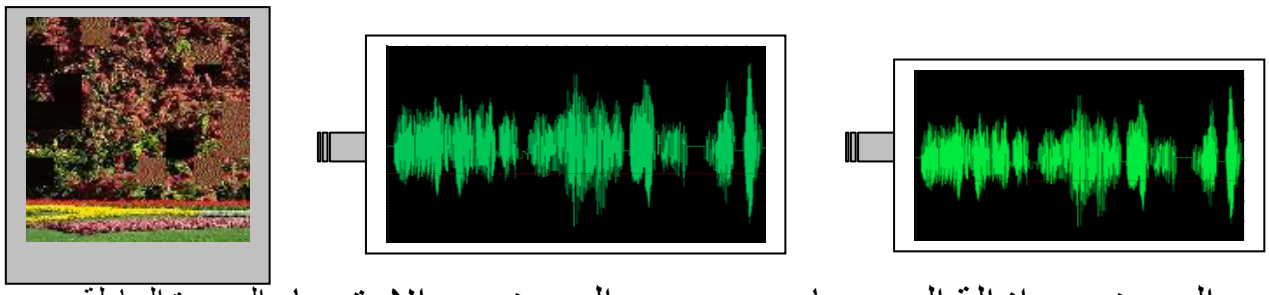


ملف الصو

أُختيرَت الصورة الغطاء لإجراء الإخفاء ،حجم القطعة يساوي(٨×٨) بعد ضغط ملف الصوت بنفس الأسلوب السابق.



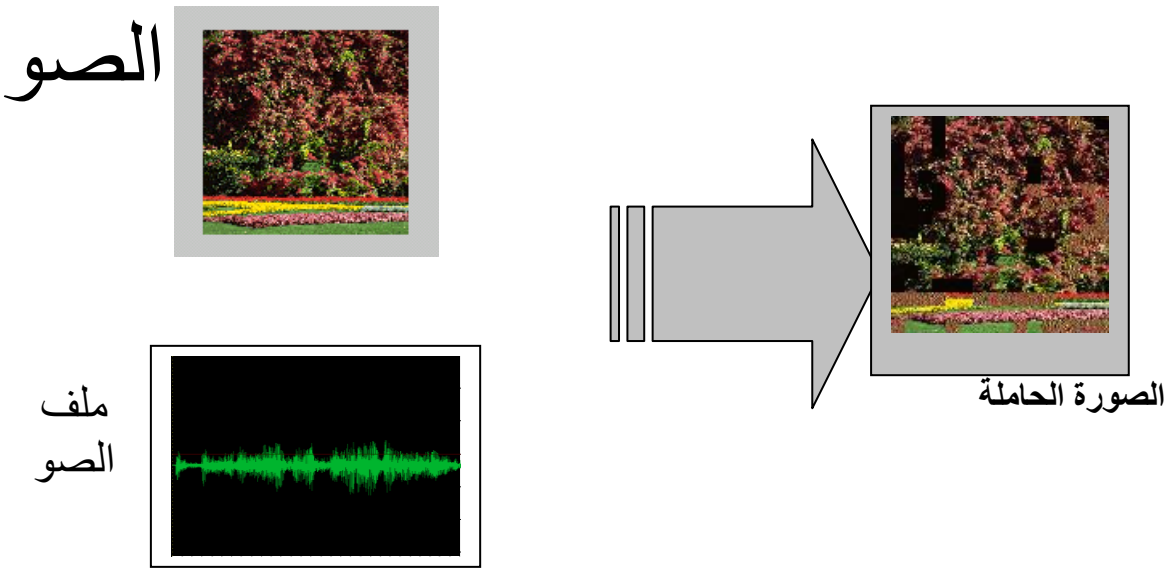

استُرجِع الصوت من الصورة الحاملة وأُزيلَت الضوضاء منه باستخدام(CEP) .




**تجربة ١١ :**

تبين التجربة اللاحقة الصوت المخفي الآية(الحمد لله رب العالمين) والصورة الغطاء ، والصورة الحاملة الناتجة من عملية الإخفاء، والصوت المسترجع الناتج من عملية استخراجه من الصورة المخفية الحاملة والذي يختبر في النظام المقترح .

أُختيرَت الصورة الغطاء لإجراء الإخفاء ،حجم القطعة يساوي(٨×٨) بعد ضغط ملف الصوت بنفس الأسلوب السابق.




استُرجِع الصوت من الصورة الحاملة وأُزيلَت الضوضاء منه باستخدام(CEP) .