نظام لإخفاء صورة ملونة داخل صورة ملونة

رسالة مقدمة

الى مجلس كلية العلوم / جامعة بابل

وهي جزء من متطلبات نيل درجة الماجستير في علوم الحاسبات

من قبل الطالبة

هبه محمد جعفر الخفاجي

رجب 1423 هـ **أيلول 2003 م**

e

﴿نرْفعُ دَرَجَاتٍ مَنْ نشاءُ وَفوْق كلِ ذِي عِلمٍ عَلِيمٌ﴾

سورة يوسف(76)

شكر وتقدير

لايسعني وأنا اكمل هذه الرسالة إلا أن احمد الله سبحانه وتعالى واشكر فضله علـى ما أمدني به من القوة والصبر والإرادة، وأقدم شكري إلى:

- رئاسة جامعة بابل وعلى رأسها الأستاذ الدكتور فاضل فرهود لتعاونه فـي تطوير مستوى الدراسات العليا في كليات وأقسام الجامعة كافة.
- عمادة كلية العلوم وعلى رأسها الأسـتاذ الـدكتور عـودة مزعـل ياسـر لإرشاداته المتواصلة في دعم طلبة الدراسات العليا في كلية العلوم.
- أستاذي المشرف الأستاذ الدكتور نبيل هاشـم كاغـد لملاحظاتـه القيمـة وجهوده المتواصلة في دعم هذه الرسالة.
- قسم علوم الحاسبات وعلى رأسه الأستاذ الدكتور نبيل هاشم كاغد لجهوده في توفير كل ما نحتاج إليه من مستلزمات بحثية خلال مدة الدراسة.
- طلبة الدراسات العليا ، ولاسيما مَنْ في مرحلة البحث لتعـاونهم ودعمهـم خلال مرحلة البحث.
- عائلتي لصبرهم طيلة مدة البحث ، والى كل من ساهم في هذا البحث.

الباحثة

قرار لجنة المناقشة

نحن أعضاء لجنة المناقشة ، نشهد إننا قد اطلعنا على الرسالة الموسومةبـــــ(نظـــام لإخفاء صورة ملونة داخل صورة ملونة). وقد ناقشنا الطالبة ((هبه محمـــد جعفـــر)) فـي محتوياتها وفيما له علاقة بها وذلك بتاريخ 9 / 2003/10 ووجدنا إنها جـــديرة بـــالقبول بدرجة (**إمتياز**) لنيل درجة الماجستير في علوم الحاسبات.

التوقيع:
رئيس اللجنة:د. ستار بدر سدخان
المرتبة العلمية: استاذ
العنوان: وزارة العلم والتكنلوجيا/ شركة الميلاد العامة
التأريخ: / /

التوقيع:
عضو اللجنة:د. أديب حمدون سلمان
المرتبة العلمية: استاذ مساعد
العنوان:كلية الرافدين الجامعة
التأريخ: / /

التوقيع:
عضو اللجنة:توفيق عبد الخالق عباس كاغد
المرتبة العلمية: استاذ مساعد
العنوان:جامعة بابل /كلية العلوم
التأريخ: / /

التوقيع:
عضو اللجنة(مشرفا):د. نبيل هاشـــم
المرتبة العلمية: استاذ
العنوان: جامعة بابل /كلية العلوم
التأريخ: / /

مصادقة عمادة كلية العلوم

أصادق على ماجاء في قرار اللجنة في أعلاه.

التوقيع:
الاسم: د.عودة مزعل ياسر
المرتبة العلمية: أستاذ مساعد
العنوان: جامعة بابل/ كلية العلوم /عميد كلية العلوم
التأريخ: / /

إقرار الأستاذ المشرف

أ إعداد هذه الرسالة الموسومة بـــ(نظام لإخفاء صورة ملونة داخل صورة ملونة) قد جرى تحت إشرافي في قسم علم الحاسبات - كلية العلوم - جامعة بابل وهـــي جـــزء مـــن متطلبات نيل درجة الماجستير في علوم الحاسبات.

التوقيع :

اسم المشرف: د. نبيل هاشم كاغد

المرتبة العلمية: أستاذ

التاريخ: / /2003

توصية رئيس القسم

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

التوقيع :

اسم المشرف: د. نبيل هاشم كاغد

المرتبة العلمية: أستاذ

التاريخ: / /2003

الخلاصة

تعد أمنية المعلومات من المواضيع التي تنال اهتماما كبيرا في العديد من المجالا ومنها إخفاء المعلومات ،لحماية المعلومات المهمة من وصول لأشخاص المتطفلين إليها .

يهدف البحث الى إخفاء صورة ذات تدرجات لونية مختلفة (صور ذات تدرج رمادي و صور ملونة ذات (256) لونا و صور طبيعية) وبدرجات تعقيد مختلفة داخل صورة أخرى لها نفس الحجم وبتدرجات لونية مختلفة ،تضمن النظام المقترح تنفيذ خمس طرق إخفاء مختلفة :

- طريقة Image Downgrading :وفيها يتم إبدال الثنائيات الأقل أهمية من صورة الغطاء بالثنائيات الأكثر أهمية من الصورة المراد إخفاؤها بعد أنْ تشفر بوساطة دالة او الحصرية (XOR) مع مفتاح سري . وقد نفذت توافيق مجموعة الصور المختلفة الأنواع والتعقيدات في عملية الإخفاء وكانت النتائج جيدة في جميع الحالات وخالية من التشوهات عدا حالة إخفاء صورة ملونة ذات (256) لونا إذ ظهر فيها بعض التشوهات البسيطة (غير الملحوظة)، كما حققت الصور المعقدة نتائج أفضل لان تأثير عملية الإخفاء يندمج مع تفاصيل الصورة.
- طريقة حشر الثنائيات الأقل أهمية :وفيها يتم إخفاء الصورة المراد إخفاؤها كاملة داخل الثنائيات الأقل أهمية من صورة الغطاء ، إذ تم إخفاء صور ذات تدرج رمادي أو ملونة ذات (256) لونا داخل صور طبيعية، وكانت النتائج جيدة لجميع أنواع الصور بتعقيداتها .

- طريقة الاسلوب الرياضي :تعتمد هذه الطريقة على استعمال الاسلوب الرياضي في عملية الإخفاء ،إذ تدمج البيانات السرية بصورة الغطاء وفي مواقع عشوائية لذا تعد اكثر أمنية نسبة إلى الطريقتين السابقتين،وقد نفذت توافيق مجموعة الصور المختلفة الأنواع والتعقيدات في عملية الإخفاء وكانت النتائج جيدة في جميع الحالات وخالية من التشوهات .
- طريقة هجينة: تتضمن هذه الطريقة مرحلتين هما مرحلة الضغط ومرحلة الإخفاء ، أما عملية الاسترجاع فتكون بمرحلتين هما مرحلة الاسترجاع ومرحلة فك الضغط ،وقد نفذت توافيق مجموعة الصور المختلفة الأنواع والتعقيدات في عملية الإخفاء وكانت النتائج جيدة في جميع الحالات وخالية من التشوهات .
- طريقة القطاعات المتشابهة: وهي طريقة جديدة تعتمد على إبدال القطاعات المتشابهة بين الصورة الإخفاؤها وصورة الغطاء. تعدُّ أكثر الطرق أمنية وحصانة ضد التغييرات والمعالجات التي تنجز على الصورة الحاملة للصورة المخفية، وقد نفذت على مجموعة صور مختلفة الأنواع والتعقيدات في عملية الإخفاء وكانت النتائج جيدة للصور ذات التدرج الرمادي والصور الطبيعية، أما بالنسبة للصور الملونة ذات (256) لونا ظهرت فيها بعض التشوهات (غير مدركة).

تم تنفيذ النظام المقترح على حاسب معالجه بنتيوم **4** واستعمال لغة (**Delphi**) الإصدار

.4

المحتويات

الرقم	الموضوع	رقم الصفحة
.....	.....	.....

1-1 مقدمة عامة (General Introduction)

تعد أمنية المعلومات (**Information Security**) من المواضيع المهمة التي تنال اهتماما لعديد من المجالات ومنها مجال الحاسبات . إذ ظهرت الكثير من أنظمة التشفير و الترميز (**Cipher and Coding Systems**) لحماية المعلومات المهمة من وصول الأشخاص غير المخولين إليها.لكن نقطة الضعف فيها هي سهولة اكتشافها ومن ثمَّ كسرها[1].

زيادة على ذلك فإنَّ بعض الحكومات منعت استعمال التشفير للأغراض سرية . لذا بدأت الحاجة إلى أنظمة جديده تكون مادرة على حماية المعلومات المهمة ومنها إخفاء المعلومات (**Information Hiding**) . فعندما يتعذر إرسال رسالة مشفرة بسبب العمل في شركة لا تسمح بتشفير البريد الإلكتروني (**E- mail**) أو أنَّ الحكومات المحلية لاتسمح باستعمال التشفير فيمكن إخفاؤها في أوساط متعددة منها رسالة (**Message**) أو صورة (**Image**) أو صوت (**Audio**) .[2]

فإخفاء المعلومات هي أحدى التقنيات العالية الأمنية التي تستعمل لاخفاء المعلومات المهمة مختلفة الهيئات داخل وسائط مختلفة (**Various Forms of Media**) بهيئة لا تشعر نظام الرؤيا البشري **HVS** (**Human Visual System**)بوجودها .

بصورة عامة توجد ثلاثة اتجاهات لاخفاء المعلومات هي[1] :

أولا : الإخفاء (**Steganography**) :- ويعني إخفاء المعلومات المهمة والمختلفة الهيئات داخل وسائط أخرى بطريقة لا تسمح للمتطفل باكتشافها .

ثانيا : العلامة المائية (**Watermarking**) :- تعدُّ العلامة المائية الرقمية (**Digital Watermarking**) وسيلة فعالة لحماية حقوق النسخ (**Copyright**) للوسائط الرقمية (**Digitized Media**) مثل صورة(**Image**)،صوت(**Audio**) وغيرها،إذ يتم إخفاء المعلومات السرية داخل إشارات رقمية .

ثالثا : بصمة الإصبع (**Fingerprint**) :-تعدُّ بصمة الإصبع(**Fingerprint**) صفة تلازم كيان واد تمييزه عن كيان آخر مشابه له.إذ يتم إضافة بصمة الإصبع إلى الكيان لغرض حماية حقوق نسخ البيانات ،إن هذا يدعى باستحصال البصمة (**Fingerprinting**) .

إن أحدى المساؤى الشائعة في معظم طرائق الإخفاء الموجودة هي التشويه(**Distortion**) الظاهر في صوره الغطاء الذي يبدو كضضاء (**Noise**) نتيجة لإخفاء البيانات .

وعلى الرغم من أنّ هذا التشويه يكون في بعض الأحيان قليلا جدا ولكنه غير مقبول في بعض الحالات مثل الصور الطبية (**Medical Images**) والصور الحربية (**Military Images**) [3] .

وبصوره عامه تقسم تطبيقات إخفاء البيانات على مجموعتين اعتمادا على وجود أو عدم وجود علاقة الرسالة وصورة الغطاء. تمثل المجموعة الأولى تطبيقات الإخفاء (**Steganographic Applications**) وفيها لاتكون هنالك أي علاقة بين الرسالة وصورة الغطاء،وتمثل الاخيره وعاء يحمل الرسالة (بطريقه سريه). لذلك فإنّ صورة الغطاء ليس لها أي أهميه بالنسبة إلى المرسل أو المستلم،فالهدف الرئيس هو إرسالة بطريقه سريه (أمينة) لذا فإنّ مثل هذه التطبيقات لاتهتم بصورة الغطاء ولا تتطلب أنْ تكون خالٍ التشوهات نتيجه لاخفاء الرسالة .

أما المجوعة الثانية فهي تقنيات العلامة المائية الرقمية (**Digital Watermarking Applications**) وفيها توجد علاقة قويه بين الرسالة وصورة الغطاء ، بحيث إنّ الرسالة تدعم

(تضيف) معلومات مكملة (اضافيه) لصورة الغطاء مثل عنوان الصورة (**Image Caption**) أو بصمة المؤلف (**Author Signature**) لذا فإنّ التشوهات يجب أن تكون اقل ما يمكن[3].

إنّ المتطلبات الأساسية لأي نظام إخفاء هي التحصين وعدم القدرة على الاكتشاف والسرية و عدم الرؤيا والسعة ولكن لا يمكن الحصول على نظام يجمع هذه المتطلبات بصورةمثالية .لذلك يجب أن تكو هنالك موازنة مقبولة بين هذه العناصر(المتطلبات) تحدد من قبل التطبيق [4] .

على سبيل المثال ، إن إخفاء المعلومات قد يتسامح بالنسبة إلى التحصين و لكن يطلب سعة كبيرقدر الإمكان و اقل إدراك (بدون حدوث تشويه واضح في صورة الغطاء).على حين لا تحتاج العلامة المائية الرقمية إلى سعة كبيرة وإلى تقليل الإدراك و إنما تحتاج إلى زيادة في التحصين [5].

يتكون النظام المقترح من خمس طرائق إخفاء مختلفة، كل طريقة لها مجموعة مقاييس تعتمد عليها في عملية الإخفاء(**Embedding Process**) التي تختلف عن الطرائق الأخرى.وقد تم تنفيذ النظام على تواع من الصور هي : الصور ذات التدرجات الرمادية(**Gray Scale Image**)، والصور الملونة ذات(**256**) لونا و الصور الطبيعية (**True Color**)،وقد تم التركيز على الصور الملونة و بدرجات تعقيد مختلفة،حيث يتم اختيار الصور وافق مع مقاييس كل طريقة و ليس بالضرورة أن تتوافق مع كل الطرائق.فالهدف هو إخفاء اكبر كمية ممكنة من المعلومات وهو مساوٍ لحجم صورة الغطاء.إنّ الحجم الكبير لصورة الغطاء يكون غير طبيعي وقد يثير شكوك المتطفلين،كما يكون مربك في ل والاستلام ، ولزيادة أمنية المعلومات تم استعمال الاسلوب العشوائي في اختيار مواقع الإخفاء .

2-1 ملخص لأدبيات سابقة:

ظهرت العديد من الأدبيات حول الموضوع و بطرائق وهيئات مختلفة إذ يمكـن إجمـال مـا

ظهرت ضمن أهداف الرسالة على النحو الآتي :-

اقترح كل من(**B.O.Comisky , J.R.Smith**) في عام **1996** عدة طرائـق لاخفـاء بيانات الطيف المنتشر(**Spread Spectrum Data-Hiding**) باستعمال بيانات الرسالة الثنائيه إذ إنّ $b_i \in \{-1,1\}$ ، لنمذجة الإشارة الحاملة $\ddot{i}(x,y)$ (**Carrier Signal**)

$$S(x,y)=\sum_i b_i \ \ddot{}_i(x,y) \qquad (1-1)$$

في الحالة المثالية تكون الاشاره الحاملة وهي دالة أساسية عمودية على صورة الغطاء N(x,y) ، ولكن لا تكون عمودية بصورة تامة .

$$\left\langle \ddot{}_i, N \right\rangle = \sum_{x,y} \Phi i(x,y) \quad N(x,y) \quad \approx 0 \qquad (1-2)$$

تضاف الإشارة المراد إخفاؤها S(x,y) إلى صورة الغطاء N(x,y) ، لتكوين الصورة الحاويـة على الإشارة المخفيه $D(x,y)$ (**Stego - Image**) .

$$D(x,y)=S(x,y)+N(x,y) \qquad (1-3)$$

تسترجع الرسالة عن طريق حساب الارتباط المشـترك (**Cross-Correlation**) بـين الصـورة الناتجة (**Stego-Image**)والصورة الحاملة المولدة (**Carrier Regenerated**) بوسـاطة مرجـع محلي(**Local Reference**) .

$$o_i = \sum_{x,y} D(x,y) \ \ddot{}_i(x,y) \qquad (1-4)$$

تستعمل عملية التعتيب (**Thresholding Operation**) على O_i لتحديد القيمـة الثنائيـة لثنائيات البيانات المخفية.إنّ هذه الطريقة قادرة على إخفاء واسترجاع (**100 Bit**) من المعلومات داخل

صورة رمادية التدرج ذات حجم 320×320 عنصراً، ومعدل المعلومات(**Information Rate**) يساوي 0.0001 [6] .

عرض كل من(**W.Bender,D. Gruhl, N.Morimoto and A.Lu**) عام **1996** عدة طرائق لاخفاء البيانات في هيئات مختلفة.أحدى هذه الطرائق تسمى بـ(**Patchwork**) ،حيث يتم تغير الصفات الاحصائيه (**Statistical Features**) لصورة الغطاء.أولا، ثم يتم اختيار أزواج من مناطق الصورة (**Pairs of Image Regions**) بصورة عشوائية.يختار الزوج مرة ويتم تغيير العناصر لتكوين علاقة بين المناطق لتعكس البيانات المخفيه.على سبيل المثال ،إذا كانت كل عناصر أول منطقه مختارة هي اكبر من عناصر المنطقة الثانية فأنّ ثنائية البيانات المخفيه تساوي واحد.تكون التغيرات نوعا ما قليله وتبدو غير محسوسة لذلك فإنها حصينة ضد الهجوم ولكن كمية المعلومات المخفيه تكون قليله[7] .

اقترح كل من (**P. Davern and M. Scott**)عام **1996** طريقة إخفاء باستعمال عمليات ضغط الصور المبعثرة (**Fractal Image Compression Operations**) . تضمن عملية ضغط الصور الجزئيه تقسيم الصورة إلى قطاعات(**Blocks**) والتي تبدو متشابهة يتم تحديدها.ولاخفاء ثنائية واحدة يتم تغيير قطاع واحد بآخر مقارب له ثم يخزن الأخير في موقع القطاع الأصلي.ولاسترجاع البيانات يستعمل مفتاح (**Key**)لتحديد مواقع المناطق الحاوية على بيانات مخفيه.ولسوء الحظ, فإنّ هذه الطريقة تستعمل لاخفاء كمية صغيره من البيانات(ثنائية واحدة لكل قطاع) وكذلك يمكن أن تدمر البيانات بسهولة(غير محصنة).زيادة على أنّ عملية البحث عن القطاعات المتشابهة ،الإخفاء وعمليات المقارنة في عمليات الاسترجاع تحتاج إلى عمليات احتساب عالية [8] .

قدم كل من(**M.D.Swanson,B.Zhu and A.H.Tewfik**)عام **1996** طريقتين لاخفاء البيانات في الصور.تستعمل الطريقة الأولى القناع الحيزي(**Spatial Masking**),إذ يتم

حسابة لكل قطاع في الصورة ثم تخفى الومات السرية بطريقة عشوائية.أمّا الطريقة الثانية فتعتمد على استعمال القناع الترددي(**Frequency Masking**)على كل قطاع بعد تحويله باستعمال تحويل جيب التمام المتقطع **DCT** (**Discrete Cosine Transform**) [9] .

عرض كل من(**J.Rimell and J.Hankinson**) عام **1997** طريقة جديدة لاخفاء المعلومات داخل صور هيأة **TIFF** (**Targged Image File Format**)،إذ تخفى البيانات في الثنائيات الأقل أهميه **LSB** (**Least Significant Bit**) لكل عنصر في الصورة،وكذلك استعمل القناع(Mask)،لذلك فإنّ عملية الإخفاء لا تؤثر على محتوى الصورة و يتم خلق القناع اعتمادا على محتوى الصورة ثم بعدها تخفى البيانات [2] .

اقترح كل من(**J.Fridrich and R.Simard**) عام **1997** طريقة لاخفاء صور ذات تدرج رمادي داخ صور ذات تدرج رمادي أيضا.إذ يتم تشفير الصور المراد إخفاؤها باستعمال(**Discrete Chaotic Mapping Function**)ومسجل الإزاحة(**Linear Shift Register**).وباستعمال طريقة حشر الثنائيات الأقل أهميه(**LSB**)يتم إخفاء الصور(يجب أن يكون حجم صورة الغطاء اكبر بأربع مرات من حجم الصورة المخفيه) [10] .

اقترح كل من(**A.Westfeld and G.Wolf**) عام **1998** طريقة لاخفاء رسالة داخل سلسلة صور فيديو (**Video Stream**)وقد استعمل تحويل جيب التمام المتقطع(**DCT**)لضغط الصور،حيث يتم اختبار كل قطاع(**Block**) بعد تحويلة لمعرفة فيما إذا كان ملائما لاخفاء ثنائية الرسالة أم غير ملائم. وتعتمد عملية الاختبار على حساب (**sum modulo 2**) حيث (**sum**) يمثل مجموع القطاع وهو نوع من التطابق(**Parity**)فإذا كان مساويا إلى الثنائية المراد إخفاؤها فإنّ القطاع يرسل بدون تغيير وإلا فإنه يغير [11] .

وفي نفس العام قدم كل من (**L.M.Marvel,C.G.Boncelet and C.T.Retter**) طريقة أمينة لاخفاء واسترجاع رسالة ذات طول محدد في صور رقمية بعد أن يتم تشفيرها باستعمال مفتاح (**Key**) مع الحفاظ على الحجم الأصلي [12] .

وفي عام **1999** قدم (**J.Fridrich**) طريقة جديدة تعتمد على لوحة ألوان الصورة (**Palette-Based Images**)،حيث يتم إخفاء ثنائيات الرسالة في مواقع عشوائية تولد بوساطة مولد الأرقام شبه العشوائية (**Pseudo-Random Generator**) ويكون المفتاح السري هو قيمة البذرة (**Seed**) له.فيبحث عن اقرب لون للعنصر المراد الإخفاء فيه بالاعتماد على حساب الفرق (**Distance**) بين الألوان (**R1,G1,B1**) و(**R2,G2,B2**) وفق المعادلة :

$$\sqrt{(R1-R2)^2+(G1-G2)^2+(B1-B2)^2} \qquad (1-5)$$

ثم يجد ثنائية التطابق(**Parity Bit**) له وهي تساوي (**(R+G+B) Mod 2**)فإذا كانت تتطابق مع الثنائية المراد إخفاؤها فإنّ هذا العنصر يبدل مكان العنصر السابق [13] .

وفي نفس العام عرض(**L.M.Marvel**)طريقة لاخفاء رسالة(**Message**) داخل صور ذات تدرج رمادي(**Gray scale**) بحجم 256×256 وقد اهتم بجانبين مهمين لأي نظام إخفاء هما زيادة كمية المعلومات المخفيه(**Capacity**)وتقديم مستوى عالٍ من عدم الإدراك (**Imperceptibility**) مقابل مقاومتها للتدمير أو الإزالة(**Removal Resistance**).وقد قام بتشفير الرسالة وأضاف ضوضاء(**Noise**)قبل إخفائها في صورة الغطاء(**Cover Image**)،إذ كانت كمية المعلومات المخفيه(**Payload**) تساوي(1364) ثمانية في صور ذات تدرج رمادي بحجم 256×256 [14] .

قدم كل من(**B.S.Manjunath and J.J.Chae**) عام **1999** طريقة لاخفاء صور ذات تدرج رمادي بحجم 128×128 داخل صور ذات تدرج رمادي أيضا إمّا بحجم 512× 512 وإمّا بحجم 256×256 .تضاف بيانات الصورة أو الإشارة (**Signature**) إلى صورة الغطاء في مجال

تحويل جيب تمام المتقطع (**DCT**)،حيث تشفر معاملات الإشارة المحولـــة(**Signature DCT Coefficients**) باستعمال(**Lattice Coding Scheme**) قبل الإخفاء.ويتم فحص المحتـــوى التركيبي(**Texture Content**)لكل قطاع محول من معاملات الغطاء ورموز الإشارة(**Signatured Codes**) المتوافقة (المناسبة)لتحشر اعتمادا على مقيـــاس النســـيج المحلـــي(**Local Texture Measure**) . وقد كانت الصورة المسترجعة ذات نوعية جيدة وبدون أي تشـــوهات ملحوظـــة،وإنّ عملية الاسترجاع لا تتطلب وجود صورة اغطاء الأصلية [15] .

قـــدم كل مـــن(**S.Areepongsa,N.Kamnerd Y.F.Syed and K.R.Rao**) عام **2000** طريقة لاسترجاع الصورة باستعمال تقنية إخفاء المعلومات(**Steganography**).حيـــث يتم استخلاص بعض صفات الصورة(**Features Extraction**) مثل الهيئـــة (**Shape**)،واللـــون (**Color**)والنسيج (**Texture**) ثم تخفى في قاعدة بيانات تضغط باستعمال (**Wavelet Coder**)بدل من إخفاء الصورة نفسها [16] .

قدمت الباحثة (**L. Z.Avedissian**) عـــام **2000** نظامـــا لإخفـــاء صـــورة ذات تـــدرج رمادي(صغيرة) داخل صورة ذات تدرج رمادي أو ملون(كبيـــرة) ،حيـــث تضـــمن النظـــام ســـت مراحل:الفحص والتغيير،و التناقل،وخوارزمية أحسن_بحث،وإخفاء الأماكن وأخيرا المفتاح.وقـــد أعطى النظام نتائج جيدة [17] .

قـــدم الباحث (**F.A.Sedeek**) عام **2001** طريقة لاخفاء رسالة بعد أن شـــفرها باســـتعمال نظام التشفير الانسيابي (**Stream Cipher System**)في الثنائيات الأقل أهميـــة (**LSB**) لصـــورة الغطاء وقد استعمل طريقتي الوثب الموحد والعشوائي(**Uniform and Random Hopping**)في توزيع ثنائيات الرسالة السرية [1] .

قدم الباحث (**R.Samiar**) عام **2002** نظاما لإخفاء نص في صورة وقد استعمل التقنيات الآتية: تقنيات مجال التحويل (**Transform Domain**) والطيف المنتشر (**Spread Spectrum**) والأنظمة الابدالية (**Substitution System**) [18] .

3-1 إخفاء المعلومات (Information Hiding)

تعدُّ طريقة إخفاء المعلومات أحدى التقنيات التي لهاه كبرى في حماية المعلومات الخاصة (السرية)،إذ نجد خلال التاريخ الكثير من الطرائق التي استعملت لاخفاء المعلومات،ويمثل كاسر الشفرة(**David Kahn**)افضل مثالٍ في هذا التاريخ [19] .

كذلك نجد في تاريخ الإغريق القديم قصصا كثيرة حول الإخفاء.منها قصة (**Demeratus**) عندما أراد أن ينذر(**Sparta**) بان (**Xerxes**) عزم على غزو الإغريق،إذ قام بإزالة شمع الألواح وكتب رسالة في اسفل الخشب ثم غطى الألواح بالشمع مرة أخرى،فظهرت وكأنها فارغة وغير مستعملة وتمكنت من اجتياز نقطة التفتيش بلا استفسار [20] .

كذلك عندما أراد (**Histiaeus**) أن يخبر أصدقاءه بأنّ الثورة قد بدأت ضد (**Medes**) و(**Persians**) فقام بحلق شعر راس خادمه الأمين وكتب رسالة على رأسه وانتظر لحين ظهور شعره ثم أرسله إذ إنّ الرسالة لا يمكن اكتشافها إلا بحلق رأسه مرة أخرى [19].

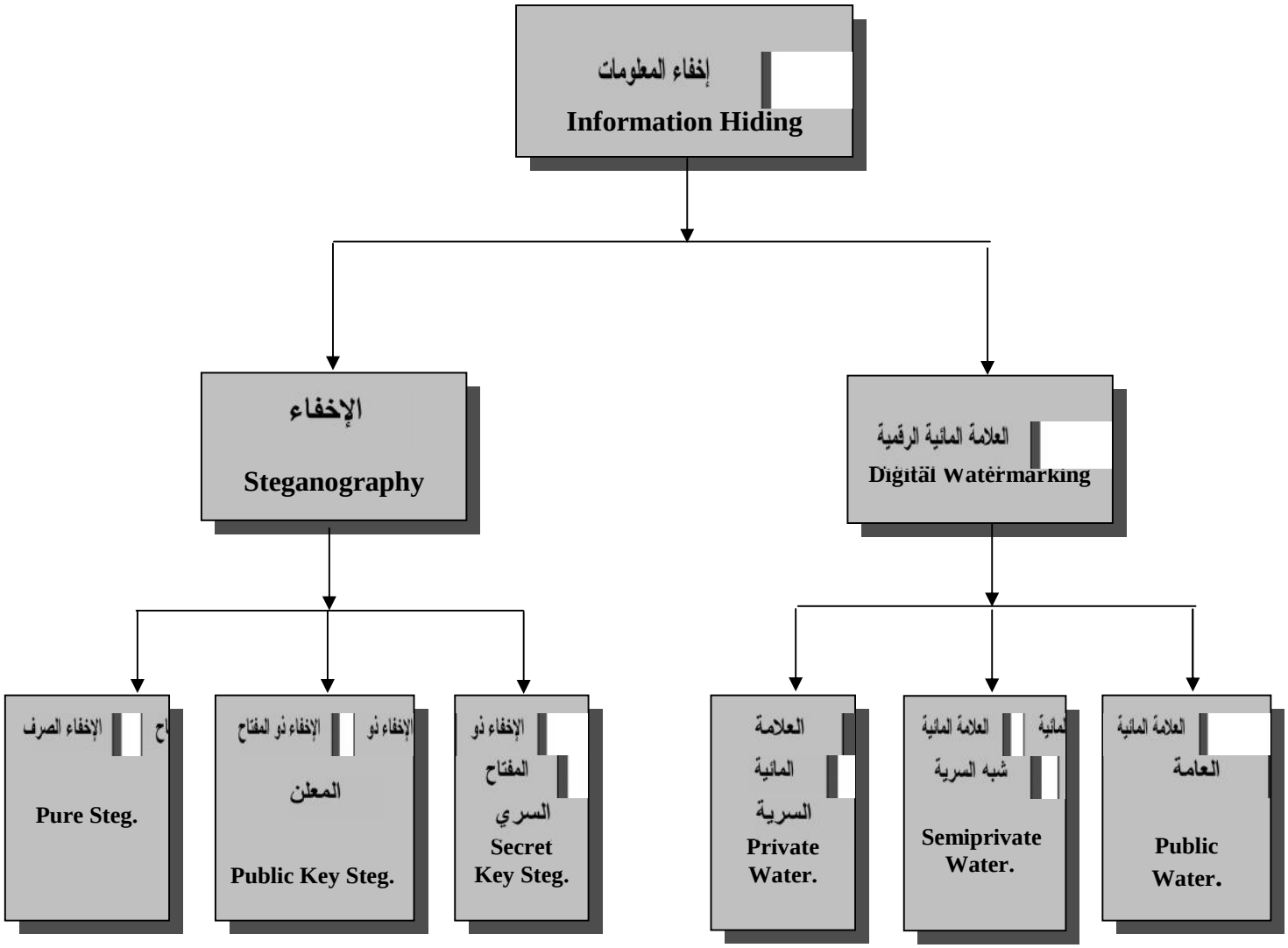
كما نجد في (**Tudor England**) عندما سجنت (**Mary**) ملكة (**Scots**) في قلعة (**Chartley**) أرسلت رسائل سرية إلى (**Catholics**) عن طريق إخفاء الحروف داخل براميل جعة فارغة [19].

كذلك يوجد نوع آخر شائع للكتابة المخفيــة باســتعمال الأحبــار الســرية **(Invisible Ink)** والمصادر الشائعة لها هي الحليب ،والـ ،وعصير الفواكه .حيث إنها تصبح عاتمة عندما تتعــرض للحرارة ومع التطور التكنولوجي تطورت هذه الأحبار و أصبحت اكثر تعقيــد ومقاومــة للتغيــرات الكيميائية [20] .

بصورة عامة يمكن تصنيف إخفاء المعلومات على نوعين رئيسيين هما :

- الإخفاء **(Steganography)** :- وهو علم وفن الاتصال بطريقة تخفي وجود الرسالة (هدف التنصت) داخل رســالة أخــرى أو أي وســط حامــل بحيــث لا يمكــن للعــدو اكتشــافها .إنّ الكلمـــة**(Steganography)**مشـــتقة مـــن الكلمتـــين الإغـــريقيتين **(Stegein)**و **(Grajein)** والترجمة الحرفية لها هي الكتابة المخفية **(Covered Writing)**.

- العلامة المائية الرقمية**(Digital Watermarking)** : -وتعنــي إخفــاء المعلومــات متعــددة إلهيات**(Multi Media Information)**ولكــن قــد تكــون مرئيــة(تحــول بعــض المعلومــات لتشكل صفة في الغطاء مثل حق النسخ **(Copyright)** أو تكون غير مرئيــة،و لا يمكــن إزالتهــا [20][21] و يوضح الشكل (1-1) التصنيف العام لاخفاء المعلومات .



يوضح الشكل (1-1) التصنيف العـــام لاخفـــاء المعـــلومات

1-4 أنواع الإخفاء (Steganography Types)

يقسم الإخفاء(**Steganography**) على ثلاث أنواع رئيسية :-

- الإخفاء الصرف (**Pure Steganography**)
- الإخفاء ذو المفتاح السري (**Secret Key Steganography**)
- الإخفاء ذو المفتاح المعلن (**Public Key Steganography**)

1-4-1 الإخفاء الصرف

يدعى نظام الإخفاء الذي لا يتطلب معلومات سرية مثل المفتاح السري (**Secret Key**) بنظام الإخفاء الصرف.يمكن وصف عملية الإخفاء(**Embedding Process**) بحسب العلاقة $E:C\times M\to C$ ،أمّا عملية الاسترجاع (**Extraction Process**) فتمثل بالعلاقة $D:C\to M$ ،حيث إنّ $|C|\geq|M|$ ويجب أن تكون خوارزمية الإخفاء والاسترجاع سرية بحيث يستطيع الوصول إلى المعلومات السرية إلا المرسل والمستلم فقط.

تعريف [20]

الرباعي (**Quadruple**) $\Im=\langle C,M,D,E\rangle$ ،حيث C هي مجموعة الغطاء وM هي مجموعة الرسائل السرية بحيث إن $|C|\geq|M|$ ودالة الإخفاء هي $E:C\times M\to C$.

في حين دالة الاسترجاع $D:C\to M$ مع خاصية $D(E(c,m))=m$ لكل $m\in M$ و $c\in C$ وهذا يسمى بالإخفاء الصرف .

1-4-2 الإخفاء ذو المفتاح السري

يدعى نظام الإخفاء الذي يعتمد في عملية الإخفاء على مفتاح سري(**Secret Key**) بنظام الإخفاء ذو المفتاح السري.يمتاز هذا النظام بأنه اكثر أمنية من نظام الإخفاء الصرف لانه يعتمد على مفتاح سري في عملية الإخفاء وهذا المفتاح يكون معروف من قبل المرسل والمستلم فقط ولا يستطيع أي شخص الحصول على المعلومات السرية مالم يعرف المفتاح السري ومن ثم فانه يحصل على معلومات مبهمة وقد تكون مشفرة على حين تعتمد أمنية نظام الإخفاء الصرف بصورة كلية على خوارزمية الإخفاء بحيث يجب أن تكون الصورة الناتجة بعد الإخفاء(**Stego-Image**)وصورة الغطاء الأصلية متشابهتين من ناحية النظر .

تعريف [20]

الرباعي (**Quadruple**) $\Im=\langle C,M,K,D_k,E_k\rangle$ ،إذ تمثل C مجموعة الغطاء،و M مجموعة الرسائل المراد إخفاؤها وإنّ $|C|\geq|M|$ وتمثل K مجموعة المفاتيح السرية وتمثل دالة الإخفاء بـ $E_k:C\times M\times K\to C$ ودالة الاسترجاع بـ $D_k:C\times M\times K\to C$ مع خاصية $D_k(E_k(c,m,k),k)=m$ لكل $m\in M$ و $c\in C$ وهذا يعرف بنظام الإخفاء ذي المفتاح السري .

3-4-1 الإخفاء ذو المفتاح المعلن

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

تعدُّ طريقة استعمال نظام التشفير ذي المفتاح المعلن أحدى طرائق بناء نظام إخفاء ذي مفتاح معلن ،إذ يستعظام الإخفاء ذو المفتاح المعلن الدالة **D** لاسترجاع الرسالة السرية التي تكون عبارة عن عناصر عشوائية **M** وهذا ما يعرف بالعشوائية الطبيعية(**Natural Randomness**)للغطاء.لبناء نظام إخفاء أمين يتم إخفاء النص المشفر بدلا من النص (الرسالة) الواضح [20] .

افترض (**Anderson**) بروتوكولا لنظام إخفاء ذي مفتاح معلن يعتمد على حقيقة أنّ المعلومات المشفرة تكون عشوائية ويمكن إخفاؤها في نص واضح [22] .

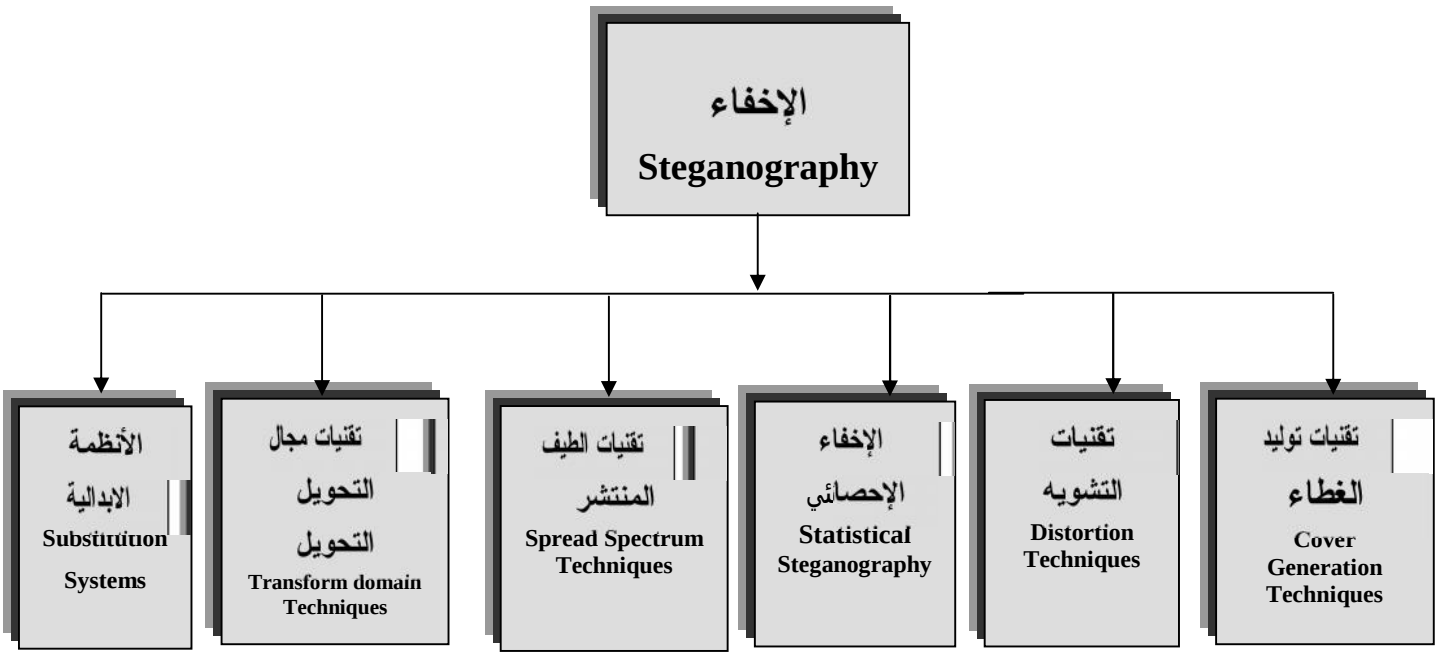
وقد وسع(**Craver**) هذا البروتوكول ليحاكي نظام الإخفاء الصرف مستعملا المفتاحين كليهما المعلن والسري .ففي عملية الإخفاء يفضل نظام الإخفاء الصرف في معظم ا لتطبيقات لانه لا يحتاج

إلى مفتاح سري مشترك بين طرفي الاتصال ولكنه لا يوفر أي أمنيه في حالة معرفة المهاجم لطريقة الإخفاء [23] .

1-5 تقنيات الإخفاء (Steganographic Techniques)

يوجد العديد من الطرائق المستخدمة لتصنيف أنظمة الإخفاء فمنها من يعتمد ن نو ع الغطـــاء المستعمل في الاتصالات السرية و أخرى تعتمد على إجراء تغيرات(تعديلات) في الغطاء المستعمل في عملية الإخفاء [20] .

يوضح الشكل (1- 2) التصنيف العام لتقنيات الإخفاء .



يوح الشكل (1-2) تصنيف تقنيات الاخفاء

وفيما يأتي هذه التقنيات بالتفصيل [20] .

1-5-1 الأ نظمة الابدالية(Substitution Systems)

توجد العديد من الطرائق التي تستعمل لاخفاء المعلومات وبهيات مختلفة،ابتداءا من طرائق حشر الثنائيات الأقل أهمية **LSB** (**Least Significant Bit**)وتسمى أيضا بمستوى الثنائية (**Bit Plane**) أو الضوضاء(**Noise**)إلى تغيير (تعديل) خصائص الصورة ..

تعد الأنظمة الابدالية من ابسط التقنيات المستعملة فإء المعلومات.فمنها من يستعمل الأجزاء الأقل أهمية من الغطاء لاخفاء ثنائيات الرسالة السرية،و يستطيع المستلم استرجاع الرسالة السرية من مواقعفاء،كذلك تمتاز هذه الطريقة إضافة إلى بساطتها بان المهاجم الخامل (**Passive Attacker**) لن يكتشفها،لأنها لا تسبب أي تشويه في الغطاء و إنما تعديلات طفيفة(بسيطة)في أجزاء غير مهمة من الغطاء .

تقسم الأنظمة الابدالية إلى ثمانٍ مجا ميع كما مبين في الشكل الآتي :

أ. إبدال الثنائيات الأقل أهمية(Least Significant Bit Substitution)

وتسمى أيضا بأدوات مستوى الثنائية (**Bit Plane Tools**) ومعالجة الضوضاء (**Noise**) وهذه الطرائق شائعة جدا وسهلة التطبيق ولا سيما مع الصور (**Image**) والصوت (**Audio**) ولكن المعلومات التي تخفى بوساطالطريقة يجب أن تكون قليلة لئلا يشعر بها .

توجد عدة أدوات(**Tools**) تستعمل ضمن هذه المجموعة منها (**S-Tools,Hide and Seek White Noise Storm**)و إنّ هيات الصور التي تستعمل يجب أن تكون من النوع الذي لا يحتوي على فقدان للبيانات (**Lossless**) ،كذلك فإنّ البيانات تخفى وتسترجع بصورة مباشرة . تطبق بعض هذه البرامج التشفير (**Encryption**) والضغط (**Compression**) قبل عملية الإخفاء لتوفير مستوى آخر من الحماية للبيانات المخفية .

تتضمن عملية الإخفاء اختيار مجموعة من عناصر الغطاء $\{j_1,...,j_{\ell(m)}\}$ لإنجاز عملية الإبدال $c_{ji} \leftrightarrow m_j$ عليها،حيث يتم إبدال الثنائيات الأقل أهمية (**LSB**) لعناصر الغطاء c_{ji} بثنائيات الرسالة السرية m_i (حيث m_i تكون أما 1 أو 0).في عملية الاسترجاع،يتم استرجاع الثنائيات الأق أهمية (**LSB**) لعناصر الغطاء المختارة لاعادة تكوين الرسالة السرية .

الجزء الآتي يوضح خوارزميتي الإخفاء و الاسترجاع [20]

Algorithm Embedding Process: Least Significant Bit Substitution

For i=1,…, $\ell(c)$ do

$s_i \leftarrow c_i$

End for

For i=1,…, do

Compute index j_i, where to store i-th message bit

$s_i \leftarrow c_i = m_i$

End for

Algorithm Extraction Process Least Significant Bit Substitution

For i=1,…, $\ell(m)$ do

Compute index j_i, where the i-th bit is stored

$$m_i \leftarrow LSB(c_{ij})$$

End for

ولاسترجاع الرسالة السرية يجب على المُلم أن يعرف مواقع الإخفاء(**سلسلة فهارس العناصر المستعملة في الإخفاء**)،وفي ابسط الحالات يتم إخفاء الرسالة في عناصر الغطاء ابتداءً من أول عنصر حتى انتهاء الرسالة،و بما أن طول الرسالة $\ell(M)$ يكون عادة اقل من طول عناصر الغطاء $\ell(c)$،فهذا يعني إن الرسالة تخفى في جزء من الغطاء على حين يبقى الجزء الآخر بدون تغيير وهذا يقود إلى مشكلة أمنية ،ة لان الجزء الأول(**الذي يحتوي على رسالة**)يختلف في خصائصه الاحصائيه عن الجزء الآخر(**الذي لا يحتوي على رسالة**) .

للتغلب على هذه المشكلة،فان بعض البرامج توسع حجم الرسالة السرية بإضافة ثنائيات عشوائية إلى رسالة لخلق تغيرات متساوية في بداية ونهاية الغطاء،ولكن هذه الطريقة تزيد من حجم التغيرات في الغطاء،زيادة على أنّ المواقع تكون متسلسلة وم المهاجم إذا بدا بأول عنصر في الغطاء يمكنه استرجاع الرسالة السرية. لذلك فقد استعملت طريقة اكثر تعقيدا من الطريقة السابقة هي توليد أرقام شبه عشوائية(**Pseudorandom Number Generator**) تستعمل كمواقع لاخفاء الرسالة السرية: الطريقة الشائعة هي طريقة الفترة العشوائية(**Random Interval Method**)ويمكن استعمال مفتاح سري يعد بذرة(**Seed**)لتوليد الرقم العشوائي،إذ يتم توليد سلسلة من الأرقام العشوائية $\{k_1,\ldots\ldots k_{\ell(m)}\}$.

الجزء الآتي يوضح خوارزميتي الإخفاء والاسترجاع :

Algorithm Embedding Process Random Interval Method

For i=1,…, $\ell(c)$ do

$s_i \leftarrow c_i$

End for

Generate random sequence k_1 using seed k

$n \leftarrow k_1$

For i=1,…, $\ell(M)$ do

$s_n \leftarrow c_n = m_i$

$n \leftarrow n + k_1$

End for

Algorithm Extraction Process Random Interval Method

Generate random sequence k_1 using seed k

$n \leftarrow k_1$

For i=1,…, $\ell(M)$ do

$m_i \leftarrow LSB(c_n)$

$n \leftarrow n + k_1$

End for

إذ إنّ المستلم يجب أنْ يعرف البذرة(**Seed**) ليستطيع توليد الأرقام العشوائية لاسترجاع الرسالة السرية .

ب. التباديل شبه العشوائية(Pseudorandom Permutations)

على الرغم مما تمتاز به طريقة الفترة العشوائية من الأمنية العالية والتعقيد بالنسبة للمهاجم

(لان ثنائيات الرسالة توزع على عناصر الغطاء بصورة عشوائية وبالاعتماد على مفتاح سري

وليس بصورة متسلسلة، حيث إن المسافة بين كل (bit 2) تحدد بصورة عشوائية)،فإنها تعاني من مشكلة التكرار **(Collision)** أي ظهور نفس الفهرس اكثر من مرة في سلسلة الأرقام المولدة وهذا يعني إخفاء اكثر من ثنائية من الرسالة بنفس الموقع **(الفهرس)** وهذا يؤدي إلى فقدان بعض ثنائيات الرسالة،لان مخرجات المولد شبه العشوائي لا يمكن التحكم بها أو السيطرة عليها .

للتغلب على هذه المشكلة،يتم توليد المواقع بطريقة عشوائية وفي كل مرة يولد فيها موقع يختبر مع المواقع المولدة سابقا فإذا كانا غير موجود

فإنه يستعمل لاة من الرسالة و إلا فانه يولد رقم جديد وهكذا.ولاسترجاع الرسالة يتم توليد المواقع بنفس الطريقة .

كما قدم **Aura** [24] طريقة أخرى للتغلب على هذه المشكلة وذلك عن طريق حساب التباديل شبه العشوائية لمجموعة عناصر الغطاء $\{1, \ldots, \ell(c)\}$.حيث افترض أنّ العدد $\ell(c)$ يمكن أن يُعبرَ عنه بحاصل ضرب العددين X, Y واستعمال دالة تشفير عشوائية h_k تعتمد على مفتاح k الذي يجزأ إلى ثلاثة مفاتيح سرية k_1, k_2, k_3 .

الخوارزمية الآتية توضح الطريقة :

Algorithm Computing the index j_i using pseudorandom permutation

$v \leftarrow i \quad div \quad X$

$u \leftarrow i \mod X$

$v \leftarrow (v + h_{k1}(u)) \mod Y$

$u \leftarrow (u + h_{k2}(v)) \mod X$

$v \leftarrow (v + h_{k3}(u)) \mod Y$

$j_i \leftarrow vX + u$

تولد الخوارزمية أعلاه أرقام مختلفة j_i لكل مدخل i حيث $\{1 \le i \le XY\}$ (أي عبارة عن تباديل شبه عشوائية للمجموعة $\{1,\ldots, \ell(i)\}$ ويُجزأ المفتاح k إلى ثلاثة مفاتيح k_1, k_2, k_3 .في عملية الإخفاء،يتم إخفاء ثة الرسالة i-th في عنصر الغطاء ذي الفهرس j_i الذي يحسب تبعا للخوارزمية اعلاه . ولاسترجاع ثنائيات الرسالة السرية فإنّ المستلم يجب أن يعرف

المفاتيح k_1, k_2, k_3. بالرغم من أنّ هذه الطريقة قد تغلبت على شكلة التكرار **(لأنها لا تعطي فهارس متكررة)** إلا أنهّا تحتاج إلى وقت احتساب كبير.بسبب دالة hash التي تحتاج إلى وقت يعادل ثلاثة أضعاف طول الرسالة $\ell(M)$.

ج. تشويه الصور و قنوات الغطاء (Image Downgrading and Cover Channels)

وهي حالة خاصة من الأنظمة الابدالية ، تستعمل لاخفاء صورة داخل صورة أخرى وبنفس الحجم ، حيثستعمل الثنائيات الأربع الأقل أهمية من صورة الغطاء **(رمادية التدرج أو الملونة)** بالبع الأكثر أهمية من الصورة السرية.ولاسترجاع الصورة السرية ،تستخلص الثنائيات الأقل أهمية من الصورة الحاملة للصورة السرية **(Stego-Image)**.في العديد من الحالات، نجد أنّ إرسال أربع ثنائيات فقط من الصورة السرية كافية تقريبا.

في هذه الطريقة يكون تشوه الغطاء كبير بالرغم من أنه نظريا يكون غير ملحوظ ولكنه في التطبيق العملي يكون غير ذلك .

د. مناطق الغطاء و ثنائيات التطابق (Cover Regions and Parity Bits)

يمكن أن نعرف أي مجموعة جزئية غير فارغة $\{c_1,....,c_{\ell(C)}\}$ بمنطقة الغطاء(**Cover Region**).يقسم الغطاء على عدة مناطق مختلفة،ثم يتم إخفاء ثنائية واحدة من المعلومات السرية في كل منطقة بدل من كل عنصر،إذ تستعمل ثنائية التطبق**(Parity Bit)**من كل منطقة في عملية الإخفاء. يمكن حساب ثنائية التطابق كما يأتي :

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

في عملية الإخفاء يتم اختيار مناطق الغطاء I_i بحيث تكـــون $(1 \le i \le \ell(m))$ ويمثـــل $\ell(m)$ طول الثنائيات المراد إخفاؤها،حيث يتم إخفاء الثنائية السرية m_i في ثنائية المطابقة $b(I_i)$ فإذا كانت الأخيرة لا تتطابق ة السرية يتم إبدالها بالـــ m_i .أمّا في عملية الاسترجاع فيتم اســـتخلاص ثنائياتتطابق لكل منطقة مختارة لاعادة تكوين الرسالة .

و يمكن أيضا استعمال طريقة شبه عشوائية في اختيار مناطق الغطاء وبالاعتماد على مفتاح سري .

هـــ. صور معتمدة على لوحة الألوان(Based Images Palette)

توجد طريقتان لاخفاء المعلومات في الصور المعتمدة على لوحة الألان هما: أما الإخفاء في لوحة الألوان **(Palette)** و الإخفاء في بيانات الصورة **(Image Data)** .

تخفى المعلومات السرية في الثنائيات الأقـــل أهميـــة لمتجهـــات الألـــوان**(Color Vectors)** باستعمال طرق الإبدال**(Substitution Methods)** وبدون الحاجة إلى ترتيـــب لوحـــة الألـــوان **(Palette)** .

يوجد **N!** من الطرائق المختلفة التي تستعمل لترتيب لوحة الألوان وهي تكفي لاخفاء رســـالة صغيرة،ولكن كل الطرائق التي تعتمد في عملية الإخفاء على ترتيب لوحـــة الألـــوان تكـــون غيـــر حصينة،لان المهاجم يستطيع وببساطة أن يرب المداخل**(Entries)** بطريقة مختلفة ويدمر الرسالة .

كبديل يتم إخفاء المعلومات السرية في بيانات الصورة **(Image Data)**،ولكي تكـــون عمليـــة الإخفاء ناجحة فإن القيم اللونية المتجاورة يجب أن تكون متشابهة أو متقاربة،حيث ترتب لوحة الألوان قبل عملية الإخفاء.فمثلا ترتب قيم الألوان تبعا للمسافة الاقليدية **(Euclidian Distance)** لفضـــاء **RGB (RGB Space)** :

$$D = \sqrt{R^2 + G^2 + B^2} \qquad (1-7)$$

وبما أنّ نظام الرؤيا البشري (HVS) يكون اكثر تحسس (تأثر)بتغيرات شدة الإضاءة (The Luminance of a color) فإنّ ترتيب لوحة الألوان تبعا لشدة الإضاءة يعطي نتائج افضل.

وقد اقترح Fridrich [13] طريقة مختلفة قليلا لا تحتاج إلى ترتيب لوحة الألوان،حيث يحسب مجموعة الألوان القريبة لكل عنصر و يبدأ بأقرب لون،حيث يجد المرسل ثاني اقرب لون له تكون ثنائية تطابق له (R + G +B Mod 2)مساوية إلى الثنائية السرية المراد إخفاؤها.فيبدل هذا العنصر باللون الجديد .

هناك طريقة أخرى تعتمد على تقليص العدد الكلي لقيم ألوان الصورة إلى [N/2] باستعمال بعض طرائق الاهتياج(Dithering Method)ومضاعفة مداخل لوحة الألوان،لذلك فإنّ كل المداخل المضاعفة تتغير قليلا.بعد هذه المعالجة الأولية فإنّ كل لون من الصورة الناتجة من عملية الاهتياج (Dithering Image)تقابل مدخلين من لوحة الألوان من أي واحدة تختار تبعا لثنائية الرسالة السرية.

و. التكمية والاهتياج(Quantization and Dithering)

تستعمل عمليات التكمية والاهتياج لاخفاء المعلومات السرية في الصور الرمية.تعمل بعض أنظمة الإخفاء على الصور المكماة (Quantized Images)، حيث يتم حساب الفرق e_i بين العناصر المتجاورة x_i و x_{i+1} ثم يدخل إلى المكمم Q (Quantizer) لينتج تقريبات متقطعة Δ_i لاشارة الفرق(Deference Signal) $x_i - x_{i-1}$.

لغرض الإخفاء،يستعمل خطا التكمية(Quantization Error)في مقطع الترميز التنبؤي PCS (Predictive Coding Scheme) ولا سيما عند تعديل إشارة الفرق Δ_i لإرسال

معلومات اضافيه،حيث يتكون مفتاح الإخفاء(**Stego –Key**)من جدول يسند ثنائية خاصة لكل قيمة ممكنه Δ_i .

لاجل إخفاء ثنائية الرسالة i-th في إشارة الغطاء،يتم حساب إشارة الفرق المكممة Δ_i فإذا كانت لا تتطابق(**تبعا إلى الجدول السري**)مع الثنائية السرية المراد إخفاؤها،حيث يبدل Δ_i بأقرب Δ_i ،تكون الثنائية المرافقة له مساوية إلى ثنائية الرسالة السرية والقيم الناتجة Δ_i تدخل إلى (**Entropy Coder**) .على الجانب الآخر فإنّ المستلم يستطيع استرجاع الرسالة عن طريق حساب إشارة الفرق Δ_i ومفتاح الإخفاء(**Stego – Key**).

ز. إخفاء المعلومات في الصور الثنائيه

(Information Hiding in Binary Images)

تحتوي الصور الثنائيه(**Binary Images**)على تكرارات من العناصر البيضاء والسوداء. و على الرغم من إمكانية تطبيق عملية الإبدال البسيطة عليها إلا أنها تتأثر بصورة كبيره بأخطاء الإرسال لذلك تكون غير حصينة .

تقسم الصور الثنائيه إلى قطاعات(**Blocks**) مستطيلة B_{ij} لتكن$P_0(B_i)$ هي النسبة المئوية للعناصر السودلي قطاع الصورة B_{ij} و$P_1(B_i)$ هي النسبة المئوية للعناصر البيضاء.بصورة عامه يتم إخفاء 1 في قطاع واحد إذا كانت($P_1(B_i) > 0.50$) و 0 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 الثنائيه ذات التباين الحاد تنجز التغيت على حدود العناصر البيضاء والسوداء لكي تكون غير محسوسة .

ح. الفضاء غير المستعمل أو الاحتياطي في أنظمة الحاسبات

Unused or Reserved Space in Computer Systems

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

طريقة أخرى لاخفاء المعلومات في نظام الملف(**File System**) هو خلق أجزاء مخفيه،حيث تكون غير مرئية إذا كان النظام يعمل بصورة طبيعية.

1-5-2 تقنيات مجال التحويل Transform Domain Techniques

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

على أية حال فهي اكثر مقاومة لأنواع مختلفة من معالجات الإشارة زيادة على أنّ 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 هنالك موازنة بين كمية المعلو، المضافة إلى الصورة(**المعلومات المخفيه**)والتحصين الذي يتم الحصول عليه،كما إنّ بعض طرائق مجال التحويل لا تعتمد على هيأة الصورة(**Image Format**).

1-5-2 الطيف المنتشر و إخفاء المعلومات

(Spread Spectrum and Information Hiding)

طورت تكنولوجيا الطيف المنتشر **SS (Spread Spectrum)** منذ عـام **1950** كمحاولـة لتوفير وسائل الاتصالات باحتمالية واطئه للجزء المدوغير المضغوط.يمكن تعريـف تقنيـات الطيف المنتشر بأنها وسائل إرسال بحيث تكون الإشارة محصورة بمـدى يتجـاوز الحـد الأدنـى الضروري(المقبول)لإرسال المعلومات،انتشار الحزمة يتم الحصول عليه بوسئل الشفرة التي تكـون مستقلة عن البيانات، ويتزامن مع الشفرة في الاستلام التي استعملت من اجل تجميع سلسلة البيانـات المسترجعة.على الرغم من أنّ طاقة الإشارة المرسلة تكون كبيرة فإن نسبة الإشارة إلـى الضوضـاء **SNR (The Signal to– Noise ratio)** في كل مدى ترددي تكون صغيرة.حتى في حالة حذف أجزاء من الإشارة في بعض المجالات(النطاقات)الترددية.فإنّ المعلومات الموجـودة فـي النطاقـات الأخرى تكون كافيه لاسترجاع الإشارة،وهذا مشابه لنظام الإخفاء الذي يحاول نشر الرسالة السـرية على كل الغطاء لتبدو غير محسوسـة،وبمان نشـر(توزيـع) الإشـارات يكـاد يكـون صـعب الحذف(الإزالة)فإنّ عملية الإخفاء التي تعتمد على(SS)تعطي مستوى عاليا من التحصين .

يوجد نوعان مختلفان من الـ **SS** يستعملان في إخفاء المعلومات: السلسلة المباشرة **(Direct Sequence)** والوثـب التـرددي(**Frequency – hopping**).فـي السلسـلة المباشـرة،يتم نشر(توزيع)الرسالة السرية بوساطة ثابت يسمى معدل القطعة**(Chip Rate)**،لنمذجة الإشـارة شـبه العشوائيتضاف إلى الغطاء.أمّا في الوثب الترددي فإنّ تردد الإشارة الحاملة يتغير بطريقـة قفـز سريع من تردد إلى آخر.يستعمل الـSS بصورة واسعة في سياق العلامة المائيـة **(Context of Watermarking)**.

4-5-1 الإخفاء الإحصائي (Statistical Steganography)

تستعمل تقنيات الإخفاء الإحصائية (1 bit) لاخفاء ثنائية واحدة من المعلومات في الحامل الرقمي، وذلك بتغيير الخصائص الإحلغطاء إذا تم إرسال "1" و إلا فإنّ الغطاء يبقى بدون تغيير،و إنّ المستلم يجب أن يكون قادرا على التمييز بين الأجزاء المعدلة من الأجزاء التي لم يطرأ عليها تعديل .

ولتركيب(بناء) نظام إخفاء $\ell(m)$ من الثنائيات من تعدد أنظمة إخفاء(1 bit)،تقسم الغطاء إلى $\ell(m)$ من القطاعات المختلفة $\{B_1,...,B_{\ell(m)}\}$.ولحشر الثنائية السرية m_i في القطاع i-th يتم إحلال "1" في B_i إذا كانت $(m_i=1)$ و إلا فإنّ القطاع يبقى من دون تغيير.ولاسترجاع الثنائية السرية تستعمل .الة اختبار(Test Function)لتمييز القطاعات المعدلة عن القطاعات غير المعدلة.

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

تعدُّ الدالة f دالة اختبار الفرضية (Hypothesis-Testing Function) لاختبار فرضية العدم(Null-Hypothesis) "القطاع لم يتغير" وإلا فإنّ 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 يوجدَ افضل اختبار إحصائي للتمييز بين قطاعات الغطاء المعدلة وغير المعدلة ،زيادة على أن التوزيع يجب أن يكون طبيعي، وتعد مهمة تحقيق هذه الشروط عملية صعبة الحصول .

1-5-5 تقنيات التشويه (Distortion Techniques)

تختلف تقنيات التشويه عن تقنيات الإبدال بأنها تتطلب وجود الغطـــاء الأصـــلي(**Original Cover**) في عملية الاسترجاع،تتضمن عملية الإخفاء سلسلة من التغيرات التي تنجز علـــى الغطـــاء وهذه التغيرات تمثل (تقابل) الرسالة السرية المراد إرسالها .أمّا في عملية الاسترجاع فـــإنّ المســـتلم يحسب الفرق بين الوسط الحامل (الغطاء) للرسالة والغطاء الأصلي من أجل استرجاع سلسلة التغيرات التي طبقت من قبل المرسل والتي تقابل (تمثل) الرسالة السرية .في العديد من التطبيقات نجد أنّ مثـــل هذه الأنظمة غير مفيدة ، لأنّ المستلم يجب أن يعرف الغطاء الأصلي لطيع استرجاع الرسالة.فـــإذا استطاع المهاجم أن يصل إليها.فإنه سوف يكتشف التغيرات التي طرأت على الغطاء وبعد ذلك يحصل على الرسالة السرية .

كذلك في حالـــة كـــون دوال الإخفـــاء والاســـترجاع (**Embedding and Extraction Functions**) معلنة (**Public**) ولا تعتمد على مفتاح سري(**Stego-Key**) فإنها تكون سهلة الكســـر من قبل المهاجم وبعد ذلك يستطيع استرجاع الرسالة السرية بصورة كلية .

1-5-6 تقنيات توليد الغطاء (Cover Generation Techniques)

تختلف هذه الت عن كل الطرق السابقة .فمن اجل إضافة معلومـــات ســـرية إلـــى غطـــاء خاص،بتطبيق خوارمية إخفاء تقوم بعض تطبيقات الإخفاء بتوليد كيان(غطاء-وسط) رقمي(**Digital Object**) فقط لغرض جعله غطاءً لاخفاء المعلومات .

1-6 متطلبات نظام الإخفاء (Requirements of Steganography System)

توجد مجموعة من الصفات أو المتطلبات التي يجب توافرها في أي نظام إخفـاء هـي [25] [26]:

1-التحصين Robustness

2-عدم القدرة على الاكتشاف Undetectability

3-عدم الرؤيا أو غير مرئي Invisibility

4-السرية Security

5- السعة Capacity

وفيما يأتي توضيح(تعريف) للمفاهيم المذكورة آنفا :

1-6-1 التحصين Robustness

تدعى المعلوت المخفية بأنها محصنة في حالة كون بقاؤها أمينة عند إجراء تعـديلات علـى صورة الغطاء و أو التشويه بعـد التمييـز.علـى سـبيل المثـال، المرشـحات الخطيـة اللاخطية **Linear and Nonlinear Filtering** (مثل مرشحات الحـدة والوسـيط) ،الضـغط الحاوي على فقدان للبيانات **Lossy Compression** و التقيـيس **Scaling** والتـدوير **Rotation** وإضافة الضوضاء **Noise Adding** وتكميم اللون **Color Quantization** وغيرها [26].

2-6-1 عدم القدرة على الاكتشاف Undetectability

تمثل هذه الخاصية المثالي لأي نظام اتصال أمين.نقول أن المعلومات المخفية لا يمكن اكتشافها إذا كانت تشكل مع صورة الغطاء نموذجا متماسكا(**متلائم**).على سبيل المثـال،إذا اسـتعملت

مكونات(**أجزاء**) الضوضاء للصور الرقمية لإخفاء المعلومات المهمة فإنّ هذا لا يؤدي إلى تغيير كبير و مهم في الخصائص الإحصائية للصورة لذا فإن مفهوم عدم القدرة على الاكتشاف(**Undetectability**) يرتبط مع النموذج الإحصائي لمصدر الصورة.فإذا كان للمهاجم معرفة تفصيلية بمصدر الصورة فإنه سوف يكتشف رسالة مخفية فيها.ولكنّ قدرة اكتشاف وجود الرسالة لا يعني إمكانية قراءة الرسالة [26].

1-6-3 عدم الرؤيا Invisibility

يعتمد هذا المفهوم على خصائص نظام الرؤيو السمع البشري(**Human Visual or Audio System**).تكون المعلومات غير محسوسة(**مدركة**) إذا كان معدل الأشخاص (**Average Human Subject**) 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 تحتو على معلومات مخفية.وكانت نسبة النجاح قريبة من 50% ،أثبتت أنّ هؤلاء الأشخاص غير قادرين على التمييز بين الصور الأصلية والحاوية على معلومات مخفية [26].

1-6-4 السرية Security

إنّ خوارزمية الإخفاء أمينة إذا كانت المعلومات المخفية غير قابلة للإزالة(**الحذف**) بعد اكتشافها من قبل المهاجم اعتمادا على المعرفة الكاملة بخوارزمية الإخفاء والمفتاح السري [26] .

1-6-5 السعة Capacity

تتنافس المتطلبات المذكورة آنفاً بالتبادل ولكنها لا تستطيع الوصول إلى حالة الأمثلية بنفس الوقت. فلإخفاء رسالة كبيرة داخل أي صورة فإننا لا نشرط الحصانة الكبيرة وعدم الاكتشاف المطلق.أي أنّ الاتفاق المعقول هو بحسب الحاجة أو الضرورة فالحاجة إلى التحصين تعني أنّ الرسالة يجب أن تكون صغيرة حتى لا تؤدي إلى تشوه الوسط الغطاء [26].

1-7 أدوات الإخفاء Steganography Tools

يحتوي الاعلى العديد من الأدوات(الخوارزميات) لإخفاء المعلومات في ملفات الصور الرقمية وملفات الصوت من بينها [21][27]:

- **S-Tools by Andy Brown:** –تخفى البيانات في الثنائيات الأقل أهمية(**LSB**) لملفات الصوت (**Wave .**) أو ملفات الصور هيأة (**BMP or GIF**).وقد استعملت المناطق غير المستعملة من الأقراص (**Diskettes**) لإخفاء البيانات.وقد استعملت طرائق تشفير منها(**DES,IDEA**) لتشفير البيانات السرية.
- **Hide and Seek by Colin Maroney:**–تخفى البيانات في ملفات صور هيأة (**GIF**) وبحجم 320×320 عنصرا حد أدنى،أمّا في حالة كون حجم الصورة أصغر فإنّ جانبي الصورة تضلل بمساحات سوداء وباستعمال الثنائيات أقل أهمية(**LSB**) من كل عنصر في الصورة لإخفاء المعلومات السرية.
- **StegoDos by Black Wolf:**–تخفى الرسائل باستعمال الثنائيات الأقل أهمية (**LSB**) لفايلات الصور ذات التدرجات الرمادية والملونة التي بحجم 320×200 وذات(**256**) لونا،وتعد أقل نجاحا نسبة إلى بقية الأدوات.
- **White Noise Storm by Arsen Arachelian:**–صمم معتمدا في فكرته على تكنولوجيا الطيف المنتشر(**Spread Spectrum**) والوثب الترددي(**Frequency**

Hopping)،إذ تبعثر الرسالة خلال الصور (**مشابه إلى DES**) بعد أن تشفر باستعمال طرائق التشفير يتم إخفاؤها في الثنائيات الأقل أهمية من صورة الغطاء.

1-8 طرائق الإخفاء (Methods for Hiding Information)

أعطى الهجوم على تكنو الحاسبات والانترنيت حياة جديدة للإخفاء وإلى ظهور طرائق جديدة . تؤدي تقنيات الإخفاء إلى تغيرات في الوسط الحامل نتيجة لإخفاء المعلومات ولكن هذه التغيرات تكون غير محسوسة . فمنذ عام **1950** بدء الاهتمام بطرق و أدوات الإخفاء (**Steganographic Methods and Tools**) التي تطبق في الوسط الرقمي(**Digital Media**).

توجد مجموعة من الطرائق التي تستعمل لإرسال رسالة سرية بطريقة لا تشعر العدو بوجودها ،ويمكن استعمال الصوت(**Audio**)، والنص (**Text**)، وفضاء القرص (**Disk Space**) ،والصور (**Images**) والفيديو (**Video**) أو أي تمثيل رقمي،وهذه تمثل افضل الأوساط الحاملة التي يمكن استعمالها [21].

1-9 الإخفاء في الصور الرقمية Hiding in Digital Images

توجد عدة طرائق لإخفاء ومات في الصور الرقمية.فمنها من يستعمل مناطق الضوضاء (**Noise Areas**) لإخفاء ثنائيات الرسالة أو المعلومات المهمة أما بصورة متسلسلة أو تبعثر بصورة عشوائية خلال صورة الغطاء،ومنها من يستعمل التقنيع والترشيح (**Masking and Filtering**) و كذلك استعمال التحويلات(**Transformations**).وكل واحدة منها تطبق بدرجات مختلفة من النجاح لهيأت مختلفة من الصور.وقد كانت أفضل النتائج للصور ذات التدرجات الرمادية(**256**) لونا ،لأنها ـات تدريجية في الشدة اللونية(**Intensity**) بين العناصر وهذا يجعل التشويه الناتج من عملية الإخفاء قلإقد يكون غير مرئي(**معدوم**).وتعدُّ الصور ذات التباينات(**التدرجات**) اللونية القليلة (الصغيرة) ذات فعالية كبيرة [21] .

1-9-1 حشر الثنائيات الأقل أهمية Least Significant Bit

تعدُّ طريقة (**LSB**) من الطرائق البسيطة والشائعة الاستعمال.تخفى المعلومات داخل(**LSB**) لصورة الغطاء.فإذا كانت الصورة طبيعية فإنّ كلّ عنصرٍ يتكون من ثلاث ثمانيات وهذا يعني وجود ثلاث ثنائيات تسل لإخفاء المعلومات.أمّا الصور الملونة(**256**) فإنّ كل عنصر يتكون من ثمانية واحدة (**أي توجد ثنائية واحدة تستعمل لإخفاء المعلومات**).

كذلك يمكن استعمال الضغط(**Compression**) لضغط المعلومات المراد إخفاؤها لإخفاء أكبر كمية ممكنة من المعلومات.إذ يجب أن تكون الصورة الناتجة بعد الإخفاء(**Stego-Image**)متماثلة مع صورة الغطاء الأصلية(**Original Image**) [28].

2-9-1 الاقنعة والمرشحات Masking and Filtering

تستعمل تقنيات التقنيع والترشيح بصورة واسعة مع الصور ذات التدرجات الرمادية والطبيعية.تخفى المعلومات باسلوب مشابه إلى العلامة المائية(**Watermarking**) .وفي بعض الأحيان تستعمل كعلامة مائية رقمية(**Digital Watermarking**).يحدث في الصور الناتجة من عملية التقنيع(**Masking Images**) تغيير في الشدة الضوئية(**Luminance**) لمنطقة القناع (**Mask Area**) إن التغيير الصغير يقلل من فرصة اكتشافها.

تعدُّ تقنية التقنيع من الطرائق المحصنة (**Robust**) نسبة إلى طريقة حشر(**LSB**)،لأن المعلومات تخفى في مناطق مهمة من الصورة بدلا من مستوى الضوضاء(**Noise Level**) [29] .

3-9-1 الخوارزميات والتحويلات Algorithms and Transformation

بالرغم من أنّ طريقة(**LSB**) سهلة وسريعة إلا أنها سهلة الكسر،بسبب تغيير بسيط ناتج عن أي معالجة للصورة(**Image Process**) أو أي عملية ضغط.إن عملية الضغط تعطي هيأة جديدة للصورة،حيث تخزن الصورة في فايل صغير نسبيا باستعمال طرائق ضغط **JPEG** (**JPEG Compression Methods**) .يستعمل تحويل جيب التمام المتقطع (**Discrete Cosine Transform**) في عملية الضغط للحصول على صور **JPEG** .إنّ هذا التحويل هو من نوع الضغط الحاوي على فقدان للبيانات (**Lossy Compression**)،بسبب عملية التكمية (**Quantization**) .

زيادة على تحويل يب التمام المتقطع (**DCT**) يوجد تحويلات أخرى منها تحويل فور يـر السريع **FFT** (**Fast Fourier Transform**) والتحويل المويجي **WT** (**Wavelet Transform**) [27] .

و توجد بعض الطرائق التي تعتمد في عملية الإخفاء على بعض خصائص الصورة منها :

- **Patchwork**

تسمى الطرائق الإحصائية بالـ **Patchwork** وتعتمد على العمليات الإحصائية و الشبه عشوائية.تكون عملية الإخفاء غير مرئية،حيث تعتمد على صفة إحصائية لصورة الغطاء (**Host Image**) .إن هذه الطريقة تتضمن معالجة مجموعة من النقاط بدلا من نقة واحدة.كذلك تكون حصينة ولا سيما عند استعمال (**Affine Coding**) ، وبعض المعالجات المعتمدة على تمييز الصفات (**Feature Recognition**).لكن كمية البيانات تكون قليلة وهي مفيدة في تطبيقات العلامة المائيـة الرقمية [7] .

- **Texture Block Coding**

تتضمن تقنية (**Texture Block Coding**) نسخ(نقل) منطقة ذات نمط نسيجي عشوائي في صورة إلى منطقة أخرى لها نفس النسيج.وهذا ينتج أزواج من المناطق النسيجية المتماثلة.

تحدد المناطق كما يأتي :

1-حساب الارتباط الذاتي(**Autocorrelation**) للصورة مع نفسها.وهذا ينتج قمم في كل نقطة عندما تتداخل المناطق المتماثلة للصورة.

2-إزاحة الصورة المشار إليها بالقمم في الخطوة (**1**).طرح الصورة من النسخة المزاحة،جعل الحواف مساوية إلى صفر عند الحاجة.

3-تربيع النتائج واستعمال عتبة(**Threshold**) لاسترجاع القيم القريبة جدا من الصفر فقط [7].

1-10 مقاييس الموثوقية Fidelity Criteria

توجد مجموعة من المعايير القياسية التي تستعمل لتقييم إنجازيه أي طريقة(نظام) إخفاء لتحديد مدى سريتها،أمنيتها وفعاليتها في إخفاء البيانات [30] .

تقسم هذه المقاييس على فئتين أساسيتين :

1-10-1 مقاييس الموثوقية الهدف Object Fidelity Criteria's

يستعمل هذا المقياس معادلات لقياس نسبة الخطأ بين الصورة الأصلية(**Original Image**) و الصورة الناتجة(المسترجعة) ومن هذه المقاييس [31] [32]:

أ. الجذر التربيعي لمعدل مربعات الخطأ **Root Mean Square Error**

يمكن أن نعرف الفرق الكلي بين قيم عناصر الصورة الأصلية وقيم الصورة الناتجة بحسب المعادلــة

الآتية :

$$\text{Total Error} = \sum_{x=0}^{N-1}\sum_{y=0}^{M-1}\left[\tilde{I}(x,y) - I(x,y)\right] \qquad (1-9)$$

إذ إنّ $I(x,y)$ تمثل الصورة المدخلة ذات أبعاد (N,M) و $\tilde{I}(x,y)$ تمثل الصورة الناتجــة . و

يحسب الجذر التربيعي لمعدل مربات الخطأ**(RMSE)** وفقا للمعادلة الآتية :

$$\text{RMSE} = \sqrt{\frac{\sum_{x=0}^{N-1}\sum_{y=0}^{M-1}\left[\tilde{I}(x,y) - I(x,y)\right]^2}{(N \times M)}} \qquad (1-10)$$

فكلما قلت قيمة**(RMSE)** كلما كانت الصورة المسترجعة ذات نوعية جيدة .

ب. نسبة الإشارة إلى الضوضاء **Signal to Noise Ratio**

تعد نسبة الإشارة إلى الضوضاء المقياس الأكثر استعمالا لقياس نسبة مربعات الخطأ إلى كميــة

الضوضاء في الصور الأصلية–المسترجعة،إذ إنّ الصورة المسترجعة تمثل الإشارة ويعد الفرق بــين

الصورتين الأصلية والمسترجعة الضوضاء وبحسب المعادلة التالية [31][32]:

$$\text{SNR} = \sqrt{\frac{\sum_{x=0}^{N-1}\sum_{y=0}^{M-1}\left[\tilde{I}(x,y)\right]^2}{\sum_{x=0}^{N-1}\sum_{y=0}^{M-1}\left[\tilde{I}(x,y) - I(x,y)\right]^2}} \qquad (1-11)$$

ومن المقاييس الشائعة الاستعمال هو مقياس نسبة قمة الإشارة إلى الضوضاء **Peak) PSNR**

(Signal to Noise Ratio ويعرف بحسب المعادلة الآتية :

$$\text{PSNR} = 10\log_{10}\frac{(L-1)^2}{\frac{1}{(N \times M)} \times \sum_{x=0}^{N-1}\sum_{y=0}^{M-1}\left[\tilde{I}(x,y) - I(x,y)\right]^2} \qquad (1-12)$$

حيث تمثل L عدد المستويات (**Levels**) في الصورة، فإذا كانت عدد الثنائيات يساوي (**8**) فإن (L=256) .

1-10-2 مقياس الموثوقية الشخصي **Subjective Fidelity Criteria**

تعد مقاييس الموثوقية الشخصية وسائل بسيطة لتقييم كمية المعلوماتفودة في الصورة أو مدى الفرق بين الصوالأصلية والمسترجعة.حيث تقيم الصور الناتجة(المسترجعة) من قبل نظام الرؤيا لدى الإنسان (**HVS**). ومن المعروف أن نظام الرؤيا البشري له خواص مميزة،لذا فإن تقييم نوعية الصور باستعمال مقياس الموثوقية الشخصي يكون أكثر ملائمة،حيث تعرضلصور على مجموعة من الناظرين ثم يأخذ معدل التقييم [26].

1-11 الهدف من الرسالة

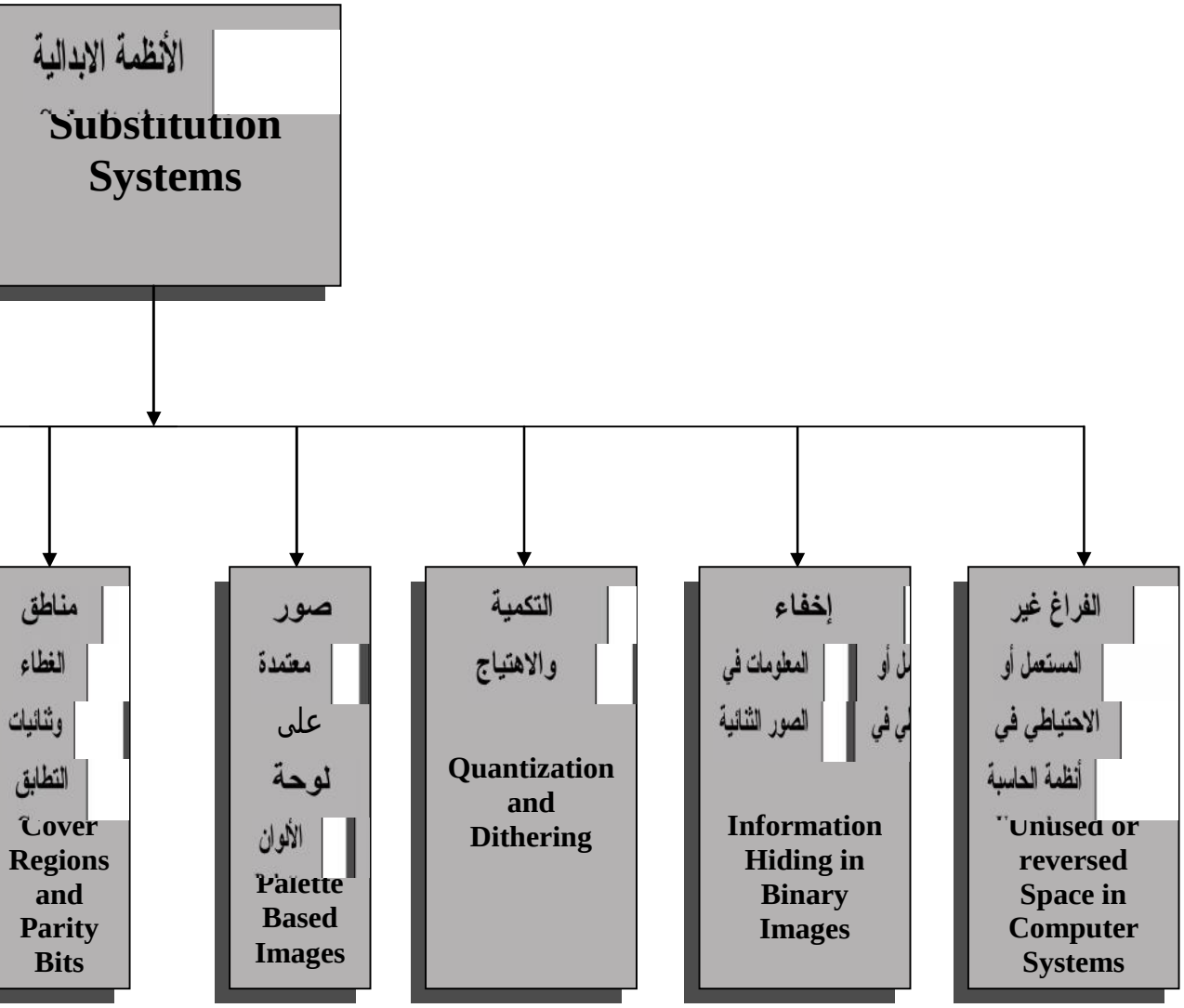
يهدف البحث إلى إخفاء صورة ذات تدرجات لونية مختلفة وبدرجات تعقيد مختلفة داخل صورة أخرى لها نفس الحجم ،وقد تضمن النظام المقترح تنفيذ خمس طرائق إخفاءكل طريقة لها مجموعة من الشروط التي تعتمد عليها .وقد تم استخدام التشفير مع بعض الطرائق لإضافة طبقة حماية أخرى إلى الصورة المخفية.

كذلك طبق الاسلوب العشوائي في عملية الإخفاء لزيادة أمنية النظام ،ولجعل النظام أكثر حصانة فإنّ بعض المعلومات السرية ترسل بصورة وهي مشتركة بين المرسل والمستلم ومن دونها لن يع المستلم استرجاع الصورة المخفية .وإنّ إجراء بعض المعالجات على الصورة الحاوية على الصورة المخفية(**Stego-Image**) سوف لن يؤثر على عملية استرجاع الصورة المخفية.كذلك فإن عملية الاسترجاع لا تتطلب وجود صورة الغطاء الأصلية.

حيث سعى البحث إلى تحقيق جانبين مهمين هما زيادة سعة الإخفاء (**Capacity**) مع تقليل قابلية الرؤيا(الإحساس)(**Impercibility**) مقابل مقاومة مقبولة نوعا ما ضد التدمير أو الإزالة (**Removal Resistance**).

1-12 محتويات الرسالة

يتكون الهيكل العام للرسالة من ثلاثة فصول،حيث تضمن الفصل الأول مقدمة عامة عن موضوع الرسالة وكذلك دراسة لأنواع وتقنيات الإخفاء المعروفة.يعطي الفصل الثاني و صفا للنظام المقترح و الخوارزميات المستعملة،أما الفصل الثالث فيبن النتائج التي تم الوصل إليها ويقدم الاستنتاجات لذلك وتوجهات العمل المستقبلي.



الشكل(1-3) يوضح أنواع الأنظمة الابدالية

قائمة المصطلحات العربية والإنكليزية

المصطلح الإنكليزي	المصطلح العربي
Information Hiding	إخفاء المعلومات
Steganography	الإخفاء
Digital Watermarking	العلامة المائية الرقمية
Parity bit	ثنائية التطابق
Spatial Domain	المجال الحيزي
Histogram	المدرج التكراري
Seed	بذرة
Gray Scale	تدرج رمادي
Contrast	تضاد لوني
Recognition	تمييز
Intensity	شدة اللون

المصطلح الإنكليزي	المصطلح العربي
Noise	ضوضاء
Thresholding	تعتيب
Threshold	عتبة
Pixel	عنصر الصورة
Peak	قمة
Object	كيان
Color	لون
Block	قطاع
Digital Image Processing	معالجة الصور الرقمية
Region	منطقة
Texture	نسيج
Pattern	نمط
Image Compression	ضغط الصور
Wavelet Transform	التحويل المويجي
Discrete Wavelet Transform	التحويل المويجي المتقطع
Discrete Cosine Transform	تحويل جيب التمام المتقطع
Lossy Compression	الضغط الحاوي على فقدان البيانات
Lossless Compression	الضغط الخالي من فقدان البيانات
Quantization	التكمية
Human Visual System	نظام الرؤيا البشري
Frequency Domain	المجال الترددي
Luminance	شدة الإضاءة
Mask	قناع

المصطلح الإنكليزي	المصطلح العربي
Dithering	اهتياج
Null-Hypothesis	فرضية العدم
Filtering	الترشيح
Autocorrelation	الارتباط الذاتي
Human Audio System	نظام السمع البشري
Error Correction Coding	مرمز تصحيح الخطأ
Malicious	خبيث
Spread Spectrum Techniques	تقنيات الطيف المنتشر
Distortion	تشويه
Transform Domain	مجال التحويل
Cover Generating Methods	طرق توليد الغطاء
Spatial Masking	القناع الحيزي
Frequency Masking	القناع الترددي
Fidelity Criteria	مقاييس الموثوقية
Object Fidelity Criteria	مقياس الموثوقية الهدف
Root Mean Square Error	الجذر التربيعي لمربعات الخطأ
Signal to Noise Ratio	نسبة الإشارة إلى الضوضاء
Subjective Fidelity Criteria	مقياس الموثوقية الشخصي

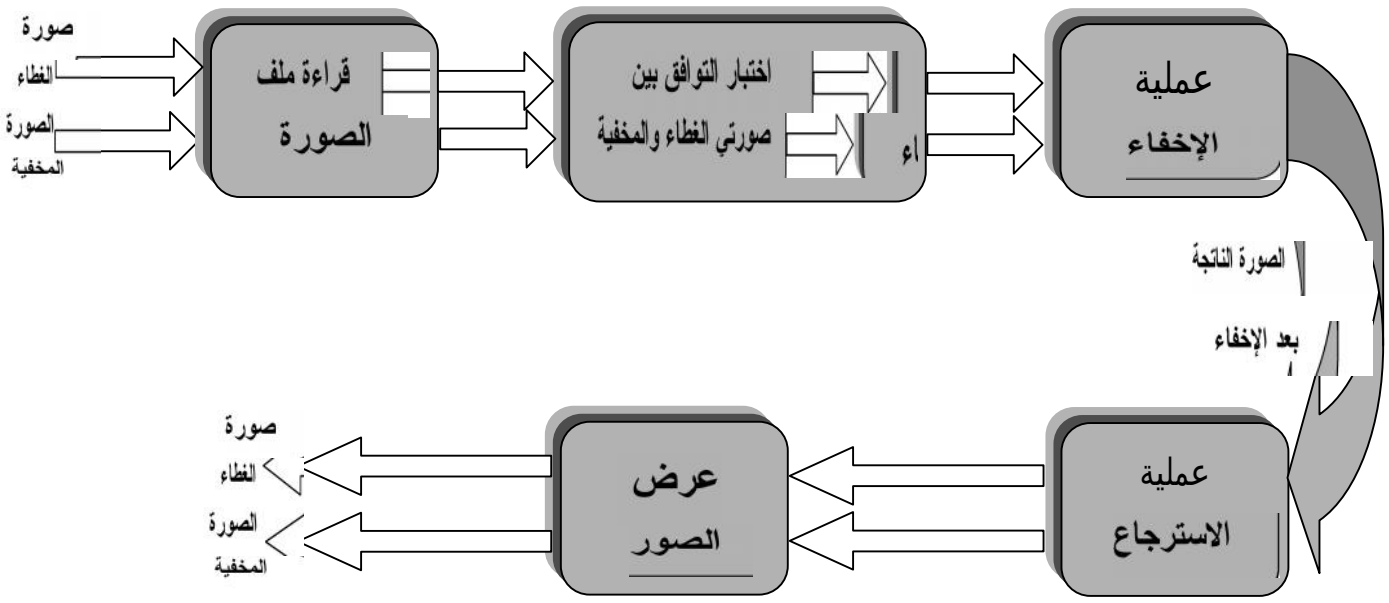
قائمة المختصرات

المختصر باللغة الإنكليزية	المصطلح باللغة الإنكليزية
	Discrete Cosine Transform
DWT	Discrete Wavelet Transform
DFT	Discrete Fourier Transform
LSB	Least Significant Bit
SS	Spread Spectrum
BMP	Bitmap
HVS	Human Visual System
RMSE	Root Mean Square Error
SNR	Signal to Noise Ratio
PSNR	Peak Signal to Noise Ratio

2-1 تصميم النظام المقترح

نستعرض الخطوات الأساس لتصميم النظام المقترح لإخفاء صورة داخل صورة،حيث يتناول البحث تنفيذ خمس طرائق إخفاء وقد طبقت على أكثر من نوع من الصور وبدرجات تعقيد مختلفة وهذه الأنواع تشمل:الصور ذات التدرجات الرمادية(**Gray Scale Image**)،والصور الملونة ذات **(256)** لونا والصور الطبيعية (**True Color**).

يتضمن النظام المقترح خمس طرائق إخفاء وكل طريقة تتكون من جزءين أساسيين هما الإخفاء (**Embedding**) والاسترجاع(**Extracting**).يشمل الجزء الأول مرحلة قراءة ملف الصور،مرحلة اختق بين صورتي الغطاء والمخفية،مرحلة الإخفاء التي تنجز بصورة عشوائية **(أما بواسطة مولد الأرقام شبه العشوائية مع مفتاح سري (Secret Key) يُعدُّ بذرة(Seed)له أو بوساطة متسلسلة أعداد مناسبة توفر خلط وتداخل للبيانات المراد إخفاؤها داخل صورة الغطاء بشكل يصعب تجميعها بشكل م من دون معرفة مفتاح تلك المتسلسلة)**.وقد تحتاج بعض طرائق الإخفاء إلى فصل الألوان**(كما في الصور الطبيعية)** أولا قبل إجراء عملية الإخفاء.وبعد عملية الإخفاء يتم تجميع الألوان لتنتج الصورة الحاملةورة السرية(**Stego-Image**).أما الجزء الثاني فيمثل عملية الاسترجاع، حيث تسترجع الصورة المخفية وذلك بعكس طريقة الإخفاء بالاعتماد على المعلومات السرية المشتركة بين المرسل وم،ويوضح الشكل(2-1) المخطط الكتلي للنظام.



يبين الشكل (2-1) المخطط الكتلي للنظام

2-2 قراءة ملف الصورة (Reading Image File)

أول مرحلة في أي نظام معالجة صور هو قراءة ملف الصور إذ تخزن بيانات الصور على شكل ملفا، يلائم استرجاعها وخزنها بالحاسوب.وتعتمد عملية قراءة ملف الصورة على هيأة ملف الصورة المستعمل(**Image File Format**)،حيث تتوافر العديد من إلهيات المستعملة لتمثيل الصور،ولقد وقع الاختيار على هيأة **BMP** (**Bitmap Format**) الذي يعد من اشهر واهم الأنواع ويرجع السبب في ذلك إلى سهولة التعامل مع هذه الملفات زيادة على أنها تمتاز بإمكانية تخزين الرسوم أو الصور من أي نظام عرض وبإمكانية عرض الرسوم أو الر من أي نظام عرض [33].

يتكون ملف **BMP** في حالة الصور الملونة أو الرمادية التدرج ذات (**256**)لونا من ثلاثة أجزاء هي الصديرة (**Header**) الذي يحتل (**54**) ثمانية ويحتوي المعلومات الضرورية ذات العلاقة بالأجزاء الأخرى لملف الصورة التي تشمل عرض وطول خارطة عناصر الصورة،عدد الثنائيات لكل عنصر في الصورة ومؤشر بداية منطقة البيانات،يمثل الجزء الثاني في ملف الصورة لوحة الألوان

(**Color Palette**) المتمثل بالشدة اللونية للأحمر (**Red**) والأخضر(**Green**) والأزرق(**Blue**)،يعتمد حجم لوحة الألوان على عدد الثنائيات لكل عنصر(**Bit Per Pixel**) فإذا كان عدد الثنائيات يساوي (**8**) فإنّ حجم لوحة الألوان يكون (**0-255**) وكل عنصر في الصورة يمثل فهرس يشير إلى أحد مداخل لوحة الألوان،يمثل الجزء الأخير بيانات الصورة [34] .أما في حالة الصور الطبيعية فإنّ ملف **BMP** يتكون من جزء ين فقط هما جزء الصديرة الذي يحتل(**54**) ثمانية وجزء بيانات الصورة،حيث يمثل كل عنفي الصورة بثلاث ثمانيات تمثل الألوان (**الأزرق و الأحمر و الأخضر**).

يمتاز ملف **BMP** بخاصية: هي أنّ طول كل سطر فيه يتم ضبطه على حدود (**4**)ثمانيات أي كلمة من (**32**)ثنائية.أي إنّ كل سطر عند قسمة طوله على (**4**) يكون الباقي صفرا ويكمل بالقيم صفر.على سبيل المثال،إذا كان عرض الصورة هو(**122**) نقطة أي إنّ طول السطر هو (122)،فعند قسمته على (**4**) يكون الباقي (**2**)،لذلك عند كتابة كل سطر في الصورة،يعدل طول السطر ليكون (**124**) وهي اقرب قيمة لطول السطر ني صفر عند قسمتها على (**4**).توضع قيم النقط الزائدة في كل سطر وهي (**2**) في هذه الحالة تساوي صفرا أو أي قيمة أخرى لأنها لن تستعمل على الإطلاق في عرض الصورة فهي فقط لضبط حدود السطور في التخزين في الملف ويمكن حساب طول السطر في الصورة كالآتي:

```
If (Imagewidth  mod  4)>0 Then
   Rowlength=Imagewidth+4-(Imagewidth  mod  4)
Endif
```

ذلك بفرض أن **Imagewidth** هو عرض الصورة و**Rowlength** هو طول السطر المطلوب كتابته أو قراءته منه.عند عرض الصورة على الشاشة يستعمل فقط العرض المحدد في ترويسة الملف في

منطقة معلومات الصورة **Imagewidth** وتهمل النقط الزائدة وهي عبارة عن الفرق بين طول السطر **Rowlength** وعرض الصورة **Imagewidth** [33] .

وفيما يأتي الخوارزمية الخاصة بعملية قراءة الصور التي يكون فيها عدد الثنائيات لكل عنصر في الصورة مساويا إلى 1,4,8,24

Reading Algorithm

Step 1: **{Read File Header}**

-Get BMP file header.

-Check the signature file.

Step 2:Get global color map,put in variable structure"palette".

Step 3:Calculate bit per pixel and block data for each row.

Case bitno. of

1: (bmp.wid+7/8).

4:(bmp.wid+7/8) shl 2.

8:(((bmp.wid+3) div 4)×4).

24:(bmp.wid×3).

Step 4:Gets the offset to reach the start of bitmap data.

Step 5:Get block data size according to step3.

Step 6:Put bitmap data in matrix.

Step 7:End.

2-3 طرائق الإخفاء

تم تنفيذ خمس طرائق إخفاء مختلفة وكل طريقة لها مجموعة من الشروط التي تعتمد عليها في عملية الإخفاء وقد طبقت على عدة أنواع من الصور ذات التدرجات المختلفة وبدرجات تعقيد مختلفة

وفيما يأتي توضيح تفصيلي للطرائق المستعملة :

2-3-1 طريقة Image Downgrading

وهي حالة خاصة من الأنظمة الابدالية وقد تم ذكرها فيصل السابق.إذ تستعمل لإخفاء صورة داخل صورة أخرى لها نفس الحجم ،فهي تستعمل الثنائيات الأربعة الأقل أهمية من صورة الغطاء لإخفاء الثنائيات الأربعة الأكثر أهمية من الصورة السرية بعد أن تشفر بوساطدالة أو الحصرية(**XOR**) مع مفتاح سري(**Key**) لإضافة مستوى آخر من الحماية [35] .

تشترط هذه الطريقة أن تكون صورة الغطاء متوافقة مع الصورة السرية،ويتم اختبار التوافقية بين الصورتين بالاعتماد على المدر التكراري (**Histogram**) .إن استعمال الاسلوب العشوائي يجعل عملية الوصول إلى البيانات المخفية صعبة،و إنّ استعمال التشفير يزيد من صعوبة استرجاع الصورة المخفية .زيادة على أنّ عملية الاسترجاع تعتمد على بعض المعلومات السرية المشتركة بين المرسل والمستلم وح المستعمل في التشفير (**Key**) ،بذرة مولد الأرقام شبه العشوائية (**Sk**)،متسلسلة الأعداد (**S**) وعدد الثنائيات المخفية (**N**) وهي تساوي (**4**) .

طبقت هذه الطريقة على اكثر من نوع من الصور وكما يأتي :

أ. إخفاء صور طبيعية داخل صور طبيعية [36][37]:

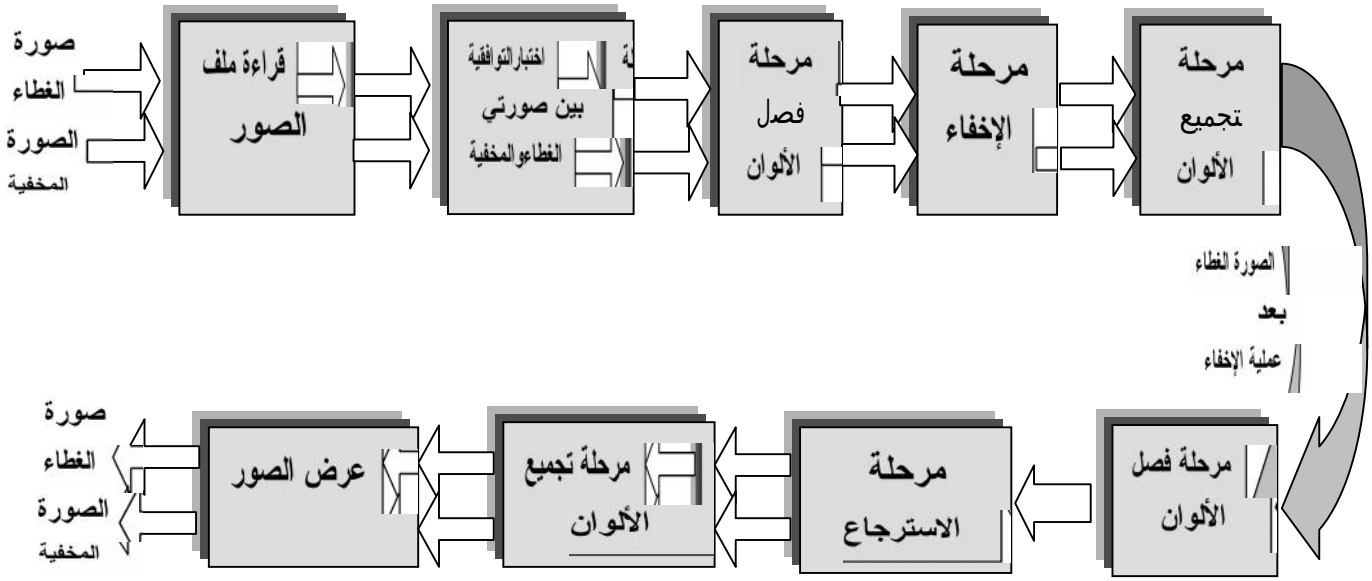
سبق وأنْ ذكرنا أنّ ملف الصور الطبيعية يمن جزءين فقط .ولاخفاء صورة طبيعية نحتاج إلى إخفاء بيانات (**عناصر**) الصورة فقط ، يتكون كل عنصر من ثلاث ثمانيات(**Red,Green,Blue**). تتضمن هذه الطريقة عدة مراحل : (مرحلة قراءة ملف الصور ومرحلة اختبار التوافقية بين صورتي الغطاء والمخفية و مرحلة فصل الألوان التي يدخل إليها ملف الصورة الطبيعية ويخرج منه ثلاثة متجهات تمثل (**الأزرق** ، **الأخضر** ، **الأحمر**) ومرحلة الإخفاء وفيها تحشر الأربع ثنائيات الأكثر أهمية المشفرة من بيانات؛ المراد إخفاؤها (**المتجهات الثلاثة**) في الأربع ثنائيات الأقل أهمية من بي صورة الغطاء (**المتجهات الثلاثة**) وفي مواقع عشوائية

تولد بوساطة متسلسلة أعداد ، مرحلة تجميع الألوان التي تعيد تجميع المتجهات الثلاثة الناتجـة بعـد

عملية الإخفاء لتكون ملف الصورة الحاوية على صورة مخفية و مرحلة فصـل الألـوان و مرحلـة

الاسترجاع التي تسترجع الصورة المخفية من المواقع العشوائية ومرحلة تجميع الألوان لتكوين ملـف

الصورة المخفية يوضح الشكل (2-2) المخطط الكتلي للطريقة.



يبين الشكل (2-2) المخطط الكتلي لطريقة Image Downgrading

وفيما يأتي خوارزمية الإخفاء :

Embedding Algorithm

Input: The cover-image, the embedded-image, N, key and S.

Output: The stego-image

Step 1:Select the embedded-image and the cover-image then calculate the histogram for both cover and embedded images.

Step 2 : For each pixel in cover-image and embedded-image , do

-Split the cover-image into three vectors “Rc, Gc, Bc”.

-Split the embedded-image into three vectors “Re, Ge, Be”.

End for

Step 3 : Generate random positions by using the sequential (S) and put them in

matrix.

Step 4 : For each position in matrix, do

-Set the N low order bits of each vector “Rc, Gc, Bc” to zero.

-Cipher each vector “Re, Ge, Be” by using “XOR” with secret key and shift right the results by 8-N .

-Add values from “Rc, Gc, Bc” and “Re, Ge, Be” in “ Rs, Gs, Bs”.

End for

Step 5 : For I := 1 to Data size , do

Combing the three vectors “Rs, Gs, Bs” in a file “ stego-image” .

End for

Step 6:End

أما خوارزمية الاسترجاع :

Extracting Algorithm :

Input : The stego-image ,N , key and S .

Output : The embedded-image .

Step 1 : For each pixel in stego-image ,do

-Split the stego-image into three vectors “Rs, Gs, Bs”.

End for

Step 2 : Generate random positions by using the sequential (S) and put them in matrix .

Step 3 : For each position in matrix , do

-Shift right each vector of “ Rs , Gs, Bs” by 8-N.

-Put the shifted value of the “ Rs , Gs, Bs” after decipher it using “XOR” with secrete key into “Rx, Gx, Bx”.

End for

Step 4 : For I := 1 to Data size ,do

-Combing the three vectors “Rx, Gx, Bx” in a file “ extracted- image”.

End for

Step 5 : End

ب. إخفاء صورة ملونة ذات (256) لون داخل صورة ملونة ذات (256) لونا :

يتكون ملف الصورة الملونة ذات **(256)** لونا وكما ذكرنا سابقا من ثلاثة أجزاء هي الصـــديرة ولوحة الألوان **(Palette)** وبيانات الصورة لذا فإننا نحتاج إلى إخفاء جزء آخر وهو لوحة الألـــوان.

تنجز عملية الإخفاء بحشر الثنائيات الأربعة الأكثر أهمية من بيانات الصورة المـــراد إخفاؤهـــا بعـــد تشفيرها باستعمال دالة أو الحصرية **(XOR)** مع مفتاح داخل الثنائيات الأربعة الأقـــل أهميـــة مـــن صورة الغطاء وفي مواقع عشوائية تولد باستعمال مولد الأرقام شبه العشوائية مع مفتاح يعـــد بـــذرة **(Seed)** له [38] .

أما لوحة الألوان للصورة المخفية فتخفى في المدة الفارغة **(غير المستعملة)** مـــن صـــورة الغطاء **(وهي الأعمدة التي تضاف إلى عرض الصورة ليصبح طول السطر ضمن حدود (4) بايت التي تم ذكرها في فقرة سابقة)** .

وفيما يأتي خوارزمية الإخفاء :

Embedding Algorithm

Input: The cover-image, the embedded-image, N, Key and Sk.

Output: The stego-image

Step 1:Select the embedded-image and the cover-image then calculate the histogram for both cover and embedded images.

Step 2 : Generate random position " I " by using the pseudo – random number generator of seed secret key "Sk" .

Step 3 : Set the N low order bits in cover-pixel[I] to zero .

-Cipher the embedded pixel [I] by using "XOR" with secret key and shift right the result by 8-N .

-Add values from cover-pixel [I] and embedded-pixel [I] into stego-

pixel [I] .

Step 4 : Hide the embedded-palette in unused rows of the stego-image .

Step 5 : End.

أما خوارزمية الاسترجاع :

Extracting Algorithm :

Input : The stego-image ,N , key and Sk .

Output : The embedded-image .

Step 1: Generate random position " I " by using the pseudo – random number generator of seed secret key "Sk".

Step 2 : Shift left the stego-pixel [I] by 8-N .

-Put the shifted value of stego-pixel [I] after decipher its by using "XOR" with key into extracted pixel [I].

Step 3 : extract the embedded palette from unused row of the stego image.

-Put the shifted value of stego-pixel [I] after decipher its by using "XOR" With key into extracted-pixel [I].

Step 4 : extract the embedded palette from unused rows of the stego image.

Step 5 : End.

ج. إخفاء صور رمادية التدرج داخل صور رمادية التدرج أو ملونة(256) لونا :

يتكون ملف السور ذات التدرج الرمادي **(256)** لونا من ثلاث أجزاء هي الصديرة ولوحة الألوان وهت كما في الصور الملونة .ولإخفاء صورة ذات تدرج رمادي يتم إخفاء جزء البيانات منها فقط وذلك بحشر الثنائيات الأربع الأقل أهمية من صورة الغطاء **(رمادية التدرج أو ملونة)** بالثنائيات الأربعة الأكثر أهمية من الصورة المراد إخفاؤها بعد أن تشفر بوساطة دالة أو الحصرية **(XOR)** مع مفتاح وفي مواقع عشوائية تولد باستعمال مولد الأرقام شبه العشوائية مع مفتاح **(Sk)** يُعد بذرة **(Seed)** له .

أما خوارزميتي الإخفاء والاسترجاع فهي مث للفقرة السابقة (2)**(مع حذف جزء إخفاء لوحة الألوان فقط)** .

2-3-2 طريقة حشر الثنائيات الأقل أهمية (LSB)

وهي من الطرائق الشائعة والبسيطة التي تم ذكي الفصل السابق.وقد استعملت لإخفاء صور ذات تدرج رمادي أو ملونة **(256)** لونا داخل صور طبيعية.تتضمن هذه الطريقة أيضا اختبار للتوافقية بين صورتي الغطاء والمخفية بالاعتماد على المدرج التكراري لإخفاء صورة كاملة داخل صورة الغطاء**(ولن الثنائيات الأقل أهمية فقط)** .وذلك لأنّ حجم صورة الغطاء يعادل تقريبا حجم الصورة المراد إخفاؤها بثلاث مرات لذا فإنّ كل عنصر من الصورة المراد إخفاؤها يجزأ إلى ثنائيات تخفى في عنصر من صورة الغطاء**(الثنائيات الأقل أهمية للأحمر(2 bit)و الأخضر(3 bit)والأزرق (3 bit))** وبصورة عشوائية باستعمال مولد به العشوائية مع مفتاح **(Sk)** يُعدُّ بذرة له، أما لوحة الألوان فتخفى في الأسطر الثلاث الأخيرة من صورة الغطاء.

إن استعمال الاسلوب العشوائي يجعل عملية الوصول إلى الصورة المخفية صعبة،كذلك استعمال مستوى الضوضاء يقلل من تأثير عملية الإخفاء بحيث تكون غير مدركة **(محسوسة)** .زيادة على أنّ

الأرقام شبه العشوائية **(Sk)**،متسلسلة الأعداد **(S)** وعدد الثنائيات المخفية **(N)** وهي تساوي **(4)**.

الجزء الآتي يصف خوارزمية الإخفاء .

Embedding Algorithm

Input: The cover-image, the embedded-image and Sk.

Output: The stego-image

Step 1:: Select the embedded-image and the cover-image then calculate the histogram for both cover and embedded images.

Step 2:For each pixel in cover-image ,do

-Split the cover-image into three vectors “Rc,Gc,Bc”.

End for

Step 3:Generate random position ”I” by using the pseudo-random number generator of seed key”Sk”.

Step 4:Set the 2 low order bits in the Rc [I] to zero.

-Shift right the embedded-pixel [I] by 6.

-Add values from Rc [I] and embedded-pixel [I] in Rs [I].

-Set the 3 low order bits in the Gc [I] and Bc[I] to zero.

-Shift right the embedded-pixel [I] by 3 then the result “AND” with 7.

-Add values from Gc [I] and embedded-pixel [I] in Gs [I].

-The embedded-pixel [I] “AND” with 7.

-Add values from Bc [I] and embedded-pixel [I] in Bs [I].

Step 5:For I=1 to datasize ,do

-Combine the three vectors ”Rs,Gs,Bs” in a file “stego-image”.

End for

Step 6:Hide the embedded-palette in last three rows of stego-image.

Step 7:End.

أما خوارزمية الاسترجاع :

Extracting Algorithm :

Input : The stego-image and Sk .

Output : The embedded-image .

Step 1:Extract the embedded-palette from the last three rows of the stego-image .

Step 2:For each pixel in stego-image ,do

-Split the stego-image into three vectors ”Rs,Gs,Bs”.

Step 3: Generate random position ”I” by using the pseudo-random number generator of seed key”Sk”.

Step 4:Add the 2 low order bits of “Rs [I]” and the 3 low order bits of “Gs” [I] and the 3 low order bits of ”Bs [I]” in an extracted-pixel [I].

Step 5:End.

2-3-3 استعمال الاسلوب الرياضي (Using Modulo Mechanism)

تعتمد هذه الطريقة على استعمال الاسلوب الرياضي(**Mathematical Modulus**) لدمج البيانات السرية (**صورة**) مع صورة الغطاء.وتعدُّ هذه الطريقة ذات أمنية عالية نسبة إلى الطريقتين السابقتين لأنّ البياناترية تضاف إلى صورة الغطاء .و إنّ البيانات المخفية لن تسترجع إلا بمعرفة خوارزمية الإخفاء .وفي حالة معرفة خوارزمية الاسترجاع فإنّ الصورة المخفية لن تسترجع إلا بمعرفة المعلومات السرية المشتركة بين المرسل والمستلم وهي بذرة مولد الأرقام شبه العشوائية **(Sk)**،متسلسلة الأعداد **(S)**،وعدد الثنائيات المخفية**(ml)** وقيمة العتبة **(T)**.

إن استعمال الاسلوب العشوائي يجعل عملية الوصول إلى الصورة المخفية صعبة،وتستعمل لإخفاء الصور ذات التدرج الرمادي أو الملونة **(256)** لونا [39] .

أ. في حالة الصور الملونة

تم تطبيقها بطريقتين:

الأولى:–تحول بيانات الصورة المراد إخفاؤها **(الثنائيات الأربعة الأكثر أهمية)** إلى ثنائيات تخزن في مصفوفة "**Bs**"،ثم تخفى بطريقة عشوائية باستعمال مولد الأرقام شبه العشوائية مع مفتاح **(Sk)** يكـــون ها وبمعدل أربع ثنائيات لكل عنصر .أما لوحة الألوان فتخفى في الأعمدة غير المستعملة .

تصف الخوارزمية الآتية هذه الطريقة :

Embedding Algorithm

Input :The cover-image C,the bit string of Bs,the seed key Sk ,the threshold value T and modulus ml.

Output:The stego-image.

Step 1:Find a workable pixel pc [I] in cover-image C by using the pseudo-random number generator of seed Sk.

Step 2:Set a threshold value T and modulus value ml. then compute a residue , $g_{\text{remainder}}$ and the possible capacity in a pixel , g_{ec} , as following form:

$$g_{ec} = \lfloor \text{Log}_2^{\text{ml}} \rfloor$$

$$g_{\text{remaimder}} = \text{pc}[\text{I}] \bmod \text{ml}$$

where pc [I] denotes the intensity of the i-th. pixel with order of top-down and left to-right in a cover-image C and $\lfloor\ \rfloor$ denotes the truncate value.

Step 3:Compute the absolute difference value, g_{dv}, such that

$$g_{\text{dV}=} |g_{\text{remainder}} - g_{\text{ev}}|$$

where g_{ev} is a value, which is fetched sequentially from Bs with bits of g_{ec} -length.

Step 4:Embed g_{dv} into the pixel pc [I](here, we define ps [I] as the intensity of the i-th pixel after embedding g_{ev})by performing the following

process:

1. if $pc[I] < \frac{ml}{2}$, gain $ps[I] = 0 + g_{ev}$.
2. $\frac{ml}{2} < pc[I] < T - \frac{ml}{2}$

   . if $g_{dv} > \frac{ml}{2}$, gain an adaptable value, $Av = ml - g_{dv}$.

   . if $g_{remainder} > g_{ev}$, gain $ps[I] = pc[I] + Av.$

   else, gain $ps[I] = pc[I] - Av.$

   . if $g_{dv} \le \frac{ml}{2}$, gain $Av = g_{dv}$

   . if $g_{remainder} > g_{ev}$, gain $ps[I] = pc[I] - Av.$

   else, gain $ps[I] = pc[I] + Av.$
3. if $(T - \frac{ml}{2}) \le pc[I] < T$, gain $ps[I] = pc[I] - g_{remainder} + g_{ev}$.

Step 5:Hide the embedded-palette in unused rows of the stego-image "ps [I]".

Step 6:End.

أما خوارزمية الاسترجاع :

Extracting Algorithm

Input :The stego-image S,the value T ,the seed key Sk and modulus ml

Output: the bit string of Bs

Step 1:Find a workable pixel ps [I] in stego-image S by using the Pseudo-random number generator of seed Sk.

Step 2:Compute the embedded information as following

$g_{remaimder} = ps[I] \bmod ml$

$g_{ec} = \lfloor Log_2^{ml} \rfloor$

Step 3:Translate the $g_{remainder}$ into the bits representation to recover the embedded information ,the bit-length for each $g_{remainder}$ is determined by the computation of g_{ec} .

Step 4:recover the embedded-palette from unused rows of ps.

Step 5:End.

الأخرى:- **تحول البيانات المراد إخفاؤها**(الثلاث ثنائيات الأكثر أهمية من بيانات الصورة+لوحة ألوانها (الأخضر والأزرق أما الأحمر فيخفى في العمود الرابع من لوحة ألوان الصورة الناتجة بعد الإخفاء)) **إلى ثنائيات تخزن في مصفوفة "Bs" ، ثم تخفى بطريقة عشوائية باستعمال متسلسلة أعداد مع مفتاح يكون البذرة لها وبمعدل أرات لكل عنصر .وباستعمال نفس الخوارزمية السابقة** (فقط إلغاء جزء لوحة الألوان) .

ب. في حالة الصور ذات التدرج الرمادي

تحو بيانات الصورة المراد إخفاؤها **(الثنائيات الأربعة الأكثر أهمية)** إلى ثنائيات تخزن في مصفوفة "Bs"،ثم تخفى بطريقة عشوائية باستعمال مولد الأرقام شبه العشوائية مع مفح يكون البذرة له وبمعدل أربع ثنائيات لكل عنصر وباستعمال الرمية السابقة (بدون لوحة الألوان) .

2-3-4 طريقة هجينه (Hybird Method)

وهي طريقة لإخفاء صور ملونة(**256**) لونا داخل صور ملونة(**256**) لونا أو صور ذات تدرج رمادي داخل صور ذات تدرج رمادي وتتضمن مرحلتن في عملية الإخفاء :-

المرحلة الأولى(مرحلة الضغط)

تتضمن هذه المرحلة استعمال نوع من أنواع الترميز وهو ترميز طول التنفيذ **RLE (-Run Length Encoding)** .يعد ترميز طول التنفيذ من طرائق الضغط التي لا تسمح بفقدان البيانات **(Lossless)** وتستعمل عادة مع خوارزميات الضغط التي تسمح بحدوث أخطاء **(Lossy)** لزيادة نسبة الضغط [40] .

تقلص بيانات الصورة المراد إخفاؤها بالاعتماد على عد عناصر الصورة المتجاورة التي لها نفس القيمة اللبطلق على هذا العدد **(Run Length)** .تخزن كل القيم اللونية مع مقدار التكرار في مصفوفة .

المرحلة الثانية(مرحلة الإخفاء)

تنجز هذه المرحلة باسلوبين :-

الاول:- تحول بيانات المصفة الناتجة من المرحلة الأولى **(القيم اللونية ومقدار التكرار)** إلى مصفوفة ثنائيات ثم تخفى باستعمال الاب الرياضي/الطريقة الأولى .

والاخر:- تحول بيانات المصفوفة الناتة من المرحلة الأولى **(القيم اللونية مع مقدار التكرار)** وكذلك لوحة ألوان الصرة المخفية **(الأزرق والأخضر)** إلى مصفوفة ثنائيات ثم تخفى باستعمال الاسلوب الرياضي/الطريقة الثانية .

تشترط هذه الطريقة أن يكون حجم المصفوفة الناتجة من مرحلة الضط **(Me)** صغير ويمكن لصورة الغداستيعابه، حيث يتم اختبار حجم المصفوفة الناتجة **(Me)** مع حجم صورة الغطاء **(Mc)** وفق العلاقة الآتية :

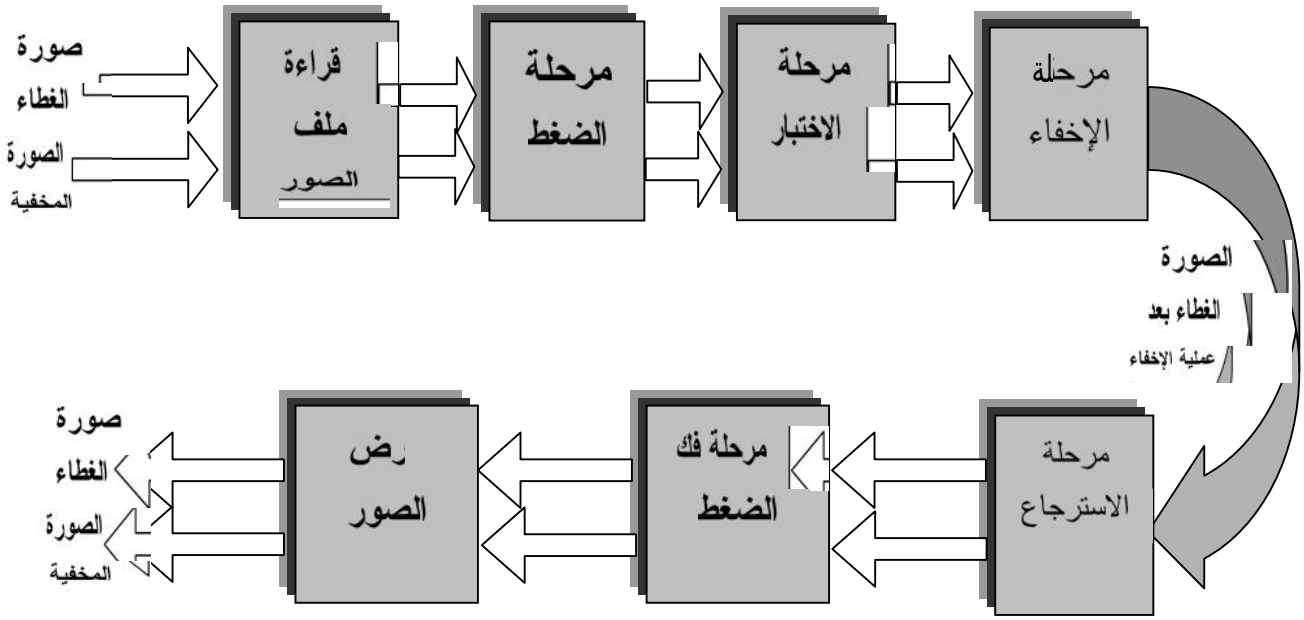
$$Me \le \frac{Mc}{2} \qquad (2-1)$$

فإذا تحققت العلاقة أعلاه فإنّ الصورة المخفية يمكن إخفاؤها في صورة الغطاء هذا في حالة الاسلوب الأول .أمّا في حالة الاسلوب الثاني فإن العلاقة تكون

$$Me \le (\frac{Mc}{2} + 1024) \qquad (2-2)$$

إذ إن **(1024)** يمثل بيانات لوحة ألوان الصورة المخفية.

المخطط الكتلي الآتي يوضح الطريقة .



يبين الشكل(2-3)المخطط الكتلي للطريقة الهجينة

تعدُّ الطريقة الهجينة ذات أمنية عالية لأنّ البيانات المخفية لن تسترجع إلا بمعرفة خوارزمية الإخفاء ولو عرفت خوارزمية الإخفاء فإنّ البيانات المسترجعة لا تعني صول إلى الصورة المخفية وإنما تمثل القيم اللونية ومقدار التكرار ولذلك يجب معرفة طريقة الضغط ومن دونها لن تسترجع الصورة المخفية.و إنّ استعمال الاسلوب العشوائي يزيد من صعوبة الوصول إلى البيانات المخفية . زيادة على أنّ عملية الاسترجاع تعتمد على وص المعلومات السرية المشتركة بين المرسل والمستلم ،مولد الأرقام شبه العشوائية **(Sk)**،متسلسلة الأعداد،وعدد الثنائيات المخفية**(ml)** وقيمة العتبة **(T)**. و إنّ ضغط الصورة المخفية يقلل من حجم البيانات المخفية ومن ثمّ يجعل تأثير عملية الإخفاء على الصورة الناتجة بعد الإخفاء ليلا **(غير محسوس)** .كذلك يمكن استغلال المساحة المتبقية معلومات إضافية مثل المفتاح .إن ضغط الصورة المخفية يجعل بالإمكان إخفاء صورة كبيرة أو أكثر من صورة داخل صورة الغطاء .

ولاسترجاع الصورة يتم أولا استرجاع مصفوفة الثنائيات ثم مرحلة فك الضغط لاستعادة الصورة المخفية.وقد تم تطبيق طريقة (**Image Downgrading**) في مرحلة الإخفاء ولكنها فشلت.

تكون الطريقة الهجينة كفوءة مع الصور البسيطة التي يكون فيها عدد المستويات اللونية قليلاً.أمّا إذا كانت الصور معقدة فإنَّ هذه الطريقة قد لا تحقق نجاحاً حيث تميل عناصر الصورة المتجاورة لأن تأخذ قيما مختلفة وبذلك يكون التكرار قليلاً وقد يكون حجم المصفوفة الناتجة اكبر من المصفوفة الأصلية .

2-3-5 طريقة القطاعات المتشابهة

تم اقتراح طريقة جديدة لإخفاء صورة داخل صورة توفر إمكانيات في عملية الإخفاء .حيث إنها تعأكثر الطرائق أمنية و حصانة وذلك لأنها تعتمد على معلومات سرية ترسل بصورة مستقلة وهذه المعلومات تمثل حجم القطاع ومواقع الإخفاء،ومن دون هذه المواقع لن يستطيع المستلم استرجاع الصورة المخفية زيادة على أنّ هذه الطريقة هي الأكثر مقاومة ضد التغيرات والمعالجات التيعلى الصورة الحاملة للصورة المخفية .

تعتمد هذه الطريقة على إيجاد القطاعات المتشابهة بين الصورة المراد إخفاؤها وصورغطاء وهي تتضمن خمس مراحل:ففي المرحلة الأولى يتم اختبار صورة الغطاء لمعرفة مدى ملاءمتها لتكون غطاءً مناسباً للصورة المراد إخفاؤها وقد استعمل مقياسان هما التشابه(**Similarity**) والاختلاف(**Dissimilarity**) بالاعتماد على حساب المدرج

) الذي يعطي خصائص إحصائية للصورة (من خلال عد عناصر **Histogram** التكراري (

الصورة التي تمتلك نفس الشدة اللونية) وكما في المعادلتين [41]:

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

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

) **E**) لقياس التشابه بين المدرج التكراري للصورة المخفية(**2-3** حيث تستعمل المعادلة(

$h_j(C)$) و**E**) في الصورة (**j** هي عدد العناصر ذات اللون ($h_j(E)$) .و**C** وصورة الغطاء (

هو حجم صورة الغطاء **Nc×Mc**) و**C**) في الصورة (**j** هي عدد العناصر ذات اللون (

) **C**) و(**E**) فتستعمل لقياس الاختلاف بين(**2-4** تمثل اصغر قيمة.أما المعادلة({}min و

تمثل القيمة المطلقة.| |) و**E** يمثل حجم الصورة المخفية (**Ne×Me**، حيث

) في عملية اختبار التوافق **Goodness of Fit** كما استعملت معادلة حسن المطابقة (

بين صورتي الغطاء والمخفية وكما في المعادلة [42]:

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

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

بعد اختيار الغطاء المناسب تأتي مرحلة الإخفاء وفيها يتم تقسيم كلا من الصورة

) ،ثم تبدأ عملية البحث عن القطاعات **Blocks** المراد إخفاؤها والغطاء إلى قطاعات(

المتشابهة .تعتمد عملية البحث على خاصية (**صفة**) تستخلص من كل قطاع من قطاعات

الصورة المراد إخفاؤها (**بعد أن يتم تقليص عدد القطاعات بحيث يتم إخفاء قطاع واحد**

من القطاعات المتشابهة) مع جميع قطاعات صورة الغطاء لإيجاد القطاع المشابه له أو القريب إليه ليتم إبداله مع ذلك القطاع .

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

Normalized Cross-وقد استعملت معادلة الارتباط المشترك المعدل( ) لقياس التشابه **(الارتباط)**بين صورتي الغطاء والمخفية **(إذ تعدُّ صفة Correlation مستخلصة عن كل قطاع)** وكما في المعادلة [21]:

$$Ncc(w1, w2) = \frac{(w1 - \overline{w1}) \bullet (w2 - \overline{w2})}{\|w1 - \overline{w1}\| \bullet \|w2 - \overline{w2}\|} \qquad (2-6)$$

يمثلان متجهين(قطاعين) أحدهما للصورة المخفية والآخر لصورة **w2 و w1**إذ إنَّ **2-6)** . إن المعادلة **(Norm** يمثل المعيار($\| \ \|$ يمثل معدل القطاعين و $\overline{w2}$ ، $\overline{w1}$ الغطاء و لم تحقق نجاحا كبيرا في علية المقارنة بين القطاعات .

) في عملية الموازنة حيث **Goodness of Fit**وقد استعملت معادلة حسن المطابقة (يمثل قطاع من صورة الغطاء .وقد حققت C_i يمثل قطاع من الصورة المخفية و E_i إنَّ هذه المعادلة نجاحا كبيرا وذلك لأن 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 جاع كل قطاع من قطاعات الصورة المخفية وذلك من معرفة موقع ذلك القطاع داخل الصورة الناتجة بعد الإخفاء (**Stego-image**). إنّ هذه المواقع ترسل بصورة مستقلة عن صورة (**Stego-image**) ومن دونها لن يستطيع المستلم استعادة الصورة المخفية (**أي أن رقم كل قطاع من قطاعات الصورة المخفية يقابله رقم قطاع في صورة الغطاء ومن هذا الرقم يستطيع استرجاع عناصر القطاع**).

كذلك تم تطبيق خصائص أخرى مثل متوسط الانحراف المطلق الذي يمثل مقياساً لشدة التباين بين القيم اللونية(**Intensity**) للصورة،فالتباين الكبير يعطي دلالة على أنّ الصورة تمتلك اختلافات عالية وبالعكس وكما في المعادلة[43]:

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

حيث إنّ x_i يمثل قطاع من الصورة و $\overline{x_i}$ يمثل معدل القطاع و N تمثل حجم القطاع .

و $\left| x_i - \overline{x_i} \right|$ يمثل الفرق المطلق لـ x_i ، $\overline{x_i}$.

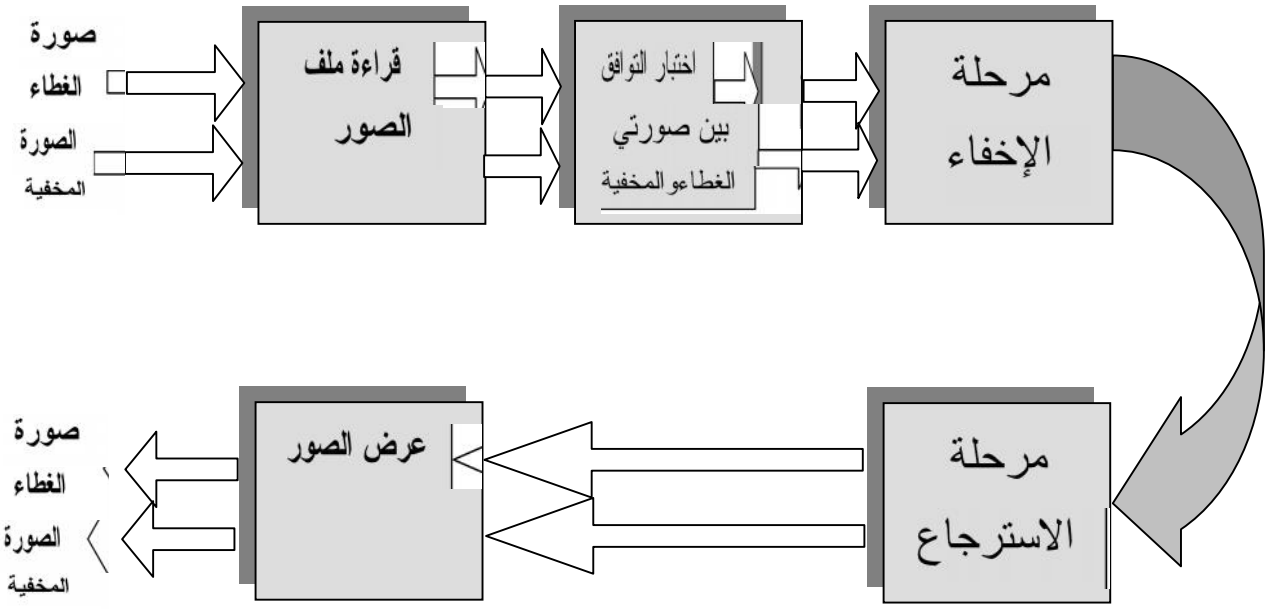
وقد تم استعمال العزوم اللامركزية وكما في المعادلة[44]:

$$M_{pq} = \sum_{x=0}^{N-1} \sum_{y=0}^{M-1} X^p Y^q f(x,y) \qquad (2-8)$$

إذ إنّ f(x,y) تمثل شدة اللون عند الإحداثي x,y و x=0,…,N-1 و y=0,…,M-1 و M×N تمثل مرتبة العزوم p,q وهو حجم الصورة أو الصورة الفرعية(**القطاع**) وقيم q,p=0,1,2,…,n. وقيمها(

إنّ كلاً من متوسط الانحراف المطلق العزوم اللامركزية فشل في إعطاء معلومات كافية للتشابه بين القطاعات ،ولكن يمكن استعمالهما كمقاييس ثانوية استعمال مقاييس أخرى إضافة إليها لكي نحصل على وصف **(دقيق)** للقطاعات.

يوضح المخطط الكتلي الآتي هذه الطريقة :



يوضح الشكل(2-4) المخطط الكتلي لطريقة القطاعات المتشابهة

إنّ هذه الطريقة طبقت على صور ملونة(256 لوناً،صور ذات تدرج رمادي) وصور طبيعية ،وقد نجحت مع الصور التي فيها تشا كبير **(نفس التدرجات اللونية)**(في حالة الصور الملونة(256 لوناً إذ تم إخفاء لة الألوان **(الأخضر والأزرق)**للصورة) **للصورة الناتجة بعد إبدال القطاعات المتشابهة أما الأحمر فقد LSBالمخفية باستعمال تم إخفاؤه في العمود الرابع من لوحة ألوانها)** .

الجزء الآتي يوضح خوارزمية الإخفاء :

Embedding Algorithm

Input : The cover-image and the embedding-image.

Output : The stego-image.

Step 1:Select the embedded-image and the cover-image.

Step 2:Calculate the histogram of both embedded and cover images.

Step 3:Perform Equation (3-2) or (4-2) or (2-5).

Step 4:If the result is true go to step 5 ,otherwise return to step1 to select new cover-image.

Step 5:Split the embedded-image and cover-image into blocks with size (N×N).

Step 6:Reduce the number blocks of embedded-image by remove the identical blocks and save one of them.

Step 7:For I=1 to No. of embedded-image blocks ,do

-Select emb-block[I] from embedded-image blocks.

-For j=1 to No. of cover-image blocks ,do

-Select cover-block[j] and perform Equation (5-2),search for greater match, and substitution it with emb-block[I].

End for

-Save the block number in matrix ”positions”.

End for

Step 8:If the embedded-image is 256 color then go to step9, else go to step10.

Step 9:Hide the embedded-palette in the LSB of the stego-image.

Step 10:End.

أما خوارزمية الاسترجاع :

Extracting Algorithm

Input : The stego-image ,the matrix ”positions” and block size.

Output : The embedding-image.

Step 1:Extract the embedded-palette from LSB of the stego-image.

Step 2: For I=1 to No. of embedded-image blocks ,do

-From a matrix ”positions” get the pos [I]

-Extract the emb-block from stego-block.

End for

Step 3:End.

3-1 أداء النظام المقترح

لاكتشاف أداء النظام الموضح في الفصل السابق،فقد تم اعتماد مجموعة من الصـور المختلفـة الأنـواع والتعقيدات **(صور ذات تدرجات رمادية،صور ملونة ذات (256) لونا وصور طبيعية)** كأمثلة تجريبيـة لبيـان سلوكية (كفاءة) النظام ،وقدت الموازنة اعتمادا على المقاييس الآتية :

- حساب نسبة قمة الإش إلى الضوضاء**(PSNR)** بين الصورة الأصلية والناتجة(المسترجعة).
- حساب الجذر التربيعي لل مربع الخطأ**(RMSE)** بين الصورة الأصلية والناتجة(المسترجعة).

وفيما يأتي التجارب التي تم القيام بها.

3-1-1 الطريقة الأولى/التجربة رقم (1)

في هذه التجربة تم تنفيذ الطريقة الأولى على مجموعة من الصور الطبيعية المختلفة في درجة تعقيدها.

يوضح الشكل(3-1) الصور الأصلية والناتجة(المسترجعة) .

الشكل (3-1)

وقد كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء **(Cover Image)** والصورة الناتجة بعد الإخفاء **(Stego Image)** تساوي (28.949201db) ،أمّا الجذر التربيعي لمعـدل مربـع الخطـأ فيسـاوي (9.100811).أمّا بالنسبة إلى الصورة المخفية **(Embedded Image)** والصورة المسترجعة (**Extracted**

Image) فانّ نسبة قمة الإشارة إلى الضوضاء تساوي (26.142396db) والجذر التربيعي لمعدل مربع الخطأ فيساوي (12.572463).

يوضح الشكل(3-2) الصور الأصلية والناتجة (المسترجعة)

الشكل (3-2)

لقد كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء (**Cover Image**) والصورة الناتجة بعد الإخفاء (**Stego Image**) تساوي(28.583683 db) ،أمّا الجذر التربيعي لمعدل مربع الخطأ فيساوي (9.491962).أما بالنسبة إلى الصورة المخفية (**Embedded Image**) والصورة المسترجعة (**Extracted Image**) فإنّ نسبة قمة الإشارة إلى الضوضاء تساوي (27.377644 db) والجذر التربيعي لمعدل مربع الخطأ يساوي (10.905810).

يوضح الشكل(3-3) الصور الأصلية والناتجة(المسترجعة) .

الصورة المخفية

صورة الغطاء

الصورة المسترجعة

الصورة الناتجة بعد الإخفاء

الشكل (3-3)

وقد كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغاء **(Cover Image)** والصورة الناتجة بعد الإخفاء **(Stego Image)** تساوي(25.428679 db) ،أمّا الجذر التربيعي لمعدل مربع الخطأ فيساوي (13.649168).أما بالنسبة إلى الصورة المخفية **(Embedded Image)** والصورة المسترجعة (**Extracted Image)** فإن نسبة قمة الإشارة إلى الضوضاءتساوي (27.014267 db) والجذر التربيعي لمعدل مربع الخطأ يساوي (11.371737).

من خلال التجارب السابقة نلاحظ أن قيمة نسبة قمة الإشارة إلى الضوضاء بين صورتي الغطاء والناتجة تتراوح بين (25.4-28.9) و الجذر التربيعي لمعدل مربع الخطأ يتراوح بين (9.1-13.6) أما بالنسبة للصورة المسترجعة فإنّ قيمة نسبة قمة الإشارة إلى الضوضاء تتراوح بين (26.1-27.3) و الجذر التربيعي لمعدل مربع الخطأ يتراوح بين (10.9-12.6) وهي قيم جيدة لان النتائج التي تم التوصل إليها جيدة وهي خالية من أي تشوهات وذلك لانّ الصور الطبيعية توفر مساحة كبيرة وهي تعادل ثلاثة أضعاف الصور الملونة ذات (256) لونا . وإنّ هذه الطريقة تستبدل الثنائيات الأربعة الأقل أهمية وبعض هذه الثنائيات تعدُّ ضوضاءً مما يجعل تأثير عملية الإخفاء قليلا أو معدوما وإنّ إجراء مرحلة اختبار التوافق بين صورتي الغطاء والمخفية يقلل من تأثير عملية الإخفاء .

الطبقة الأولى/التجربة رقم (2)

في هذه التجربة تم استعمال الصور الملونة ذات (256) لونا .

يوضح الشكل(3-4) الصور الأصلية والناتجة(المسترجعة) .

الصورة المخفية

صورة الغطاء

الصورة المسترجعة

الصورة الناتجة بعد الاخفاء

الشكل(3-4)

وقد كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء (**Cover Image**) والصورة الناتجة بعد الإخفاء (**Stego Image**) تساوي(25.347192 db) ،أمّا الجذر التربيعي لمعدل مربع الخطأ فيساوي (13.777821).أما بالنسبة إلى الصورة المخفية (**Embedded Image**) والصورة المسترجعة (**Extracted**

Image) فإن نسبة قمة الإشارة إلى الضوضاءتساوي (29.750175 db) والجذر التربيعي لمعدل مربع الخطأ يساوي (8.299107).

يوضح الشكل(3-5) الصور الأصلية والناتجة(المسترجعة) .

الصورة المخفية

صورة الغطاء

الصورة المسترجعة

الصورة الناتجة بعد الاخفاء

الشكل(3-5)

وقد كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء **(Cover Image)** والصورة الناتجة بعد الإخفاء **(Stego Image)** تساوي(22.990168 db) ،أما الجذر التربيعي لمعدل مربع الخطأ فيساوي (18.073063).أما بالنسبة إلى الصورة المخفية **(Embedded Image)** والصورة المسترجعة (**Extracted Image)** فإن نسبة قمة الإشارة إلى الضوضاءتساوي (32.407119 db) والجذر التربيعي لمعدل مربع الخطأ يساوي (6.112012).

يوضح الشكل(**3–6**) الصور الأصلية والناتجة(المسترجعة) .

الصورة المخفية

صورة الغطاء

الصورة المسترجعة

الصورة الناتجة بعد الإخفاء

الشكل (3-6)

وقد كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء (**Cover Image**) والصورة الناتجة بعد الإخفاء (**Stego Image**) تساوي(23.032647 db) ،أما الجذر التربيعي لمعدل مربع الخطأ فيساوي (17.984890).أما بالنسبة إلى الصورة المخفية (**Embedded Image**) والصورة المسترجعة (**Extracted Image**) فإن نسبة قمة الإشارة إلى الضوضاءتساوي (34.098755 db) والجذر التربيعي لمعدل مربع الخطأ يساوي (5.030398).

من خلال التجارب السابقة نلاحظ إنّ قيمة نسبة قمة الإشارة إلى الضوضاء بين صورتي الغطاء والناتجة تتراوح بين (22.9-25.3) والجذر التربيعي لمعدل مربع الخطأ يتراوح بين (13.8-18.9) أمّا بالنسبة إلى الصورة المسترجعة فإنّ قيمة نسبة قمة الإشارة إلى الضوضاء تتراوح بين (29.8-34.1) والجذر التربيعي لمعدل مربع الخطأ يتراوح بين (5.0-8.3) وهي قيم مقبولة لان النتائج التي تم الحصول عليها والتشوهات الناتجة من عملية الإخفاء قليلة وغير مدركة بالنسبة إلى الصورة الناتجة (**Stego-image**) وقد تظهر وكأنها ضوضاء ، أما بالنسبة الى الصورة المسترجعة فتظهر فيها تشوهات قليلة ويعود السبب الى ان الصورة الملونة ذات (256) لونا لاتوفر مساحة كبيرة (**كل عنصر يمثل بثمانية واحدة**) كما ان اربع ثنائيات لا تكون كافية لاسترجاع الصورة زيادة على كبر حجم الصورة الذي يزيد من مقدار الخطأ التراكمي ،في حين اننا نحتاج إلى اخفاء لوحة الالوان ،ولكن اجراء مرحلة اختبار بين الصورتين (**الغطاء والمخفية**) يجعل تاثير عملية الخفاء قليلا .

الطريقةالأولى/التجربة رقم(3)

في هذه التجربة تم تنفيذ الطريقة الأولى على صور ذات تدرج رمادي .

يوضح الشكل(3-7) الصور الأصلية والناتجة(المسترجعة) .

صورة الغطاء

الصورة المخفية

الصورة الناتجة بعد الإخفاء

الصورة المسترجعة

الشكل (3-7)

وقد كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء **(Cover Image)** والصورة الناتجة بعد الإخفاء **(Stego Image)** تساوي(31.480391 db) ،أما الجذر التربيعي لمعدل مربع الخطأ فيساوي (6.800183).أما بالنسبة إلى الصورة المخفية **(Embedded Image)** والصورة المسترجعة (**Extracted Image)** فإن نسبة قمة الإشارة إلى الضوضاء تساوي (29.854637db) والجذر التربيعي لمعدل مربع الخطأ يساوي(8.199895).

يوضح الشكل (3-8) الصور الأصلية والناتجة(المسترجعة) .

الصورة الغطاء

الصورة المخفية

الصورة الناتجة بعد الإخفاء

الصورة المسترجعة

الشكل (3-8)

كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء **(Cover Image)** والصورة الناتجة بعد الإخفاء **(Stego Image)** تساوي(32.028707 db) ،أما الجذر التربيعي لمعدل مربع الخطأ فيساوي (6.384174).أما بالنسبة إلى الصورة المخفية **(Embedded Image)** والصورة المسترجعة (**Extracted Image)** فإن نسبة قمة الإشارة إلى الضوضاء تساوي (30.996215db) والجذر التربيعي لمعدل مربع الخطأ يساوي(7.190008).

يوضح الشكل(3-9) الصور الأصلية والناتجة(المسترجعة) .

الشكل (3-9)

لقد كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء (**Cover Image**) والصورة الناتجة بعد الإخفاء (**Stego Image**) تساوي(db 32.661784) ،أما الجذر التربيعي لمعدل مربع الخطأ فيساوي (5.935412).أما بالنسبة إلى الصورة المخفية (**Embedded Image**) والصورة المسترجعة (**Extracted Image**) فإن نسبة قمة الإشارة إلى الضوضاءتساوي (30.909377db) والجذر التربيعي لمعدل مربع الخطأ يساوي(7.262293).

من خلال التجارب السابقة نلاحظ أن قيمة نسبة قمة الإشارة إلى الضوضاء بين صورتي الغطاء والناتجة تتراوح بين (31.5-32.7) و الجذر التربيعي لمعدل مربع الخطأ يتراوح بين (5.9-6.4) أما بالنسبة للصورة المسترجعة فإن قيمة نسبة قمة الإشارة إلى الضوضاء تتراوح بين (29.9-31.0) و الجذر التربيعي لمعدل مربع الخطأ يتراوح بين (7.2-8.2) وهي قيم جيدة لان النتائج التي تمالتوصل إليها جيدة ولا تحتوي على أي تشوهات. أي ان تأثير عملية الإخفاء يكون معدوما وذلك لان الصور ذات التدرجات الرمادية تتميز بانها ذات تغيرات تدريجية في الشدة اللونية بين العناصر ،وإنّ استبدال الثنائيات الأربعة الأقل أهمية لن يؤثر على

الصورة الناتجة كذلك اخفاء اربع ثنائيات تكون كافية لاسترجاع صورة جيدة وهذا يجعل هذا النوع من الصور ذا فعالية كبيرة في عملية الاخفاء .

الطريقةالأولى/التجربة رقم (4)

في هذه التجربة تم إخفاء صور ذات تدرج رمادي داخل صور ملونة (256) لونا .

يوضح الشكل (3-10) الصور الأصلية والناتجة(المسترجعة).

الشكل (3-10)

وقد كانت قمة نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء (**Cover Image**) والصورة الناتجة بعد الإخفاء (**Stego Image**) تساوي(32.939194 db) ،أما الجذر التربيعي لمعدل مربع الخطأ فيساوي (5.748842).أما بالنسبة إلى الصورة المخفية (**Embedded Image**) والصورة المسترجعة (**Extracted Image**) فإن نسبة قمة الإشارة إلى الضوضاءتساوي (33.087196db) والجذر التربيعي لمعدل مربع الخطأ يساوي(5.651716).

يوضح الشكل(3-11) الصور الأصلية والناتجة(المسترجعة) .

صورة الغطاء

الصورة المخفية

الصورة الناتجة بعد الإخفاء

الصورة المسترجعة

الشكل (3-11)

وقد كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء **(Cover Image)** والصورة الناتجة بعد الإخفاء **(Stego Image)** تساوي(32.033660db) ، أما الجذر التربيعي لمعدل مربع الخطأ فيساوي (6.380536). أما بالنسبة إلى الصورة المخفية **(Embedded Image)** والصورة المسترجعة **(Extracted Image)** فإن نسبة قمة الإشارة إلى الضوضاء تساوي (30.088426db) والجذر التربيعي لمعدل مربع الخطأ يساوي (7.982131).

يوضح الشكل(3-12) الصور الأصلية والمسترجعة .

صورة الغطاء

الصورة المخفية

الصورة الناتجة بعد الإخفاء

الصورة المسترجعة

الشكل (3-12)

وقد كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء (**Cover Image**) والصورة الناتجة بعد الإخفاء (**Stego Image**) تساوي(31.859218 db) ،أما الجذر التربيعي لمعدل مربع الخطأ فيساوي (6.509973).أما بالنسبة إلى الصورة المخفية (**Embedded Image**) والصورة المسترجعة (**Extracted Image**) فإن نسبة قمة الإشارة إلى الضوضاء تساوي (29.045674db) والجذر التربيعي لمعدل مربع الخطأ يساوي(9.045674).

من خلال التجارب السابقة نلاحظ أن قيمة نسبة قمة الإشارة إلى الضوضاء بين صورتي الغطاء والناتجة تتراوح بين (31.9-32.9) و الجذر التربيعي لمعدل مربع الخطأ يتراوح بين (5.7-6.5) أما بالنسبة للصورة المسترجعة فإن قيمة نسبة قمة الإشارة إلى الضوضاء تتراوح بين (30.1-33.1) و الجذر التربيعي لمعدل مربع

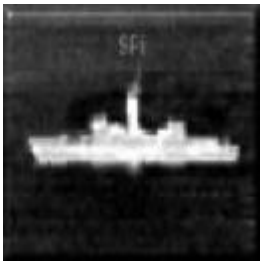
الخطأ يتراوح بين (5.7-9.0) وهي قيم جيدة لان النتائج التي تم التوصل إليها جيدة ولا تحتوي على أي تشوهات أي ان تأثير عملية الإخفاء يكون قليلا وذلك لاستعمال الثنائيات الأربعة الأقل يـة **(مستوى الضوضاء)** كذلك اخفاء اربع ثنائيات تكون كافية لاسترجاع صورة جيدة.

الطريقةالأولى/التجربة رقم(5)

لمعرفة مدى تأثير الضوضاء في هذه الطريقة ،فقد تم استعمال الصورتين **(Exp,Ship4)** وهي من الصور الحرارية**(Filer Images)** التي يتم التقاطها في ظروف خاصة وتمتاز باحتوائها على ضوضاء عالية،مما يجعل عملية الإخفاء فيها تكون صعبة .

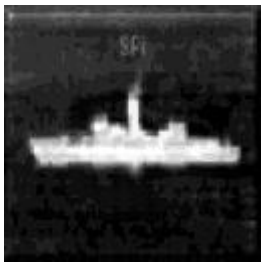
يوضح الشكل(3-13) الصور الأصلية والمسترجعة .

صورة الغطاء



الصورة المخفية

الصورة الناتجة بعد الإخفاء



الصورة المسترجعة

الشكل (3-13)

وقد كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء **(Cover Image)** والصورة الناتجة بعد الإخفاء **(Stego Image)** تساوي(30.493449 db) ،أما الجذر التربيعي لمعدل مربع الخطأ فيساوي(7.618469).أما بالنسبة إلى الصورة المخفية **(Embedded Image)** والصورة المسترجعة

(Extracted Image) فإن نسبة قمة الإشارة إلى الضوضاء تساوي (31.123696db) والجذر التربيعي لمعدل مربع الخطأ يساوي (7.085252).

على الرغم من إنّ هذا النوع من الصور يحتوي على ضوضاء إلا أنّ النتائج كانت جيدة لكلا الصورتين الناتجة والمسترجعة ،كما انهما لاتحتويان على أي تشوهات نتيجة الاخفاء وذلك لاستخدام الثنائيات الاقل اهمية **(مستوى الضوضاء)** كما ان اخفاء اربع ثنائيات تكون كافية لاسترجاع صورة جيدة.

الطريقة الأولى/التجربة رقم(6)

في هذه التجربة تم إخفاء صورة ذات تدرج رمادي داخل صورة حرارية .

يوضح الشكل(3-14) الصور الأصلية والناتجة(المسترجعة) .

صورة الغطاء

الصورة المخفية

الصورة الناتجة بعد

الصورة المسترجعة

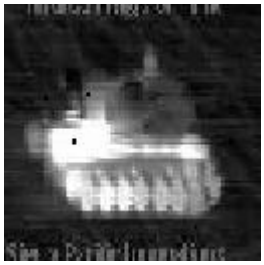
الشكل (3-14)

وقد كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء **(Cover Image)** والصورة الناتجة بعد الإخفاء **(Stego Image)** تساوي(29.406477 db) ،أما الجذر التربيعي لمعدل مربع الخطأ فيساوي(8.634085).أما بالنسبة إلى الصورة المخفية **(Embedded Image)** والصورة المسترجعة

(Extracted Image) فإن نسبة قمة الإشارة إلى الضوضاء تساوي (37.182215db) والجذر التربيعي لمعدل مربع الخطأ يساوي(3.527194).

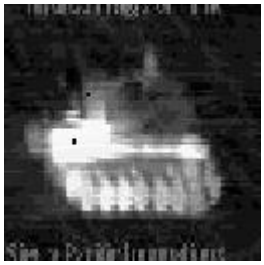
من خلال التجربة أعلاه نلاحظ ان إخفاء صورة ذات تدرج رمادي داخل صورة حرارية يعطي نتائجا جيدة وإنّ كلا الصورتين لا تحتويان على أي تشوهات لاستعمال الثنائيات الاقل أهمية ، كذلك إخفاء اربع ثنائيات كافية لاسترجاع صورة جيدة .

الشكل (3- 15) يوضح إخفاء صورة حرارية داخل صورة ذات تدرج رمادي .



الصورة المخفية

صورة الغطاء



الصورة المسترجعة

الصورة الناتجة بعد

الشكل (3-15)

وقد كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء **(Cover Image)** والصورة الناتجة بعد الإخفاء **(Stego Image)** تساوي(29.689414 db) ،أما الجذر التربيعي لمعدل مربع الخطأ فيساوي(8.357366).أما بالنسبة إلى الصورة المخفية **(Embedded Image)** والصورة المسترجعة **(Extracted Image)** فإن نسبة قمة الإشارة إلى الضوضاء تساوي (30.694656db) والجذر التربيعي لمعدل مربع الخطأ يساوي(7.444017).

من خلال التجربة المذكورة آنفا نلاحظ أنّ إخفاء صورة حرارية داخل صورة ذات تدرج رمادي يعطي نتـائج

جيدة وإنّ كلا الصورتين لا تحتويان على أي تشوهات لاستعمال الثنائيات الاقل أهمية ، وإنّ إخفاء اربع ثنائيات

كافية لاسترجاع صورة جيدة .

3-1-2 الطريقة الثانية / التجربة رقم (1)

في هذه التجربة تم إخفاء صوملونة ذات (256) لونا داخل صور طبيعية .

يوضح الشكل(3-16) الصور الأصلية والناتجة(المسترجعة) .

صورة الغطاء

الصورة المخفية

الصورة الناتجة بعد الإخفاء

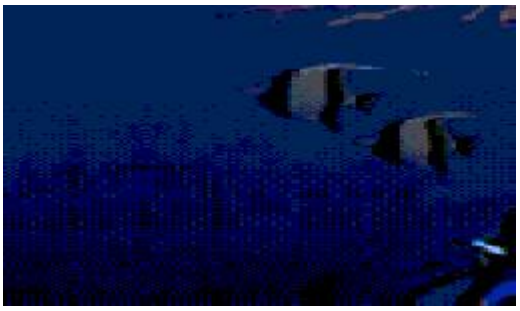
الصوة المسترجعة

الشكل (3-16)

وقد كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء (**Cover Image**) والصورة الناتجة بعد الإخفاء (**Stego Image**) تساوي(22.371142 db) ،أما الجذر التربيعي لمعدل مربع الخطأ فيساوي (19.408102).أما بالنسبة إلى الصورة المخفية (**Embedded Image**) والصورة المسترجعة (**Extracted Image**) فإن نسبة قمة الإشارة إلى الضوضاءتساوي (29.513614 db) والجذر التربيعي لمعدل مربع الخطأ يساوي (8.528240).

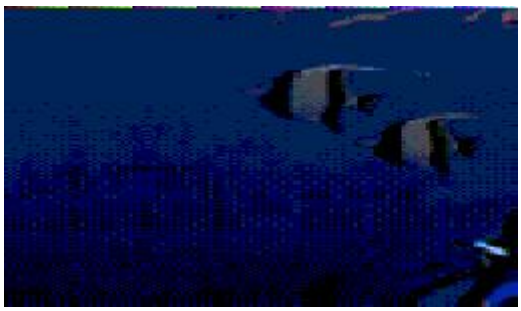
يوضح الشكل(3-17) الصور الأصلية والناتجة (المسترجعة) .

صورة الغطاء



الصورة المخفية

الصورة الناتجة بعد الإخفاء

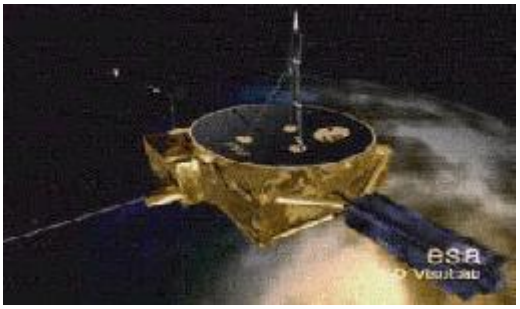


الصورة المسترجعة

الشكل (3-17)

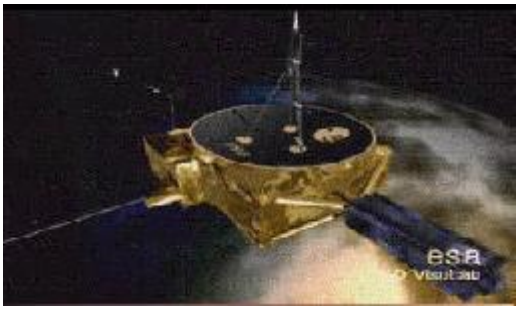
وقد كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء (**Cover Image**) والصورة الناتجة بعد الإخفاء (**Stego Image**) تساوي(21.751729 db) ،أما الجذر التربيعي لمعدل مربع الخطأ فيساوي (20.842685).أما بالنسبة إلى الصورة المخفية (**Embedded Image**) والصورة المسترجعة (**Extracted Image**) فإن نسبة قمة الإشارة إلى الضوضاءتساوي (27.436410 db) والجذر التربيعي لمعدل مربع الخطأ يساوي (10.832274).

يوضح الشكل(3-18) الصور الأصلية والناتجة(المسترجعة) .



صورة الغطاء

الصورة المخفية



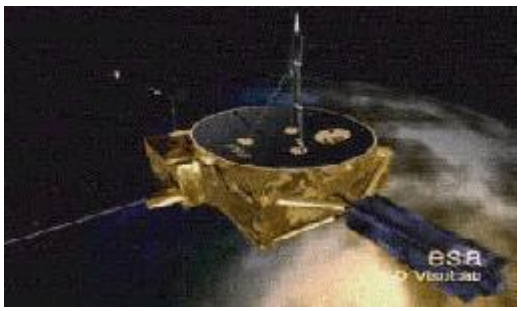
الصورة الناتجة بعد الاخفاء

الصورة المسترجعة

الشكل (3-18)

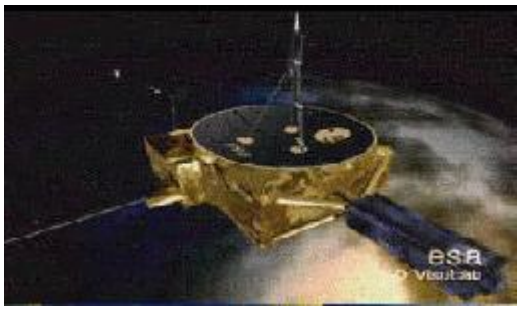
وقد كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء (**Cover Image**) والصورة الناتجة بعد الإخفاء (**Stego Image**) تساوي(26.508079 db) ،أما الجذر التربيعي لمعدل مربع الخطأ فيساوي (12.054138).أما بالنسبة إلى الصورة المخفية (**Embedded Image**) والصورة المسترجعة (**Extracted Image**) فإن نسبة قمة الإشارة إلى الضوضاءتساوي (28.288707 db) والجذر التربيعي لمعدل مربع الخطأ يساوي (9.819848).

يوضح الشكل(3–19) الصور الأصلية والناتجة(المسترجعة) .



صورة الغطاء

الصورة المخفية



الصورة الناتجة بعد الإخفاء

الصورة المسترجعة

الشكل (3-19)

وقد كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء (**Cover Image**) والصورة الناتجة بعد الإخفاء (**Stego Image**) تساوي(24.685003 db) ،أما الجذر التربيعي لمعدل مربع الخطأ فيساوي (14.869281).أما بالنسبة إلى الصورة المخفية (**Embedded Image**) والصورة المسترجعة (**Extracted Image**) فإن نسبة قمة الإشارة إلى الضوضاءتساوي (30.178613 db) والجذر التربيعي لمعدل مربع الخطأ يساوي (7.899680).

يوضح الشكل(3-20) الصور الأصلية والمسترجعة .

صورة الغطاء

الصورة المخفية

الصورة الناتجة بعد الاخفاء

الصورة المسترجعة

الشكل (3-20)

وقد كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء (**Cover Image**) والصورة الناتجة بعد الإخفاء (**Stego Image**) تساوي(24.288127 db) ،أما الجذر التربيعي لمعدل مربع الخطأ فيساوي (15.564450).أما بالنسبة إلى الصورة المخفية (**Embedded Image**) والصورة المسترجعة (**Extracted Image**) فإن نسبة قمة الإشارة إلى الضوضاءتساوي (30.178613 db) والجذر التربيعي لمعدل مربع الخطأ يساوي (7.899680).

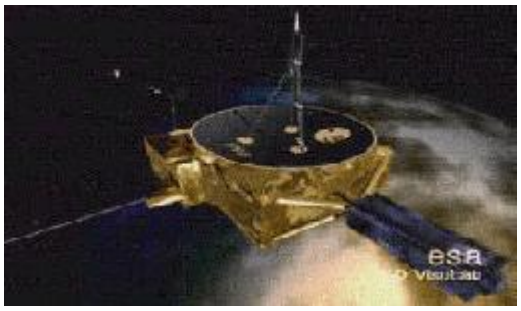
من خارب السابقة نلاحظ أنّ قيمة نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء والصورة الناتجة تتراوح بين (21.8-26.5) والجذر التربيعي لمعدل مربع الخطأ يتراوح بين (12.1-20-8) أما بالنسبة لى الصورة المسترجعة فإن قيمة نسبة قمة الإشارة إلى الضوضاء تتراوح بين (27.4-30.2) والجذر التربيعي ل مربع الخطأ يتراوح بين (7.9-10.8) وهي قيم جيدة لان النتائج التي تم الحصول عليها لا تحتوي على أي تشوهات وذلك لاستعمال الثنائيات الاقل أهمية زيادة على أنّ اخفاء صورة ملونات (256) لونا داخل صورة طبيعية تعادل ثلاثة اضعافها تقريبا يجعل

ر عمليـــة الإخفاء معدوما كذلك تم إخفاء الصورة المخفية بكاملها وليس فقط الثنائيات الاقل أهمية وبهذا فإنّ الصورة المسترجعة تكون جيدة .

الطريقة الثانية/التجربة رقم (2)

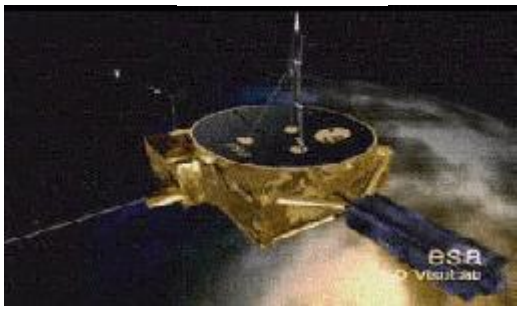
في هذه التجربة تم إخفاء صور ذات تدرج رمادي لون داخل صور طبيعية .

يوضح الشكل(3-21) الصور الأصلية والناتجة(المسترجعة) .



صورة الغطاء

الصورة المخفية



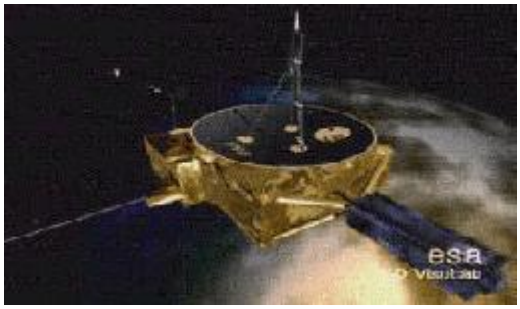
الصورة الناتجة بعد الإخفاء

الصورة المسترجعة

الشكل (3-21)

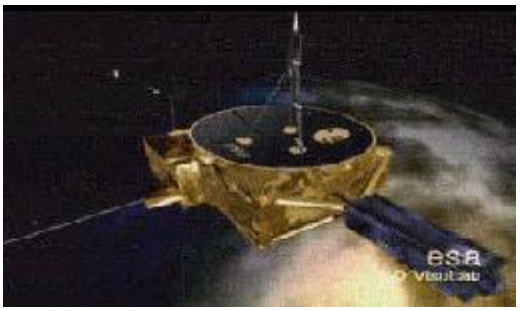
وقد كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء **(Cover Image)** والصورة الناتجة بعد الإخفاء **(Stego Image)** تساوي(db 29.766512) ،أما الجذر التربيعي لمعـــدل مربـــع الخطـــأ فيســـاوي (8.283513).أما بالنسبة إلى الصورة المخفية **(Embedded Image)** والصورة المسترجعة **(Extracted Image)** فإ التربيعي لمعدل مربع الخطأ يساوي (0) وهذا يعني أنّ نسبة قمة الإشارة إلى الضوضـــاء تساوي قيمة كبيرة تقترب الى ما لانهاية .

يوضح الشكل(3-22) الصور الأصلية والناتجة(المسترجعة) .



صورة الغطاء

الصورة المخفية



الصورة الناتجة بعد الإخفاء

الصورة المسترجعة

الشكل (3-22)

وقد كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء (**Cover Image**) والصورة الناتجة بعد الإخفاء (**Stego Image**) تساوي(29.555064 db) ،أما الجذر التربيعي لمعدل مربع الخطأ فيساوي (8.487639).أما بالنسبة إلى الصورة المخفية (**Embedded Image**) والصورة المسترجعة (**Extracted Image**) فإن تربيعي لمعدل مربع الخطأ يساوي (0) وهذا يعني ان نسبة قمة الإشارة إلى الضوضاء تساوي قيمة كبيرة تقترب الى ما لانهاية .

يوضح الشكل(3-23) الصور الأصلية والناتجة(المسترجعة) .

صورة الغطاء

الصورة المخفية

الصورة الناتجة بعد الإخفاء

الصورة المسترجعة

الشكل (3-23)

وقد كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء (**Cover Image**) والصورة الناتجة بعد الإخفاء (**Stego Image**) تساوي(28.841738 db) ،أما الجذر التربيعي لمعدل مربع الخطأ فيساوي (9.214106).أما بالنسبة إلى الصورة المخفية (**Embedded Image**) والصورة المسترجعة (**Extracted Image**) فإن الجذري لمعدل مربع الخطأ يساوي (0) وهذا يعني ان نسبة قمة الإشارة إلى الضوضاء تساوي قيمة كبيرة تقترب الى ما لانهاية .

يوضح الشكل(3-24)الصور الأصلية والناتجة(المسترجعة) .

صورة الغطاء

الصورة المخفية

الصورة الناتجة بعد الإخفاء

الصورة المسترجعة

الشكل (3-24)

وقد كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء (**Cover Image**) والصورة الناتجة بعد الإخفاء (**Stego Image**) تساوي(32.544405 db) ،أما الجذر التربيعي لمعدل مربع الخطأ فيساوي (6.016167).أما بالنسبة إلى الصورة المخفية (**Embedded Image**) والصورة المسترجعة (**Extracted Image**) فإن تربيعي لمعدل مربع الخطأ يساوي (0) وهذا يعني ان نسبة قمة الإشارة إلى الضوضاء تساوي قيمة كبيرة تقترب الى ما لانهاية .

من خلال التجارب السابقة نلاحظ أنّ قيمة نسبة قمة الإشارة إلى الضوضاء بين صورتي الغطاء والناتجة تتراوح بين (28.8-32.5) والجذر التربيعي لمعدل مربع الخطأ يتراوح بين (6.0-9.2) أما بالنسبة إلى الصورة المسترجعة فإن الجذر النل مربع الخطأ يساوي (0) أي ان الصورة المسترجعة تطابق الصورة

المخفية الاصلية وهذا يعني أنّ قيمة نسبة الإشارة إلى الضوضاء تكون كبيرة وتقترب لى ما لانهاية .إنّ النتائج التي تم الحصول عليها جيدة و لا تحتوي على أي تشوهات

نتيجة عملية الإخفاء ويعود سبب ذلك لإاع الصور المستعملة **(حيث يتم اخفـــاء صـــور ذات تـــدرج رمادبطبيعية تعادل حجمها بثلاث مرات)** ،كذلك اســـتعمال التثائيـــات الاقـــل أهميـــة (مســـتوى الضوضاء) واجراء مرحلة اختبار للتوافق بين صورتي الغطاء والمخفية يجعل تاثير عملية الاخفاء غير مدرك .

3-1-3 الطريقة الثالثة/التجربة رقم (1)

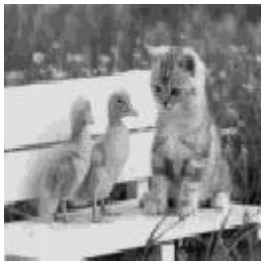
في هذه التجربة تم تنفيذ الطريقة الثالثة على صور ذات تدرج رمادي .

يوضح الشكل(3-25) الصور الأصلية والناتجة(المسترجعة) .

صورة الغطاء

الصورة المخفية

الصورة الناتجة بعد الإخفاء



الصورة المسترجعة

الشكل (3-25)

وقد كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء (**Cover Image**) والصورة الناتجة بعد الإخفاء (**Stego Image**) تساوي (34.723078 db) ،أما الجذر التربيعي لمعدل مربع الخطأ فيساوي (4.681513).أما بالنسبة إلى الصورة المخفية (**Embedded Image**) والصورة المسترجعة (**Extracted Image**) فإن نسبة قمة الإشارة إلى الضوضاءتساوي (29.115893 db) والجذر التربيعي لمعدل مربع الخطأ فيساوي (8.927821).

يوضح الشكل(3-26) الصور الأصلية والناتجة(المسترجعة) .

صورة الغطاء

الصورة المخفية

سورة الناتجة بعد الإخفاء

الصورة المسترجعة

الشكل (3-26)

وقد كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء (**Cover Image**) والصورة الناتجة بعد الإخفاء (**Stego Image**) تساوي(34.147789 db) ،أما الجذر التربيعي لمعدل مربع الخطأ فيساوي (5.002080).أما بالنسبة إلى الصورة المخفية (**Embedded Image**) والصورة المسترجعة (**Extracted Image**) فإن نسبة قمة الإشارة إلى الضوضاءتساوي (28.870576 db) والجذر التربيعي لمعدل مربع الخطأ يساوي (9.183566).

يوضح الشكل(3-27) الصور الأصلية والناتجة(المسترجعة) .

الصورة المخفية

صورة الغطاء

الصورة المسترجعة

الصورة الناتجة بعد الإخفاء

الشكل (3-27)

وقد كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء (**Cover Image**) والصورة الناتجة بعد الإخفاء (**Stego Image**) تساوي(34.921631 db) ،أما الجذر التربيعي لمعدل مربع الخطأ فيساوي (4.575711).أما بالنسبة إلى الصورة المخفية (**Embedded Image**) والصورة المسترجعة (**Extracted Image**) فإن نسبة قمة الإشارة إلى الضوضاءتساوي (28.200404 db) والجذر التربيعي لمعدل مربع الخطأ يساوي (9.920189).

من خلال التجارب السابقة نلاحظ أنّ قيمة نسبة قمة الإشارة إلى الضوضاء بين صورتي الغطاء والناتجة تتراوح بين (34.1-34.9) والجذر التربيعي لمعدل مربع الخطأ يتراوح بين (4.6-5.0) أما بالنسبة إلى الصورة المسترجعة فإنّ قيمة نسبة قمة الإشارة إلى الضوضاء تتراوح بين (28.2-29.1) والجذر التربيعي لمعدل مربع

الأ يتراوح بين (8.9-10.2) وهي قيم جيدة لان النتائج التي تم الحصول عليها جيدة ولا تحتـــوي علـــى أي تشوهات نتيجة عملية الإخفاء وذلك لاستعمال الاسلوب الرياضي ، إذ إنّ بيانات الصورة المراد إخفاؤها تـــدمج مع صورة الغطاء .

الطريقة الثالثة/التجربة رقم (2)

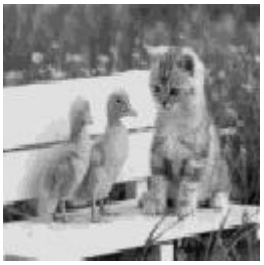
في هذه التجربة تم إخفاء صور ذات تدرج رمادي داخل صور ملونة(256) لونا.

يوضح الشكل(3-28) الصور الأصلية والناتجة (المسترجعة) .

صورة الغطاء

الصورة المخفية

الصورة الناتجة بعد الاخفاء



الصورة المسترجعة

الشكل (3-28)

وقد كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء (**Cover Image**) والصورة الناتجة بعد الإخفاء (**Stego Image**) تساوي(34.482301 db) ،أما الجذر التربيعي لمعـــدل مربـــع الخطـــأ فيســـاوي (4.813102).أما بالنسبة إلى الصورة المخفية (**Embedded Image**) والصورة المسترجعة (**Extracted Image**) فإن نسبة قمة الإشارة إلى الضوضاءتساوي (29.115893 db) والجذر التربيعي لمعدل مربع الخطأ يساوي (8.927821).

يوضح الشكل(3-29) الصور الأصلية والناتجة (المسترجعة) .

الصورة المخفية

صورة الغطاء

الصورة المسترجعة

الصورة الناتجة بعد الاخفاء

الشكل (3-29)

وقد كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء (**Cover Image**) والصورة الناتجة بعد الإخفاء (**Stego Image**) تساوي(34.418906 db) ،أما الجذر التربيعي لمعدل مربع الخطأ فيساوي (4.848359).أما بالنسبة إلى الصورة المخفية (**Embedded Image**) والصورة المسترجعة (**Extracted Image**) فإن نسبة قمة الإشارة إلى الضوضاء تساوي (27.970268 db) والجذر التربيعي لمعدل مربع الخطأ يساوي (10.186541).

يوضح الشكل(3-30) الصور الأصلية والناتجة (المسترجعة) .

الصورة المخفية

صورة الغطاء

الصرة المسترجعة

وقد كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء (**Cover Image**) والصورة الناتجة بعد الإخفاء (**Stego Image**) تساوي(34.372069 db) ،أما الجذر التربيعي لمعدل مربع الخطأ فيساوي (4.874574).أما بالنسبة إلى الصورة المخفية (**Embedded Image**) والصورة المسترجعة (**Extracted Image**) فإن نسبة قمة الإشارة إلى الضوضاءتساوي (28.831518 db) والجذر التربيعي لمعدل مربع الخطأ يساوي (9.224954).

من خلال التجارب السابقة نلاحظ إن قيمة نسبة قمة الإشارة إلى الضوضاء بين صورتي الغطاء والناتجة تتراوح بين (34.4-34.5) والجذر التربيعي لمعدل مربع الخطأ يتراوح بين (4.8-9.9) أما بالنسبة إلى الصورة المسترجعة فإن قيمة نسبة قمة الإشارة إلى الضوضاء تتراوح بين (28.0-29.1) والجذر التربيعي لمعدل مربع الخطأ يتراوح بين (8.9-10.2) وهي قيم مقبولة لان النتائج التي تم الحصول عليها مقبولة والتشوهات الناتجة من عملية الإخفاء تكون قليلة وذلك لاستعمال الاسلوب الرياضي ، إذ إنّ بيانات الصورة المراد إخفاؤها تدمج مع صورة الغطاء .

الطريقة الثالثة/التجربة رقم (3)

في هذه التجربة تم تنفيذ الطريقة الثالثة على صور ملونة(256) لون.

يوضح الشكل(3-31) الصور الأصلية والناتجة(المسترجعة) .

صورة الغطاء

الصورة المخفية

وقد كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء **(Cover Image)** والصورة الناتجة بعد الإخفاء **(Stego Image)** تساوي(35.476932 db) ،أما الجذر التربيعي لمعدل مربع الخطأ فيساوي (4.292334).أما بالنسبة إلى الصورة المخفية **(Embedded Image)** والصورة المسترجعة (**Extracted Image)** فإن نسبة قمة الإشارة إلى الضوضاء تساوي (22.793583 db) والجذر التربيعي لمعدل مربع الخطأ يساوي (18.486768).

يوضح الشكل(3-32) الصور الاصلية والناتجة (المسترجعة) .

الشكل (3-32)

وقد كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء **(Cover Image)** والصورة الناتجة بعد الإخفاء **(Stego Image)** تساوي(35.373633 db) ،أما الجذر التربيعي لمعدل مربع الخطأ فيساوي (4.343686).أما بالنسبة إلى الصورة المخفية **(Embedded Image)** والصورة المسترجعة (Extracted Image) فإن نسبة قمة الإشارة إلى الضوضاءساوي (22.793583 db) والجذر التربيعي لمعدل مربع الخطأ يساوي (18.486768).

يوضح الشكل(3-33) الصور الاصلية والناتجة (المسترجعة) .

صورة الغطاء

الصورة المخفية

الصورة الناتجة بعد الاخفاء

الصورة السترجعة

الشكل (3-33)

وقد كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء (**Cover Image**) والصورة الناتجة بعد الإخفاء (**Stego Image**) تساوي(35.314068 db) ،أما الجذر التربيعي لمعدل مربع الخطأ فيساوي (4.373576).أما بالنسبة إلى الصورة المخفية (**Embedded Image**) والصورة المسترجعة (**Extracted Image**) فإن نسبة قمة الإشارة إلى الضوضاءتساوي (23.703694 db) والجذر التربيعي لمعدل مربع الخطأ يساوي (16.647746).

ن خلال التجارب السابقة نلاحظ أنّ قيمة نسبة قمة الإشارة إلى الضوضاء بين صورتي الغطاء والناتجة تتراوح بين (35.3-35.5) والجذر التربيعي لمعدل مربع الخطأ يتراوح بين (4.3-4.4) أما بالنسبة إلى الصورة المسترجعة فإن قيمة نسبة قمة الإشارة إلى الضوضاء تتراوح بين (22.8-23.7) والجذر التربيعي لمعدل مربع الخطأ يتراوح بين (16.6-18.5) وهي قيم جيدة لان النتائج التي تم الحصول عليها جيدة وتاثير عملية الإخفاء غير مدرك وذلك لاستعمال الاسلوب الرياضي ، إذ إنّ بيانات الصورة المراد إخفاؤها تدمج مع صورة الغطاء .

الطريقة الثالثة/التجربة رقم (4)

في هذه التجربة تم تنفيذ الطريقة الثالثة على صور ملونة(256) لونا.

يوضح الشكل(3-34)الصور الاصلية والناتجة(المسترجعة) .

الصورة المخفية

صورة الغطاء

الصورة المسترجعة

الصورة الناتجة بعد الاخفاء

الشكل (3-34)

وقد كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء (**Cover Image**) والصورة الناتجة بعد الإخفاء (**Stego Image**) تساوي(23.280062 db) ،أما الجذر التربيعي لمعدل مربع الخطأ فيساوي (17.479823).أما بالنسبة إلى الصورة المخفية (**Embedded Image**) والصورة المسترجعة (**Extracted Image**) فإن نسبة قمة الإشارة إلى الضوضاءتساوي (29.715874 db) والجذر التربيعي لمعدل مربع الخطأ يساوي (8.331946).

يوضح الشكل(3-35)الصور الاصلية والناتجة(المسترجعة) .

الصورة المخفية

صورة الغطاء

الصورة المسترجعة

الصورة الناتجة بعد الاخفاء

الشكل (3-35)

وقد كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء **(Cover Image)** والصورة الناتجة بعد الإخفاء **(Stego Image)** تساوي(22.796741 db) ،أما الجذر التربيعي لمعدل مربع الخطأ فيساوي (18.480049).أما بالنسبة إلى الصورة المخفية **(Embedded Image)** والصورة المسترجعة **(Extracted Image)** فإن نسبة قمة الإشارة إلى الضوضاءتساوي (29.526493 db) والجذر التربيعي لمعدل مربع الخطأ يساوي (8.515604).

يوضح الشكل(3-36)الصور الاصلية والناتجة(المسترجعة) .

صورة الغطاء

الصورة المخفية

الصورة الناتجة بعد الاخفاء

الصورة المسترجعة

الشكل (3-36)

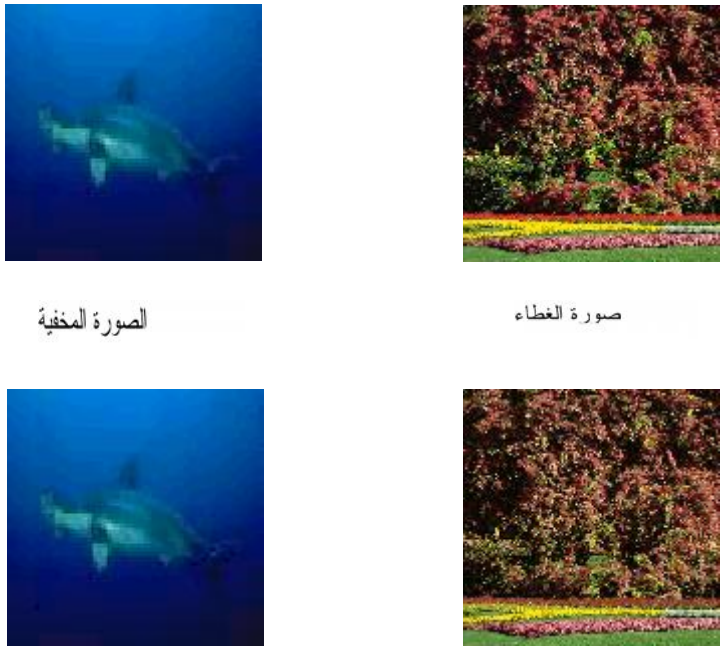
وقد كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء (**Cover Image**) والصورة الناتجة بعد الإخفاء (**Stego Image**) تساوي(db 23.263623) ،أما الجذر التربيعي لمعدل مربع الخطأ فيساوي (17.512937).أما بالنسبة إلى الصورة المخفية (**Embedded Image**) والصورة المسترجعة (**Extracted Image**) فإن نسبة قمة الإشارة إلى الضوضاء تساوي (29.715874) والجذر التربيعي لمعدل مربع الخطأ يساوي (8.331946).

من خلال التجارب السابقة نلاحظ أنّ قيمة نسبة قمة الإشارة إلى الضوضاء بين صورتي الغطاء والناتجة تتراوح بين (22.8-23.3) والجذر التربيعي لمعدل مربع الخطأ يتراوح بين (17.5-18.5)

أة إلى الصورة المسترجعة فإن قيمة نسبة قمة الإشارة إلى الضوضاء تتراوح بين (29.5-29.7) والجذر التربيعي لمعدل مربع الخطأ يتراوحين (8.3-8.5) وهي قيم مقبولة لان النتائج التي تم الحصول عليها مقبولة وتاثير عملية الإخفاء غير مدرك بالنسبة إلى الصورة الناتجة وذللستعمال الاسلوب الرياضي ، إذ إنّ بيانات الماؤها تدمج مع صورة الغطاء .اما بالنسبة الى الصورة المسترجعة فانها تحتوي على بعض التشوهات نتيجة لكبر حجم الصورة مما يزيد من مقدار الخطأ التراكمي .

3-1-4 الطريقة الرابعة/التجربة رقم(1)

في هذه التجربة تم تنفيذ النظام على مجموعة من الصور الملونة ذات (256) لونا .
يوضح الشكل(3-37) الصور الأصلية والناتجة(المسترجعة) .

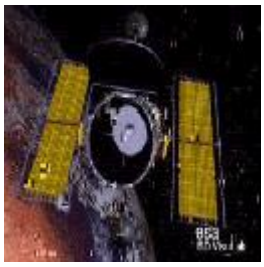


الشكل (3-37)

وقد كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء (**Cover Image**) والصورة الناتجة بعد الإخفاء (**Stego Image**) تساوي(28.748817 db) ،أما الجذر التربيعي لمعدل مربع الخطأ فيساوي (9.313207).أما بالنسبة إلى الصورة المخفية (**Embedded Image**) والصورة المسترجعة (**Extracted**

Image) فإن نسبة قمة الإشارة إلى الضوضاءتساوي (25.818673 db) والجذر التربيعي لمعدل مربع الخطأ يساوي (13.049880).

الشكل(3-38)يوضح الصور الاصلية والناتجة(المسترجعة) .



صورة الغطاء

الصورة المخفية

الصورة الناتجة بعد الاخفاء

الصورة المسترجعة

الشكل (3-38)

وقد كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء (**Cover Image**) والصورة الناتجة بعد الإخفاء (**Stego Image**) تساوي(27.943411 db) ،أما الجذر التربيعي لمعدل مربع الخطأ فيساوي (10.218086).أما بالنسبة إلى الصورة المخفية (**Embedded Image**) والصورة المسترجعة (**Extracted Image**) فإن نسبة قمة الإشارة إلى الضوضاءتساوي (29.860934 db) والجذر التربيعي لمعدل مربع الخطأ يساوي (8.193953).

الشكل(3–39) يوضح الصور الاصلية والناتجة(المسترجعة) .

صورة الغطاء

الصورة المخفية

سورة الناتجة بعد الاخفاء

الصورة المسترجعة

الشكل (3- 39)

وقد كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء **(Cover Image)** والصورة الناتجة بعد الإخفاء **(Stego Image)** تساوي(27.512501 db) ،أما الجذر التربيعي لمعدل مربع الخطأ فيساوي (10.737794).أما بالنسبة إلى الصورة المخفية **(Embedded Image)** والصورة المسترجعة (**Extracted Image)** فإن نسبة قمة الإشارة إلى الضوضاء تساوي (24.257634 db) والجذر التربيعي لمعدل مربع الخطأ يساوي (15.619188).

من خلال التجارب السابقة نلاحظ أن قيمة نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء والصورة الناتجاراوح بين (27.5-28.7) و الجذر التربيعي لمعدل مربع الخطأ يتراوح بين (9.3-10.7) أما بالنسبة للصورة المسترجعة فإن قيمة نسبة قمة الإشارة إلى الضوضاء تتراوح بين (24.3-29.9) و الجذر التربيعي لمعدل مربع الخطأ يتراوح بين (8.2-15.6) وقد كانت النتائج التي تم التوصل إليها جيدة وهي خالية من أي تشوهات باالى الصورة الناتجة **(Stego-image)** ويعود سبب ذلك الى مرحلة الضغط التي يتم فيها

بيانات الصوثم تخفى في صورة الغطاء (ليس فقط الثنائيات الاقل أهمية) .

التجربة رقم (2)

في هذه التجربة تم تنفيذ الطريقة الرابعة على صور ملونة ذات (256) لونا .

الشكل (3-40)يوضح الصور الاصلية والناتجة(المسترجعة) .

صورة الغطاء

الصورة المخفية

الصورة الناتجة بعد الإخفاء

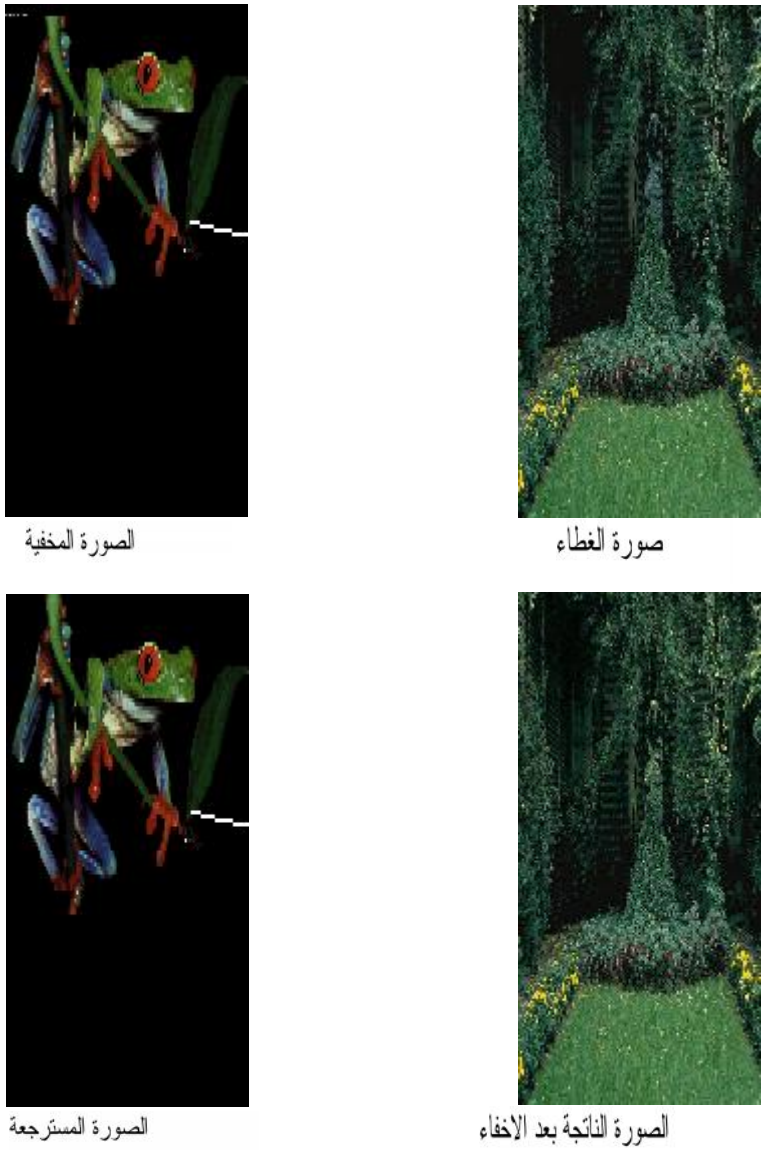
الصورة المسترجعة

الشكل (3-40)

وقد كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء **(Cover Image)** والصورة الناتجة بعد الإخفاء **(Stego Image)** تساوي(23.827977 db) ،أما الجذر التربيعي لمعدل مربع الخطأ فيساوي

(16.411235). أما بالنسبة إلى الصورة المخفية (**Embedded Image**) والصورة المسترجعة (Extracted Image) فإن اربيعي لمعدل مربع الخطأ يساوي (0) وهذا يعني ان نسبة قمة الإشارة إلى الضوضـــاء تاخذ قيمة كبيرة تقترب الى ما لانهاية.

الشكل (3-41)يوضح الصور الاصلية والناتجة (المسترجعة) .



الشكل (3-41)

وقد كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء (**Cover Image**) والصورة الناتجة بعد الإخفاء (**Stego Image**) تساوي(23.813831 db) ،أما الجذر التربيعي لمعـــدل مربـــع الخطـــأ فيســـاوي

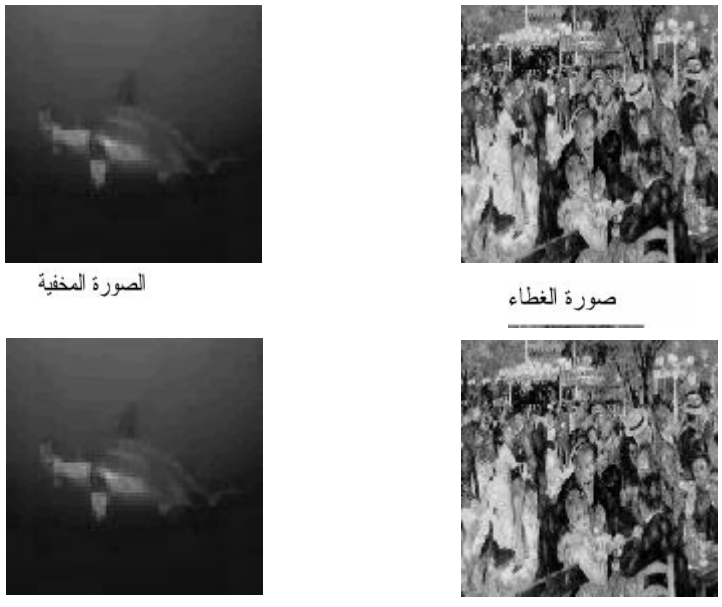
(16.437986). أما الجذر التربيعي لمعدل مربع الخطأ فيساوي (16.411235). أما بالنسبة إلى الصورة المخفية (**Embedded Image**) والصورة المسترجعة (Extracted Image) فإن الجذر التربيعي لمعدل مربع الخطأ يساوي (0) وهذا يعني ازسبة قمة الإشارة إلى الضوضاء تاخذ قيمة كبيرة تقترب الى ما لانهاية.

من خلال التجارب السابقة نلاحظ أن قيمة نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء والصورة لناتجة تتراوح بين (23.82-23.81) و الجذر التربيعي لمعدل مربع الخطأ يتراوح بين (16.43-16.41) أما سبة للصورة المسترجعة فإن الجذر التربيعي لمعدل مربع الخطأ يساوي (0) أي ان الصورة المسترجعة تطابق الصورة المخفية الاصلية تماما ،وهذا يعني أنّ نسبة قمة الإشارة إلى الضوضاء تاخذ قيمة كبيرة تقترب الى ما لانهاية ويعود سبب ذلك لان بيانات الصورة تضغط ثم تخصورة الغطاء (ليس فقط الثنائيات الاقل أهمية) ، زيادة على مرحلة الضغط التي يتم فيها تقليص حجم الصورة ومن ثمّ يكون تاثير عملية الإخفاء غير مدرك .

التجربة رقم(3)

في هذه التجربة تم تنفيذ الطريقة الرابعة على صور ذات تدرج رمادي .

يوضح الشكل(3-42) الصور الأصلية والناتجة (المسترجعة) .



الشكل (3-42)

وقد كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء (**Cover Image**) والصورة الناتجة بعد الإخفاء (**Stego Image**) تساوي(35.809724 db) ،أما الجذر التربيعي لمعدل مربع الخطأ يساوي (4.130988).أما بالنسبة إلى الصورة المخفية (**Embedded Image**) والصورة المسترجعة (Extracted Image) فإن اربيعي لمعدل مربع الخطأ يساوي (0) وهذا يعني ان نسبة قمة الإشارة إلى الضوضاء تاخذ قيمة كبيرة تقترب الى ما لانهاية.

الشكل(3-43)يوضح الصور الاصلية والناتجة(المسترجعة).

الصورة المخفية

صورة الغطاء

الصورة المسترجعة

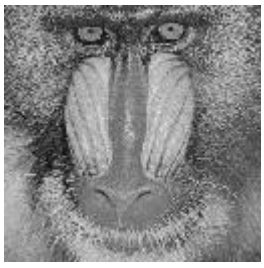
الصورة الناتجة بعد الاخفاء

الشكل (3-43)

وقد كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء (**Cover Image**) والصورة الناتجة بعد الإخفاء (**Stego Image**) تساوي(35.366516 db) ،أما الجذر التربيعي لمعدل مربع الخطأ يساوي (4.347247).أما بالنسبة إلى الصورة المخفية (**Embedded Image**) والصورة المسترجعة (**Extracted**

Image) فإن الجذر التربيعي لمعدل مربع الخطأ يساوي (0) وهذا يعني ان نسبة قمة الإشارة إلى الضوضـــاء تاخذ قيمة كبيرة تقترب الى ما لانهاية.

الشكل(3-44)يوضح الصور الاصلية والنائجة(المسترجعة) .



صورة الغطاء

الصورة المخفية

الصورة الناتجة بعد الاخفاء

الصورة المسترجعة

الشكل (3-44)

وقد كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء **(Cover Image)** والصورة الناتجة بعد الإخفاء **(Stego Image)** تساوي(35.769971 db) ،أما الجذر التربيعـــي لمعـــدل مربـــع الخطـــأ يســـاوي (4.149937).أما بالنسبة إلى الصورة المخفية **(Embedded Image)** والصورة المسترجعة (**Extracted Image)** فإن الجذر التربيعدل مربع الخطأ يساوي (0) وهذا يعني ان نسبة قمة الإشارة إلى الضوضـــاء تاخذ قيمة كبيرة تقترب الى ما لانهاية.

من خلال التجارب السابقة نلاحظ أن قيمة نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء والصورة الناتجة تتراوح بين (35.4-35.8) و الجذر التربيعي لمعدل مربع الخطأ يتراوح بين (4.1-4.3) أما بالنسبة للصورة المسترجعة فإن الجذر التربيعي له مربع الخطأ يساوي (0) أي ان الصـــورة المســـترجعة تطـــابق الصورة المخفية الاصلية تماما ،وهذا يعني أنّ نسبة قمة الإشارة إلى الضوضاء تاخذ قيمة كبيرة تقترب الى ما

لانهاية ويعود سبب ذلك لان بيانات الصورة تضغم في صورة الغطاء (ليس فقط الثنائيات الاقل أهمية)

، زيادة على مرحلة الضغط التي يتم فيها تقليص حجم الصورة ومن ثمَّ يكون تاثير عملية الإخفاء غير مدرك .

التجربة رقم(4)

في هذه التجربة تم إخفاء صورة ذات تدرج رمادي داخل صورة ملونة(256) لونا.

يوضح الشكل(**3–45**) الصور الأصلية والناتجة(المسترجعة) .

صورة الغطاء

الصورة المخفية

الصورة الناتجة بعد الاخفاء

الصورة المسترجعة

الشكل (3-45)

وقد كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء (**Cover Image**) والصورة الناتجة بعد الإخفاء (**Stego Image**) تساوي(35.513863) ،أما الجذر التربيعي لمعدل مربع الخطأ فيساوي (4.274123).أما بالنسبة إلى الصورة المخفية (**Embedded Image**) والصورة المسترجعة (**Extracted Image**) فإن تربيعي لمعدل مربع الخطأ يساوي (0) وهذا يعني ان نسبة قمة الإشارة إلى الضوضاء تكون كبيرة وتقترب الى ما لا نهاية .

الشكل(3-46)يوضح الصور الاصلية والنائجة(المسترجعة)

صورة الغطاء

الصورة المخفية

الصورة الناتجة بعد الاخفاء

اء الصورة المسترجعة

الشكل (3-46)

وقد كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء **(Cover Image)** والصورة الناتجة بعد الإخفاء **(Stego Image)** تساوي(29.816025) ،أما الجذر التربيعي لمعدل مربع الخطأ فيساوي (8.236427).أما بالنسبة إلى الصورة المخفية **(Embedded Image)** والصورة المسترجعة (**Extracted Image)** فإن نسبة قمة الإشارة إلى الضوضاء تساوي (38.043601) والجذر التربيعي لمعدل مربع الخطأ يساوي (3.194185).

الشكل(3-47)يوضح الصور الاصلية والنائجة(المسترجعة)

الشكل (3-47)

وقد كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء (**Cover Image**) والصورة الناتجة بعد الإخفاء (**Stego Image**) تساوي(32.389049) ،أما الجذر التربيعي لمعدل مربع الخطأ فيساوي (6.124740).أما بالنسبة إلى الصورة المخفية (**Embedded Image**) والصورة المسترجعة (**Extracted Image**) فإن نسبة قمة الإشارة إلى الضضاء تساوي (33.215058) والجذر التربيعي لمعدل مربع الخطأ يساوي (5.569128).

من خلال التجارب السابقة نلاحظ أن قيمة نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء والصورة الناتجة تتراوح بين (29.8-35.5) و الجذر التربيعي لمعدل مربع الخطأ يتراوح بين (4.3-8.2) أما بالنسبة رة المسترجعة فإن قيمة نسبة قمة الإشارة إلى الضوضاء تتراوح بين (قيمة كبيرة تقترب الى مالانهاية-33.2) اما الجذر التربيعي لمعدلع الخطأ فإنه يساوي (0-5.6) وقد كانت النتائج جيدة ويعود سبب ذلك لان بيانات الصوتم تخفى في صورة الغطاء (ليس فقط الثنائيات الاقل أهمية) ، زيادة على مرحلة الضغط التي يتم فيها تقليص حجم الصورة ومن ثمَّ يكون تاثير عملية الإخفاء غير مدرك .

3-1-5 الطريقة الخامسة/التجربة رقم(1)

في هذه التجربة تم تنفيذ النظام على مجموعة من الصور الملونة ذات (256) لونا .

يوضح الشكل(3-48) الصور الأصلية والناتجة(المسترجعة) .

وقد كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء (**Cover Image**) والصورة الناتجة بعد الإخفاء (**Stego Image**) تساوي(29.624815 db) ،أما الجذر التربيعي لمعدل مربع الخطأ فيساوي (8.419753).أما بالنسبة إلى الصورة المخفية (**Embedded Image**) والصورة المسترجعة (**Extracted Image**) فإن نسبة قمة الإشارة إلى الضوضاءتساوي (15.919170 db) والجذر التربيعي لمعدل مربع الخطأ يساوي (40.792623).

الشكل(3-49)يوضح الصور الاصلية والناتجة(المسترجعة) .

وقد كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء (**Cover Image**) والصورة الناتجة بعد الإخفاء (**Stego Image**) تساوي(27.148887 db)27 ،أما الجذر التربيعي لمعدل مربع الخطأ فيساوي

الشكل (3-49)

(11.196884).أما بالنسبة إلى الصورة المخفية (**Embedded Image**) والصورة المسترجعة (**Extracted Image**) فإن نسبة قمة الإشارة إلى الضوضاء تساوي (16.093882 db) وإنّ الجذر التربيعي لمعدل مربع الخطأ يساوي (39.980300).

الشكل (3-50) يوضح الصور الاصلية والناتجة(المسترجعة) .

الشكل (3-50)

وقد كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء (**Cover Image**) والصورة الناتجة بعد الإخفاء (**Stego Image**) تساوي(28.358963 db) ،أما الجذر التربيعي لمعدل مربع الخطأ فيساوي (9.740740).أما بالنسبة إلى الصورة المخفية (**Embedded Image**) والصورة المسترجعة (**Extracted Image**) فإن نسبة قمة الإشارة إلى الضوضاء تاوي (16.540076 db) وإنّ الجذر التربيعي لمعدل مربع الخطأ يساوي (37.978373).

الشكل(3-51)يوضح الصور الاصلية والناتجة(المسترجعة) .

الشكل (3- 51)

وقد كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء (**Cover Image**) والصورة الناتجة بعد الإخفاء (**Stego Image**) تساوي(27.617805 db) ،أما الجذر التربيعي لمعدل مربع الخطأ فيساوي (10.608440).أما بالنسبة إلى الصورة المخفية (**Embedded Image**) والصورة المسترجعة (**Extracted Image**) فإن نسبة قمة الإشارة إلى الضوضاء تاوي (16.316423 db) وإنّ الجذر التربيعي لمعدل مربع الخطأ يساوي (38.968978).

الشكل(3−52)يوضح الصور الاصلية والناتجة(المسترجعة) .

الصورة المخفية

صورة الغطاء

الصورة المسترجعة

الصورة الناتجة بعد الاخفاء

الشكل (3- 52)

وقد كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء (**Cover Image**) والصورة الناتجة بعد الإخفاء (**Stego Image**) تساوي(26.704719 db) ،أما الجذر التربيعي لمعدل مربع الخطأ فيساوي (11.784310).أما بالنسبة إلى الصورة المخفية (**Embedded Image**) والصورة المسترجعة (**Extracted Image**) فإن نسبة قمة الإشارة إلى الضوضاء تساوي (16.014083 db) وإنّ الجذر التربيعي لمعدل مربع الخطأ فيساوي (40.349298).

من خلال التجارب السابقة نلاحظ أن قيمة نسبة قمة الإشارة إلى الضوضاء بين صورتي الغطاء والناتجة تتراوح بين (26.7-29.7) و الجذر التربيعي لمعدل مربع الخطأ يتراوح بين (8.4-11.8) أما بالنسبة للصورة المسترجعة فإن قيمة نسبة قمة الإشارة إلى الضوضاء تتراوح بين (15.9-16.3) أمّا الجذر التربيعي لمعدل مربع الخطأ فيساوي (39.0-40.8) وقد كانت النتائج مقبولة بالنسبة للصورة الناتجة، أمّا بالنسبة للصورة المسترجعة فقد ظهرت فيها بعض التشوهات القليلة ويعود ذلك الى مدى التشابه بين صورتي الغطاء والمخفية، فكلما كان كانت الصورة المسترجعة افضل. وإنّ تاثير عملية الاخفاء يصبح اقل ادراكا بالنسبة للصورة الناتجة .

التجربة رقم (2)

الشكل(3-53)يوضح الصور الاصلية والناتجة(المسترجعة) .

الشكل (3-53)

وقد كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء **(Cover Image)** والصورة الناتجة بعد الإخفاء **(Stego Image)** تساوي(31.678917 db) ،أما الجذر التربيعي لمعدل مربع الخطأ فيساوي (6.646519).أما بالنسبة إلى الصورة المخفية **(Embedded Image)** والصورة المسترجعة (**Extracted Image)** فإن نسبة قمة الإشارة إلى الضوضاء تاوي (38.399187 db) وإنّ الجذر التربيعي لمعدل مربع الخطأ يساوي (16.316423).

الشكل (3-54) يوضح الصور الاصلية والناتجة(المسترجعة) .

الشكل (3-54)

وقد كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء (**Cover Image**) والصورة الناتجة بعد الإخفاء (**Stego Image**) تساوي(30.903680 db) ،أما الجذر التربيعي لمعدل مربع الخطأ فيساوي (7.267016).أما بالنسبة إلى الصورة المخفية (**Embedded Image**) والصورة المسترجعة (**Extracted Image**) فإن نسبة قمة الإشارة إلى الضوضاء تاوي (16.560537 db) وإنّ الجذر التربيعي لمعدل مربع الخطأ يساوي (37.889014).

الشكل(3-55)يوضح الصور الاصلية والناتجة(المسترجعة) .

الشكل (3-55)

وقد كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء (**Cover Image**) والصورة الناتجة بعد الإخفاء (**Stego Image**) تساوي(30.119759 db) ،أما الجذر التربيعي لمعدل مربع الخطأ فيساوي (7.953388).أما بالنسبة إلى الصورة المخفية (**Embedded Image**) والصورة المسترجعة (**Extracted**

Image) فإن نسبة قمة الإشارة إلى الضوضاء تساوي (db 16.565516) وإنّ الجذر التربيعي لمعدل مربـــع الخطأ يساوي (37.867302).

الشكل(3-56) يوضح الصور الأصلية والناتجة(المسترجعة) .

الصورة المخفية

صورة الغطاء

الصورة المسترجعة

الصورة الناتجة بعد الإخفاء

الشكل (3-56)

وقد كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء (**Cover Image**) والصورة الناتجة بعد الإخفاء (**Stego Image**) تساوي(db 31.593359) ،أما الجذر التربيعي لمعـــدل مربـــع الخطـــأ فيســـاوي (6.712313).أما بالنسبة إلى الصورة المخفية (**Embedded Image**) والصورة المسترجعة (**Extracted Image**) فإن نسبة قمة الإشارة إلى الضوضاء تساوي (db 16.678420) وإنّ الجذر التربيعي لمعدل مربـــع الخطأ يساوي (37.378268).

الشكل(3-57)يوضح الصور الاصلية والنائجة(المسترجعة) .

الصورة المخفية

صورة الغطاء

الشكل (3-57)

وقد كانت نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء (**Cover Image**) والصورة الناتجة بعد الإخفاء (**Stego Image**) تساوي(30.176789 db) ،أما الجذر التربيعي لمعدل مربع الخطأ فيساوي (7.901338).أما بالنسبة إلى الصورة المخفية (**Embedded Image**) والصورة المسترجعة (**Extracted Image**) فإن نسبة قمة الإشارة إلى الضوضاء تاوي (14.902625 db) وإنّ الجذر التربيعي لمعدل مربع الخطأ يساوي (45.857345).

من خلال التجارب السابقة نلاحظ أن قيمة نسبة قمة الإشارة إلى الضوضاء بين صورة الغطاء والصورة الناتجة تتراوح ين (30.1-31.7) و الجذر التربيعي لمعدل مربع الخطأ يتراوح بين (6.6-8.0) أما بالنسبة للصورة المسترجعة فإن قيمة نسبة قمة الإشارة إلى الضوضاء تتراوح بين (14.9-16.7) اما الجذر التربيعي لمعدل مربع الخطأ فيساوي (37.4-45.9) وقد كانت النتائج مقبولة بالنسبة للصورة الناتجة اما بالنسبة للصورة المسترجعة فقد ظهر فيها بعض التشوهات القليلة ويعود ذلك الى مدى التشابه بين صورة الغطاء والصورة المخفية، فكلما كان التوافق بينهما كبيرا كانت الصورة المسترجعة افضل وإنّ تاثير عملية الاخفاء يصبح اقل ادراكا بالنسبة للصورة الناتجة .

المصادر

[1] F.A.Seddek, **Image Steganography**, M.Sc thesis, Saddam University, 2001.

[2] J. Rimell, **Data Hiding Inside TIFF Images**, Computer Science Tripos PartII, St. John's College, Cambridge, England, 1997.

[3] M.Goljan, J.J.Fridrich and R. Du, **Distortion-Free Data Embeddeing For Images**, LNCS, **2137**, 25, (2001).

[4] Y.K. Lee and L.H. Chen, **High Capacity Image Steganographic Model**, IEE Proceeding Vision, Image and Signal Processing, **147**, 3, 288, (2000).

[5] L.M. Marvel and C.T. Retter, **A methodology for Data Hiding using Images**, IEEE, Boston, (1998).

[6] J.R. Smith and B.O. Comisky, **Modulation and Information Hiding in images**, Information Hiding, LNCS **1174**, 207, (1996).

[7] W. Bender, D. Gruhl, N. Morimoto and A. Lu, **Techniques for Data Hiding** , IBM systems Journal, **35**, 3&4, 313, (1996).

[8] P. Davern and M. Scott, **Fractal Based Image Steganography**, Information Hiding, LNCS **1174**, 279, (1996).

[9] M.D. Swanson, B. Zhu and A.H. Tewfik**, Robust Data Hiding for Images**, IEEE Digital Signal Processing, Loen, Norway,37, (1996).

[10] J.Fridrich ,**Secure Image Ciphering based on Choas** , Technical Report RL-TR ,97,Rome Laboratory ,NewYork ,(1997).

[11] A.Westfeld and G.Wolf, **Steganography in a Video Conferencing system** , Information Hiding ,LNCS **1525**,32,(1998).

[12] L.M.Marvel,C.G.Boncelet and C.T.Retter, **Reliable Blind Information Hiding for Images** , Information Hiding, LNCS **1525**,48,(1998).

[13] J.Fridrich ,**A new Steganographic Method for Palette-based Images** , IS&TPICS conference ,Savannah ,Georgia ,285, (1998).

[14] L.M.Mavel,**Image Steganogaphy for Hidden communication** , Ph.D. thesis , University of Delaware ,1999.

[15] J.J.Chae and B.S.Manjunath , **A Technique for Image Data Hiding and Reconstruction without Host Image** ,SPIEEI '99 ,Security and Watermarking Multimedia contents ,San Jose ,California , (1999) .

[16] S. Areepongsa ,N.Kaewkamnerd ,Y.F.Syed and K.R.Rao , **Information Hiding in Image Retrieval Systems** ,ICCS ,(2000) .

[17] L.Z.Avedissiain, **Image in Image Steganography System** ,Ph.D. thesis , University of Technology , 2000.

[18] R.S.Youial **, Combining of Steganography and Error-Correction Code** , M.Sc thesis , University of Saddam , 2002.

[19] D.Kahn, **The History of Steganography** , Information Hiding , LNCS **1174**,1, (1996).

[20] S.Katzenbeisser and F.A.Petitcolas , **Information Hiding Techniques for Steganography and Digital Watermarking** , Artech House INC. , Boston /London , 2000.

[21] N . F. Johnson , Z . Duricand and S.Jajodia , **Information Hiding:Steganography and Watermarking-Attacks and Countermeasures** , Kluwer Academic Publishers , Boston / Dordrecht / London , 2001.

[22] R . Anderson , **Stretching the Limits of Steganography** , Information Hiding ,LNCS **1525** ,355,(1998) .

[23] S . Craver ,**On Public-Key Steganography in the Presence of an Activer Warden** , Information Hiding , LNCS **1525 ,** 355, (1998) **.**

[24] T . Aura , **Practical Invisibility in Digital Communication** , Information Hiding , LNCS **1174** , 265, (1996) .

[25] Y . Lee and L . Chen , **A Secure Robust Image Steganographic Model** , Automatic Information Processing Laboratory CIS , NCTU , Hualiean , Taiwan ,2000 .

[26] J .Fridrich ,**Applications of Data Hiding in digital Images** , Tutuorial for the ISPACS '98 conference in Melourne , Australia , (1998) .

[27] N . F . Johnson and S . Jajodia **, Exploring Steganography :Seeing the Unseen** , IEEE ,computer , **31** , 26 , (1998) .

[28] R . A . Isbell , **Steganography Hidden Menace or Hidden Saviour** , M.Sc IEng FIIE. Thesis ,LIRIC Associates Ltd. ,1,2002 .

[29] F . Queirolo ,**Steganography in Images** ,Communications Report , (2001) .

[30] I.Avcibas **, Image Quality Statistics and their use in Steganalysis and Compression** ,Ph.D. thesis , Bogazici University ,2001.

[31] R .C . Gonzalez , R . E. Wood and A . Wesley , **Digital Image Processing** , Addision Wesley publishing Company INC. ,1992.

[32] S . E . Umbaugh ,**Computer Vision and Image Processing** , Pretice Hall , London ,1998 .

[33] د.الششتاوي، أحمد أمين، **برمجة ومعالجة الصور**، مكتبة الدار العربيـــة للكتـــاب، ط1، 1997.

[34] E . H . Obead , **Parallel Structure for Image Compression Using Neural Network** ,M.Sc thesis ,Babylon University , 2000 .

[35] B . Schneier ,**Applied Cryptography** , NewYork , Chichester . Bisbane .Tornoto .Sigapore ,1996 .

[36] P. Biswas ,**Image downgrading-A Steganographic Technique to Hid**e **Secret Messages** ,Submitted towards Partial Completion of Requirement in ICS268, (2001) .

[37] I. S . Moskowitz ,G .E. Longdon and L.Chang , **A New Paradigm Hiding in steganography** , in New Security Paradigms , Proceedings, ACM press , 41 , (2000) .

[38] C . Kurak and J .Mc.Hugh ,**A Cautionary Note on Image Downgrading** ,IEEE Computer Society 153, (1992) .

[39] S .Wang and K . Yang , **A Scheme of High Capacity Embedding on Image Data Using Modulo Mechanism** ,WISA ,Souel ,Korea , (2001) .

[40] D . Salomon ,**Data Compression** ,Springer-Verlag NewYork ,1998.

[41] T . Y .Kim and J. Han , **Partial Image Matching by Measures from Connected Color Regions**,Technical Report Supported by Minstry of Education of Korea , (1999) .

[42] R . Johnson and G .Bhattacharyya ,**Statistics Principles and Methods** , John Wiley & Sons ,INC,1985 .

[43] S.M. Chaudhry, **Introduction to statistical Theory** , Kutub Khana, Lahore , Pakistan , 1984.

[44] M.G.Shayesteh,S.Rostamzadeh and K.Faez , **Recognition of Different Cars Using Moment Invariants and Back-Propagation Neural Network**, International Conference on Neural Network and Brain Procedings,563,1998 .

Color Image in Color Image Steganography System

Athesis
Submitted to the Council of the Science College of Babylon University in Partial Fulfillment of the Requirements for the Degree of Master of Science in Computer Science

By

Hiba Mohammed Ja'far Al - khafaji

September 2003

Abstract

Data security is one of important subjects which has a great interest in different fields, one of these is information hiding, to protect the important information from un-authorized persons .

This research aim's to hide an image with different color levels (natural, color-256, gray) and different degrees of complexity inside anther image with the same size .

Five different methods where used:

1-Image Downgrading Method :

In this method the least significant bits of the cover image will be exchanged by the most significant bits of the embedded image using xor function .All the combinations of the images were taken and a good results were achieved for all the case, except a little distortion in embedding a 256-color .Also , good results has been shown for complex images images.

2-Least Significant Bit Insertion :

In this method all the elements of the image is to be embedded inside the least significant bit of the cover image . Different combinations of the color images . Good result has been shown.

3-Modulo Mechanism :

The method depends on the mathematical procedure in hiding process . The secure data will be emerged with the cover image taking random positions . This method is more secure than the last two method . Best results shown for all the combinations of the images .

4-Hybrid Method :

This method consist of two stages compression and hiding stages ,and so the restore process . Best results is shown for all cases under study .

5-Similar-blocks method :

A proposed method depends on substituting the similar blocks of the embedded image within the cover . This method is more secure and robust against the changes and treatments done for the cover image .Best results has been shown for all cases ,except a little distortion is seen for 256-color images.

Delphi version 4.0 were used in executing the suggested system.

3-2 الاستنتاجات

تم استعمال خمس طرائق إخفاء هـــي طريقـــة (Image Downgrading) و طريقـــة حشـــر الثنائيات الأقل أهمية و استعمال الاسلوب الرياضي و الطريقة الهجينة وطريقة القطاعات المتشـــابهة

وقد نفذت على مجموعة من الصور مختلفة الأنواع والتعقيدات وذات تدرجات لونيةتعددة(**صور ذات تدرج رمادي ،صور ملونة ذات (256) لونا وصور طبيعية**) .

من خلال تنفيذ النظام على عدة أنواع من الصور المختلفة يمكننا أن نستنتج ما يأتي :

- من خلال تنفيذ **طريقة (Image Downgrading)** على عدة أنواع من الصور نجد أنّ افضـــل النتائج كانت للصور ، التدرجات الرمادية حيث كانت قيم **PSNR** تتـــراوح بـــين (31.5-32.7) **(وذلك لان مثل هذا النوع من الصور يتميز بأنه ذو تغيرات تدريجية في الشدة اللونية بين العناصر وهذا يجعل التشوه الناتج من عملية الإخفاء قليلا وقد يكون معدوم ، لذلك تعدُّ الصور ذات التباينات (التدرجات)اللونية القليلة ذات فعالية كبيرة)** .كما حققت الصور الطبيعية نتائج جيدة أيضا إذ كانـــت قيم **PSNR** تتراوح بين (25.4-28.9) ،اما بالنسبة للصور الملونة ذات (256) لونا فقد ظهرت فيها بعض التشوهات وكانت النتائج مقبولة إذ قيم **PSNR** كانت تتراوح بين (22.6-25.3) .
- من خلال تنفيذ **طريقة حشر الثنائيات الأقل أهمية** نجد أنّ إخفاء صور ذات تدرج رمادي داخـــل صور طبيعية يعطي نتائج افضل إذ إنقيم **PSNR** كانت تتراوح بين (28.8-32.5) .أما عند إخفاء صور ملونة ذات (256) لونا فإنّ قيم **PSNR** تتراوح بين (21.8-26.5) وهي نتائج جيدة أيضا.
- من خلال تنفيذ **طريقة الاسلوب الرياضي** نجد أن افضل النتائج كانت للصور ذات التدرج الرمادي إذ إنّ قيم **PSNR** تتراوح بين (34.1-34.9) .اما بالنسبة الى الصور الملونة ذات (256) لونا فقـــد ظهرت فيها بعض التشوهات رغم من أن قيم **PSNR** عالية إذ كانت تتراوح بين (35.3-35.5) .

- من خلال تنفيذ **الطريقة الهجينة** نجد أن افضل النتائج كانت للصور ذات التدرج الرمادي إذ إنّ قيم **PSNR** تتراوح بين (35.4-35.8) .اما بالنسبة الى الصور الملونة ذات (256) لونا فإنّ قيم **PSNR** تتراوح بين (27.5-28.7) .
- من خلال تنفيذ **طريقة القطاعات المتشابهة** نجد أنّ افضل النتائج كانت للصور ذات التدرج الرمادي إذ إن قيم **PSNR** تتراوح بين (30.1-31.7) .اما بالنسبة الى الصور الملونة ذات (256) لونا فإنّ قيم **PSNR** تتراوح بين (26.7-29.7) .
- تعدُّ مرحلة إختيار الغطاء المناسب عملية مهمة جدا بالنسبة لعملية الإخفاء، إذ يتم اختبار التوافق بين صورة الغطاء والصورة المخفية وهذا يجعل تأثير عملية الإخفاء أقل إدراكا كما في طريقة **(Image Downgrading)**، طريقة حشر الثنائيات الأقل أهمية وطريقة القطاعات المتشابهة، و إنّ إختيار الصوري تكون أقل تأثر (غير قابلة للتشويه) كأن تكون الصور معقدة حيث يندمج تأثير عملية الإخفاء مع تفاصيل الصورة.
- من خلال تنفيذ **طريقة (Image Downgrading)** و**طريقة حشر الثنائيات الاقل اهمية** نجد أن استعمال الصور الطبيعية كغطاء يعطي نتائج جيدة ولا سيما عندما يتم اخفاء صور ذات تدرج رمادي او صور ملونة ذات (256) لونا فيها **(لأنها توفر مساحة أكبر وهي تعادل حجمها بثلاث مرات تقريبا)** .
- أعطت **الطريقة الهجينة** افضل النتائج حيث كانت قيم **PSNR** عالية جدا وكانت الصور الناتجة جيدة لجميع أنواع الصور **(لان الصورة المخفية تضغط قبل إخفائها وبذلك فان حجم التغيرات الناتجة علية الإخفاء تصبح اقل إدراكا)** وبذلك فإنها تعدُّ افضل الطرائق ،وقد حققت **طريقة الاسلوب الرياضي** نتائج جيدة وكانت قيم **PSNR** عالية أيضا ولجميع أنواع الصور وتأتي بالمرتبة الثانية ،أما **طريقر الثنائيات الأقل أهمية** فتأتي بالمرتبة الثالثة أما **طريقة (Image Downgrading)** فتأتي بالمرتبة الرابعة وطريقة القطاعات المتشابهة تأتي بالمرتبة الخامسة .

- تعتبر عملية الضغط التي تحتوي على فقدان للبيانات افضل في عملية الإخفاء من عملية الضغط التي لا تحتوي على فقدان للبيانات ، لان اضافة نسوضاء **(Noise)** أو اجـراء أي تعـديل علـى الصورة الحاملة للصورة المخفية سوف لن يؤثر كثيرا على الصورة المخفية وبالتالي يمكن استرجاع الصورة المخفية ؟،اضافة الى ان نسبة الضغط فيها تكون اعلى ،حيث توجد علاقة عكسية بين نسبة فقدان البيانات ونسبة الضغط .

- تم إخفاء البيانات السرية داخل بيانات الغطاء وليس في صديرة الفايل في جميع أنواع الطرائق من اجل ان تبقى البيانات تامة عندما تتغير هيأة فايل البيانات.

- إن استعمال الاسلوب العشوائي يجعل عملية الوصول إلى بيانات الصورة المخفية صعبة،إذ تـم تطبيق اسلوبين الأول :باستعمال مولد الأرقام شبه العشوائية مع مفتاح يُعد بذرة له **(من دون معرفـة المفتاح لن يستطيع توليد الأرقام العشوائية المستعملة)**،الآخر :متسلسلة أعداد مناسبة توافر خلـط وتداخل للبيانات المراد اخفاؤها بشكل يصعب تجميعها بشكل مرتب بدون مفتاح تلك المتسلسلة(**علمـا إنّ لا تعتمد على أي دالة مبنية سابقة)** وإنّ الوصول إلى بيانات الصورة لا يعنـي استرجاع الصورة المخفية لأنها تعتمد أيضا على معلومات سرية بين المرسل والمستلم .

- تعدُّ **طريقة القطاعات المتشابهة** اكثر الطرائق امنية ضد التغيرات الناتجة من بعض المعالجات إذ إنها تعتمد على ابدال القطاعات المتشابهة كما إنّ عملية الاسترجاع تعتمد علـى بعـضلمعلومـات السرية التي ترسل بصورة منفصلة والتي تمثل مواقع الاخفاء كذلك تعد طريقة الاسـلوب الرياضـي امينة نوعا ما .

- إن استعمال الثنائيات الاقل اهمية يجعل عملية الإخفاء غير ملحوظة لأن المعلومات السرية تخفى في مناطق غير مهمة(لان هذه الثنائيات تحتوي علـى ضوضـاء)وكمـا فـي طريقتـي (Image Downgrading) و حشر الثنائيات الاقل اهمية .إن هذه الخاصية في الصور مهمـة فـي جـانبين :الاول إن إخفاء المعلومات السرية في هذه الثنائيات يكون غير مدرك .الآخر: لإخفـاء صـورة لا

نحتاج إلى إخفاء العنصر كاملا لأن بعض الثنائيات لا تحمل معلومات عنصورة (فيها ضوضـــاء)

لذلك يتم إخفاء الثنائيات الأكثر أهمية فقط فبدلا من إخفاء ثمان ثنائيات يتم إخفاء أربع ثنائيات فقـط

وهذا يقلص حجم الصورة إلى النصف.

وقد أثبتت النتائج العملية أنّ إخفاء أربع ثنائيات فقط يكون كافي لاسترجاع صورة مقبولة،كذلك

تم إخفاء ثلاث ثنائيات وكانت الصورة المسترجعة واضحة .

بصورة عامة توجد موازنة بين كمية البيانات المخفية ودرجة أمنيتها ضد ات الغطاء .ان التقيـد

بدرجة انحطاط (تشوه) الغطاء يجعل طرائق إخفاء البيانات تعمل إمّا بمعدل إخفاء عالٍ للبيانات وإمّـا

بدرجة مقامة عالية ضد التغيرات (التعديلات) ولا تعمل بهما معا ،فعند زيادة أحدهما ينقص الآخر .

3-3 الأعمال المستقبلية

من خلال النتائج التي توصل إليها النظام المقترح يمكن أن نوصي بالمقترحات الآتية :

- ❖ استعمال نماذج فضاءات لونية أخرىير الفضاء اللوني RGB بالنسبة للصور الملونة طبقـا لنماذج رياضية معينة بالاعتماد على الفضاء اللوني RGB في عملية الإخفاء .
- ❖ استعمال التحويلات (Transformation) مع طريقة القطاعات المتشابهة .
- ❖ إخفاء صور متحركة (Movies) داخل :
  - ➢ صورة واحدة .
  - ➢ وسائط مختلفة (Multi-Media)
- ❖ استعمال تقنيات جديدة للإخفاء مثل التحويل المويجي (WT) .