تقنية الكتابة المغطاة في المجال المكاني

دجان بشير طه **غادة محمد طاهر**

كلية علوم الحاسبات والرياضيات

جامعة الموصل

تاريخ استلام البحث: ٢٠٠٦/١٠/١١ **تاريخ قبول البحث: ٢٠٠٦/١٢/٢٤**

ABSTRACT

This research deals with design and implementation of a new steganographic algorithm to hide secret messages inside digital images. To achieve security to the transmitted messages, a secret key is used to prevent unauthorized persons from extracting these messages.

Embedding has been achieved using grey and color images as a cover. Matlab is used to implement the algorithm due to the facilities it provides for dealing with digital images and matrices as well as GUI.

Finally, experimental results demonstrate the effieciency of the algorithm in hiding information in imperceptible manner.

الملخص

تم في هذا البحث تصميم وتنفيذ خوارزمية جديدة لغرض إخفاء الرسائل السرية داخل الصور الرقمية ولزيادة سرية الرسائل المنقولة تم استخدام مفتاح سري بإذ لا يمكن استرجاع الرسالة دون معرفته أي أن الجهة المخولة التي تعلم المفتاح السري هي التي تستطيع فقط استرجاع الرسالة السرية.

تم الإخفاء باستخدام الصور الملونة والرمادية كغطاء كما تم استخدام لغة (Matlab) في هذا البحث وذلك لكون الإخفاء تم في الصور الرقمية التي هي مصفوفات من القيم الرقمية وان لغة (Matlab) تسهل لنا التعامل مع المصفوفات فضلاً عن كونها توفر واجهات للتعامل مع المستخدمين.

وأخيرا، فان التجارب العملية أثبتت كفاءة الخوارزمية المقترحة في إخفاء المعلومات في الصور دون إدراك ذلك.

1. مقدمة في إخفاء المعلومات

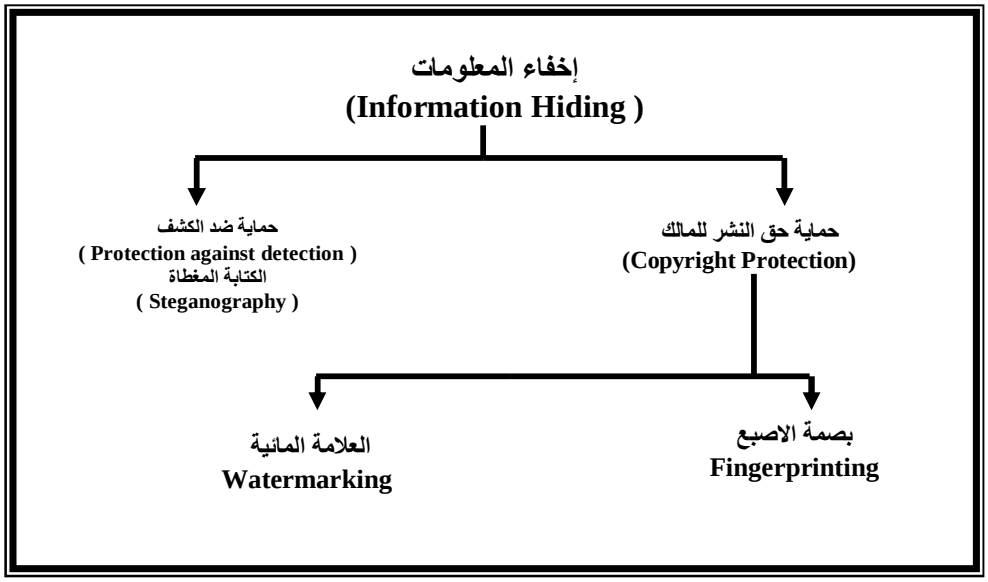
إن فكرة إخفاء المعلومات البسيطة استخدمت منذ مئات السنين،ولكن مع ازدياد استخدام الملفات بالصيغة الالكترونية ونتيجة لتطور التقنيات الحديثة في الوقت الحاضر دخل الحاسوب في كل مجالات المجتمع ومنها مجال إرسال المعلومات التي تزداد بشكل هائل فالمعلومات ترسل وتعالج آليا على نطاق واسع وهذا يتطلب الحرص على الخزن السري لنقل المعلومات ويوجد العديد من أسباب حماية المعلومات منها حراسة الاقتصاد لتجنب الاحتيال أو ضمان حماية المواطنين فأصبح من الضروري تطوير تقنيات جديدة لإخفاء المعلومات .

إخفاء المعلومات عنوان عام لنوعين من التقنيات، النوع الأول يستخدم لحماية المعلومات من المراقبين والمهاجمين ويدعى بالكتابة المغطاة أو ما يطلق عليه مصطلح نظام التغطية الذي هو موضوع البحث والنوع الثاني يستخدم لإثبات حقوق الملكية الفكرية أو لضمان الوثوقية وهو ما يدعى بالعلامة المائية الرقمية.

يوضح الشكل (1)أنواع إخفاء المعلومات وكيف أن إخفاء المعلومات يتفرع إلى مساحات مختلفة. إذ أن نظام التغطية يستخدم لإخفاء أية رسالة تعد لتسليمها شخص معين أو مجموعة من الأشخاص، وفي هذه الحالة يكون الهدف منع تلك الرسالة من أن يكتشفها أي شخص أخر.

وكذلك فانه من الاستخدامات الرئيسية لإخفاء المعلومات حماية حقوق النشر للمالك التي تدرج وتستخدم للتأكيد على حقوق الاستنساخ والنشر. ويمكن أن يصنف هذا إلى العلامة المائية و بصمة الإصبع التي هي عبارة عن أرقام سرية أو خصائص شخصية لا تتكرر [9,3,2].

وللمقارنة بين التقنيات المختلفة لتامين سرية الاتصالات نجد أن التشفير يعطينا اتصالا أمينا لأنه يتطلب مفتاحا لقراءة المعلومات ولكن إذا كان المهاجم لا يستطيع إزالة التشفير فهو يستطيع بسهولة التحوير في الملف بإذ يجعل الملف غير صالح للقراءة من قبل المستلم. وعلم الإخفاء يمدنا بأسلوب أمين للاتصالات لا يمكن إزالته دون عمل تغييرات جوهرية على البيانات التي أدرجت وتكون البيانات المدرجة ذات ثقة كبيرة ما لم يحاول المهاجم أن يجد أية طريقة لكشفها .



الشكل (1) أنواع إخفاء المعلومات

في تطبيقات إخفاء المعلومات، من غير الممكن أن نحصل على قوة أو متانة للخوارزمية، ووضوحية أو عدم تشويه في الصورة، وسعة للرسالة المخفية في نفس الوقت لذلك سوف نعمل على الموازنة بين هذه العوامل اعتمادا على التطبيق على سبيل المثال، في تطبيق ما قد نحصل على القوة على حساب الوضوحية والسعة [7].

وأخيرا فان التقنيات المستخدمة لإخفاء المعلومات تتنوع بالاعتماد على كمية البيانات المخفية ولكن من الملحوظ عدم توافر طريقة واحدة قادرة على إنجاز جميع الأهداف المطلوبة من الإخفاء.

2. متطلبات إخفاء المعلومات رقميا

هناك عدة تقنيات تضمين تمكننا من إخفاء البيانات في غطاء معين، وجميع هذه التقنيات يجب أن تحقق عددا من المتطلبات لكي يمكن تطبيق نظرية إخفاء المعلومات بصورة صحيحة وفي أدناه مجموعة من المتطلبات الرئيسية [4,1]:

1.الإكمال الصحيح للمعلومات المخفية لدى تضمينها داخل الغطاء الحامل، بإذ أن الرسالة السرية يجب أن لا تتغير بأية طريقة في حالة إضافة معلومات أو فقدان معلومات أو تغيير أية معلومات مضمنة بعد إخفائها ويعني تغير البيانات المضمنة فشل العملية .

2.الوسط الناقل الذي يغطي الرسالة السرية يجب أن لا يتغير أيضا وعلى الأقل أن لا تكون تغيراته ظاهرة للعيان وفي حالة كون التغيرات على الوسط الحامل كبيرة وظاهرة للعيان ، فان الشخص الذي يشاهدها سوف يشك بان هنالك معلومات مخفية داخلها فيحاول أن يفتحها أو يدمرها.

3.في العلامات المائية يجب أن لا تؤثر التغيرات التي تحدث في الرسالة على متانة العلامات المائية . ومن المعالجات التي يمكن أن تقع العلامة المائية تحت تأثيرها :عمليات التكبير والتصغير والقص وتدوير الصورة .

4.يؤخذ بنظر الاعتبار أن المهاجم يشك دائما بوجود معلومات مخفية داخل الغطاء الحامل.

3. نظام التغطية

نظام التغطية كلمة يونانية الأصل تعني لغويا الكتابة المغطاة إذ أنها تتألف من مقطعين (Steganos) وتعني مغطاة أو سرية و(Graphy) وتعني الكتابة أو الرسم. ويمكن تعريف نظام التغطية على أنه فن وعلم إخفاء المعلومات باستخدام ملف يستخدم كناقل لتلك المعلومات بطريقة لا تسمح لأي عدو أو مراقب بان يكتشف أن هناك بيانات سرية أخرى مخفية في هذا الملف.والهدف من نظام التغطية إخفاء ماهية الرسالة لمنع أي متطفل خارجي من الشك بوجود رسالة مخفية داخل الملف الحامل. إن نظام التغطية يعتبر وسيلة من وسائل الاتصال السري بأسلوب يخفي وجود الاتصال ويقابله علم التشفير أي تشفير الكتابة ويعني أن الرسالة موجودة ولكن ليس باستطاعة أي شخص أن يفك شفرتها .

ونظام التغطية ببساطة يأخذ جزءا من المعلومات ويخفيها بملف حاسوبي آخر سواء أكان ذلك الملف صورة أو صوتا أو نصا...الخ يحتوي على مساحات فارغة غير مستخدمة لأن نظام التغطية يستغل المساحات الفارغة وغير المستخدمة ويستبدلها بمعلومات أخرى [6,5].

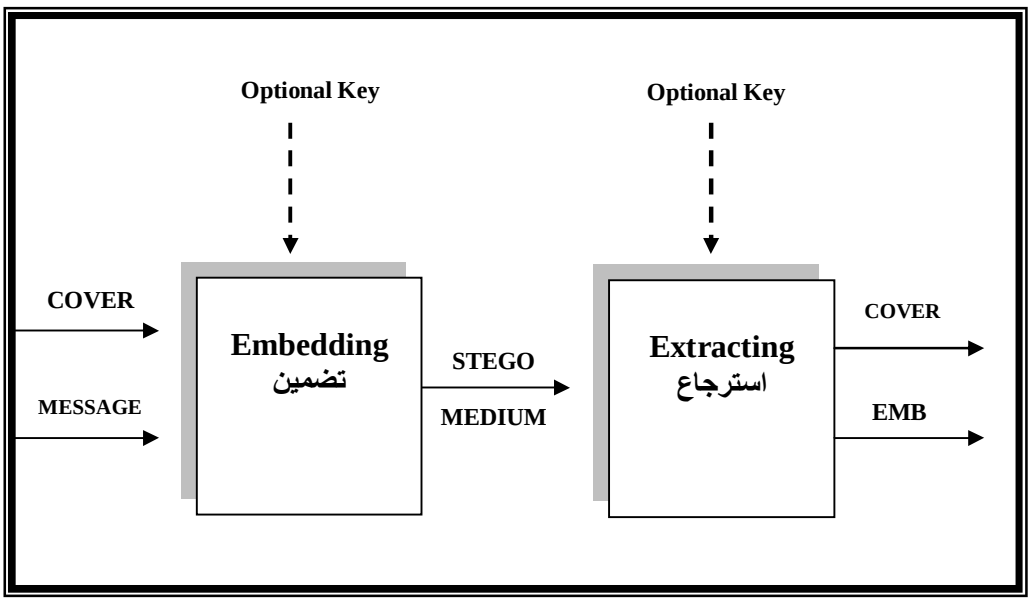
4. نموذج نظام التغطية:

إن النموذج الأساسي لنظام التغطية مبين في الشكل (2). إذ توجد أربعة عناصر في الإخفاء هي [8,6]:

* الناقل أو الغطاء (COVER).
* الرسالة السرية (MESSAGE) التي سوف نخفيها.
* وسط الإخفاء (STEGO_MEDIUM) وهو إخراج الناتج بعد الإخفاء.
* مفتاح الإخفاء(Optional_key) يكون اختياريا ويستخدم لزيادة درجة السرية ومن الممكن تجاوزه.

ويمكن تمثيل نظام التغطية باستخدام المعادلة الآتية :

Cover_medium+Embedded Message+Stego_key=Stego_medium



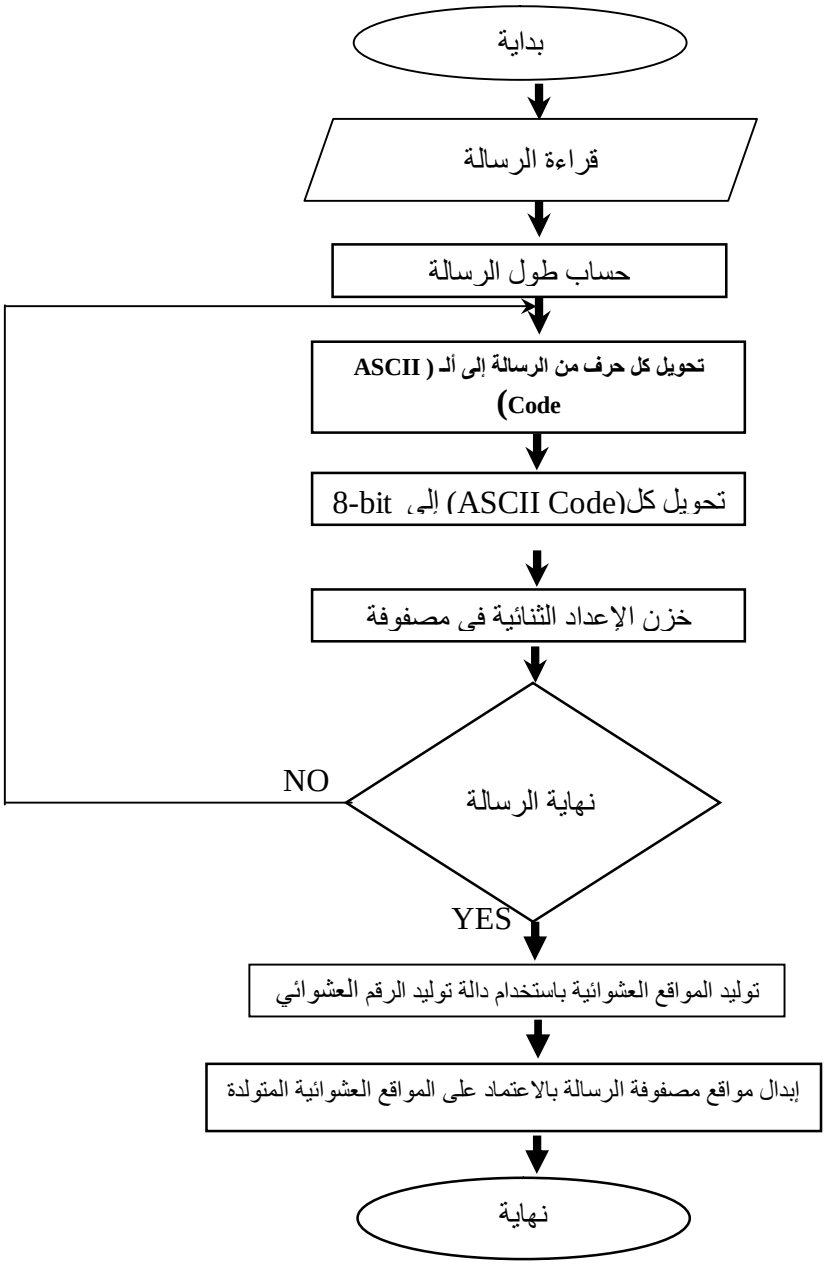
الشكل (2) النموذج الأساسي لنظام التغطية

5. تصميم الخوارزمية المقترحة:

1.مرحلة توليد الرسالة:

تبدأ هذه المرحلة بقراءة الرسالة المراد إخفاؤها داخل صورة ثم يتم تحويل أحرف الرسالة إلى مصفوفة من ألـ(ASCII Code) إذ يمثل كل حرف في الرسالة بما يقابله من ألـ (ASCII Code) وتكون المصفوفة الناتجة من هذه العملية ذات بعد واحد. ثم يتم تحويل كل رمز من المصفوفة إلى صيغة النظام الثنائي (8 bit) .

ومن ثم يتم دمج هذه القيم الثنائية في مصفوفة ذات بعد واحد ولزيادة سرية الرسالة المضمنة نقوم بإبدال مواقع قيم المصفوفة باستخدام مواقع عشوائية يتم توليدها من دالة الأرقام العشوائية.ويتم استخدام مفتاح سري الذي يمثل البذرة لدالة توليد الأرقام العشوائية . يوضح الشكل (3) المخطط الانسيابي لعملية توليد الرسالة .



الشكل (3) المخطط الانسيابي لعملية توليد الرسالة

2. مرحلة تضمين الرسالة:

يوضح الشكل (4) عملية تضمين الرسالة إذ يكون الإدخال هنا هو الرسالة (M) والصورة الأصلية (P) ويكون الإخراج لهذه المرحلة هو الصورة بعد تضمين الرسالة فيها (P'). يتم فحص الصورة قبل التضمين فإذا كانت ملونة يتم تحويلها إلى صيغة (Ycbcr) واخذ (Y) التي تمثل شدة الإضاءة لغرض التضمين .

تتلخص خوارزمية تضمين الرسالة بالخطوات الآتية :

1. تقسيم الصورة المراد إخفاء الرسالة فيها إلى عدد من المقاطع إبعاد المقطع الواحد(8*8).
2. إيجاد عدة حسابات للمقطع الواحد تتمثل بما يأتي :

* حساب معدل المقطع (mean) .
* إيجاد اكبر قيمة في المقطع (max) .
* إيجاد اقل قيمة في المقطع (min).
* إيجاد القيم التي هي أعلى من المعدل (hi) وحساب معدل هذه القيم (mhi)
* إيجاد القيم التي هي اقل من المعدل (low) وحساب معدل هذه القيم (mlow).

3. يتم تغيير قيم كل مقطع بالاعتماد على قيمة العنصر الحالي لمصفوفة الرسالة (M) الناتجة من مرحلة توليد الرسالة :

a. إذا كان العنصر الحالي لمصفوفة الرسالة هو(1) فيتم تغيير قيم عناصر المقطع كالآتي:

* إذا كانت القيمة الحالية للعنصر هي اكبر من(mhi) عندئذ تكون القيمة الجديدة للمقطع هي(max).
* أما إذا كانت القيمة الحالية للعنصر هي اكبر أو تساوي (mlow) و اقل من ألـ (mean) فتكون القيمة الجديدة للمقطع هي (mean).
* أما إذا لم تحقق أياً من الشروط أعلاه عندئذ تكون القيمة الجديدة للمقطع هي القيمة الحالية للمقطع مضافا إليها قيمة ثابتة (a) وهذه القيمة تم تحديدها في البرنامج بحيث لا تؤثر في الصورة المضمنة .

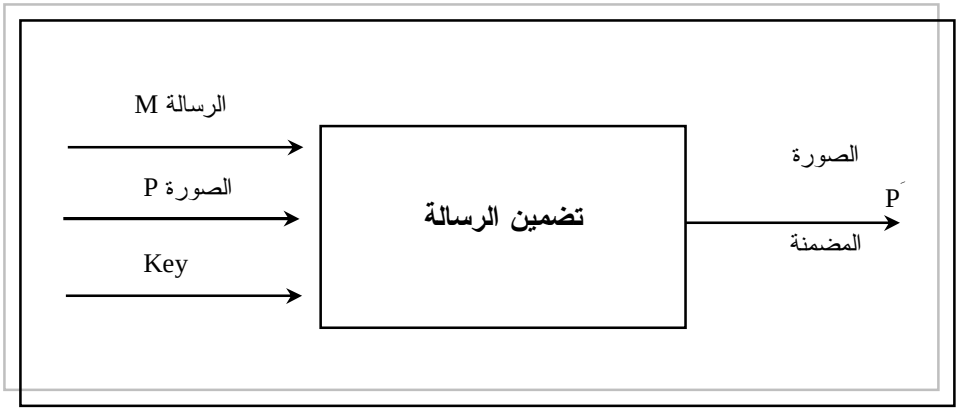
b. أما في حالة كون العنصر الحالي لمصفوفة الرسالة هو(0) فيتم تغيير قيم المقطع كالأتي:

* إذا كانت القيمة الحالية للمقطع هي اقل من (mlow) فستكون القيمة الجديدة للمقطع هي (min) .

* إما إذا كانت القيمة الحالية للمقطع هي اكبر أو تساوي (mean) واقل من(mhi) فعندها ستكون القيمة الجديدة للمقطع هي (mean).

* إما إذا لم تحقق القيمة الحالة أياً من الشروط المذكورة أنفاً فستكون القيمة الجديدة تساوي القيمة الحالية مطروحا منها a .

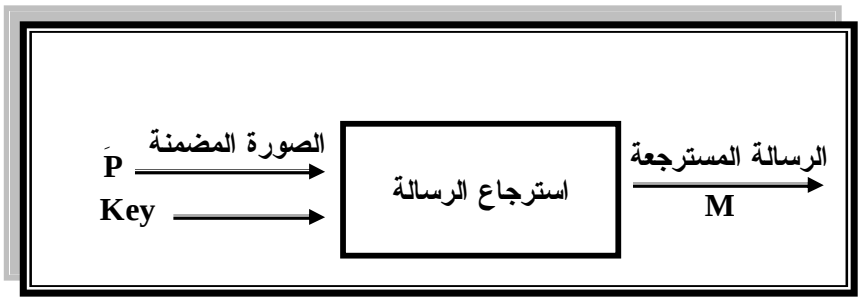
وتستمر عملية التضمين هذه إلى نهاية عناصر مصفوفة الرسالة (M) , ويمثل الشكل (5) المخطط الانسيابي لعملية التضمين .



الشكل(4) تضمين الرسالة

3. استرجاع الرسالة المضمنة

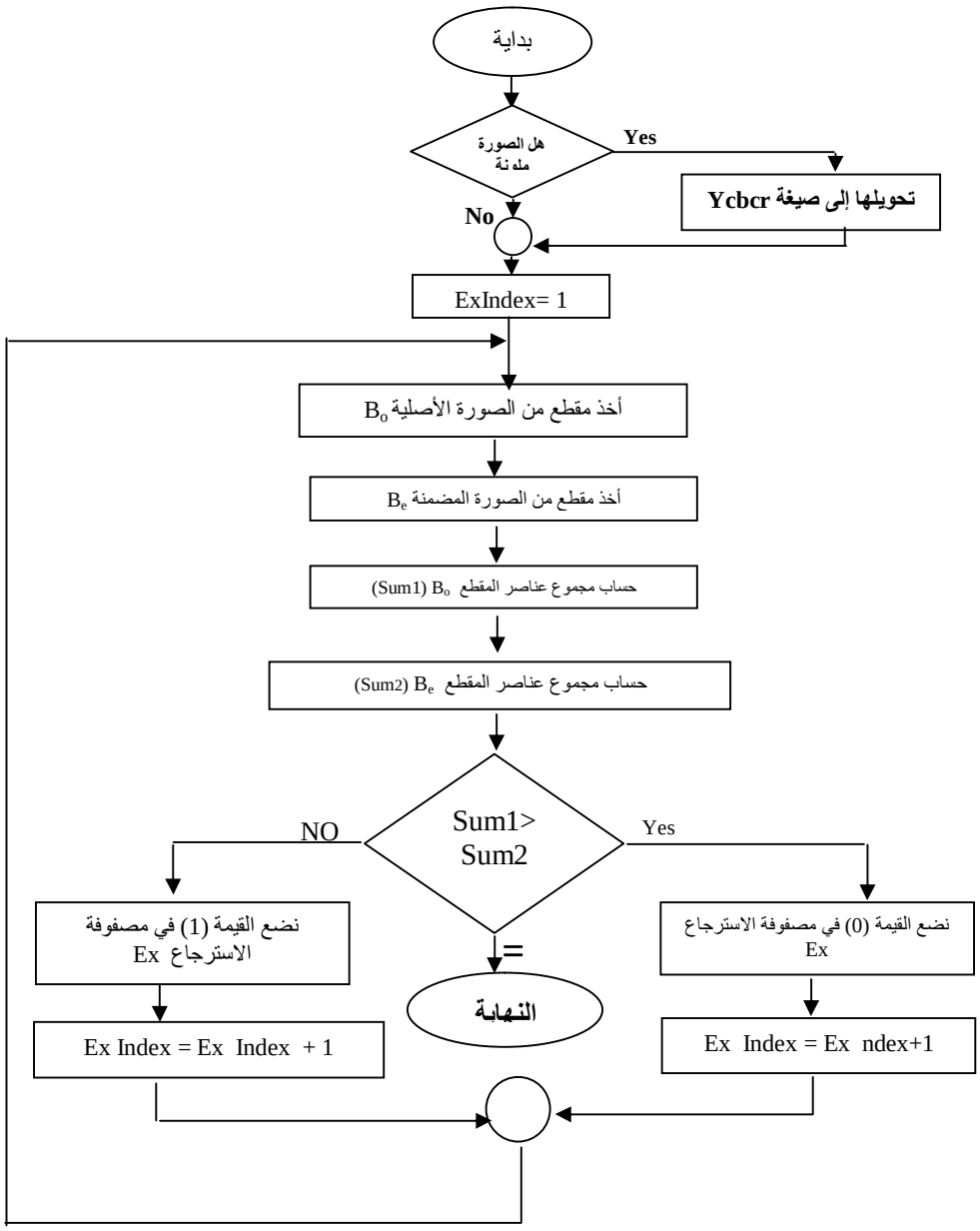
إن عملية استرجاع الرسالة من الصورة هي العملية المعاكسة لعملية التضمين ,ويمثل الشكل (6) عملية استرجاع الرسالة إذ يكون الإدخال هنا هو الصورة بعد تضمين الرسالة فيها (P') والإخراج لهذه العملية سيكون الرسالة المسترجعة بحيث يتم مطابقتها مع الرسالة الأصلية الناتجة من عملية توليد الرسالة (M) ويجب إن تكون الرسالتان متطابقتين تماما عندما لا تكون الصورة المضمنة قد تعرضت لأي تغيير بسبب التهديدات التي يمكن أن تتعرض لها .



الشكل (6) استرجاع الرسالة

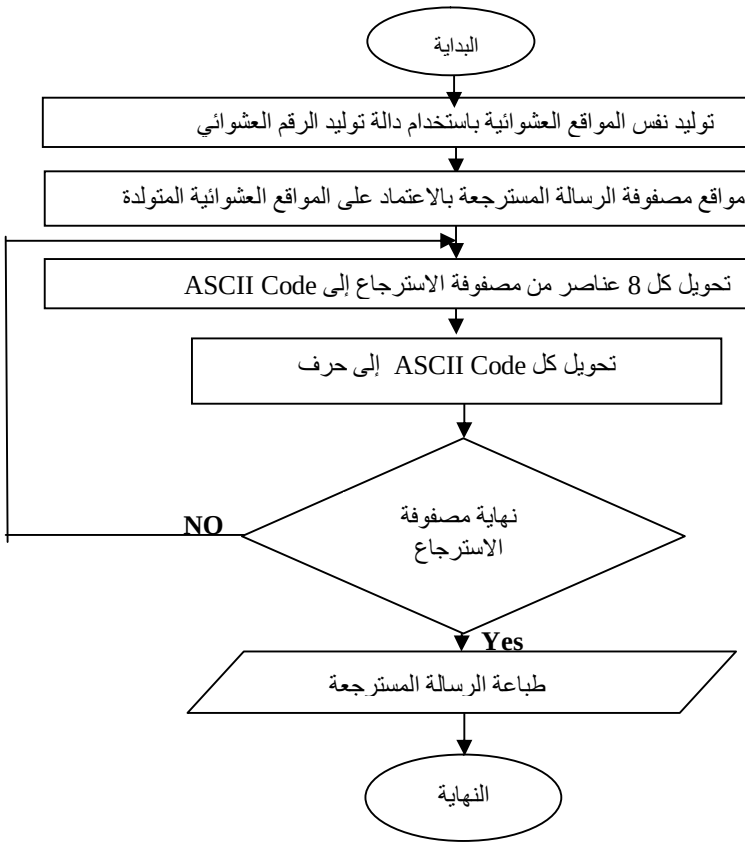
إن عملية استرجاع الرسالة تتلخص بمرحلتين همـــا الاســـترجاع وعـــرض الرســـالة. تتلخص خوارزمية الاسترجاع بما يأتي:

يتم تقسيم الصورة الأصلية إلى عدد من المقاطع المشابهة للمقاطع في عملية التـــضمين وكذلك يتم تقسيم الصورة الناتجة من عملية تضمين الرسالة إلى نفس العدد من المقاطع ,ومن ثـــم يتم حساب مجموع قيم كل مقطع من مقاطع الصورة الأصلية (sum1) وأيضا يتم حساب مجموع قيم كل مقطع من مقاطع الصورة بعد التضمين (sum2) وبعدها يتم فحص إذا كان sum1 لأحد المقاطع في الصورة الأصلية اكبر من sum2 للمقطع المقابل له في الصورة المـــضمنة فعنـــدها يكون البت المسترجع هو صفر إذا كان sum1 اقل أو يـــساوي sum2 فعنـــدها يكـــون البـــت المسترجع هو واحد ويتم خزن القيم الثنائية المسترجعة في مصفوفة الاســـترجاع (Ex). ويمثـــل الشكل (7) المخطط الانسيابي لعملية الاسترجاع.



الشكل (7) المخطط الانسيابي لعملية استرجاع الرسالة

إن مرحلة عرض الرسالة هي العملية المعاكسة لعملية توليد الرسالة إذ يكون الإدخـــال هنا هو مصفوفة الاسترجاع التي تحوي على القيم الثنائية المسترجعة من الصورة المضمنة، وبما أنه تم استخدام الرقم العشوائي قبل عملية تضمين الرسالة فلا بد من استرجاع المواقع الأصـــلية لحروف الرسالة المسترجعة قبل عرضها فيتم استخدام نفس المفتاح لتوليد نفس السلسة العشوائية قبل تحويل القيم المسترجعة إلى ألـــ (ASCII Code) وبعد استرجاع المواقع الأصلية للقيم يتم تحويل كل 8 عناصر من مصفوفة الاسترجاع إلى ألـــ Code (ASCII) الذي يقابلها وبعـــدها يتم تحويل كل من هذه الرموز إلى الحرف المقابل له وأخيرا توضع جميع الحروف في مصفوفة لغرض عرضها. ويمثل الشكل (8) المخطط الانسيابي لعملية عرض الرسالة.



الشكل (8) المخطط الانسيابي لعملية عرض الرسالة

6.النتائج والاستنتاجات

1- النتائج

- التضمين

إن واجهة التضمين (الشكل 9) تتألف من مجموعة مكونات هي:-

a- **Enter message**

يتم إدخال الرسالة المراد إخفاؤها.

b- **Enter Key**

يتم إدخال المفتاح السري للرسالة ويمكن تغيير المفتاح في أي وقت عند الحاجة.

c- **Choose the Cover**

يتم اختيار صورة من بين مجموعة من الصور.

d- **Next**

يتم الانتقال إلى برنامج التضمين وعرض النتيجة وهي الصورة بعد تضمين الرسالة فيها. إذ عند اختيار صورة ملونة تكون النتيجة كما موضحة في الشكل (10) وإذا تم اختيار صور رمادية تكون النتيجة كما في الشكل (11). تم حساب PSNR والتي تقاس بوحدة dB لمعرفة فيما إذا كان هناك تشوه في الصورة ولوحظ أن الصورة الناتجة خالية من أي تشوه إذ كانت قيمة PSNR تساوي 45.59dB و 41.99dB للصورة الملونة والرمادية على الترتيب وهي قيمة جيدة جدا.

الشكل (9) واجهة التضمين

الشكل (10)التضمين في الصورة الملونة

الشكل (11)التضمين في الصورة الرمادية

- **الاسترجاع**

إن واجهة الاسترجاع (الشكل 12) تتألف من المكونات الأتية:

Enter key -a

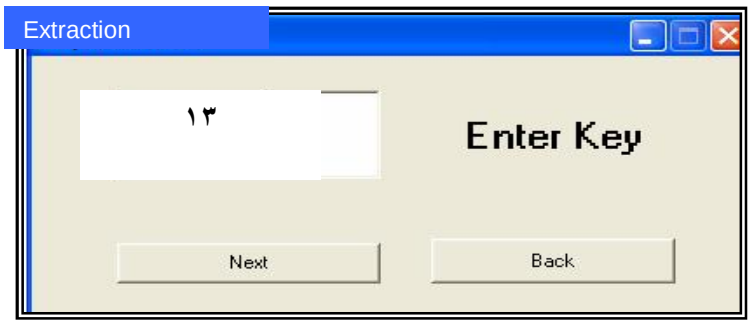
يتم إدخال نفس المفتاح السري المستخدم في تضمين الرسالة لغرض استرجاعها.

Next -b

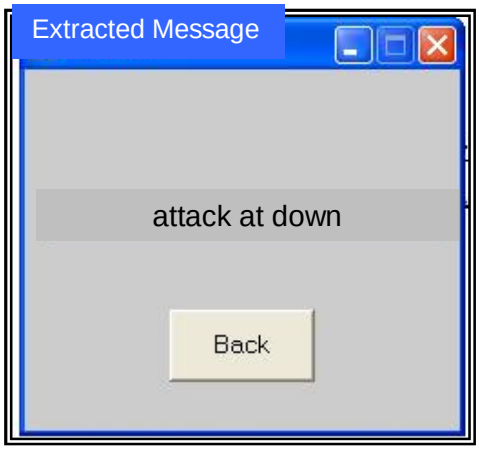
يتم الانتقال إلى برنامج الاسترجاع وعرض الرسالة المسترجعة من الصورة كما في الشكل (13).

Back -c

يتم الرجوع إلى الواجهة الرئيسية .



الشكل (12) واجهة الاسترجاع



الشكل (13) واجهة عرض الرسالة المسترجعة

2- الاستنتاجات

1. يوفر البرنامج واجهة مرئية سهلة الاستخدام من قبل المستخدم ومرنة وواضحة تمكن المستخدم من تحديد العملية واختيار الصورة.

2. الخوارزمية المستخدمة في هذا المشروع توفر سرية كبيرة في إرسال الرسائل والتي تتضمن ما يأتي:

أ. استخدام الإبدال العشوائي لمواقع المراتب الثنائية للرسالة الأصلية وهذا يوفر سرية للرسالة المرسلة.

ب. القيام بعملية الإبدال العشوائي عن طريق استخدام مفتاح سري خاص لا يمكن إرجاع الرسالة الأصلية من دون معرفته ويكون معروف من قبل الشخص المخول فقط.

3. تم تنفيذ البرنامج على الصور الملونة والرمادية إذ أن الصور الملونة قد يكون التشوه فيها واضحا أو نسبة التشوه كبيرة ولهذا تم تحويلها إلى صور رمادية باستخدام صيغة (Ycbcr) ومن ثم تضمينها وبعد التضمين تم إرجاعها إلى صيغتها الأصلية وهي صيغة (RGB) .

4. يمكن تنفيذ البرنامج على صور غير محددة الأبعاد واكبر من حجم الرسالة المراد إخفاؤها.

5. تم الحصول على نتائج جيدة في الإخفاء باستخدام هذه الخوارزمية إذ تم حساب نسبة التشوه في الصور الناتجة بعد التضمين ولوحظ إنها نسبة جيدة جدا تشير إلى عدم حصول أي تشوه ملحوظ.

المصادر

[1] Bender, W. ; D. Gruhl, ; N. Morimoto, and A. Lu (1996) "Techniques for data hiding", **IBM Systems Journal**, Vol. 35.

[2] Bret, D. (2002) "A detailed look steganographic techniques and their use in open-system environment" ,**SANS Institute**.

[3] Cummins, J.; P. Diskin, and R. Parlett (2000) "Steganography and digital watermarking", **school of computer science**, University of Bermingham.

[4] Hopper, N.; J. Langford, and L. Ahn (2002) " Provably secure steganography", **CRYPTO** August 2002.

[5] Johnson, N. and Z. Duric, (2000) **Information hiding: steganography and watermarking attacks and countermeasures**, Kluwer Academic Publishers.

[6] Karzenbeisser, S. and F. Petitcolas (2000) **Information hiding techniques for steganography and digital watermarking** , Artech House.

[7] Kharrazi, M. and H. Sencar, (2004) "Image steganography: concepts and practice".

[8] Law, C. (1995) "Steganography hiding writing", **Information Network**.

[9] Petitcolas, F. and R. Anderson (1999) "Information hiding-A survey", **IEEE**.