طريقة مقترحة لإخفاء المعلومات داخل الصور الملونة باستخدام تقنيات الكتابة المخفية

خالد السلطان(•)

الملخص

هذا البحث يقدم طريقة لإخفاء البيانات السرية في الصور الملونة عن طريق إخفاء حروف النص داخل عناصر الصورة، وذلك بالاعتماد على تقسيم الكود الثنائي للمحرف إلى ثلاثة أجزاء و إخفاء كل جزء في بتات كل لون من الألوان الثلاثة (R,G,B) التي تمثل عنصر الصورة الملونة دون ملاحظة أي تغير أو تشويه بالصورة الحاملة للبيانات السرية.

إن هذه الطريقة تعتمد على الإخفاء المبعثر أي إخفاء حروف الرسالة السرية داخل عناصر الصورة بطريقة غير متتابعة أي جعل المسافة بين العناصر المستخدمة في عملية الإخفاء غير ثابتة مما يصعب إمكانية توقع مواقع إخفاء البيانات السرية المراد اخفائها داخل الصورة باستخدام طرائق تحليل الصورة أو باستخدام طرائق التحاليل الاحصائية التي تهدف إلى توقع أماكن اخفاء البيانات.

نجحت هذه الطريقة في إخفاء الملفات النصية دون حدوث حالة تشوه للصورة الأصلية، أو إمكانية ملاحظة التغيرات الحاصلة فيها جراء عملية الإخفاء. ومن أجل أثبات دقة النتائج وكفاءة طريقة الإخفاء المقترحة في هذا البحث طبقت المقايس(MSE, PSNR, and NCC)، أما التنفيذ تم باستخدام Matlab 9.

الكلمات المفتاحية: إخفاء المعلومات، الكتابة المخفي، معالجة الصور.

• أستاذ مساعد، قسم الاقتصاد الزراعي، كلية الزراعة بجامعة دمشق، سورية.

Proposed Method for Information Hiding In color Images Using Steganography Techniques

Khaled AlSultan(*)

Abstract

This research provides a method for hiding secret data in color images. The binary represatintation of characters of the secret message is divided into three parts by dividing the bits of the character into three parts, and every part is hidden in bits of each color of the three colors (RGB), which represents the colored image element.

The characters of the secret message are embedded in non-sequential pixels, therefore the distance between characters is not constant. It will be difficult to quest the place of bits of character in the pixels by image analysis or statistical analysis methods. The method succeeded in hiding many types of text in different images without degrading or seeing any difference between the Stego image and the original image. Measures such as MSE, PSNR and NCC are used to prove the accuracy of the results and efficiency. The application implemented using Matlab 9.

Keywords: Information Hiding, Steganography, Image processing.

* Assocaite Professor, Department of Agricultural Economics, Faculty of Agriculture, University of Damascus, Syria

١ – مقدمة:

نظراً للتطور الهائل في مجال التقنية الرقمية وشبكة الانترنيت والاتصالات، أصبحت الخصوصية الشخصية عرضة للانتهاك بسهولة أكثر من ذي قبل، لذلك كان لابد من طرائق تُحفظ بها سرية البيانات الشخصية اثناء تداولها عبر الشبكات المحلية والعالمية والبريد الالكتروني و الهواتف النقالة لمنع المتطفلين من الاطلاع على محتوياتها أو سرقة المعلومات المهمة أو العبث بها، لهذا لغرض أوجدت تقنية الكتابة المخفية الرقمية.

الكتابة المخفية (Steganography): هي علم وفن إخفاء البيانات المُراد إرسالها (قد تكون رسائل نصّية أو صورية) بصورة مبهمة داخل بيانات مُرسلة (صور– صوت – فيديو). والهدف منه بصورة عامة هو إخفاء وجود البيانات بحيث إن المتطفل لا يشك بوجود بيانات مخفية أصلا، ويعتمد سر نجاح نظام الكتابة المخفية على استخدام طرائق وتقنيات بعيدة عن التوقع، فضلا عن كونه يمكن استخدامه في جميع الوسائط الحاسوبية من صور ونصوص و صوت و فيديو وحزم الشبكة وذلك بعكس طرق التشفير التي تعتمد على خوارزميات قياسية ومعروفة [1] .

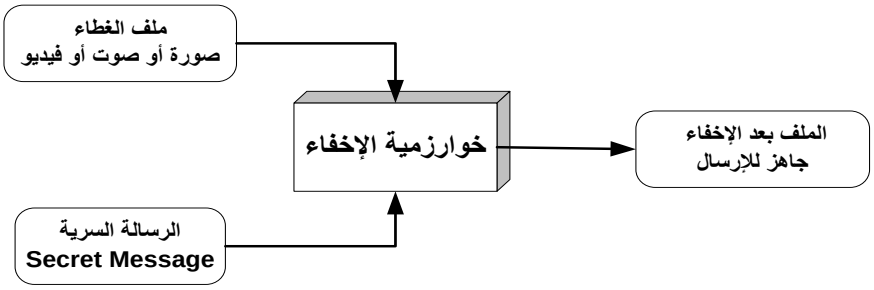
تهدف تقنية الكتابة المخفية (Steganography) إلى إخفاء البينات داخل بيانات أخرى، بطريقة لا تؤدي إلى التأثير في هذه الأخيرة، بحيث لا تثير أي شبهة أو شك قد يؤديان إلى كشف الحقيقة، والغرض من عملية الإخفاء هذه أن لا يعلم المهاجم المحتمل عن وجود هذه البيانات، وبالتالي يتم حمايتها من القراءة أو التغيير أو التدمير عن طريق هذا المهاجم.

وبشكل خاص إن تقنيات إخفاء المعلومات داخل الصور أصبحت واسعة الانتشار في الوقت الحاضر، فالصور الرقمية لها استخدامات في كثير من التطبيقات الرقمية على شبكة الانترنت، حيث إن الصور الحاملة للرسائل السرية يمكن أن تنتشر بسهولة عبر الانترنيت

وبالتالي فهي مغرية لإخفاء المعلومات. ونتيجة لذلك شهد العقد الماضي اهتماماً متزايداً بالبحوث في مجال الكتابة المخفية داخل الصور الرقمية [2]. أما حاليا تشغل الأبحاث في مجال هذه التقنية حيزا كبيرا من اهتمام الباحثين، لسبب بسيط وهو أن لهما استخدامات هامة في مجال التجارة الإلكترونية (E-Commerce) التي تزداد تطبيقاتها، والاهتمام بها يوما بعد آخر.

أيضاً من أهم تطبيقات تقنية الكتابة المخفية (Steganography) هي العلامات المائية الرقمية أو ما يعرف بـ(Digital Watermarks) والتي تستخدم في عمليات حفظ حقوق الملكية للمنتجات الرقمية، والحد من عمليات القرصنة، مثل الاسطوانات الخاصة بالموسيقى وغيرها، وكذلك الصور والبرامج التي تباع عبر الإنترنت .فبالرغم من المشتري هنا قد يعلم بوجود هذه العلامات، لكنه لا يعرف أين توجد داخل المنتج، ولا البرنامج الذي استخدم في عملية الإخفاء، ولا كلمة السر ومفتاح التشفير، وبالتالي يصعب عليه إزالتها، وإعادة النسخ [2].

لتطبيق تقنية إخفاء البيانات يتطلب جود ثلاثة عناصر موضحة بالشكل رقم (١) الذي يبين مخطط عملية إخفاء الرسالة السرية داخل ملف الغطاء[1].



الشكل (١): مخطط عملية إخفاء ملف التضمين داخل ملف الغطاء.

- ملف الغطاء: وهو عبارة عن ملف (صورة أو صوت أو فيديو) يستخدم لإخفاء البيانات المطلوب إخفائها، يتم الإختيار حسب كمية البيانات المطلوب إخفائها، مع مراعاة خفض نسبة التشوه الذي يحصل له عنداخفاء البيانات.
- الملف المضمَّن (الرسالة السرية): هو ملف يتضمن البيانات السرية المطلوب إخفائها، وقد يكون نص رسالة أو صورة، مع ملاحظة حجم تلك البيانات ومقارنتها بملف الغطاء المستخدم.
- خوارزمية الإخفاء: الأسلوب الذي يستخدم في إخفاء البيانات، وهنالك عدة خوارزميات معتمدة في الإخفاء ومنها:
  - خوارزمية البت الأقل أهمية (Least Significant Bit)
  - طريقة التحويلات في المجال الترددي (Wavelet and Cosine Transformation)
  - طرق العلامات المائية الرقمية (Digital Watermarking)

2- أهمية البحث:

ظهرت في العقود الأخيرة تقنيات تشفير البيانات كطرائق لحماية لخصوصية وأمنية المعلومات والاتصلات عبر شبكة الانترنت، لكن مع مرور الوقت أثبتت التجارب أن هذه الطرق غير ناجحة لأن أمنية الاتصالات ليس فقط التشفير وإنما أيضا أمنية المرور التي يكون جوهرها موجود في إخفاء المعلومات، لذلك برزت الحاجة لإيجاد طرق لإخفاءالمعلومات بدلًا من تشفيرها.

تمثل تقنية إخفاء المعلومات الحبر السري للوثائق الرقمية، أي إن اخفاء المعلومات يعني إخفاء معلومات في معلومات أخرى بريئة المظهر ولا تجلب الانتباه وجعلها غير مدركة من قبل المتطفلين والمهاجمين وهكذا تكون المعلومات مجهولة لمستخدمين الشبكة بينما يبقى محتواها حكرا على الجهات ذات العلاقة والتي تعرف كيفية استخراج محتواها.

لإخفاء المعلومات أهمية كبيرة وذلك لأن عدم ظهور المعلومات سواء مشفرة أو غير مشفرة للعيان عاملاً مساعداً لإضفاء حماية وأمناً على المعلومات، ويستخدم هذا العلم في عدد من المجالات أهمها التجارة الإلكترونية التي تزداد تطبيقاتها والأهتمام بها على مستوى العالم يوماً بعد أخر. ومن تطبيقات هذا العلم، العلامات المائية الرقمية (Digital Watermarks) والتي تستخدم في عمليات حفظ حقوق الملكية للمنتجات الرقمية والحد من عمليات القرصنة.

3- هدف البحث:

إن الهدف الأساسي من هذا البحث هو إيجاد طريقة جديدة لإخفاء الأنواع المختلفة من الملفات النصية السرية والمهمة داخل الصور الملونة دون أن يلاحظ أي تغير أو تشوه واضح في معلومات الصورة بعد عملية الإخفاء، أو محاولة اكتشافها من قبل المتطفلين. ثم استخلاص الرسالة السرية المخفية من الصورة المرسلة بشكل كامل وبدون خسارة أو ضياع أو تشويه لأي من محتوياتها وبدون الاعتماد عل الصورة الأصلية. وكذلك من أجل التأكد من كفاءة الطريقة المقدمة يتم تطبيق عدة مقاييس لمعرفة مدى دقة الاخفاء وعدم تمييز النص المخفي داخل الصورة.

4- استعراض البحث:

يكون تمثيل الحروف والأرقام والعلامات الأخرى داخل الحاسب حسب الترميز القياسي الأمريكي للمعلومات المتبادلة (ASCII: American Standard Code for Information Interchange) وهذا الترميز يستخدم الأرقام من 0 إلى 255 ، حيث أن كل رقم يتمثل ببايت واحد والترميز بهذه الصيغة يسهل نقل النصوص بين الحاسبات و الأجهزة الملحقة، كونها تتمثل بصيغة قياسية موحدة عالمياً.

وتتكون الصورة من مصفوفة من العناصر (Pixels) حيث يمثل كل عنصر من عناصرها بقيمة حسب نوع الصورة حيث يوجد ثلاثة أنواع من الصور كما يلي:

- **النوع الأول:** الصور الثنائية (Binary Image): هي ابسط أنواع الصور وتتكون من لونين الأبيض والأسود حيث يمثل كل عنصر من عناصرها ببت واحد قيمته إما (٠) للون الأسود أو (١) للون الأبيض.
- **النوع الثاني:** الصور رمادية التدرج (Monochrome Images): أو تسمى الصور ذات تدرج اللون الواحد (One Color Image). هذا النوع من الصور الرقمية تحتوي معلومات الإضاءة (Brightness) فقط و لاتحتوي على معلومات عن الألوان. يتمثل كل عنصر (pixel) من عناصر الصورة بعدد من البتات من خلالها يمكن معرفة عدد التدريجات اللونية في هذه الصورة، فمثلا إذا تم تمثيل عنصر الصورة بثلاث بتات فإن ذلك يدل على أن لهذه الصورة على الأكثر ثمان من التدريجات (من٠٠٠ إلى ١١١) وإذا تمثل عنصر الصورة بـ (٨ بت) (٨ Bit/Pixel) فان الصورة لها على الأكثر٢٥٦ تدرج لوني (أو مستويات الإضاءة) إذ تمثل القيمة (٠) أدنى قيمة (٠٠٠٠٠٠٠٠) وتمثل اللون الأسود، والقيمة (255) تمثل أعلى قيمة (١١١١١١١١) وتمثل اللون الأبيض، والقيم بين العدد (٠) والعدد (٢٥٥) تمثل تدرج الالوان من الاسود إلى الابيض .في هذا النوع من الصور يتم إخفاء النص داخل الصور أحادية اللون بإخفاء (٢ بت) من بتات الرسالة السرية على الأكثر في بتات عنصر الصورة وفي هذه الحالة يكون تأثير الإخفاء على الصورة قليل جدا.
- **النوع الثالث:** الصور الملونة :هناك مجموعة من الألوان تدركها العين البشرية والتي تنتج ببساطة بإضافة نسب من الألوان الأساسية (الأحمر والأخضر والأزرق)، (Red, Green, Blue)، هذه الألوان تشكل الأساس لفضاء الألوان ومن الممكن تكوين أي لون بالوجود بواسطة تجميع هذه الألوان الأساسية (RGB) الثلاثة بنسب مختلفة.

في هذا النوع من الصور لون كل عنصر (pixel) من عناصر الصورة يتمثل بثلاثة أحزمة (3 Bands) كل حزمة تمثل لون من الألوان الأساسية الثلاثة وكل لون يتمثل ب (1

(Byte= 8 bit) وبالتالي كل عنصر يتمثل ب (3 Byte) أي (24 bit) هذا يعني أي قيمة كل بكسل بالصور الملونة تتراوح من (٠ إلى ١٦٧٧٧٢١٦) وكل قيمة تمثل لون مختلف للبكسل وهذا يوضح سبب كبر حجم الصور الملونة بالمقارنة مع سابقاتها.

تتم عملية الإخفاء بصورة عامة بتحويل الملف الذي يمثل الرسالة السرية المراد إخفائها إلى سلسلة من البتات يتم إخفاؤها داخل بتات عناصر الصور ة وذلك باستبدال عدد من بتات عنصر الصورة بنفس العدد من بتات الحرف المراد إخفاؤه في مواقع البتات الأقل أهمية (Least Significant Bits) ويرمز لها اختصارا (LSB). إذ أن التلاعب بقيم البتات الأقل أهمية لا يؤثر كثيرا على قيمة اللون، وهذا التأثير الطفيف لا يمكن ملاحظته بالعين البشرية.

وفي طرائق أخرى تخفي البتات داخل عناصر الصورة في أماكن متفرقة ويلزم ذلك عمل خارطة أو جدول لمواقع التوزيع، وعندها يستوجب وجود الخارطة أو الجدول أو الصورة الأصلية لاستخلاص بتات الملف المخفي مما يثير الشك لدى المتطفلين وبالتالي يزيد احتمال اكتشاف النص.

وبما أن إخفاء بتات الرسالة السرية داخل عناصر الصورة بشكل متسلسل (عنصر بعد عنصر) يزيد من احتمالية اكتشاف النص المخفي بطرق تحليل الصورة أو باستخدام العمليات الإحصائية ، لذلك تم اقتراح استخدام الأسلوب الآتي:

5- الطريقة المقترحة لإخفاء البيانات واسترجاعها:

تعتمد الطريقة المقترحة في عملية الإخفاء على الصور الملونة. حيث يتم تجزئة بايت الحرف (من الرسالة السرية) إلى ثلاثة أجزاء احدها يحوي على بتين والآخران كل منهما يحوي على ثلاث بتات، و يتم إخفاء كل جزء في بايت كل لون من الألوان الثلاثة التي تمثل عنصر الصورة الملونة، و بما أن نظام الرؤية البشرية يؤكد إلى أن العين البشرية

أكثر تحسساً للون الأزرق من اللونين الآخرين (الأحمر الأخضر). لذلك تم اعتماد صيغة إخفاء البتين في اللون الأزرق (B) والجزأين الآخرين في اللونين الأحمر و الأخضر (R,G) وهكذا نستطيع اخفاء محرف واحد من الرسالة السرية ب عنصر (Pixel) واحد من عناصر الصورة.

بما أن إخفاء بتات الرسالة السرية داخل عناصر الصورة بشكل متسلسل (عنصر بعد عنصر) يزيد من احتمالية اكتشاف النص المخفي، ولزيادة دقة الإخفاء وتقليل احتمالية الكشف عن النص المخفي داخل الصورة، فإن الطريقة المقترحة في هذا البحث تعتمد على الإخفاء المبعثر أي إخفاء أجزاء بايت حروف الرسالة السرية داخل بايتات عناصر الصورة بطريقة غير متتابعة إذ ستكون المسافة بينها غير منتظمة، و هذه المسافة تسمى مسافة البعثرة ويرمز لها بـ (D) وتحسب كما يلي: D = S+key.

حيث key هو المفتاح السري و(S) تمثل قيمة الإزاحة التي تتمثل بـ(٣ بتات) وتؤخذ من بايتات الألوان الثلاثة (R G B) لعنصر الصورة بحيث يؤخذ البت الأكثر أهمية (Most Significant Bits-MSB) من بتات كل لون بالترتيب.

كذلك إن إضافة المفتاح السري لقيمة الإزاحة تعد وسيلة أمان لكي لا يتم الإخفاء في نفس الموقع الحالي عندما تكون قيمة الإزاحة تساوي الصفر (S=000=0).وهذه الحالة ممكن تحدث أذا تصادف أن البتات الأكثر أهمية للألوان الثلاثة كانت أصفار. أن مسافة البعثرة سوف تضاف إلى موقع العنصر الحالي (في مصفوفة الصورة) إلى الاحداثي الشاقولي لتحديد موقع عنصر الصورة اللاحق الذي ستتم فيه عملية الإخفاء.

5-١ مرحلة التضمين:

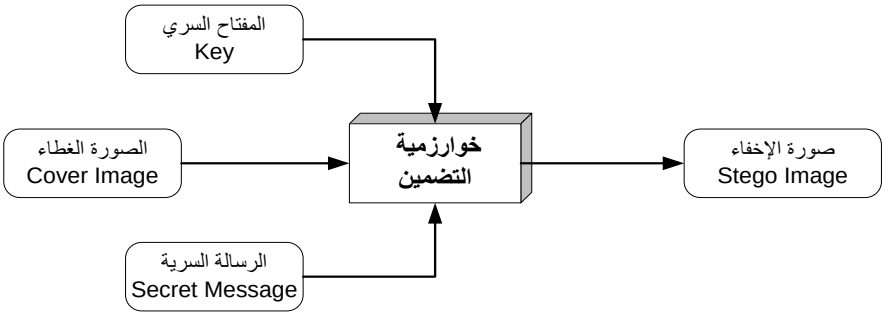
هي المرحلة التي يتم فيها تضمين البيانات السرية في الغطاء، وتتألف مدخلات هذه المرحلة من:

١- صورة الغطاء (Cover Image): هي الصورة التي تستخدم لتضمين البيانات السرية داخلها.

٢- الرسالة السرية (Secret Message): وهي البيانات السرية المراد إخفائها داخل صورة الغطاء.

٣- المفتاح (Key): هو المفتاح السري والمعروف مسبقاً من قبل المرسل والمستقبل فقط.

أما مخرجات هذه المرحلة فإنها تمثل الصورة بعد أخفاء البيانات السرية داخلها وتسمى صورة الأخفاء (Stego Image). الشكل رقم (٢) يبين مدخلات ومخرجات مرحلة التضمين.



الشكل (2): مخطط عملية إخفاء الرسالة السرية داخل صورة الغطاء.

خوارزمية الإخفاء (التضمين):

إن خوارزمية الإخفاء في الصور الملونة يمكن إجمالها بالخطوات الآتية:

١- يوجد مفتاح سري (Key) قبل بداية الإخفاء ومعروف من قبل المرسل والمستقبل فقط.

2- عرض الرسالة السرية المراد إخفاءها بوساطة احد البرامج لعرض النصوص وإضافة محرف مميز لأخر الرسال كمؤشر لنهاية عملية الإخفاء.

٣ –اختيار صورة الغطاء (Cover Image) وبحجم مناسب لإخفاء النص بداخلها.

٤– قراءة الحرف من النص وإيجاد صيغة الآسكي المقابلة له بالبايت، ثم يجزأ البايت إلى ثلاثة أجزاء (P1,P2,P3) الجزء الأول يحوي على (٢ بت) البتين الأولين أما الجزأين الثاني والثالث فكل منهما يحوي على (٣ بت) بالتتابع.

٥ – تعيين موقع عنصر الصورة الذي سيتم إخفاء أول حرف من حروف الرسالة السرية (E1= (2, Key

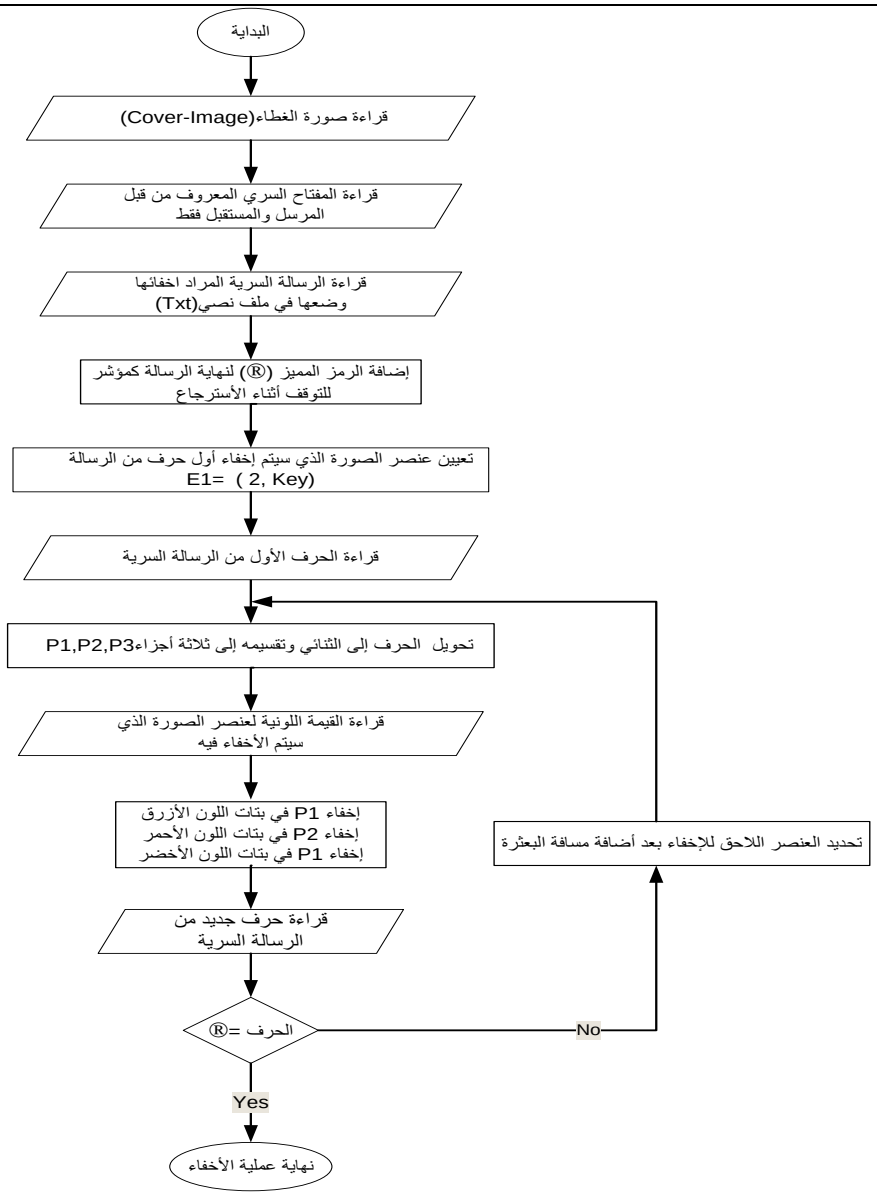
٦– قراءة القيمة اللونية لعنصر الصورة باستخلاص قيم البايتات الثلاثة الممثلة للألوان الأساسية (الأحمر، الأخضر والأزرق) (R,G, B).

٧– استبدال أول (٢ بت) من بتات اللون الأزرق ببتات الجزء P1، واستبدال أول (٣ بت) من بتات اللون الأحمر ببتات الجزء الثانيP2، واستبدال أول (٣ بت) من بتات اللون الأخضر ببتات الجزء الثالث P3، لتكوين قيمة بايتات الألوان الثلاثة الجديدة للعنصر.

٨– تحديد موقع العنصر اللاحق الذي ستتم فيه عملية الإخفاء وذلك بحساب مسافة البعثرة (D) وإضافتها إلى موقع العنصر الحالي.

٩– تكرار الخطوات(٥،٦،٧،8) لحين انتهاء حروف الرسالة السرية والوصول للحرف المميز في نهاية الرسالة.

١٠– في نهاية عملية الإخفاء تتحول الصورة الأصلية (Cover Image) إلى صورة الإخفاء (Stego Image) التي تحوي بداخلها الرسالة السرية (Secret Message) لارسالها للهدف. الشكل (3) يوضح خطوات خوارزمية الإخفاء.


البداية
قراءة صورة الغطاء(Cover-Image)
قراءة المفتاح السري المعروف من قبل
المرسل والمستقبل فقط
قراءة الرسالة السرية المراد اخفائها
وضعها في ملف نصي(Txt)
إضافة الرمز المميز (Ⓡ) لنهاية الرسالة كمؤشر
للتوقف أثناء الأسترجاع
تعيين عنصر الصورة الذي سيتم إخفاء أول حرف من الرسالة
E1= (2, Key)
قراءة الحرف الأول من الرسالة السرية
تحويل الحرف إلى الثنائي وتقسيمه إلى ثلاثة أجزاءP1,P2,P3
قراءة القيمة اللونية لعنصر الصورة الذي
سيتم الأخفاء فيه
إخفاء P1 في بتات اللون الأزرق
إخفاء P2 في بتات اللون الأحمر
إخفاء P1 في بتات اللون الأخضر
تحديد العنصر اللاحق للإخفاء بعد أضافة مسافة البعثرة
قراءة حرف جديد من
الرسالة السرية
الحرف =Ⓡ
No
Yes
نهاية عملية الأخفاء

الشكل (3): خطوات خوارزمية إخفاء الرسالة السرية داخل صورة الغطاء.

مثال تطبيقي:

المثال التالي يوضح طريقة الإخفاء المقترحة:

بفرض أن المفتاح السري بين المرسل والمستلم هو (Key=6)، ونريد إخفاء الحرف (M) في عنصرالصورة الملونة.

١– تحويل قيمة الحرف إلى النظام الثنائي $M=(109)_{10}=(01101101)_2$

٢– تجزئة بايت الحرف إلى ثلاثة أجزاء(P1,P2,P3) على أن يبدأ التقسيم من اليمين أي من البت الأقل أهمية كما يلي:

- الجزء الأول (P١) يتالف من (٢ بت) أي $P١=(01)_٢$
- الجزء الثاني (P٢) يتالف من (٣ بت) أي $P٢=(011)_٢$
- الجزء الثالث (P٣) يتالف من (٣ بت) أي $P١=(011)_٢$

٣– تحديد مكان أول عنصر من عناصر الصورة ليتم بداية الأخفاء فيه من العلاقة:

$E1=(2, Key)=(2, ٦)$

ثم يتم قراءة قيم هذا العنصر $E1=(R, G, B)=(150,202,138)$

٤– تحويل القيم اللونية الثلاثة للعنصر (E1) إلى الثنائي.

$R=(150)_{10}=(10010110)_2$

$G=(202)_{10}=(11001010)_2$

$B=(138)_{10}=(10001010)_2$

٥– إخفاء الجزء الأول في(LSBs) من بايت اللون الأزق

$B_{new}=(10001001)_2=(137)_{10}$

٦– إخفاء الجزء الثاني في(LSBs) من بايت اللون الأحمر

$R_{new} = (10010011)_2 = (147)_{10}$

٧- إخفاء الجزء الثالث في(LSBs) من بايت اللون الأخضر

. $G_{new} = (11001011)_2 = (203)_{10}$

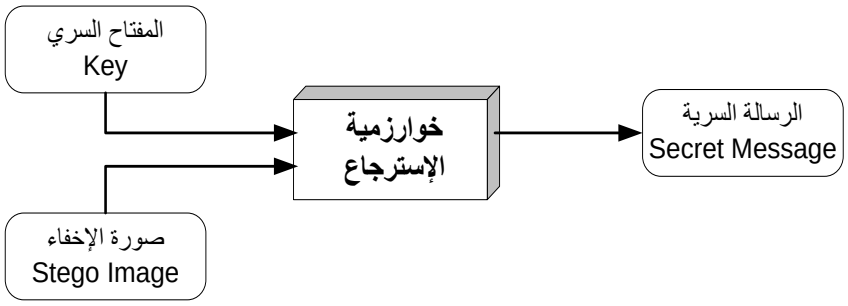
٨- لحساب عنوان العنصر التالي .نحسب قيمة الإزاحة S ومسافة الإخفاء D.

S=(111)=7 D=S+Key =7+6=13

En=(2 ,D+٦) = (2 ,١٣+٦)=(2, ١٩)

٥-٢ مرحلة الاسترجاع:

هي المرحلة التي يتم فيها استرجاع الرسالة السرية من صورة الإخفاء وتتألف مدخلات هذه المرحلة من صورة الإخفاء (Stego Image) والمفتاح السري (Key) الذي استخدم نفسه في عملية الإخفاء. أما مخرجات هذه المرحلة هي الرسالة المخفية (Secret Message). الشكل رقم (٤) يبين مدخلات ومخرجات مرحلة الإسترجاع.



الشكل (٤): مخطط عملية استرجاع الرسالة السرية من صورة الإخفاء.

خوارزمية الإسترجاع :

وهذه العملية هدفها استخلاص الرسالة السرية المخفية داخل الصورة المرسلة بواسطة المفتاح السري المتفق عليه مسبقاً بين المرسل والمستقبل، وخطوات هذه الخوارزمية كما يلي:

١– عرض ملف نصي فارغ لأحد برامج النصوص من أجل تجميع حروف الرسالة المخفية ضمن هذا الملف.

٢– عرض الصورة التي تحمل الرسالة السرية (Stego Image).

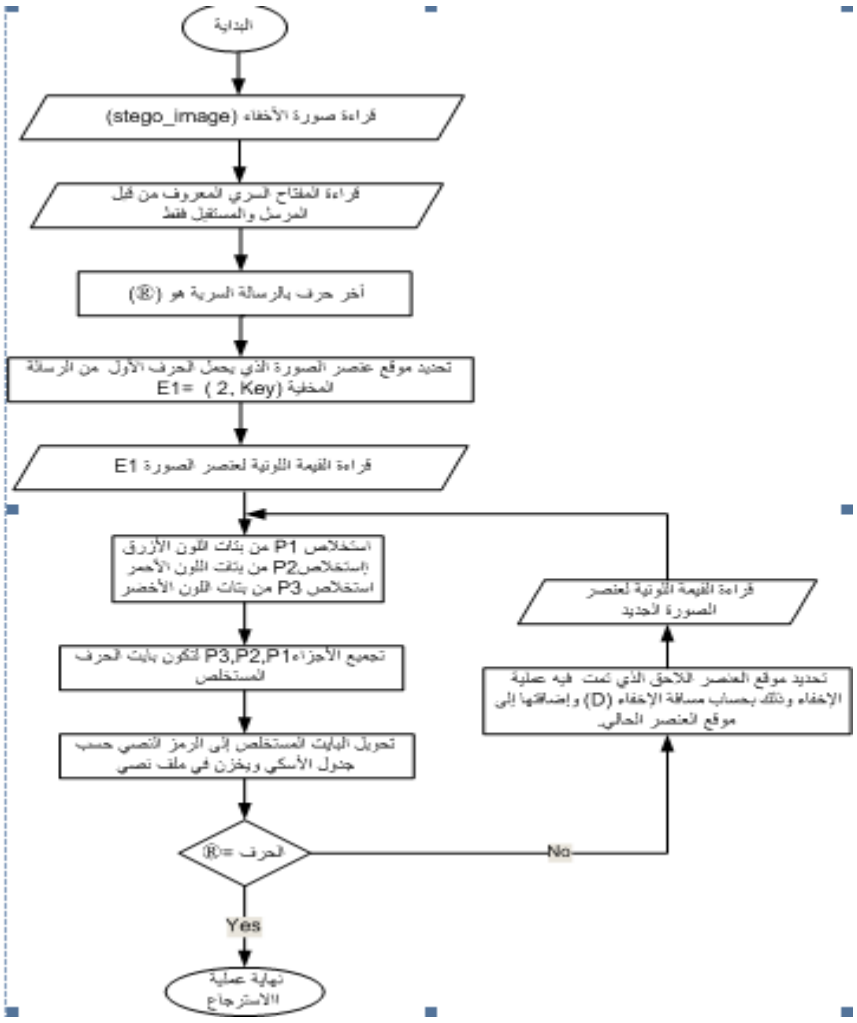
٣– تحديد موقع عنصر الصورة الذي يحمل الحرف الأول من حروف الرسالة المخفية (Stego Massage) وهو العنصر E1= (2, Key)

٤– قراءة القيمة اللونية لعنصر الصورة E1 واستخلاص قيم البايتات الثلاثة التي تمثل اللون الأحمر والأخضر والأزرق، ثم تؤخذ البتات المستبدلة في عملية الإخفاء من كل لون من الألوان الثلاثة (أول بتين من بتات اللون الأزرق وأول ثلاث بتات من بتات اللون الأحمر وأول ثلاث بتات من بتات اللون الأخضر) ثم يتم تجميعها بالترتيب لتكون (٨ بت) قيمة بايت الحرف المستخلص.

٥– تحويل قيمة الحرف المستخلص من صيغة الآسكي إلى الشكل الذي يمثله ويوضع في ملف برنامج النصوص.

٦– تحديد موقع العنصر اللاحق الذي تمت فيه عملية الإخفاء وذلك بحساب مسافة الإخفاء (D) وإضافتها إلى موقع العنصر الحالي.

٧– تكرار الخطوات (٤،٥،٦) لحين استرجاع حروف الرسالة المخفية بالكامل والوصول للحرف المميز الذي يدل على نهاية الرسالة السرية وانتهاء عملية الاسترجاع والحصول على الرسالة السرية (Secret Message). الشكل (٥) يعرض خطوات خوارزمية استرجاع الرسالة السرية من صورة الإخفاء.


البداية
قراءة صورة الأخفاء (stego_image)
قراءة المفتاح السري المعروف من قبل المرسل والمستقبل فقط
آخر حرف بالرسالة السرية هو (®)
تحديد موقع عنصر الصورة الذي يحمل الحرف الأول من الرسالة المخفية E1= (2, Key)
قراءة القيمة اللونية لعنصر الصورة E1
استخلاص P1 من بتات اللون الأزرق
إستخلاصP2 من بتات اللون الأحمر
استخلاص P3 من بتات اللون الأخضر
تجميع الأجزاءP3,P2,P1 لتكون بايت الحرف المستخلص
تحويل البايت المستخلص إلى الرمز النصي حسب جدول الأسكي ويخزن في ملف نصي
®= الحرف
No
Yes
نهاية عملية الاسترجاع
قراءة القيمة اللونية لعنصر الصورة الجديد
تحديد موقع العنصر اللاحق الذي تمت فيه عملية الإخفاء وذلك بحساب مسافة الإخفاء (D) وإضافتها إلى موقع العنصر الحالي.

٦- عرض ومناقشة النتائج:

طبقت طريقة الإخفاء المقترحة في هذا البحث على خمسة صور ملونة بامتدادات مختلفة (JPG, JPEG, BMP) وذات أبعاد مختلفة. ومن أجل قياس كفاءة طريقة الاخفاء المستخدمة تم استخدام عدة مقاييس لمعرفة مدى دقة الاخفاء وعدم تمييز النص المخفي في الصورة بالعين البشرية أهم هذه المقاييس [3]:

١- متوسط مربع الخطأ (Mean Squared Error(MSE:

لحساب متوسط الخطأ بين الصورة الأصلية وصورة الإخفاء يجب أن نعرف الفرق بين لون عنصر الصورة pixel بين الصورتين قبل الإخفاء وبعده، وذلك وفق المعادلة الآتية:

$$MSE = \frac{1}{mn}\sum_{x=0}^{m-1}\sum_{y=0}^{n-1} stego\_im(x,y) - \text{cover}\_im(x,y) \quad \ldots\ldots\ldots\ldots(1)$$

٢- نسبة قمة الإشارة إلى الضوضاء (Peak Signal to Noise Ratio (PSNR :

ويسمى مقياس مقدار التشوه في الصورة بعد أخفاء البيانات فيها، وهو يقيس مقدار الفرق بين الصورة الأصلية و صورة الإخفا وتسمى وحدة قياس PSNR بالديسبل db. وتعبر هذه القيمة عن خاصية عدم الاكتشاف Undetectabililty وتحسب بالمعادلة التالية:

$$PSNR = 10Log_{10}\left(\frac{MAX(\text{cover}\_im)}{MSE}\right) \quad \ldots\ldots\ldots\ldots\ldots(٢)$$

٣- معامل الارتباط Normalization Correlation Coefficient:

يستخدم هذا المقياس لحساب الفرق بين الصورة الأصلية قبل الإخفاء(صورة الغطاء) والصورة الناتجة بعد الإخفاء (صورة الإخفاء) لقياس مدى التقارب بينهما فكلما كانت قيمة

معامل الأرتباط قريبة من الواحد كان ذلك دليلاً على عدم وجود تشوه بالصورة بعد إخفاء البيانات داخلها وعدم تميزها عن الصورة الأصلية، ومعامل الارتباط يمكن حسابه بالمعادلة التالية [4]:

$$NCC = \sum_{x=0}^{m-1}\sum_{y=0}^{n-1} stego\_im(x,y) * cover\_im(x,y) / \sum_{x=0}^{m-1}\sum_{y=0}^{n=1}((cover\_im(x,y))^2$$

m,n: تمثل طول الصورة وعرضها

im _ stego : تمثل الصورة التي تحوي الرسالة السرية (صورة الإخفاء).

im _ cover: تمثل الصورة الأصلية (الغطاء)

MAX(cover_im) اكبر قيمة لونية في الصورة وتساوي (2^B-1) حيث B عدد البتات الممثلة لعنصر الصورة. الجدول رقم (١) يعرض نتائج تنفيذ الطريقة المقترحة و حساب قيم المقايس الثلاثة (MSE, PSNR, NCC) على خمس صور بأحجام مختلفة وأطوال نصوص مختلفة.

NCC	PSNR (db)	MSE	Text Length (Byte)	Image Size	Image type	Image Name	
0.998	61.751	0.042	1300	350 X 500	BMP	flowers	١
0.996	57.654	0.063	2500				
0.999	66.278	0.021	1300	550 X 750			
0.998	62.921	0.037	2500				
0.997	58.236	0.058	1300	350 X 500	JPEG	birds	٢
0.996	58.325	0.064	2500				
0.998	63.124	0.035	1300	550 X 750			
0.998	60.543	0.048	2500				
0.995	55.745	0.074	1300	350 X 500	BMP	ship	٣
0.995	51.278	0.081	2500				
0.998	60.007	0.049	1300	550 X 750			
0.996	57.107	0.062	2500				
0.999	64.218	0.028	1300	350 X 500	JPG	Coast	٤
0.998	62.745	0.038	2500				
0.999	68.254	0.012	1300	550 X 750			

						0.026	65.981	0.999
٥	Car	JPEG	350 X 500	1300	0.065	58.758	0.996
				2500	0.078	54.214	0.995
			550 X 750	1300	0.050	61.254	0.997
				2500	0.061	57.324	0.996

جدول (١): نتائج تنفيذ الطريقة المقترحة و قيم المقاييس NCC, MSE،PSNR على خمس صور مختلفة.

المصدر: نتائج البحث.

من خلال الجدول (1) نلاحظ أن معامل الارتباط متقارب جداً بين الصورة الأصلية(Cover_Image) والصورة المضمنة للرسالة (Stego_Image) كذلك يمكن ملاحظة الفرق الطفيف بين هذه الصور من خلال المقاييسMSE و PSNR والتي يتبين بشكل واضح أن تتأرجح حول محور مستقر تقريباً.

كذلك النتائج المبينة في الجدول السابق تبين أن الطريقة المقترحة قد أعطت قيما مثلى للمقياس PSNRواقل ما يمكن بالنسبة لمقياس MSE، فكانت قيمة (PSNR) تتراوح بين (68.25 4db) و (51.278 db) لمجموعة الصور التي أخذت كعينات وهذ القيم تعتبر جيدة جداً، كذلك أعطت النتائج قيم أقل ما يمكن بالنسبة لمقياس MSE حيث تراوحت قيمها بين (0.012) و(0.081)، وكذلك قيمة معامل الارتباط (NCC) كانت قريبة من (١) لمجموعة الصور التي أخذت كعينات.

كذلك الواضح من الجدول أعلاه انه بزيادة طول النص تزداد قيمة MSE وتقل قيمة PSNR ولكن نسبة الزيادة نسبة قليلة جدا مما يدل على كفاءة الخوارزمية المستخدمة في الاخفاء بالرغم من طول النص المخفي، وكذلك فانه بزيادة حجم الصورة تزداد كفاءة الاخفاء ويصعب بل ولا يمكن لاي شخص تمييز وجود أي نص داخل الصورة والاشكال (٦) و (٧) توضح الصور قبل اخفاء النص وبعده.


(a) الصورة الأصلية قبل الإخفاء من نوع JPG	(b) الصورة بعد إخفاء نص بطول ١٣٠٠ حرف

الشكل (٦):(a) صورة الزهور (350 X 500) قبل الإخفاء . (b)الصورة بعد إخفاء ١٣٠٠ حرف


(a) الصورة الأصلية قبل الإخفاء من نوع BMP	(b) الصورة بعد إخفاء نص بطول 2500 حرف

الشكل (٧): (a) صورة سفينة (350 X 500) قبل الإخفاء . (b) الصورة بعد إخفاء 2500 حرف

٧- الاستنتاجات:

١- أثبتت النتائج قوة و كفاءة الخوارزمية المقترحة من ناحية السرية وإن المعلومات المخفية لم يحدث لها أي تغير أو تشوه ، حيث أن الطريقة المقترحة قد أعطت قيماً عالية للمقياس PSNR واقل ما يمكن بالنسبة لمقياس MSE.

٢– إن مسافة البعثرة بين عناصر الصورة تؤدي إلى تقليل احتمالية كشف النص المخفي كون التوزيع يعتمد على مفتاح سري (Secret–key) يتم الاتفاق عليه، فضلا عن مسافة تزحيف غير ثابتة، أما الطرق التي تستخدم الإخفاء المتتابع وبوتيرة ثابتة فإنها تكون أكثر عرضة للاكتشاف وإثارة للشك لدى المتطفلين.

٣– امتازت الخوارزمية المقترحة بالسعة العالية إذ أن عملية إخفاء في ٣ بت من بتات كل لون أمكننا من إخفاء نص يحوي عدد كبير من الأحرف دون حصول تشويه.

٤– بينت النتائج أنه عند زيادة حجم الرسالة السرية المخفية تكون النتائج مرضية ولا يتم ظهور أي علامة أو شك في وجود بيانات مخفية داخل الصورة.

٥– أثبتت الطريقة المستخدمة نجاحا في عملية إخفاء مختلف أنواع النصوص في مختلف أنواع الصور الملونة

٦– يفضل استخدام الصور ذات تفاصيل كثيرة أي الصور التي تحوي الوان مختلفة ومتنوعة في عملية الإخفاء.

٨– التوصيات:

١– من أجل سرية البيانات المخفية يوصى باستخدام طرائق تشفير مع طرق اخفاء البيانات.

٢– استخدام طرائق إخفاء للبيانات في المجال الترددي مثل DCT أو DWT أو DFT.

٣– التوسع في اقتراح طرائق لإخفاء البيانات تستطيع اخفاء قدر أكبر من البيانات دون ظهور تشوه في الصور الناقلة.

٤– استخدام الخوارزمية الجينية في تحديد أماكن اخفاء البيانات السرية وطرق استرجاعها.

٥– يمكن تعميم هذه التقني على الوسائط المختلفة من البيانات مثل ملفات الصوت والفيديو.

٦– توظيف تقنيات الذكاء الصناعي في أخفاء البيانات كالشبكات العصبية أوالخوارزمية الجينية أو المنطق الضبابي.

المراجع العربية والأجنبية:

[1] **برزنجي** فوزي، ٢٠٠٨– **اخفاء البيانات داخل الصورة.** جامعة السليمانية، العراق. http://www.boosla.com/

[2] **الحمامي** علاء حسين، **الحمامي** محمد علاء، 2008– **إخفاء المعلومات،** الكتابة المخفية والعلامة المائية. مكتبة جامعة الشارقة.

[3] **سعيد** ميلاد جادر، **يونس** غادة ذنون ،٢٠١٢– **وثوقية البيانات المخفية في الصور الملونة باستخدام مصفوفة حدوث المشاركة.** مجلة الرافدين لعلوم الحاسوب والرياضيات المجلد (٩)، العدد (١)، ٢٠١٢.

[4] **محمد** زهراء، **محمد** فرح، **ذنون** إخلاص، **عبد الله** أزهار، ٢٠١٣– **استخدام المجال الترددي للإخفاء في بعض ملفات الصوت.** مجلة الرافدين لعلوم الحاسوب والرياضيات المجلد (١٠) العدد (١) ٢٠١٣.

[5] ABDUL LATEF A., 2011- **Color Image Steganography Based on Discrete Wavelet and Discrete Cosine Transforms**. IBN AL- HAITHAM J. FOR PURE & APPL. SCI. VOL.24 (3).

[6] ABDELWAHAB A., Hassan L.A.., 2008-**A discrete wavelet transform based technique for image data hiding**. Proceedings of 25th National Radio Science Conference, Egypt.

[7] CHIN-ChEN C., 2005- **A DCT-domain System for Hiding Fractal Compressed Images**. Proceedings of the 19th International Conference on Advanced Information Networking and Applications (AINA'05),Vol.2.

[8] HSING C., JENG S., 2010- **Transforming LSB Substitution for Image-based Steganography in Matching Algorithms**. *Journal of Information Science and Engineering*.

[9] IYENGAR V., 2003- **Hiding Messages in Images and Text:Risk Associated with the Technology of Steganography**. *ISACA®InfoBytes Journal.*

[10] SEDEEK AL-OBAIDY E., 2008-**An Algorithm for Data Hiding in Binary Images**. Raf. J. of Comp& Math، Vol. 5, No. 2,