تقديم نظام اخفاء نصوص في الصور الملونة يعتمد على تقنية هيل في تشفير النص وإخفاءه في البت الأقل أهمية LSB في الصورة

م.م. كيان عبد العزيز مطلق

مركز الحاسبة الالكترونية / جامعة البصرة

keyan.alsibahi@uobasrah.edu.iq

keyanalsibahi@gmail.com

المستخلص

تم في هذا البحث تصميم نظام لاخفاء النصوص الإنكليزية في الصور الملونة كوسط ناقل لتأمينها بطريقة الاخفاء النقي واعتماد تشفير البيانات قبل اخفاءها باستخدام خوارزمية هيل لزيادة الامنية والحماية اذ استخدم مفتاح تشفير مكون من مصفوفة ٣×٣ لها معكوس يستخدم لفك التشفير وقد اختبر مقياس PSNR لحساب نسبة تشويش الاشارة وقد سجل نتائج مرضية تباينت اعتمادا على طول النص وحجم الصورة المخفي فيها ، في هذا البحث تم اعتماد لغة ماتلاب Matlab١٣ لبرمجة النظام .

●المقدمة

اصبح الانترنت البيئة الاكثر تعاملا في ربط الاشخاص ونقل المعلومات وازداد استخدامه في الاونه الاخيرة لسهوله العمل به وتوفره ،وبسبب كثرة المعلومات المخزونة في الاجهزة ووجود عدد كبير من الابواب المفتوحة للاختراق واستلال المعلومات والتلاعب بها سواء كانت فردية او لعدة مستخدمين اصبح الاهتمام بامنية المعلومات

وسريتها من الامور الضرورية جدا لحماية المستخدمين وخصوصياتهم فيُمكن تعريف أمنية المعلومات بأنها العمليات والطرائق التي يتم تطويرها وتوظيفها في حماية البيانات والمعلومات سواء كانت مطبوعة أم ألكترونية وكذلك حماية أنظمة المعلومات من الاختراق أو الوصول غير المخول أو غير الموثوق (Unauthorized Access)، أو كشف المعلومات، أو تزييفها ، أو تحويرها، أو تدميرها [١][٢][٣] .

كانت مسالة امنية البيانات ونقلها من الهواجس التي تهم الانسان قديما والى الان ففي العلم الحديث وبعد انتشار المعلومات واتاحتها بسهولة ظهر مبدأ ومفهوم امنية المعلومات الالكترونية وقدم المختصون بهذا الجانب عدة افكار منها التشفير والتضمين والكثير من المبتدئين لايميزون الفرق بينهما [٤]

اعتمد التشفير كطريقة ناجحة لحماية البيانات بتحويلها من شكلها المفهوم الى اخر غير مفهوم وبالتالي يصعب استرجاع المعلومة الاصلية الا بعمليات رياضية وحسابية تختلف درجة تعقيدها حسب الخوارزمية المقدمة في التشفير [٥] ومهما كانت طريقة التشفير ناجحة في تضليل المعلومة الاصلية وتشويهها كي لايحصل عليها العدو تبقى قدرة العدو ومحاولاته في فك شفرتها حتى عند ابتكار طرق جديدة للتشفير وذلك لكون وجود المعلومة المشوهة دليل على وجود معلومة مهمة فلذلك تم اللجوء الى طريقة اخرى وهي اخفاء الرسالة تماما عن المعترض داخل ملف اخر بريء المظهر وبالتالي تمر دون اعتراضها .

ان علم اخفاء الرسائل له جذور قديمة خصوصا في المراسلات الحربية والسياسية ويسمى حديثا بالكتابة المغطاة او التغطية Steganography ويمكن تعريفه على أنه علم وفن الاتصال بطريقة تخفي وجود هذا الاتصال اي نقل بيانات ضمن بيانات اخرى تسمى حامل host وهذا العلم يهتم بسريه الرسالة وتحقيق سرية الاتصال وعلى المستلم معرفة استخراج البيانات وتفسيرها [٦]

ونظام التغطية شأنه شأن أنظمة التشفير الأخرى تستلزم وجود خوارزميات وكلمات سر Keyword ويرجع السبب في استخدام كلمات السر إلى صعوبة الحفاظ على سرية الخوارزميات [٣شهد . ظهرت العديد من الدراسات في مجال امنية المعلومات بفرعيه التشفير والإخفاء حيث تم تطوير خوارزميات التشفير ودراستها وتطوير طرق لاختبار قوتها وقوة المفتاح المستخدم فيها ، حيث قدم ميلاد جادر سعيد (٢٠٠٩) بحثا قدم فيه طريقة جديدة في توليد المفتاح المستخدم في التشفير الانسيابي cipher stream ،إذ يولد المفتاح عشوائيا ومن ثم اخضاعه لشروط العشوائية المعتمدة فإذا كان مطابق يتم استخدامه للتشفير وإلا يتم توليد مفتاح جيني عشوائي باستخدام خوارزمية

جينية بطول النص المراد تشفيره كما وقدم هيكلية جديدة لإخفاء المفتاح المشفر ضمن النص وإضافة دالة تمويه بسيطة لزيادة سلامة المفتاح [٧].

وقد اقترح كل من محمد ابو طه،رضوان طهبوب(٢٠١١) نموذجا لإيجاد قيمة مبعثرة لمواجهة خطر هجوم القاموس وذلك عن طريق اضافة القيمة الملحية على البيانات باستخدام مولد الارقام العشوائية مما يجعل من الصعب اعداد قاموس من القيم المبعثرة .كما وقدم مقارنة بين النموذج المقترح وأنظمة ٥MD،١SHA،٥١٢SHA [٨].

في هذا البحث تم استخدام الصور الملونة كوسط ناقل لإخفاء النصوص العربية والإنكليزية بطريقة الاخفاء النقي واعتماد تشفير البيانات قبل اخفاءها باستخدام خوارزمية هيل لزيادة الامنية والحماية باعتماد لغة ماتلاب ١٣Matlab لبرمجة النظام .

●انظمة التشفير

طورت عدة خوارزميات للتشفير واستخدمت لحماية البيانات منها خوارزمية DES التي قدمت عام ١٩٧٧ بواسطة معهد .NIST حيث تقوم الخوارزمية بتشفير قالبا مكون من ٦٤ بتا بواسطة مفتاح طوله ٥٦ بتا وتعتبر من احد انواع التشفير الذي يسمى التشفير المقطعي والذي يقوم على مبدأ تقسيم المحتوى الاصلي (نصوص أو صور أو اي شيء آخر) إلى مجموعات متساوية الطول من البتات Blocks أو مقاطع ثم تشفير كل مقطع على حدة ومنها ايضا خوارزمية ٥MD وخوارزمية AES والتي استمر العمل بها وبتطويرها [٩] . وهناك نوعا اخر من التشفير يسمى التشفير الانسيابي Stream اذ يقوم على مبدأ تشفير البيانات المتصل أو جدول البيانات بشكل مستمر. حيث يتم توليد مفتاح مستمر يتم دمجه مع البيانات الأصلية بخوارزمية تشفير ذات مفتاح متماثل وغالبا يتم ذلك بعملية XOR المنطقية.ومن خوارزميات التشفير المتصل على سبيل المثال ٤RC التي تعد خوارزمية التشفير المتصل الأوسع انتشاراً [١٠].

بالاضافة الى انواع التشفير هناك تصنيف لعملية التشفير فالتشفير التماثلي يعتمد على استخدام مفتاح واحد في التشفير من طرف المرسل وفي فك التشفير من طرف المستقبل اما عمليات التشفير غير التماثلية فتعتمد على استخدام مفتاحين مختلفين في التشفير حيث يتم استخدام مفتاح عام للتشفير في طرف المرسل ومفتاح اخر خاص لفك التشفير في طرف المستقبل[١١] .

ومن أشهر خوارزميات التشفير التماثلية تقنية هيل والتي تعتمد على استخدام مفتاح التشفير على شكل مصفوفة ومعكوس هذا المفتوح لفك التشفير والمعكوس هنا ليس المعكوس العادي للمصفوفة وانما المعكوس نسبة الى أي رقم معين [١٢] تعتبر تقنية هيل من التقنيات الممتازة لاعتمادها على الجبر الخطي في الحسابات اضافة إلى السرعة العالية والانتاجية في[٨][١٣].

•نظام التغطية

يميل نظام التغطية او ما يسمى بنظام الاخفاء باتجاه إخفاء الرسائل في ملفات تكون حاملة لها مثل اخفاء ملف نصي او صوتي في ملف صورة وعادة يتم في البت الاقل اهمية LSB يسبب حدوث تغير بسيط جدا لا يمكن إدراكه في الصورة وبدو ن مقارنة مباشرة بين الصورة الأصلية والصورة الناتجة من الإخفاء وصعوبة اكتشاف التغيير[١٤] . يوجد ثلاثة انواع من الكتابة المغطاة والمعمول بها في انظمة الاخفاء وهي:

•الاخفاء النقي Steganography Pure

وهو نظام اخفاء معلومات لا يتطلب تبادل مسبق لمعلومات مثل مفتاح سري او كيفية افاء البيانات ضمن ملف الغطاء.

•الاخفاء بالمفتاح السري Steganography Key Secret

يعتمد على أستخدام مفتاح سري واحد في كِلا الطرفين، يختار المُرسل غطاء C ويضمن الرسالة السرية في C بأستخدام مفتاح سري K. أذا كان المفتاح المستخدم في عمليه التضمين هو معروف الى المُستلم فأنه يستطيع عكس العملية وأستخلاص الرسالة السرية.

•الاخفاء بالمفتاح العام Steganography Key Public .

هذه الآلية تتطلب استخدام مفتاحين واحد خاص والآخر عام المفتاح العام يخزن في قاعدة بيانات عامة ويستخدم في عملية الإخفاء ،أما المفتاح الخاص فيستخدم لاسترجاع الرسالة السرية ليس من الضروري أن يشترك شخصان بمفتاح سري [٢][١٥].

وقد ظهرت العديد من تقنيات الكتابة المخفية [١٦][١٧]منها :

•أنظمة التعويض System Substitution: اذ تعمل بمبدأ استبدال الاجزاء غير المهمة لملف الغطاء بثنائيات الرسالة المخفية في اماكن متتابعة او مبعثرة حسب الاتفاق بين المرسل والمستلم والتي عادة يصعب ادراكها من قبل المهاجم السلبي ومثال على ذلك طريقة شفرة Bit Signification Least

(LSB) فمن السهل أستخدامها نسبياً في الصورة و الصوت. كما يمكن أخفاء كمية كبيرة من المعلومات من دون أي أثر أدراكي لناقليها.

- تقنيات تحويل المجال Technique Domain Transform:

تقوم هذه الطريقة باخفاء الرسائل في اطياف الترددات لصورة الغطاء وتمنحها مناعة ضد هجمات التقطيع ومعالجة الصور مقارنة بتقنية LSB وهذه القوة تبقي الرسالة المخفية بعيدة عن ادراك المتطفلين ومن مجالات التحويل استخدام التحويل الجيبي المتقطع DCT والتحويل المويجي Wavelet

- تقنيات الطيف المنتشر Techniques Spectrum Spread:

في وسيلة الطيف تكون الاشارة بحزمة معينة تتجاوز الحد الادنى لارسال المعلومات ويتم نشر البيانات بحزمة مستقلة ويقوم المتلقي باستعادة البيانات باستخدام شفرة معينة استخدمت عند الارسال و يستخدم بشكل عام شكلان من الطيف المنتشر، الشكل ألأول هو التتابع المباشر(Sequence Direct)، والشكل ألأخر هو التنقل السريع والمفاجئ للترددات (Hopping Frequency).

- طرق أحصائيه Methods Statistical:

تعمل هذه الطرق على تغيير خصائص احصائية عديدة للغطاء اذ يتغير الغطاء عند ارسال البت ١ بينما لايتغير عند البت ٠ فعليه يجب ان يمتلك المتلقي القدرة على تمييز الغطاء المعدل من غيره .

- **النظام المقترح**

تم تطوير نظام يعمل على تشفير النص وتغييره من شكله المفهوم الى اخر مرمز ومن ثم القيام باخفاءه ضمن صورة رقمية لزياده امنية الرسالة المنقولة حيث يتكون النظام من اربع خطوات اساسية وهي ١)التشفير ٢) الاخفاء ٣) استرجاع النص ٤)فك التشفير.

٤ . ١ تشفير النص :

تم استخدام خوارزمية هيل في تشفير النص بالاعتماد على مفتاح سري يمثل مصفوفة ٣x٣ والتي تمتلك بدورها معكوس يستخدم في فك الشفرة ويكون المفتاح متفق عليه قبل عملية الارسال ، وتكون خطوات خوارزمية التشفير كالتالي :

- تحويل النص الى ارقام تمثل قيمة الرموز :

73] → text="I love Iraq." ٣٢ ١٠٨ ١١١ ١١٨ ١٠١ ٣٢ ٧٣ ١١٤ ٩٧ ١١٣

[٤٦

- تحويلها الى مصفوفة ثنائية الابعاد بعدد صفوف مساوٍ لبعد مصفوفة المفتاح .

text_n = 73 111 32 97

١١٣ ٧٣ ١١٨ ٣٢

١٠٨ ١٠١ ١١٤ ٤٦

- ضرب مصفوفة n_text بمصفوفة المفتاح بعد طرحها من العدد ٣٢ الذي يعتبر بداية الترميز للرموز الانكليزية (٣٢-١٢٦) ومن ثم اخذ ناتج القسمة الصحيح بعد تقسيمها على ٩٥ لتصبح بالمقدار من ٠-٩٤ بعدها اضافة العدد ٣٢ لاستخراج الرموز الصحيح:

key= ١ ٥ ٣

٢ ١١ ٨

٤ ٢٤ ٢١

new_code = 111 83 103 69

٥٧ ٧٣ ٩٤ ١٢٠

٨٢ ٦١ ٧٨ ٦٠

- تحول هذه المصفوفة الى احادية البعد وتحويلها الى مايقابلها من الرموز فيظهر النص المشفر بصيغته الغير مفهومة :

">encrypt_text = "o9RSI=g^NEx

- انتهى

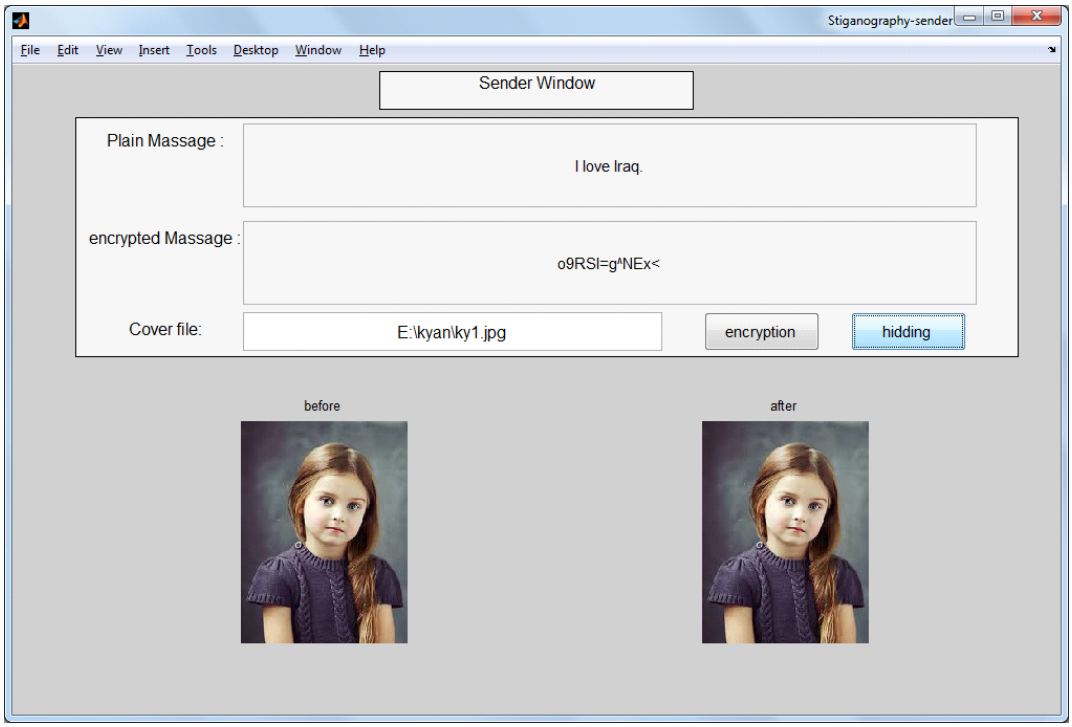
٤ . ٢ اخفاء النص

يتم اخفاء النص المشفر في الصورة الملونة بطريقة الاستبدال باستخدام البت الاقل اهمية لكل عنصر من عناصر الصورة LSB حيث تتراوح قيمته من ٠ الى ١ فعند اخفاء بت من النص فيه لن يتاثر اللون كثيرا في تلك

النقطة الا بمقدار ±١ وهي قيمة لونية طفيفة لا تدركها العين البشرية إذ يتراوح المقدار اللوني من ٠ الى ٢٥٥ فيكون تاثير تغير ١:٢٥٥ كافي لابعاد شك المهاجم بوجود نص مخفي في تلك الصورة ، ومما يزيد قوة الاخفاء هو ان النص مشفر وتكون خوارزمية الاخفاء كالتالي :

- يتم تحويل النص المشفر المطلوب اخفاءه الى شفرة الاسكي Ascii وكل رمز بطول ٧ بتات
- تحويل الصورة الى شفرة النظام الثنائي للاعداد وكل عدد بطول ٨ بت (٠-٢٥٥)
- تحديد طول النص وتحويله الى النظام الثنائي ايضا
- يتم خزن بتات النص بالتتابع في البت الثامن الاقل اهمية LSB.
- يتم خزن بتات طول النص في نهاية الصورة
- اعادة بناء الصورة بتحويلها الى الترميز العشرة ومن ثم بناء المصفوفة الثلاثية الابعاد التي تمثل المصفوفة الملونة.
- خزن الصورة بملف جديد وارسالها الى المستلم.
- انتهى

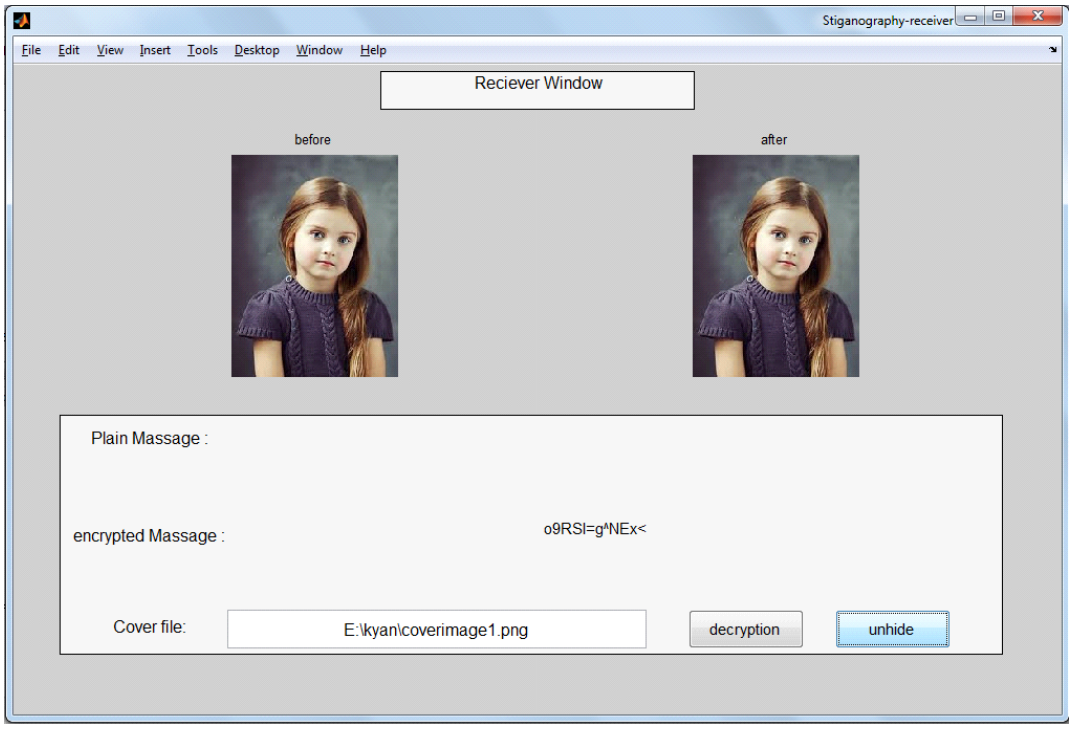
تكون واجهة النظام مصممة بالشكل (١)



شكل (١) واجهة النظام طرف المرسل حيث يقوم بتشفير النص واخفاءه وخزن الصورة الناتجة لغرض ارسالها مجددا

٤. ٣ استرجاع النص :

عند طرف المستلم بعد حصوله على الصورة يقوم بادخالها الى برنامج استخراج النص كما في الشكل (٢) :



شكل (٢) استخراج النص المشفر من الصورة واعتماد البتات الخيرة في تحديد طول النص المستخرج

حيث يتم استخراج النص عن طريق عكس عمليات الاخفاء السابقة بتحويل الصورة الى النظام الثنائي وخزن البت الثامن LSB من كل رمز في مصفوفة احادية البعد ومن ثم اخذ البتات الاخيرة من الصورة لتحديد طول النص المستخرج من الصورة لغرض اعادة بناء مصفوفة النص المشفر ويتم بعدها تحويلها الى النظام العشري واستخراج الرمز المقابل لكل رقم .

٤. ٤ فك التشفير

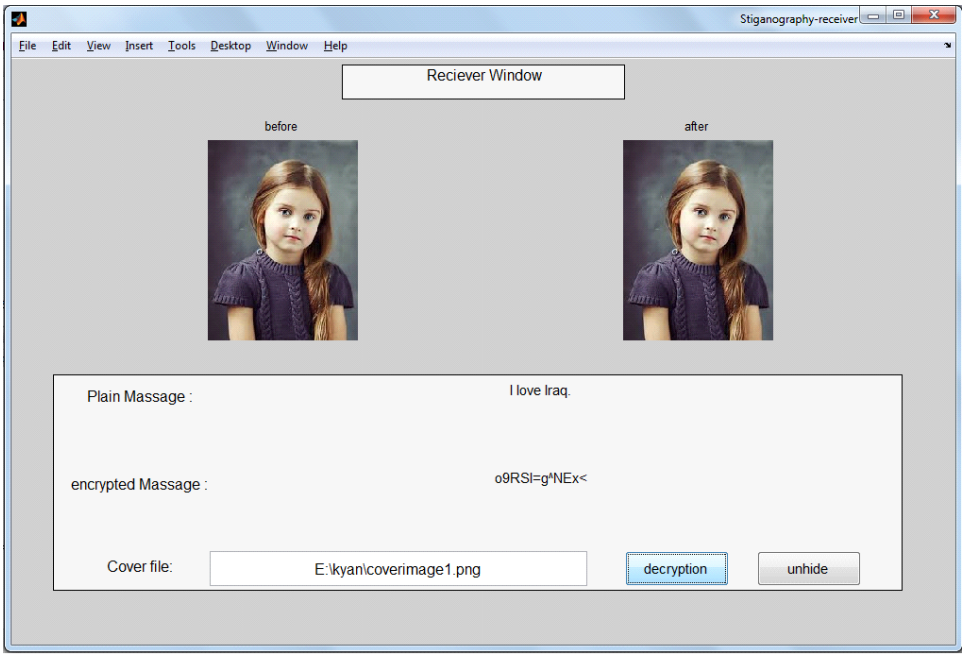
بعد استخراج النص المشفر يتم فك التشفير باعتماد معكوس مصفوفة المفتاح بطريقة عكسية لعملية التشفير وان الخطوة الاساس هو الضرب بمعكوس المصفوفة :

inv_Key= 39 −33 7

٢− ٩ ١٠−

١ ٤– ٤

حيث يتم تحويل النص الى شفرة الاسكي Ascii وتحجيمها بعدد صفوف مساوٍ لصفوف لاعمدة المفتاح ويتم طرح ال ٣٢ المضافة في خطوة التشفير من كل عنصر ومن ثم ضرب مصفوفة النص بمعكوس مصفوفة المفتاح وواخذ ناتج باقي القسمة على العدد ٩٥ واخيرا وليس اخرا اضافة العدد ٣٢ لاستخراج الرموز المقابلة والتي تمثل النص الصريح كما في الشكل (٣).



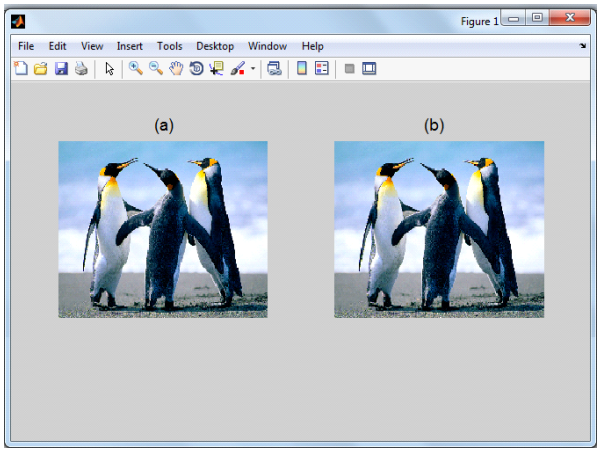
شكل (٣) استخراج النص الصريح من النص المشفر باستخدام معكوس مصفوفة المفتاح

•النتائج

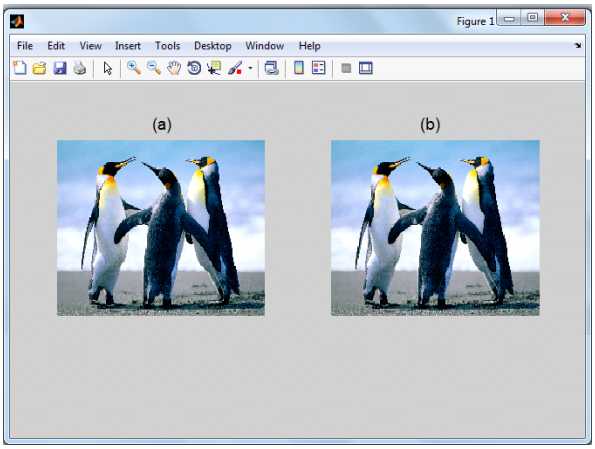
تم تطبيق البرنامج على العديد من الصور وكانت النتيجة صور واضحة وخالية من الضوضاء بالنسبة للعين البشرية ولم تظهر أي علامات على وجود نص مخفي و تم قياس مقياس الضوضاء Peak Signal to Noise ratio (PSNR) وهو يتضمن حساب مربع الخطأ والمعرف بالمعادلتين التاليتين [١٨]:

حيث ان N،M ابعاد صورة الغطاء و I صورة الغطاء قبل الاخفاء و IE هي الصورة بعد اخفاء الاشارة داخلها و L هي اعلى قيمة لبيانات الغطاء وفي حالة الصورة فهو ٢٥٥ .

وقد كانت قيمة PSNR اكبر من ٩١ عند الاخفاء بصور ملونة ذات الابعاد ٧٢٨x١٠٤٢ وتزداد قيمة الPSNR بزيادة حجم الصورة وتقل الى ٧١ بزيادة طول النص من ١٠٠ الى ٤٠٠ رمز بنفس حجم الصورة ثم تزداد بزيادة الحجم وفي الاشكال (٤)و(٥) تنفيذ البرنامج على صور ثابتة الحجم وطول نص متغير .



شكل (٤) (a) الصورة الاصلية بالابعاد ٧٢٨×١٠٢٤ (b) الصورة بعد اخفاء ملف نصي بطول ١٠٠ رمز



شكل (٥) (a) الصورة الاصلية بالابعاد ١٠٢٤×٧٢٨ (b) الصورة بعد اخفاء ملف نصي بطول ٤٠٠ رمز

٦. الاستنتاجات

- تزداد فرصة تمويه النص واخفاءه في الصورة كلما ازداد حجم الصورة وزادت دقتها بثبات طول النص وثبات ترميز القيم اللونية بـ٨bits فتزداد قيمة الـ PSNR وتقل قابلية العين المجردة في تمييز وجود نص مخفي لعدم تشوه الصورة .
- عند زيادة حجم النص تقل قيمة الـ PSNR بثبات حجم الصورة ومعدل الترميز ولكن يبقى المظهر الخارجي للصورة غير مشوه لتغيير البت الاقل اهمية والذي لا يحدث فرق واضح في اللون مع بقاء احتمالية تغيير بسيط قد يطرأ عليها .

٧. المصادر

- A. Tacticus، "**How to survive under siege / Aineias the Tac- tician**" ، pp. 84{90, 183{193. Clarendon ancient history series, Oxford, England: Clarendon Press, 1990, ISBN 0-19-814744-9, translated with introduction and commentary by David Whitehead.

- حسو، شهد عبد الرحمن ؛ عبد المجيد، ايلاف اسامة،"تطبيق نظام التغطية على الصور الملونة من نوع (BMP) " ،المؤتمر العلمي الاول لتقانة المعلومات –جامعة الموصل ٢٠٠٨ .
- الدبوني ،ميثم محمد زكي ؛ سليمان ،اديب حمدون ؛بدرسدخان،ستار ،"الرموز والشفرات والحاسبات مقدمة الى امن المعلومات "،الدار العربية للطباعة ،١٩٨٩.
- عوض،ود عقيل جواد ،"اخفاء الرسائل النصية في الوثائق النصية " رسالة ماجستير ،كلية العلوم–جامعة البصرة ،٢٠١٢.
- د. علاء و د. محمد علاء الحمامي، *أخفاء المعلومات – الكتابة المخفية والعلامة المائية*" ،الشارقة ، ٢٠٠٨.
- Arampatzis,Avi T.,"Data Hiding",report Katholieki University Nijmagen,School voor Informatica,Bedrijfsgerichte Informatica, 1999.
- سعيد؛ ميلاد جادر ،"التشفير الانسيابي باستخدام الخوارزمية الجينية " ، مجلة الرافدين لعلوم الحاسبات والرياضيات ،المجلد(٦) العدد (٣) ،٢٠٠٩.
- ابو طه ،محمد ؛ طهبوب، رضوان ،"خوارزمية البعثرة العملية ذات الاتجاه الواحد باستخدام مصفوفة لا معكوس لها اعتماداً على تقنية هيل للتشفير"، *Communications of the Arab Computer Society, Vol. 4 No.1, August, 2011.*
- Al-Turath "Chayed,Ahmed M.,"Development of AES with Permutation of DES University College Magazine,pp186-202.
- Lars R. Knudsen • Matthew J.B. Robshaw,"The Block Cipher Companion",Information Security and Cryptography ,Springer-Verlag ,Berlin Heidelberg ,2011.

- (William Stallings ,2006)، **" Cryptography and Network Security Principles and Practices"**، Prentice Hall.
- (Hill S. L, 1929) :**" Cryptography in an algebraic alphabet "** .American Math. Monthly, Vol (36), pp: 306-312.
- (Yi-Shiung. Y, and et al, 1991) :**A New Cryptosystem Using Matrix Transformation"** . Proceedings of IEEE International Canahan Conference on Security Technology, 1-3 – October – 2008, Taipei, Taiwan pp: 131-138.
- Iyenger ,Venugopal,"Hiding Messages in Image and text : Risk Associated with the Technology of Steganography "ISACA InfoBytes Journal,2003.
- Sellars , Duncan,1999,"An Introduction to Steganography " Computer Science Department ,University of Cape town South Africa,1999
- Katzenbeisser S., Petitcolas F.A.P.، **" Information hiding techniques for Steganography and digital watermarking"**،Arttech House,2000.
- د. عبد ألأمير خلف حسين، "***طرق التشفير للمبتدئين***" ، دار وائل للنشر، عمان، ٢٠١٠.
- Sander,William A.,2002;"Blind Consistency-&.Qi,Hairong ;Snyder,Wesley E Based Steganography for Information Hiding in Digital Media".Multimedia and Expo,2002.ICME '02.Proceedings 2002 IEEE International Conference on Vol.1,pp:585-588.

•الخلاصة باللغة الانجليزية

Introducing a texts hiding algorithm in colored photos depends on Hill Cryptography Technique to hide it in LSB of photo

In this paper, The new system designed to hide an English text in colored photos as a transmission media to secure it by pure hiding method and depend on encrypt the data before hide it by using Hill algorithm to increase the security and the protection, it uses a 3X3 matrix as a cryptography key and the reverse of the matrix to decrypt it , PSNR measurement used to check the signal interference and the results was good and follow the length of text and the size of the photo which used to hide the text in it, This system coded by using Matlab13.

●المصطلحات:

عربي	انجليزي
ية هيل للتشفير	*Hill cryptography algo*
قل	*Transmission m*
لاخفاء النقي	*Pure hiding m*
ة	
PSNR	PSNR measure