استخدام التغاير اللوني في إخفاء البيانات

ورقاء محمد هشام يوسف
مركز التحسس النائي
جامعة الموصل

سندس خليل إبراهيم
كلية علوم الحاسوب والرياضيات
علوم الحاسوب
جامعة الموصل

الاستلام **2011 / 09 / 27**
القبول **2012 / 01 / 08**

Abstract:

Hiding secret information and data in a cover such as audio, image, or video files makes the files unsuspicion for the an reader. So, this is the main reason for this research in the steganography field, comparing with encryption methods. The encrypt text pay the tracker to use various methods to break the encryption and get the original text. While the steganography draw no attention, and the reader may pass over it without doubt thus, the file and the hiding data stay without damage.

This paper presents a new method for hiding data in a text using color variance. In the recovery step, the text file of the covered message converted to digital image form, and image processing methods used to extract the hiding data from it. The proposed method applied on Arabic and English texts. Most types of attacking are applied in the messages. It shows a high efficiency versus all applied types of attacking. Matlab 2010a is used in programming the proposed method.

الملخص:

إن إخفاء المعلومات والبيانات السرية في غطاء مثل الملفات الصوتية أو الصور أو ملفات الفيديو يصعب على القارئ معرفة وجود شئ مخفي فيها, لذا يعد هذا سببا رئيسيا للبحث في مجال الكتابة المخفية مقارنة بطرق التشفير حيث إن الكتابة المشفرة أو المشوهة تدفع المتابع إلى الخوض بشتى الوسائل للحصول على المعلومة الأصلية ومحاولة كسر الشفرة في حين إن الكتابة المخفية لا تثير الشك عند المشاهد أو المتطفل وقد يمر عليها مرور الكرام دون أن يترك أثرا على المعلومة المخفية داخل الملف.

تم في هذا البحث عرض طريقة جديدة لإخفاء البيانات السرية في نص باستخدام التغاير اللوني, أما عملية فك الإخفاء فانه تم بتحويل الملف النصي للرسالة المخفية إلى صورة لاستخلاص الرسالة أو البيانات المخفية من الصورة الرقمية باستخدام طرق المعالجة الصورية الرقمية وقد تم تطبيق هذه الطريقة على الرسائل الانكليزية والعربية وتم تطبيق معظم أنواع الهجوم على الرسائل, وأظهرت الطريقة كفاءة في الإخفاء ضد كل أنواع الهجوم المطبقة, وتم برمجة الطريقة باستخدام Matlab 2010a.

1- المقدمة

نتيجة لتطور التقنيات الحديثة في الوقت الحاضر دخل الحاسوب في كل مجالات المجتمع ومنها مجال إرسال المعلومات التي تزداد بشكل هائل، فالمعلومات ترسل وتعالج أوتوماتيكيا على نطاق واسع، وهذا يتطلب الحرص على الخزن السري لنقل المعلومات[7].

لذا ظهرت الحاجة إلى إيجاد وسائل متعددة, لغرض إيصال المعلومات والبيانات بصورة صحيحة ومحمية من الجهات الغير مخولة لها بالاطلاع على هذه المعلومات[3]. فظهر علم التشفير (Cryptography) فهو العلم الذي يعنى بالطرق التي تجهزنا بحماية خزن المعلومات ونقلها في مجال واسع، وهذه الطرق تعتمد على مفتاح سري يستخدم لتشفير البيانات. وبالرغم من كونه طريقة جيدة لحفظ المعلومات إلا انه سهل الاكتشاف ويمكن لأي متطفل التلاعب به فكانت الحاجة إلى تقنية أكثر تطورا وأكثر سرية وحفاظا على المعلومات وخصوصا مع ظهور وتطور شبكة الانترنت فتم اللجوء إلى نظام التغطية [4], لان رؤية البيانات بصيغتها المشفرة تكفي لدفع المتطفل أو المهاجم إلى الاعتقاد بوجود بيانات مهمة أو حساسة تكمن في هذه العشوائية أو النص المشفر, فيبدأ باستخدام التقنيات المضادة للتشفير لمحاولة إيجاد محتواها, وحتى لو عجز عن تحقيق ذلك فانه قد يعبث بها أو يحرفها أو يستخدم بعض الوسائل المتاحة لمنع وصولها إلى هدفها [6].

بما أن مجتمع المعلوماتية يهتم في هذه الأيام أكثر وأكثر بأمنية المعلومات حيث أصبحت المعلومات مورد مهم يجب حمايته مثلما نحمي الأموال أو الأشياء الثمينة الخاصة الأخرى [5]. ومع النمو السريع لتقنيات الشبكات والاتصالات, فإن تقنيات إخفاء المعلومات أصبحت تستخدم بصورة واسعة لتحقيق أغراض متعددة منها حماية حقوق الطبع وتثبيت الملكية وتحقيق الاتصال بصورة سرية. فإخفاء المعلومات هو احد الوسائل المستخدمة لإيصال المعلومات بسرية إلى الجهات المقصودة بعيدا عن معرفة الجهات المضادة [1].

بما انه في الوقت الحاضر ازدادت أهمية إخفاء البيانات في نص أو في وسط رقمي (Digital Media) مثل الصورة أو الصوت وان بعض الحكومات قيدت خدمات التشفير

وازدادت الحاجة لإخفاء البيانات بطرق أخرى [7]. لذا جاءت فكرة البحث في إخفاء نص في نص أخر بطباعته باستخدام (Word) وباستخدام الصفات اللونية والتي لا تميزها العين في الكتابة كما ستوضح لاحقا في عملية الإخفاء ثم تحويلها إلى صورة ذات الامتداد BMP أو JPG لاستخلاص الرسالة المخفية من الصورة الرقمية في عمليات فك الإخفاء.

2- الدراسات السابقة Previous Studies

لا يعد إخفاء البيانات من المواضيع الجديدة في الوقت الحالي فقد قام العديد من الباحثين في السابق بالعمل في هذا المجال حيث تم إخفاء البيانات في وسائط متعددة كالنص والصورة والصوت والفيديو...الخ وحاول الباحثون إيجاد تقنيات إخفاء متطورة تواكب التطور السريع في تقنيات الإخفاء, سنستعرض هنا ما قدمه الباحثون في السنوات الخمسة الأخيرة.

في عام 2002 طبق الصميدعي نظام التغطية باستخدام تقنيات الإخفاء على ملفات الوسائط المتعددة نصاً وصورة وصوتاً وحصل على نتائج جيدة في الإخفاء في النص ونسب لا بأس بها في الإخفاء في الوسائط الأخرى, وإمكانية استخدام أي نوع من أنواع الكبس من دون ضياع بعد الإخفاء [6].

وكذلك قام أبو طبيخ وتوفيق بتصميم وتنفيذ تقنية جديدة ثنائية الشكل للحروف في النصوص المطبوعة للإخفاء المعلوماتي باستخدام الحاسوب وذلك عندما استخدم الطباعة الحاسوبية في توليد نصوص مطبوعة تخفي نصوصا" وبيانات أخرى لإيصالها بصورة فردية. ويمكن تنفيذ هذا النظام باستخدام وسائط الطباعة العادية كالصحف والمجلات [1].

ففي 2007 قدم Gutub و Fattani طريقة جديدة في إخفاء البيانات داخل نص مناسبةٍ للنصوصِ العربيةِ, ممكن أن تصنف تحت طرق ترميز الصفة (Feature Coding Methods) [9].

وفي 2008 قدم الحمامي دراسة عن تقنيات الإخفاء في النص وقسمها إلى طريقتين رئيستين وهما أولا ترميز المعلومات مباشرة في النص والطريقة الثانية ترميز المعلومات في شكل النص, واقترح طريقة للإخفاء في النص حيث اعتمد على استغلال الخواص الطبيعية لأشكال الحروف الانكليزية بدون تحوير الشكل الطبيعي للحرف وبالتالي الحصول على رسالة ذات شكل مقبول ومعنى واضح غير مثير لشك القارئ. وفي حالة استرداد الرسائل السرية (من جانب المستلم), فان نظام الاستلام يحتاج إلى وجود غطاء الرسالة فقط وهذا يزيد من سرية النظام المقترح إضافة إلى ذلك لا يحتاج المستلم إلى وجود القاموس الذي اعتمده المرسل في إخفاء الرسالة السرية مما يزيد من كفاءة النظام [2].

وفي 2009 اقترحت الباحثة البلاسيني نظام امني لإخفاء معلومات سرية وإرسالها بصورة مخفية عبر شبكات الاتصال، باستخدام تقنيتين من تقنيات إخفاء المعلومات، الأولى

الكتابة المغطاة (Steganography) ودمجها مع الشبكات العصبية لإخفاء المعلومات السرية بعد تشفيرها باستخدام تقنيات تشفير في صورة ملونة من نوع BMP باستخدام تقنية الكتابة المغطاة الهجينة وهي الإخفاء في الخلية الثنائية الأقل أهمية (LSB). أما التقنية الثانية فهي استخدام القنوات المخفية من نوع قناة الخزن المخفية (Covert Storage Channel) لإخفاء بيانات نصية أو صورة مخفية فيها بيانات سرية في بروتوكولات مختلفة [8].

وفي 2010 اقترح Mary طريقة جديدة لإخفاء البيانات في الوقت الحقيقي(real-time) باستخدام تدفق بت bit من الفيديو وتم في هذه الطريقة الربط بين الإخفاء في الفيديو, والصوت, والنص حيث استخدم طريقة لتشفير الرسالة ثم التحويل إلى DCT (Discrete Cosine Transform) كمعالجة أولية لتضمين البيانات وتم تنفيذ الخوارزمية المقترحة في المجال المكبوس لتلبية متطلبات الوقت الحقيقي دون الحاجة إلى فك الكبس في هذا المجال وبهذه الحالة سوف تنقل البيانات بسرية أكثر وتم تحسين الطريقة بحيث نحصل على فيديو بدون أن يحوي أي ضوضاء ظاهرة [11].

أما في 2011 فقد قام Mihaela بعمل مسح لتقنيات الإخفاء واستخداماتها وأنواعها وطرق الهجوم في عملية الإخفاء, حيث قام بدراسة احتمالية تراسل الخارجين عن القانون عبر الانترنت باستخدام الإخفاء وتوصل إلى أن التحقق من هذا الموضوع صعب جدا وذلك بسبب احتمال إن هذه المجموعات يستخدمون مواقع عامة أو خاصة للتراسل ليس بإمكان المحقق أن يتصفح جميع المواقع على الانترنت فضلا عن أن هناك طرق جديدة تظهر في الأسواق ممكن لهذه المجموعة استخدامها [12], حيث أن أكثر طرق الإخفاء نجاحا هي التي تكون غير اعتيادية بالرغم من بساطتها وأنها غير مطروقة سابقا مما يصعب على المحقق كشفها لأنها تحتاج إلى معرفة وخبرة سابقة.

3- مراحل الهجوم

يعد فهم تأثير تقنيات إخفاء البيانات على النواقل (carriers) أساسياً لكشف أو تعطيل الرسائل المخفية, ويكون المهاجم ناجحاً في الهجوم عند اكتشافه وجود الرسالة المخفية. إن الهجوم من قبل المتطفل على البيانات أو الرسالة المخفية يتكون من مرحلتان أساسيتان وهما [2,7]:

1- الاكتشاف (Detection).

المهاجم متأكد من وجود نص مخفي داخل الغطاء الحامل, وهذا الخلل غالبا ما يحدث لسببين [6]:

السبب الأول: إفشاء المرسل أو المستلم المتعمد أو غير المتعمد عن وجود الرسالة المخفية.
السبب الثاني: استخدام المهاجم أساليبه في التوصل للرسالة المخفية وهذه الوسائل هي:

1- سرقته للنظام أو لأحد أجزائه.
2- استخدامه لأساليب التحليل المتبعة لاكتشاف ذلك ومنها:

قياس معامل الضوضاء وذلك بحساب نسبة الضوضاء إلى الحجم الكلي للملف أو إدراك الإخفاء نتيجة لضعف نظام التغطية بحيث يبدو ذلك مدركا عند بعض الأجزاء, وغالبا ما يتم ذلك بالاستعانة بإحدى البرامج الخدمية التطبيقية [6].

2- فك الإخفاء, التشويش أو الإزالة (Extraction, Distortion or Removal).

الخطوات الأولى التي يقوم بها المهاجم عند تأكده من وجود نص مخفي هي استخدامه الوسائل الممكنة لفك ذلك الإخفاء واستخراج البيانات المخفية وإذا عجز عن ذلك قد يلجا إلى تحريفها أو التشويش بتغيير محتواها, إن هدف التشويش هو معالجة الناقل إلى درجة أن تتشوش الرسالة المخفية بحيث لا يمكن تمييزها. إن التشويش الناجح للرسالة يعني إن الرسالة عند استرجاعها تكون غير مقروءة بدون إحداث تغييرات محسوسة سريعة إلى النواقل أو يعمد حتى إلى منع وصولها إلى الهدف بحذف وإزالة جميع أو جزء من محتوياتها, إن هدف الإزالة هو منع الرسالة المخفية من الوصول إلى الجهة المرسلة إليها [2,6].

4- أنواع الهجوم

نظام الإخفاء غالبا ما يتعرض إلى أنواع عديدة من الهجوم على ملف الغطاء المرسل, كما هو الحال مع نظم التشفير, وقد تطرق لها الكثير من الباحثين وقام بتصنيفها حسب اعتبارات معينة وأعطيت تسميات مختلفة لأنواع الهجوم [3,6,10] وفيما يأتي أنواع الهجوم كما قدمها الباحث Mihaela في(2011) [12]:

1- معرفة الملف فقط (File Only)

المهاجم يعرف فقط الملف الغطاء الذي يحوي الرسالة السرية فقط , فيلجا المحلل هنا إلى الكثير من التحليلات الإحصائية لاكتشاف الرسالة السرية.

2- معرفة الملف والنسخة الأصلية (File and Original Copy)

المهاجم يعرف الملف الأصلي وكذلك الملف الذي يحوي الرسالة السرية, في هذه الحالة معرفة الرسالة السرية تكون سهلة جدا, حيث يتم مقارنة الملفين واستخراج الفرق الذي يمثل الرسالة السرية.

3- معرفة العديد من الملفات المشفرة (Multiple Encoded Files)

المهاجم يحصل على العديد من الملفات, وبنفس الغطاء مع عدة رسائل سرية مضمنة داخل ملفات الغطاء, هذا قَدْ يَحْدثُ خصوصاً في ملفِ يحوي العلامة المائية الرقمية **digital watermarking** والتي تستخدم لحماية حقوق الملكيةِ, لنفرض إن المهاجم حصل على نسخ متعددة من الكتاب الذي يحوي معلومات المستخدم المختلفةِ (ضمنَت كُلّ نسخة من الكتابِ بمعلومات حول المستخدم الذي أستلم النسخةَ), في هذه الحالةِ، من السهل على المهاجم أَنْ يَمْزجَ الملفاتَ سوية ويكون ملف هجين.

4- معرفة ملف الغطاء والخوارزمية المستخدمة (Access to File and Algorithm)

يعتبر من أكثر أنواع الهجوم خطورة بسبب كون الملف الغطاء معلوم وكذلك الخوارزمية المستخدمة لنظام التغطية, وهنا يقوم المهاجم بتطبيق الخوارزمية مباشرة لفك الإخفاء, لذا فالوصول للرسالة السرية يكون سهل جدا.

5- الهجوم الذي يحطم كل شئ (Destroy Everything Attack)

هذا النوع من أهداف الهجوم هو تحطيم الرسالة بالكامل والمهاجم قد لا يحاول حتى أن يسترجع الرسالة السرية.

6- هجوم اللف العشوائية (Random Tweaking Attack)

إضافة تغير بسيط على الملف بهدف جعل الرسالة المخفية غير صالحة للقراءة.

7- هجوم إضافة معلومات جديدة (Add New Information)

يعمد المهاجم إلى إضافة معلومات جديدة إلى الرسالة الأصلية , وفي بعض الأحيان يستخدم نفس البرمجيات التي استخدمها المرسل لكي يحاول التغير من معالم الرسالة.

8- هجوم إعادة صيغة (Reformat Attack)

هذا النوع من الهجوم يقوم بتحطيم المعلومات المخفية عن طريق تغيير صيغة أو شكل (Format) الملف الحامل للرسالة المخفية, حيث يترك هذا النوع من الهجوم الكثير من الأضرار على الرسالة المخفية.

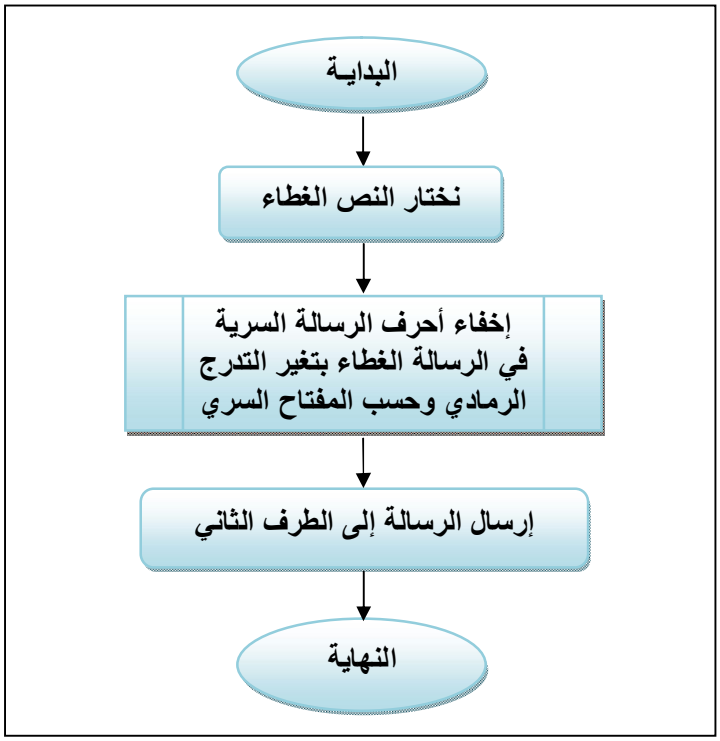
9- هجوم كبس الملف (Compression Attack)

المهاجم يقوم بكبس الملف مما يودي بالنتيجة إلى فقدان أو خسارة المعلومات المخفية داخل الرسالة الأصلية , لان خوارزميات الكبس تودي إلى مسح المعلومات الإضافية خلال عملية الكبس.

5- مراحل تنفيذ الطريقة المقترحة:

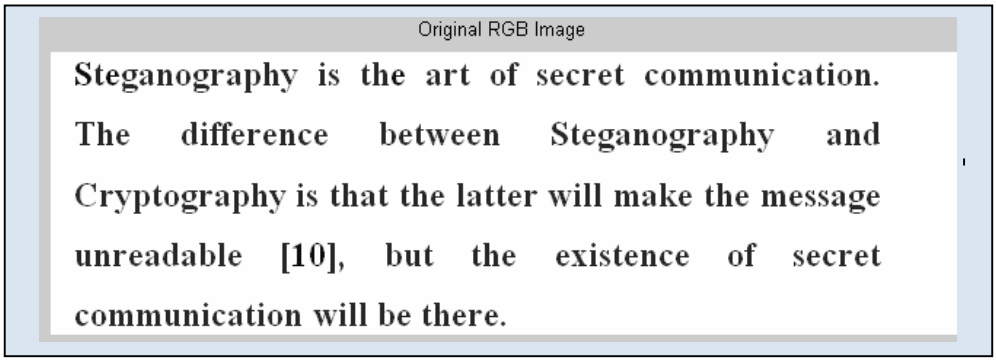
5-1 المرحلة الأولى

عملية الإخفاء: في هذه المرحلة سنبين خطوات عملية الإخفاء باستخدام التغاير اللوني, انظر المخطط في الشكل (1) وكما يأتي:



الشكل (1): المخطط الانسيابي لخطوات عملية الإخفاء

1- نختار نص معين يكون كغطاء للرسالة المخفية كما في الشكل (2), ثم يتم تحديد حجم ولون الخط للنص الأصلي.



الشكل (2): النص المستخدم كغطاء

1- نحدد نص الرسالة المخفية وليكن كمثال ("see 10") بأخذ حرف تلو الأخر نختار ما يقابله من الأحرف في الرسالة الغطاء وذلك بتغير التدرج اللوني للحرف, وهذا التدرج اللوني يحدد بالاتفاق على قيمته بين الطرفين (المرسل والمستلم) والذي يمثل المفتاح السري (Key Secret).

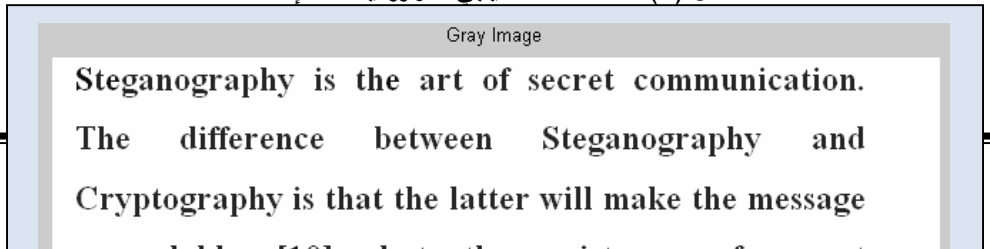
2- ترسل الرسالة إلى الطرف الثاني (المستلم).

2-5 المرحلة الثانية

عملية فك الإخفاء: في هذه العملية ستعرض خطوات الخوارزمية بشكل مفصل مع الأمثلة, انظر المخطط في الشكل (3).

1- تحويل الرسالة إلى صورة بامتداد BMP ملونة (أو (Gray) أي صورة ذات تدرج رمادي) والتي تحوي النص الأصلي كغطاء مع الرسالة المخفية, ثم قراءة الصورة لأخذ احد المستويات اللونية ولتكن الحزمة الثالثة (Blue) مثلا وكما موضح في الشكل (4).

الشكل (3): المخطط الانسيابي لخوارزمية فك الإخفاء



الشكل (4): النص المستخدم كغطاء مع الرسالة المخفية

حيث نلاحظ إن الرسالة السرية المضمنة في الرسالة الغطاء لا يمكن تمييزها بالعين المجردة ولم يدع أي شك للمهاجم بوجود إخفاء في هذه الرسالة.

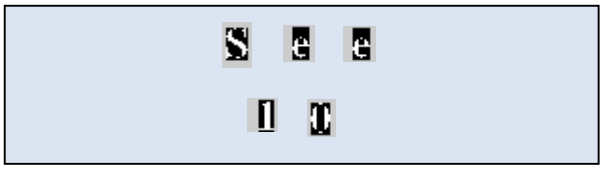
2- بالاعتماد على المفتاح السري أي قيمة حد العتبة نستخلص حروف الرسالة السرية من الرسالة الغطاء الشكل (5).

3- تقطيع الصورة أفقيا (وكما سيوضح في فقرة التقطيع الأفقي لاحقا) إلى شرائح من الصورة الأصلية كما في الشكل (6) حيث تضم كل شريحة أحرف متفرقة من الرسالة المخفية والتي تكون على سطر واحد.

الشكل (6): التقطيع الأفقي

4- قطع صورة الشريحة الأفقية إلى شرائح عمودية تضم كل شريحة حرف واحد فقط كما في الشكل (7), وكما سيوضح في فقرة التقطيع العمودي لاحقا.

5- تكرر الخطوة (4) على كل الشرائح الأفقية.



الشكل (7): التقطيع العمودي

بهذه الطريقة تم الحصول على كل أحرف الرسالة المخفية بشكل صور متفرقة.

6- يتم تنسيق وربط حروف الرسالة السرية بحيث تظهر كرسالة واضحة أمام المحلل كما في الشكل (8) الذي يبين مراحل ربط الحروف مع بعضها.

الشكل (8): تنسيق حروف الرسالة السرية وربطها مع بعضها

7- عرض صورة الرسالة السرية كما في الشكل (9).

الشكل (9): صورة الرسالة السرية

5-3 التقطيع الأفقي

تتمثل خوارزمية التقطيع الأفقي كما يأتي, انظر المخطط في الشكل (10).

1- تقطيع صورة الرسالة السرية إلى شرائح من صور الأسطر ويتم ذلك باستخدام الإيعاز

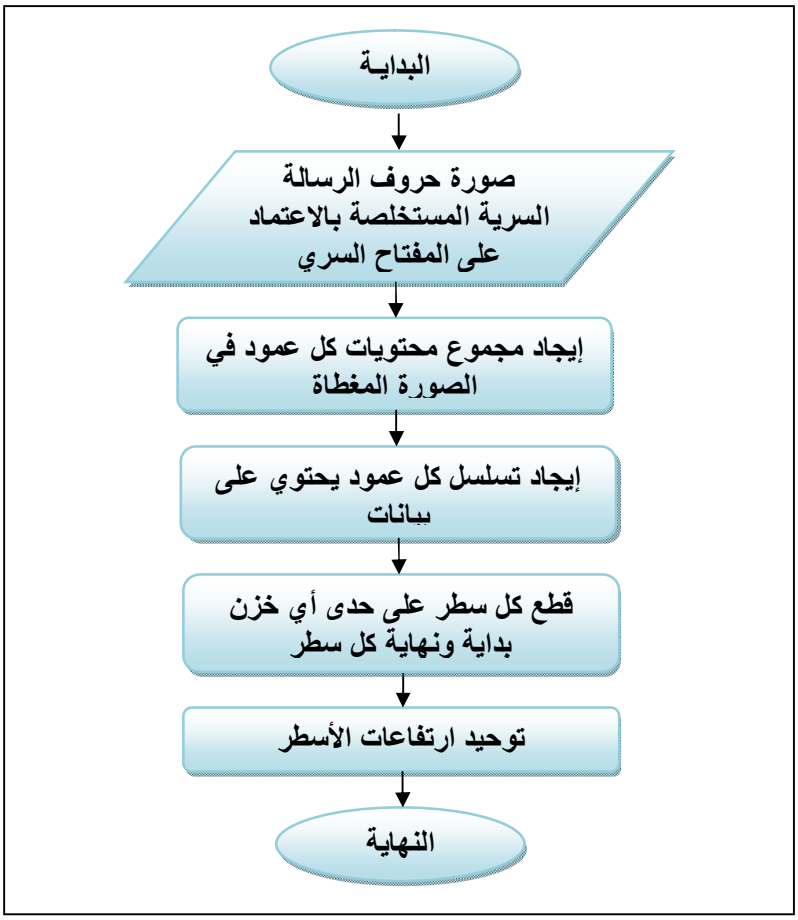
S = sum (II)

الذي يعطي مجموع كل عمود حيث إن العمود الذي لا يحتوي على نقاط الحروف سيكون مجموعه (0). وعليه يجب تدوير الصورة (90°) للحصول على مجموع النقاط في الأسطر.

إيجاد تسلسل الأعمدة (الأسطر بعد التدوير) التي تحوي على نقاط الأحرف للرسالة السرية (أي التي مجموعها اكبر من الصفر) كما في المقطع البرمجي الآتي حيث يحتوي المتجه

(indexes) على تسلسل الأعمدة التي فيها نقاط الحروف, ويمثل المتغير II مصفوفة بيانات الصورة, ويمثل S المصفوفة التي تحتوي مجاميع الأعمدة.

```
S=sum(II);
[row col] = size(II);
i=1;
for j=1:col
   if (S(j)>0)
      indexes(i)=j;
      i=i+1;
   end
end
```



الشكل (10): مخطط انسيابي لمراحل تنفيذ التقطيع الأفقي

2- يتم قطع كل سطر من أحرف الرسالة (وهي عبارة عن مجموعة من الأعمدة في البرنامج) على حدى بالاعتماد على المتجه (indexes) الناتج من الخطوة السابقة وذلك بخزن بداية ونهاية كل سطر من صورة الرسالة السرية في كل من المصفوفات BeginRow, EndRow على التوالي, كما في المقطع البرمجي الآتي:

```
i=1;
BeginRow(1)=indexes(1);
for j=2:length(indexes)
   if (indexes(j)-indexes(j-1) >2)
      EndRow (i)=indexes(j-1);
      i=i+1;
      BeginRow (i)= indexes(j);
   end
end
 EndRow (i)=indexes(j);
```

3- يتم في هذه الخطوة توحيد ارتفاعات الأسطر للاستفادة منها في الخطوة التي تليها وكما يأتي:

أ- حساب ارتفاع كل سطر على حدى واخذ اكبر قيمة بينها وحسب المقطع البرمجي الآتي:

```
mrows=max( EndRow-BeginRow)+1;
```

حيث تضم (BeginRow) تسلسل بداية كل الأسطر بينما تضم (EndRow) تسلسل نهاية كل الأسطر و(mrows) بعد تنفيذ الإيعاز السابق ستحتوي على اكبر ارتفاع من بين الأسطر.

ب- يتم في هذه الخطوة توحيد ارتفاع الأسطر وجعلها مساوية لقيمة mrows الذي يمثل أعلى ارتفاع للسطر في الصورة وكما يأتي:

الخطوة الأولى: نحدد تسلسل السطر (i).

الخطوة الثانية: نحسب الفرق بين بداية ونهاية السطر الواحد الممثل بالمتغير(D) للحصول على ارتفاع ذلك السطر في الصورة.

الخطوة الثالثة: حساب الفرق بين ارتفاع السطر الحالي (D) وأعلى ارتفاع الممثل بالمتغير (mrows) مقسوما على 2 والحصول على قيمة E, التي تمثل نصف قيمة الفرق المضافة إلى الارتفاع. حيث ستضاف قيمة E إلى أعلى والى أسفل الصورة وذلك لكي يبقى الحرف في وسط الصورة, انظر المقطع البرمجي الآتي:

```
for i=1: length( EndRow)
   D=EndRow(i)-BeginRow(i);
   E= (mrows - D)/2;
   if  (D < mrows)
      EndRow(i)=EndRow(i) + E;
      BeginRow(i)=BeginRow(i)-E;
   end
end
```

5-4 التقطيع العمودي

تتمثل خوارزمية التقطيع العمودي كما يأتي, انظر المخطط في الشكل (11).

1- تعاد الخطوة (1-3) من فقرة التقطيع الأفقي وذلك بتطبيقها على شريحة من صورة سطر من الرسالة السرية وذلك للحصول على بداية ونهاية كل حرف من حروف صورة السطر الواحد, ممثلة بالمصفوفة BeginCol, EndCol على التوالي.

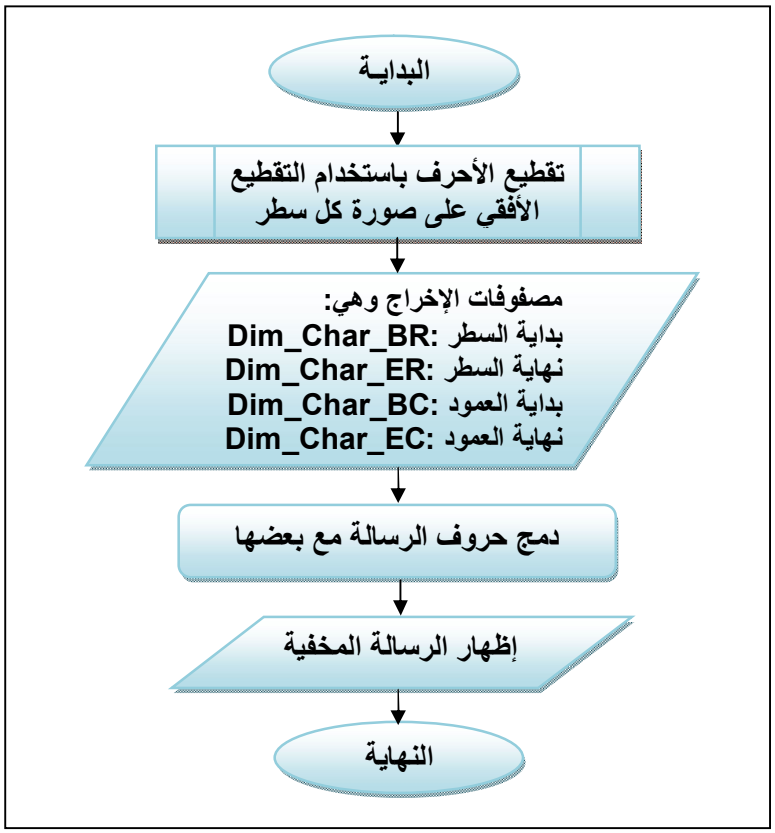
2- بعد تنفيذ خطوات التقطيع الأفقي على شريحة من صورة سنحصل على مصفوفات Dim_Char_ EC,Dim_Char_ BC,Dim_Char_ER,Dim_Char_BR تضم كل منها وعلى التوالي تسلسل بداية ونهاية السطر وتسلسل بداية ونهاية العمود لكل حرف وكما موضح في المقطع البرمجي الآتي:

```
for Cj=1: length( EndCol)
    Dim_Char_BR(n)= BeginRow(Rj);
    Dim_Char_ER(n)= EndRow(Rj);
    Dim_Char_BC(n)= BeginCol(Cj);
    Dim_Char_EC(n)= EndCol(Cj);
end
```

3- يتم دمج صور الأحرف مع بعضها باستخدام الإيعاز horzcat وكما في المقطع البرمجي الآتي:

```
  Result=II( Dim_Char_BR(1): Dim_Char_ER(1), Dim_Char_BC(1):Dim_Char_EC(1));
for m=2:NoOfChar
  B=II( Dim_Char_BR(m): Dim_Char_ER(m), Dim_Char_BC(m):Dim_Char_EC(m));
  Result = horzcat(Result,B);
  figure;
  imshow(Result);
end
```

حيث يمثل (NoOfChar) عدد الأحرف في الرسالة السرية, وتمثل B صورة الحرف المقتطع من المصفوفة II التي تمثل مصفوفة بيانات الرسالة السرية المستخلصة.



الشكل (11): المخطط الانسيابي لخطوات التقطيع العمودي

6- مثال تطبيقي:

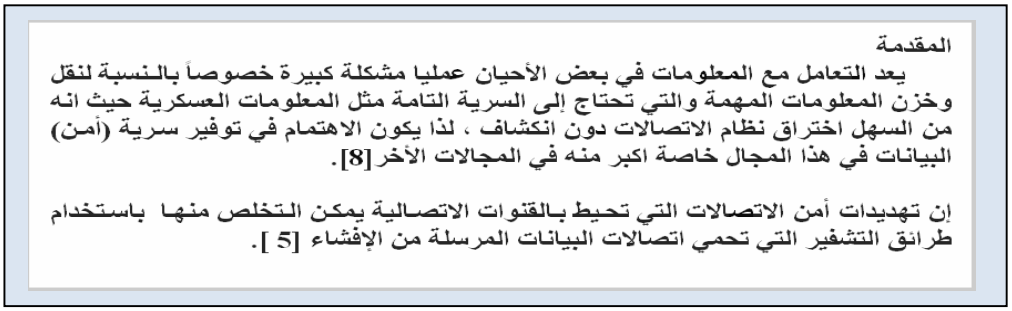
تم تطبيق الطريقة المقترحة على الرسالة باللغة العربية, وكما في المثال الآتي:

أ- المرحلة الأولى: الإخفاء

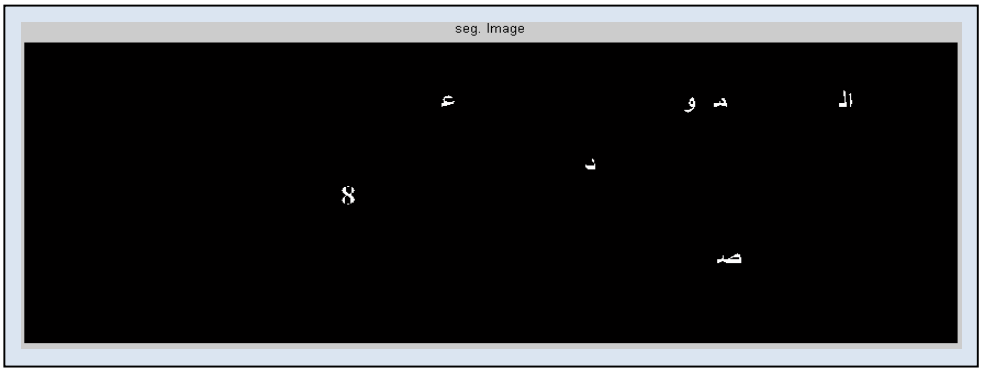
1. نختار نصاً معيناً يكون كغطاء للرسالة المخفية كما في الشكل (12), ثم نحدد نص الرسالة المخفية "الموعد 8 ص".

ب- المرحلة الثانية: فك الإخفاء

1. تحويل الرسالة إلى صورة بامتداد BMP ملونة وذلك بأخذ المستوى اللوني الأزرق كما موضح في الشكل (13).



2. نستخلص حروف الرسالة بالاعتماد على المفتاح السري انظر الشكل (14) الذي يظهر حروف الرسالة السرية.



الشكل (14): حروف الرسالة السرية المستخلصة من الرسالة الغطاء

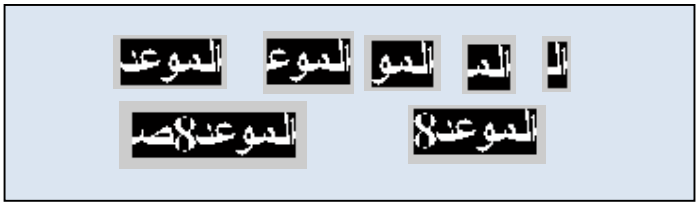
3. التقطيع الأفقي للصورة كما في الشكل (15).

الشكل (15): التقطيع الأفقي

4. الصور الناتجة بعد عملية التقطيع العمودي موضحة بالشكل (16).

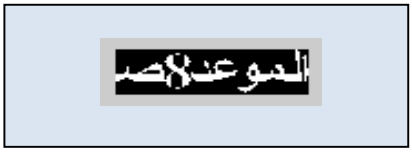
الشكل (16): التقطيع العمودي

5. والشكل (17) يوضح مراحل ربط حروف الرسالة السرية مع بعضها.



الشكل (17): تنسيق حروف الرسالة السرية

6. الشكل (18) يوضح صورة الرسالة السرية.



الشكل (18): صورة الرسالة السرية

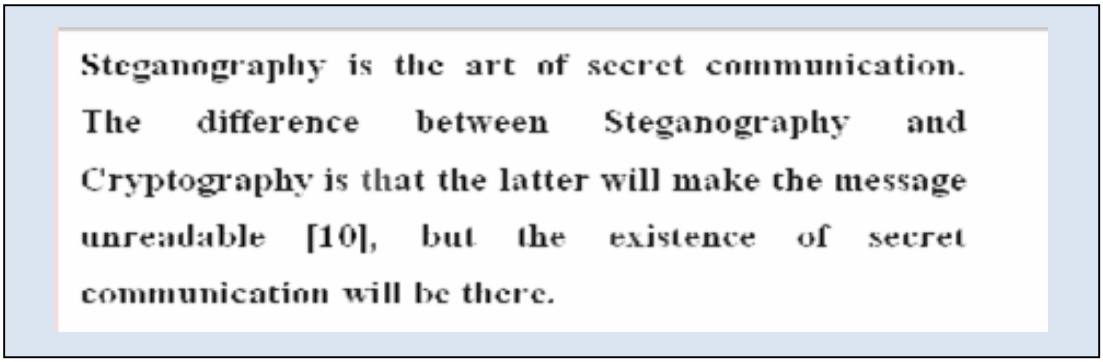
7- عرض النتائج ومناقشتها

سنناقش في هذه الفقرة أهم النتائج التي توصل إليها البحث وكما يأتي:

1- إن إخفاء نص في نص أخر بهذه الطريقة وإرساله كوثيقة Document وان النص الغطاء يكون بموضوع عادي جدا دون اختيار للجمل سيزيل الشك لأنه سوف لن يخمن

المهاجم وجود نص مخفي في الملف مما يزيد من أمنية ومتانة الطريقة رغم بساطتها, وبذلك تقل أو تنعدم إمكانية الهجوم على هذا الملف.

2- إن استخدام أكثر من تدريجيين من اللون في إخفاء الرسالة السرية يزيل الشك ويصعب معها التمييز فيما إذا كانت الرسالة قد ضمنت بيانات أم لا وبذلك يصعب على المهاجم عملية كسر الشفرة انظر الشكل (19), في هذا الشكل تم استخدام أربع تدرجات لونية ولم يلاحظ أي تغيير ظاهري على الشكل العام للرسالة.



الشكل (19): صورة الرسالة الغطاء بأربع تدرجات لونية

3- في الشكل (20) نلاحظ إن الرسالة السرية لم تتأثر بهذه التدرجات لأننا نعتمد على المفتاح السري الذي يمثل التدرج اللوني.

الشكل (20): الرسالة السرية

4- هنالك عشوائية جزئية في إخفاء الحروف في كلمات نص الغطاء. حيث لا نتحدد بأول حرف تصادفه من الرسالة الغطاء فمثلا لإخفاء كلمة the في نص الغطاء

We explore Steganographic and Cryptographic algorithms and techniques throughout the word ……

فيمكن اختيار الحرف t من الكلمة S**t**eganographic والحرف h من كلمة Cryptograp**h**ic بالرغم من وجود الحرف h في الكلمة Steganographic والحرف e من كلمة the يخفى في الحرف e الثاني من كلمة techniqu**e**s رغم وجود حرف e في بداية هذه الكلمة, هذا يزيد من العشوائية المتتابعة في اختيار حروف الرسالة بحيث يصعب عملية الهجوم. أي ليس هنالك شروط لاختيار أحرف الرسالة السرية المقابلة لأحرف الرسالة الغطاء.

5- إن طريقة فك الإخفاء هي ليست طريقة معاكسة لعملية الإخفاء, حيث إن عملية الإخفاء هي إخفاء نص في نص باستخدام التلوين, أي يكون الإدخال نص والإخراج نص أيضا, أما عملية فك الإخفاء من قبل المستلم سيكون الإدخال عبارة عن صورة والإخراج عبارة عن صورة أيضا تحتوي النص المخفي.

6- إن طريقة فك الإخفاء تكون بالاعتماد على برنامج يتم برمجته لإظهار الحروف بالاعتماد على المفتاح السري الذي يكون متوفر لدى المستلم ليستطيع فك الإخفاء.
ففي حالة أن المهاجم حصل على خوارزمية الإخفاء فانه سيحتاج إلى وقت لعمل خوارزمية فك الإخفاء واكتشاف المفتاح السري مما يزيد من الوقت اللازم لكسر الإخفاء ويزيد من أمنية الطريقة.

7- إذا علم المتطفل الخوارزمية المطبقة لإخفاء النص ولم يحصل على المفتاح, فان ذلك لا يوثر كثيرا لأنه سيحتاج إلى عدة احتمالات لتجربة الألوان مرة على النص الغطاء ومرة أخرى على الرسالة السرية. وهل إن عملية الإخفاء تمت على الحروف أم على الكلمات مما يزيد من الوقت اللازم لكسر الإخفاء وبذلك يزيد من أمنية الطريقة.

8- بالمقارنة مع طريقة إخفاء حروف معينة في الكلمات, كالإخفاء في الحرف الأول من الكلمة الأولى والحرف الثاني من الكلمة الثانية وهكذا أو الإخفاء في الحروف الأولى من الكلمات في النص الغطاء [6,9], فان الطريقة المقترحة تستوعب كمية اكبر من البيانات (الحروف) المضمنة لأنه قد نختار من الكلمة الواحدة حرف واحد أو حرفين أو ثلاثة أو يمكن أن يختار مقطع من كلمة كذلك يمكن أن نختار كلمة كاملة.

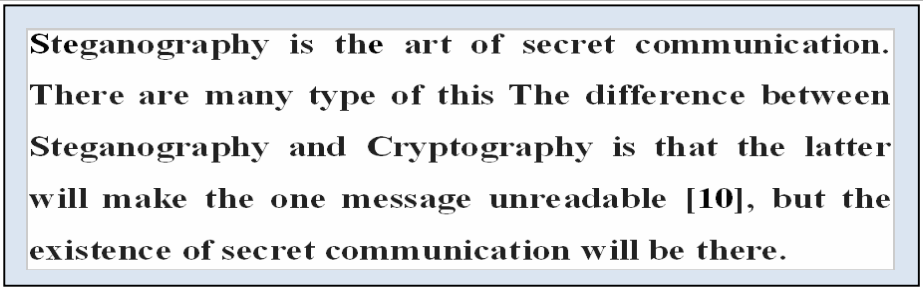
8- التحويرات التي يمكن أن تتعرض لها الرسالة

إذا عجز المهاجم عن فك الإخفاء فإنه قد يلجأ إلى تحريف أو تغيير محتوى الرسالة أو يمنع وصولها إلى الهدف بحذف جزء أو كل محتواها ومن هذه التغيرات وتأثيرها على الرسالة المخفية بالطريقة المقترحة:

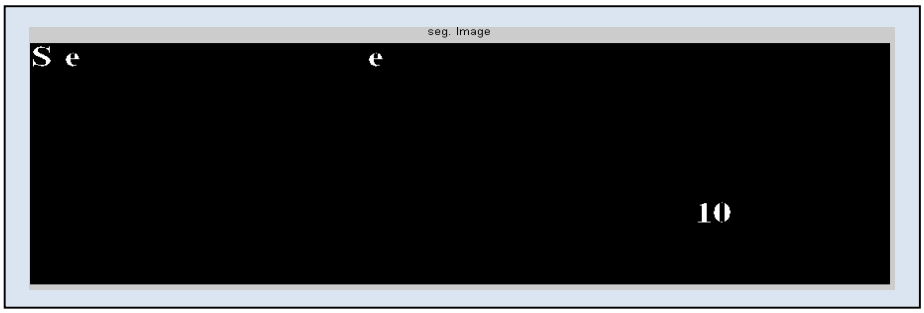
1- إضافة نص إلى نص الغطاء, فهذا لن يوثر نهائيا على الرسالة السرية, لأنه سيأخذ الصفة اللونية نفسها لكلمات الغطاء وبذلك سيبدو عند فك الرسالة كفراغات أضيفت للرسالة كما هو موضح بالشكل (21) والشكل (22) والشكل (23) والشكل (24).

Steganography is the art of secret communication. The difference between Steganography and Cryptography is that the latter will make the message unreadable [10], but the existence of secret communication will be there.

الشكل (21): صورة الرسالة الغطاء



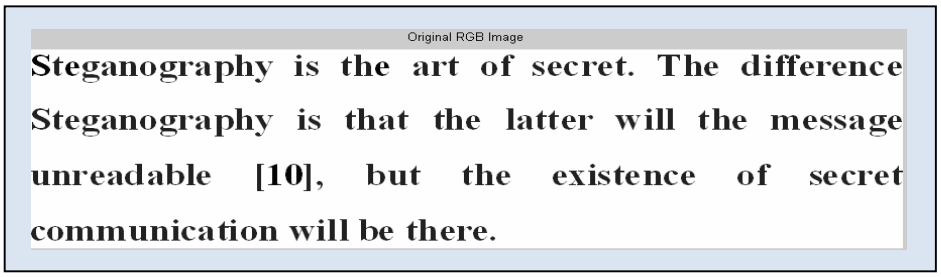
الشكل (22): النص الغطاء بعد إضافة نص



الشكل (23): حروف الرسالة السرية المقتطعة

الشكل (24): الرسالة السرية

2- حذف جزء من النص وليس فيه جزء من أحرف الرسالة السرية فإنه لن يوثر في الرسالة السرية كما هو موضح بالشكل (25) والشكل (26) والشكل (27).

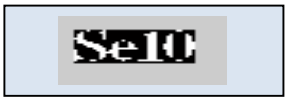


الشكل (25): النص الغطاء بعد حذف جزء منه

الشكل (26): حروف الرسالة السرية المقتطعة

الشكل (27): الرسالة السرية

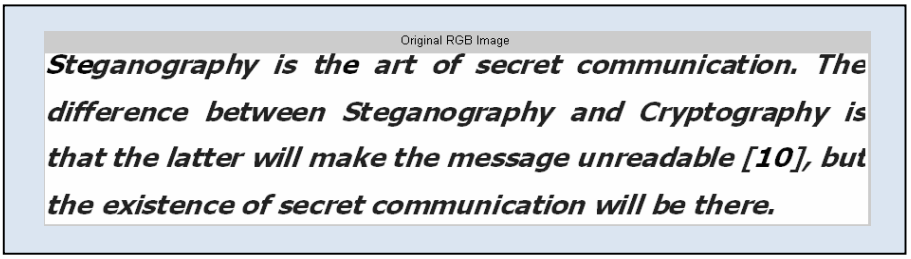
3- في حالة حذف جزء من النص يحتوي على بعض أحرف الرسالة السرية, فإنه سيوثر في النتيجة بمقدار معين الذي يؤدي إلى تنبو الطرف المستلم إلى أن الرسالة قد تعرضت للهجوم وقد اجري عليه تغييرات كما هو موضح بالشكل (28).



الشكل (28): حذف جزء من الرسالة السرية لتعرضها لهجوم

4- إن التحوير بالخصائص العامة للخط:

أ- تغيير نوع أو حجم الخط أو جعله غامق أو مائل أو وضع خط تحت الحروف لن يوثر في الرسالة نهائيا وكما موضح بالشكل (29) والشكل (30).

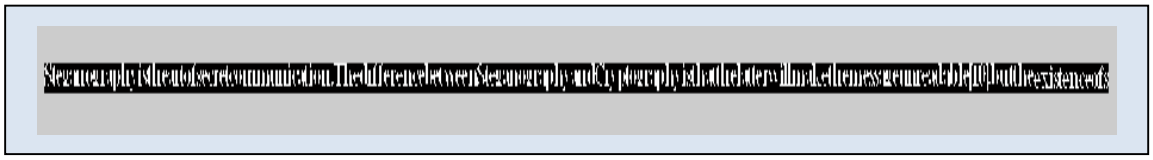


الشكل (29): النص الغطاء بعد تكبير حجم الخط وجعله مائلاً

الشكل (30): الرسالة السرية

ب- تغيير لون الخط: في هذه الحالة لن يستطيع محلل الشفرة (المستلم) الحصول على الرسالة السرية.

وبذلك سيعلم أن الرسالة المستلمة قد تعرضت لنوع من الهجوم وتم تغييرها كما هو موضح بالشكل (31).



الشكل (31): الرسالة السرية بعد تعرضها لنوع من الهجوم

(تغيير لون حروف الرسالة الغطاء كلها)

9- مناقشة سرية الطريقة وكفاءتها

أما من حيث مناقشة الطريقة المقترحة لفرضية أسوا الاحتمالات:

1- في حالة معرفة ملف الغطاء والخوارزمية, فإن سرية الرسالة وأمنيتها تكمن في المفتاح السري, إذ أن أمام المهاجم 256 قيمة لونية فضلا" عن توفر ثلاثة مستويات لونية, عليه ستكون عدد الاحتمالات $(256)^3$ وتساوي (16,777,216) احتمال لإيجاد قيمة المفتاح السري مما يوثر في الوقت اللازم لكسر الرسالة.

2- في حالة معرفة الغطاء دون معرفة الخوارزمية فان السرية تكون في أن المهاجم لا يستطيع أن يخمن وجود رسالة مخفية بواسطة العين, هذا من ناحية ولا يخطر بباله طريقة الإخفاء لبساطتها وكذلك قيمة الحد (المفتاح) من ناحية أخرى.

3- عند توفر ملف الغطاء مع توفر نسخة الرسالة الأصلية فان تحليل الملف الحامل للرسالة لا يكون بهذه السهولة فلا يوجد تغيير في الشكل العام الخارجي الظاهر للعين ولا يستطيع أن يخمن الخوارزمية بسهولة رغم بساطتها لأنه سيحتاج أن يعلم أيضا المفتاح وليس من السهل تطبيق برامجيات جاهزة إذ لا تستطيع البرامجيات الجاهزة أن تعطي القيمة اللونية لكل حرف في الرسالة المكتوبة بالبرنامج الخدمي.Word

4- أما في حالة عدم توفر ملف الغطاء والخوارزمية, أي فقط يعلم بوجود رسالة سرية فانه لا يستطيع تخمين أي من الرسائل المتوفرة لديه تحتوي الرسالة المخفية, لذا قد يلجا المتطفل إلى قياس معامل الضوضاء, وذلك بالاستعانة بإحدى البرامج الخدمية التطبيقية وهذا لا يوثر في هذه الطريقة وذلك لصعوبة تخمين الخوارزمية لبساطتها ولا يستطيع الحصول على المفتاح المستخدم إلا بالتجربة والخطأ مما يستغرق وقت في ذلك.

5- في حالة الهجوم العشوائي سيحاول المتطفل تدمير كل شئ وبالتالي سيودى ذلك إلى عدم وصول الرسالة المخفية إلى الطرف الثاني (المستلم) في الوقت المناسب وعليه سيعلم المستلم إن هنالك تطفل قد حصل ويقوم باتخاذ الإجراء المناسب.

6- في حالة شك المتطفل بوجود رسالة سرية فانه قد يلجا إلى تغيير صيغة الملفات وان ذلك لا يوثر على هذه الطريقة وذلك لان الطرف المستلم يعلم نوع صيغة الرسالة التي سيستلمها, لذا يستطيع أن يعيدها إلى صيغتها الحقيقية دون تغيير.

7- إن إجراء كبس على الرسالة المستلمة سيودى إلى معرفة الطرف الثاني (المستلم) بوجود تلاعب وتطفل على الرسالة وهذا لا يوثر على هذه الطريقة لأنه في جميع الأحوال فان المتطفل لم يستطيع قراءة الرسالة.

10- الاستنتاجات Conclusions

1- إن الإخفاء بهذه الطريقة سوف لن يوثر على الغطاء حيث انه لن يبدو مشوها ولا يحوي أي تغييرات ملحوظة وان البيانات ستبقى سليمة ولها قابلية الاستعادة.
2- إن طرائق الكتابة المغطاة في النص تحتاج لاختيار نص الغطاء بحيث يضم الكلمات أو الحروف أو الرموز المناسبة لعملية الإخفاء, أما بالنسبة للطريقة المقترحة في البحث فيمكن استخدام أي نص كغطاء وفي أي مجال. أي ليس هناك شروط لاختيار النص الغطاء.

مثلا لإخفاء نص في نص باستخدام الحرف الثاني من كل كلمة في الرسالة الغطاء, هذا يستدعي وجوب اختيار الكلمات في النص الغطاء بحيث يحتوي الحرف الثاني من كل كلمة فيها على حروف الرسالة السرية وبشكل متسلسل. أما الطريقة المقترحة فإنها لن تحدد المرسل بأي موقع للحرف وان عملية اختيار حروف الرسالة السرية في الرسالة الغطاء تكون غير محددة بتسلسل معين للحرف في الكلمة أو موقع معين للكلمة في الرسالة.

3- بما إن عملية فك الإخفاء هي ليست معاكسة لعملية الإخفاء, ففي حالة توفر احدهما (عملية الإخفاء مثلا) لدى المهاجم سوف لا يستطيع بوقت قياسي أن يكَون برنامج لعملية فك الإخفاء.
4- تغيير حجم النص في عملية الإخفاء لا يوثر في عملية فك الإخفاء.
5- بما إن سرية الطريقة تكمن في المفتاح السري (حد العتبة) وان عملية الإخفاء تختلف كليا عن عملية فك الإخفاء, لذا تندرج هذه الطريقة تحت تقنيات الكتابة المغطاة ذات المفتاح السري.
6- إن تغيير صيغة الملف من Doc أو Docx إلى صيغة أخرى كالـ PDF مثلا لا يغير ولا يحطم الإخفاء.
7- إن زيادة طول الفقرات أو زيادة امتداد الحرف في الكلمة لا يوثرعلى الرسالة السرية.
8- إن إرسال الملف بشكل وثيقة بصيغة Doc. يزيد من عدم انتباه المتطفل على وجود إخفاء, وما من طريقة لكشف الرسالة بهذه الصيغة عما إذا كانت صورة.

المصادر

1) أبو طبيخ, عبد المنعم صالح وتوفيق, محمد علي, "تصميم وتنفيذ تقنية ثنائية الشكل للحروف في النصوص المطبوعة للإخفاء المعلوماتي باستخدام الحاسوب", مجلة أبحاث الحاسوب, المجلد السادس–العدد الأول, ص79–91, (2002).

2) الحمامي, علاء حسين, الحمامي, محمد علاء, "إخفاء المعلومات: الكتابة المخفية والعلامة المائية", الطبعة الأولى– إثراء للنشر والتوزيع, الشارقة, (2008).

3) برزنجي، فوزي، "إخفاء البيانات داخل الصورة"، جامعة السليمانية, العراق, (2008).

4) الجوهرجي، شيماء شكيب، "الإخفاء في ملف صوت مكبوس", بحث ماجستير، قسم علوم الحاسبات، كلية علوم الحاسبات والرياضيات، جامعة الموصل، العراق، (2004).

5) الحمامي، علاء حسين والعاني, سعد عبد العزيز، "تكنولوجيا أمنية المعلومات وأنظمة الحماية", الطبعة الأولى– دار وائل للنشر، (2007).

6) الصميدعي، عامر تحسين سهيل، "تطبيق نظام التغطية", بحث ماجستير، قسم علوم الحاسبات، كلية علوم الحاسبات والرياضيات، جامعة الموصل، العراق، (2002).

7) الغريري، شهد عبد الرحمن حسو، "تصميم نظام حماية هجين وتطبيقه على النصوص"، بحث ماجستير، قسم علوم الحاسبات، كلية علوم الحاسبات والرياضيات، جامعة الموصل، العراق، (2003).

8) البلاسيني، أميرة بيبو، "تقنيات إخفاء المعلومات باستخدام الشبكات العصبية وبروتوكولات الشبكة", بحث ماجستير، قسم علوم الحاسبات، كلية علوم الحاسبات والرياضيات، جامعة الموصل، العراق، (2009).

9) Gutub, Adnan Abdul-Aziz, and Fattani, Manal Mohammad, "A Novel Arabic Text Steganography Method Using Letter Points and Extensions", World Academy of Science, Engineering and Technology, (2007).

10) Hübne, Simone Fischerr, PET-IV PET for Protecting Personal Data, PP 150-160, 12. Steganography, Update (2011/8/10).

11) Mary, S. Suma Christal, "Improved Protection In Video Steganography Used Compressed Video Bitstreams", (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 03, PP. 764-766,(2010).

12) Mihaela, Lavinia, "Survey of the Use of Steganography over the Internet", Informatica Economică Vol. 15, no. 2, PP.153-164, (2011).