جامعة البعث

مديرية البحث العلمي والدراسات العليا

عنوان البحث:

الإخفاء المتقن لملف نصي في صورة

Sturdy Hiding of Text File in Image

د.عمَّار سعد الريماوي

ملخص البحث Abstract

شهد مجتمع تقانة المعلومات خلال السنوات الأخيرة تطورا سريعاً، رافق التطور الهائل في الاقتصاد، فمعظم الهيئات الحكومية ومنها الهيئة العامة للتخطيط والتطوير العمراني لديها مواقع على الإنترنت، وتستخدم تقانة المعلومات في تسيير معظم أعمالها أو تسعى لذلك، الأمر الذي يتطلب الانتباه بشدة إلى ضرورة تأمين معلوماتنا ومواقع الإنترنت ضد أي اختراقات أو محاولات نسخ أو سرقة للمعلومات الحساسة (كالحسابات المصرفية أو كلمات المرور أو حقوق ملكية أي معلومات أثناء نقلها)، كما يتوجب أيضاً تأمين المعلومات ضد الهجمات أو الاختراقات التي تحاول سرقة المعلومات أو تشويهها، فيجب القيام بذلك عن طريق نقلها عبر الشبكة بشكل سري وآمن بعد تشفيرها وإخفاءها.

سنعرض في هذا البحث طريقة متقنة لإخفاء ملف نصي داخل صورة باستخدام خوارزمية البت الأقل استخداماً وتشفير ذلك النص، مما يسمح بتخزين النصوص باللغة الإنكليزية والعربية وبأحجام مختلفة مما يضمن لنا وصول الملف النصي بالشكل الصحيح وبسرية كبيرة.

الكلمات المفتاحية Keywords

إخفاء، تشفير، تعمية، هش، علم الإخفاء، المتقن، المتين.

Abstract

The technology information community has seen rapid development at length, accompanied by the enormous development in economy.

Most state centers, including that of architectural planning and development, have internet websites and use, or look forward to, technology information in propelling most of their work, which requires to be attention to the necessity of securing our information and internet websites against any attempt of hacking, copying, or plagiarizing sensitive information (bank accountancies, passwords, or any information during its transfer). Information is also required to be secured against any attacks or hacking that attempts at plagiarizing or distorting information. Thus, it is necessary to do so through transferring it via the network most secretly and safely after encrypting, or hiding, it.

This research will show a sturdy method to hide a text file into an image using least significant bit algorithm and encrypting this text, which allows to store English and Arabic texts with various sizes and ensure that the text file is delivered correctly and secretly.

الكلمات المفتاحية Keywords

Data Hiding, Cryptography, Steganography, Sturdy, Encryption, Robust.

1- المقدمة Introduction:

في خضم التطور المعلوماتي الهائل أصبح لنقل المعلومة من خلال الانترنت أهمية كبيرة لسرعة وصولها رغم تباعد المسافات، ومن أجل ذلك أصبحت الحاجة ملحة لمنع المتطفلين (الهاكرز) من سرقة البيانات الهامة فظهر علم التشفير (Cryptography) لتشفير هذه المعلومات، ولكن مع استمرار عمل المتطفلين المستمر لمحاولة سرقة المعلومات ظهرت الحاجة لتغطية نقاط الضعف الموجودة في التشفير فظهر علم الإخفاء (Steganography).

كما ظهر ما يسمى نظام التغطية وهو علم إخفاء المعلومات والذي يعتمد على فكرة زرع معلومات داخل حامل معلومات آخر، بحيث لا يدرك المتطفلين وجود معلومات من نوع آخر وتكون معروفة فقط من قبل أشخاص معينين مسموح لهم بالاطلاع على هذه المعلومات (المرسل والمستقبل)، بحيث يتم إخفاء المعلومات السرية في ملف غطاء والذي يمكن أن يكون ملف صوتي أو فيديو أو صورة وبحيث لا يمكن للشخص العادي ملاحظة ذلك[4] [6].

2- هدف البحث Research Propose

تعاني الحسابات المصرفية أو كلمات المرور أو حقوق ملكية أو أي معلومات أثناء نقلها عبر شبكة الانترنت، إلى محاولة السرقة أو التشويه بغاية الدخول إلى الحسابات الخاصة وسرقة الأموال أو الدخول إلى إدارة المواقع بغاية نشر أخبار غير حقيقية، أو لتغيير ملكية البيانات مثل الصور ...الخ.

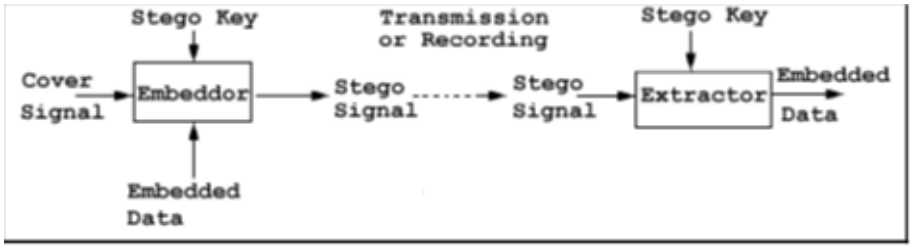
مما يتوجب علينا ايجاد وسيلة نقل آمنة وسرية للبيانات الحساسة ككلمات المرور أو الحسابات المصرفية أو حماية ملكية البيانات، بتشفير وإخفاء البيانات، باعتبار أن هذه البيانات يتم نقلها بشكل مستمر عبر شبكة الانترنت.

3- طرق البحث Research Methods

علم الإخفاء:

إن أصل مصطلح Steganography هو من الكلمة اليونانية Stego وتعني التعمية أو الحجب، والكلمة Graphia وتعني الكتابة ليصبح المصطلح الكتابة المحجوبة "Covered Writing".

وبالتالي فان مصطلح Steganography يعني فن وعلم إخفاء المعلومات السرية ضمن معلومات غير ذات أهمية ظاهريا، وبالتالي لا أحد يعلم بالمعلومات الأصلية السرية غير الطرفين المعنيين (المرسل والمستقبل) والذين يملكون مفاتيح خاصة للإخفاء والاستخلاص[1].



الشكل -1- آلية عمل نظام الإخفاء

بالاعتماد على الشكل أعلاه يمكن القول إن هناك رسالة ظاهرية (Cover signal) غير ذات أهمية (مقالة من صحيفة مثلا)، إضافة إلى رسالة أخرى سرية (Embedded data) مخبأة بأسلوب ما ضمن الرسالة الظاهرية عن طريق مفاتيح خاصة (Stego keys) [7].

ظاهرياً ، إن أي إنسان غير الطرفين الأساسيين (المرسل والمستقبل) لا يرى أي شيء ذو أهمية في الرسالة، لكن عمليا فإن الرسالة هي رسالة أخرى مختلفة بالنسبة للمستقبل بعد أن يقوم باستخلاصها عن طريق المفاتيح.

في مجال تكنولوجيا المعلومات يعتبر علم الإخفاء هو عملية إخفاء ملف ما ضمن ملف آخر دون تشويه أو تغير في خصائص الملف الحامل[5].

إن أهم ما يميز هذا العلم هي الطرق الذكية المستخدمة في الإخفاء والتي تصعب من مهمة كشف المعلومات، حيث كلما كانت الطريقة المستخدمة أقوى كان الكشف أصعب.

تكمن أهمية علم الإخفاء في أيامنا هذه في عمليات تبادل المعلومات بطرائق سرية عبر الأنظمة المفتوحة (open system) كالإنترنت، وبالتالي الحفاظ على سرية وخصوصية المعلومات المتبادلة عبر بيئات هذه الأنظمة.

مصطلحات وتعاريف:

سنقوم بتوضيح بعض المصطلحات والتعاريف التي سوف نستخدمها:

التشفير Encryption:

يُعرَّف التشفير بأنه عملية تحويل المعلومات إلى شيفرات غير مفهومة (تبدو غير ذات معنى) لمنع الأشخاص غير المُرخَّص لهم من الاطلاع على المعلومات أو فهمها، ولهذا تنطوي عملية التشفير على تحويل النصوص العادية إلى نصوص مُشفَّرَة، يستخدم في التشفير بشكل عام طرائق رياضية لتوليد النص المشفر، هناك العديد من خوارزميات التشفير للقيام بذلك [2].

الشكل –2– آلية عمل التشفير

التوقيع الرقمي Digital Signature:

وسيلة لمُنشئ رسالة، أو ملف، أو معلومات أخرى مرمّزة رقمياً لربط هويتهم بالمعلومات. عملية التوقيع الرقمي على المعلومات تستلزم تحويل المعلومات، وكذلك بعض المعلومات السرية التي يحتفظ بها المرسل، إلى علامة تسمى توقيعاً.

توفر التواقيع الرقمية خدمات عدم الإنكار(Non-repudiation) وسلامة المعطيات (Data integrity).

العلامة المائية Watermark:

هي شعار (صورة، عبارة...) يوضع على الوثائق، الملفات... الخ الورقية أو الرقمية عند إنشائها، يستخدم بشكل رئيسي لمنع عمليات القرصنة (انتهاك الحقوق) على المعلومات، كمثال على ذلك العلامة المائية التي تضاف إلى الأوراق النقدية [7].

المفتاح Key:

هو قيمة رقمية تستخدم في خوارزميات التشفير وذلك لتوليد شيفرة محددة، يقاس طول المفتاح بالبت وكلما كان مفتاح التشفير أكبر كانت الشيفرة المولدة أكثر أماناً.

الملف الحامل Carrier File:

في علم الإخفاء يسمى الملف الذي سوف تخبأ به المعلومات السرية بالملف الحامل، قد يكون الملف الحامل أي نوع من أنواع الملفات (صورة ملف نصي... الخ) ولكن يجب أن يكون ذو حجم كبير بحيث يكفي لإخفاء المعلومات.

الملف المخبئ Embedded File:

وهو الملف السري والذي نريد إخفاؤه، أيضا يمكن لهذا الملف أن يكون أي نوع من أنواع الملفات (نصي، صورة، صوت.... الخ).

أنواع الخفاء:

بشكل أساسي هناك نوعين أساسيين لعملية الإخفاء:

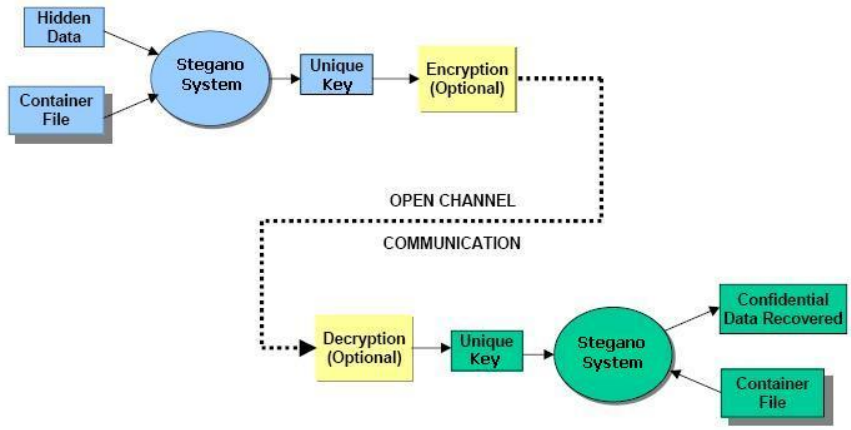
1- الإخفاء الهش (Fragile):

في هذا النوع من الإخفاء يتم تخريب المعلومات المخفية ضمن الملف، وبالتالي زوالها وذلك عند أي تعديل لبنية الملف.

2- الإخفاء المتين (Robust):

في هذا النوع لا يمكن تدمير المعلومات المخفية بسهولة عند إجراء بعض التعديلات على الملف الحامل، ولكن يمكننا القول إن كمية التعديلات الواجب إجراؤها لتخريب المعلومات المخبأة ستؤدي أيضاً إلى تخريب الملف المضيف، يستخدم هذا النوع من الإخفاء بشكل عام لوضع العلامات المائية.

التقنيات المستخدمة في عمليات الإخفاء:

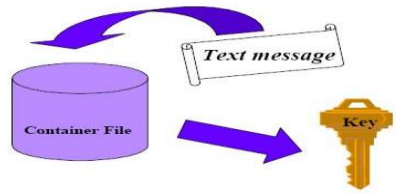


الشكل -3- تبادل المعلومات المخفية عبر نظام مفتوح

إن الهدف الأساسي من عملية الإخفاء كما رأينا هي عملية الإرسال للرسالة المخبئة عبر قناة إرسال ما (انترنت مثلا) دون علم أحد غير الطرفين المرسلين، وبالتالي فالمهمة الأساسية للمرسل هي إخفاء الرسالة باستخدام تقانة ما (ملف صورة)، دون معرفة أن هذا الملف يحوي على رسالة سرية [3].

هناك العديد من التقنيات التي تستخدم من أجل عملية إخفاء المعلومات وذلك تبعاً لنوع الملف الحامل، حيث يمكننا تقسيم الملفات إلى:

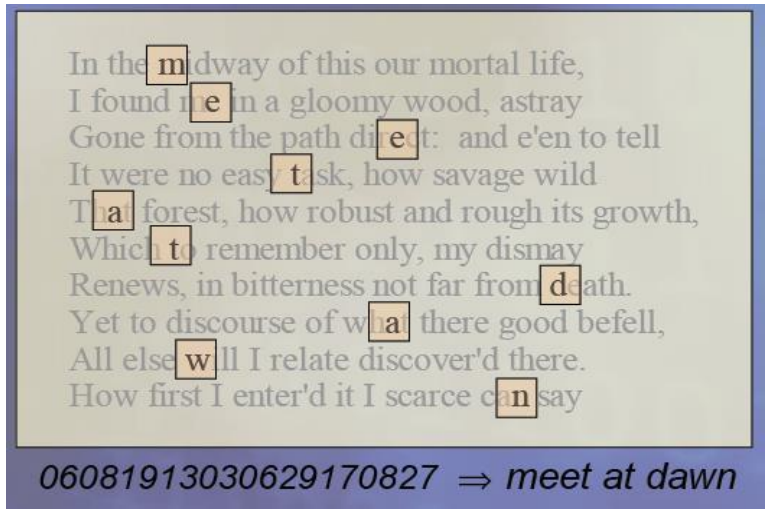
الملفات النصية Text File:



الشكل-4- إخفاء ملف نصي

تستخدم بشكل عام تقنيتين:

تعتمد على إرسال رسالة ما إضافة إلى إرسال شيفرة رقمية تدل على رقم الحرف في كل سطر، وذلك كما يلي:



الشكل -5- طريقة الإخفاء عن طريق أرقام الأسطر والأحرف

التقانة الثانية هي باستخدام الفراغات بين الكلمات والسطور الجديدة.

ملفات الصور Image File:

هناك عدد من التقنيات أهمها:

التقنيع والترشيح (Masking and Filtering):

تستخدم عادة مع الصور 24 بت أو ذات التدرج الرمادي، ويستفاد منها فقط في عملية وضع العلامة المائية Watermarking.

المبدأ الأساسي لهذه التقانة هو في تغيير السطوع Luminance أجزاء من الصورة، حيث تكون هذه التغيرات غير مرئية للعين البشرية.

وتعد هذه التقانة من التقانات الأكثر متانة Robustness، لأنها أكثر مناعة ضد التغيرات مثل الضغط Compression والقص Cropping ومختلف عمليات معالجة الصور.

تقنيات التحويل (Transformation):

وتعتمد هذه التقانة على استخدام تحويل التجيب المتقطع(DCT) الذي يستخدم في خوارزمية ضغط ملفات JPEG، معادلة(DCT) بالعلاقة [3]:

$$F(u,v) = \frac{1}{4}C(u)C(v)\left[\sum_{x=0}^{7}\sum_{y=0}^{7} f(x,y) * cos\frac{(2x+1)u\pi}{16} cos\frac{(2y+1)v\pi}{16}\right]$$

حيث أن:

$C(x) = 1/\sqrt{2}$ عندما X تساوي 1،

$C(x) = 1$ عندما X غير ذلك.

ويمكن تمثيل عملية الإخفاء وفق هذه التقانة بالخوارزمية:

```
Input: message, cover image
Output: steganographic image containing message
while data left to embed do
        get next DCT coefficient from cover image
        if DCT ≠ 0 and DCT ≠ 1 then
                get next LSB from message
                replace DCT LSB with message bit
        end if
        insert DCT into steganographic image
end while
```

تقانة الإخفاء باستخدام الخانة الأقل أهمية(LSB):

وهي من الطرائق ذات الاستخدام الواسع، حيث تقوم باستخدام الخانة الأقل أهمية من بيكسل معين لتخزين المعلومة.

متطلبات عملية الإخفاء:

عند القيام بعملية إخفاء ومن أجل ضمان جودة عالية لهذه العملية لابد من الأخذ بعين الاعتبار الخواص الثلاث التالية:

معدل الخانة (Bit rate): وهي تعبر عن كمية المعلومات الممكن إخفاؤها في واحدة الزمن.

المتطلبات العتادية (Hardware Requirement): وتمثل تكلفة عملية الإخفاء والاستخلاص، لأنها في بعض الحالات يجب أن يتم ذلك بالزمن الحقيقي.

الشمولية(Universality): وتعني إيجاد خوارزميات يمكن تطبيقها على أنواع مختلفة من الملفات مثلا النص والصورة والصوت.

إضافة إلى الخواص السابقة يمكن إضافة بعض التوصيات بعين الاعتبار، وهي:
المحافظة على سلامة ووحدة المعلومات المخبأة ضمن الملف المضيف.

يجب ألا يتغير الملف المضيف بعد عملية الإخفاء، أو أن هذا التغيير يجب أن يكون غير محسوس لأي طرف آخر وإلا فإنه قد يحاول تدمير الملف.

يجب ألا تتغير العلامة المائية بالتغيرات التي قد تحدث للملف المضيف مثل تغير حجم الملف المضيف أو نسخه.

يجب أن نفترض دائما أن المعترض يعلم بأن هناك معلومات مخفية ضمن الملف المرسل.

كشف الإخفاء (Steganalysis):

إن مصطلح Steganalysis يعني عملية الهجوم على طرق الإخفاء (Steganography) وذلك بهدف كشف، استخلاص، تخريب، أو حتى التلاعب بالمعلومات المخفية ضمن ملف ما، إن عملية كشف الإخفاء تتطلب من ممارسها إلمام واسع بطرائق الإخفاء وتقنياته حتى يتمكن من كشف المعلومات بكفاءة عالية[10].

مما سبق يمكننا القول إن كشف الإخفاء هو علم قائم بذاته هدفه الرئيسي اكتشاف وجود معلومات مخبئة والحصول عليها، يصنف الكشف إلى عدة أنواع وذلك بحسب المعلومات المتاحة، حيث هناك عمليات هدفها فقط اكتشاف وجود معلومات، بينما هناك أنواع أخرى تهدف إلى حذف المعلومات المخبئة دون إمكانية معرفتها، ومنها ما يهدف إلى استخلاص المعلومات المخبأة أو حتى استبدالها بأخرى مزيفيه، إن تلك العمليات تعتمد على المعلومات المتوفرة عند الشخص الساعي لكشف المعلومات، حيث يمكن أن يكون لديه فقط الملف الحامل للمعلومات، كما يمكن أن يكون لديه الملف الذي يحوي المعلومات السرية إضافة إلى الملف الأصلي، كما يمكن أن يكون على علم بخوارزمية الإخفاء ... الخ.

أنواع كشف الإخفاء:

هناك ثلاثة أنواع من الكشف وهي[1]:

الكشف البصري (Visual Detection):

وذلك بالمقارنة بين البايتات في الملفين (الحامل والأصلي) واكتشاف الفرق.

الكشف البنيوي (Structural Detection):

حيث أن بنية الملف الحامل تتغير في بعض الأحيان عند إخفاء معلومات فيها، إن كشف هذا التغير في بنية الملف تساعد على كشف المعلومات المخبأة.

الكشف الإحصائي (Statistical Detection):

في هذا النمط يتم الكشف عن المعلومات المخبأة عن طريق الصيغ والمعادلات الرياضية التي تساعد على تحديد وجود هذه المعلومات، حيث أنه وبشكل عام تكون بنية الملف الحاوي على معلومات سرية أكثر عشوائية من الملفات العادية.

تم استخدام عدة مقاييس للدراسة وهي[8] [9] [12] :

1- نسبة الخطأ في الصورة Mean Square Error(MSE)

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(f_{ij} - g_{ij})^2$$

حيث:

M,N عدد الصفوف والأعمدة بالنسبة للصورة الغطاء

f_{ij} الصورة الغطاء قبل الاخفاء

g_{ij} الصورة بعد اخفاء النص داخلها

2- معدل الإشارة إلى الضجيج Signal to Noise Ratio(SNR) وهو مقدار بين 0 و100 يعبر عن علاقة الإشارة الأصلية W والإشارة المضجة $\hat{W}$ ويعطى بالعلاقة الرياضية الآتية:

$$SNR(W,\hat{W}) = 10\log_{10}\frac{\sum_{i=1}^{N} w_i^2}{\sum_{i=1}^{N}(W_i - \hat{W}_i)^2}$$

3- معدل طاقة الإشارة إلى الضجيج Peak Signal to Noise Ratio(PSNR) وهو مقدار بين 0 و100 يعبر عن علاقة الصورة الأصلية f(m,n) والصورة المضجة f'(m,n) ويعطى بالعلاقة الرياضية التالية:

$$PSNR = 20\log_{10}[255/RMSE]$$

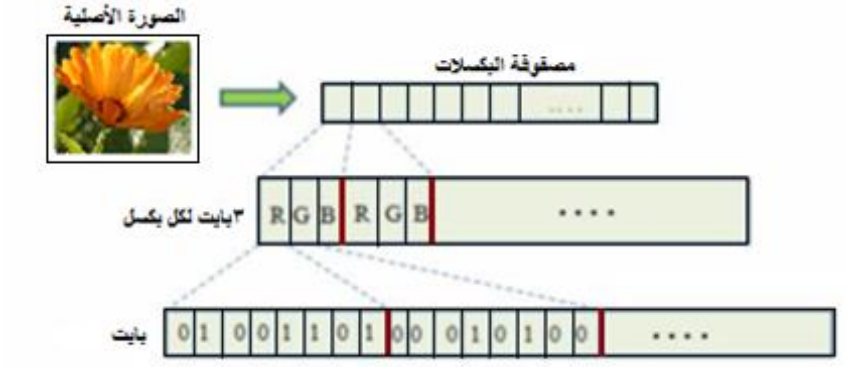
Where

$$RMSE = \sqrt{\frac{1}{M*N}\sum_{i=1}^{M}\sum_{j=1}^{N}[\tilde{f}(m,n)-f(m,n)]^2}$$

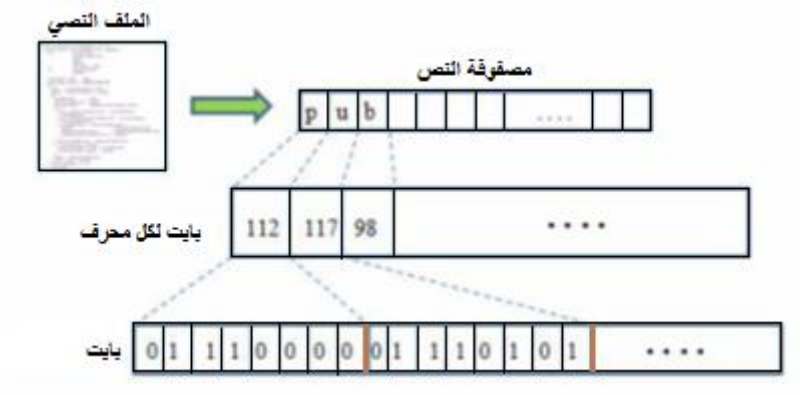
4- الطريقة المقترحة Proposed Method

تم الاعتماد على طريقة LSB بحيث يتم الإخفاء في البت الأقل أهمية، وبهذه الطريقة لا نستطيع تميز الفرق بين الصورة الغطاء قبل وبعد الاخفاء بالعين المجردة، وقمنا بتشفير الملف النصي قبل عملية الاخفاء لزيادة الإخفاء المتقن للملف في الصورة، ويتم ذلك عن طريق تبديل البت الأول في كل حرف إلى قيمة عكسية، ومن ثم تبديل البتات من الثاني وحتى الرابع بالبتات من الخامس وحتى السابع ووضع النتائج في مصفوفة، والقيام بعملية الإخفاء في الصورة، مما يضمن القيام بإخفاء نصوص باللغة الإنكليزية أو نصوص باللغة العربية وذلك ضمن الصور الرمادية أو الملونة.

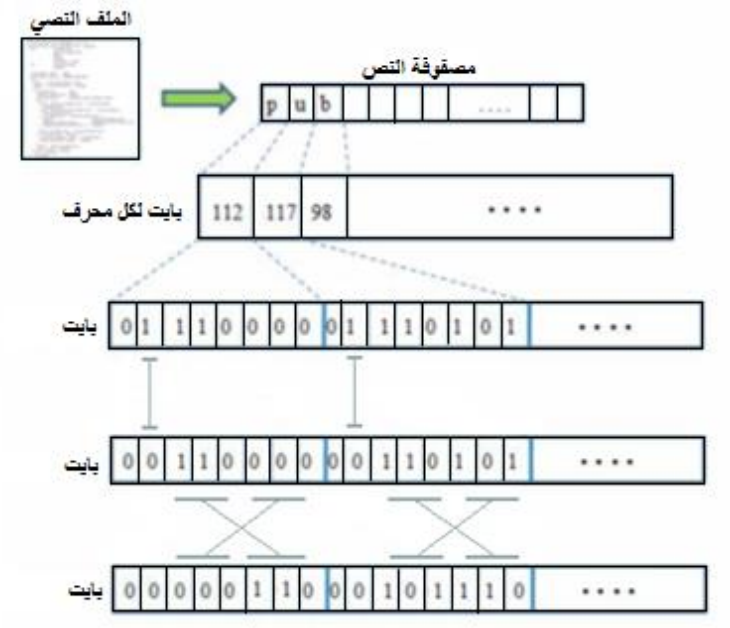
في هذه الطريقة يتم إخفاء النص كما يلي:



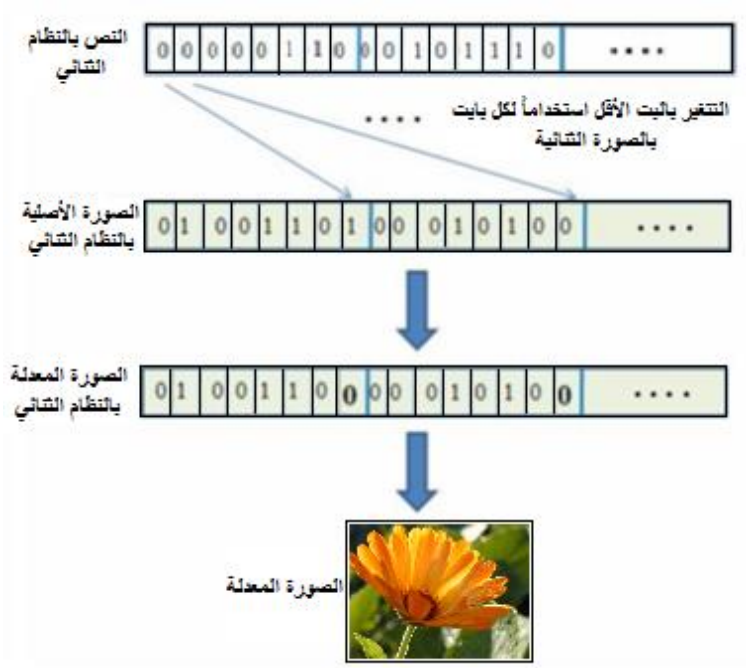
الشكل -6- الصيغة الثنائية للصورة من نوع png أو bmp



الشكل –7– الصيغة الثنائية للنص المراد إخفاءه

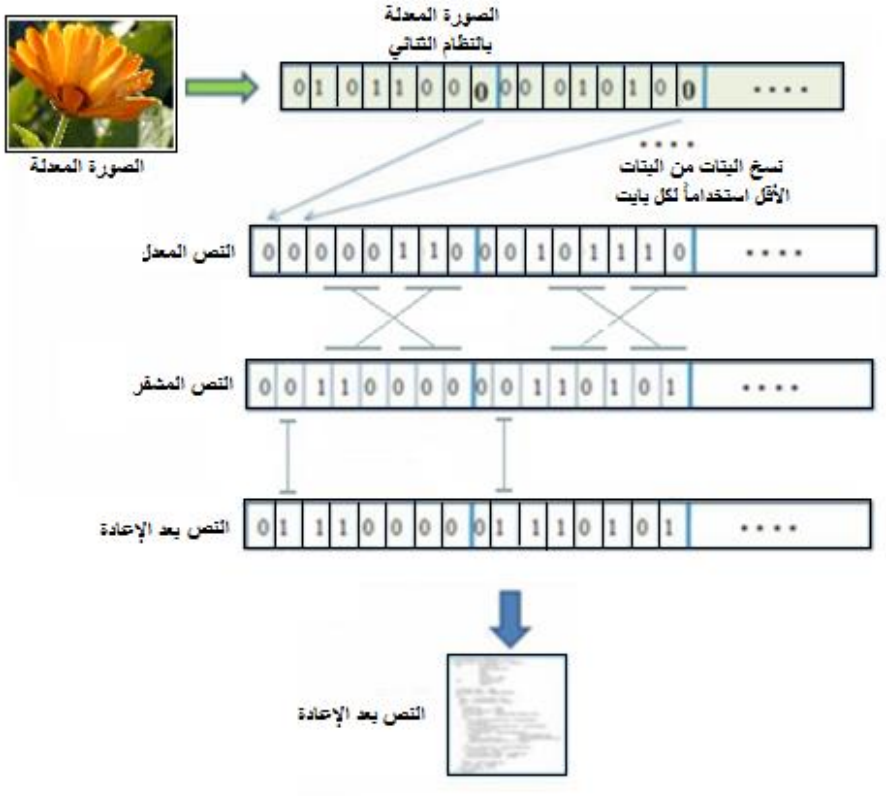


الشكل –8– الصيغة الثنائية للنص بعد تشفيره

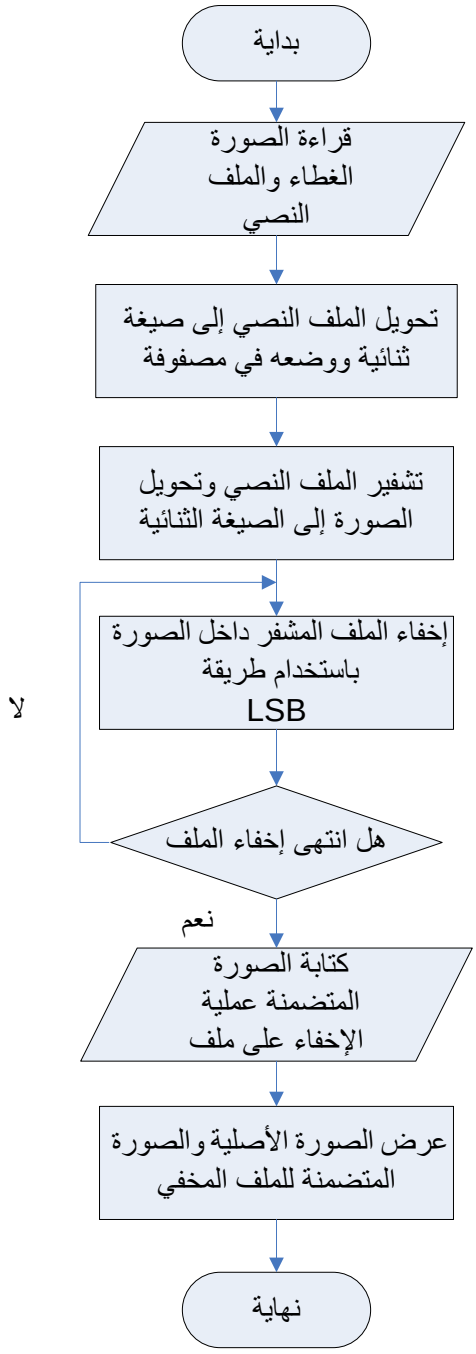


الشكل –9– طريقة الإخفاء بالصورة

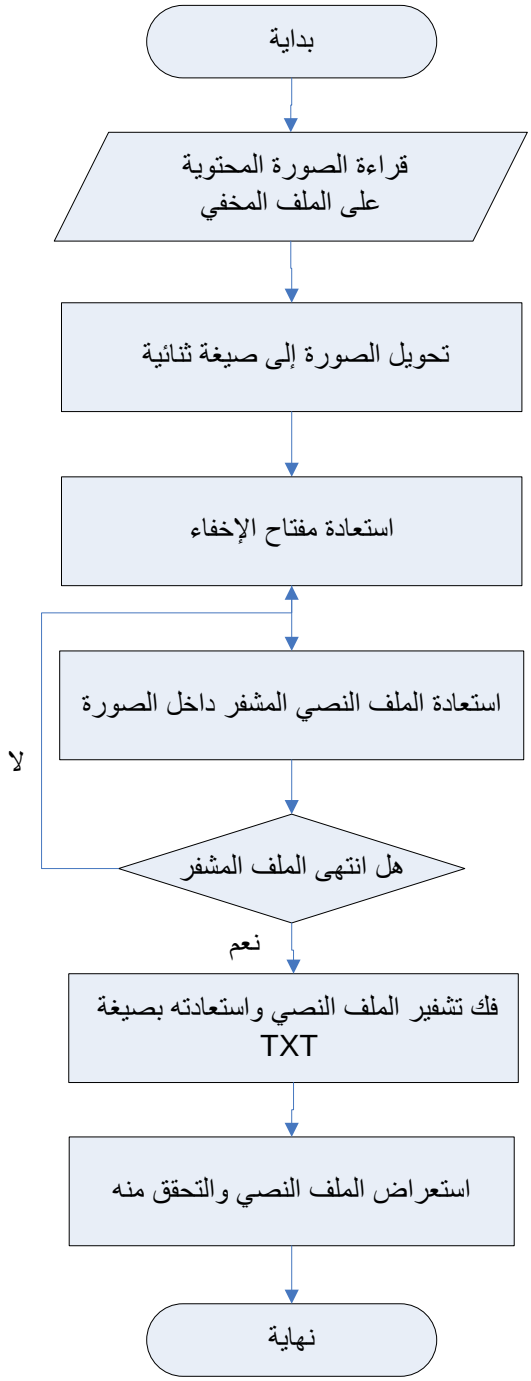
في هذه الطريقة تظهر الصورة بعد عملية الاخفاء مماثلة للصورة الغطاء بالنسبة للعين المجردة وتم الإخفاء في البت الثامن لكل مركبة لونية للصورة وذلك لتحميل أكبر عدد من البيانات (الملف النصي).



الشكل –9– طريقة استعادة النص المخفي



الشكل –10– المخطط الخوارزمي لعملية إخفاء الملف



الشكل -11- المخطط الخوارزمي لعملية استعادة الملف المخفي

1- دراسة أثر إخفاء عدة نصوص باللغة الانكليزية على عدة صور

IMAGES	IMG-SIZE	TXT-SIZE	SNR	PSNR	MSE
Image1	217 k.byte	5 byte	54.09	61.77	0.043
Image1	217 k.byte	33 byte	48.50	56.18	0.156
Image1	217 k.byte	68 byte	47.10	54.79	0.215
Image1	217 k.byte	488 byte	46.03	53.72	0.275
Image1	217 k.byte	8.23 k.byte	43.57	51.25	0.486

جدول -1- نتائج pnsr و mse لصورة رمادية 1 ونصوص مختلفة الحجم باللغة الانكليزية

الشكل -12- الصورة الرمادية الأصلية 1 على اليسار والصورة المحتوية على الملف المخفي

IMAGES	IMG-SIZE	TXT-SIZE	SNR	PSNR	MSE
Image1	843 k.byte	5 byte	53.64	61.38	0.047
Image1	843 k.byte	33 byte	59.92	61.77	0.066
Image1	843 k.byte	68 byte	53.61	61.34	0.085
Image1	843 k.byte	488 byte	48.82	56.55	0.143
Image1	843 k.byte	8.23 k.byte	48.42	56.15	0.157

جدول -2- نتائج pnsr و mse لصورة ملونة ونصوص مختلفة الحجم باللغة الانكليزية

الشكل –13– الصورة الملونة الأصلية 1 على اليسار والصورة المحتوية على الملف المخفي

IMAGES	IMG–SIZE	TXT–SIZE	SNR	PSNR	MSE
Image2	271 k.byte	5byte	47.98	54.09	0.253
Image2	271 k.byte	33byte	49.00	55.11	0.200
Image2	271 k.byte	68byte	48.99	55.10	0.200
Image2	271 k.byte	488byte	45.28	51.38	0.472
Image2	271 k.byte	8.23 k.byte	44.96	51.06	0.508

جدول –3– نتائج pnsr و mse لصورة رمادية 2 ونصوص مختلفة باللغة الانكليزية

الشكل –14– الصورة الرمادية الأصلية 2 على اليسار والصورة المحتوية على الملف المخفي

IMAGES	IMG-SIZE	TXT-SIZE	SNR	PSNR	MSE
Image2	531 k.byte	5byte	52.72	58.87	0.084
Image2	531 k.byte	33byte	53.74	59.89	0.066
Image2	531 k.byte	68byte	53.69	59.84	0.067
Image2	531 k.byte	488byte	50.02	56.17	0.157
Image2	531 k.byte	8.23 k.byt	49.69	55.84	0.169

جدول -4- نتائج pnsr و mse لصورة ملونة 2 ونصوص مختلفة باللغة الانكليزية

الشكل -15- الصورة الملونة الأصلية 2 على اليسار والصورة المحتوية على الملف المخفي

2- دراسة أثر إخفاء عدة نصوص باللغة العربية على عدة صور

MAGES	IMG-SIZE	TXT-SIZE	SNR	PSNR	MSE
Image1	843 k.byte	5byte	55.78	63.52	0.028
Image1	843 k.byte	28byte	51.05	58.78	0.086
Image1	843 k.byte	1.21k.byte	48.06	55.80	0.170
Image1	843 k.byte	6.10k.byte	47.75	55.49	0.183
Image1	843 k.byte	12.2k.byte	46.90	54.63	0.223
Image1	843 k.byte	24.4k.byte	45.58	53.31	0.302

جدول -5- نتائج pnsr و mse لصورة ملونة ونصوص مختلفة الحجم باللغة العربية

الشكل –16– الصورة الملونة الأصلية 1 على اليسار والصورة المحتوية على الملف المخفي

IMAGES	IMG–SIZE	TXT–SIZE	SNR	PSNR	MSE
Image2	531 k.byte	5byte	55.03	61.18	0.049
Image2	531 k.byte	28byte	53.74	59.89	0.066
Image2	531 k.byte	1.21k.byte	49.38	55.53	0.181
Image2	531 k.byte	6.10k.byte	49.13	55.27	0.192
Image2	531 k.byte	12.2k.byte	48.37	54.52	0.229
Image2	531 k.byte	24.4k.byte	47.14	53.29	0.304

جدول –6– نتائج pnsr وmse لصورة ملونة ونصوص مختلفة الحجم باللغة العربية

الشكل –17– الصورة الملونة الأصلية 2 على اليسار والصورة المحتوية على الملف المخفي

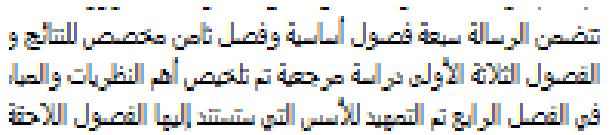
في اللغة العربية كل محرف يزيد بمقدار 4 بت عن اللغة الإنكليزية مما يعطي لإخفاء النص باللغة العربية مساحة أكبر ضمن الصورة المضيفة.

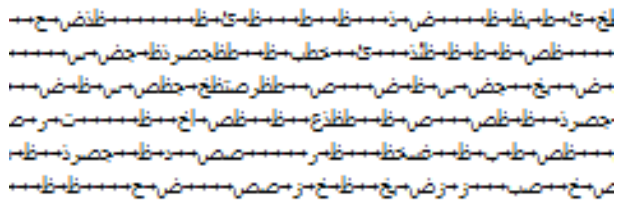
بعض النصوص قبل وبعد التشفير:

r¦¦ra ammar

ammar ammar ammar ammar ammar

r¦¦ra/r¦¦ra/r¦¦ra/r¦¦ra/r¦¦ra





نلاحظ أن النص المشفر لا يعطي علامات نهائياً عن النص الأصلي بالإضافة إلى أن حجم النص المشفر هو نفس حجم النص قبل التشفير لزيادة تبسيط التشفير وتعقيد عملية فك التشفير.

وبمقارنة الجداول السابقة مع الجداول التالية لطريقة المرجع 11 والذي أعتمد طريقة الإخفاء بالاعتماد على LSB مع التشفير باستخدام خوارزمية blow fish:

IMAGES	IMG-SIZE	TXT-SIZE	SNR	PSNR	MSE
Image2	531 k.byte	5byte	49.59	55.74	0.173
Image2	531 k.byte	33byte	51.87	58.02	0.102
Image2	531 k.byte	68byte	50.58	56.73	0.138
Image2	531 k.byte	488byte	51.04	57.19	0.124
Image2	531 k.byte	8.23 k.byt	48.55	54.70	0.220

جدول -7- الطريقة في المرجع11 مع صورة ملونة ونصوص مختلفة الحجم باللغة الإنكليزية

IMAGES	IMG-SIZE	TXT-SIZE	SNR	PSNR	MSE
Image1	843 k.byte	5 byte	51.05	58.79	0.085
Image1	843 k.byte	33 byte	49.47	57.21	0.123
Image1	843 k.byte	68 byte	49.46	57.20	0.146
Image1	843 k.byte	488 byte	50.04	57.77	0.168
Image1	843 k.byte	8.23 k.byte	47.16	54.90	0.210

جدول -8- الطريقة في المرجع11 مع صورة ملونة ونصوص مختلفة الحجم باللغة الإنكليزية

نجد أن MSE في هذه الطريقة أعلى من MSE الموجود في الجدول 4 والجدول 2 الخاص بالطريقة المقترحة بالإضافة إلى انخفاض كل من PSNR **و** SNR المرتبط بشكل عكسي مع MSE مما يدل على كفاءة الطريقة المقترحة، وحيث قمنا بالمقارنة مع المرجع 11 لاستخدامه نفس طريقة الإخفاء مع اختلاف طريقة التشفير.

5- الاستنتاجات والتوصيات Conclusions and recommendations

1- نلاحظ أننا لا نستطيع إيجاد فرق بالعين المجردة عند مقارنة الصورة الغطاء قبل وبعد عملية الإخفاء.

2- القيام بتشفير النص يزيد من صعوبة اكتشاف النص المخفي مما يضمن عملية الاخفاء المتقن للنص.

3- نلاحظ انه بزيادة طول النص تزداد قيمة MSE وتقل قيمة PSNR مما يدل على كفاءة الطريقة المستخدمة في الاخفاء بالإضافة إلى أن طول النص لا يؤثر بشكل واضح على عملية الاخفاء.

4- حجم الصورة لا يتغير قبل وبعد عملية الاخفاء لأن الإخفاء تم بتبديل بت مكان بت آخر مع الحفاظ على عدد البتات مما يزيد من الاخفاء المتقن.

5- نقترح تطبيق الطريقة المقترحة على ملفات الفيديو والصوت.

6- نقترح دمج أكثر من طريقة للإخفاء مثل الطريقة المقترحة مع طريقة التجيب المتقطع DCT أو طريقة التحويل الموجي DWT.

6- المراجع Reference

1. HAMAMI, A H, 2008, "Information Hidings, Steganography and watermark". Ethraa for Publishing and Distribution, Jordan, 550p.
2. STALLINGS, W, 2005, "Cryptography and Network Security Principles and Practices". Prentice Hall, USA, 592p.
3. Pan J, Snasel V, Corchado E, Abraham A, Wang S, "Intelligent Data Analysis and Its Applications", Proceeding of the First Euro-China Conference on Intelligent Data Analysis and Applications, June 13-15, 2014, Shenzhen, China, 298p.
4. PAN J. S, 2007, "Progressive watermarking techniques using genetic algorithms", Circuits, Systems, and Signal Processing, vol. 26, 671-687p.
5. EL-ZOUKA, H A, 2010, "Distortion Free Steganography System Based on Genetic Algorithm ", Journal of Information Hiding and Multimedia Signal Prossing, vol. 2, 11-16p.
6. HAJJARA S, ABDALLAH M, HUDAIB A, 2009, "Digital Image Watermarking Using Localized Biothogonal Wavelets", European Journal Of Scientific Research, vol 26, 594-608p.
7. LIU W, Dong L, Zeng W, 2007, "Optimum Detection For Spread-Spectrum Watermarking That Employs Self-Masking", IEEE Transactions on Information Forensics and Security, vol 4, 645–654p.
8. JABER S, FADHIL H, ABDUL KHALIB Z, KADHIM R, 2014, "Survey On Recent Digital Image Steganography Techniques", Journal of Theoretical and Applied Information Technology, Vol. 66, 714-728p.
9. WANG S, YANG B, NIU X, 2010, " A Secure Steganography Method based on Genetic Algorithm", Journal of Information Hiding and Multimedia Signal Processing, Vol. 1, 28-35p.
10. BEGUM R, PRADEEP S, 2014, "Best Approach for LSB Based Steganography Using Genetic Algorithm and Visual

Cryptography for Secured Data Hiding and Transmission over Networks", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4, 114-119p.

11. KOMAL P, SUMIT U, HITESH G, 2013 "Information Hiding using Least Significant Bit Steganography and Blowfish Algorithm" International Journal of Computer Applications, Vol. 63, 24-28p.
12. ATASSI Y, 2011, "Robust Watermarking Algorithm", Journal of Al-Baath University, Vol. 33, 119-146p.