طريقة جديدة لاستخدام الصور الرقمية في إخفاء الملفات النصية السرية[+]

New Method for Using Digital Images to Hide Secret Text Files

معن عبد الخالق يحيى البكوع* **عامر تحسين سهيل****

المستخلص:-

تم خلال البحث استحداث طريقة لإخفاء الملفات النصية السرية داخل الصور أحادية اللـــون أو الملونـــة، وذلك عن طريق إخفاء حروف النص داخل عناصر الصورة، بأسلوب جعل المسافة بين العناصر المستخدمة فـــي عملية الإخفاء غير ثابتة، مما يصعب إمكانية توقع مواقع إخفاء تلك الحروف داخل عناصر الـــصورة باســـتخدام طرائق تحليل الصورة أو عن طريق التحليلات الإحصائية.

نجحت هذه الطريقة في إخفاء الملفات النصية دون حدوث حالة تـــشوه للـــصورة الأصـــلية، أو إمكانيـــة ملاحظة التغيرات الحاصلة فيها جراء عملية الإخفاء، وتم استرجاع تلك الملفات بـــسهولة دون فقـــدان لأي مـــن مكوناتها، فضلا عن أن عملية الاسترجاع هذه تتم دون الاستعانة بالصورة الأصلية أو الحاجة لإنشاء جدول يبـــين مواقع الإخفاء.

ABSTRACT

In this research we found out a new method for hiding secret text files in two types of images, monochrome and color, the characters of the text embedded is not sequence 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 out come and the original images. The text files are retrieving easily and without losing any character, Rather than that no need to returning to the source image or creating any table of hiding places.

١ - المقدمة:

أصبح استخدام الحاسبات في الوقت الحاضر الوسيلة الأكثر أهميـــة وانتـــشاراً فـــي خـــزن واســـترجاع المعلومات وتداولها ع[+]بر الشبكات المحلية ،العالمية ،البريد الالكتروني و الهواتف النقالة عن طريـــق الوســـائط الرقمية مثل النصوص، الصوت، الصورة والصور المتحركة.

[+] تاريخ استلام البحث ٢٠٠٦/٢/١ ، تاريخ قبول النشر ٢٠١٠/١/٤

*مدرس مساعد / المعهد التقني /نينوى

** مدرس المعهد التقني/ نينوى

لقد بات من السهل اعتراض المعلومات المرسلة عبر شبكات الاتصال المختلفة أو الدخول إلى تلك الحاسبات سواءً أكانت مستقلة أم مرتبطة مع الشبكة، بقصد الاطلاع على محتوياتها أو سرقة المعلومات المهمة أو العبث بها.

وفي ضوء ذلك يتوجب تأمين الحماية والموثوقية والمصداقية للمعلومات والمحافظة عليها فظهرت وسائل حماية متنوعة مثل وضع كلمات السر، استخدام التشفير(Cryptography)، وتقنيات إخفاء (Hiding) أو تغطية المعلومات. حيث تتلخص عملية التشفير بتحويل الرسائل والبيانات السرية إلى صيغة لا يمكن قراءتها وذلك باستخدام مفتاح سري (Secret key) ويتم استرجاعها باستخدام ذلك المفتاح.

إن شكل الرسالة والبيانات الناتجة بعد عملية التشفير يثير الشك لظهور محتواها بشكل غير مرتب وظهور ألفاظ من غير اللغة المستخدمة مما يلفت انتباه المتطفلين أو قراصنة المعلومات إلى العبث بالرسالة إن لم يتمكنوا من فك الشفرة [١] [٢].

أما الإخفاء فيتم من خلال وضع البيانات داخل ملفات الوسائط بحيث لا يمكن ملاحظتها أو كشفها أو إدراك وجود معلومات منقولة من خلال تلك الملفات وإنما تبدو كملفات عادية حيث يتم فيها المحافظة على الشكل العام للملف الناقل، ويكون الإخفاء على صنفين الأول العلامات المائية (Watermarking) وفيه يتم إخفاء معلومات قليلة مثل التوقيع، علامة الشركة أو ختم المؤسسة لتوثيق المستندات المرسلة، بطريقة يصعب التلاعب بها أو محوها من خلال عمليات المعالجة الصورية مثل الترشيح ، التحويلات الهندسية أو إضافة الضوضاء [٣] [٤] [٥].

أما الصنف الثاني فهو الإخفاء الصوري (Image Hiding) حيث يتضمن إخفاء أكبر ما يمكن من المعلومات المهمة (وثيقة، رسالة، مخططات أو صور) داخل ملفات نصوص أو صور بطريقة لا تثير الفضول وإنما تبدو كصور إعلان أو نصوص عادية [٦].

٢- هدف البحث :

إيجاد طريقة جديدة لإخفاء الأنواع المختلفة من الملفات النصية السرية والمهمة داخل الصور دون أن يُلاحظ أي تغير أو تشوه واضح في معلومات الصورة بعد عملية الإخفاء،أو محاولة اكتشافها من قبل المتطفلين. ثم استخلاص هذه النصوص واسترجاعها عند الطلب دون خسارة أو ضياع أو تشويه لأي من محتوياتها .

٣- استعراض البحث :

يكون تمثيل الحروف والأرقام والعلامات الأخرى داخل الحاسبة حسب الترميز القياسي الأمريكي للمعلومات المتبادلة (ASCII: American Standard Code for Information Interchange) وهذا الترميز يستخدم الأرقام من ٠ إلى ٢٥٥، حيث أن كل رقم يمثل بايت واحد والترميز بهذه الصيغة يسهل نقل النصوص بين الحاسبات و الأجهزة الملحقة، كونها صيغة قياسية موحدة عالميا".

وتتكون الصورة من مصفوفة من العناصر (Pixels) حيث يمثل كل عنصر من عناصرها بقيمة حسب نوع الصورة، فالثنائية (Binary Image) تتكون من لونين، حيث يمثل كل عنصر من عناصرها بيت واحد قيمته إما (٠) للون الأسود أو (١) للون الأبيض.

النوع الآخر هو الصور أحادية اللون (ذات تدرج اللون الواحد) (Monochrome) والتي يمثل فيها عنصر الصورة بعدد من البتات من خلالها يمكن معرفة عدد التدريجات اللونية في هذه الصورة، فمثلا إذا تم

تمثيل العنصر بثلاث بتات فإن ذلك يدل على أن لهذه الصورة على الأكثر ثمان من التدريجات ،وإذا مثل بثمان بتات (بايت واحد) فان الصورة لها على الأكثر ٢٥٦ تدرج لوني ، إذ تمثل القيمة (٠) لا لون والقيمة (٢٥٥) أعلى قيمة لذلك اللون وبين هاتين القيمتين يكون تدرج اللون.

أما الصور الملونة فتمثل بثلاث حزم من بيانات صورة أحادية اللون، وان كل حزمة تمثل لون مختلف عن الحزمتين الباقيتين ومعظم الصور الملونة ممثلة بالألوان الأساسية الثلاثة الأحمر، الأخضر ، الأزرق (Red ,Green ,Blue)، وإن كل عنصر ممثل بثلاث بايتات (24bits) كل منها يحمل قيمة لون من الألوان الأساسية أي بالإمكان الحصول على (١٦٧٧٧٢١٦) لون مختلف، ويتم احتساب قيمة أي تدرج لوني في معظم تطبيقات الحاسوب بالمعادلة الآتية [٧] :-

$$Color = (Blue * 65536) + (Green* 256) + Red \quad \ldots\ldots\ldots\ldots\ldots\ldots (1)$$

تتم عملية الإخفاء بصورة عامة بتحويل الملف المراد إخفائه إلى سلسلة من البتات يتم إخفاؤها داخل بايتات عناصر الصورة وذلك باستبدال عدد من بتات بايت 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 لان قدرة العين البشرية على التميز بين التدريجات اللونية المتقاربة ضعيفة فضلا عن ضعف قدرتها في التمييز بين التدريجات الغامقة [٨] [٩].

في بعض طرائق الإخفاء السابقة يتم إخفاء النصوص أو المخططات ثنائية اللون داخل الصور الثنائية [١٠]. أما في الصور أحادية اللون فيتم إخفاء بتين على الأكثر في بتات بايت عنصر الصورة .وفي هذه الحالة يكون تأثير الإخفاء على الصورة قليل جدا [١١] ، وفي طرائق أخرى تخفى البتات داخل عناصر الصورة في أماكن متفرقة ويلزم ذلك عمل خارطة أو جدول لمواقع التوزيع ، وعندها يستوجب وجود الخارطة أو الجدول أو الصورة ألأصلية لاستخلاص بتات الملف المخفي مما يثير الشك لدى المتطفلين وبالتالي يزيد احتمال اكتشاف النص.

وبأسلوب آخر يتم تحويل حروف النص إلى سلسلة من البتات ثم إخفاء كل ٤ بت في بايت عنصر الصورة، وفي هذه الطريقة يمكن إخفاء كمية أكبر من حروف النص [١٢].

إن إخفاء بتات الملف داخل عناصر الصورة بشكل متسلسل (عنصر بعد عنصر) يزيد من احتمالية اكتشاف النص بطرق تحليل الصورة أو العمليات الإحصائية ، عليه تم اقتراح استخدام الأسلوب الآتي .

٤- خوارزمية الإخفاء المبعثر المقترحة:-

تعتمد الطريقة المقترحة في عملية الإخفاء على الصور أحادية اللون أو الصور الملونة. فعند انتخاب الصورة أحادية اللون ،يجزأ بايت كل حرف من حروف النص إلى جزأين كل منهما يحوي أربعة بتات حيث يخفى كل جزء في بايت عنصر من عناصر الصورة وبهذا يلزم عنصرين من عناصر الصورة لإخفاء حرف واحد.

أما في الصورة الملونة فيتم تجزئة بايت الحرف 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، وبالرجوع إلى نظام الرؤية البشرية [HVS: Human Visualize System] الذي يشير الى ان العين البشرية اكثر تحسسا للون الأزرق من اللونين الآخرين (الأحمر والأخضر) [٧]، عليه تم اعتماد

صيغة إخفاء البتين في اللون الأزرق (B) والجزأين الآخرين من البتات الثلاث في اللونين الآخرين الأخضر والأحمر (G,R)، وهكذا يلزم عنصر واحد من عناصر الصورة الملونة لإخفاء حرف واحد.

ولزيادة دقة الإخفاء وتقليل احتمالية الكشف عن النص داخل الصورة، لأن فرصة الكشف عن الإخفاء المرتب أكبر، تتم عملية الإخفاء المبعثر بإخفاء أجزاء بايت حروف النص داخل بايتات عناصر الصورة بطريقة غير متتابعة إذ ستكون المسافة بينها غير منتظمة ، وتحدد هذه المسافة (S) عن طريق أخذ قيمة عدد من بتات عنصر الصورة (N) الناتج بعد عملية الإخفاء الحالية وتضاف إليها قيمة معينة كمفتاح (Key)، سيطلق على هذه المسافة بمسافة البعثرة حيث ستضاف هذه المسافة إلى موقع العنصر الحالي (في مصفوفة الصورة) إلى الاحداثي الصادي لتحديد موقع عنصر الصورة اللاحق الذي ستتم فيه عملية الإخفاء.

فمثلا لو كان موقع العنصر الحالي E هو (٥، ٢٥) وأصبحت قيمة البايت بعد الإخفاء ($(205)_{10}$=(٥، ٢٥)E) وعدد البتات المختارة لإضافة قيمتها هو (٣) بت وقيمة المفتاح تساوي (٧) فسيكون موقع العنصر اللاحق كما يأتي :

$S= (N)_2 +(Key)_{10}$ .....(2)

$(205)_{10} = (1100\ 1\underline{101})_2$

$S = (\underline{101})_2 +(7)_{10} = (5+7)_{10} =(12)_{10}$

$E_n = E(25 , 5 + S) = E(25, 17)$

إن إضافة المفتاح تعد وسيلة أمان لكي لا يتم الإخفاء في نفس الموقع الحالي عندما تكون قيمة البتات المختارة تساوي صفر. والمثالين التاليين يوضحان كيفية إخفاء حرف في عنصر الصورة الأحادية اللون والملونة.

١- إخفاء الحرف (k) في عنصر صورة أحادية اللون E_1 حيث أن موقع العنصر الأول هو (٧ ، ٢) والقيمة اللونية

للعنصر هي (١٣٢) وقيمة المفتاح (10) وعدد البتات المختارة لإضافة قيمتها هي (٤) بت.

أ- تحويل قيمة الحرف إلى الثنائي.

$k=(107)_{10}=(0110\ 1011)_2$

ب- تجزئة بايت الحرف إلى جزأين وذلك بإجراء عملية (AND) بين قيمة بايت العنصر والقيمة

٢(٠٠٠٠١١١١) للحصول على الجزء الأول (P1) ثم عملية (AND) بين قيمة بايت العنصر والقيمة

٢ (٠٠٠٠ ١١١١) و تزحيف الناتج أربع مراتب إلى اليمين للحصول على الجزء الثاني (P2).

$P1=(1011)_2$

$P2=(0110)_2$

ج- تحويل القيمة اللونية للعنصر إلى الثنائي .

$E_1(2 ,7) =(132)_{10}=(1000\ 0100)_2$

د- إخفاء الجزء الأول في (LSB_s) من بايت عنصر الصورة .

E_{1new}=(1000

$\underline{1011})_2=(139)_{10}$

ه- حساب مسافة الإخفاء.

$S=(\underline{1011})_2+(10)_{10}=21$

و- حساب عنوان العنصر اللاحق وذلك بإضافة قيمة (S) إلى قيمة الاحداثي الصادي.

$E_n=(2,7+21)$ =

(2,28)

ز- تحويل القيمة اللونية للعنصر اللاحق إلى الثنائي (نفرض أن القيمة تساوي (١٤٥)).

$E_n(2\ ,28)=(145)_{10}=(1001\ 0001)_2$

ح- إخفاء الجزء الثاني في (LSB_s) من بايت عنصر الصورة.

$E_{n\ new}$=(1001

$0110)_2=(150)_{10}$

٢- إخفاء الحرف (k) في عنصر الصورة الملونة E_1 وموقع العنصر الأول هو (٧ ، ٢) ، علما أن قيمة اللون الأحمر (R=200)، اللون الأخضر (G=210) واللون الأزرق (B=180)، وقيمة المفتاح (٩) وعدد البتات المختارة لإضافتها هي (٤) بت.

أ- تحويل قيمة الحرف إلى الثنائي

$k=(107)_{10}$=(0110

$1011)_2$

ب- تجزئة بايت الحرف إلى ثلاثة أجزاء وذلك بإجراء عملية (AND) بين قيمة بايت العنصر والقيمة

٢ (٠٠١١ ٠٠٠٠) للحصول على الجزء الأول ثم عملية (AND) بين قيمة بايت العنصر والقيمة

٢(1100 0001) و تزحيف الناتج مرتبتين إلى اليمين للحصول على الجزء الثاني. ثم عملية (AND) بين

قيمة بايت العنصر والقيمة ٢(0000 1110) و تزحيف الناتج خمسة مراتب إلى اليمين للحصول على الجزء

الثالث.

$P1=(11)_2$

$P2=(010)_2$

$P3=(011)_2$

ج-تحويل القيمة اللونية للعنصر إلى الثنائي .

$R=(200)_{10}=(1100\ 1000)_2$

$G=(210)_{10}=(1101\ 0010)_2$

$B=(186)_{10}=(1011\ 1010)_2$

د- إخفاء الجزء الأول في (LSB_s) من بايت اللون الأحمر.

$R_{new}=(1100\ 10\mathbf{11})_2$

$=(203)_{10}$

ه - إخفاء الجزء الثاني في (LSB_s) من بايت اللون الأخضر.

$G_{new}=(1101\ \ =(210)_{10}$

$0\mathbf{010})_2$

و- إخفاء الجزء الثالث في (LSB_s) من بايت اللون الأزرق.

$B_{new}=(1011\ 1\mathbf{011})_2=(187)_1$

ز-حساب مسافة الإخفاء بأخذ (٤) بت من اللون الأخضر أو أي لون أخر.

$S=(\underline{0010})_2+(9)_{10}=11$

ح- حساب عنوان العنصر اللاحق.

$E_n=(2\ ,7+11)=(2\ ,18)$

تجدر الإشارة هنا إلى انه من الضروري تقدير حجم الصورة المناسب لإخفاء كامل النص، ويمكن احتساب ذلك باستخدام المعادلات التالية والتي تم استنتاجها عن طريق الإحصاءات التي أجريت على مجموعة مختلفة من الصور بعد تطبيق عملية الاخفاء المبعثر عليها وكما يلي:-

حجم الصورة أحادية اللون = عدد حروف الملف × ٢ × ٤١٣ أعلى مسافة للإخفاء .....(٣)

حجم الصورة الملونـــــة = عدد حروف الملف × ٤١٣ أعلى مسافة للإخفاء .....(٤)

ويمكن تلخيص خوارزمية الإخفاء في الصور أحادية اللون كما في الخطوات الآتية :

١- عرض ملف النص المراد إخفاءه بوساطة احد البرامج التطبيقية لعرض النصوص.

٢- إضافة رمز خاص في نهاية النص، لغرض التوقف عند ظهوره في عملية فك الإخفاء.

٣- اختيار حجم الصورة المناسب لعملية الإخفاء.

٤- تعيين موقع عنصر الصورة الذي سيتم فيه إخفاء أول حرف من حروف النص.

٥- قراءة الحرف من النص وإيجاد صيغة الآسكي المقابلة له بالبايت ثم يجزأ البايت إلى جزأين كل جزء منهما

يتكون من (٤) بت.

٦- قراءة القيمة اللونية لبايت عنصر الصورة .

٧- استبدال بتات بايت عنصر الصورة في موقع البتات الأقل أهمية ببتات الجزء الأول لتكوين قيمة البايت الجديد

للعنصر ثم تحويلها إلى القيمة اللونية. وبعد ذلك تحديد موقع العنصر اللاحق الذي ستتم فيه عملية الإخفاء، وذلك

بحساب مسافة الإخفاء وإضافتها إلى موقع العنصر الحالي.

٨- تكرار الخطوات (٦، ٧) لخزن الجزء الثاني من بايت الحرف.

٩- الرجوع إلى الخطوة (٥) لحين انتهاء حروف النص.

١٠- خزن الصورة لاستخدامها فيما بعد أو إرسالها عبر شبكات الاتصال أو عن طريق البريد الالكتروني.

وتتم عملية استرجاع النص المخفي داخل الصورة أحادية اللون بالخطوات الآتية:

١- عرض صفحة فارغة لأحد البرامج التطبيقية لعرض النصوص.

٢- عرض الصورة التي تحمل النص.

٣- تحديد موقع عنصر الصورة الذي يحمل الجزء الأول من الحرف الأول من حروف النص المخفي، وحسب

المفتاح الذي تم الاتفاق عليه بين المرسل والمستقبل .

٤- قراءة القيمة اللونية لعنصر الصورة وتحويلها إلى صيغة البايت وأخذ البتات الأربعة المستبدلة وخزنها في موقع

معين (حيث يخصص موقعان في كل موقع يتم خزن أحد جزئي الحرف).

٥- تحديد عنصر الصورة اللاحق وذلك بحساب مسافة الإخفاء وإضافتها إلى موقع العنصر الحالي.

٦- تكرار الخطوتين (٤، ٥) لكي يكتمل خزن جزئي الحرف وتحديد عنصر الصورة اللاحق.

٧- تجميع جزئي الحرف لتكوين بايت الحرف ثم تحويل قيمته إلى الآسكي ثم إلى شكل الحرف ووضعه في صفحة

محرر النصوص.

٨- تكرار الخطوات (٤ ، ٥، ٦، ٧) لحين ظهور الرمز الخاص بنهاية النص.

٩- خزن النص داخل الحاسبة للإفادة منه لاحقا.

أما خوارزمية الإخفاء في الصور الملونة فيمكن إجمالها بالخطوات الآتية :

١-عرض ملف النص المراد إخفاءه بوساطة احد البرامج التطبيقية لعرض النصوص.

٢-إضافة رمز خاص في نهاية النص،للاستفادة منه عند استرجاع الإخفاء.

٣-اختيار حجم الصورة المناسب لعملية الإخفاء.

٤-تعيين موقع عنصر الصورة الذي سيتم إخفاء أول حرف من حروف النص فيه .

٥-قراءة الحرف من النص وإيجاد صيغة الآسكي المقابلة له بالبايت، ثم يجزأ البايت إلى ثلاثة أجزاء الجزء الأول

٦- يحوي على (٢) البتين الأولين أما الجزأين الثاني والثالث فكل منهما يحوي على (٣) بتات بالتتابع.

٧- قراءة القيمة اللونية لعنصر الصورة باستخلاص قيم البايتات الثلاثة الممثلة للألوان الأساسية (الأحمر، الأخضر

والأزرق) (R,G,B).

٨-استبدال بتات بايت كل لون من الألوان الثلاثة ببتات أحد أجزاء الحرف في موقع البتات الأقل أهمية لتكوين قيمة

بايتات الألوان الثلاثة الجديدة للعنصر.

٩-تحديد موقع العنصر اللاحق الذي ستتم فيه عملية الإخفاء وذلك بحساب مسافة البعثرة (التزحيف) وإضافتها إلى
موقع العنصر الحالي.
١٠- تكرار الخطوات (٥ ، ٦ ، ٧ ،٨) لحين انتهاء حروف النص.
١١- خزن الصورة لاستخدامها فيما بعد أو إرسالها بالبريد الالكتروني.

وخوارزمية استرجاع النص المخفي داخل الصورة الملونة تكون كالآتي :-

١- عرض صفحة فارغة لأحد البرامج التطبيقية لعرض النصوص.
٢- عرض الصورة التي تحمل النص.
٣- تحديد موقع عنصر الصورة الذي يحمل الحرف الأول من حروف النص المخفي .
٤- قراءة القيمة اللونية لعنصر الصورة واستخلاص قيم البايتات الثلاثة التي تمثل اللون الأحمر والأخضر والأزرق،
ثم تؤخذ البتات المستبدلة في عملية الإخفاء من كل لون من الألوان ويتم تجميعها لتكوّن قيمة بايت الحرف.
٥- تحويل قيمة الحرف من صيغة الآسكي إلى الشكل الذي يمثله ويوضع في صفحة محرر النصوص .
٦- تحديد موقع العنصر اللاحق الذي ستتم فيه عملية الإخفاء وذلك بحساب مسافة الإخفاء وإضافتها إلى موقع العنصر الحالي.
٧- تكرار الخطوات (٦،٥،٤) لحين ظهور الرمز الخاص بنهاية النص.
٨- خزن الصورة لاستخدامها فيما بعد أو إرسالها عبر شبكات الاتصال أو عن طريق البريد الالكتروني.

لمعرفة جودة الصورة الناتجة بعد عملية الإخفاء يتم حساب معادلة جذر متوسط مربع الخطأ (Root Mean Square error) بين الصورة الأصل والصورة الناتجة وكما يلي [7] :-

$$e_{RMS} = \sqrt{\frac{1}{N^2}\sum_{r=0}^{N-1}\sum_{c=0}^{N-1}[\bar{I}(r,c) - I(r,c)]^2} \qquad \text{..... (٥)}$$

حيث أن:

e_{RMS} : جذر متوسط مربع الخطأ للصورة.
N: بُعد الصورة (بالبكسل).
$\bar{I}(r,c)$: يمثل عنصر الصورة بعد الإخفاء.
$I(r,c)$: يمثل عنصر الصورة قبل الإخفاء .

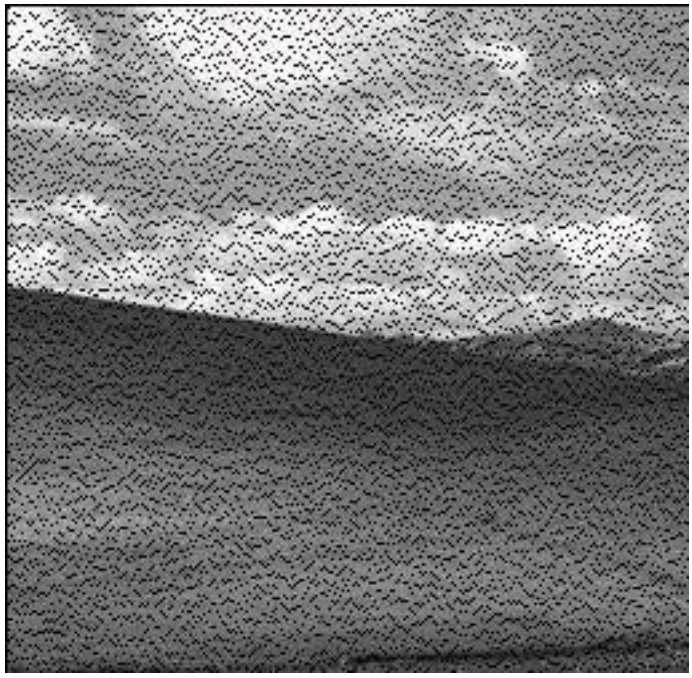
٥- النتائج والمناقشة:

تم تطبيق خوارزمية الإخفاء المبعثر لإخفاء نصوص متنوعة في نماذج صور ذات تفاصيل مختلفة قياس (٢٥٦*٢٥٦) عنصر، أحادية اللون وملونة ، وحساب نسبة الخطأ بين الصورة الأصلية والصورة الناتجة بعد عملية الإخفاء باستخدام المعادلة (٥) ، وذلك من خلال تنفيذ برنامج بلغة (Visual Basic) أعد لهذا الغرض ، حيث أخفي ما يقرب من (٤٥٠٠) حرف داخل صورة أحادية اللون وما يقرب من (٩٠٠٠) حرف داخل صورة ملونة وبمسافة إخفاء (S) كان فيها N=3 ، Key=3 .

وكانت نسبة الخطأ بصورة عامة قليلة حيث تراوحت بين (0.17 - 0.05) ولم يلاحظ ظهور أية تشوهات على الصورة الناتجة، لكلا النوعين من الصور، الشكل (١) والشكل(٢).

(أ)

(ب)



الشكل (١)
يبين التوزيع المبعثر لحروف النص المخفي داخل عناصر صورة أحادية اللون
ا- الصورة الأصلية، ب-الصورة بعد الإخفاء، ج- توزيع الحروف داخل الصورة

(أ)

(ب)

(ج)

٦- الاستنتاجات :

- أثبتت الطريقة المستخدمة نجاحا في عملية إخفاء مختلف أنواع النصوص في الصور أحادية اللون والملونة.
- إن مسافة البعثرة بين عناصر الصورة تودي 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 السراق أو المتطفلين.
- إن استخدام قيمة المفتاح (key) مع قيمة جزء من عنصر الصورة الناتج بعد عملية الإخفاء يمكّن من التحكم بمسافة البعثرة وبالتالي عمل موازنة (tradeoff) بين حجم النص المراد إخفاءه وحجم الصورة الغطاء.
- نسبة الإخفاء في هذه الطريقة يكون اقل قياسا بالطرق التقليدية لوجود المساحات المتروكة دون إخفاء بسبب اعتماد آلية التزحيف في العملية.
- يفضل استخدام الصور ذات تفاصيل كثيرة (أي الصور عالية النسيج) في عملية الإخفاء.
- إن إجراء أية عملية كبس أو تحسين للصورة الحاملة للنص المخفي أو تغيير لامتدادها سوف يؤدي إلى ضياع كل
  أو جزء من النص المخفي وتعذر استرجاعه بالكامل.
- لزيادة كفاءة الإخفاء في الصورة الملونة فانه بالإمكان توزيع إخفاء الأجزاء الثلاثة على الألوان الثلاث على أن
  يتم احتساب مقدار التزحيف لكل لون على حدا وبذلك يكون كل جزء من أجزاء الحرف المراد إخفائه في عنصر
  مختلف من عناصر الصورة كون ذلك يقلل من احتمالية الكشف.

المصادر:-

[1] D. Kohn, "The Codebreakers: The Story of Secret Writing" , *Scribner*, New York, 1996.

[2] W. Stallings," Cryptography and Network Security", *Prentice Hall*, New Jersey, 1999.

[3]. Lenti, Jozsef, "Steganographic Methods". *Budapest: Budapest University of Technology*
and Economics, 2000.

[4]. Johnson, N. F., Duric, Z., Jajodia, S., " Information Hiding: Steganography and Watermarking- Attacks and Countermeasure", *Kluwer Academic Press. Norwrll*, MA, New York, The Huague, London, 2000.

[5]. Prof Rudko , "A Survey of Techniques for Digital Watermarking", *Chris Shoemaker Independent Study*, EER-290. Spring 2002.

[6]Marvel, Lisa M, et al, "Hiding Information in Images". *Aberdeen Proving Ground, MD: US Army Research Laboratory*, 1998.

[7] Scott E Umbaugh " Computer Vision and Image Processing : A Practical Approach Using CVIPtools" , (1998),.

[8] Chin-Chen Chang, Min-Hui Lin and Yu-Chen Hu, "A fast and secure image hiding scheme based on LSB substitution" , *International journal of pattern recognition and artificial intelligence*, Vol. 16, No. 4 (2002), 399-416.

[9] Chi-Kwong Chan and L. M. Chen, "hiding data in images by simple LSB substitution", *Pattern Recognition*, 37 (2004), 469-474.

[10] Yu-Yuan Chen, Hsiang-Kuang Pan, and Yu-Chee Tseng, "A Secure Data Hiding Scheme for Two-Color Images," *IEEE Symp. on Computers and Communications*, 2000.

[11] Ran-Zan Wang, Chi-Fang Lin and Ja-Chen Lin, "Hiding data in images by optimal moderately significant bit replacement", *Electronics Letters*, Vol. 36, NO. 25, December 2000.

[12] Alkhraisat Habes, "Information Hiding in BMP image Implementation, Analysis and Evaluatio...,