المجلة العراقية للعلوم الإحصائية (25) 2013
عدد خاص بوقائع المؤتمر العلمي السادس لكلية علوم الحاسوب والرياضيات
ص ص[398-414]

استخدام الألوان لإخفاء النص المشفر في الصور الرقمية

سندس خليل إبراهيم* ميعاد عبد الرزاق احمد كشمولة**

الملخص

تم في هذا البحث اقتراح طريقة تدمج تقنية التشفير مع الإخفاء، فقد تم تشفير نص ثم إخفاؤه في صورة باستخدام الألوان، وذلك لتكون البيانات المرسلة في منأى عن اكتشافها ويصعب فك تشفيرها إذا تم الكشف عن وجودها، وقد تم عرض الطريقة المقترحة لتشفير وإخفاء البيانات السرية في الصورة، بالاعتماد على المفتاح السري الذي يمثل الجدول والدرجة اللونية الأساس باستخدام برنامج معالجة النصوصMicrosoft Word 2007، أما في عملية فك الإخفاء والتشفير فقد تم تحويل حروف الرسالة المخفية إلى نص لاستخلاص الرسالة أو البيانات المخفية من الصورة الرقمية، وبالاعتماد على المفتاح السري لعملية التشفير والإخفاء باستخدام طرائق معالجة الصور الرقمية للحصول على حروف الرسالة السرية المستلمة، وقد تم تطبيق هذه الطريقة في عملية التشفير والإخفاء على نصوص بأطوال مختلفة، وكانت قيمة PSNR لجميع الصور المطبقة وبدرجات لونية مختلفة (∞)، كما كانت قيمة الارتباط لإيجاد التطابق مساوية للواحد(1) ولجميع الصور أيضا، مما يثبت أن الرسالة المخفية بهذه الطريقة لا تثير الشك عندما يشاهدها المتطفل وهذا يثبت كفاءة الطريقة المقترحة.

Using the Colors to Hide Encrypted text in the Digital Images

Abstract

This paper presents a method mixes encryption technique with hiding. In which a text encrypted and then hid in an image by using colors, for the reason that the transferred data to be away from doubt and to be difficult to analyze if there is doubt about it. The proposed method depends on secret key in a table and a color value of the text in Microsoft word 2007. In the recovery step, depending on the secret key and by using digital image processing methods, letters of the hidden message converted to a text to extract the message from the digital image.

*مدرس/ قسم علوم الحاسوب/ كلية علوم الحاسوب والرياضيات / جامعة الموصل
**باحثة / قسم الرياضيات / كلية علوم الحاسوب والرياضيات / جامعة الموصل

تاريخ استلام البحث 2013/9/30 ـــــــــــــــــــ **تأريخ القبول** 2013/11/21

Various text length and various color values were applied in the proposed method.Results show that the values of the PSNR were (∞), and the values of correlation coefficient were equal to (1) for all applied images. That proves that message hidden by using this method is above suspicion for analysts, which means the proposed method is very efficient.

1 - المقدمة

منذ العهود القديمة كان هناك حاجة ملحة لإيجاد وسائل سرية للحفاظ على أمنية الرسائل المرسلة، ولكن مع تطور وسائل الاتصال وتطور علم الحاسوب أصبحت هناك حاجة ملحة لإيجاد وسائل أكثر تطوراً لخدمة هذا الغرض، فكان ظهور التشفير وعلى الرغم من كونه طريقة جيدة لحفظ المعلومات إلا انه قابل للاكتشاف 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 الذي يعتمد على مبدأ أن الرسالة المرسلة تكون غير مرئية لأي شخص بواسطة إخفائها داخل إحدى وسائل الاتصال(الصوت والصورة والنص والفيديو ومساحات القرص الصلب وبروتوكولات الشبكة والبرامج....الخ)(البلاسيني، 2009)(الجبوري، 2011).

2 - الدراسات السابقة

لا يعد إخفاء البيانات من المواضيع الجديدة في الوقت الحالي إذ قام العديد من الباحثين في السابق بالعمل في هذا المجال، وحاول الباحثون إيجاد تقانات إخفاء متطورة تواكب التطور السريع في تقانات الإخفاء.

فقد قدم Sahoo وTiwri في عام 2008 بحثا لإخفاء نص في ملف هجين(صورتين)، حيث تم إخفاء النص في الصورة الأولى التي تسمى صورة الحاوية، باستبدال كتلة ثنائية كاملة بحرف من النص، أي أن كل نقطة ضوئية سيتم إخفاء ثلاثة حروف فيها، ثم حشرها في صورة أخرى تسمى صورة المساندةو إن التشويه الذي سيحدث يكون غير ملحوظ بحيث أن صورة الحاوية تبدو وكأنها جزء من صورة المساندة(Sahoo and Tiwari, 2008). وفي عام 2009 اقترحت الباحث البلاسيني نظاما" امنيا" لإخفاء معلومات سرية، وإرسالها بصورة مخفية عبر شبكات الاتصال، باستخدام تقنيتين من تقانات إخفاء المعلومات، الأولى الكتابة المغطاة (Steganography) ودمجها مع الشبكات العصبية لإخفاء المعلومات السرية باستخدام الإخفاء في الخلية الثنائية الأقل أهمية بعد تشفيرها باستخدام القنوات المخفية من نوع قناة الخزن

المخفية(Covert Storage Channel) لإخفاء بيانات نصية أو صورة تحوي بيانات سرية في بروتوكولات مختلفة (البلاسيني، 2009).

بينما في عام 2010 قدم كل من Rana وSingh بحثا لإخفاء ملف نصي في الصور، وذلك بتشفير الملف النصي، ثم تحويله إلى النظام الثنائي ثم تقسيمه إلى أربعة أجزاء ويتم تقسيم الصورة أيضا إلى أربعة أجزاء ويتم إخفاء كل جزء من البيانات بجزء من الصورة بصورة عشوائية باستخدام تقنية الإخفاء في الخلية الثنائية الأقل أهمية (LSB) Least Significant Bit (Rana and Singh, 2010) .

اما في عام 2011 اقتراح كل من إبراهيم وآخرون طريقة للإخفاء بالاعتماد على جزء من معلومات فضاء كارهونين لويف ثم استخدام طريقة (RLE) Run Length Encoding لكبس المعلومات الناتجة ثم تطبيق طريقة(LSB) لإخفاء البيانات باستخدام صيغة عشوائية في اختيار مواقع خزن المعلومات في الصورة الغطاء بالاعتماد على معادلة رياضياتية. وقد أظهرت الطريقة كفاءة عالية في الكبس والإخفاء في الصور الرقمية(إبراهيم وآخرون،2011). وقد اقترح Lin في عام 2012 مخطط قابل للعكس لإخفاء البيانات مبني على معاملات متنوعة باستخدام Discrete Cosine Transform(DCT) للصورة حيث يتم تحويل صورة الغطاء الى عدة ترددات مختلفة ويتم إخفاء البيانات في الأجزاء ذات الترددات العالية(Lin, 2012). بينما في عام 2013 عرض الباحث يوسفو الباحث إبراهيم 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 (يوسف وإبراهيم، 2013). لذا تم في هذا البحث دراسة هذه الطريقة وتم تطويرها لتشمل الإخفاء في الطبقات الثلاثة حيث تم تقديم طريقة مقترحة تدمج بين التشفير والإخفاء.

3- مساوئ الإخفاء في النص

بما أن طرائق الإخفاء في النص ضعيفة وغير كفوءة وتعد مهمة وصعبة نوعا ما، لأن النص يحوي على بيانات متكررة قليلة لاستبدالها بالرسالة السرية، ولا تصلح للتطبيق واهم مساوئها ما يأتي (يوسف، 2011) (يوسف وإبراهيم، 2013) :

- تحتاج إلى نص كبير لإخفاء رسالة صغيرة .
- تحتاج بعض الطرائق إلى تقانات معقدة بوصفها طريقة الإخفاء في الكلمات .
- إمكانية ملاحظة التغيرات بالرسالة الحاملة مقارنة بالنص الأصلي .

- احتمالية تحطم نظام الإخفاء في حالة عرض الرسالة باستخدام أحد التطبيقات الخدمية (Word)، نتيجة لاحتوائه على بعض المعالجات مثل التنسيق التلقائي الذي يودي إلى تغيير طول الفراغات بين الكلمات(هذا بالنسبة للنص الانكليزي).
- الإخفاء يقتصر على الرسالة النصية مع صعوبة إخفاء أنواع أخرى من الرسائل مثل المعادلات والمخططات والصور والأصوات، ومن الجدير بالذكر أن معظم التقانات التي تستخدم النص تحتاج إلى معرفة النص الأصلي لغرض استخراج الرسالة .

4- مساوئ الإخفاء في الصور

تعد الصور الرقمية من أفضل طرائق الإخفاء المستخدمة بكثرة، إلا أن هناك بعض المساوئ عند تضمين المعلومات في الصور وهي(يوسف، 2011) (يوسف وإبراهيم، 2013):

- حجم الغطاء المراد إخفاء المعلومات به يجب أن يكون كبيرا"، اكبر من المعلومات المخفية بحوالي الضعف كي لا يستطيع المهاجم أو المراقب كشفه، ومع ذلك أيضا وبسبب حجمها الكبير نسبيا تكون أكثر عرضة للشكوك .
- حدوث ضرر هائل في هذه الطريقة عند كبس الصورة ، لذلك فالمعلومات المخفية سوف تتحطم.

4- هدف البحث

يهدف البحث إلى تشفير بيانات الى بيانات أخرى ثم إخفائها بطريقة لا تودي إلى التأثير في الأخيرة، إذ لا تثير أية شبهة أو شك قد يؤدي إلى كشف حقيقة البيانات، والغرض من عملية التشفير والإخفاء هذه أن لا يعلم المهاجم المحتمل عن وجود هذه البيانات، ثم يتم حمايتها من القراءة أو التغيير عن طريق هذا المهاجم.

5- مقاييس كفاءة خوارزميات الكتابة المغطاة

قيست كفاءة الخوارزمية الجديدة باعتماد المعايير الرئيسة لتقييم كفاءة خوارزميات الكتابة المغطاة وهي كما يأتي (عبد المجيد، 2011):

5-1 قياس نسبة ذروة الإشارة إلى الضوضاء -Peak-Signal-to-Noise Ratio(PSNR):

وهو من أكثر المقاييس استخداماً في قياس مدى تشوه الصورة الناتجة من عملية التضمين stego-image ويحسب من المعادلة الآتية (Gonzalez and Woods, 2008):

$$PSNR = 10\log_{10}\left(\frac{C_{\max}^2}{MSE}\right) in\ dB \text{..... ....(1)}$$

ويحسب Mean Square Error (MSE) من خلال المعادلة الآتية:

$$MSE = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}(S_{xy} - C_{xy})^2 \quad \text{.....(2)}$$

علما أن M, N: تمثلان أبعاد الصورة.

S_{xy}, C_{xy}: تمثلان الصورة الغطاء وstego-image على التوالي.

C_{max}: أعلى قيمة لونية في الصورة وقيمتها الافتراضية في الصور ذات العمق اللوني (8 bit) تساوي 255 .

يمكن حساب مقياس PSNR للصور الملونة عن طريق إيجاد معدل قيم PSNR للمستويات الثلاثة.

2-5 الارتباط Correlation:

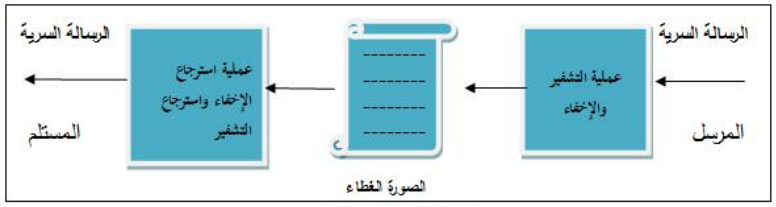
إن الاستخدام الأساس لعملية الارتباط هو لإيجاد التطابق، فإذا كانت الصورة f(x,y) تحتوي على مجموعة من الكيانات والإشكال وأريد تحديد شكل معين أو كيان ضمن تلك الصورة f ولتكن w(x,y) فسيكون الشكل أو الكيان موجودا في المنطقة التي فيها اعلى قيمة للارتباط (المولى، 2007). التعبير الرياضي لعملية الارتباط بين الدالتين f(x,y)،w(x,y) يمثل بالمعادلة الآتية(Gonzalez and Woods,2008):

$$r = \frac{\sum_x \sum_y (f_{xy} - \bar{f})(w_{xy} - \overline{w})}{\sqrt{\sum_x \sum_y (f_{xy} - \bar{f})^2 (\sum_x \sum_y (w_{xy} - \overline{w})^2}} \quad \text{.....(3)}$$

حيث تمثل $f_{x,y}$ الصورة الأولى و$w_{x,y}$ صورة الشكل أو الكيان وتمثل كل من $\overline{f}$ و $\overline{W}$ بـ(average or mean of matrix elements).

6- خطوات العمل باستخدام الخوارزمية المقترحة

تكمن خطوات العمل في عملية تشفير وإخفاء الرسالة السرية، ثم بعد ذلك استرجاع الإخفاء والتشفير ويوضح الشكل (1) المراحل الأساسية في التنفيذ .



الشكل(1) مراحل التنفيذ

6-1 عملية التشفير والإخفاء

خطوات خوارزمية عملية التشفير والإخفاء وهي كما يأتي:

1- البداية .

2- اختيار النص ليكون غطاءا" للرسالة السرية كما في الشكل(2) وتحديد لون الأساس لكل طبقة لونية لجميع أحرف النص الغطاء.

Steganography technique and covert channels to hide the data. The secret data needed to be sent encoded by using Data Encryption Standard (DES) algorithm or by Triple Data Encryption Standard (TDES) algorithm.

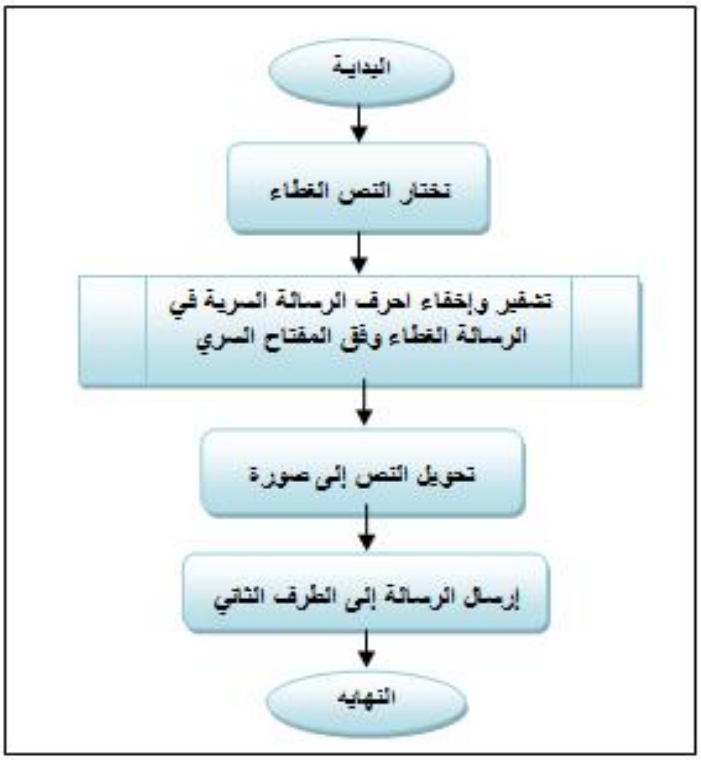
الشكل(2) نص الغطاء المستخدم

3- نحدد نص الرسالة السرية وليكن كمثال(""force 5") بأخذ حرف تلو الأخر، إذ يتم اختيار الطبقة اللونية وتغير الدرجة اللونية وعدد الأحرف المقابلة لكل حرف من حروف الرسالة السرية وعلى وفق الجدول (2) الذي يمثل الحرف وعدد الأحرف المستخدمة في التشفير والطبقة اللونية وزيادة في الدرجة اللونية الذي يمثل مع الطبقة اللونية للأساس المفتاح السري للخوارزمية المقترحة.

4- تحويل النص الغطاء إلى صورة ثم ترسل الرسالة إلى الطرف الثاني (المستلم).

5- النهاية.

والمخطط في الشكل (3) يوضح خطوات خوارزمية التشفير والإخفاء.



الشكل (3) المخطط الانسيابي لخطوات عملية التشفير والإخفاء

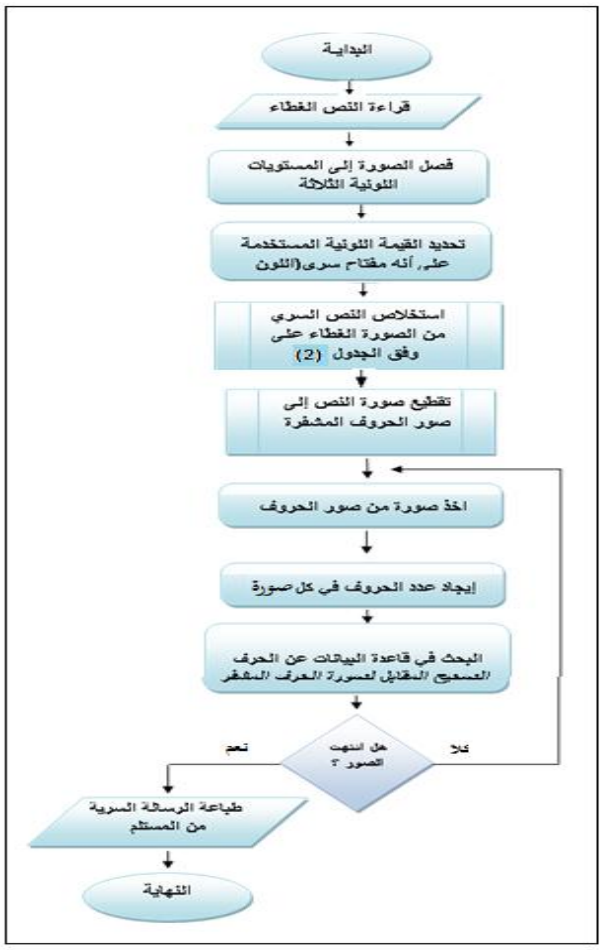
الجدول (2) تشفير الحروف الانكليزية والأرقام والرموز في عملية التشفير والإخفاء

الحرف	عدد الأحرف المستخدمة في التشفير	الطبقة اللونية	الزيادة في الدرجة اللونية	الحرف	عدد الأحرف المستخدمة في التشفير	الطبقة اللونية	الزيادة في الدرجة اللونية
a	1	R	1	w	3	G	2
b	2	R	1	x	4	G	2
c	3	R	1	y	1	G	3
d	4	R	1	z	2	G	3
e	1	R	2	space	3	G	3
f	2	R	2	0	4	G	3
g	3	R	2	1	1	G	4
h	4	R	2	2	2	G	4
i	1	R	3	3	3	G	4
j	2	R	3	4	4	G	4
k	3	R	3	5	1	B	1
l	4	R	3	6	2	B	1
m	1	R	4	7	3	B	1
n	2	R	4	8	4	B	1
o	3	R	4	9	1	B	2
p	4	R	4	:	2	B	2
q	1	G	1	|	3	B	2
r	2	G	1	,	4	B	2
s	3	G	1	!	1	B	3
t	4	G	1	&	2	B	3
u	1	G	2	$	3	B	3
v	2	G	2	%	4	B	3

6-2عملية استرجاع الإخفاء واسترجاع التشفير

أما خطوات الخوارزمية المستخدمة في عملية استرجاع الإخفاء والتشفير هي كما يأتي انظر الشكل(4).

1- قراءة صورة النص الغطاء للرسالة السرية.
2- فصل الصورة إلى المستويات اللونية الثلاثة وهي الأحمر والأخضر والأزرق.
3- تحديد القيمة اللونية المستخدمة على إنها أساس في لون النص الغطاء والذي يعد مفتاحا سريا في هذه الخوارزمية.
4- استخلاص النص السري من الصورة الغطاء في المستويات



الشكل (4) المخطط الانسيابي لخطوات عملية استرجاع الإخفاء واسترجاع التشفير

اللونية الثلاثة وذلك بتقطيع الحروف المشفرة المخفية بالاعتماد على مقدار الزيادة في القيمة اللونية التي سيتم توضيحها في الفقرة التالية.

5- تقطيع صورة النص إلى صور الحروف المشفرة في الدرجة اللونية لكل مستوى لوني.

6- إيجاد عدد الحروف في كل صورة ناتجة من الخطوات السابقة.

7- البحث في الجدول عن الحرف الصحيح المقابل لكل صورة من الصورة الناتجة.

8- تكرر الخطوة 6و7 لكل صور الحروف المشفرة.

9- النهاية.

الشكل (5) يوضح النص المستخدم بوصفه غطاء مع الرسالة السرية، نلاحظ أن الرسالة السرية المضمنة في الرسالة الغطاء لم تدع أي شك للمهاجم بوجود إخفاء في هذه الرسالة .

Steganography technique and covert channels to hide the data. The secret data needed to be sent encoded by using Data Encryption Standard (DES) algorithm or by Triple Data Encryption Standard (TDES) algorithm.

الشكل (5) النص الغطاء مع الرسالة السرية

6-3 تقطيع الحروف المشفرة المخفية

يتم استخلاص النص السري من صورة الغطاء حسب خطوات الخوارزمية الآتية :

1- يتم فصل الطبقات اللونية الثلاث كلا على حدة.

2- استخلاص النص السري من كل طبقة من الطبقات اللونية الثلاث بالاعتماد على القيم اللونية (مقدار درجة الزيادة في اللون مضاف إليها القيمة اللونية الأساس التي تم تحديدها في الخطوة 3 من خوارزمية استرجاع الإخفاء والتشفير).

3- تقطيع الحروف المشفرة المتجاورة إلى صور منفصلة بحيث تحتوي كل صورة على حروف متجاورة مابين 1-4 أحرف .

4- يتم تحديد عدد الكائنات (object) في كل صورة ، التي تمثل عدد الحروف المقابلة للحرف المشفر عن طريق الإيعاز الأتي :

```
[ B,L,N,A] = bwboundaries(im);
```

حيث N هي عدد الكائنات وim هي الصورة التي تحتوي على الحروف وB تمثل نقاط الحدود الخارجية لكل شكل.

5- يتم تحديد الحرف الذي تم إخفاؤه وذلك باستدعاء دالة يكون الإدخال لها هو عدد الكائنات والطبقة اللونية ودرجة القيمة اللونية والإخراج هو الحرف الصحيح حسب الجدول 2.

6- تكرر الخطوة 5 لكل الصور الناتجة من الخطوة 4.

7- طباعة النص الصريح.

8- النهاية.

7- مثال تطبيقي :

تم تطبيق الطريقة المقترحة على الرسالة باللغة الانكليزية كما يأتي:

7-1 عملية التشفير والإخفاء

نختار نصا" معينا" يكون غطاء للرسالة السرية، ثم يتم تلوينه باللون الأساس كما في الشكل (6).

Steganography technique and covert channels to hide the data. The secret data needed to be sent encoded by using Data Encryption Standard (DES) algorithm or by Triple Data Encryption Standard (TDES) algorithm.

الشكل (6) النص الغطاء

ثم نأخذ نص الرسالة السرية وهي مثلا " force 5" حرف تلو الأخر، ونبدأ بعملية التشفير و الإخفاء على وفق الجدول(2) كما يأتي :

1- إخفاء الحرف f برسالة الغطاء باختيار الطبقة اللونية r وعدد الأحرف 2 في اي كلمة في النص مثلا "te " من الكلمة (technique) في الرسالة السرية والدرجة اللونية 2.

2- إخفاء الحرف o برسالة الغطاء باختيار الطبقة اللونية r وعدد الأحرف 3 وهي "cha " من الكلمة (channels) من الرسالة السرية والدرجة اللونية 4 .

3- إخفاء الحرف r برسالة الغطاء باختيار الطبقة اللونية g وعدد الأحرف 2 وهي "da" من الكلمة (data) من الرسالة السرية والدرجة اللونية 1.

4- إخفاء الحرف c برسالة الغطاء باختيار الطبقة اللونية r وعدد الأحرف 3 وهي"sec " من الكلمة (secret) من الرسالة السرية والدرجة اللونية 1.

5- إخفاء الحرف e برسالة الغطاء باختيار الطبقة اللونية r وعدد الأحرف 1 وهي " n " من الكلمة (needed) من الرسالة السرية والدرجة اللونية 2 .

6- إخفاء الفراغ برسالة الغطاء باختيار الطبقة اللونية g وعدد الأحرف 3 وهي "enc" من الكلمة (encoded) من الرسالة السرية والدرجة اللونية 3.

7- إخفاء الرقم 5 برسالة الغطاء باختيار الطبقة اللونية b وعدد الأحرف 1 وهي "b" من الكلمة (by) من الرسالة السرية والدرجة اللونية 1.

8- يتم تحويل الرسالة الغطاء بعد عملية التشفير والإخفاء إلى صورة كما في الشكل(7).

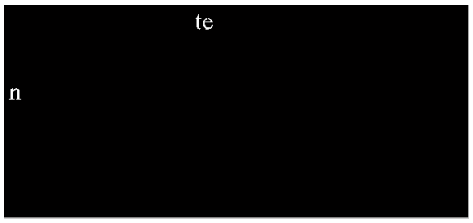
Steganography technique and covert channels to hide the data. The secret data needed to be sent encoded by using Data Encryption Standard (DES) algorithm or by Triple Data Encryption Standard (TDES) algorithm.

الشكل (7) صورة النص الغطاء بعد إخفاء الرسالة السرية

7-2عملية استرجاع الإخفاء واسترجاع التشفير

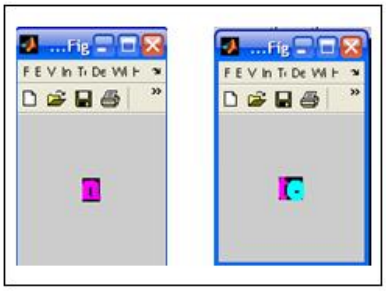
تُستخلص حروف الرسالة المخفية بالاعتماد على المفتاح السري لكل مستوى لوني على حدى، ولكل درجة لونية وحسب مقدار الزيادة على حدى أيضا، علما أن الصورة الأصلية غير متوفرة لدى المستلم وكالاتي :

- الشكل (8) حروف الرسالة السرية المستخلصة من المستوى اللوني الأحمر في الدرجة اللونية(2+)، التي سيتم قطع كل مجموعة منها إلى صورة منفصلة.



الشكل (8) حروف الرسالة المخفية في المستوى اللوني الأحمر في الدرجة اللونية(2+)

- الشكل(9) صو ة كل مجموعة من الأحرف في الشكل (8) في صورة مستقلة.

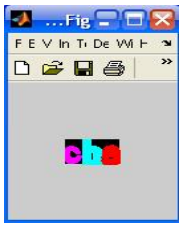


الشكل (9) حروف الرسالة السرية المقطعة من الصورة في المستوى اللوني الأحمر ذات الدرجة اللونية (2+)

- الشكل (10) حروف الرسالة السرية المستخلصة من المستوى اللوني الأحمر في الدرجة اللونية(4+) ، التي سيتم قطع كل مجموعة منها إلى صورة منفصلة.

- الشكل (11) صورة كل مجموعة من الأحرف في الشكل (10) في صورة مستقلة.

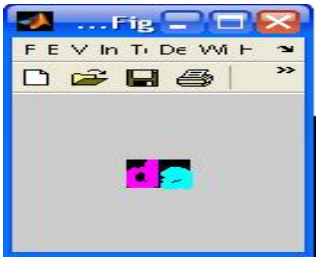
الشكل (10) حروف الرسالة المخفية في المستوى اللوني الأحمر في الدرجة اللونية (+4)



الشكل (11) حروف الرسالة السرية المقطعة من الصورة في المستوى اللوني الأحمر ذات الدرجة اللونية (+4)

- الشكل (12) حروف الرسالة السرية المستخلصة من المستوى اللوني الأخضر في الدرجة اللونية(+1)، التي سيتم قطع كل مجموعة منها إلى صورة منفصلة.
- الشكل (13) صورة كل مجموعة من الأحرف في الشكل (12) في صورة مستقلة

الشكل (12) حروف الرسالة المخفية في المستوى اللوني الأخضر في الدرجة اللونية(1+)



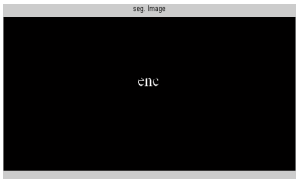
الشكل (13) حروف الرسالة السرية المقطعة من الصورة في المستوى اللوني الأخضر ذات الدرجة اللونية (+1)

- الشكل (14) حروف الرسالة السرية المستخلصة من المستوى اللوني الأحمر في الدرجة اللونية(+1) ، التي سيتم قطع كل مجموعة منها إلى صورة منفصلة.
- الشكل (15) صورة كل مجموعة من الأحرف في الشكل (14) في صورة مستقلة.

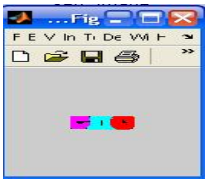
الشكل (14) حروف الرسالة المخفية في المستوى الدرجة اللونية (+1)

الشكل (15) حروف الرسالة السرية المقطعة من الصورة اللوني الأحمر في في المستوى اللوني الأحمر ذات الدرجة اللونية (+1)

- الشكل (16) حروف الرسالة السرية المستخلصة من المستوى اللوني الأخضر في الدرجة اللونية(+3)، التي سيتم قطع كل مجموعة منها إلى صورة منفصلة.
- الشكل(17) صورة كل مجموعة من الأحرف في صورة مستقلة.

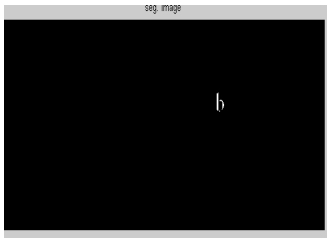


الشكل (16) حروف الرسالة المخفية في المستوى اللوني الأخضر في الدرجة اللونية(3+)



الشكل (17) حروف الرسالة السرية المقطعة من الصورة في المستوى اللوني الأخضر ذات الدرجة اللونية (3+).

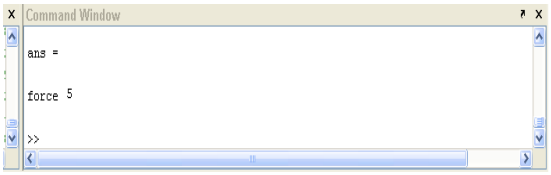
- الشكل (18) حروف الرسالة السرية المستخلصة من المستوى اللوني الأزرق في الدرجة اللونية(1+)، التي سيتم قطع كل مجموعة منها إلى صورة منفصلة.
- الشكل (19) صورة كل مجموعة من الأحرف في الشكل (18) في صورة مستقلة.



الشكل (18) حروف الرسالة المخفية في المستوى اللوني الأزرق في الدرجة اللونية (1+)

الشكل (19) حروف الرسالة السرية المقطعة من الصورة في المستوى اللوني الأزرق ذات الدرجة اللونية (1+).

- الشكل (20) يوضح الرسالة الصحيحة بعد استرجاع الإخفاء والتشفير.



الشكل (20) الناتج النهائي بعد استرجاع الإخفاء والتشفير

8- مناقشة النتائج

تم تطبيق الطريقة المقترحة على عدة رسائل، وكانت النتائج كما يأتي:

1- بما أنه توجد عدة طرائق لاكتشاف الرسالة المخفية أشهرها هو اكتشاف التشويش أو التشوه في الصورة باستخدام مقاييس خاصة منها مقياس نسبة ذروة الإشارة إلى الضوضاء (PSNR) والارتباط(Correlation) لذا فقد تم في هذا البحث قياس نسبة ذروة الإشارة إلى الضوضاء ومعامل الارتباط لجميع الصور وبدرجات لونية مختلفة، وتبين أن الدرجة اللونية مابين (1-4) درجات لونية لكل مستوى لوني من المستويات الثلاثة (الأحمر والأخضر والأزرق) لم تؤثر في هذين المقياسين فقد كانت قيمة نسبة ذروة الإشارة إلى الضوضاء (∞) أي أن قيمة MES هي صفر ولا يوجد أي تشوه. وكان معامل الارتباط هو(1) أي الصورتان (قبل الإخفاء وبعده) متطابقتان ولا يوجد أي اختلاف بينهما، مما يدل على أن الرسالة لا تدعو للشك بوجود إخفاء بيانات فيها، أما الدرجات اللوني الأكبر من 4 فيمكن

ملاحظة بان مقياس نسبة ذروة الإشارة إلى الضوضاء ومعامل الارتباط بدا يقل هذا دليل على وجود التشوه في الصورة. أنظر إلى الجدول (3) والجدول (4).

الجدول (3) يبين قيم PSNR وحسب تغير قيم الدرجة اللونية

مقدار الزيادة في الدرجة اللونية	1	2	3	4	5	6
PSNR%	∞	∞	∞	∞	52.3433	36.7182

الجدول (4) يبين قيم correlation وحسب تغير قيم الدرجة اللونية

مقدار الزيادة في الدرجة اللونية	1	2	3	4	5	6
Correlation	1	1	1	1	1.000	0.991

2- هنالك عشوائية جزئية في إخفاء الحروف في كلمات نص الغطاء، إذ لا تحدد بأول حرف نصادفه من الرسالة الغطاء، حيث يتم اختيار أية كلمة تحتوي عدد الأحرف المقابلة للحرف المراد تشفره أو أكثر في الطبقة اللونية حسب الجدول 2. فمثلا لإخفاء كلمة or في نص الغطاء:

The hiding in image was done by using one slide or three slides of image in one bit or two bits or three bits where the transfer taken place…….

فيمكن أخفاء الحرف o من الكلمة or حسب الجدول، إذ يتم اختيار أية كلمة من النص السابق فيها عدد الأحرف ثلاثة أو أكثر، ثم اختيار الطبقة اللونية R وزيادة القيمة اللونية بمقدار4، ويمكن أخفاء الحرف r من الكلمة or حسب الجدول أيضا، إذ يتم اختيار أية كلمة من النص السابق فيها عدد الأحرف 2 أو أكثر والطبقة اللونية G وزيادة القيمة اللونية بمقدار1.

3- الذي يزيد من العشوائية المتتابعة في اختيار حروف الرسالة ويصعب من عملية الهجوم، هو عدم وجود شروط لاختيار أحرف الرسالة السرية المقابلة لأحرف الرسالة الغطاء(أي عشوائية).

4- إن طريقة استرجاع الإخفاء تكون بالاعتماد على برنامج يتم برمجته لإظهار الحروف بالاعتماد على المفتاح السري الذي يكون متوافرا" لدى المستلم ليستطيع استرجاع الإخفاء، وفي حالة أن حصل المهاجم على خوارزمية الإخفاء فإنه سيحتاج إلى وقت لعمل خوارزمية استرجاع الإخفاء، واكتشاف المفتاح السري مما يزيد من الوقت اللازم لكسر الإخفاء ويزيد من أمنية الطريقة.

5- إذا علم المتطفل الخوارزمية المطبقة لإخفاء النص، ولم يحصل على المفتاح السري (الجدول والدرجة اللونية الأساس)، فان ذلك لا يوثر كثيرا، لأنه سيحتاج إلى عدة احتمالات

لتجربة الألوان على النص الغطاء، مما يزيد من الوقت اللازم لكسر الإخفاء، وبذلك يزيد من أمنية الطريقة.

6- إذا علم المتطفل الجدول والخوارزمية، ولم يعلم درجة لون الأساس فأنه سيحتاج إلى n من الاحتمالات بعدد الألوان المتوفرة للصورة لتجربة درجات الألوان على النص الغطاء.

7- التحويرات التي يمكن أن تتعرض لها الرسالة، فإذا عجز المهاجم عن استرجاع الإخفاء فإنه قد يلجأ إلى تحريف أو تغيير محتوى الرسالة أو يمنع وصولها إلى الهدف بحذف جزء أو كل محتواها، ومن هذه التغيرات وتأثيرها في الرسالة المخفية بالطريقة المقترحة :

- عمل نسخة من نص الغطاء، فهذا لن يوثر نهائيا في الرسالة السرية إذا لم يكن بها إخفاء، وإذا كان بها أخفاء فيتكرر الحرف أو الحروف المشفرة المخفية في النص الغطاء للرسالة السرية .
- إضافة نص إلى نص الغطاء، فهذا لن يؤثر نهائيا في الرسالة السرية، إذا لم يستخدم الدرجة اللونية المستعملة في التشفير والإخفاء.
- أما إذا أضاف المهاجم نصا إلى نص الغطاء، واستخدم الدرجة اللونية المستعملة في التشفير والإخفاء فهذا يوثر في الرسالة السرية، باستخدام أداة سحب (استنساخ) اللون، مثلا عند إضافة النص" The encoded data and " إلى الرسالة الغطاء بعد استخدام أداة سحب (استنساخ) اللون لسحب اللون من حرف وكان هذا الحرف بالصدفة يحتوي على إخفاء، دون أن يعلم بذلك المهاجم، فعند استرجاع الإخفاء سيظهر النص المضاف في الصورة المستوى اللوني المستخدم في الاخفاء، الذي يؤثر في الرسالة السرية وذلك بظهور حروف مضافة إلى الرسالة السرية وبشكل عشوائي.
- مسح جزء من النص وليس فيه جزء من أحرف الرسالة السرية لن يؤثر في الرسالة السرية.
- 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.
- التحوير بالخصائص العامة للخط:

ا- تغيير نوع أو حجم الخط أو جعله غامقا أو مائلا أو وضع خط تحت الحروف لن يؤثر في الرسالة نهائيا .

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.

9- مقارنة الطريقة المقترحة مع طرائق سابقة

تم في هذه الفقرة عمل مقارنة للطريقة المقترحة مع طريقة يوسف[9] وعلى النحو الآتي:

1- في طريقة يوسف تم التغيير في طبقة لونية واحدة في حين في الطريقة المقترحة يتم التغيير في الطبقات اللونية الثلاثة RGB.

2- في طريقة يوسف آختير الحرف نفسه في ملف الغطاء، أما في الطريقة المقترحة يتم اختيار الحروف بالاعتماد على الجدول مما يزيد من عشوائية الإخفاء .

3- في طريقة يوسف لا يوجد تشفير للنص المخفي، أما في الطريقة المقترحة فيتم تشفير النص لإخفائه في النص الغطاء.

وبذلك تعد الطريقة ذات سرية أعلى، وذلك لأن عملية التشفير وزيادة الطبقات اللونية في الإخفاء والتغيير في قيمة الدرجات اللونية في كل طبقة يؤدي إلى زيادة الوقت اللاز م للهجوم.

10- الاستنتاجات Conclusions

تعد الطريقة المقترحة غير معقدة من حيث التطبيق بالحاسوب، لأنها لاتتطلب نظاما خبيرا في مجال قواعد اللغة.

1-تعد هذه الطريقة فعالة من حيث أنها لا تبعث على الشك أو الريب عند أي شخص، لأنها تكون غير مرئية للعين البشرية.

2-هذه الطريقة سهلة التنفيذ وتعد مقاومة للتشويه الحاصل نتيجة للاستنساخ، إذ كانت قيمة PSNR مساوية لـ(∞) ومعامل الارتباط يساوي (1).

3-يكمن المفتاح السري في الجدول والدرجة اللونية للأساس.

4-حجم الغطاء المراد تشفير المعلومات به لا يحتاج أن يكون كبيرا.

5-هذه الطريقة لا تعتمد على كلمة معينة أو حرف معين مكرر في اللغة.

6-لا تحتاج هذه الطريقة إلى تحديد النص الغطاء، لأنها لا تعتمد في التشفير على تحديد الحرف، إذ أن التشفير يعتمد على ترميز كل حرف بعدد من الحروف والطبقة اللونية المستخدمة والدرجة اللون في تلك الطبقة.

7-بما أنه تعتمد في عملية فك التشفير على عدد العناصر في الصورة في الطريقة المقترحة لذا لا يتم استخدام الحروف التي تحوي على نقاط مثل الحرفين (j، i) وذلك لان الحرف (i) سيعد حرفين منفصلين وليس حرفا واحدا إذ أن النقطة هي كائن وبقية الحرف هو كائن آخر وكذلك الحرف(j).

8- تعد الطريقة المقترحة أسلوب عام لتشفير وإخفاء النص بلغات أخرى حيث يمكن تحويل الجدول 2 من الحروف الانكليزية إلى العربية مثلا لتشفير وإخفاء النص باللغة العربية.

11 - التوصيات Recommendation

بما انه لا يمكن إخفاء حرف من حروف الرسالة السرية التي تحوي على نقاط مثل الحرفين (i ,j) لذا نوصي بتطوير الطريقة بحيث يمكن استخدام الحروف التي تحوي على نقاط مثل هذين الحرفين.

المصـــادر

[1] إبراهيم، سندس خليل ويونس، غادة محمد و يوسف، ورقاء محمد هشام، 2011، "إخفاء البيانات النصية في حيز كارهونين لويف باستخدام صيغة عشوائية في الصور الرقمية"، المجلة العراقية لعلوم الإحصاء، العدد 20 المجلد 11.

[2] البلاسيني، أميرة بيبو، 2009، " تقنيات إخفاء المعلومات باستخدام الشبكات العصبية وبروتوكولات الشبكة "، بحث ماجستير، قسم علوم الحاسبات، كلية علوم الحاسبات والرياضيات، جامعة الموصل، العراق.

[3] الجبوري، رشا عواد حسن، 2011، " تصميم وتنفيذ نظام هجين لتشفير وإخفاء الملف النصي في بروتوكولات الصوت عبر الانترنت"، بحث ماجستير، قسم علوم الحاسوب، كلية علوم الحاسوب والرياضيات، جامعة الموصل، العراق.

[4] عبد المجيد، أنسام أسامة، 2011، " طريقة جديدة للكتابة المغطاة في الصور المكبوسة بالتكتيم ألاتجاهي"، بحث ماجستير، قسم علوم الحاسبات، كلية علوم الحاسبات والرياضيات، جامعة الموصل، العراق.

[5] المولى، محمد ناظم داؤد، 2007، "تقطيع صور أورام الدماغ ممثلة بالخوارزميات الجينية"، بحث ماجستير، قسم علوم الحاسبات، كلية علوم الحاسوب والرياضيات، جامعة الموصل، العراق.

[6] يوسف، ورقاء محمد هشام، 2011، " إخفاء البيانات باستخدام الصفات اللونية الغير مميزة"، بحث دبلوم عالي، قسم علوم الحاسوب، كلية علوم الحاسوب والرياضيات، جامعة الموصل، العراق.

[7] يوسف، ورقاء محمد هشام وإبراهيم، سندس خليل، 2013، "استخدام التغاير اللوني في إخفاء البيانات"، مجلة التربية والعلم، المجلد26،العدد3، ص194-215.

[8] Gonzalez, Rafael C. and Woods ,Richard E. ,(2008),"Digital Image Processing", Prentice Hall, Inc.

[9] Lin, Yith-Kail, 2012, "High capacity reversible data hiding scheme based upon discrete cosine transformation", the journal of system and software, PP2395-2404.

[10] Rana, Rita and Singh, Er. Dheerendra, 2010, "Steganography-Cocealing Messages in Images using LSB Replacement Technique

with Pre determined Random Pixel and Segmentation Image", International Journal of Computer Science & Communication, Vol.1, No.2, PP. 113-116.

[11] Sahoo, G. and Tiwari, R.K., 2008,"Designing an Embedded Algorithm for Data Hiding using Steganographic Technique by File Hybridization" International Journal of Computer Science and Network Security, Vol.8, No.1..