استخدام خواص البيانات الفضائية في إخفاء الرسائل النصية السرية

كنار محمد سامي مصطفى

قسم الحاسبات / كلية التربية

جامعة الموصل

الاستلام	القبول
٠٤ / ٠٦ / ٢٠٠٩	٠٦ / ١٠ / ٢٠٠٩

Abstract

The research deals with the concept of hiding information in one of the media where the 'Least Significant bit' which is one of the methods of steganography is used. Satellite images were chosen as a means of hiding because they have certain features and characteristics which make them an effective method for hiding. The satellite data have more than one taken image of the same land with different spectra, and each image is called 'band'.

Distributing the text on these bands and combining them to form the false colour composite image make the possibility of getting a sequential complete text complex. If hackers could get such images, it would raise suspicion about the area captured by the satellite while this area has nothing to do with required hidden information and transforming them to the second part.

The research aims at developing the hiding process by using satellite image features which depend on the method of distributing texts on spectral bands of the satellite image rather than hiding it in one image.

الملخص

يتناول البحث مفهوم إخفاء المعلومات داخل إحدى الوسائط، حيث تم استخدام طريقة البت ذي الدلال الصغرى (Least significant bit) وهي إحدى الطرق المستخدمة في عمليات الإخفاء كما تم اختيار البيانات الفضائية كأداة للإخفاء وذلك لما تتمتع به تلك البيانات من خواص وميزات

تجعل منها أداة فعالة للإخفاء حيث تمتلك الأخيرة أكثر من صورة ملتقطة لنفس المنطقة بأطوال موجية مختلفة تسمى كل صورة (حزمة طيفية – Band) وبتوزيع النص على تلك الحزم ثم دمجها مع بعضها لتكوين ما يسمى بالصورة الملونة الكاذبة (False color composite) يجعل من إمكانية الحصول على النص كاملاً ومرتباً أمراً معقداً، كما ان وقوع تلك البيانات بيد المتطفلين يجعل الشك يدور حول المنطقة الملتقطة من القمر الصناعي في حين ان تلك المنطقة لا علاقة لها بالمعلومات المطلوب إخفائها ونقلها إلى الطرف الثاني.

يهدف البحث إلى تطوير عملية الإخفاء باستخدام خواص البيانات الفضائية التي تعتمد على أسلوب توزيع النص على الحزم الطيفية للبيان الفضائي بدلاً من إخفاءه في صورة واحدة.

١. مقدمة

برغم كل التطورات وما وصلت اليه تكن ولوجيا المعلومات الا انها لم تصل الى حد الكمال التي طالما سعت اليه وذلك بسبب وجود ما يسمى بـ (اعداء التكنولوجيا) واحد اشكال هؤلاء الاعداء هو سراق المعلومات او (المتطفلون) وللأسباب اعلاه جاءت الحاجة الى وجود علاج لحل هذه المسألة وهو علم التشفير (Cryptography). ومع تطور اساليب سرقة المعلومات كان لابد لهذا العلم ان يتطور حيث ظهرت نظم وتقنيات تشفير كفوءة جداً .

لكن بعد ظهور الشبكات والانترنت لم يعد هذا العلم كافياً لوحده فالمعلومات الشخصية والرسائل السرية اصبحت في متناول يد الجميع كما تناقلت امكانيات فك التشفير وتكاد تكون اقوى من امكانيات التشفير نفسها وان لم يستطع الخصم فك الشفرة قد يعيق ايصالها الى الجهة المعنية لعلمه بوجود المعلومة.

من هنا نشأت تقنيات جديدة تعمل على اخفاء المعلومة بدلاً من تشفيرها تسمى تقنيات اخفاء المعلومات (Information Hiding) او (steganography) حيث يتم طمر المعلومات (Information Embedding) داخل وسائط نقل اخرى حاملة لها . وبهذا يتم ضمان وصول المعلومة حتى لو اطلع الخصم على الوسيلة المرسل عليها لعدم معرفته بوجود معلومة مخفية اصلاً، فالتحايل على المتطفل في نقل المعلومة هو اكثر أماناً من تشفيرها له.

٢. علم الإخفاء (Steganography):

يترجم التعريف الاغريقي لعلم الاخفاء ب شكل قاطع الى "كتابة مخفية "[3]، ويعرف (Jojodia&Johnson) [2] عملية الاخفاء على انها "العملية التي تقوم بلخفاء المعلومات بطريقة

لا تسمح باكتشافها"، اما (Leung) [5] فيعرفها "الطريقة التي يتم من خلالها اخفاء رسائل داخل انواع متعددة من الوسائط"، وبالنسبة الى (Kuhn)[4] فقد أعطى تعريفاً مع مقارنه هذا العلم بعلم التشفير حيث اشار الى ان "علم الاخفاء هو فن وعلم تبادل المعلومات عند اجراء اتصالات بين طرفين بحيث يتم فيه اخفاء وجود تلك المعلومات اثناء الاتصال". وعلى عكس علم التشفير الذي يسمح (للعدو) اكتشاف وتفسير وتعديل الرسائل دون قدرته على خرق بعض المزايا الامنية التي يضمنها نظام التشفير، فان هدف علم الاخفاء هو اخفاء الرسائل داخل رسائل اخرى (دون الحاق الضرر بها) بحيث لا تسمح (لأي عدو) حتى باكتشاف وجود رسالة سرية ثانية "، كما يضيف "ان الهدف الرئيسي من هذه التقنية هو اخفاء الرسالة السرية داخل رسالة عادية بطريقة تجعل المستلم غير قادر على اكتشاف وجود رسالة سرية اصلاً".

ومن احدث التعريفات التي ذكرت عن علم الاخفاء هي "اخفاء المعلومات بطريقة لا تجعل احداً يظن انها موجودة هناك . انها عبارة عن شكل من اشكال الحبر الألكتروني السري او الخفي ويمكن تخزين المعلومات في اجهزة (MP3) وفي الفيديوهات وحتى في المساحات الفارغة المتوفرة في الاقراص الصلبة" [9].

ومما سبق يمكن استخلاص تعريف عام لعلم الاخفاء هو ذلك العلم الذي يهتم باسلوب اخفاء رسالة ما (بيانات) داخل رسالة اخرى (بيانات اخرى) بهدف اخفاء وجود الرسالة الاولى، لهدف محدد. في عملية الاخفاء تكون الحاجة الى ملفين احدهما يسمى الغطاء، والآخر هو المادة المراد اخفاؤها. وهكذا فلن ميزة الاخفاء على التشفير هي ان الاول يخفي وجود الرسالة في حين الثاني يثبت وجودها ولكنها غير مقروءة [7].

٣. وسائط الإخفاء

يمكن ان تكون البيانات المستخدمة كظرف او وعاء للأخفاء عبارة عن ملفات الوسائط المتعددة كالصور، والنصوص، وملفات الصوت او الفيديو، وغيرها . وقد تكون كذلك ملفات تنفيذية لبرامج مختلفة من نوع (exe).

وفي حالة الاخفاء داخل الصور يجب مراعاة عدة عوامل منها :

- عدم استخدام صور معروفة او نماذج من صور يمكن لأي شخص الحصول على نسخ منها (مثل صور الانترنت) للأخفاء حيث تسهل المقارنة في حالة وجود الصورة الاصلية.
- مراعاة ان لا يحدث تغير ظاهر في الصور كتشوهها او تغير الوانها بشكل واضح ولهذا ينصح بعدم اخفاء بيانات كثيرة في ذات الصورة خوفاً من تغيير هيئتها، بطريقة تهدم الهدف الاساسي من استخدام التقنية، لان اثارة الشبهة يعني فشل العملية.

ووفقاً لهذه المعايير تم اختيار صورة الغطاء وهي عبارة عن بيان فضائي متكون من ثلاث حزم هي (الرابعة التي تمثل الاشعة ذات الطول الموجي تحت الحمراء القريب و الثالثة التي تمثل الطول الموجي الاحمر المرئي والحزمة الاخيرة وهي الثانية ذات الطول الموجي الاخضر المرئي). تمثل مركز مدينة الموصل ملتقطة بالمتحسس TM المرابط على القمر الصناعي لاندسات ٥ ذي القدرة التمييزية ٣٠ متر، ولمضاعفة عملية الاخفاء تم دمج تلك الحزم للحصول على صورة ملونة كاذبة ((False color composite(FCC)).

ومن اهم خواص البيانات الفضائية ان المشهد الواحد للغطاء الارضي يصور بعدة اطوال موجية كل طول يمثل حزمة والاخيرة تختلف عن مثيلاتها من الحزم بالقيم الرمادية (Gray scale) ولكنها تتوحد بالحجم فالمتحسس TM المرابط على القمر الصناعي لاندسات على سبيل المثال يملك سبعة حزم ذات اطوال موجية (الأزرق(0.45-0.52)، الاخضر (0.52-0.60)، الأحمر (0.63-0.69)، تحت الحمراء القريبة المنعكسة (0.76-0.90)، تحت الحمراء المنعكسة (1.55-1.75)، تحت الحمراء المنعكسة (2.08-2.35) وأخيراً تحت الحمراء الحرارية(10.4-12.5)) [6]. وحجم كل حزمة ٥١٢*٥١٢ وبامتداد (Bmp) عند تحليلها رقمياً.

من الجدير بالذكر ان الصور الرقمية التي ينتجها القمر الصناعي لاندسات هي عبارة عن صور ذات امتداد (BMP) وبتدرجات رمادية وتحوي نقاطها كبقية انواع الصور على قيم رقمية تسمى وحدات صورية (Pixels) تتراوح هذه القيم بين (٠-٢٥٥) وتمثل كل قيمة بـ (8 bit) على شكل جملة ثنائية حيث (2^8=256) والأرقام التي بين ذلك وهي (00000000-11111111) تمثل المستويات الرمادية بين الابيض والاسود .

٤. خوارزمية الاخفاء باستخدام طريقة البت ذي الدلالة الصغرى
Least Significant Bits algorithm

٤-١: مرحلة إخفاء الرسالة

تسمى الطريقة المستخدمة لإخفاء رسالة في صورة في هذا البحث بـ (Least Significant bits) او البت ذي الدلالة الصغرى ومختصرها (lsb) حيث يتم اخفاء الرسائل في البت الواقع في اقصى اليمين (bit0) ضمن الجملة الثنائية المتكونة من ٨ بت التي تمثل القيم الرمادية للصورة. تم اختيار هذا البت دونا عن غيره لأن أي تغيير في قيمته يمثل فرقاً بسيطاً جداً في اللون، فاللون الاسود النقي على سبيل المثال الذي يحمل القيمة (00000000) واللون الاسود ذي القيمة (00000001) بينهما فرق يصعب على العين تمييزه.

الخطوة الاولى: يتم تحويل الوحدات الصورية للصورة الغطاء (cover image) الى التمثيل الثنائي (Binary) باستخدام احدى ادوات اللغة البرمجية المستخدمة او اي نظام تحويل فالوحدة الصورية التي تحمل القيمة الرمادية (129) تحول الى (10000001).

الخطوة الثانية: يتم تحويل كل حرف في النص الى قيمته الرقمية الصحيحة تحت نظام (ASCII) وتتراوح هذه القيمة من 255-0. حيث يمكن تمثيل جميع الاحرف والارقام والرموز....الخ تحت هذا النظام بارقام صحيحة . مثال 'A' تمثل القيمة 65، واذا كان النص مكتوباً باللغة العربية فيمكن تحويله الى الـASCII باستخدام نظام خاص.

الخطوة الثالثة: تحول كل قيمة (ASCII) الى التمثيل الثنائي لها فالقيمة "65" للحرف A تحول الى (01000001).

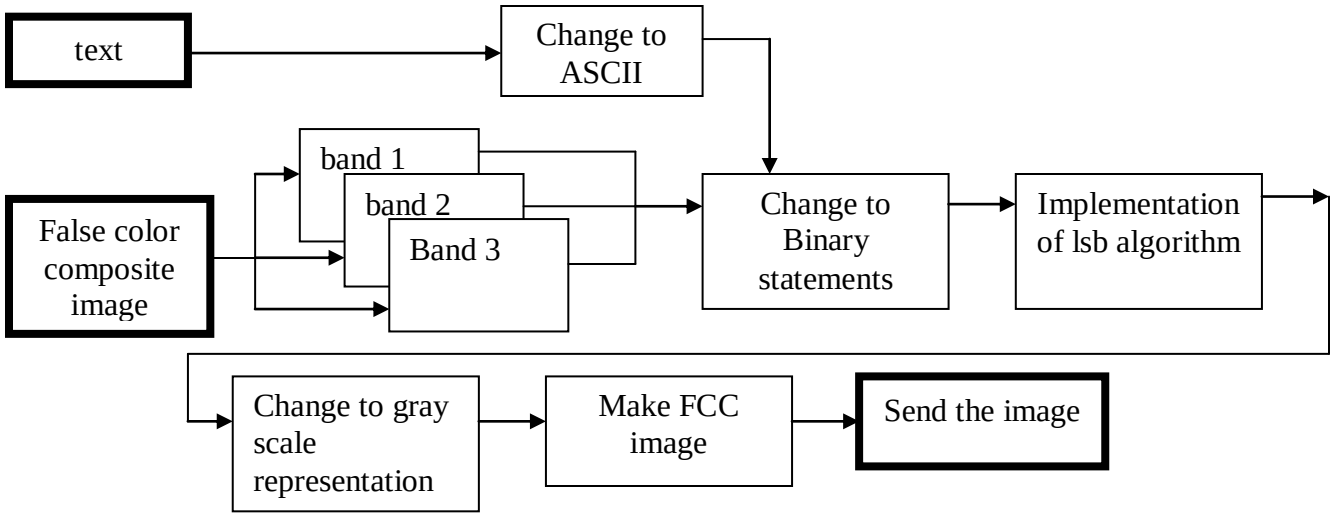
الخطوة الثالثة: يوضع كل بت للحرف على اول بت من الوحدة الصورية (bit 0) _حيث يستبدل البت الاول للوحدة الصورية (**1** 1000000) بالبت الثامن للحرف (1000001 **0**) فتصبح الوحدة الصورية بالشكل (10000000) وتحمل القيمة (128) بدلاً من (129)، وتعاد العملية على البت السابع للحرف (000001 **1** 0) بوضعه محل البت الاول للوحدة الصورية التالية... وهكذا.

الخطوة الرابعة: يتم تقسيم النص المراد إخفاءه الى ثلاث اجزاء وذلك لان الصورة الغطاء تمثل بيان فضائي متكون من ثلاثة حزم حيث ي وضع الجزء الاول للنص في العمود الاول للحزمة الاولى و الجزء الثاني في العمود الثاني للحزمة الثانية و هكذا بالنسبة للجزء الثالث من النص.

الخطوة الخامسة: تتضمن هذه الخطوة اجراء عملية دمج الحزم الثلاث للحصول على صورة ملونة كاذبة(FCC) وبهذه الطريقة يمكن الحصول على النص كاملاً بعد اجراء عملية فك الاخفاء.

الخطوة السادسة: بعد الانتهاء من ابدال القيم الثنائية للرسالة محل (bit 0) للصورة الغطاء تُكرر العمليات السابقة ولكن بشكل معكوس حي ث يتم ارجاع الصورة الغطاء من شكلها الحالي (جمل ثنائية) الى ارقام صحيحة تمثل الوحدات الصورية وتصبح جاهزة للأرسال الى الطرف الآخر .

يوضح المخطط (٤-١) خطوات عملية إخفاء الرسالة:



شكل (٤-١): يمثل خطوات إخفاء الرسالة

٤-٢: مرحلة فك الإخفاء (Steganalysis)

تسمى العملية التي تتم فيها محاولة طرف ما اكتشاف وجود المعلومات المخفية وفكها، او قراءتها او تغيرها او حذفهاب (steganalysis). فبعد استلام الصورة الملونة الكاذبة يتم اجراء الخطوات الآتية:

الخطوة الاولى: يتم ترتيب البيانات الفضائية بالتسلسل المتفق عليه مسبقاً من قبل الطرفين.

الخطوة الثانية: تتضمن هذه الخطوة قراءة الـ(byte) الاخير للحزمة الاخيرة والـ (byte) قبل الاخير بواحد للحزمة الثانية والـ (byte) قبل الاخير باثنين للحزمة الاولى حيث يمثل كل (byte) طول النص الذي تحمله تلك الحزمة وبمجموع قراءات تلك الـ (bytes) نحصل على طول النص المخفي.

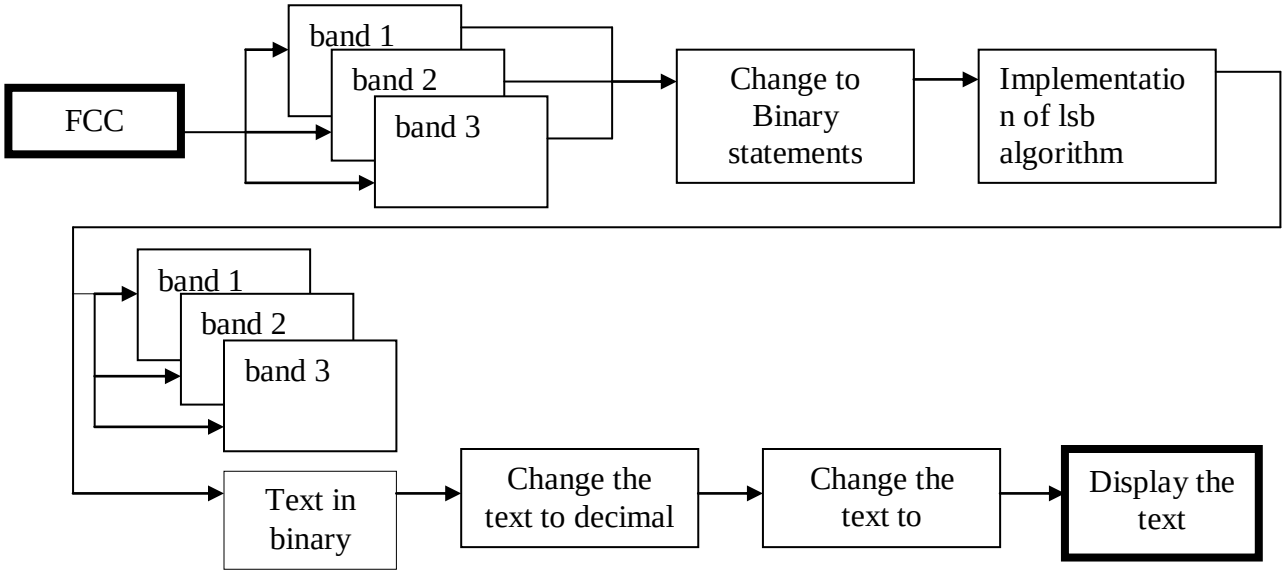
الخطوة الثالثة: تحول القيم الرمادية للحزمة الاولى (Gray Scale) الى جمل ثنائية (Binary Statement) وتعاد نفس العملية على الحزمة الثانية والثالثة.

الخطوة الرابعة: يؤخذ البت الاول (bit 0) من كل ثمانية وحدات صورية متتالية وتجمع لتكون (byte) مثلاً.

الخطوة الخامسة: يتم تحويل تلك (bytes) التي تم جمعها الى ارقام صحيحة فاذا كان احدى الـ(bytes) يمثل (01000001) يحول الى الرقم الصحيح (65).

الخطوة السادسة: في هذه الخطوة يتم ارجاع تلك الارقام الى وضعها الاول على شكل حروف كبيرة وصغيرة ورمو ز حسب الرمز الذي تمثله تلك القيمة أي (65 تمثل في نظام ASCII الحرف "A") وبهذا نحصل على النص صحيحاً وكاملاً بدون تقطيع او نقص او تغيير فيه.

يمثل المخطط (٤-٢) خطوات عملية فك الاخفاء:



شكل (٤-٢): يمثل خطوات فك الإخفاء

٥. النتائج

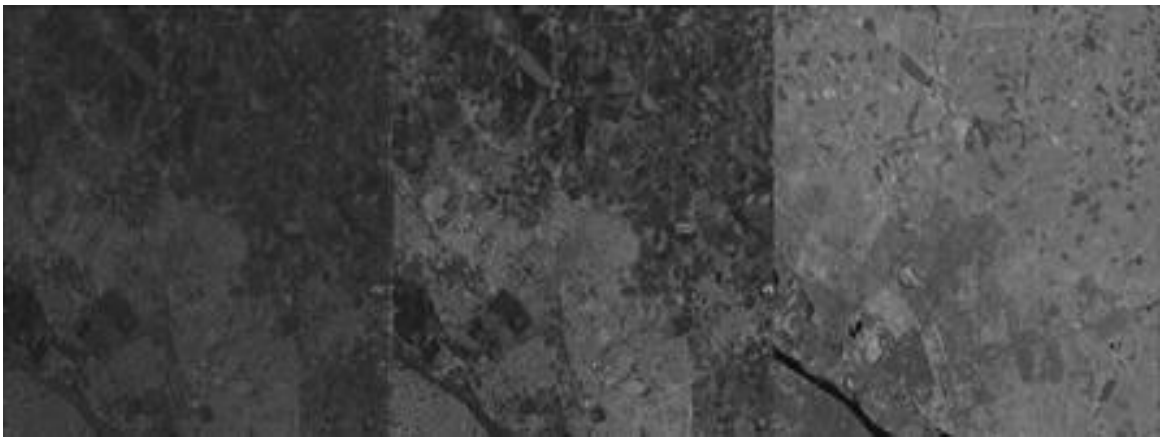
لقد تم تطبيق خوارزمي ة الاخفاء باستخدام لغة البرمجة (Matlab 7) تحت بيئة نظام Windows XP وذلك لما تتمتع به هذ ه اللغة من خواص وميزات حيث تتوفر فيه الكثير من الوظائف والدوال الرياضية المبنية داخلياً والتي يسهل حل مختلف انواع المعادلات الرياضية كما يساعد على كتابة دوال وبرامج خاصة[1] .

ولتنفيذ أي برنامج اخفاء يجب توفر ثلاثة امور مهمة اولها توفر احدى وسائط الاخفاء وثانيها اختيار طريقة للاخفاء اما الامر الثالث فهو توفر النص المراد إخفاءه.

فبالنسبة للأمر الأول والثاني فقد تم ذكرهما في الفقرات السابقة اما ثالثاً فقد تم اختيار نص يمثل اربعة مقاطع لأحدى قصائد شكسبير الشهيرة المكتوبة باللغة الانكليزية القديمة [8] وهي كالتالي:

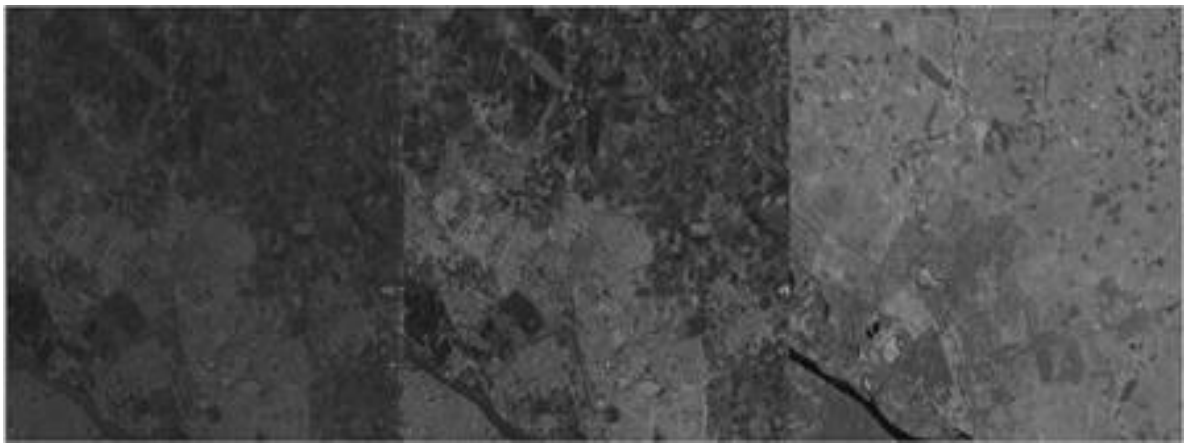
Shall I compare thee to a summers day?
Thou art more lovely and more temporate
Rough winds do shake the darling buds of May,
And Summer lease hath all too short a date

وقد تم عرض الحزم الثلاثة للبيان الفضائي لم ركز مدينة الموصل والصورة المركبة الكاذبة لها قبل وبعد احتواء النص داخلها بغية المقارنة بين الحالتين:



a b c

شكل (٥-١): يمثل (a,b,c) حزم البيانات الفضائية (2,3,4) على التوالي لمركز مدينة الموصل قبل إخفاء الرسالة



a b c

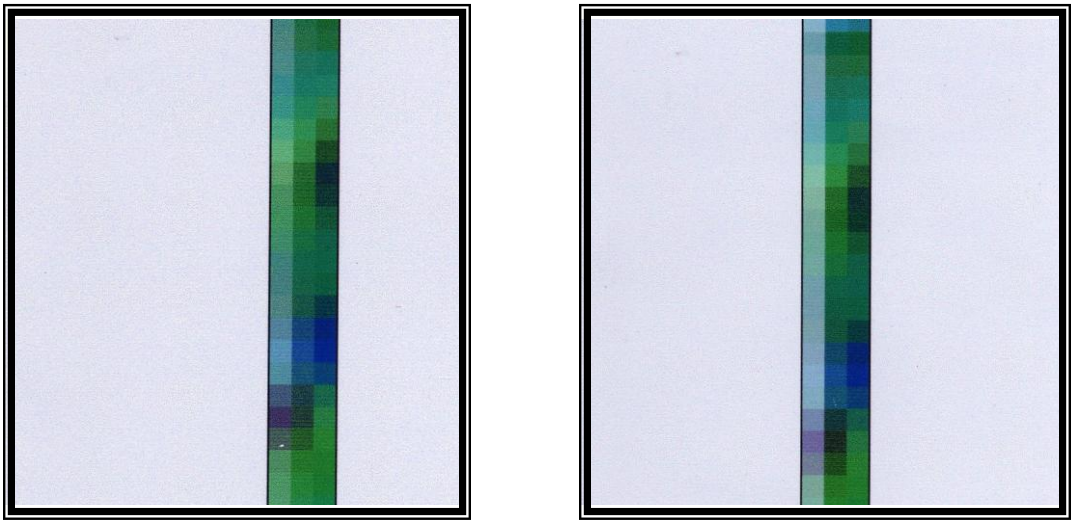
شكل (٥-٢): يمثل (a,b,c) حزم البيانات الفضائية (2,3,4) على التوالي لمركز مدينة الموصل بعد إخفاء الرسالة

(a)

(b)

شكل (٥-٣): تمثل (a) الصورة الملونة الكاذبة للحزم (2,3,4) للموصل قبل اخفاء الرسالة اما (b) فتمثل الصورة الملونة الكاذبة للحزم السابقة بعد اخفاء الرسالة

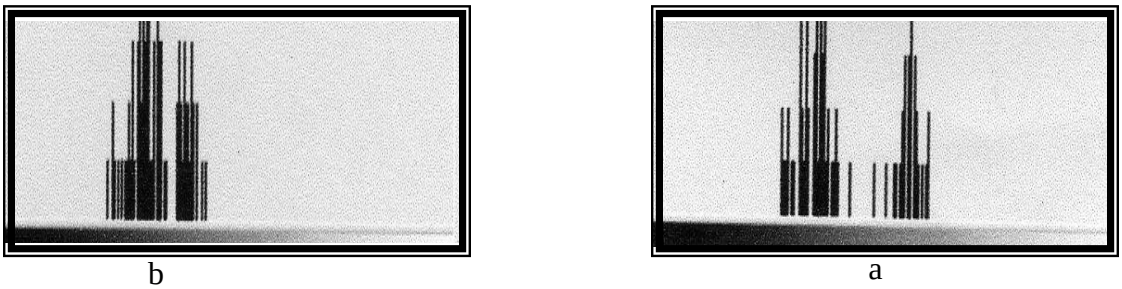
ولأن العين المجردة لا تستطيع تمييز الاخفاء في الصورتين تم تكبير المقطع المستخدم للإخفاء لكي يستطيع القارئ تمييز التباين في التدرجات اللونية والشكل (٥-٤) يمثل تكبير لمقطع الصورة الغطاء الذي يحوي النص المخفي قبل وبعد اخفاء النص.



b a

شكل (٥-٤): يمثل تكبير لمقطع الصورة الغطاء حيث يمثل (a) المقطع قبل اخفاء النص اما (b) فيمثل نفس المقطع المذكور بعد الاخفاء

أما الشكل (٥-٥) فيمثل الرسم البياني (histogram) للمقطع المذكور قبل وبعد عملية الاخفاء.



b a

شكل (٥-٥): يمثل الرسم البياني لمقطع الصورة الغطاء حيث يمثل (a) الرسم البياني للمقطع قبل اخفاء النص اما (b) فيمثل نفس المقطع المذكور بعد الاخفاء

كما تم عمل مقارنات لهيانات الحزم الفضائية قبل وبعد تنفيذ خوارزمية الاخفاء وبالشكل التالي :

أ. يمثل الجدول (٥-١) السلم الرمادي (gray scale) للبيانات الفضائية ويقصد بالرمز (B) band أي الحزمة والرقم (١و٢و٣) فيمثل الحزمة الاولى والثانية والثالثة على التوالي، والرمز (a) يمثل القيم الرمادية للحزمة قبل تنفيذ خوارزمية الاخفاء اما الرمز (b) فيعني القيم الرمادية لتلك الحزمة بعد تنفيذ الخوارزمية.

B1(a)	B1(b)
60	60
53	53
52	52
57	57
60	60
59	58
54	55
45	45
44	44
43	43
48	49
54	54
57	57
58	58
52	52
43	42
40	40
44	45
50	51
54	54
56	56
56	56
58	58
68	69
70	70
77	77
65	65
60	60
61	61
61	61
60	60
56	56
53	52
51	51
50	51

B2(a)	B2(b)
131	130
78	79
63	63
66	66
72	73
78	79
81	81
79	79
78	78
74	75
66	67
60	61
49	48
49	49
58	59
54	54
46	46
55	55
71	71
72	72
72	72
69	69
73	72
79	79
110	110
111	111
101	101
83	82
75	75
65	65
54	54
55	54
50	50
49	49
59	59

B3(a)	B3(b)
107	106
107	107
107	107
107	106
111	111
114	115
111	111
114	114
115	114
120	121
124	125
122	122
104	104
87	87
99	99
109	109
108	108
102	102
96	97
96	96
97	96
100	100
96	96
76	76
72	72
80	81
92	93
79	78
76	76
95	94
110	111
112	112
110	110
113	113
117	117

جدول (٥-١): يمثل بيانات الحزم الثلاثة قبل وبعد تنفيذ خوارزمية(lsb)

تم اختيار اول ٣٥ قيمة عن كل حزمة كنموذج لأن ادراجها جميعها يسبب الاطالة في النتائج . وكما هو واضح ان الاختلاف الحاصل للقيم بعد الاخفاء يمثل زيادة او نقصان للقيمة بمقدار واحد فقط وهو فرق ضئيل جدا لا تستطيع العين البشرية تمييزه.

ب. يمثل الجدول (٥-٢) القيم السابقة الذكر في النقطة (أ) ولكن بعد تحويلها الى جمل ثنائية.

B1(a)	B1(b)
00111100	00111100
00110101	00110101
00110100	00110100
00111001	00111001
00111100	00111100
00111011	00111010
00110110	00110111
00101101	00101101
00101100	00101100
00101011	00101011
00110000	00110001
00110110	00110110
00111001	00111001
00111010	00111010
00110100	00110100
00101011	00101010
00101000	00101000
00101100	00101101
00110010	00110011
00110110	00110110
00111000	00111000
00111000	00111000
00111010	00111010
01000100	01000101
01000110	01000110
01001101	01001101
01000001	01000001
00111100	00111100
00111101	00111101
00111101	00111101
00111100	00111100
00111000	00111000
00110101	00110100
00110011	00110011
00110010	00110011

B2(a)	B2(b)
10000011	10000010
01001110	01001111
00111111	00111111
01000010	01000010
01001000	01001001
01001110	01001111
01010001	01010001
01001111	01001111
01001110	01001110
01001010	01001011
01000010	01000011
00111100	00111101
00110001	00110000
00110001	00110001
00111010	00111011
00110110	00110110
00101110	00101110
00110111	00110111
01000111	01000111
01001000	01001000
01001000	01001000
01000101	01000101
01001001	01001000
01001111	01001111
01101110	01101110
01101111	01101111
01100101	01100101
01010011	01010010
01001011	01001011
01000001	01000001
00110110	00110110
00110111	00110110
00110010	00110010
00110001	00110001
00111011	00111011

B3(a)	B3(b)
01101011	01101010
01101011	01101011
01101011	01101011
01101011	01101010
01101111	01101111
01110010	01110011
01101111	01101111
01110010	01110010
01110011	01110010
01111000	01111001
01111100	01111101
01111010	01111010
01101000	01101000
01010111	01010111
01100011	01100011
01101101	01101101
01101100	01101100
01100110	01100110
01100000	01100001
01100000	01100000
01100001	01100000
01100100	01100100
01100000	01100000
01001100	01001100
01001000	01001000
01010000	01010001
01011100	01011101
01001111	01001110
01001100	01001100
01011111	01011110
01101110	01101111
01110000	01110000
01101110	01101110
01110001	01110001
01110101	01110101

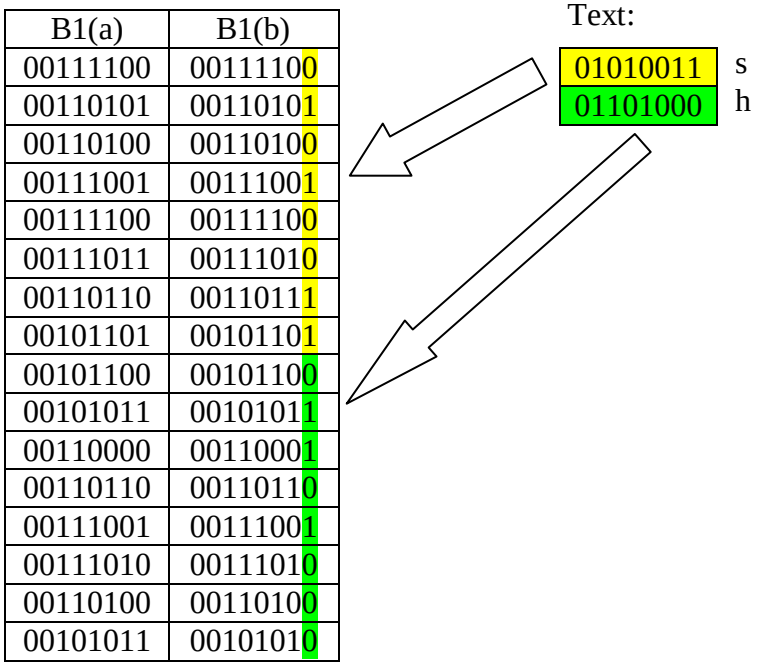
جدول (٥-٢): بيانات الحزم الثلاثة الثنائية قبل وبعد تنفيذ خوارزمية(lsb)

جـ. يمثل الجدول (٥-٣) التمثيل الثنائي للسطر الأول لقصيدة شكسبير :

01010011	S
01101000	h
01100001	a
01101100	l
01101100	l
00100000	
01001001	I
00100000	
01100011	c
01101111	o
01101101	m
01110000	p
01100001	a
01110010	r
01100101	e
00100000	
01110100	t
01101000	h
01100101	e
01100101	e
00100000	
01110100	t
01101111	o
00100000	
01100001	a
00100000	
01110011	s
01110101	u
01101101	m
01101101	m
01100101	e
01110010	r
01110011	s
00100000	
01100100	d
01100001	a
01111001	y
00111111	?

جدول (٥-٣): التمثيل الثنائي للنص المطلوب اخفاءه (قصيدة شكسبير)

وكما هو موضح ادناه فان (bit 0) هو الوحيد الذي يتغير احياناً وتبقى باقي الجملة الثنائية كما هي وليس بالضرورة ان يكون التغيير في جميع الجمل وحسب بل حسب ما يقتضيه النص المخفي، فـ(bit 0) في بعض الجمل الثنائية للأعمدة (B1(b),B2(b),B3(b)) هو ليس تتمة للجمل الثنائية للقيم الرمادية للصورة الغطاء وانما هو عبارة عن الجمل الثنائية للنص المطلوب إخفاءه وهذا ما تم ايضاحه في الشكل التالي:

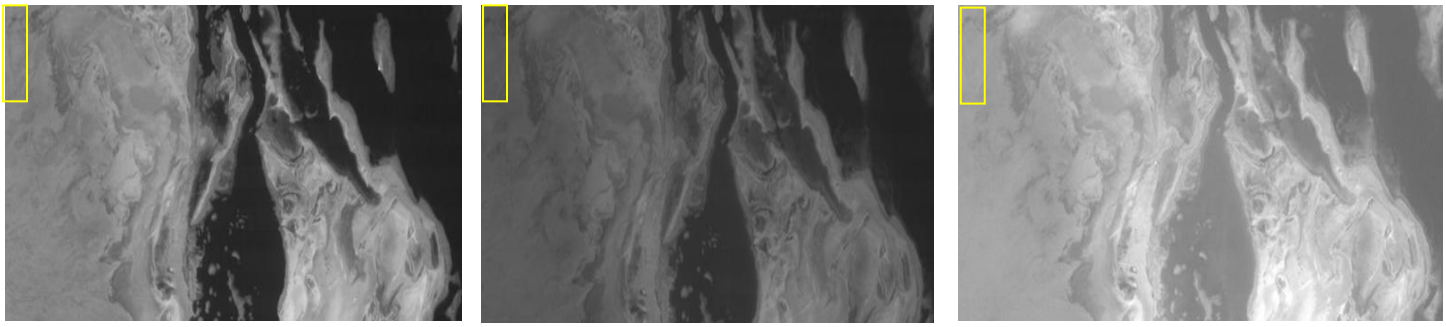


B1(a)	B1(b)
00111100	00111100
00110101	00110101
00110100	00110100
00111001	00111001
00111100	00111100
00111011	00111010
00110110	00110111
00101101	00101101
00101100	00101100
00101011	00101011
00110000	00110001
00110110	00110110
00111001	00111001
00111010	00111010
00110100	00110100
00101011	00101010

شكل (٥-٦): يمثل حرفي (sh) من كلمة shall من القصيدة سابقة الذكر وقد تم توزيعهما على بيانات الصورة وهكذا الحال مع بقية الاحرف

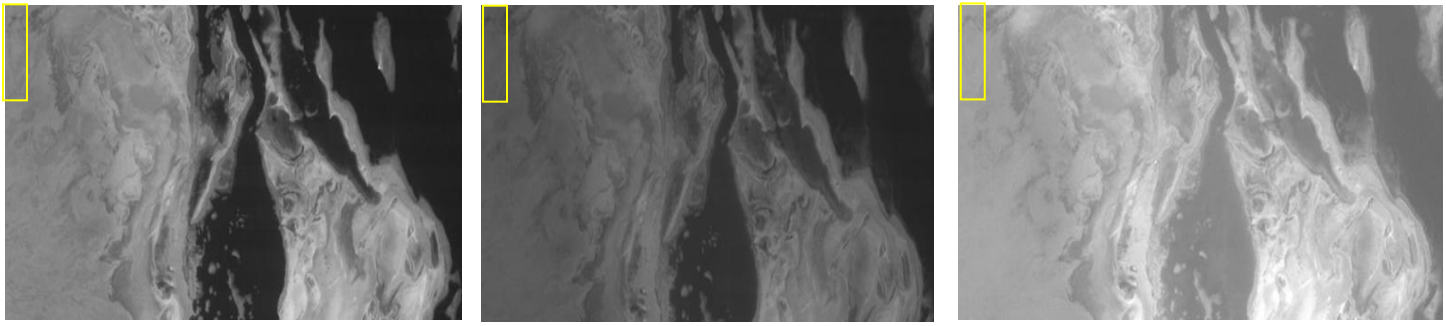
من الجدير بالذكر ان حجم النص الذي يمكن اخفاءه باستخدام هذه الطريقة يعادل حجم الصورة الغطاء (عدد الوحدات الصورية) مقسوماً على الرقم (٨) وهو حجم البايت الذي يمثل الحرف في النص ومضروباً في عدد الحزم المستخدمة في الاخفاء وهي (٣)، ثم يطرح منها ثلاثة بايتات الذي يتم خزن طول النص المخفي في كل حزمة.

اما إذا تم اخذ مثال ثاني للصورة الغطاء يمثل بيان فضائي خشن النسجة فقد تكون احتمالية حصول تفاوت في الالوان اك ثر مما ه و عليه بالبيان الفضائي ذ ي النسجة الناعمة والالوان المتداخلة، خاصة اذا حدث الاخفاء في مناطق احادية اللون كما في الشكل التالي:



a b c

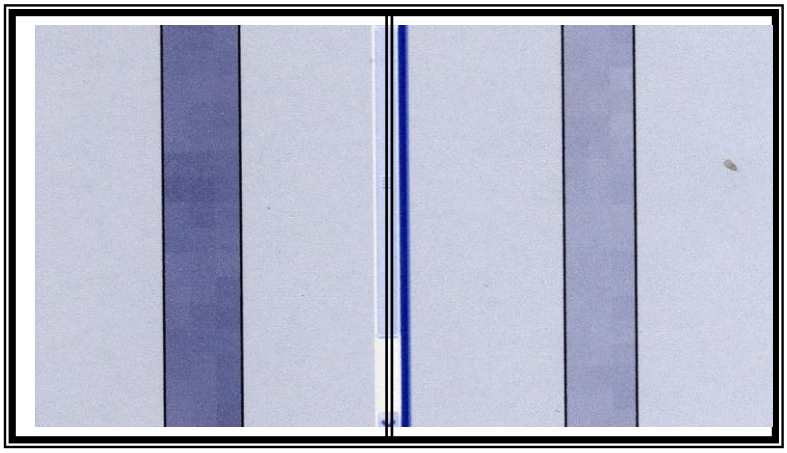
شكل (٥-٧): يمثل (a,b,c) حزم البيانات الفضائية (3,2,1)
على التوالي للبحر الاحمر قبل اخفاء الرسالة



a b c

شكل (٥-٨): يمثل (a,b,c) حزم البيانات الفضائية (3,2,1)
على التوالي للبحر الاحمر بعد الاخفاء

وعند اخذ صورة مكبرة لمقطع الصورة الغطاء المؤشرة اعلاه نلاحظ تقارب وتجانس كبير في مستويات الالوان للوحدات الصورية فهي تحمل قيم صورية متقاربة بحيث تبدو وكأنها في مستوى لوني واحد وان ادخال مستوى لوني جديد قد يبدو اوضح مما هو عليه في المثال السابق .



شكل (٥-٩): صورة مكبرة لمقطع الإخفاء للبيان الفضائي (1,2)

٦. الاستنتاجات:

مما سبق يمكن استنتاج مايأتي:

١. ان تقنيات اخفاء المعلومات تمثل خوارزميات بسيطة نسبة لما تحققه من السرية العالية حيث تعتمد على التحايل البصري اكثر من اعتمادها على طرق رياضية معقدة كما هو الحال في خوارزميات التشفير.

٢. لا يختلف حجم البيانات المرسلة عن المستلمة وبهذا لا تتطلب العملية خوارزميات كبس وفك كبس نتيجة لزيادة في حجم البيانات المرسلة.

٣. كلما كانت الصورة ذات تفاوت وتشابك في القيم الر مادية كلما كانت الامنية في اخفاء المعلومات اقوى.

٤. ان استخدام البيانات الفضائية كصورة غطاء (cover image) عوضاً عن الصور العادية يضيف حيلة جديدة للمتطفل حيث تقع المنطقة المصورة في البيان الفضائي في دائرة الشك خصوصاً اذا تم اختيار مناطق تحوي اصناف متعددة من الغطاء الأرضي.

٥. ان توزيع النص المراد اخفاءه على الحزم الطيفية تقلل من حجم النص في الحزمة الواحدة وتزيد من مساحات الاخفاء وبالتالي يصبح اخفاء النص بهذا الشكل افضل من اخفاءه كاملاً داخل صورة واحدة.

٦. يمكن تقليص عدد الوحدات الصورية المستخدمة في الاخفاء وذلك باستخ دام نفس الطريقة ولكن الاخفاء يتم بـابدال بتين او ثلاثة بتات بدلاً من بت واحد فقط، وعلى الرغم من ان التغيير في التدرجات الرمادية تكون اكثر تبايناً من السابق الا ان ادراكها من قبل العين يبقى صعباً.

٧. المصادر:

[1] Herniter, Marc E., Programming in Matlab, Thomson, Canada, 2001.

[2] Jojodia S., Johnson N. F., Steganalysis:The Investigation of Hidden Information , IEEE information technology conference, Syracuse, New York, USA, 1998. available at http://www.simovits.com/archive/it98jjgmu.pdf.

[3] Jupin J., Final Project-Steganography, 2004. available at http://stro.temple.edu/~joejupin/Steganography.pdf.

[4] Kuhn M., Steganography mailing list, 1995, available at http://www.jjtc.com/steganography/steglist.htm

[5] Leung K. M., Introduction to Steganography, Polytechnic University, Department of Computer and Information Science, 2004.

[6] Lillesand T. M. , Kiefer R. W., Remote Sensing and Image Interpretation, second edition, John Wiley & Sons, Inc. Canada, 1987.

[7] Maccawy M., Steganography, KSA, 2007, available at http://marammaccawy.maktoobblog.com/644257/

[8] Wilson J. D., The Sonnets. Cambridge: Cambridge university press, 1966.

[9] الإخفاء بعد التشفير للنقل الامن للمعلومات، ٢٠٠٧. متوفرة في الموقع:
http://Arabi.wordpress.com/2007/10/02/