مجلة القادسية لعلوم الحاسوب والرياضيات المجلد(٨) العدد(١)
السنة(٢٠١٦)

صفحة ١-١١ زياد صفاء

إخفاء المعلومات في الصور باستخدام تقنية استغلال تعديل الاتجاه (EMD) وخوارزمية مسألة الحصان

زياد صفاء يونس الصفاوي
جامعة الموصل / كلية علوم الحاسوب والرياضيات
Email: ziead_1979@yahoo.com zeyad.s.safawi@gmail.com

استلام البحث: ٢٠١٥/١١/٢٦ إرسال التعديلات: ١٦ /٢٠١٦/٣ قبول النشر: ٢٠١٦/٤/٤

المستخلص :

في هذه الدراسة، اقترحنا تقنية جديدة في إخفاء المعلومات في الصور من خلال استخدام طريقة استغلال تعديل الاتجاه (Exploiting Modification Direction(EMD)) وتحسينها باستخدام خوارزمية مسالة الحصان (Knight's Tour) لإخفاء المعلومات في الصورة واستخدام طريقة LZW(Lempel-Zev-Welch) في تشفير وكبس محتويات الرسالة السرية. في هذه التقنية، تستخدم خوارزمية الـ LZW لغرض تشفير وكبس وتحويل أحرف الرسالة السرية إلى سلسلة من الارقام الثنائية (bits stream) وذلك لغرض حماية البيانات وتقليل حجم الرسالة. وفي الخطوة التالية، سنستخدم تقنيتي الـ EMD والـ Knight tour لغرض طمر الأرقام السرية حيث سيتم تقسيم الصورة (cover image) الى مجاميع. هذه المجاميع تحتوي على 4 من البكسل (pixels) في كل مجموعة. بعد ذلك، سيتم تقسيم الصورة الى كتل بحجم (4*4) مجموعة للكتلة الواحدة. يستخدم نظام الترميز (2n+1)-ary لغرض تمثيل الأرقام السرية للرسالة التي ستطمر في الصورة. ولغرض زيادة السرية والقوة (Robustness) للطريقة المقترحة تستخدم خوارزمية الـ Knight tour لغرض اختيار المجموعة التي سيتم إخفاء الرقم السري بداخلها. حيث سيتم طمر رقم سري واحد من خلال تعديل قيمة رمادية واحدة داخل البكسل المحدد في المجموعة باستخدام تقنية الـ EMD. بعد ذلك، يتم توليد هجمات إحصائية باستخدام طريقة x^2 على الصورة (stego image) بعد طمر المعلومات بداخلها لتقييم قوة الطريقة المقترحة في مواجهة الهجمات. النتائج العملية تظهر ان كل من الـ Peak signal to Noise Ratio (PSNR) وكمية البيانات المطمورة في الصورة (Payload) للطريقة المقترحة أفضل بالمقارنة مع الطرق السابقة المستخدمة في إخفاء المعلومات.

الكلمات المفتاحية : اخفاء المعلومات، استغلال تعديل الاتجاه، مسألة الحصان، طريقة LZW.

١- المقدمة :

أصبحت حماية الوسائط الرقمية على شبكة الانترنيت من المسائل المهمة نتيجة للتطور الهائل في مجال الحاسبات وتكنولوجيا المعلومات والزيادة الكبيرة في استخدام شبكات الانترنيت في إرسال واستقبال المعلومات والبيانات. وقد انصب اهتمام الباحثين على بناء طرق لحماية البيانات والمعلومات وجعلها أكثر سرية لمنع وصولها للمتطفلين ومخترقي الشبكة [4,3,2,1].

إخفاء المعلومات (steganography)هي تقنية تستخدم لغرض إخفاء المعلومات أو إخفاء وجود أي اتصال عن مستخدمي الشبكة باستثناء الشخص المرسل والشخص المستلم للرسالة السرية عبر وسط رقمي حامل للمعلومات والذي يمكن أن يكون نص أو صورة أو صوت أو فيديو [7,6,5]. مصطلح إخفاء المعلومات هي كلمة إغريقية تعني الكتابة المخفية [12,11, 10, 9,8] .

إن التحدي الرئيسي في عملية إخفاء المعلومات هو في حجم البيانات التي سوف تطمر في الصورة مع الحفاظ على جودة الصورة (quality) والتي تتطلب طرق خاصة في إخفاء اكبر كمية من البيانات المدخلة (payload) بالإضافة إلى القوة (Robustness) للطريقة المستخدمة في الإخفاء لمواجهة الهجمات من قبل مخترقي الشبكة. يعتبر الـ Peak Signal to noise ratio(PSNR) واحد من أهم المقاييس

للحكم على الجودة للصورة (stego image) التي تحتوي على المعلومات بداخلها. حيث انه، يعتمد على القيمة القياسية لنظام العين البشرية Human Visual System (HSV) والذي قيمته (30 dB) إذا كانت قيمة الـ PSNR اكبر او تساوي هذه القيمة. فهذا يعني إن البيانات السرية التي سوف تطمر في الصورة سوف تكون غير مرئية للعين البشرية [15,14,13]. في هذه الدراسة، اقترحنا طريقة لغرض إخفاء المعلومات وذلك من خلال استخدام طريقة LZW لتشفير وكبس الرسالة السرية لغرض حماية البيانات وتقليل حجمها وطمرها داخل الصورة من خلال استخدام تقنية الـ EMD للإخفاء والتي سيتم تحسينها من خلال استخدام خوارزمية الـ Knight tour لزيادة السرية من خلال طريقة اختيار المجاميع التي سيتم طمر الأرقام السرية فيها وكذلك لغرض زيادة كمية البيانات المطمورة داخل الصورة بالإضافة إلى المحافظة على الجودة للصورة(stego image) وجعلها مشابهة إلى حد كبير للصورة الأصلية وزيادة القوة للطريقة المقترحة في مواجهة هجمات المتطفلين واللصوص.

2- دراسات سابقة

هناك العديد من التقنيات والطرق المختلفة تم اقتراحها من قبل العديد من الباحثين لإخفاء المعلومات داخل الصور. حيث أن، الصورة تتكون من مجموعة من البكسل وان قيمها في الصورة الرمادية تكون ما بين (0 - 255). وبصورة عامة، لتمثيل قيمة البكسل في الصورة باستخدام النظام الثنائي هناك على الاقل 8 بت ويتم تمثيلها من البت $(a_8 \ldots a_1)$ [17,16].

تم اقتراح طريقة الـ EMD من قبل (Zhang and Wang) في عام 2006. وذلك لغرض التقليل من التغيير الحاصل في الصورة خلال عملية طمر المعلومات بداخلها [7]. هذه الطريقة تعمل على تقسيم الصورة إلى مجاميع (groups) متساوية كل مجموعة تحتوي على n من البكسل وذلك لغرض طمر الأرقام السرية بنظام الترميز (2n+1)-ary . خلال عملية الطمر سيتم إضافة أو طرح 1 من قيمة البكسل التي سيتم اختيارها داخل المجموعة . في عام 2007 قدم (Lee) واخرون طريقة جديدة لتحسين طريقة الـ EMD اطلق عليها (IEMD). هذه الطريقة حققت نسبة طمر للمعلومات اكبر بالمقارنة مع الطريقة الاصلية ومن دون التاثير على جودة الصورة التي تحمل الرسالة او التاثير على السرية. في هذه الطريقة الرسالة السرية سيتم تحويلها الى ارقام سرية بنظام ترميز 8-ary وكل رقم سري يطمر في المجموعة المكونة من اثنان من البكسل. في هذه الطريقة تم اخفاء كمية اكبر من البيانات في الصورة لكن جودة الصورة كانت اقل من طريقة EMD الاصلية [18] .

وقد تم اقتراح طريقة الـ Opt EMD من قبل (K. lin) وآخرون في عام 2010 [1]. حيث تم تحليل العلاقة ما بين عدد البكسل n في المجموعة وكمية البيانات التي سيتم تضمينها داخل الصورة (Payload) وذلك لتحسين طريقة الـ EMD في إخفاء البيانات. أي انه. سيتم حساب العدد المناسب للبكسل في كل مجموعة للحصول على اقل تشويه في الصورة بعد اجراء عملية الطمر. الغرض منها، هو إخفاء اكبر كمية من البيانات في الصورة لكن مع تقليل التشوه الحاصل في الصورة بعد طمر البيانات فيها.

في عام 2013 قدم (kuo) واخرون طريقة جديدة لتحسين خوارزمية الـ EMD وذلك من خلال اخفاء $(n+1)$ بت من الرسالة السرية في n من البكسل في الصورة. حيث ان البكسل سوف يتم اضافة او طرح واحد من قيمتها او تبقى قيمتها بدون تغيير [19]. في عام 2014 اقترح الباحثان (Cheng and Wu) طريقة جديدة لتحسين طريقة الـ EMD الاصلية. في هذه الطريقة رقمين سريين يتم طمرهم في بكسل واحدة في المجموعة حيث سيكون معدل طمر المعلومات في هذه الطريقة مضاعف بالمقارنة مع الطريقة الاصلية [20].

في عام 2015 قدم (Niu) وآخرون طريقة جديدة في اخفاء المعلومات من خلال اقتراح طريقة EMD-3 [14]. في هذه الطريقة، سيتم طمر رقم سري واحد بنظام الترميز 3^n–ary في المجموعة والهدف منها لزيادة كمية المعلومات التي ستطمر في الصورة.

3- الطريقة المقترحة

التحدي الرئيسي في عملية إخفاء المعلومات يكمن في بناء علاقة متوازنة ما بين جودة الصورة (quality) وحجم البيانات (payload) التي سوف تطمر بداخلها. بالإضافة إلى، قوة التقنية في مواجهة الهجمات الالكترونية والحفاظ على سرية البيانات. لذلك، تهدف هذه الطريقة إلى إخفاء اكبر كمية من البيانات مع المحافظة على جودة الصورة وعدم حدوث أي تغيير او تشويه على الصورة (stego image) بعد طمر البيانات داخلها بالإضافة إلى الحصول على سرية عالية في إخفاء البيانات داخل الصورة (cover image).

3-1 عملية تحضير الرسالة السرية

في البدء، ستتم كتابة الرسالة السرية التي سيتم طمرها داخل الصورة بصيغة نص اعتيادي من الأحرف الأبجدية الانكليزية. ان تقليل حجم الرسالة سوف لن يؤثر فقط على زيادة كمية البيانات (Payload) التي ستطمر في الصورة ولكن ايضا سيقلل من احتمالية اكتشاف وجود الرسالة داخل الصورة. لذلك، تستخدم خوارزمية الـ LZW لتشفير وكبس أحرف الرسالة السرية ومن ثم تحويلها إلى سلسلة من الارقام الثنائية لحماية البيانات وتقليل حجمها لذلك تستخدم هذه الخوارزمية بشكل كبير من قبل الباحثين في مجال إخفاء المعلومات [22,21].

في هذه الطريقة، سيتم بناء جدول لاستبدال سلسلة الاحرف الشائعة الاستخدام في الرسالة السرية بسلسلة من الارقام الثنائية لغرض حماية البيانات وكبس هذه السلسلة لتقليل حجم الأحرف وزيادة كمية البيانات التي سيتم طمرها داخل الصورة. هذا الجدول يعرف بالقاموس (dictionary) والذي سيتم استخدامه من قبل الشخص المستلم للرسالة خلال مرحلة الاسترجاع وفك الشفرة.

3-2 عملية طمر المعلومات في الصورة

تمثل هذه المرحلة عملية تهيئة الصورة لغرض طمر المعلومات بداخلها. حيث سيتم استخدام خوارزميتين لغرض طمر المعلومات هما الـ EMD والـ knight tour. في البدء، ستتم عملية تحضير الصورة قبل اجراء عملية طمر المعلومات فيها من خلال تقسيم الصورة إلى مجاميع وكل مجموعة تتكون من اربعة بكسل. حيث ان، عدد المجاميع gr في الصورة يمثل تقسيم حجم الصورة على n. بعد ذلك، سيتم تكوين كتل بحجم 4*4 مجموعة للكتلة الواحدة. بعدئذ، سيتم استدعاء خوارزمية الـ knight tour لغرض اختيار المجاميع التي سيتم تغيير قيمة بكسل محددة فيها لغرض طمر المعلومات بداخلها باستخدام خوارزمية الـ EMD.

3-2-1 خوارزمية Knight tour

تستخدم هذه الطريقة لغرض التغلب على إحدى نقاط الضعف في طريقة الـ EMD في الاختيار المتسلسل للمجاميع التي سيتم طمر المعلومات فيها. في هذه التقنية، سيتم اختيار المجاميع التي سيتم طمر الارقام السرية فيها والتي تكون على الأغلب غير معروفة من قبل الأشخاص غير مخولين باستلام الرسالة السرية. بعد ان يتم اختيار أول مجموعة لغرض طمر البيانات بداخلها يتم الانتقال إلى المجموعة التالية التي سيتم اختيارها لطمر البيانات باستخدام خوارزمية الـ Knight Tour . في هذه الطريقة، بعد عملية تقسيم الصورة إلى كتل يتم تمثيل الصورة على أنها عبارة عن رقعة شطرنج كبيرة. من خلال هذه الخوارزمية سيتم تحديد الاتجاه الذي سيستخدم لاختيار المجموعة التالية من خلال تحديد حركة الحصان في رقعة الشطرنج (chessboard) والتي ستكون اما صف واحد وعمودين او يمكن ان تكون صفين وعمود واحد باتجاهات متنوعة والتي تتمثل بشكل حرف (L) [23]. ومن خلال استخدام هذه الطريقة، فان اختيار المجاميع من خلال هذه التقنية ستكون مجهولة في حالة استلامها من قبل الأشخاص غير المخولين وسيزيد من صعوبة معرفة فك الأرقام السرية للرسالة. حيث أن، كل رقم سري من البيانات سوف يتم طمرها داخل المجموعة التي سيقع عليها الاختيار في الصورة وذلك لغرض زيادة القوة (robustness) للطريقة في مواجهة الهجمات المحتملة. والخطوات المستخدمة في هذه الطريقة ستكون كالاتي:

زياد صفاء

الإدخال : الصورة (cover image) بحجم M*N.

الإخراج : المجاميع التي تحتوي على $n = 4$ بكسل التي سيتم اختيارها لغرض طمر البيانات فيها.

الخطوة رقم ١: تقسيم الصورة الى كتل بحجم 4*4 مجموعة للكتلة الواحدة. حيث ان b تمثل عدد الكتل في الصورة.

الخطوة رقم ٢:تحديد الموقع الأول الذي ستبدأ منه الخوارزمية لاختيار المجاميع من خلال تمثيل الكتلة على انها عبارة عن رقعة شطرنج (مصفوفة ثنائية) بحجم (m*c). حيث ان، m تمثل عدد الصفوف في الكتلة بينما c تمثل عدد المجاميع في كل صف.

الخطوة رقم ٣: نعطي i=1 , j=1 , k=1 .

الخطوة رقم ٤: while (k<=b).

الخطوة رقم ٥: i يمثل عداد من 1 الى m.

j تمثل عداد من 1 الى c.

الخطوة رقم ٦:البدء باختيار مجموعة جديدة من خلال تحديد اتجاه الحركة لاختيار المجموعة التالية التي سيتم طمر البيانات فيها. حيث ان، اذا كانت المجموعة الحالية هي gr (i,j) فان المجموعة التالية التي سيتم اختيارها لغرض طمر المعلومات فيها من خلال تحديد اتجاه الحركة سيكون كما يلي:

- اذا كانت gr(i+1,j+2) لم يتم استخدامها لطمر المعلومات وان i+1<m , j+2< c فان : gr(i+1,j+2) سيتم اختيارها لطمر المعلومات بداخلها i=i+1 , j=j+2.
- والا اذا كانت gr(i+1,j-2) لم يتم استخدامها لطمر المعلومات وان i+1<m , j-2>= 1 فان: gr(i+1,j-2) سيتم اختيارها لطمر المعلومات بداخلها i=i+1 , j=j-2.
- والا اذا كانت gr(i-1,j+2) لم يتم استخدامها لطمر المعلومات وان i-1>=1 , j+2<c فان: gr(i-1,j+2) سيتم اختيارها لطمر المعلومات بداخلها i=i-1 , j=j+2.
- والا اذا كانت gr(i-1,j-2) لم يتم استخدامها لطمر المعلومات وان i-1>=1 , j-2>=1 فان: gr(i-1,j-2) سيتم اختيارها لطمر المعلومات بداخلها i=i-1 , j=j-2.
- والا اذا كانت gr(i+2,j+1) لم يتم استخدامها لطمر المعلومات وان i+2<m ، j+1<c فان : gr(i+2,j+1) سيتم اختيارها لطمر المعلومات بداخلها i=i+2, j=j+1.
- والا اذا كانت gr(i+2,j-1) لم يتم استخدامها لطمر المعلومات وان i+2<m ، j-1>=1 فان : gr(i+2,j-1) سيتم اختيارها لطمر المعلومات بداخلها i=i+2 , j=j-1.
- والا اذا كانت gr(i-2,j+1) لم يتم استخدامها لطمر المعلومات وان i-2>=1 ، j+1<c فان : gr(i-2,j+1) سيتم اختيارها لطمر المعلومات بداخلها i=i-2 , j=j+1.
- والا اذا كانت gr(i-2,j-1) لم يتم استخدامها لطمر المعلومات وان i-2>=1 ، j-1>=1 فان : gr(i-2,j-1) سيتم اختيارها لطمر المعلومات بداخلها i=i-2 , j=j-1.

الخطوة رقم ٧: تكرار الخطوة رقم ٦ لحين الانتهاء من اختيار المجاميع التي ستطمر فيها الرسالة السرية داخل الكتلة.

الخطوة رقم ٨: الانتقال الى الكتلة التالية k=k+1 .

2-2-3 خوارزمية الـ EMD

بعد الانتهاء من عملية اختيار المجاميع التي ستطمر بداخلها المعلومات باستخدام خوارزمية الـ Knight tour سيتم اجراء عملية طمر المعلومات باستخدام خوارزمية الـ EMD. تستخدم خوارزمية الـ EMD نظام الترميز (2n+1)-ary لتمثيل الأرقام السرية التي ستطمر داخل الصورة (cover image). حيث أن، الأرقام السرية التي تم

زياد صفاء

الحصول عليها باستخدام طريقة الـ LZW سيتم طمرها داخل المجموعة من خلال إضافة او طرح واحد من قيمة البكسل المحدد في المجموعة. المعادلة رقم (1) تستخدم لغرض حساب قيمة دالة الاسترجاع التي يرمز لها بالرمز f لكل البكسل داخل المجموعة حيث أن :

$$f = f(g_1,g_2,..,g_n)=[\sum_{i=1}^{n}(g_i \times i) \bmod (2n+1)]...(1)$$

حيث ان $(g_1,g_2,..,g_n)$ تمثل قيم البكسل داخل المجموعة بينما n تمثل عدد البكسل في المجموعة. بعد ان يتم جمع قيمة f سيتم مقارنتها مع قيمة الرقم السري التي سيرمز له بالرمز d. اذا كانت $d=f$ لا يوجد حاجة لتغيير قيمة البكسل وذلك بسبب أن قيمة الرقم السري ستكون مساوية لقيمة دالة الاسترجاع المأخوذة من مجموع البكسل الأصلية . أما في حالة أن $d \neq f$ نقوم بحساب قيمة مؤشر الصورة sالتي تمثل الفرق مابين قيمتي (d,f) باستخدام المعادلة رقم (2):

$$s = d - f .mod(2n+1)...(2)$$

بعد ذلك، من خلال استخدام المقارنة التالية إذا كانت قيمة s $\leq n$ في هذه الحالة ستزداد قيمة البكسل g_s بمقدار 1. أما في حالة كون $s > n$ فسيتم تقليل قيمة البكسل g_{2n+1-s} بمقدار 1. الخطوات المستخدمة في هذه الخوارزمية يمكن توضيحها كما يأتي:

الإدخال: الصورة (cover image) بحجم $M*N$، المجاميع التي تم اختيارها لغرض طمر البيانات، الارقام السرية d

الإخراج: الصورة بعد طمر الشفرات فيها (stego image).

الخطوة رقم ١: $n=4$ *تمثل عدد البكسل في كل مجموعة.*

الخطوة رقم ٢: k *تمثل طول الرسالة السرية،* $m=1$.

الخطوة رقم ٣: $while \ \ m<=k$.

الخطوة رقم ٤: المجموعة التي تم اختيارها لغرض طمر البيانات فيها باستخدام خوارزمية الـ Knight tour.

الخطوة رقم ٥: نعتبر أن i تمثل عداد من 1 إلى n.

$f = sum\ (g_i \times i)\ mod\ (2n+1)$ نهاية التكرار i.

الخطوة رقم ٦: إذا كانت $f \neq d$ فان $s=d - f \bmod (2n+1)$.

الخطوة رقم ٧: إذا كانت قيمة $s \leq n$ إذن تزداد قيمة g_s بمقدار 1.

الخطوة رقم ٨: إذا كانت قيمة $s > n$ إذن تتناقص قيمة $g_{(2n+1-s)}$ بمقدار 1.

الخطوة رقم ٩: $m=m+1$.

الخطوة رقم ١٠: نهاية التكرار m.

3-3 عملية استرجاع الرسالة السرية

بعد اكتمال عملية طمر المعلومات في الصورة يقوم المرسل بإرسال الصورة (stego image) التي تحتوي على الرسالة السرية. عملية الاتصال ستكتمل عندما يتم استلام الرسالة من قبل الشخص المخول باستلامها. وان المستلم يجب أن يكون له القدرة على تحديد وجود الرسالة السرية داخل الصورة. لذلك، ولغرض استرجاع محتويات الرسالة من الصورة وإعادة صياغتها إلى شكلها الأصلي ستكون هناك مجموعة من الخطوات. في البدء، سيتم تقسيم الصورة الى كتل بحجم 4*4 مجموعة وكل مجموعة تحتوي على اربعة بكسل. بعد ذلك، تستخدم خوارزمية الـ Knight tour لتحديد أي من المجاميع المكونة للصورة (stego image) تحتوي على الرسالة من خلال اعتبار الصورة على انها لوحة شطرنج وباستخدام نفس اتجاه الحركة المستخدم في مرحلة الطمر لتحديد المجموعة التي تحتوي على الأرقام السرية للرسالة المخفية. من ثم، تستخدم خوارزمية الـ EMD لغرض استرجاع الأرقام السرية للرسالة باستخدام المعادلة رقم (3).

$$d = f(g'_1,g'_2,...,g'_n)=[\sum_{i=1}^{n}(g'_i \times i)]mod(2n+1)...(3)$$

زياد صفاء

حيث ان، d تمثل قيمة الرقم السري الذي سيتم استخراجه من المجموعة في الصورة، n تمثل عدد البكسل في المجموعة بينما $(g'_1, g'_2, \ldots, g'_n)$ تمثل قيم البكسل في المجموعة التي تحتوي على الرقم السري المطمور في الصورة (stego image). بعد ذلك ، الأرقام السرية المستخرجة من المجاميع سيتم تحويلها إلى أرقام بالنظام الثنائي لتكوين سلسلة من البتات ثم يتم تحويل هذه السلسلة الى النظام العشري للحصول على الشفرة السرية. بعد ذلك، وباستخدام خوارزمية LZW الشفرة السرية سيتم فك تشفيرها للحصول على الرسالة الأصلية للنص. والخطوات المستخدمة في عملية الاسترجاع يمكن توضيحها كما ياتي:

الإدخال: الصورة (stego image) بحجم $M*N$.

الإخراج: الأرقام السرية d.

الخطوة رقم ١: h *تمثل طول الرسالة السرية ،* $a=1$.

الخطوة رقم ٢: $n=4$ *تمثل عدد البكسل في كل مجموعة.*

الخطوة رقم ٣: *while(* $j<=h$ *)*

الخطوة رقم ٤: تحديد المجاميع التي تم طمر البيانات فيها باستخدام خوارزمية الـ Knight tour.

الخطوة رقم ٥: i تمثل عداد من 1 إلى n.

$d= sum\ (g'_i \times i)\ mod\ (2n+1)$ نهاية التكرار i.

الخطوة رقم ٦: تحويل الأرقام السرية d إلى نظام الترميز الثنائي.

الخطوة رقم ٧: a=a+1.

الخطوة ٨: اذا كانت a > h اذن الذهاب الى الخطوة رقم ١٣ والا

الخطوة رقم ٩: تحويل الأرقام بالنظام الثنائي إلى أرقام بالنظام العشري.

الخطوة رقم ١٠: j=j+1.

الخطوة رقم ١١: تكرار الخطوة رقم ٨

الخطوة رقم ١٢: نهاية التكرار j

الخطوة رقم ١٣: فك شفرة الأرقام الناتجة وتحويلها إلى الأحرف التي تمثلها في الرسالة الأصلية من خلال استخدام خوارزمية LZW

4- النتائج العملية:

تمثل عملية طمر اكبر كمية من المعلومات مع الحفاظ على جودة الصورة وجعلها مشابهة للصورة الأصلية وكذلك الحفاظ على سرية المعلومات هو الهدف الرئيسي من هذا البحث. هناك عدة عوامل تستخدم في عملية التقييم وهي:

١- Imperceptibility وهي تمثل عدم القدرة على اكتشاف وجود الرسالة داخل الصورة (stego image).

٢- Payload تمثل اكبر كمية من البيانات التي يمكن طمرها داخل الصورة.

٣- Robustness تمثل قوة الطريقة المقترحة في مواجهة الهجمات الالكترونية على الصورة الحاملة للبيانات.

سيتم اختبار الطريقة المقترحة من خلال استخدام أربعة صور رمادية بحجم 512*512 بكسل. هذه الصور سوف تستخدم لإخفاء المعلومات بداخلها. وهي تحتوي على قيم رمادية متنوعة تساعد في الحصول على نتائج دقيقة لتقييم الـ Imperceptibility.

شكل رقم (1) الصور المستخدمة لتقييم الدراسة

زياد صفاء

لغرض تقييم الـ Imperceptibility للصورة (stego image) يتم استخدام مقياس الـ PSNR وحسب المعادلة رقم (4):

$$PSNR = 10log_{10}\frac{255^2}{MSE} \ldots(4)$$

حيث ان MSE يمثل متوسط مربعات الخطأ (Mean Square Error) ما بين البكسل والتي تحسب قيمته باستخدام المعادلة رقم (5) .

$$MSE = \sum_{i=1}^{M*N} (g_i - g_i')^2 / (M * N) \ldots(5)$$

حيث ان $M*N$ تمثل حجم الصورة بينما g_i و g_i' تمثل قيمة البكسل قبل وبعد طمر المعلومات في الصورة.

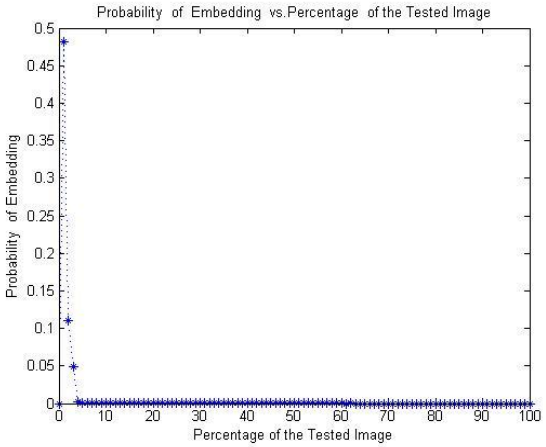
الجدول رقم (1) يظهر نتائج المقارنة ما بين الطريقة المقترحة والطرق السابقة اعتمادا على كمية وحجم البيانات (Payload) التي تم طمرها داخل الصورة وباستخدام نفس الصور (dataset) لغرض التقييم. نلاحظ ان قيمة الـ PSNR للطريقة المقترحة هي 54.80 dB عند استخدام حجم كامل من البيانات لطمره في الصورة وهو 65536 byte وان قيمة الـ PSNR لطريقتي EMD وOpt EMD هي تجاوز السعة (overflow) بسبب أن حجم البيانات تجاوز الحد الأعلى المسموح به من البيانات التي يمكن طمرها داخل الصورة باستخدام هاتين الخوارزميتين. في حين، ان قيمة الـ PSNR عندما يكون حجم البيانات المطمورة فيها 49152 byte و32768 byte و 16384 byte هو 55.08 dB و 56.62 dB و59.88 dB على التوالي للطريقة المقترحة. النتائج العملية توضح ان قيمة الـ PSNR للطريقة المقترحة أفضل من الطرق السابقة مع القدرة على طمر اكبر كمية من البيانات السرية داخل الصورة من دون التأثير على جودتها.

جدول رقم (1) المقارنة مابين الطريقة المقترحة والطرق السابقة.

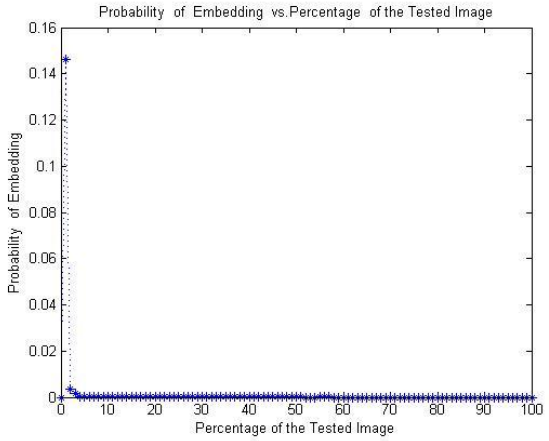
الطرق المستخدمة	حجم البيانات Payload	مقياس الـ PSNR للصور (dataset)				معدل الـ PSNR
		Lena	Baboon	Airplane	Tiffany	
الطريقة المقترحة	65536 byte	54.79	54.79	54.82	54.81	54.80
طريقة Opt EMD [1]		تجاوز الحد المسموح من البيانات overflow				
طريقة EMD [7]		تجاوز الحد المسموح من البيانات overflow				
الطريقة المقترحة	49152 byte	55.08	55.09	55.12	55.06	55.08
طريقة Opt EMD [1]		52.11	52.11	52.10	52.11	52.11
طريقة EMD [7]		52.11	52.11	52.10	52.11	52.11
الطريقة المقترحة	32768 byte	56.86	56.85	55.89	56.90	56.62
طريقة Opt EMD [1]		54.67	54.66	54.67	54.66	54.66
طريقة EMD [7]		53.86	53.87	53.87	53.86	53.87
الطريقة المقترحة	16384 byte	59.84	59.92	59.85	59.93	59.88
طريقة Opt EMD [1]		58.37	58.38	58.36	58.36	58.37
طريقة EMD [7]		56.88	56.89	56.89	56.88	58.89

لغرض تقييم السرية والقوة Robustness للطريقة المقترحة سيتم استخدام طريقة إحصائية وهي طريقة x^2 حيث يتم استخدام التحليل الإحصائي بدلا من الفحص الفيزيائي يتم توليده على الصورة لغرض معرفة هل الصورة تحتوي على رسالة سرية أم لا [24]. تستخدم هذه الطريقة الاختلاف ما بين التوزيع الترددي المتوقع للصورة والتوزيع الترددي الذي سيتم الحصول عليه خلال عملية التحليل [25]. إذا كانت القيمة الناتجة من التحليل قريبة من الواحد معنى هذا وجود رسالة سرية داخل الصورة أما إذا كانت القيمة قريبة أو مساوية للصفر فهذا يعني أن التردد الناتج هو مشابه للتردد الأصلي للصورة ولا وجود لرسالة سرية بداخلها. الشكل رقم (2) يمثل الصورة (Lena) قبل وبعد اجراء عملية الطمر فيها بينما الشكل رقم (3) والشكل رقم (4) يمثلان استخدام طريقة x^2 على الصورة (Lena) الاصلية وعلى نفس الصورة بعد طمر الرسالة السرية بداخلها.

شكل رقم (2) الصورة Lena قبل وبعد اجراء عملية الاخفاء



شكل رقم (3) نتيجة توليد طريقة x^2 على الصورة Lena قبل عملية الاخفاء



شكل رقم (4) نتيجة توليد طريقة x^2 على الصورة Lena بعد عملية الاخفاء

من الشكلين أعلاه، ومن خلال توليد طريقة x^2 على الصورة قبل وبعد إخفاء البيانات بداخلها نلاحظ أن الصورتان تعطيان نفس التوزيع الترددي وبالنتيجة فان الشخص المهاجم (stego analysis) سوف لن يكتشف وجود الرسالة السرية داخل الصورة (stego image) مما يشير إلا أن الطريقة المقترحة تكون قوية في مواجهة الهجمات الالكترونية مع الحفاظ على سرية المعلومات.

5-الاستنتاجات

في هذه الدراسة، تم اقتراح طريقة لإخفاء المعلومات من خلال استخدام تقنية الـ EMD وخوارزميتي Knight tour و LZW. الطريقة ستبدأ من خلال تشفير وكبس البيانات باستخدام تقنية الـ LZW حيث ان كل من المرسل والمستلم سيكون لديه جدول لغرض تشفير وفك شفرة الرسالة السرية يسمى بالقاموس. بعد ذلك، الأرقام السرية للرسالة سيتم إخفائها داخل الصورة من خلال استخدام خوارزمية الطمر المقترحة. ولغرض إضفاء اكبر قدر من السرية للطريقة المقترحة وجعلها أكثر قوة في مواجهة الهجمات تم اختيار خوارزمية الـ Knight tour لغرض تحديد المجاميع التي سيتم طمر المعلومات بداخلها لغرض التغلب على مشكلة الاختيار التسلسلي للمجاميع في تقنية الـ EMD الأصلية والتي من السهولة تحديدها واستخراج البيانات منها. النتائج العملية تظهر أن كل من الـ PSNR و Payload للطريقة المقترحة أفضل بالمقارنة مع الطرق السابقة. بالإضافة إلى القوة Robustness في مواجهة

الهجمات الالكترونية. في الأعمال المستقبلية، من الممكن استخدام تقنيات ذكائية لغرض تحسين عمل خوارزمية الـ EMD وكذلك من الممكن استخدام طرق إحصائية أخرى لاختبار الطريقة المقترحة في مواجهة الهجمات .

المصادر

[1] K. Lin, w. Hong, J. Chen, T. Chen and w. Chiang " Data Hiding by Exploiting Modification Direction Technique Using Optimal Pixel Grouping ", 2nd international Conference on Education Technology and Computer (ICETC) ,(2010).

[2] N. Provos and P. Honeyman, "Hide and Seek: An Introduction to Steganography", IEEE Security and Privacy Magazine, 1(3), 32-44,(2003).

[3] S. Joshi and S. Nipanikar, "Implementation Of Exploiting Modification Direction (Emd) - A Steganography Technique Using Raspberry Pi", International Journal Of Current Engineering And Scientific Research (IJCESR),2(8),(2015).

[4] W. Kuo, J. Cheng and C. Wang, "Data Hiding Method With High Embedding Capacity Character", International Journal of Image Processing (IJIP), 3(6), (2010).

[5] عبد المجيد، أنسام أسامة،، "طريقة جديدة للكتابة المغطاة في الصور المكبوسة بالتكميم الاتجاهي" ، رسالة ماجستير مقدمة الى قسم الحاسوب، كلية علوم الحاسوب والرياضيات، جامعة الموصل (2011).

[6] M. Habibi, R. Karimi, and M. Nosrati " Using SFLA and LSB for Text Message Steganography in 24-Bit RGBColor Images", International Journal of Engineering, 2(3), 68-75,(2013).

[7] X. Zhang and S. Wang, "Efficient Steganographic Embedding by Exploiting Modification Direction", IEEE Communications Letters, 10(11),781-783 ,(2006).

[8] محمد، همسة معن، محمد، نادية معن، محمد، شيماء شكيب، "طريقة خوارزمية جينية مثلى للإخفاء"، المجلة العراقية للعلوم الاحصائية عدد خاص بوقائع المؤتمر العلمي الرابع لكلية علوم الحاسوب والرياضيات – جامعة الموصل، 11(20)،(2011).

[9] A. Cheddad, J. Condell, K. Curran and P. McKevitt, "Digital image steganography: Survey and analysis of current methods", Signal Processing, 90, 727-752,(2010).

[10] C. Hsing and S. Jeng, "Transforming LSB Substitution for Image-based Steganography in Matching Algorithms" , Journal of Information Science and Engineering, (2010).

[11] M. Kalra and P. Singh ,"EMD Techniques of Image Steganography A Comparative Study", International Journal Of Technological Exploration And Learning (IJTEL), 3(2),(2014).

[12] R. Hassan and G. Sulong, " A New Colour Image Steganography Using LSB Approach With Halftoning Determination Embedding Position", International Journal of Scientific & Engineering Research,5(4),285-291,(2014).

[13] K. Jung and K. Yoo, "Improved Exploiting Modification Direction Method by Modulus

[14] X. Niu, M. Ma, R. Tang and Z. Yin "Image Steganography via Fully Exploiting Modification Direction", International Journal of Security and Its Applications, 9(5),(2015).

[15] W. Kuo , M. Kao and C. Chang " A Generalization of Fully Exploiting Modification Directions Data Hiding Scheme" , Journal of Information Hiding and Multimedia Signal Processing,6,(2015).

[16] C. Chan and L. Cheng, "Hiding Data in Images by Simple LSB Substitution," Pattern Recognition, 37, 469-474,(2004).

[17] E. Adelson., "Digital signal encoding and decoding apparatus", US Patent, no. 4939515, (1990).

[18] C. Lee, Y. Wang and C. Chang, "A Steganography Method With High Capacity By Improving Exploiting Modification Direction", Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP), 1, 497 – 500,(2007).

[19] W. Kuo and C. Wang " Data hiding based on generalized exploiting modification direction method", The Imaging Science Journal,61, (2013).

[20] C. Chang and H. Wu, "A Large Payload Information Hiding Scheme Using Two Level Exploiting Modification Direction", Tenth International Conference On Intelligent Information Hiding And Multimedia Signal Processing IEEE,(2014).

[21] I. Kajal, H. Rohil, A. Kajal, " LZW based Image Steganography using Kekre's Algorithm ", International Journal of Computer Science and Information Technologies, 5(2), (2014).

[22] S. Goel P. Kumar R. Saraswat, "High Capacity Image Steganography Method Using LZW, IWT and Modified Pixel Indicator Technique", International Journal of Computer Science and Information Technologies,5(3),(2014).

[23] S. Ganzfried, "A New Algorithm For Knight's Tours", REU program in Mathematics at Oregon State University, (2004).

[24] A. Nissar, & A. Mir, "Classification of steganalysis techniques: A study on Digital Signal Processing", 20, 1758-1770, (2010).

[25] A. Westfeld, and A. Pfitzmann, ,"Attacks on steganographic systems. Information Hiding", Springer, 61-76, (2000) .

Image Steganography by Using Exploiting Modification Direction and Knight Tour Algorithm

ZEYAD SAFAA YOUNUS ALSAFFAWI

College of computer Sciences and Mathematics University of Mosul

Email: ziead_1979@yahoo.com ; zeyad.s.safawi@gmail.com

Abstract :

In this study, a new technique for information hiding have been proposed by using Exploiting Modification Direction (EMD) technique and enhanced it by using Knight Tour algorithm for embedded the information within the image and by using LZW for encrypt and compress the secret message. In this technique, LZW have been used for the purpose of encrypted, compressed and transformed the characters of secret message into stream of bits for the purpose of protect and reduce the size of the message. In the next step, the EMD technique and Knight tour algorithm have been used to embed the secret digits where the cover image is segmented into groups. Each group have 4 pixels. Afterward, the image is segmented into blocks size (4*4) group for each block. The (2n+1)-ary notational system is used to represent the secret digits for the message that embedded within image. To increase the robustness and the security for the proposed method the Knight tour algorithm is used to select which group can be used to hide the secret digit. Where, one secret digit is embedded by modifying one gray-scale value for the particular pixel inside the group by using EMD technique. Afterward, the statistical attacks by using x^2 method is applied on the stego image to assess the robustness of the proposed method against the attacks. The experimental results have depicted that the PSNR and the Payload of proposed method is better than the previous methods that used in Steganography.