تقنيتي آلة المتجه الداعم ومميز فيشر الخطي للكشف عن الإخفاء في JPG

سماح فخري عزيز

قسم علوم الحاسوب، كلية التربية، جامعة الحمدانية، موصل – العراق.

أحمد سامي نوري

قسم علوم الحاسوب، كلية علوم الحاسوب والرياضيات، جامعة الموصل.

المستخلص

يعد الإخفاء (Steganography) النظام الجديد والمتمم لعلم التشفير الذي استغرق وقتاً طويلاً في تناقل الرسائل السرية والمهمة عبر الشبكات والانترنيت. ومن ثم ظهر ما يقابل الإخفاء من علم تحليل وكشف محتوى الرسائل السرية فكان علم كشف الإخفاء (Steganalysis).

لغرض الكشف عن الاخفاء في الصور الملونة تم العمل على تقنيتين مهمتين في عمليات التصنيف تسمى الأولى آلة المتجه الداعم SVM (Support Vector Machine) والثانية مميز فيشر الخطي FLD (Fisher Linear Discriminator).

إذ تم استخدام تقنية SVM مع فكرة التطبيق الأعمى، في حين تم استخدام FLD مع أفكار التطبيق الأعمى وغير الأعمى. اما الصور الملونة فكان الاختيار للنوع المميز بالامتداد JPG. وأثبتت النتائج الكفاءة العالية للتقنيتين في الكشف عن الصور التي تحوي الرسائل السرية وتفاوتت المقارنات مابين التقنيتين من ناحية نسبة الكشف ومقدار الخطأ وزمن التنفيذ.

الكلمات المفتاحية: علم الاخفاء، آلة المتجه الداعم، مميز فيشر الخطي، علم تحليل الاخفاء، نسبة الكشف، صور JPG.

SVM and FLD Techniques for Steganalysis in JPG

Samah F. Aziz
Department of Computer Science, College of Education, AlHamdaniya University, Mosul – Iraq.
Ahmed S. Nori
Department of Computer Science, College of Computer Science and Mathematics, Mosul University, Iraq.

Abstract

Steganography is considered as the new and the complementary system of Cryptography that took a long time in transferring secret and important messages through the networks and the Internet. Then there was the emergence of what complements Steganography as a science that analysis and discover the content of the secret messages and this science is (Steganalysis).

For Steganalysis in colored images, the work relied on two important technologies; the first is called Support Vector Machine (SVM) and the second is called Fisher Linear Discriminator (FLD). The SVM technology has been used with the (blind) application idea while FLD has been used with the (blind and non-blind) application ideas using best type of colored images JPG.

Results proved the high efficiency of the two technologies in detecting the image that includes the secret messages and comparisons were varied between the two technologies in terms of detection rate, fault and the execution time.

Keywords: Steganography, Support Vector Machine (SVM), Fisher Linear Discriminator (FLD), Steganalysis, Detection rate, JPG images.

المقدمة:

خلال السنوات الماضية، أصبح علم أمن المعلومات محل اهتمام الكثير من الباحثين الذين تحاول جهودهم أن تتوصل إلى حلول وتقنيات جديدة لضمان حماية المعلومات التي ترسل وتستقبل عبر الانترنيت من دون حدوث أي اختراق أو كشف، لذلك كان لابد من تطوير أمنية المعلومات وإنشاء تقنيات ووسائل جديدة، من هنا ظهر علم إخفاء المعلومات (Information Hiding) الذي تضمّنَ تقنية الإخفاء (Steganography). إذ تعد تقنية الإخفاء من طرائق الحماية التي تجعل الاتصال غير مرئي عن طريق إخفاء رسائل معينة داخل غطاء معين.

تهدف تقنية الإخفاء (Steganography) إلى إخفاء البيانات داخل بيانات أخرى، بطريقة لا تؤدي إلى التأثير في هذه الأخيرة، بحيث لا تثير أي شبهة أو شك قد يؤديان إلى كشف المعلومات المخفية.

إن الذي شجع على إحياء وتطوير تقنية الإخفاء هو هذا الانفجار الهائل في تقنية الحاسوب والاتصالات، والشيء المميز فيها أنها تواكب التقنيات الحديثة واستخداماتها في جميع الوسائط الحاسوبية من صور ونصوص وصوت وفيديو...الخ. إذ أصبحت أمنية المعلومات من الموضوعات الحساسة والمهمة جدا في حياة البشر خاصة بعد انتشار الحكومات الالكترونية في معظم دول العالم[1].

القصد من هذه المقدمة، أنه مع تطور العلم والأساليب المستخدمة في الإخفاء فهنالك أساليب تتطور بموازاتها في فن تحليل وكسر هذا العلم. فهدف القائم بالإخفاء هو عدم إثارة أي نقطة للشك بوجود بيانات مخفية، أما هدف محلل الإخفاء هو الشك في كل الرسائل المُرسَلة، و فحصها للتأكد من وجود بيانات مخفية مرسلة. تسمى العملية التي تتم فيها محاولة طرف ما اكتشاف وجود المعلومات المخفية، أو قراءتها، أو تغييرها أو حذفها بـ Steganalysis[2].

٢- الدراسات السابقة

في عام ٢٠٠٣ قدم الباحثان Hany Farid و Siwei Lyu **بحثاً يصف طريقة** Multi-scale Wavelet Decomposition **يعتمد على بناء أنموذج إحصائي**

Higher Order لكشف البيانات المخفية في الصور الرمادية. ويستعمل تقنية آلة المتجه الداعم Support Vector Machine (SVM) لكشف هذه الاختلافات الإحصائية في صورة الاختبار[6].

قدم الباحثون Jiang وWong وMemon وWu عام ٢٠٠٥ تقنية Steganalysis جديدة في صور Halftone من دون معرفة صورة الغطاء الأصلي. بالاعتماد على تقنية Fisher Linear Discriminant (FLD) Analysis وسيتم التمييز بين الصور الأصلية والمخفية[5].

في عام ٢٠٠٦ قدم الباحثان Hany Farid وSiwei Lyu بحثاً اقترح Steganalysis عالمياً يستخدم Higher Order Statistics عن طريق Wavelet Decomposition يعتمد على QMF للحصول على إحصائيات الصورة. مع اعتماد One Class and Multi Class SVM للتصنيف. من مساوئ الخوارزمية أن عدد الميزات المطلوب لتدريب SVM يكون عالياً[8].

أما في عام ٢٠٠٧ قدم الباحثون Ge وGao وWang بحثاً اقترحوا فيه أنموذجاً عاماً لتطبيق تقنيات تعليم الآلة لكشف المعلومات المخفية باستخدام تقنية إخفاء في البت الأقل أهمية. والاعتماد على مصنف إحصائي لتصنيف الصور[4].

وفي عام ٢٠٠٩ قدم الباحث Zhang بحثاً يقترح فيه طريقة كشف جديدة وهي كشف LSB matching. يتم حساب كل من المدرج الإحصائي لصورة الاختبار وLocal Maximums وLocal Minimums ومن ثم حساب المنطقة بين Upper Envelope وLower Envelope للمدرج الإحصائي، ويتم تحويل المدرج الإحصائي باستخدام DWT لحساب الفرق بين كل من Local Maximums و Local Minimums وNeighbors للحصول على ميزات الصورة، وإدخال هذه الميزات إلى Fisher linear discriminator لتصنيف الصور[10].

٣- الإخفاء وتحليل الإخفاء

إخفاء المعلومات ضمن وسط إلكتروني يتطلّب تعديلات على خصائص ذلك الوسط التي قد تُقدم شكلاً من الاضمحلال أَو الخصائص غير العادية، هذه الخصائص قد تمثل كالتواقيع التي أذاعت وجود الرسالة المُضَمَّنة، وهذا يضعف الغرض من الإخفاء.

تحليل الإخفاء Steganalysis هو علم اكتشاف الرسائل المخفية باستخدام الإخفاء. من الناحية الأخرى، Steganalysis يمكن أن يعمل بوصفه طريقة فعالة لتحكيم أداء أمن تقنيات الإخفاء[9]. الهدف من Steganalysis أن يكتشف وجود الرسالة السرية في الأجسام (objects) يُميز الأجسام بالرسالة السرية مِن الأجسام من دون أي رسالة سرية.

الهجمات والتحليل على المعلومات المخفية قد تأخذ عدة أشكال: اكتشاف أو انتزاع أو تعطيل أَو تحطيم المعلومات المخفية. المهاجم قد يُضمّن معلومات مضادة أيضاً على المعلومات المخفية. إن Steganalysis بشكل عام يُحاول هزيمة هدف الإخفاء باكتشاف المعلومات المخفية واستخلاصها أو تحطيمها.

عملية كشف الإخفاء تتم من قبل جهة أخرى غير المرسل والمستقبل وهو محلل الإخفاء Steganalyst وهو الشخص الذي يطبق تحليل الإخفاء في محاولة لكشف وجود المعلومات المخفية. [1]

٤- الهجمات على الإخفاء

جَذب الإخفاء وتحليل الإخفاء الكثير من الانتباه حول العالم في المستقبل القريب، وذلك لاهتمام البعض بضمان اتصالاتهم خلال إخفاء حقيقة خاصة بأنهم يتبادلون المعلومات وآخرون يهتمون باكتشاف وجود مثل هذه الاتصالات. لهذا السبب كانت الحاجة لتصميم وتقييم تقنيات كشف قوية قادرة على تفادي أو تقليل مثل هذه الأعمال[7].

يُمكن أَن تكون الهجمات على الإخفاء بأنواع مختلفة تعتمد على الأسباب أَو الغرض من الهجوم ضد بيانات stego. يمكن تصنيف أنواع الهجمات على الإخفاء إلى صنفين عامّين هما:

١- **الهجوم السلبي Passive Attacks:** هذا الهجوم يكشف حضور أو غياب الرسالة السرية المتضمنة في بيانات stego أو تحديد نوع تضمين الخوارزمية المستخدمة، والمهاجم قادر على اعتراض البيانات فقط. وتتضمن:

- ❖ فحص الوسط إذا كان يحتوي على رسالة سرية أم لا؟.
- ❖ استخلاص الرسالة السرية إذا كان بالإمكان استخلاصها.
- ❖ تحطيم الرسالة السرية.

٢- **الهجوم الفعال Active Attacks:** تخمين أو انتزاع خصائص الرسالة أو خوارزمية التضمين لتحوير بيانات stego من اجل تدمير البيانات المضمنة، من دون تحطيمها. أي انه قادر على معالجة البيانات[1].

وبشكل عام، تُصنف تقنيات تحليل الإخفاء إلى صنفين وكما يأتي:

١- **تحليل الإخفاء المستهدف Targeted Steganalysis:** وتعني عملية الكشف عن خوارزمية إخفاء معروفة. إذ يُمكن أن يكشف الرسالةَ السرية أو حتى يُخمّن نسبة التضمين مع معرفة خوارزمية الإخفاء.

٢- **تحليل الإخفاء الأعمى Blind Steganalysis:** يتضمن اكتشاف مدى من خوارزمية الإخفاء. هذا النوع أولاً ينتزع بعض الميزات من المحتويات (الصور)، ثم يختار أَو يصمم مصنف Classifier ويُدربه باستخدام الميزات التي انتزعت من مجموعات الصور بعد تدريبها، ثم التصنيف اعتمادا على الميزات السابقة[10].

٥. آلة المتجه الداعم Support Vector Machine

قُدّمت هذه التقنية في عام ١٩٩٢ من قبل الباحث [3](Vapnik)، وهي عبارة عن خوارزمية تعلم عن طريق مشرف أو موجه Supervised تستعمل للتصنيف مستندة إلى نظرية التعلم الإحصائية Statistical Learning Theory[4].

تعد SVM تقنية مفيدة لتصنيف البيانات، وذلك لأنها لاتستخدم لحل مسائل التصنيف الخطية فقط ولكنها تعدّ أيضا علماً منهجياً قوياً لحل المسائل في التصنيف

اللاخطي[3]. يعتمد بناء الأنموذج على عدد من المعلمات مثل المستوى الفاصل (Hyperplane). وتعد عملية استخلاص الخواص للحصول على المتجهات خطوة أساسية وأولية للبدء في تقنية SVM. بعدها يتم تدريب التقنية على مجموعة البيانات الناتجة من استخلاص الخواص للحصول على الأوزان المثالية، لاعتمادها بعملية التصنيف وإعطاء النتيجة. إن ناتج العملية السابقة هو قاعدة بيانات تحوي مجموعة من متجهات الخواص لمجموعة صور التدريب.

أما في عملية التصنيف فيتم تطبيق الخطوات السابقة من عملية التدريب وباستخدام صورة جديدة (صورة الاختبار) لينتج لنا مجموعة من النماذج الإحصائية والتي ستعتمد أساساً للتصنيف.

٦. تقنية مميز فيشر الخطي Fisher Linear Discriminator (FLD)

طريقة تصنيف إحصائية، إذ قُدم في عام ١٩٣٦ من قبل الباحث فيشر (Fisher)، وهو تقنية تصنيف قياسية مستخدمة على نطاق واسع في الكثير من تطبيقات العالم الحقيقي، مثل (تمييز الأنماط)[9].

تهدف الطريقة إلى إيجاد أفضل إسقاط خطي مثالي (Optimal Linear Projection) بين مجموعتين أو أكثر في عملية التصنيف، والحصول على أعلى تمييز بين المجتمعات وذلك يكون بجعل نسبة التباين بين المجموعات إلى التباين داخل المجموعات كبيراً[3].

تقوم فكرة هذه الخوارزمية على تدريب مجموعة متجهات الخواص الناتجة من عملية استخلاص الخواص لمجموعة الصور التي تم التدريب عليها، ومن ثم التصنيف لصورة الاختبار.

٧. فكرة البحث الأساسية

نتيجة الإخفاء المستمر وظهور تقنيات إخفاء جديدة تم اقتراح نظام للتقصي عن تحليل الإخفاء (Steganalysis) باستخدام نوع مميز من الصور، وذلك باعتماده على بناء نماذج إحصائية يتم تكوينها باستخدام عمليات معينة. قبل الدخول إلى النظام

الجديد، بالنسبة للصور الملونة بالامتداد JPG فقد تم الإخفاء عن طريق برنامج كُتب باستخدام بيئة Matlab (R2008a) البرمجية.

يتم تطبيق النظام المقترح على مرحلتين رئيستين هما كالآتي:

١. عملية استخلاص الخواص Features Extraction.

٢. اختيار عدد محدد وقليل من هذه الخواص (٣ خواص) فقط.

عملية تطبيق الخوارزمية الجديدة عن طريق تنفيذ: تقنية آلة المتجه الداعم (Blind SVM)، وتقنية مميز فيشر الخطي (Blind and Non-Blind FLD).

ويمكن توضيح ذلك من خلال الشكل رقم (١).

٨. استخلاص الخواص Features Extraction

تعتمد عملية استخلاص الخواص من الصور الملونة بالامتداد (JPG) على بناء أنموذج إحصائي يستخدم فيه المدرج الإحصائي (Histogram) وتحويل فوريير (Discrete Fourier Transform) وذلك للحصول على متجهات الخواص (Features Vectors). وتوضيح الخوارزمية يكون كالآتي:

- ✓ **الإدخال**: صورة الاختبار (JPG).
- ✓ **الإخراج**: متجهات الخواص (Vectors Features)، وعددها (٢٤) متجه.
- ✓ **أما الخطوات** فتشمل:

١- تحليل الصورة إلى مستوياتها اللونية الثلاثة (RGB).

٢- بناء مدرج إحصائي لكل مستوى لوني (B, G, R) 1 Dimension.

٣- حساب العزوم الأولى والثانية (First and Second Moments)، بمعنى آخر، المتوسط (Mean) والتباين (Variance) لمعاملات المدرج الإحصائي. وتكون نتيجتهُ (٦) إحصائيات.

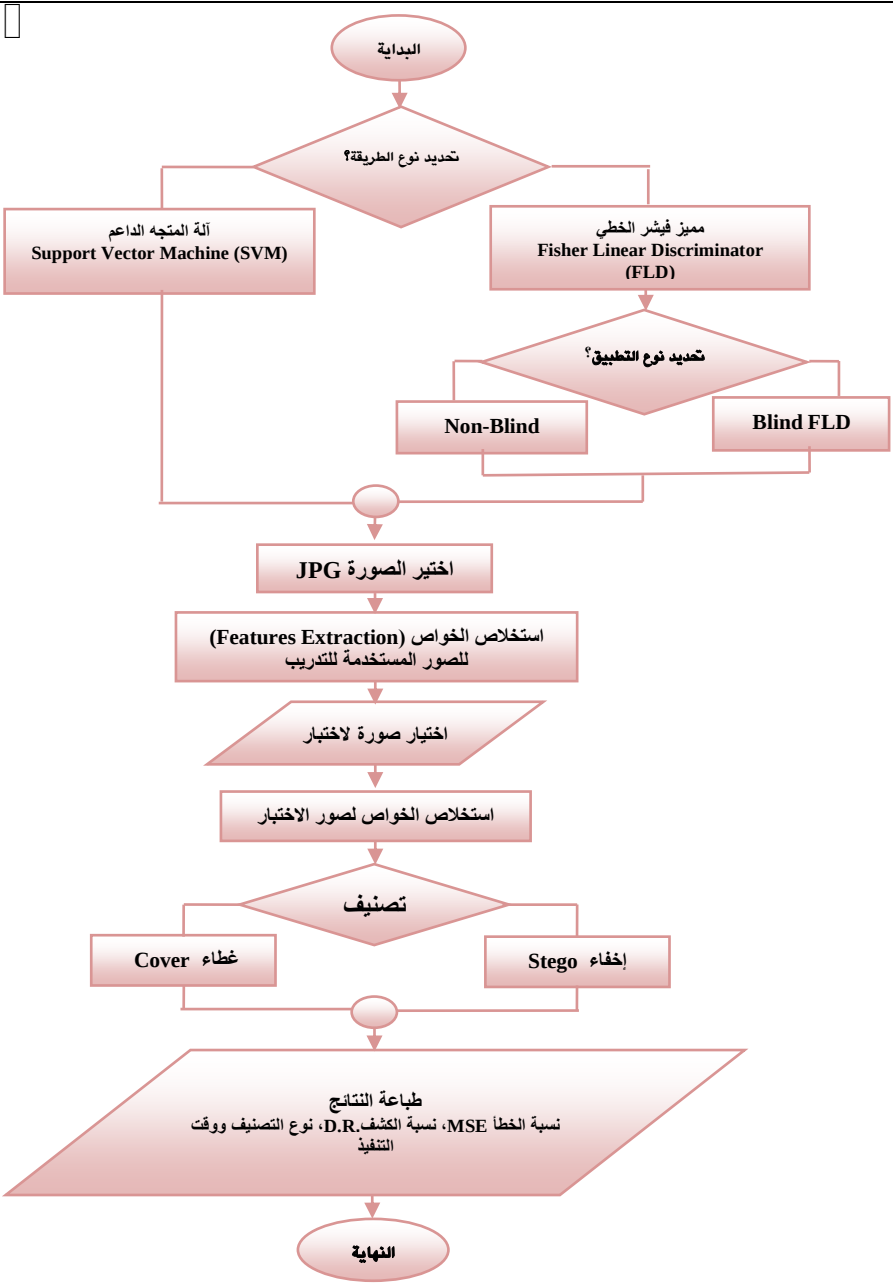
٤- تطبيق تحويل فوريير (Discrete Fourier Transform) على المدرج الإحصائي ولكل مستوى لوني (RGB).

٥- **حساب العزوم (الأولى، الثانية، الثالثة والرابعة) بمعنى آخر، المتوسط، التباين، الالتواء** (Skewness) و(Kurtosis) **لمعاملات تحويل فوريير** (DFT). **وهنا ينتج (١٢) إحصائية.**

٦- **حساب الطاقة الكلية** (Total Energy) **لمعاملات تحويل فوريير** (DFT) **ولكل مستوى لوني. وهذا ينتج (٣) إحصائيات.**

٧- **حساب متوسط الفرق بين معاملات المدرج الإحصائي و تحويل فوريير المنفصل لكل مستوى لوني ، هذا ينتج أيضاً (٣) إحصائيات.**

٨- **تجميع الإحصائيات في متجهات الخواص لتصبح (٢٤) إحصائية.**



الشكل (١)

المخطط الانسيابي العام للتنفيذ

٩. النتائج

تم اعتماد مجموعة صور ملونة (٤٠٠×٦٠٠) وبالامتداد (JPG) اما الإخفاء فكان باستخدام LSB والنص بحجم ٦٢٧٨٦ حرف. إذ بلغ عدد الصور المستخدمة للتدريب (١٠٠ غطاء/١٠٠ إخفاء). أما عدد الصور المستخدمة في الاختبار (١٠٠ غطاء/١٠٠ إخفاء). تم التطبيق لتقنية آلة المتجه الداعم على مرحلتين:

- **مرحلة التدريب Training Phase**

شَملت هذه المرحلة تدريب تقنية آلة المتجه الداعم SVM على مجموعتين من متجهات الخواص: **الأولى** تمثل متجهات خواص صور الغطاء، **والثانية** هي متجهات خواص صور الإخفاء. وتم اعتماد ثلاثة فقط من الميزات الناتجة. بعدها تقوم التقنية بعملية التصنيف وإعطاء التصنيف النهائي.

- **مرحلة الاختبار Testing Phase**

وشملت تطبيق تقنية آلة المتجه الداعم SVM على مجموعة جديدة من متجهات الخواص لمجموعة جديدة من صور الغطاء والإخفاء. في عملية التصنيف تؤخذ النماذج الإحصائية لصورة الاختبار ليتم تصنيف الصورة إما (اخفاء (Stego-Image) أو غطاء (Cover-Image)).

وكانت نتائج اختبار صور ملونة باستخدام تطبيق تقنية آلة المتجه الداعم SVM كما في الجدول رقم (١).

فيما يخص نتائج تطبيق تقنية FLD بنوعيها الأعمى (Blind FLD) و غير الأعمى (Non-Blind FLD) تم اعتماد نفس المعلومات السابقة المستخدمة في تطبيق تقنية SVM. كما في الجداولين (٢) و(٣).

$$\text{نسبة الكشف (DR)} = \frac{\text{عدد الصور المضمنة بصورة}}{\text{عدد الصور في الاختبار}}$$

مقدار الخطأ (MSE) $= \sum_{M,N} [\ stego\text{-}im(m,n) - cover\text{-}im(m,n)]^2 / (M*N)$

M: **عدد الصفوف لصور الإدخال.**

N: **عدد الأعمدة الصور الإدخال.**

الجدول (١)

نتائج تطبيق تقنية SVM على صور JPG الملونة

ت	اسم الصورة	مقدار الخطأ MSE	زمن التنفيذ (ثانية)	نسبة الكشف Detection Rate %	اسم الصورة	مقدار الخطأ MSE	زمن التنفيذ (ثانية)	نسبة الكشف Detection Rate %
1	Balloon	0.04	0.06	90	balloon	0.03	0.12	91
٢	Sea	0.09	0.10	94	Sea	0.06	0.06	92
٣	Book	0.05	0.12	90	book	0.08	0.05	93
٤	Girls	0.04	0.12	92	Girls	0.05	0.06	92
٥	Tree	0.09	0.09	95	tree	0.07	0.05	94
٦	bird	0.06	0.09	91	bird	0.07	0.12	95
٧	flowers	0.08	0.09	95	flowers	0.05	0.06	91
٨	Pen	0.06	0.08	91	pen	0.06	0.06	92
٩	digital	0.06	0.08	95	digital	0.09	0.07	94
١٠	cat	0.08	0.07	93	cat	0.08	0.09	92
نوع التصنيف				**100% Cover**				**100% Stego**

ومن خلال ملاحظة الجدول السابق يتبين ما يأتي:

- **إن هناك فرقاً في المقاييس (نسبة الكشف، مقدار نسبة الخطأ، زمن التنفيذ) بحيث تراوحت نسب الكشف عن (Cover) و(Stego) بين (٩٠ – ٩٥)٪ وهذا يعني الأداء العالي للتقنية.**
- **اما مقدار الخطأ فنلاحظ أن النسبة لم تتجاوز (٠,٠٩)٪ وهذا دليلاً على عدم وجود مقدار خطأ ملحوظ.**

الجدول (٢)

نتائج تطبيق تقنية Blind FLD على صور JPG الملونة

ت	اسم الصورة	زمن التنفيذ (ثانية)	نوع التصنيف	اسم الصورة	زمن التنفيذ (ثانية)	نوع التصنيف
1	yellow bird	0.12	Cover	s-yellow bird	0.11	Stego
٢	coffee	0.13	Cover	s-coffee	0.11	Stego
٣	blue car	0.13	Cover	s-blue car	0.10	Stego
٤	sunflower	0.12	Cover	s-sunflower	0.13	Stego
٥	horse race	0.13	Cover	s-horse race	0.11	Stego
٦	flowers	0.12	Cover	s-flowers	0.13	Stego
٧	child	0.13	Cover	s-child	0.12	Stego
٨	natural	0.13	Cover	s-natural	0.11	Stego
٩	bird	0.12	Cover	s-bird	0.12	Stego
١٠	girl	0.11	Cover	s-girl	0.10	Stego
نسبة الكشف			**١٠٠ ٪ صور غطاء**			**١٠٠ ٪ صور اخفاء**

الجدول (٣)

نتائج تطبيق تقنية Non-Blind FLD على صور JPG الملونة

ت	اسم الصورة	زمن التنفيذ (ثانية)	نوع التصنيف	اسم الصورة	زمن التنفيذ (ثانية)	نوع التصنيف
1	Color	0.13	stego	s-color	0.13	cover
٢	Sun	0.09	cover	s-sun	0.09	stego
٣	Green	0.10	cover	s-green	0.10	stego
٤	gray car	0.09	stego	s-gray car	0.09	cover
٥	Digital	0.09	cover	s-digital	0.09	stego
٦	apple	0.09	cover	s-apple	0.09	stego
٧	yellow car	0.09	cover	s-yellow car	0.09	stego
٨	player	0.10	cover	s-player	0.10	stego
٩	Motor	0.09	cover	s-motor	0.09	stego
١٠	Pen	0.09	cover	s-pen	0.09	stego
نسبة الكشف		٪ ٨٠ صور غطاء			٪ ٨٠ صور اخفاء	

و من خلال ملاحظة الجدولين (٢) و(٣) يتبين أن الزمن لم يتجاوز (0.13) ثانية لصور الغطاء والإخفاء وهذا بسبب اختيار الصورتين في الوقت نفسه للتصنيف وهو دليل على سرعة التنفيذ في الكشف عن الصور، مما يعني كفاءة التقنية.

ويعرض الشكل رقم (٢) انموذجاً من الصور التي أجريت عليها اختبارات الكشف بالامتداد JPG .

(أ): الصورة الاصلية قبل الاخفاء

الشكل

نموذج صورة JPG قبل وبعد الاخفاء والتي اجريت عليها اختبارات الكشف

١٠. الاستنتاجات

١. للتوصل إلى عملية كشف صحيحة ودقيقة لابد من توفر إحدى المعلومات (Cover, Secret Message, Algorithm).

٢. هناك علاقة طردية بين كمية البيانات المخفية وتقنية الكشف.

٣. فكرة التدريب العشوائي لمجموعة التدريب تكون أفضل لان نسبة الكشف تتغير حسب التدريب بدلاً من تثبيت مجموعة التدريب، وكلما زادت أحجام مجموعة التدريب كان الكشف أفضل.

٤. التحكم في اختيار الخواص (الميزات الإحصائية) من الصورة أعطى قابلية اكبر للكشف عن الإخفاء.

٥. أثبتت النتائج جودة تقنية آلة المتجه الداعم (SVM) في الكشف عن الإخفاء في الصور بالاعتماد على مقياس نسبة الكشف التي تجاوزت (٩٠٪).

٦. امتازت تقنية مميز فيشر الخطي (FLD) بأداء عالٍ وسرعة كبيرة في الكشف نظراً لقلة الوقت المستغرق في التدريب.

٧. وكمقارنة بين التقنيتين فيما بينهما (وبشكل عام) كانت الأفضلية لتقنية SVM على FLD من ناحية (نسبة الكشف ومقدار الخطأ)، أما من ناحية (سرعة التقنية) فكانت تقنية FLD هي الأسرع.

١١. المصادر

[1] الحمامي، علاء حسين و الحمامي، محمد علاء، ٢٠٠٨، "إخفاء المعلومات: الكتابة المخفية والعلامة المائية"، إثراء للنشر والتوزيع، الشارقة.

[2] برزنجي، فوزي، ٢٠٠٨، "اخفاء البيانات داخل الصورة"، جامعة السليمانية، العراق.

[3] Farid H., 2002, "Detecting Hidden Messages Using Higher-Order Statistical MoDELS", Department of Computer Science, Dartmouth College, Hanover.

[4] Ge S., Gao Y. and Wang R., 2007 ACM, "Least Significant Bit Steganography Detection with Machine Learning Techniques", National Laboratory for Novel Software Technology Nanjing University 210093 Nanjing, Jiangsu, China,

[5] Jiang M., Wong E., Memon N. and Wu X., ICASSP 2005, "Steganalysis of Halftone Images", IEEE Int'l Conf on Acoustics, Speech, and Signal Processing, Philadelphia, PA.2005.

[6] Lyu S. and Farid H., Springer-Verlag Berlin Heidelberg 2003, "Detecting Hidden Messages Using Higher-Order Statistics and Support Vector Machines", Dartmouth College, Hanover, USA

[7] Rocha A., and Goldenstein S., 2008, "Steganography and Steganalysis in Digital Multimedia: Hype or Hallelujah?", RITA, Vol. 15, No. 1, pp.83-110.

[8] Siwei Lyu and Hany Farid, 2006, "Steganalysis using Higher-Order Image Statistics", IEEE Transaction on Information Forensics and Security, vol. 1, pp. 111-119.

[9] Yang J., Jina Z., Yang Y. and Frang A., 2003, "Essence of kernel Fisher discriminant: KPCA plus LDA", Department of Computer Science, Nanjing University of Science and Technology, Nanjing.

[10] Zhang J., Hu Y. and Yuan Z., ACADEMY PUBLISHER 2009, "Detection of LSB Matching Steganography using the Envelope of Histogram", Guangdong University of Business

Studies, Guangzhou P.R. China, JOURNAL OF COMPUTERS, VOL. 4, NO. 7, JULY 2009.