Blind Steganalysis using One-Class Classification

Mohammed A. Karem M. **Ahmed Sami Nori**
ahmed.s.nori@uomosul.edu.iq
Department of Computer Sciences
College of Computer Sciences and Mathematics
University of Mosul, Mosul, Iraq

Received on: 05/03/2019 **Accepted on: 12/05/2019**

ABSTRACT

Steganography is the science/art of hiding information in a way that must not draw attention to the message hidden in the transmitted media, if a suspicion is raised then there is no meaning to the purpose of steganography. Then appeared its counterpart, Steganalysis, which aims to suspect and analyze the transmitted media to decide wither it contain an embedded data or not which we present in a blind Steganalysis way. One-Class Classification (OCC) machine learning algorithms aim to build classification models depending on positive class only when the negative class is not available or poorly sampled. Here in this paper we depend on a one-class support vector machines (OCSVM) which has been trained on only one class of images that is clean images class, so that the trained classifier can classify new reviews to their correct class i.e. clean or stego. Training an OCC turned to be hard work and required long execution time since classifier parameters tuning, data separation and model evaluation needed to be done manually in a brute force way. A powerful programming language (Python) with the powerful machine learning library (Scikit-Learn) gave a promising classification results in deciding whether an input image is clean or stego image.

Keywords: Steganography, Steganalysis, blind Steganalysis, OCC (One-Class Classification), Python, Machin Learning, Scikit-Learn.

تحليل غطاء الاخفاء الاعمى باستخدام تصنيف الفئة الواحدة

محمد عبد الكريم محمد التميمي **احمد سامي نوري**
قسم علوم الحاسوب
كلية علوم الحاسوب والرياضيات
جامعة الموصل، الموصل، العراق

تاريخ استلام البحث: 2019\03\05 **تاريخ قبول البحث: 2019\05\12**

الملخص

الكتابة المغطاة هو علم/فن إخفاء المعلومات بطريقة لا تجذب الانتباه للرسالة المخفية في الوسط المرسل، إذا اثير شك فإن الغرض من الكتابة المغطاة يصبح بلا معنى. ثم ظهر جزؤه المضاد، كشف الكتابة المغطاة، الذي يهدف للشك بالوسط المرسل وتحليله للتقرير فيما إذا كان يحوي بيانات مخفية او لا، والذي نقدمه هنا بطريقة كشف الكتابة المغطاة الاعمى. تهدف خوارزميات تعليم الآلة ذات التصنيف احادي الفئة الى بناء نموذج تصنيف بالاعتماد على الفئة الموجبة عندما تكون الفئة السالبة غير متوافرة او فقيرة العينات. اعتمد على آلة متجه داعم

وحيدة الفئة تم تدريبها على صنف واحد من الصور وهو صنف الصور التي لا تحوي بيانات مخفية بهدف ان يكون المصنّف الذي تم تدريبه قادراً على تصنيف المشاهدات الى صنفها الصحيح بمعنى صور لا تحوي بيانات مخفية (clean images) وصور تحوي بيانات مخفية (stego images). تدريب مصنف وحيد الفئة يتطلب عملاً شاقاً ويحتاج زمن تنفيذ طويل حيث ان ضبط معاملات المصنف، وتقسيم البيانات، وتقييم نموذج التصنيف تمت يدويا بطريقة القوة الغاشمة. ان لغة البرمجة القوية (Python) مع قوة مكتبة تعليم الآلة (Scikit–Learn) أعطت نتائج تصنيف واعدة في التقرير فيما إذا كانت الصورة المدخلة تحوي بيانات مخفية او لا.

الكلمات المفتاحية: الكتابة المغطاة، كشف الاخطاء الاعمى، تصنيف احادي الاتجاه، بايثون، تعليم الالة، Scikit-learn.

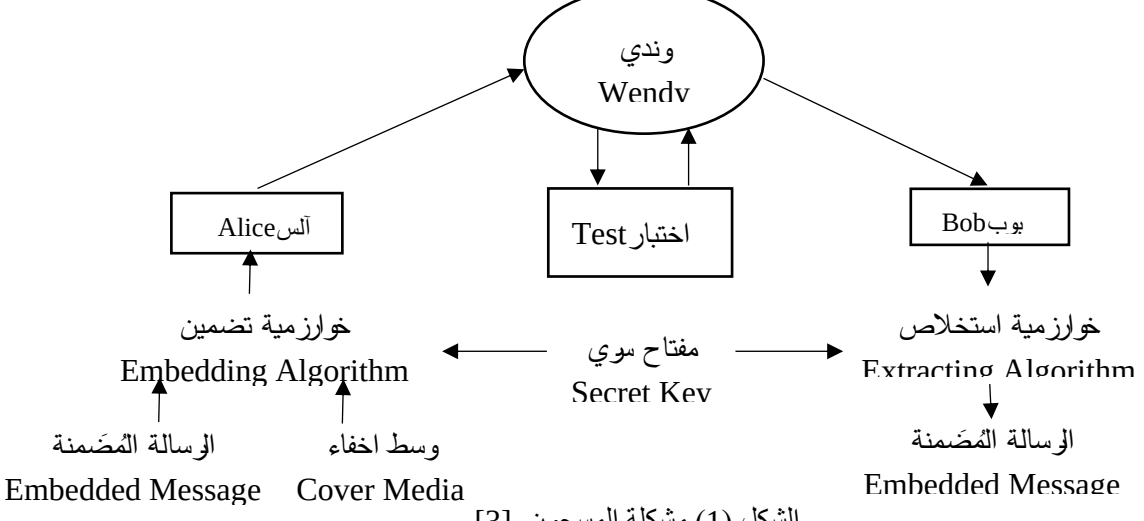
1.مقدمة

كان ولا يزال امن المعلومات من اهم المواضيع التي تجذب الباحثين والمهتمين بتطوير تقانات أمنية تضمن سرية تناقل المعلومات وحمايتها من التطفّل وبمرور الوقت ظهرت ونمت الكثير من هذه التقانات مثل التشفير بأنواعه ثم دعت الحاجة الى أساليب امنية تعالج بعض مآخذ التشفير مثل وقت المعالجة واستهلاك موارد الحاسوب وإثارة الشك فنتج علم إخفاء المعلومات (Information Hiding) والذي تكون تقانة الكتابة المغطاة (Steganography) أحد فقراته. تعمل تقانة الكتابة المغطاة كما يدل الاسم على إخفاء البيانات المراد ارسالها داخل وسط حامل يسمى الغطاء الذي يرسل متضمناً البيانات السرية بطريقة لا تثير ريبة او شكاً أي طرف ثالث متطفل.

مع تطور تقانة الكتابة المغطاة وازدياد استخداماتها وتعددها نشأ علم جديد متمم ومضاد لها يحاول كشف وابطال تراسل هذه الرسائل المخفية يدعى كشف الكتابة المغطاة (Steganalysis).[1]

كشف الكتابة المغطاة هو العملية المستخدمة لكشف المعلومات السرية المضمّنة في الصور عن طريق الكتابة المغطاة. معظم طرائق الكتابة المغطاة تغير خصائص واحصائيات صورة الغطاء بطريقة ما. التحليل الاحصائي لتلك الصورة ممكن ان يكشف إذا ما عدلت الصورة بواسطة الكتابة المغطاة او لا.[2]

هدف محلل الكتابة المغطاة (steganalyst) هو كشف أي تراسل خفي ومنعه او اتخاذ اجراء اخر بشأنه مثل تغيير محتوى الرسالة المغطاة أي انه يكون طرف ثالث وسطي بين طرفين مرسل ومستقبل وبما انه عادة ما يتم تمثيل الكتابة المغطاة بمشكلة السجين (prisoner's problem) فإن آمر السجن (وندي) سيمثل محلل الكتابة المغطاة الذي يهدف الى منع أي تراسل خفي بين (آلس و بوب) كما في الشكل (1).[3]



الشكل (1) مشكلة المسجون. [3]

2. الهدف من البحث

يهدف البحث الى تكوين مصنّف وحيد الفئة (one-class classifier) يستطيع تمييز الصور والتقرير فيما إذا كانت تحوي بينات مخفية او لا باستخدام تقانة آلة المتجه الداعم وحيدة الفئة (OC-SVM) بنوعها الاعمى، حيث تم التدريب على صور خالية من التضمين (Clean Images) ومن ثم تصنيف صور تمت عليها عمليات إخفاء باستخدام البرامج التالية JPHS,OGR, SteganPEG, VSL وبنسب تضمين مختلفة.

3. مبدأ التضمين

الكتابة المغطاة هي تقانة تضمين البيانات في وسط رقمي من دون جذب أي شك او ريبة تجاه ذلك الوسط ومن الممكن استخدامه لتبادل سري للمعلومات مع توفير خصوصية للمستخدم، حيث يتم حشر الرسالة المراد ارسالها في ملف حامل مع إمكانية تشفير المحتوى بمفتاح سري، تعاني الكتابة المغطاة من نقاط ضعف أهمها السّعة والأمان، اذ انها تتم من خلال تقانة تضمين البيانات التي قد تؤدي الى تشوه في الوسط الحامل مثلاً الصور مما يحدث تعديلاً على بعض قيم نقاط الصورة (pixels) وهو امر ضروري للتضمين لكن غير مرغوب فيه.[4]

بشكل أساسي للكتابة المغطاة ثلاث تقانات تصنف اعتمادا على ما إذا كانت التقانة تستخدم تقانات تشفير او لا، وإذا كانت تستخدم تقانات تشفير فهل تستخدم تشفير المفتاح المتماثل ام غير المتماثل وهي الكتابة المغطاة (النقية، استخدام مفتاح سري، استخدام المفتاح العام) وتتم هذا التقانات على وسائط إخفاء متعددة مثل الكتابة المغطاة داخل النص والصوت والصور والفيديو وبروتوكولات الشبكة والحمض النووي ... الخ. .[5][6]

4. الدراسات السابقة

قام الباحثون بالعديد من الدراسات حول كشف الكتابة المغطاة باستعمال تصنيف الفئة الواحدة وتنوعت طرائقهم ونتائجهم وبيانات التدريب والاختبار التي استخدموها والجدول (1) يعرض بعضاً منها.

الجدول (1) يوضح الدراسات السابقة.

رقم المصدر	السنة Year	الباحث Researcher	البحث Research	التقنية المستخدمة Used Technique	إحصاءات Statistics			نسبة الكشف Detection Ratio %
					نماذج التدريب Training samples	عدد الميزات Features	البرامج الجاهزة Steganography Apps	
[15]	2004	-Lyu -Farid	كشف الكتابة المغطاة باستخدام إحصاءات ال color wavelet وآلة المتجه الداعم وحيدة الصنف	One class support victor machine (OC-SVM)	40,000 cover images	216	-Jsteg -Outguess -F5 -Jphide -Steghide	متنوعة وعديدة
[16]	2013	-wei -mingqiang -Tingting -Weiwen	التقصي حول كشف الكتابة المغطاة وحيد الصنف في صور JPEG بالاعتماد على تقليل ابعاد صفات الترابط	One-class Support Vector Data Description (SVDD)	لم تذكر	لم تذكر	لم تذكر	متنوعة وعديدة

رقم المصدر	السنة Year	الباحث Researcher	البحث Research	التقنية المستخدمة Used Technique	إحصاءات Statistics			نسبة الكشف Detection Ratio %
					نماذج التدريب Training samples	عدد الميزات Features	البرامج الجاهزة Steganography Apps	
[17]	2008	-Pevny -Fridrich	اكتشاف الحداثة في كشف الكتابة المغطاة الاعمى	One class support victor machine (OC-SVM)	لم تذكر	لم تذكر	لم تذكر	متنوعة وعديدة
[18]	2007	-Rodriguez -Peterson -Agaian	كشف شذوذ الكتابة المغطاة باستخدام تصنيف الفئة الواحدة	One class support victor machine (OC-SVM)	لم تذكر	لم تذكر	-F5 -JP Hide -JSteg -Outguess -StegHide	88.0±2.1% Anomaly 90.0±2.5% clean
[19]	2017	-Sandoval -Hernandez -Perez -Medina -Meana -Miyatake	كشف إخفاء محكم في الصور لطريقة LSB-) (Matching	support victor machine (SVM)	لم تذكر	12	لم تذكر	عديدة ومتنوعة لنسب إخفاء متغيرة
[20]	2009	-Manjula Devi - Manjunatha -Raja Venugopal- -Patnaik	كشف الصورة الاصلية بأستخدام المدرج التكراري وتحويل فورير وآلة المتجه الداعم	One class support victor machine	لم تذكر	24	JPHS	عديدة ومتنوعة
[21]	2012	Yang- Guo- Luo-	كشف الكتابة المغطاة بالاعتماد على المصنف وحيد الفئة وطريقتي عنقدة	One class support victor machine (OC-SVM)	32000	لم تذكر	-No-steg -Jsteg -Outguess -F5 -Jphide -Steghide	عديدة ومتنوعة

5. الهجمات على الكتابة المغطاة

ان لازدياد استخدام تقانات الكتابة المغطاة وتنوعها تأثيراً على طرائق الكشف، اذ زادت الحاجة الى مثل هذه التقانات المضادة التي تمنع او تحد الاستخدام السيء لتقنيات الكتابة المغطاة وهي على نوعين فعال (active) و سلبي (passive)، ففي كشف الكتابة المغطاة الفعال يقوم المهاجم بالتلاعب بالبيانات المخفية بعد اكتشافها اما في كشف الكتابة المغطاة السلبي فيكتفي المهاجم بتحليل العنصر المشكوك فيه والتقرير فيما اذا كان يحوي بيانات مخفية او لا وهو ليس هدفاً لكشف الكتابة المغطاة النهائي، اذ انه في الحالة المثالية تحدد محتويات الرسالة المخفية ولمحلل الكتابة المغطاة عدة طرائق لمهاجمة ملفات تحوي بيانات مخفية وكما يأتي:[8][7]

- الهجوم بمعرفة الجسم الحامل للبيانات المخفية Stego Only Attack
- الهجوم بمعرفة ملف الغطاء Known Cover Attack
- الهجوم بمعرفة الرسالة المخفية Known Massage Attack
- الهجوم بالخوارزمية المختارة Chosen Stego Attack
- الهجوم بالرسالة المختارة Chosen Massage Attack
- الهجوم بمعرفة الخوارزمية المستخدمة Known Stego Attack
- الهجمات البصرية Visual Attacks

- هجوم الهيكلة Structural Attack
- الهجوم الاحصائي Statistical Attack

6. أنواع تقانات كشف الكتابة المغطاة

ينقسم كشف الكتابة المغطاة عموماً الى قسمين رئيسين كالآتي:[9]

- كشف الكتابة المغطاة المستهدف (Targeted Steganalysis)

وهو النوع الذي يصمم خصيصاً لمهاجمة نوع محدد من خوارزميات الكتابة المغطاة ولمحلل الكتابة المغطاة (steganalyst) دراية بطرائق التضمين والخصائص الإحصائية المتأثرة بالخوارزميات المستخدمة وهو فعال جدا في حال كانت تقانة التضمين معلومة ويفشل بشكل ذريع عند استخدامه في كشف خوارزمية تضمين غير التي خصص لها او إذا كانت تقانة التضمين غير معلومة.

- كشف الكتابة المغطاة الاعمى (Blind Steganalysis)

صنف اعّم من تقانات كشف الكتابة المغطاة يمكن تصميمه لكشف أي خوارزمية تضمين حتى غير المعروفة منها ويسمى أيضا بكشف الكتابة المغطاة العام وهي طريقة حديثة وقوية في الهجوم على الوسائط الحاملة للبيانات التي تعتمد على مصنّف (classifier) يصمم بالاعتماد على ميزات (features) مأخوذة من صور غطاء وان أشهر وأحدث الطرائق الحالية تعتمد على استخلاص خصائص إحصائية تسمى ميزات من مجموعة صور.

7. كشف الكتابة المغطاة وتعليم الالة

تعليم الالة هو احد فروع الذكاء الاصطناعي الذي يتيح لأنظمة الحاسوب التعلم من الأمثلة والبيانات والخبرات عن طريق السماح للحاسوب بالقيام بمهام محددة بذكاء فإنه يمكن انظمة الحاسوب من القيام بمعالجات معقدة بدلاً من اتباع قواعد برمجية مبرمجة مسبقا أي باختصار تحويل الخبرة الى معرفة، اذ يمثل ادخال خوارزمية التعليم بيانات تدريب الخبرة ويكون الإخراج بعضاً من المعرفة، ويتم اللجوء الى طرائق تعليم الالة عندما تكون المشكلة معقدة وفي حال الرغبة بكون البرنامج قابلاً للتكيف مع معطيات جديدة مدخلة. [10]

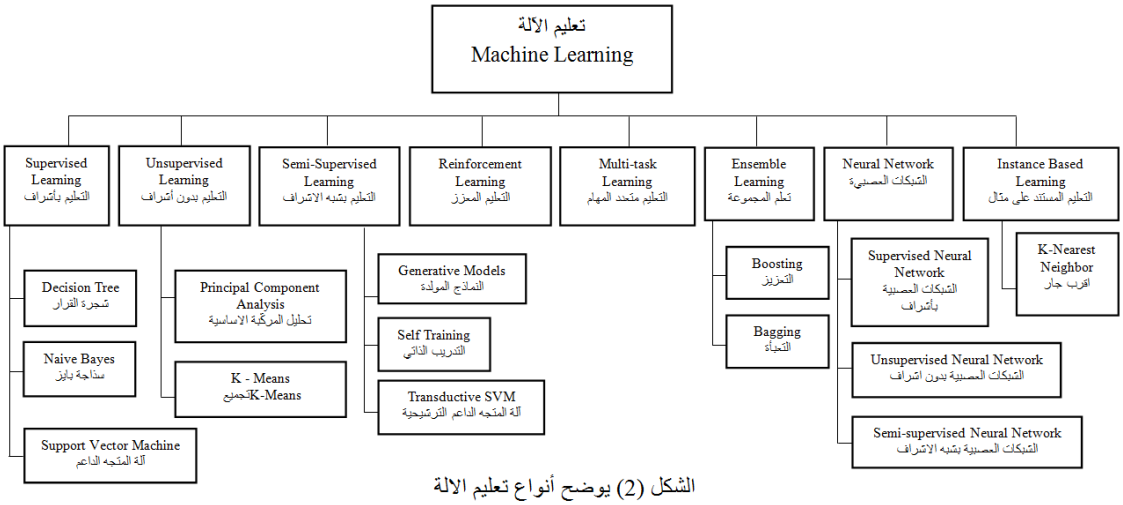
فمثلا برنامج لتمييز الاجسام او وجوه الأشخاص قد يحتاج الى عدد كبير من القواعد والاسطر البرمجية لتمييز فاكهة معينة او وجه انسان معين فمثلا قد يعتمد مبرمج على القيم اللونية لصورة الجسم او الوجه لكن ماذا لو تغيرت هذه القيم؟، بينما تكون هذا المهمة اسهل بكثير في تعليم الالة، اذ يعتمد على مجموعة ميزات تستخلص من الاجسام او الوجوه وتدريب مصنّف عليها يكون باستطاعته لاحقا التقرير فيما اذا كانت المشاهدة الجديدة هي وجه او جسم قد تدرب عليه او لا وهي طريقة اشمل واعم وانجح من استخدام قواعد محددة مسبقاً. ولتعليم الالة عدة فروع كما موضح في الشكل (2).

1.7 تعليم الالة لغرض كشف الكتابة المغطاة

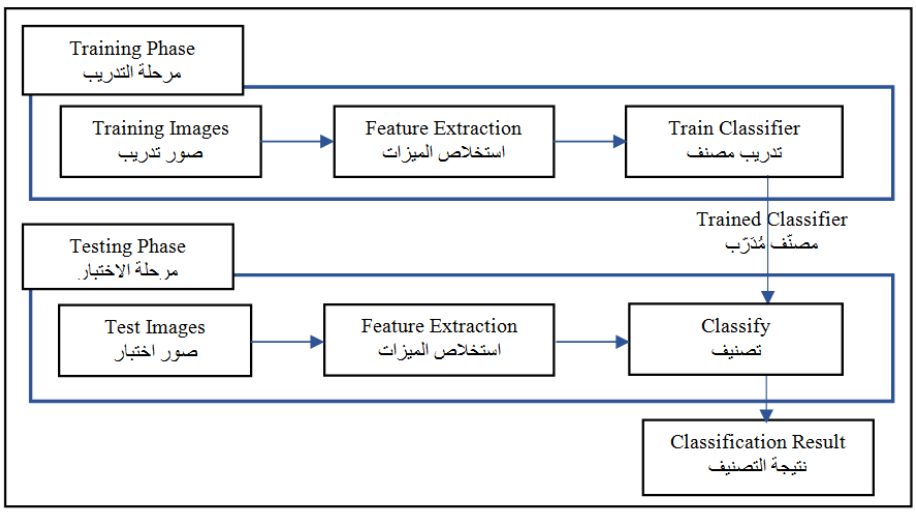
ان مهمة كشف الكتابة المغطاة هي التقرير فيما إذا كان الجسم المشكوك فيه يحوي بيانات او لا، ان مسائل تصميم خوارزمية تقوم بتعيين الاجسام الى أصناف مختلفة يسمى بتمييز الأنماط (pattern recognition)

وقد اعتمد على إحصاءات تحليلية للبيانات، تعليم الالة يوفر طريقة بديلة للطريقة التحليلية، وفيما يأتي خطوات توظيف تعليم الالة لغرض كشف الكتابة المغطاة كما موضح في الشكل (3). [11][12][13]

- تهيئة مجموعة البيانات (Dataset) :وهي البيانات التي ستستخدم لغرض تدريب المصنف وحيد الفئة واختبار أدائه وقدرته على التصنيف وقد تم التعامل مع صور من نوع JPEG.
- استخلاص الميزات (Features Extraction): خواص مجموعة البيانات المستخلصة من الصور وهي في الحقيقة عملية تقليص ابعاد وفي الوقت نفسه عملية تهديمية، إذ لا يمكن لمجاميع من القيم ان تصف صورة بالكامل لكنها عملية ضرورية لتقليص مدى التحليل وتقليل زمن المعالجة لزيادة أداء التصنيف مع امل ان تكون الصفات المستخلصة الضرورية لكشف الكتابة المغطاة قد حفظت.
- اختيار مصنّف (Classifier): وهو المقرر الذي يميز الصور في مجموعة البيانات الى اصنافها بناءً على الخواص التي يتم إدخالها له ويتم اختياره اعتمادا على نمط المشكلة فيما إذا كانت مشكلة تصنيف احادي او ثنائي او متعدد وهكذا.
- اختيار مقياس أداء (Performance Measure): لتقييم أداء المصنف المختار يجب اختيار مقياس لكفاءة تصنيف المصنّف وعادة ما يتم اللجوء الى الدقة (accuracy) ، اذ يحسب عدد الصور التي صنفت بشكل صحيح من مجموع الصور المدخلة.



الشكل (2) يوضح أنواع تعليم الالة



الشكل (3) عملية كشف الكتابة المغطاة في الصور الرقمية باستخدام تعليم الالة.[13]

8. آلة المتجه الداعم وحيدة الصنف One-Class Support Victor Machine

آلة المتجه الداعم وحيدة الصنف هي امتداد لآلة المتجه الداعم القياسية الثنائية، اقترح العالم (Schölkopf) واخرون آلة متجه داعم وحيدة الصنف لتعالج مشاكل التصنيف الأحادي. يهدف نموذج التصنيف التقليدي المتعدد الأصناف الى تصنيف عنصر بيانات غير معروف الى أحد الفئات المحددة مسبقا (فئتين في الحالة البسيطة وهي التصنيف الثنائي) لكن تبرز المشكلة في حالة كون عنصر البيانات المراد تصنيفه لا ينتمي الى أي من الفئات المعرّفة مسبقا. كمثال لنفترض بيانات تدريب تحوي على تواقيع شخصين وتم تدريب مصنف ثنائي لتمييز هذه التواقيع، والمراد تصنيف توقيع شخص من خارج مجموعة التدريب فأن المصنف سيقوم بتصنيف التوقيع ضمن أحد الفئات التي تم تدريبه عليها وهي حالة خاطئة في جميع الأحوال. اذن فعملية التصنيف قد لا تقتصر على تخصيص فئة معينة لبيانات غير معروفة وانما التقرير فيما إذا كانت تلك البيانات تنتمي لفئة معينة محددة مسبقا او لا وفي المثال أعلاه فأن توقيع الشخص لا يشبه توقيع أي من التواقيع التي تم تدريب المصنف عليها.

في التصنيف احادي الفئة، احدى الفئات التي تسمى بالفئة الموجبة او الفئة الهدف معرفة جيدا بنماذج في بيانات التدريب بينما الفئات الأخرى او بتسمية أخرى الفئات السالبة او الناشزة تكون معدومة النماذج او تملك نماذج قليلة جدا في بيانات التدريب او لا تكوّن عينة تمثيلية احصائية لمفهوم السالب او الناشز.

ان المشاكل التي تواجه اساليب التصنيف المألوفة مثل تقدير أخطاء التصنيف، قياس تعقيد الحل، لعنة الابعاد (dimensionality curse) وتعميم طريقة التصنيف كلها موجودة في التصنيف احادي الفئة بل قد تبرز بشكل أكبر، اذ انه وكما ذكرنا سابقا فأن الفئة السالبة تكون معدومة او متوافرة بشكل محدود جدا أي انه يجب تعيين حد القرار (decision boundary) باستخدام بيانات من الفئة الموجبة فقط. هذا يجعل مشكلة التصنيف الأحادي أصعب من مشاكل التصنيف العادية. ان مهمة التصنيف احادي الفئة هي إيجاد حد تصنيف حول الفئة الموجبة بحيث انه يقبل أكبر عدد من عينات تلك الفئة بينما يقلل فرصة قبول عينة خارجية ناشزة لا تنتمي للفئة المحاطة بحد التصنيف، من الصعب تقرير ضيق حد التصنيف حول الفئة الموجبة في كل الاتجاهات بناءً على فئة واحدة فقط من البيانات. كما انه من الصعب تقرير أي من الميزات (features) يجب استخدامها لإيجاد أفضل فصل بين الفئة الموجبة والاجسام التابعة للفئات الناشزة الأخرى. [14]

9. قياس أداء التصنيف للمصنفات ذات الفئة الواحدة

من الممكن استخدام مصفوفة الارتباك كما في الشكل (4) لحساب أداء تصنيف المصنف ذي الفئة الواحدة. لحساب الخطأ الحقيقي كما يحسب في التصنيف متعدد الفئات، يجب معرفة الكثافة الاحتمالية (probability density) لكلتا الفئتين. وفي حالة التصنيف ذو الفئة الواحدة، فأن الكثافة الاحتمالية تكون معلومة للفئة الموجبة فقط. معنى هذا انه يمكن تقليل الاجسام المرفوضة التابعة للفئة الموجبة فقط (false negatives, F^-). وبغياب امثلة وتوزيع العينات من الفئة الشاذة فأنه من غير الممكن تقدير الاجسام الشاذة التي سيقبلها المصنف وحيد الفئة (false positives, F^+). كذلك بما ان $T^+ + F^- = 1$ و $T^- + F^+ = 1$ فأنه يجب ملاحظة التعقيد الحاصل في التصنيف وحيد الفئة وهو انه من الممكن تقدير T^+ and F^- فقط وليس هنالك معلومة عن F^+ and T^-. ولذلك فأنه من المطلوب توافر كمية محدودة من بيانات الفئة الشاذة لتقدير أداء

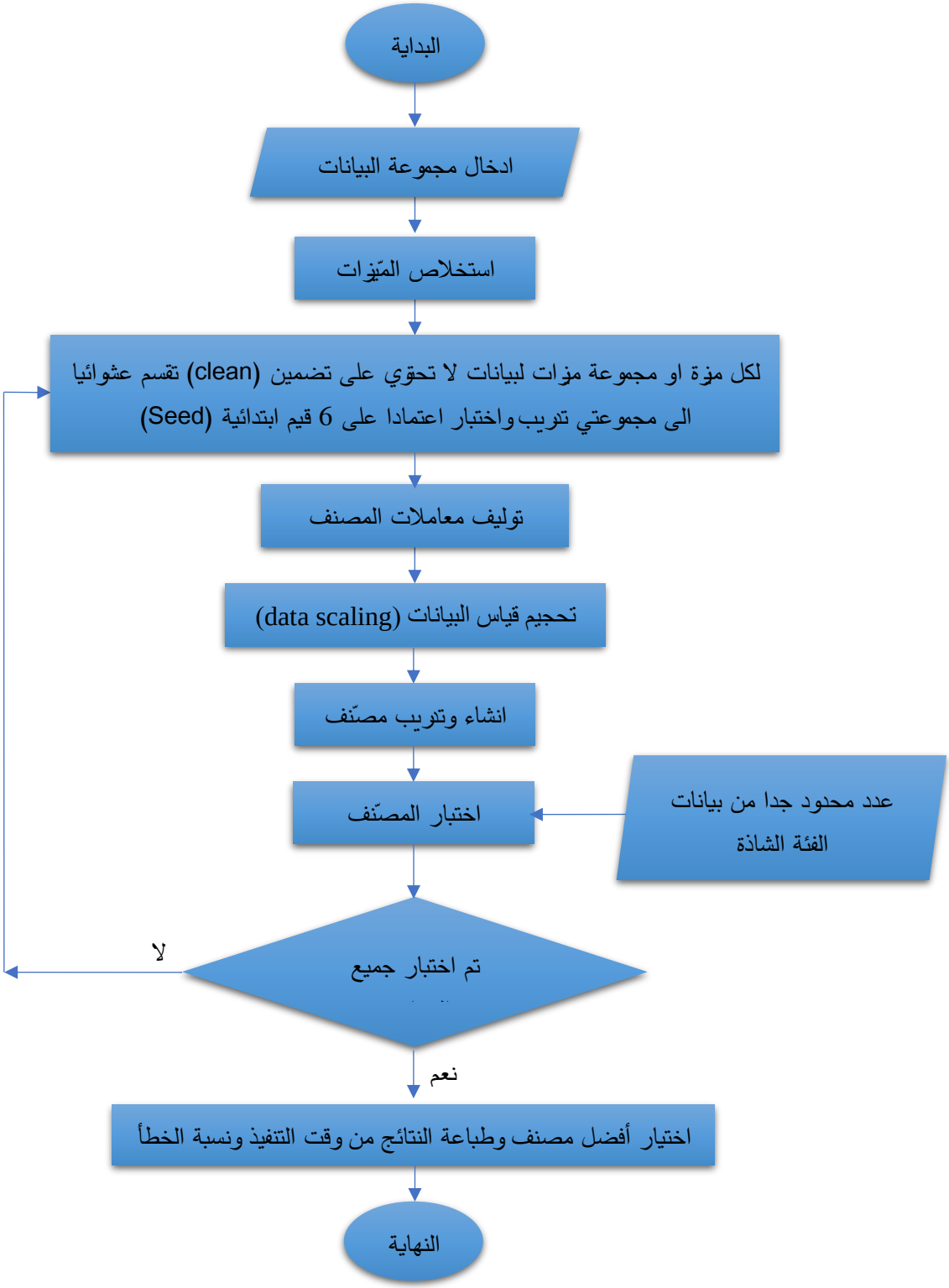
المصنّف وتعميم دقة تصنيفه. مع ذلك فأنه واثناء الفحص إذا كانت الفئة الشاذة غير ممثلة بنسبة معقولة فأن الدقة الحقيقة للمصنّف قد لا تكون حقيقية ولا تمثل وحدة قياس فعلية للأداء. [14]

	عناصر من الصنف الهدف	عناصر من الأصناف الاخرى
Classified as a target object	True positive, T^+	False positive, F^+
Classified as an outlier object	False negative, F^-	True negative, T^-

الشكل (4) مصفوفة الإرتباك للمصنّف وحيد الفئة. [14]

10. خطوات تصميم نظام كشف الكتابة المغطاة المقترح

يتّبع النظام مجموعة من الخطوات للوصول الى مصنّف يستطيع تمييز الصور الى أحد صنفين اما صورة لا تحوي بيانات مضمّنة (clean images) او صور (stego images) بمعنى تحتوي بيانات مضمّنة اعتمادا على مصنف وحيد الفئة، إذ تجمع البيانات وتكون مجموعة البيانات وهي ما سيتم تدريب المصنّف عليه ثم اختباره به وفي هذا البحث فأن البيانات هي صور من نوع JPEG جمعت يدويا بالإضافة الى مجاميع بيانات جاهزة أخرى استحصلت من مصادر مختلفة. بعد ذلك يتم استخلاص الميزات لتقليل التعقيد وإعطاء طابع البساطة للبيانات أي تمثيلها بميزات فاصلة بين الأصناف، وقد كانت الميزات التي استخلصت من مجاميع البيانات عبارة عن خمس ميزات للصور الرمادية تمثل بمجموعها متجه ميّزات ذو 55 قيمة وسبعة ميزات للصور الملونة تمثل بمجموعها متجه ميّزات ذو 69 قيمة يتبع ذلك توليف معاملات المصنف وحيد الفئة، إذ يتحكم المعامل الأول بعدد العينات المرفوضة من الصنف الهدف ويعديل في مرحلة التدريب ليرفض الضوضاء في بيانات التدريب، اما المعامل الثاني فيتحكم بسلاسة حد القرار الخاص بالمصنف ولايجاد أفضل قيم لمعاملات المصنف فأنه يجب اجراء مجموعة من الاختبارات ومعرفة النتائج وذلك عن طريق البحث الاعمى أي تجربة مجاميع مختلفة من القيم ومشاهدة النتائج للوصول الى أفضل قيم من قيم المعاملات بعدها يبدأ تحجيم قياس البيانات (data scaling) إذ يجب تغيير قيم ميزات البيانات لتكون بين [1,+1−] او بين [0,1] قبل تقديمها الى آلة المتجه الداعم والغرض الأساسي من ذلك يكمن في تجنب القيم الرقمية الكبيرة التي قد تسبب مشاكل حسابية، كما انه من المهم جدا تطبيق تحجيم القياس على بيانات الاختبار والتدريب على حد سواء ثم يدرب مصنّف وحيد الفئة و اختباره بعدد كبير من الأشواط عن طريق ادخال ميزات مجموعة البيانات حيث يتم في كل شوط تدريب المصنف على مجموعة مختارة من مجموعة الميزات او ميزة واحدة فقط ثم تقسيم البيانات الى مجموعة تدريب ومجموعة اختبار بشكل عشوائي وكذلك اختيار عدد من قيم معاملات المصنف وحيد الفئة التي تختبر مع كل مجموعة ميزات وعند الانتهاء يختار المصنف الأقل عددا في أخطاء التدريب والاختبار ومن الجدير بالذكر انه من الضروري وجود عدد محدود من عناصر الفئة الشاذة التي لا تنتمي للفئة الهدف بغية التأكد من نتائج اختبار المصنف والمخطط (1) يوضح خطوات تصميم نظام كشف الكتابة المغطاة المقترح.



المخطط (1) يوضح خطوات تصميم نظام كشف الكتابة المغطاة المقترح

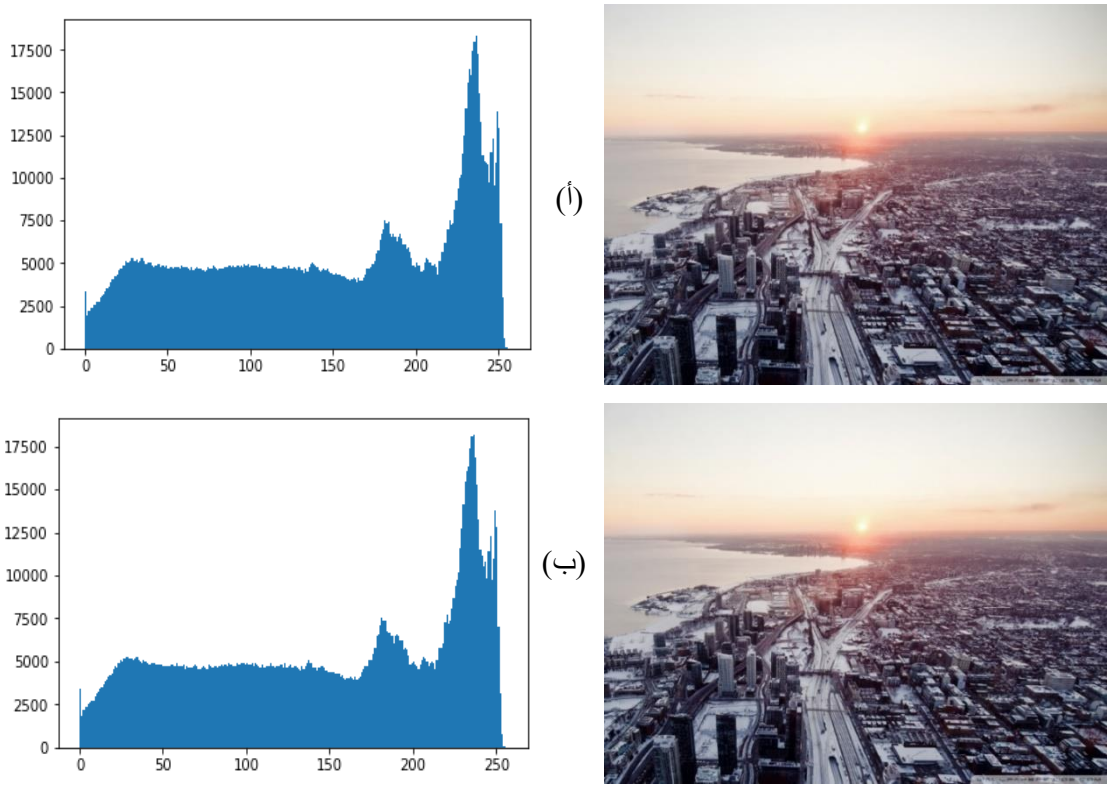
11. الحاجة الى عينات سالبة

كما أسلفنا فأنه يتطلب عينات محدودة من الفئة الخارجية التي لا تنتمي للفئة الهدف لتقييم أداء دقة المصنّف، وقد تم توليد العينات المطلوبة وذلك باختيار 10 صور من كل مجموعة بيانات انفة الذكر ومن ثم إخفاء بيانات بنسب مختلفة داخلها مثل (1KBو 2KB و 3KB و 25KB و 50KB) باستخدام البرامج في الجدول (2).

الجدول (2) برامج الكتابة المغطاة المستخدمة لتوليد العينات

ت	اسم التطبيق	مجال الكتابة المغطاة	خوارزمية الكتابة المغطاة	سعة الكتابة المغطاة	نوع صور الغطاء	اصدار البرنامج
1	JP hide and seek	Frequency domain	LSB	Up to 17.5%	JPEG	Rev 0.5
2	Outguess Rebirth	Frequency domain	LSB	/	JPEG	V1.3
3	SteganPEG	Frequency domain	Partial Decoding	/	JPEG	V1.0
4	Virtual Steganographic Laboratory	Frequency domain	F5	Up to 13%	JPEG	V1.1

كما يعرض الشكل (5) احدى صور الاختبار مع المدرج التكراري الخاص بها قبل إخفاء 50KB وبعده من البيانات النصية داخلها ويلاحظ انعدام التأثير في شكل او لون الصورة كما يكاد انعدام ملاحظة التغيير الطفيف في المدرج التكراري للصورة دلالة على قوة برنامج الكتابة المغطاة.



الشكل (5) انموذج للإخفاء باستخدام برنامج JPHS
(أ) الصورة الاصلية والمدرج التكراري لها، (ب) الصورة والمدرج التكراري لها بعد الكتابة المغطاة.

12. نتائج المُصنّف احادي الفئة

كانت نتائج التطبيق مختلفة ومتنوعة باختلاف مجموعة البيانات ونسب التضمين كما في الجدول (3)، وقد تمت عمليات استخلاص الميّزات وضبط معاملات المصنف وضبط قياس البيانات والتدريب والاختبار واختيار المصنف بأفضل نتيجة والموضح زمن تنفيذها في الجدول ادناه على حاسوب بالمواصفات الاتية:

(نظام التشغيل: windows 10 v1803) (المعالج المركزي: intel core i7-7700HQ)

(الذاكرة العشوائية :12GB)

الجدول (3) نتائج آلة المتجه الداعم وحيدة الفئة

مجموعة البيانات	برنامج الكتابة المغطاة	نسبة الكشف عن البيانات المضمنة					نسبة الكشف في بيانات الاختبار	زمن التنفيذ HH:MM:SS	الميزات بأفضل نتيجة	عدد الميزات
		1KB	2KB	3KB	25 KB	50 KB				
My Dataset	VSL	90 %	90 %	90 %	90 %	80 %	74.2%	0:28:32	ale0 ale1d ale2d farid36 HCF-COM	5
	JPHS	90 %	90 %	90 %	90 %	90 %				
	OGR	80 %	80 %	100%	/	/				
	SteganPEG	90 %	90 %	90 %	90 %	90 %				
CALTECH	VSL	60 %	70 %	70 %	/	/	71.9%	2:55:49	ale2d HCF-COM	2
	JPHS	70 %	70 %	70 %	80 %	70 %				
	OGR	80 %	80 %	/	/	/				
	SteganPEG	80 %	80 %	80 %	80 %	80 %				
BOSS Base	VSL	100 %	10 0%	10 0%	10 0%	10 0%	91.55 %	2:31:08	ale0 ale1d	2
	SteganPEG	40 %	40 %	50 %	50 %	50 %				

يمكن تلخيص الجدول أعلاه كما يأتي: ان النتائج في الجدول شملت تنفيذ أكثر من برنامج وبنسب إخفاء مختلفة تراوحت بين (1KB – 50KB) وتجاوزت نسبة الكشف فيها 90% في حين ان نسبة كشف النماذج الخالية من التضمين (clean) تجاوزت ال 90% أيضا.

اما ما يخص مقارنة العمل الحالي بالدراسات السابقة فمن الصعوبة تحديد النسبة، اذ انه بالرغم من كون تقانة آلة المتجه الداعم وحيد الفئة عامل مشترك في البحوث الا ان لكل بحث برامج إخفاء مختلفة ونسب تضمين عديدة ومجاميع بيانات مختلفة ايضاً.

13. الاستنتاجات

استنادا الى ما ذكر وبالنظر الى نتائج التصنيف يمكن استنتاج ما يأتي:

- رغم كون البيانات متناثرة ومتنوعة الا ان للمصنف القدرة العالية على تصنيف الاجسام الحاملة للبيانات.
- بالرغم من عدم معرفة خوارزمية الكتابة المغطاة او نسبها او وجود عينات سالبة للتدريب فقد كانت نسب الكشف عالية جدا.
- بناءً على النقطتين 2 و3 فأن المصنف وحيد الفئة قد اثبت جودته في تصنيف العينات بدقة عالية.
- عملية البحث عن أفضل نتيجة بوجود متغيرات كثيرة من معاملات المصّنف وطريقة تقسيم البيانات الى مجموعة تدريب واختبار واختيار حجم كل مجموعة وتجربة تراكيب الميزات هي عملية طويلة ونوعا ما معقدة وتحتاج الى وقت تنفيذ طويل وحاسوب ذو مواصفات جيدة.
- ليس بالضرورة ان تزداد دقة التصنيف بزيادة العينات او تقليلها او زيادة او تقليل ميّزات البيانات انما الحل الأمثل لأيجاد أفضل نتيجة هو تجربة احجام مختلفة من بيانات التدريب مع تراكيب مختلفة من ميّزات البيانات فضلاً عن عامل مهم جدا هو معاملات المصنف التي يجب ضبطها بالتجربة.
- رغم كون الصور من نوع JPEG وهي صور مكبوسة الا ان برامج الكتابة المغطاة اثبتت كفاءتها في أداء العمل ذلك انه رغم إخفاء 50KB من البيانات وهو ما قد يمثل نسبة 50% من حجم بعض الصور الا ان الصور الناتجة حافظت على جودتها وحجمها مع تغير طفيف في خصائصها الإحصائية وهو ما اعتمد عليه المصنف في رصد تلك الصور وتصنيفها الى صنفها الصحيح.
- بعد عملية التدريب والاختبار والوصول الى مصنف وحيد الفئة بأفضل نسبة كشف واقل نسبة خطأ مع انّسب عوامل، يكون هذا المصنف انموذجا يمكن استخدامه في أي تطبيق برمجي وبإمكانه التصنيف في أجزاء من الثانية بمجرد ادخال ميزات العينة المراد تصنيفها عليه.

14. الاعمال المستقبلية

يمكن تلخيص فكرة الاعمال المقترحة بما يأتي:

- تجربة ميزات جديدة واختبارها لغرض التصنيف ومقارنتها مع الميزات المستعملة حاليا.
- اختبار مدى أوسع من قيم معاملات المصّنف.
- استعمال برامج إخفاء أكثر وأحدث، وتجربة المصنف الناتج عليها للوصول الى درجة اعلى في كشف الكتابة المغطاة الاعمى.
- تجربة أنواع أخرى من الصور أو وسائط إخفاء أخرى كالصوت والفيديو.
- استعمال المصنّف في مجالات أخرى او جعله بديلاً للمصنفات الأخرى كالمصنفات ثنائية الصنف او متعددة الصنف، ولاسيما تلك التي تتعدم فيها بيانات أحد الاصناف او تكون الكثافة غير متوازنة.

المصادر

[1] Johnson, Neil and Jajodia, Sushil, Steganalysis: The Investigation of Hidden Information, IEEE Information Technology Conference, Syracuse, New York, USA, September 1st - 3rd, pp. 113-116, 1998. IVSL.

[2] Bachrach, Mayra and Shih, Frank, Image Steganography and Steganalysis, John Wiley & Sons, pp. 251-259, 2011.

[3] Chen, Wen, Study of Steganalysis Methods, New Jersey Institute of Technology, 2005.

[4] K. Saranya, C. Suresh, George, Minu Data Embedding Techniques in Steganography, International Journal of Latest Trends in Engineering and Technology, pp. 200-205, 2013.

[5] S. I. mrutu, Computer Networks And Information Security, University of Dodoma, College of Informatics and Virtual Education, Dept. of Computer Science, 2015.

[6] نوري، احمد، عبد الله، سعدون، اخفاء المعلومات باستخدام الاستبدال في الطفرة الصامتة لتسلسلات الحمض النووي، مجلة الرافدين لعلوم الحاسوب والرياضيات.

[7] Johnson, Neil, Duric, Zoran, Jajodia, Sushil, Information Hiding: Steganography and Watermarking Attacks and Countermeasures, Boston: Artech house, 2001.

[8] Ferreira, Alexandre, An Overview on Hiding and Detecting Stego-data in Video Streams, University of Amsterdam, 2015.

[9] Dwivedi, Yadvendra, Bera, Swagota, Sharma, Monisha, Review on Universal Steganalysis Techniques Based on the Feature Extraction in Transform Domain, International Journal of Engineering Research and Development, pp. 07-11, 2017.

[10] Shalev-Shwartz, Shai, Ben-David, Shai, Understanding Machine Learning: From Theory to Algorithms, Cambridge University Press, 2014.

[11] Miche, Yoan, Developing Fast Machine Learning Techniques With Applications To Steganalysis Problems, Doctoral Dissertation, Department of Information and Computer Science Faculty of Natural Sciences Aalto, University School of Science and Technology, 2012.

[12] Devi, Kirthiga, Ranjan, Rahul, Jpeg Image Steganalysis Using Machine Learning, Int. Jou. of Computer Science and Information Security (IJCSIS), pp. 96-99, 2016.

[13] Bhasin, Veenu, Bedi, Punam, Steganalysis for JPEG Images Using Extreme Learning Machine, IEEE International Conference on Systems, Man, and Cybernetics, pp. 1361-1366, 2013.

[14] Madden, Michael, Khan, Shehroz, One-Class Classification: Taxonomy of Study and Review of Techniques, Cambridge University Press, pp.1-30, 2014.

[15] Lyu, Siwei, Farid, Hany, Steganalysis Using Color Wavelet Statistics and

One-Class Support Vector Machines, SPIE - The International Society for Optical Engineering, 2004.

[16] Wei, Li, Mingqiang, Wu, Tingting, Zhu, et al., Research on One-Class JPEG Steganalysis Based on Dimensionality-Reduced Correlation Features, International Conference on Mechatronic Sciences, Electric Engineering and Computer (MEC) Dec 20-22, pp. 1998-2001, 2013.

[17] Pevny, Tomas, Fridrich, Jessica, Novelty Detection in Blind Steganalysis, 10th workshop on Multimedia & Security, pp. 167-176, 2008.

[18] Rodriguez, Benjamin, Peterson, Gilbert, Agaian, Sos, Steganography Anomaly Detection Using Simple One-Class Classification, Mobile Multimedia/Image Processing for Military and Security Applications, 2007.

[19] Sandoval, Oswaldo, Hernandez, Manuel, Perez, Gabriel, et al., Compact Image Steganalysis for LSB-Matching Steganography, 5th International Workshop on Biometrics and Forensics (IWBF), 2017.

[20] Devi, T. H. Manjula, Reddy, H.S.Manjunatha, Raja, K. B., et al., Detecting Original Image Using Histogram, DFT and SVM, International Journal of Recent Trends in Engineering, pp. 367-371, 2009.

[21] Yang, Haibin, Guo, Duntao, Luo, Peng, A Steganalysis based on OC-SVM and two Clustering Methods, Applied Mechanics and Materials, pp 3096-3099, 2013.