Neural Network Using for Extracting Hidden Information in Images

Safwan Omar Hasoon **Farhad M. Khalifa**
Dr.safwan1971@yahoo.com
College of Computer Sciences and Mathematics
University of Mosul, Mosul, Iraq

Received on: 20/03/2012 **Accepted on: 28/06/2012**

ABSTRACT

Steganography technique widely spread and varied. With the widening in using steganography, its misuse alarmists arisen. Thus steganalysis comes into sight to deter unwanted secret communications.

In this paper a new scheme proposed for extracting hidden information, this scheme relies on the capability of artificial neural networks for prediction to estimate the original values of the pixels which values of some of them were changed by the affection of data embedding process, and then the present pixel values will be compared with estimated values to identify the embedded data. Multilayer Perceptron MLP neural network used in this scheme to estimate the pixel's original value using its neighbor pixels. The proposed schemes programmed using Matlab v. 7.10.0.499. The proposed schemes has been trained and tested using a data base prepared for this purpose. Then its performance compared with another work in the same field applied in similar conditions. The results showed that the proposed scheme has the ability to achieving the desired with a good rate of success.

Keywords: Steganography, Stegnoanalysis, Neural Network.

استخدام الشبكات العصبية لاستخلاص البيانات المخفية في الصور

صفوان عمر حسون **فرهاد محي الدين خليفة**
كلية علوم الحاسوب والرياضيات
جامعة الموصل، الموصل، العراق

تاريخ استلام البحث: 2012/03/20 **تاريخ قبول البحث: 2012/06/28**

الملخص

انتشرت تقنية الكتابة المخفية واسعاً وتنوعت طرائقها, ومع هذا التوسع في استخدام الكتابة المخفية ظهرت المخاوف من سوء استخدامها. فلأجل ذلك ظهر علم تحليل الإخفاء لردع الاتصالات السرية غير المرغوب بها.

اقترح في هذا البحث نظام لاستخلاص البيانات المخفية, هذا النظام يعول على قدرة الشبكات العصبية الاصطناعية على التنبؤ لتخمين القيم الأصلية للخلايا الصورية التي تغيرت قيم بعضها بتأثير عملية تضمين البيانات فيها, ثم تقارن قيم الخلايا الصورية الحالية مع القيم المخمنة لتحديد البيانات المضمنة. استخدمت شبكة بيرسبترون متعددة الطبقات Multilayer Perceptron MLP في هذا النظام لأجل تخمين القيم الأصلية للخلية الصورية عن طريق الخلايا المجاورة لها. تمت برمجة النظام المقترح باستخدام Matlab v. 7.10.0.499. دُرب النظام واختبر باستخدام قاعدة بيانات معدّة لهذا الغرض. ثم تمت مقارنة أداء النظام المقترح مع عمل آخر في

مجال نفسه مطبقاً في ظروف متشابهة. أظهرت النتائج أن النظام له القدرة على إنجاز المطلوب منه بنسبة جيدة من النجاح.

الكلمات المفتاحية: الكتابة المخفية، تحليل الاخفاء، الشبكة العصبية.

1- مقدمة

نظراً للتطور الهائل في مجال التقنية الرقمية وشبكة الانترنيت والاتصالات أصبحت الخصوصية الشخصية عرضة للانتهاك بسهولة أكبر من ذي قبل. فكان لابد من طرائق تُحفظ بها سرية البيانات الشخصية حال تناقلها لمنع المتطفلين من الاطلاع عليها. لهذا لغرض أوجدت تقنية الكتابة المخفية الرقمية.

الكتابة المخفية Steganography هي فن وعلم إخفاء بيانات سرية مهمة في ناقل غير مؤذٍ على نحو يخفي وجود البيانات المخفية بدون إثارة الشبهة بهدف إبقاء الاتصال بين الطرفين المتصلين سرياً [20][10]. Steganography كلمة يونانية مركبة من شقين, الأول "Steganos" الذي يعني مخفي Hidden أو مغطى Covered أو سري Secret, والشق الثاني "Graphy" الذي يعني كتابة Writing أو رسم Drawing, لذا فهي حرفياً تعني الكتابة المخفية أو الكتابة المغطاة أو الكتابة السرية [8][15].

إخفاء المعلومات داخل الصور تقنية واسعة الانتشار في الوقت الحاضر. فالصور الرقمية لها درجة كبيرة من التكرار غير المفيد في التمثيل ولها تطبيقات واسعة الانتشار في الحياة اليومية. إذ إن الصور الحاملة للرسائل السرية يمكن أن تنتشر بسهولة عبر الانترنيت أو المجاميع الإخبارية. وبالتالي فهي مغرية لإخفاء المعلومات. ونتيجة لذلك شهد العقد الماضي اهتماماً متزايداً بالبحوث في مجال الكتابة المخفية في الصور وتحليل الإخفاء للصور [10][12].

شهدت بدايات العقد الأخير من القرن الماضي ظهور طليعة البحوث حول الكتابة المخفية الرقمية, على الرغم من أن الكتابة المخفية عموماً لها جذور موغلة في عمق التاريخ , إذ استخدمت طرائق مختلفة لانجاز الكتابة المخفية بعضها بدائي. وفي نهايات العقد ذاته ظهرت أوائل البحوث التي تحاول كشف الكتابة المخفية في الوسائط الرقمية فكان بداية لعلم تحليل الإخفاء Steganalysis, فُتح بذلك الباب على مصراعيه أمام الباحثين للخوض في مجالي الكتابة المخفية و تحليل الإخفاء فكان حقلاً خصباً من حقول البحث العلمي و أنتجت طرائق عديدة لا حصر لها في كلا المجالين.

2- تحليل الإخفاء

على النقيض من الهدف من إخفاء المعلومات Information Hiding, فإن تحليل الإخفاء Steganalysis هو فن كشف الرسائل المخفية وجعل مثل هذه الرسائل عديمة الفائدة وإفشال إخفاء المعلومات [16].

اكتسب تحليل الإخفاء أهمية في حقلي الأمن القومي والعلوم العدلية, لكون كشف الرسائل المخفية يمكن أن يؤدي إلى منع الحوادث الأمنية الكارثية. إن حقل تحليل الإخفاء حقل صعب جداً بسبب ندرة المعرفة بشأن الخصائص المعينة لوسائط الغطاء (ملفات الصور والصوت والفيديو) التي يمكن أن تستغل لإخفاء المعلومات أو اكتشافها على حد سواء. والأساليب المعتمدة في تحليل الإخفاء تعتمد في بعض الأحيان على أساس الخوارزميات المستخدمة في الإخفاء [11].

إن أتمتة كشف الرسائل المخفية ضرورة لابد منها لأن الكمية الهائلة من بيانات الصور المخزونة على أجهزة الحاسوب أو في مواقع الانترنيت تجعل من المستحيل على شخص أن يتحرّى كل صورة على انفراد [4].

تقسم خوارزميات تحليل الإخفاء للصورة حسب خوارزميات الإخفاء التي تعمل عليها إلى نوعين: **الأسلوب المحدد** Specific Approach ويدعى أيضاً تحليل الإخفاء المستهدف Targeted Steganalysis [7]. الأسلوب المحدد يمثل فئة تقنيات تحليل الإخفاء التي تعتمد كثيراً على أساس خوارزمية الإخفاء المستخدمة, هذا الأسلوب له نسبة نجاح عالية لاكتشاف وجود الرسالة السرية إذا كانت الرسالة مخفية باستخدام خوارزمية الإخفاء المستهدفة من قبل تقنية التحليل [11]. في الأسلوب المحدد تُستغل نقطة ضعف خوارزمية الإخفاء المحددة لأجل التحليل [10]. في هذا الأسلوب يتم التركيز على الاختلافات التي تحدثها خوارزمية إخفاء معينة في ملف الغطاء بحيث تعطي مؤشراً على وجود رسالة مخفية.

والنوع الثاني هو **الأسلوب العام** Generic Approach ويدعى أيضاً تحليل الإخفاء الأعمى Blind Steganalysis [7]. وهو يمثل فئة تقنيات تحليل الإخفاء التي لا تتطلب معلومات مسبقة حول خوارزميات الإخفاء المستخدمة في إخفاء الرسالة السرية, هذا الأسلوب يحقق نتائج جيدة لاكتشاف وجود رسالة سرية مخفية باستخدام خوارزمية إخفاء جديدة أو غير تقليدية [11]. إن هذا الأسلوب في تحليل الإخفاء عادة يعتمد على إستراتيجية تعتمد على التعلم, هذه الإستراتيجية تتضمن مرحلة تدريب و مرحلة اختبار. في الأسلوب العام يكون التركيز على خصائص ملفات الغطاء الطبيعية, إذ إن أي تشوه في هذه الخصائص يعطي مؤشراً على حدوث تلاعب بالغطاء مما يعني احتمال وجود رسالة مخفية.

تقنيات تحليل الإخفاء للصور في كلتا الحالتين المحدد والعام تصمم غالباً لاكتشاف وجود أو عدم وجود رسالة سرية, ويعد استخلاص الرسالة المخفية شيئاً مكملاً وليس أساسيا [11]. ففن الإخفاء Steganography يخفق في أداء غرضه إذا كان وجود الرسالة في الوسائط قابلاً للكشف [9]. تحليل الإخفاء يمكن أن يصنف بصورة عامة إلى صنفين [3][8][13].

أ- تحليل سلبي للإخفاء Passive Steganalysis

- تحديد فيما إذا كان الملف يحوي بيانات مخفية أم لا.
- تحديد الخوارزمية المستخدمة في الإخفاء.

ب- تحليل فعال للإخفاء Active Steganalysis

- تخمين طول الرسالة وموقعها.
- تخمين المفتاح السري المستخدم في التضمين.
- تخمين بعض معاملات خوارزمية الإخفاء المستخدمة.
- استخلاص الرسالة.

تحليل الإخفاء مجال بحثي جديد نسبياً يهدف إلى كشف و/أو تخمين المعلومات المخفية بمعرفة معلومات قليلة أو بدون معرفة أية معلومات حول خوارزمية الإخفاء المستخدمة أو معاملاتها [2]. قلة المعلومات المتوفرة حول الملف المشكوك فيه يولد الكثير من التساؤلات والتحديات. وهناك على الأقل خمسة تحديات تتعلق بالمعرفة حول الملف المشكوك فيه تواجه تحليل الإخفاء [5]:

أ- الملف المشكوك فيه ربما يحوي أو قد لا يحوي بيانات مخفية.

ب- البيانات المخفية قد تكون أو قد لا تكون مشفرة قبل تضمينها في الوسط المضيف.

ج- الملف المشكوك فيه ربما يحوي ضوضاء أو قد يكون خالياً من الضوضاء.
د- قد يكون بالإمكان أو ربما يكون من المستحيل استعادة البيانات المخفية أو استخلاصها.
هـ- عملية تحليل الإخفاء تستغرق وقتاً طويلاً.

3- الدراسات السابقة

في عام 2003 قدم R. Chadromoulig, Shalin Trivedi طريقة لتحليل الإخفاء إذ استغلا التغيير المفاجئ الذي يطرأ على البيانات جراء الإخفاء التتابعي، تهتم الطريقة بتحديد موقع الرسالة المخفية وطولها باستخدام خوارزميات الإخفاء التتابعي, قدم الباحثان الاشتقاقات التحليلية للحالات عندما تكون معاملات الإخفاء معروفة كلياً أو معروفة جزئياً [17].

في عام 2005 قدم R.Chadromoulig, Shalin Trivedi طريقة كشف تخمن المفتاح السري في تضمين البيانات السرية باستخدام خوارزميات الإخفاء التتابعي، وكفاءة النظام تعتمد على طبيعة الإخفاء، ففي حالة الإخفاء في التردد الواطئ لمعاملات تحويل التجيب المتقطع DCT يكون النظام غير كفوء [18].

وفي العام ذاته قدم Aruna Ambalavanan و Rajarathnam Chandramouli طريقة تحليل إخفاء لتخمين الرسالة المخفية بالاعتماد على نظرية باياس Bayes, وذلك بتشكيل الصورة على شكل حقل Markov العشوائي, واستغلال التناظر بين الصور والأنظمة الإحصائية الآلية. تحاول هذه الطريقة ربط صورة الغطاء مع الغطاء المضمن عن طريق دالة احتمالية [1].

وفي عام 2010 اقترح M.Revathi وآخرون نظاماً عاماً لاكتشاف وجود الإخفاء وتخمين طول الرسالة السرية المخفية في نماذج LSB, يستند هذا العمل على فرضية أن نظام إخفاء الرسالة السرية يترك دلائل إحصائية في الصورة يمكن أن تستغل لاكتشاف الإخفاء. لهذا الغرض استخدموا مقاييس جودة الصورة Image Quality Metric (IQM) وتحليل التباين ANOVA وتحليل الانحدار متعدد المتغيرات بوصفه مصنفاً مثالياً [14].

4- النظام المقترح

تكتفي معظم بحوث تحليل الإخفاء بدراسة كشف وجود الإخفاء في الوسائط, أو تخمين بعض معاملات الإخفاء كطول الرسالة المخفية أو المفتاح السري المستخدم في الإخفاء. في هذا الجزء من البحث نحاول استخلاص الرسالة المخفية في الصورة من دون توفر الغطاء الأصلي للمقارنة, إذ يمكن تخمين الرسالة المخفية من الفرق بين الغطاء والغطاء المضمّن في حال توفر الغطاء.

هذا العمل يرتكز على إمكانية تخمين الغطاء الأصلي من الغطاء المضمّن, إذ يكون الإخفاء في نسبة معينة من الخلايا الصورية. هذا العمل يعول على أمرين, أولهما: قدرة التنبؤ العالية للشبكات العصبية الاصطناعية التي استخدمت في هذا العمل لغرض تخمين الخلايا الصورية الأصلية, إذ إن من المعلوم أن الشبكات العصبية لها إمكانية إعطاء نتائج صحيحة أو تقريبية حتى بفقدان أو تغير بعض البيانات المدخلة, فالبيانات المتغيرة في هذه الحالة هي الخلايا الصورية التي يجري تضمين البيانات السرية فيها. والأمر الثاني: انتظام تدرج الألوان وأنماط توزيعها في معظم مناطق الصورة, مما يتيح للشبكة العصبية التخمين بدقة عالية.

ونظراً لكمية البيانات الهائلة المتوفرة, يكون من الصعب إيجاد نظام يستطيع تخمين الغطاء الأصلي لكل أنواع الصور المتاحة معاً, لذلك كان من المنطقي تقسيم الصور المتوفرة للتدريب إلى عدة مجموعات, كل مجموعة

تحوي صوراً متشابهة في مضمونها لتسهيل عملية تخمين الغطاء الأصلي عن طريق توزيع الجهد على أنظمة متعددة كل منها تخمن الصور الأصلية لمجموعة من هذه المجموعات.

أحد أهم التحديات التي تواجه استخلاص البيانات المخفية هو أن البيانات المخفية لا تغير بالضرورة كل الخلايا الثنائية التي تخفى البيانات فيها, إذ لو كانت قيمة الخلية الثنائية المراد إخفاؤها مطابقة لقيمة الخلية الثنائية المضيفة فلن يحصل أي تغيير, مما يجعل من المستحيل كشف هذه الخلية الثنائية دون معرفة مسبقة بمكانها. إن احتمالية عدم تغير خلية ثنائية مضيفة معينة هي 0.5, أي أن نصف عدد البيانات التي تخفى فقط هي قابلة للاكتشاف, لذلك أخفيت البيانات بقلب قيمة الخلية الثنائية المضيفة, أي أن القيمة صفر تصبح 1 والقيمة 1 تصبح صفراً. ولا بد من الإشارة إلى أن هذه الطريقة للإخفاء ليست عملية وقد استخدمت فقط لقياس كفاءة النظام لتجنب تأثير تغير قيم البيانات الفعلية على أداء النظام.

النظام المقترح لاستخلاص البيانات المخفية ينجز على مرحلتين, المرحلة الأولى تدرب فيها شبكة بيرسبترون متعددة الطبقات العصبية الاصطناعية على بيانات مأخوذة من عدة صور غطاء لا تحوي بيانات مخفية, وذلك لأجل تخمين الخلايا الصورية الأصلية من الخلايا الصورية المجاورة لها. وفي المرحلة الثانية تخمن الخلايا الصورية الأصلية من صور غطاء مضمّن ثم تقارن الخلايا الصورية المخمنة مع الخلايا المقابلة لها في الغطاء المضمّن وتستخلص البيانات المخفية من ناتج المقارنة.

4-1- افتراضات النظام

صنفت الصور الرمادية المستخدمة للتدريب والاختبار إلى أربع مجموعات, كل مجموعة تضم صوراً متقاربة في مضمونها (صنفت الصور إلى هذه المجموعات بصرياً), أخفيت البيانات في هذه الصور في الخلية الثنائية الأقل أهمية LSB وأيضاً في مستويات خلايا ثنائية Bit Planes أعلى (المستوى الثاني والثالث والرابع والخامس) لأجل اختبار مدى قابلية النظام المقترح على استخلاص الرسالة المخفية في هذه المستويات, وكذلك أخفيت البيانات بخمس نسب بداية من نسبة 25% من سعة الغطاء نزولاً إلى 5% من سعة الغطاء (يمكن أن يقال أن احتمالية الإخفاء هي 0.25 و0.20 و0.15 و0.10 و0.05). وكان توزيع الرسالة المخفية في الصورة المضيفة بشكل منتظم لتغطية كامل الصورة. وأخيراً تدرب شبكات مستقلة لكل مجموعة (صنف) من هذه المجاميع.

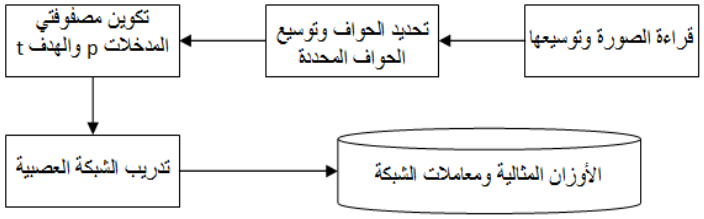
4-2- مرحلة التدريب

لكي تتمكن الشبكات العصبية من تخمين القيم الأصلية للخلايا الصورية بمعرفة الخلايا الصورية المجاورة لها, لا بد من تدريب هذه الشبكة على بيانات صور غطاء, ويساعد في ذلك كون معظم مناطق الصورة تتألف من خلايا صورية تحمل ألواناً منسجمة ومتناسقة تتوزع بأنماط معينة غالباً ما تكون قريبة من بعضها, عدا بعض الأماكن مثل الحواف (الحدود) التي تفصل بين الأشياء الموجودة ضمن الصورة, إذ تحدث اختلافات كبيرة بين الخلايا الصورية المتجاورة, مما يُحدث إرباكاً في عملية تحديد القيم الأصلية للخلايا الصورية الواقعة ضمن هذه المنطقة, لذا استثنيت الخلايا الصورية التي تشكل الحواف والخلايا الصورية المجاورة لها من الدخول في عملية التدريب منعاً لإرباك الشبكة العصبية.

تبدأ هذه المرحلة بتجميع وتجهيز البيانات لغرض التدريب, ثم إدخال هذه البيانات إلى الشبكة العصبية وتدريبها. والخوارزمية التالية توضح خطوات عمل هذه المرحلة من العمل. والمخطط الانسيابي في الشكل (1) يلخص هذه الخوارزمية.

4-2-1- خوارزمية مرحلة التدريب

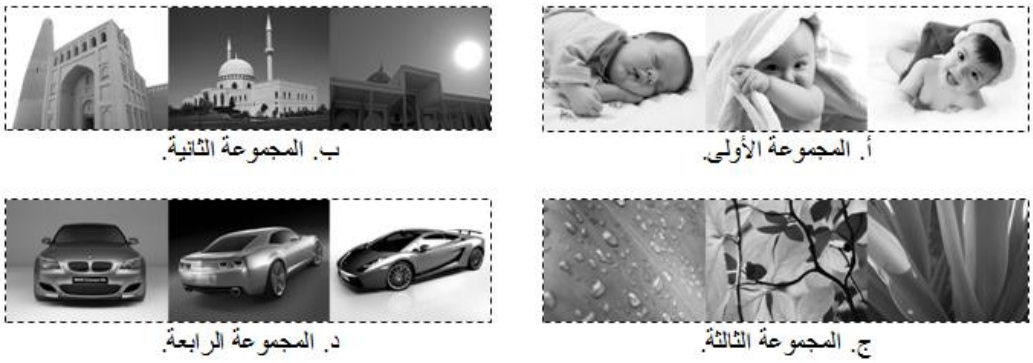
1- قراءة الصور الغطاء وتوسيعها بمقدار خلية واحدة من كل جهة.
2- تحديد حواف الأشياء داخل الصورة وتوسيع الحواف المحددة بعملية Dialation.
3- إضافة الخلايا الصورية غير الواقعة ضمن الحواف الموسعة إلى مصفوفة الهدف t ضمن أزواج التدريب, وإضافة الخلايا المجاورة لها إلى مصفوفة المدخلات p.
4- تدريب شبكة بيرسبترون متعددة الطبقات باستخدام أزواج التدريب (p, t).
5- خزن الأوزان المثالية ومعاملات الشبكة المدربة في ملف.



الشكل (1). المخطط الانسيابي لنظام استخلاص البيانات المخفية (مرحلة التدريب).

4-2-2- تجميع البيانات

في هذه المرحلة هيأت صور رمادية نظيفة خالية من الاخفاء, صنفت الصور حسب مضمونها إلى أربع مجموعات, كل منها تحوي 11 صورة متقاربة في مضمونها, الشكل (2) يعرض نماذجاً من الصور من كل مجموعة من هذه المجموعات.



الشكل (2). نماذج من الصور ضمن قاعدة بيانات التدريب.

4-2-3- توسيع الصورة

بعد قراءة الصورة وخزنها في المصفوفة x, تجري عملية التوسيع لهذه الصورة بمقدار خلية صورية واحدة من كل جهة. تأخذ الخلايا المضافة بياناتها مما جاورها من الخلايا, فتكون النتيجة تكرار العمود الأول والأخير وكذلك الصف الأول والأخير من الصورة الأصلية, وسبب إجراء هذه العملية هو لكي تدخل الخلايا المتواجدة على أطراف الصورة الأصلية في المعالجة في الخطوات اللاحقة وتخمن بصورة صحيحة.

4-2-4- تحديد الحواف

في هذه الخطوة تحدد حواف الأشياء داخل الصورة, بما أن هذه الحواف تمثل منطقة انتقال بين منطقتين كل منها ذات نمط معين لتوزيع الألوان تختلف عن المنطقة الأخرى, فستكون الاختلافات كبيرة بين النقاط المتجاورة. لذلك يكون من المفيد استثناء هذه المناطق من إدخالها في عملية التدريب وذلك بعدم ادراجها ضمن أزواج التدريب, لتجنب إرباك الشبكة العصبية.

تحدد الحواف عادة بتنفيذ اللافوف الرياضي بين مصفوفة خلايا الصورة ومرشح المرور العالي. وتحديد الحواف يعتمد على تقريب متقطع لعملية الاشتقاق, وعملية الاشتقاق تقيس معدل التغير في الدالة (الإضاءة في هذه الحالة). والتغير الكبير في إضاءة الصورة ضمن حيز مكاني صغير يدل على وجود حافة [19]. يستخدم عامل برويت Prewitt Operator لأجل تحديد الحواف في هذا العمل. اختير مرشح برويت لكونه يناسب الصور ذات التباين العالي [19].

يبحث عامل برويت لتحديد الحواف عن الحواف بالاتجاهين الأفقي X والعمودي Y ثم تدمج هذه المعلومات للحصول على حواف موحدة. ويعتمد على مرشحين أحدهما للاتجاه الأفقي والآخر للاتجاه العمودي. تجري عملية اللافوف الرياضي لكل منهما مع الصورة, فعند كل خلية صورية توجد قيمتان, p_x تمثل الناتج من نافذة الصفوف, و p_y إلتي تمثل الناتج من نافذة الأعمدة , وتحسب المحصلة حسب المعادلة (1) [19]. الشكل (3) يظهر النوافذ المستخدمة في حساب قيمة الانحدار باتجاه X و Y. والشكل (4)(ب) يظهر مثالاً على تحديد الحواف للصورة المعروضة في الشكل (4)(أ).

$$\begin{bmatrix} -1 & -1 & -1 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \end{bmatrix} \qquad \begin{bmatrix} -1 & 0 & 1 \\ -1 & 0 & 1 \\ -1 & 0 & 1 \end{bmatrix}$$

المرشح الأفقي — المرشح العمودي

الشكل (3). النوافذ (المرشحات) المستخدمة في حساب قيمة الانحدار.

وتحسب محصلة الانحدار كالآتي :

$$p(i,j) = \sqrt{p_x^2(i,j) + p_y^2(i,j)} \quad \cdots (1)$$

إذ إن :

$p(i,j)$: محصلة الانحدار عند الخلية الصورية (i , j)

p_x : تمثل قيمة الانحدار باتجاه X

$$p_x(x, y) = [\, f(x-1, y-1) + f(x, y-1) + f(x+1, y-1)] - [f(x-1, y+1) + f(x, y+1) + f(x+1, y+1)]$$

p_y : تمثل قيمة الانحدار باتجاه Y

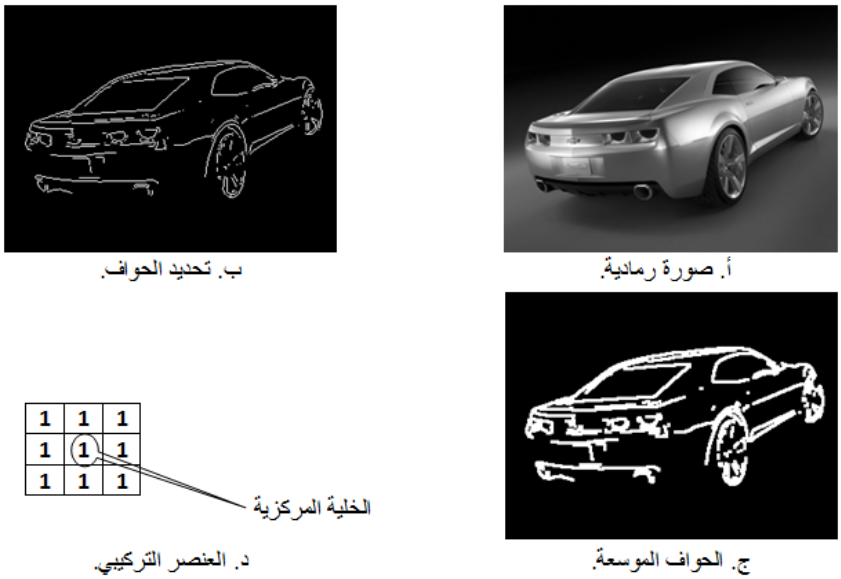
$$p_y(x, y) = [\, f(x-1, y-1) + f(x-1, y) + f(x-1, y+1)] - [\, f(x+1, y-1) + f(x+1, y) + f(x+1, y+1)]$$

f(x, y) : هي الصورة عند النقطة (x, y).

4 -2-5- توسيع الحواف المحددة

في هذه الخطوة توسع الحواف المحددة من الخطوة السابقة, إذ أن معظم هذه الحواف هي بسمك خلية صورية واحدة, لكن منطقة الاختلافات اللونية الكبيرة بين الخلايا المتجاورة ضمن الحدود الفاصلة بين شيئين داخل الصورة تكون أوسع من مجرد خلية صورية واحدة؛ لذا من المفيد توسيع منطقة الاستثناء من الدخول في عملية التدريب. لهذا الغرض توسع الحواف بعملية تمديد Dilation التي هي إحدى العمليات الشكلية Morphological Operations.

تجرى عملية التمديد بإسقاط نافذة صغيرة الحجم (تمثل العنصر التركيبي للشكل) على الصورة وتزحيفها عبر الصورة بأسلوب مشابه للالتفاف الرياضي تسمى عملية تزحيف النافذة. يتم اختيار الخلية الصورية المطابقة للخلية المركزية للنافذة فإذا كانت قيمتها صفراً فيتم إجراء عملية الجبر المنطقي نوع (OR) بين كل خلية من خلايا النافذة مع الخلايا الصورية المطابقة لها, أما إذا كانت قيمتها تساوي 1 فلا تجرى عملية الجبر المنطقي وتزحف النافذة بمسافة خلية صورية واحدة [19]. الشكل (4)(ج) يظهر مثالاً على توسيع الحواف المحددة. والشكل (4)(د) يبين العنصر التركيبي المستخدم لإجراء عملية التمديد في هذا العمل.



الشكل (4). نموذج لتحديد الحواف وتوسيعها.

4-2-6- تجهيز بيانات التدريب (المدخلات والهدف)

تجهز في هذه الخطوة مصفوفتان, مصفوفة المدخلات p بحجم (8×n) ومصفوفة هدف t بحجم (1×n)، إذ إن n هو عدد الخلايا الصورية في قاعدة بيانات التدريب. تجهز بيانات هاتين المصفوفتين بتزحيف نافذة بحجم 3×3 على الصورة الرمادية الموسعة. إذا كانت قيمة الخلية الصورية لمصفوفة الحواف الموسعة المقابلة للخلية المركزية للنافذة تساوي صفراً فسوف تعطى قيمة الخلية الصورية للصورة الرمادية الموسعة المقابلة للخلية المركزية للنافذة إلى العنصر i من مصفوفة الهدف t, وأيضاً تعطى قيم الخلايا الصورية للصورة الرمادية الموسعة المقابلة لبقية خلايا النافذة إلى العمود i من مصفوفة المدخلات p وحسب التسلسل الموضح في الشكل (5), أما إذا كانت قيمة الخلية الصورية لمصفوفة الحواف الموسعة المقابلة للخلية المركزية للنافذة تساوي 1 فتُهمل بيانات الصورة

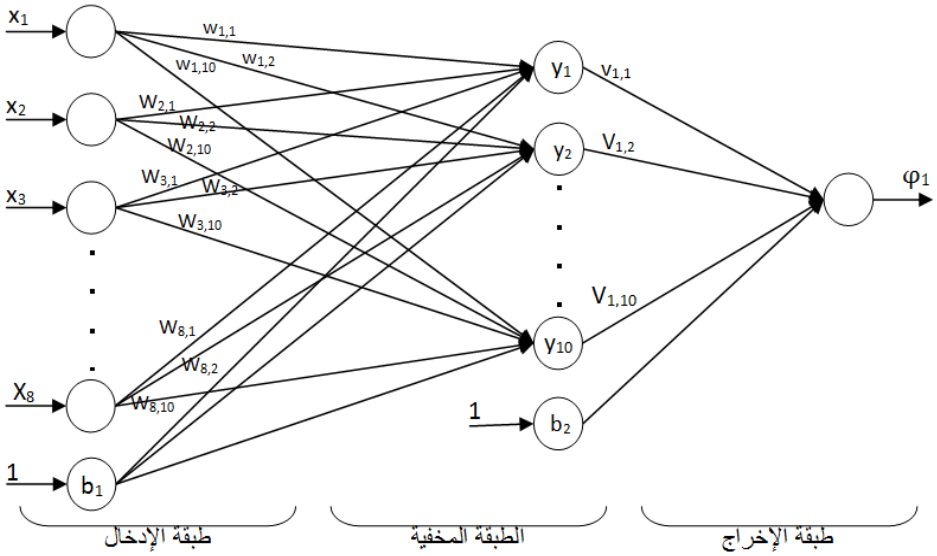
الرمادية الموسعة المقابلة للنافذة. ثم تزحف النافذة بمسافة خلية واحدة وتكرر العملية لتشمل جميع الخلايا الصورية ضمن قاعدة بيانات التدريب.

P_{1i}	P_{2i}	P_{3i}
P_{4i}	t_i	P_{5i}
P_{6i}	P_{7i}	P_{8i}

الشكل (5). تسلسل توزيع الخلايا الصورية المقابلة للنافذة على مصفوفتي بيانات التدريب ضمن العمود i.

4-2-7- تدريب الشبكة العصبية

استخدمت شبكة بيرسبترون متعددة الطبقات Multilayer Perceptron MLP في النظام المقترح لأجل تخمين خلية صورية معينة مما جاورها من خلايا صورية, وذلك بتلقيمها الخلايا الصورية المجاورة للخلية المراد تخمينها بوصفها مدخلات, وعدُّ الخلية نفسها هدفاً للشبكة. معمارية شبكة بيرسبترون متعددة الطبقات المستخدمة في هذا العمل موضحة في الشكل (6). طبقة الإدخال تتكون من ثمان عقد إذ تستقبل أعمدة المصفوفة P بوصفها مدخلات, في حين أن الطبقة المخفية الوحيدة تحتوي على عشر عقد, أما طبقة الإخراج فتتكون من عقدة وحيدة مخرجاتها أعداد صحيحة قيمة إخراجها



الشكل (6). معمارية شبكة بيرسبترون متعددة الطبقات المستخدمة في النظام المقترح.

المستهدف يتراوح من صفر إلى 255 التي تمثل قيمة الخلية الصورية المراد تخمينها. تدرب الشبكة باستخدام عدد من أزواج التدريب (الإدخال والهدف), إذ استخدمت خوارزمية الانتشار العكسي للخطأ باستخدام قاعدة التدريب Gradient descent with momentum, وقد حددت نسبة التعلم بالقيمة 0.01 والزخم بالقيمة 0.9. بعد إتمام التدريب تحفظ أوزان ومعاملات الشبكة المدربة في ملف لغرض استخدامها لتخمين الخلايا الصورية فيما بعد.

4-3- مرحلة التخمين

بعد إجراء عملية تدريب الشبكة العصبية والحصول على الأوزان المثالية, تستخدم هذه الشبكة بوضعها المثالي لأجل تخمين القيم الأصلية للخلايا الصورية للغطاء المضمّن. يستخدم في هذا العمل صور غطاء مضمّن أخفيت فيها البيانات في الخلايا الثنائية من عدة مستويات, ابتداءً من المستوى الأول الأقل أهمية وإلى المستوى

الخامس وأخفيت البيانات في هذه المستويات بنسب مختلفة من إجمالي سعة الغطاء, ابتداءً من 25% إلى 5%, مع العلم أن صور الغطاء المضمّن مصنفة أيضاً إلى الأصناف نفسها التي استخدمت في التدريب. واستخدمت هذه التشكيلة لأجل بيان أداء النظام في هذه الحالات وكذلك بيان تأثير نسبة الإخفاء وكذلك مستوى الإخفاء على أداء النظام المقترح.

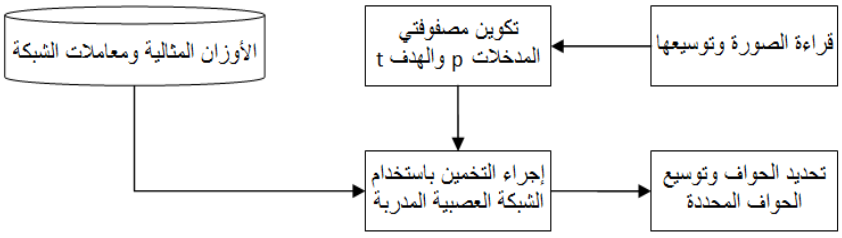
تبدأ مرحلة التخمين بتجميع بيانات الاختبار وتجهيزها, ثم إدخال هذه البيانات إلى الشبكة العصبية الاصطناعية المدربة للحصول على الناتج الذي يمثل تخميناً للقيمة الأصلية للخلية الصورية, ثم تقارن هذه النتائج مع القيم الحالية للخلايا الصورية نفسها لتحديد فيما إذا كانت الخلية متأثرة بإخفاء البيانات أم لا. الخوارزمية التالية توضح خطوات عمل النظام في مرحلة التخمين, والمخطط الانسيابي في الشكل (7) يلخص هذه الخوارزمية.

4-3-1- خوارزمية مرحلة التخمين

1- قراءة محتويات الصورة (الغطاء المضمّن) وتوسيعها بمقدار خلية واحدة من كل جهة.
2- إضافة الخلايا الصورية إلى مصفوفة الهدف t, وإضافة الخلايا المجاورة لكل خلية صورية إلى مصفوفة المدخلات p في عمود المقابل لتلك الخلية.
3- إجراء عملية التخمين باستخدام الشبكة العصبية المدربة ومصفوفة المدخلات p, وخزن الناتج في المصفوفة y.
4- قارنة الناتج y مع مصفوفة الهدف t وإجراء عملية تعتيب لناتج المقارنة للحصول على سلسلة ثنائية تمثل الخلايا الثنائية المخفية.

4-3-2- تهيئة مدخلات الشبكة

تقرأ الصور الغطاء المضمّن المراد استخلاص البيانات المخفية منها وتخزن في المصفوفة x, ثم تجرى عليها عملية توسيع كما في الفقرة (4-3-3). ثم تجهز مصفوفتان, مصفوفة المدخلات p بحجم (8×n) ومصفوفة هدف t بحجم (1×n)، إذ إن n هو عدد الخلايا الصورية في صورة الغطاء المضمّن. تجهز بيانات هاتين المصفوفتين بتمرير نافذة بحجم 3×3 على المصفوفة x بعد التوسيع, إذ تعطى قيمة الخلية للمصفوفة الموسعة المقابلة للخلية المركزية للنافذة إلى العنصر i من مصفوفة الهدف t , وأيضاً تعطى قيم الخلايا للمصفوفة الموسعة المقابلة لبقية خلايا النافذة إلى العمود i من مصفوفة المدخلات p وحسب التسلسل الموضح في الشكل (5). ثم تزحف النافذة بمسافة خلية واحدة وتكرر العملية لتشمل جميع الخلايا الصورية ضمن الصور الغطاء المضمّن المراد استخلاص البيانات المخفية منها.



الشكل (7). المخطط الانسيابي لنظام استخلاص البيانات المخفية (مرحلة التخمين).

4-3-3- إجراء التخمين باستخدام الشبكة العصبية

تخمن الخلايا الصورية باستخدام شبكة الانتشار العكسي العصبية المدربة في المرحلة السابقة, وذلك بتلقيمها عموداً من مصفوفة المدخلات p المهيأة من الخطوة السابقة (الفقرة 4-4-2), عندها تحسب مخرجات الطبقة المخفية للشبكة العصبية كما في المعادلة (2).

$$HO_j = f\left(\left(\sum_{i=1}^{8} I_i * w_{ij}\right) + w_{0j}\right) \quad \cdots (2)$$

إذ إن: j: تسلسل العقدة في الطبقة المخفية, تتراوح من1 إلى 10.

HO: يمثل مخرجات الطبقة المخفية.

i_i: يمثل عموداً من مصفوفة المدخلات p.

w_{ij}: أوزان المدخلات إلى الطبقة المخفية.

w_{0j}: قيمة معامل التحيز bias لكل عقدة مخفية.

ثم تحسب مخرجات طبقة الإخراج للشبكة (أي الناتج النهائي للشبكة) كما في المعادلة (3).

$$y = f\left(\left(\sum_{j=1}^{10} HO_j * w_j\right) + v_0\right) \quad \cdots (3)$$

إذ إن: y: مخرجات الشبكة.

v_j: قيم الأوزان بين الطبقة المخفية وطبقة الإخراج.

v_0: قيمة معامل التحيز bias لطبقة الإخراج.

هذا الناتج يمثل القيمة الأصلية المخمنة للخلية الصورية المراد تخمين قيمتها الأصلية, وهكذا تكرر العملية لتخمين القيم الأصلية لجميع الخلايا الصورية.

4-3-4- استخلاص البيانات المخفية

بعد الحصول على القيم المخمنة للخلايا الصورية y تقارن مع القيم الحالية لهذه الخلايا الصورية التي وضعت في t, ثم نجرى عملية تعتيب لمطلق الفرق بين القيمتين و كما موضح في المعادلة (4).

$$e = \begin{cases} 0 & if\ |y-t| < \theta \\ 1 & if\ |y-t| \geq \theta \end{cases} \quad \cdots (4)$$

إذ إن: θ: قيمة العتبة. e: مؤشر تغير الخلية الصورية.

فإذا كانت قيمة مطلق الفرق بين القيمتين دون العتبة فهذا يعني أن الخلية الصورية لم تتأثر بتضمين البيانات المخفية فتكون قيمة e صفراً. أما إذا كانت قيمة مطلق الفرق مساوية أو أكبر من العتبة فهذه الحالة تدل على أن الخلية الصورية قد تأثرت بتضمين البيانات, ما يستنتج أنها خلية مضيفة للبيانات المخفية.

4-4- نتائج نظام استخلاص البيانات المخفية

درب نظام استخلاص البيانات المخفية باستخدام بيانات التدريب ضمن قاعدة البيانات الموضحة في الفقرة 4-2-2 ولكل مجموعة من مجموعاتها الأربعة بصورة منفردة, ثم اختبر النظام باستخدام بيانات الاختبار ضمن قاعدة البيانات نفسها, تتألف بيانات الاختبار لكل مجموعة من صورٍ أخفيت البيانات ضمن خلاياها الصورية على خمس مستويات ولكل مستوىً بخمس نسب. ولأجل تقييم أداء النظام المقترح حسبت بعض المقاييس (المعايير)

الشائعة اعتماداً على مصفوفة الإرباك Confusion Matrix (وتدعى أيضا بجدول التصادف Contingency Table), ويمكن تكوين مصفوفة إرباك (Confusion Matrix) بحجم 2×2 لأي مصنف معين ومجموعة من الأمثلة (مجموعة اختبار) لتمثيل طبيعة أمثلة المجموعة. هذه المصفوفة تمثل الأساس للعديد من المعايير الشائعة. شكل (8) يظهر مصفوفة الإرباك. الأرقام على طول المحور الرئيسي للمصفوفة تمثل القرارات الصائبة المتخذة أما الأرقام على طول المحور الثانوي فتمثل القرارات الخاطئة – الإرباك – بين الأصناف المختلفة. والمعادلات (5) ... (8) هي لبعض المعايير الشائعة التي يمكن حسابها من مصفوفة الإرباك [6].

الأصناف الفعلية			
		p	n
الأصناف المتوقع {	Yes	TP الايجابي الحقيقي	FP الايجابي الكاذب
	No	FN السلبي الكاذب	TN السلبي الحقيقي
مجموع الأعمدة {		P الايجابي	N السلبي

شكل (8). مصفوفة الإرباك.

$$\text{FPrate} = \frac{FP}{N} \quad \cdots (5)$$

$$\text{TPrate} = \frac{TP}{P} \quad \cdots (6)$$

$$precision = \frac{TP}{TP + FP} \quad \cdots (7)$$

$$accuracy = \frac{\text{TP} + \text{TN}}{\text{P} + \text{N}} \quad \cdots (8)$$

إذ أن: **Tprate**: معدل الإيجابي الحقيقي (أيضا يدعى بنسبة معدل الإصابة والتذكر) للمصنف, وكذلك يشار إليه بمصطلح التذكر Recall, وأيضاً الحساسية Sensitivity.

Fprate: معدل الإيجابي الكاذب (أيضا يدعى بنسبة الإنذار الكاذب) للمصنف.

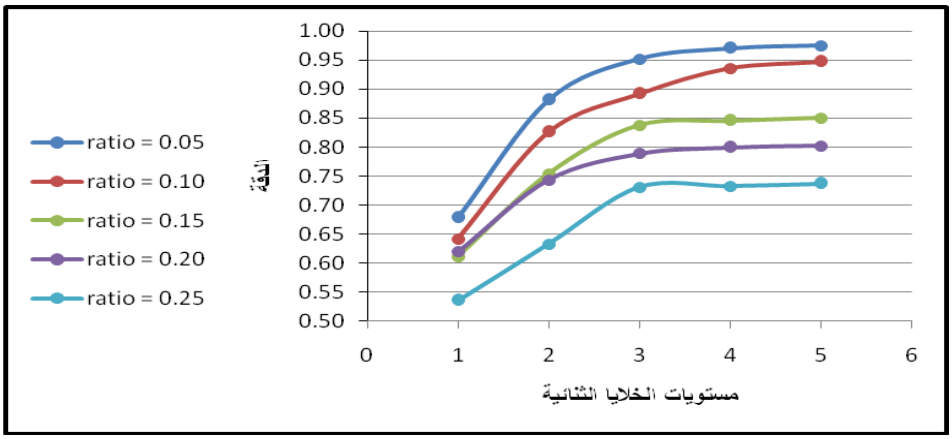
Precision: القيمة التنبؤية الإيجابية Positive Predictive Value.

Accuracy: الدقة, نسبة التنبؤ الصحيح.

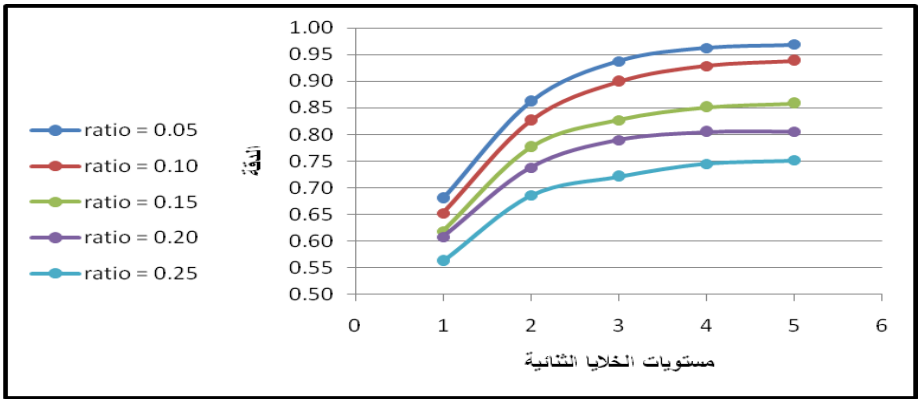
المخططات البيانية لمقياس الدقة Accuracy للمجموعات الأربعة بمختلف النسب والمستويات مبينة في الشكل (9)–الشكل (12). حسب مقياس الدقة وفقاً للمعادلة (8). من أجل تحليل نتائج اختبار النظام المقترح, أخذ معامل الارتباط بين قيم كل من المقاييس المحسوبة ونسبة الإخفاء فكانت النتائج كما في الجدول (1), وكذلك أخذ معامل الارتباط بين هذه المقاييس ومستوى الخلايا الثنائية الذي تخفى البيانات فيه فكانت النتائج كما في الجدول (2).

الجدول (1). معامل الارتباط مع نسبة الإخفاء.

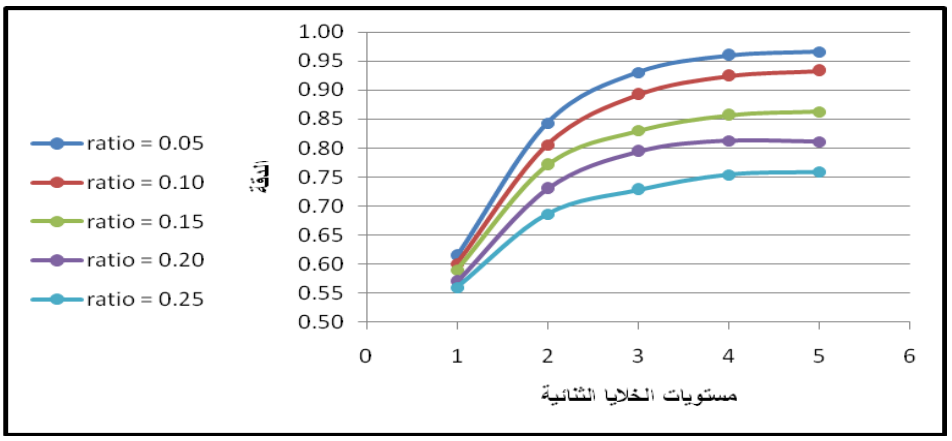
Accuracy	Precision	TP rate	FP rate	
-0. 97671	-0. 26098	-0. 75643	0. 630234	المجموعة 1
-0. 99384	0. 030304	-0. 7548	0. 736769	المجموعة 2
-0. 99616	0. 271388	-0. 7657	0. 825747	المجموعة 3
-0. 9301	-0. 28957	-0. 79892	0. 669416	المجموعة 4
-0. 9742	-0. 06221	-0. 76897	0. 715542	المعدل



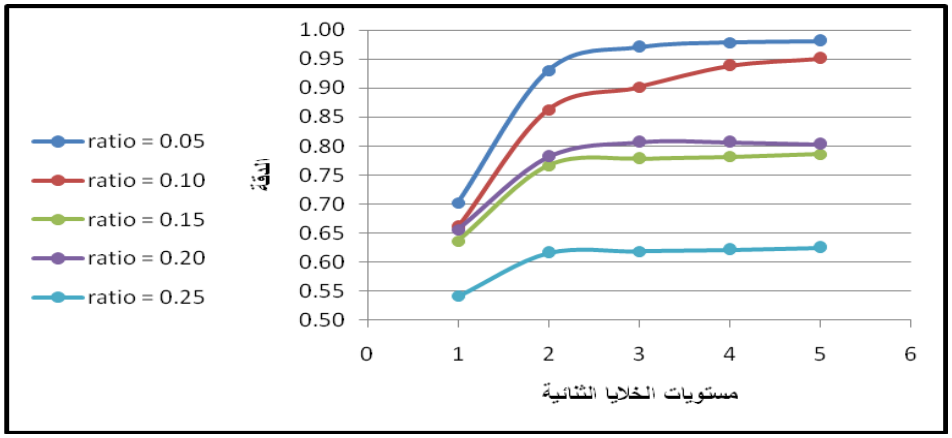
الشكل (9). المخطط البياني لمقياس الدقة Accuracy للمجموعة الأولى.



الشكل (10). المخطط البيانى لمقياس الدقة Accuracy للمجموعة الثانية.



الشكل (11). المخطط البياني لمقياس الدقة Accuracy للمجموعة الثالثة.



الشكل (12). المخطط البياني لمقياس الدقة Accuracy للمجموعة الرابعة.

الجدول (2). معامل الارتباط مع مستوى الخلايا الثنائية.

Accuracy	Precision	TP rate	FP rate	
0. 871624	0. 795778	-0. 87764	-0. 89303	المجموعة 1
0. 87813	0. 990296	-0. 92233	-0. 904	المجموعة 2
0. 872878	0. 986652	-0. 94162	-0. 90476	المجموعة 3
0. 801507	0. 244966	-0. 88446	-0. 86987	المجموعة 4
0. 856035	0. 754423	-0. 90651	-0. 89291	المعدل

نجد أن لمقياس الدقة علاقة عكسية قوية جداً مع نسبة الإخفاء, أي أنها تقل بزيادة نسبة الإخفاء, ولكن للدقة علاقة طردية قوية مع مستوى الخلايا الثنائية, فأعلى قيمة لمقياس الدقة تكون عند الإخفاء في المستوى الخامس, وتقل هذه القيمة تدريجياً مع النزول في مستوى الخلايا الثنائية. أما مقياس قيمة التنبؤ الإيجابي فنجد أن له علاقة ضعيفة مع نسبة الإخفاء, أي أنها لا تعتمد على نسبة الإخفاء. وله علاقة قوية مع مستوى الخلايا الثنائية في المجموعات الثلاثة الأولى, ولكن له علاقة ضعيفة مع مستوى الخلايا الثنائية عند استخدام المجموعة الرابعة, وهذا يظهر جلياً في الشكل (12), إذ يلاحظ عدم انتظام توزيع وتباعد المنحنيات التي تمثل نسب الإخفاء, والسبب قد يعود إلى طبيعة البيانات في هذه المجموعة.

معدل الإيجابي الحقيقي له علاقة عكسية مع نسبة الإخفاء, أما معدل الإيجابي الكاذب فله علاقة طردية مع نسبة الإخفاء. ولكن في حالة العلاقة مع مستوى الخلايا الثنائية فإن للمعدل الإيجابي الحقيقي والمعدل الإيجابي الكاذب علاقة عكسية مع مستوى الخلايا الثنائية.

إحدى المشاكل التي تواجه النظام المقترح هي وجود البيانات المتضاربة, والبيانات المتضاربة تعني أن يكون لمتجهي إدخال متساويين في القيم أهداف مختلفة, أو بتعبير آخر, أن يكون لخليتين صوريتين مختلفتين بالقيم منطقتا جوار متطابقتان, وهذا قد يسبب إرباكاً للشبكة العصبية, إذ أن الخلايا الصورية المجاورة للخلية المراد تخمين قيمتها تشكل مصفوفة المدخلات p كما موضح في الفقرة 4-2-6. من أجل رصد هذه المشكلة في النظام المقترح حسب عدد حالات البيانات المتضاربة في قاعدة البيانات الخاصة بالنظام المقترح. النسب المئوية للبيانات المتضاربة مبينة في الجدول (3), وهي نسبة البيانات المتضاربة إلى البيانات الكلية.

الجدول (3). النسبة المئوية للبيانات المتضاربة.

	النسبة المئوية
المجموعة 1	13. 53 %
المجموعة 2	20. 28 %
المجموعة 3	9. 10 %
المجموعة 4	15. 53 %

طبق النظام المقترح المدرب باستخدام المجموعات الأربعة كلاً على حدة على صورة Lena بحجم 154×103, الشكل (13), التي استخدمها Aruna Ambalavanan وRajarathnam Chandramouli لاختبار طريقة باياس لتحليل الإخفاء في الصورة Bayesian Image Steganalysis Approach المقترحة في [1] لتخمين الرسالة السرية المضمنة, وذلك لأجل مقارنة أداء النظام المقترح في ظروف تطبيق طريقة Aruna

نفسها و Rajarathnam لأنه لم يتسنَ لنا الحصول على البرنامج الخاص بهذه الطريقة لتطبيقها على قاعدة البيانات الخاصة بالنظام المقترح في هذا البحث. اقتصر التطبيق على المستويات الثالث والرابع والخامس لأن نتائج طريقة Aruna المتوفرة هي محصلة لهذه المستويات فقط.

الشكل (13). صورة Lena.

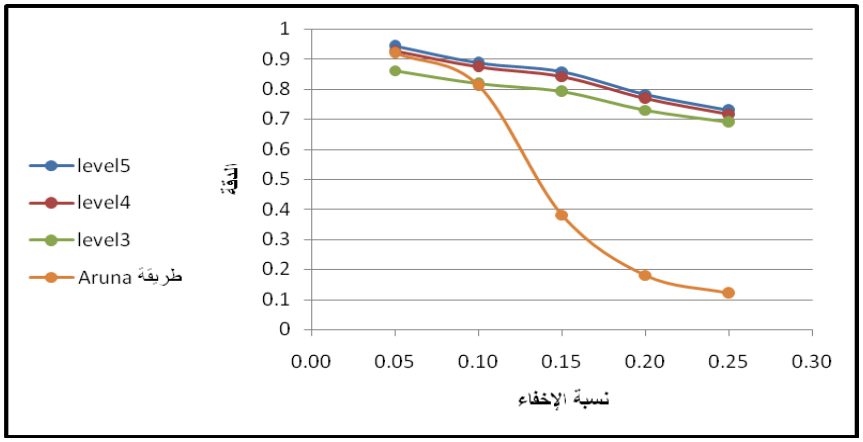
المخططات البيانية لتمثيل الدقة Accuracy للنظام المقترح بالمقارنة مع طريقة Aruna و Rajarathnam مبينة في الشكل (14) – الشكل (17). من ملاحظة المقارنة بين النظام المقترح و طريقة Aruna و Rajarathnam يتبين أن النظام المقترح أثبت كفاءة أعلى خاصة في حالة الإخفاء بنسب عالية إذ تخفق طريقة Aruna و Rajarathnam.

4-5- الاستنتاجات

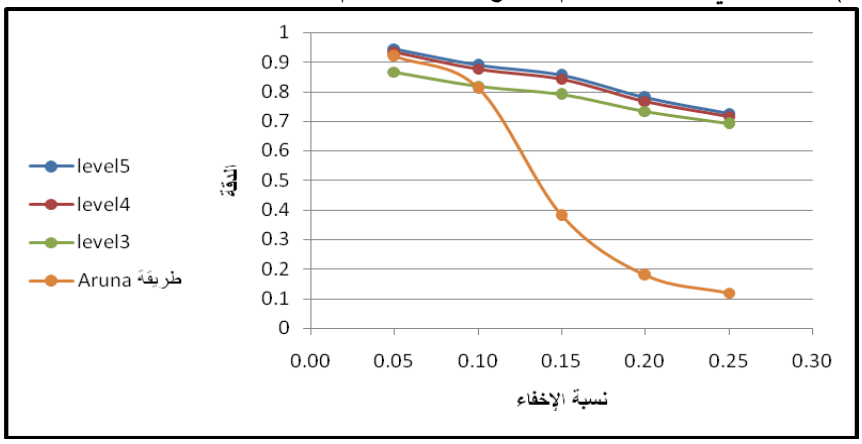
انتظام العلاقة ما بين الخلايا الصورية المتجاورة في معظم مناطق الصورة توفر الأرضية المناسبة لبناء نظام لاستخلاص البيانات المخفية في الصور. تنوع البيانات الكبير ضمن قاعدة البيانات المجهزة يتولد عنها تضارب وعدم انسجام لذا قد يكون من المفيد تصنيفها والتعامل مع كل صنف منفصلاً. فوجود البيانات المتضاربة وغير الطبيعية يربك عمل نظام استخلاص البيانات المخفية ويجعل وصوله إلى حالة الاستقرار صعباً.

العلاقة بين أداء نظام استخلاص البيانات المخفية ونسبة الإخفاء عكسية, إذ كلما قلت نسبة الإخفاء زادت كفاءة النظام المقترح, وذلك لأن النظام المقترح يعتمد على الخلايا الصورية المجاورة للخلية المراد تخمينها لتخمين قيمتها الأصلية, فكلما زادت نسبة الإخفاء زادت احتمالية تغير قيم الخلايا المجاورة لهذه الخلية مما يؤثر سلباً على دقة تخمين قيمتها الأصلية. لكن استخدام الشبكات العصبية مكَّن النظام المقترح من التقليل من تأثير البيانات المغلوطة (المتغيرة قيمتها) على دقة نتائجها والحفاظ على مرونة عالية بالمقارنة مع طريقة Aruna و Rajarathnam (المعتمد على صيغ رياضية أقل مرونة), إذ من المعروف أن الشبكات العصبية قادرة على إعطاء نتائج تقريبية حتى بفقدان أو تغير قيم بعض المدخلات. وهذا يبرر تزايد الفرق بين أداء النظامين بزيادة نسبة الإخفاء.

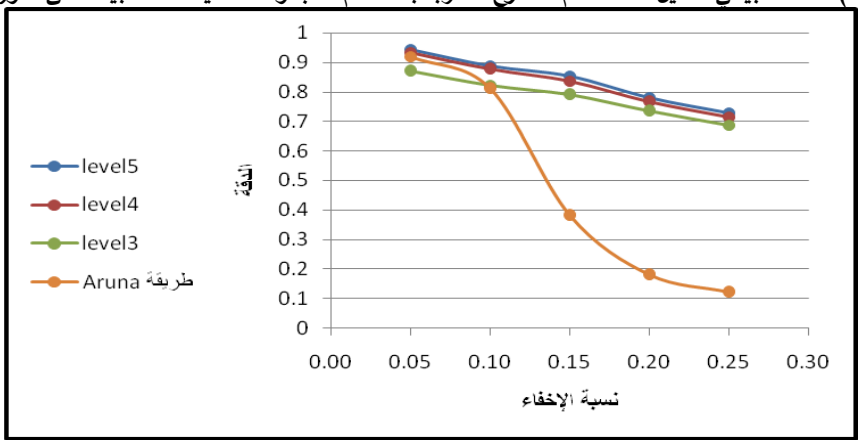
العلاقة بين أداء نظام استخلاص البيانات المخفية ومستوى الخلايا الثنائية التي تخفى فيه البيانات علاقة طردية, إذ إن أداء النظام أفضل ما يكون عند المستوى الخامس, في حين يكون الأداء أقل عند المستوى الأول (الأقل أهمية) لأن قيمة الاختلافات بين القيمة الأصلية للخلية الصورية وقيمتها بعد اخفاء البيانات تزداد عند الاخفاء في مستويات أعلى.



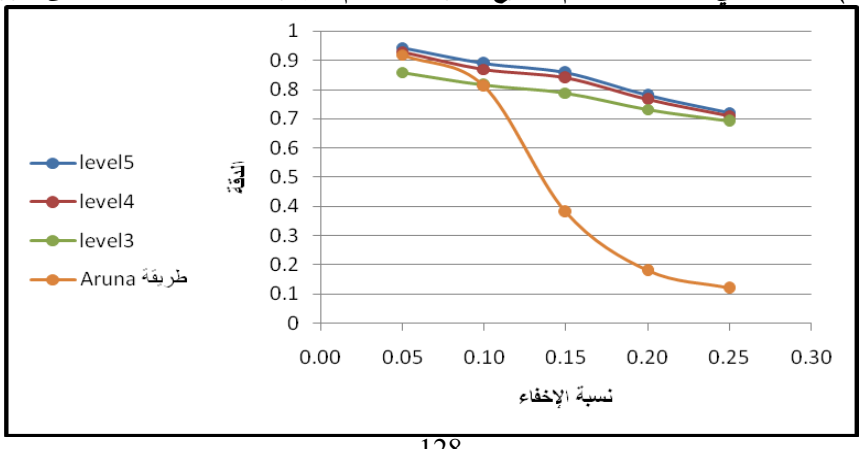
الشكل (14). مخطط بياني لتمثيل دقة النظام المقترح المدرب باستخدام المجموعة الأولى عند تطبيقه على صورة Lena.



الشكل (15). مخطط بياني لتمثيل دقة النظام المقترح المدرب باستخدام المجموعة الثانية عند تطبيقه على صورة Lena.



الشكل (16). مخطط بياني لتمثيل دقة النظام المقترح المدرب باستخدام المجموعة الثالثة عند تطبيقه على صورة Lena.



الشكل (17). مخطط بياني لتمثيل دقة النظام المقترح المدرب باستخدام المجموعة الرابعة عند تطبيقه على صورة Lena.

المصادر

[1] Ambalavanan Aruna, Chandramouli Rajarathnam. "A bayesian image steganalysis approach to estimate the embedded secret message". International Multimedia Conference, Proceedings of the Multimedia and Security, ACM Press, New York, USA, pp. 33 – 38, 2005.

[2] Chandramouli R. "A mathematical framework for active steganalysis". ACM Multimedia Systems Journal, Special Issue on Multimedia Watermarking, Multimedia Systems vol. 9, no. 3, pp. 303–311, 2003.

[3] Chandramouli R. and Memon N. D. " Steganography Capacity: A Steganalysis Perspective". SPIE Proceedings of Security and Watermarking of Multimeida Contents, 2003.

[4] Davidson Jennifer, Bergman Clifford and Bartlett Eric. "An Artificial Neural Network for Wavelet Steganalysis". Proceedings of SPIE - The International Society for Optical Engineering, vol. 5916, Mathematical Methods in Pattern and Image Analysis, pp. 1-10, 2005.

[5] Din Roshidi and Samsudin Azman. "Digital Steganalysis: Computational Intelligence Approach". International Journal of Computers, Issue 1, Vol. 3, 2009.

[6] Fawcett Tom. "ROC Graphs: Notes and Practical Considerations for Data Mining Researchers". Technical Report, Intelligent Enterprise Technologies Laboratory, HP Laboratories Palo Alto, HPL-2003-4, Hewlett-Packard Company, January 2003.

[7] Fridrich Jessica and Goljan Miroslav. "Practical Steganalysis-State of the Art". Proc. SPIE Photonics West, Vol. 4675, Electronic Imaging 2002, Security and Watermarking of Multimedia Contents, San Jose, California, pp. 1-13, January 2002.

[8] Kobsi Nouha and Merouani Hayet Farida. "Neural Network Based Image Steganalysis: A Comparative Study". JIG'2007 - 3èmes Journées Internationales sur l'Informatique Graphique. pp. 235-240, 2007.

[9] Lafferty Patricia and Ahmed Farid. "Texture Based Steganalysis: Results for Color Images". Proc. SPIE, vol. 5561, pp. 145-151, Aug 2004.

[10] Li Bin, He Junhui, Huang Jiwu and Shi Yun Qing. "A Survey on Image Steganography and Steganalysis". Journal of Information Hiding and Multimedia Signal Processing, Vol. 2, No. 2, April 2011.

[11] Meghanathan Natarajan end Nayak Lopamudra. "Steganalysis Algorithms for Detecting the Hidden Information in Image, Audio and Video Cover Media". International Journal of Network Security & Its Application (IJNSA), vol.2, no.1,pp. 43-55, January 2010.

[12] Nosrati Masoud, Karimi Ronak, Nosrati Hamed and Karimi Maryam. "An introduction to steganography methods". World Applied Programming, Vol 1, No 1, pp. 37-41, April 2011.

[13] Özer Hamza. "Audio Watermarking, Steganalysis Using Audio Quality Metrics, and Robust Audio Hashing". Ph.D. thesis, the Institute for Graduate Studies in Science and Engineering, Boğaziçi University, 2005.

[14] Revathi M., Bhattacharjee J. B., Vijayalakshmi S. "Framework of LSB, Adaptive Steganalysis with IQM and Stegnography of Digital Media". Georgian

Electronic Scientific Journal: Computer Science and Telecommunications, Vol. 24, No.1, pp. 39-48, 2010.

[15] Richer Pierre. "Steganalysis: Detecting Hidden Information with Computer Forensic Analysis". SANS Institute, 2003.

[16] Sabeti Vajiheh, Samavi Shadrokh, Mahdavi Mojtaba and Shirani Shahram. "Steganalysis of Embedding in Difference of Image Pixel Pairs by Neural Network". ISC, vol. 1, no. 1, pp. 17-26, January 2009.

[17] Trivedi Shalin and Chandramouli R. "Active Steganalysis of Sequential Steganography". SPIE conference California, Vol. 5020, No. 13, pp. 123–130, January 2003.

[18] Trivedi Shalin and Chandramouli R. "Secret Key Estimation in Sequential Steganography" IEEE Transactions on Signal Processing, Vol. 53, Issue 2, Part 2, pp. 746-757, Feb 2005.

[19] Umbaugh Scott E. "Computer Vision and Image Processing: A Practical Approach Using CVIP Tools" Prentice Hall RTP, 1998.

[20] Xie Chunhui, Cheng Yimin and Chen Yangkun. "An active steganalysis approach for echo hiding based on Sliding Windowed Cepstrum". Signal Processing, Vol. 91, pp. 87–89, 201.