المجلة العراقية للعلوم الإحصائية (24) 2013

ص ص[35-50]

إخفاء واسترجاع البيانات المشفرة بطريقة XOR في صورة باعتماد شبكتي RBF وGRNN و المقارنة ما بين أداء الشبكتين

د.عبد الستار محمد خضر* عامرة استقلال بدران ** فرهاد محي الدين***

الملخص

في هذا البحث تم إخفاء صورة داخل صورة أخرى وذلك بتطبيق عملية (XOR) بين الخليتين الثنائيتين الأقل أهمية من كل بايت من الصورة الغطاء وخليتين ثنائيتين من الرسالة المراد ارسالها لإنتاج الغطاء المضمن (stego_cover)، الذي يدخل مع الغطاء على شبكة دالة الأساس الشعاعي Radial Basis Function Network (RBF) أو شبكة الارتداد العصبية العامة General Regression Neural Network (GRNN) لاستخراج الوزن.

يرسل الغطاء مرة واحدة إلى المستلم ويمكن أن يحتفظ فيه بعدد غير محدود من الرسائل، ولكل رسالة يتم إخفاؤها سوف يتم إرسال أو ان الشبكة المدربة فقط، والذي يرسل كمفتاح إلى المستلم، عندها يقوم المستلم باستخدام الغطاء مع الوزن الذي استلمه لفك الإخفاء، وبذلك فإن هذه الطريقة تتضمن مستويين من الحماية، المستوى الأول يمثل إخفاء الرسالة في الغطاء لتكوين غطاء مضمن، والمستوى الثاني يمثل تشفير الغطاء المضمن باستخدام الشبكة العصبية (RBF) أو (GRNN) باعتبار الغطاء المضمن هو الهدف (target) والصورة الغطاء هي الإدخال إلى الشبكة، عندها يتم تكوين الأوزان التي تمثل البيانات المشفرة وذلك عن طريق تدريب الشبكة. وبعد ذلك يتمكن المستلم عن طريق شبكة (RBF) أو (GRNN) من فك الإخفاء والحصول على الغطاء المضمن ومن ثم الحصول على الرسالة.

وفي هذا البحث أجريت مقارنة بين اداء الشبكتين (RBF) و (GRNN) ولاحظنا ان شبكة (GRNN) افضل من شبكة (RBF). وقد استخدمت لغة (Matlab R2010a) لانجاز هذا البحث.

* أستاذ مساعد / الكلية التقنية / هيئة التعليم التقني

** مدرس / قسم علوم الحاسوب / كلية علوم الحاسوب والرياضيات / جامعة الموصل

*** بكالوريوس / قسم علوم الحاسوب / كلية علوم الحاسوب والرياضيات / جامعة الموصل

تاريخ استلام البحث 2013/10/7 ——— **تأريخ القبول** 2013/3/24

Hiding & Retrieval of Encrypted Data in an Image Using XOR Based on RBF and GRNN Networks and Comparison between their Performance

Abstract

In this paper an image is hidden in another image by applying logical XOR operation to the two least significant bit of each byte of the cover and two bits of the secret message to produce the stego-cover image which is used as an input with the cover to Radial Basis Function Network (RBFN) or General Regression Neural Network (GRNN) to produce the weights.

Cover is delivered once to the recipient who can use it for unlimited number of messages. The weights are delivered to the recipient for each hidden message as a key. The recipient uses the cover with the weights to unhide the message, so that this method includes two levels of security. The first one is hiding the message in the cover to produce stego-cover image. The second one is ciphering the embedded image using RBF Neural Network or GRNN. The stego-cover is considered as a target and the input to the neural network is the cover image. Then the weights, which represent the encrypted information are reconstructed by training the neural network. The recipient can use RBF Network or GRNN to unhide the message by having the stego-cover image then the message.

In this paper the performance of RBF Neural Network and GRNN are compared. Noted that the GRNN is better than RBF for this work. Matlab R2008a was used in this paper.

1- المقدمة

نظراً لتزايد استخدام التقنيات الرقمية وسهولة تناقل المعلومات وسهولة الوصول إليها باتت المعلومات الشخصية عرضة للانتهاك فأصبح من الضروري إيجاد طرائق تضمن وصول المعلومات من المرسل إلى المستلم من دون انتهاك أمنيتها ومن ثم المحافظة على سرية المعلومات وعدم إطلاع المتطفلين عليها. واحد أهم الطرائق لتحقيق أمنية المعلومات هو اخفاؤها عن أعين المتطفلين حيث يتم إخفاء البيانات داخل بيانات أخرى (cover) بطريقة لا تثير إية شبهة أو شك يؤدي إلى كشف هذا الإخفاء[2] .

استخدمت الشبكات العصبية الاصطناعية للمساعدة في إتمام عملية الإخفاء وفكه ولإضافة درجة اكبر من الصعوبة لفك الإخفاء من قبل المتطفلين، وقد استخدمت الشبكتين العصبيتين (RBF) او (GRNN) لقدرتهما على استرجاع البيانات بصورة صحيحة.

في هذا البحث اخفيت صورة (الرسالة) داخل صورة أخرى (الغطاء) بتطبيق عملية الـ (XOR) بين الخليتين الثنائيتين الأقل أهمية من كل بايت من الصورة الغطاء وخليتين ثنائيتين من الرسالة المراد ارسالها لإنتاج الغطاء المضمن (stego_cover)، ويمكن استخدام أية خوارزمية أخرى للإخفاء بحسب ما يتوافق مع الغرض المستخدم له.

2- الأعمال السابقة:

في البحث[8] استخدمت طريقة سريعة للعلامة المائية الرقمية السمعية بالاعتماد على شبكة Counter-Propagation العصبية. وفي البحث [7] اقترح الباحثون إطار عمل لتقليل نسبة التشويه المضاف إلى الغطاء بعملية الإخفاء بإستخدام خوارزميات الإخفاء العامة، استخدم الباحثون نظام ترميز Syndrome-Trellis مستندا الى ترميز ثنائي الالتفاف مزود بخوارزمية Viterbi. أما في البحث [1] فقد أجريت عملية إخفاء واسترجاعها بيانات مشفرة بطريقة LSB في صورة باعتماد شبكة RBF بطريقة بحيث تمكن المستخدم من إرسال الغطاء دون البيانات المخفية ثم الاعتماد على شبكة RBF المدربة لإيجاد الغطاء المضمن ثم استرجاع البيانات المخفية.

3- شبكة دالة الأساس ألشعاعي(Radial Basis Function Network)

وتعد من أكثر الشبكات استخداماً وهي أيضاً شبكة ذات تغذية أمامية لكن بطبقة مخفية واحدة. و(RBF) هي شبكة بطبقتين، إن لم تحتسب طبقة الإدخال إذ لا تتم في طبقة الإدخال أية معالجة على عكس الطبقة المخفية حيث تتم فيها المعالجة والطبقة الأخيرة حيث ينجز مجموع موزون مع إخراج خطي. وحدات إخراج شبكة RBF تشكل تركيبا خطيا لدوال أساسية احتسبت بواسطة الوحدات المخفية [3].

الدوال الأساسية في الطبقة المخفية تنتج استجابة محصورة في منطقة محددة للإدخال وهذه المنطقة لها مركز. وهذه الاستجابة تعد قيم إدخال خاصة ولها أعلى قيمة إخراج، وقيمة الإخراج هذه تصبح بمثابة قيم الإدخال وتنطلق من هذه النقطة[4].

الدالة الأساسية نشير إليها بوصفها دالة تنشيط وهنا الدالة الأكثر شيوعاً هي دالة كاوس (Gaussian function) ، في عام 1733 اشتق DeMoivrre المعادلة الرياضية لمنحني التوزيع الطبيعي والذي يسمى أيضا بمنحني كاوس نسبة إلى (Gauss 1777-1855) الذي اشتق معادلته عند الخطأ في القياسات المتكررة[6]. دالة التنشيط لشبكة RBF هي (radial basis)، وكما موضح في المعادلة الآتية[5]:

$$radbas\ (n) = e^{n^2} \qquad \cdots\cdots \qquad (1)$$

قيم الإخراج للوحدة المخفية تقع بين 0 و 1 ، الدخل الأقرب إلى مركز كاوس هي العقدة الأكبر استجابة(اكبر العقد استجابة) لان العقدة (العصب) تنتج إخراجا مطابقا للمدخلات بمسافة متساوية عن مركز كاوس وهذا ما يدعى بـ Radial basis [3][4].

شبكة RBF تشكل طبقة مخفية واحدة للدالة (Basis function) أو العصبونات. عند إدخال كل عصبون يتم حساب المسافة بين مركز العصبون وقيمة الإدخال ثم يتم تشكيل الإخراج للعصبون بتطبيق الدالة الأساسية (كاوس) لهذه المسافة. كذلك يمكن أن تكون شبكات RBF متعددة المخرجات[3].

3-1- تدريب شبكة RBF:

تتألف شبكة RBF من بنية ذات تغذية أمامية مع طبقة إدخال وطبقة مخفية من وحدات شبكة RBF وطبقة إخراج مؤلفة من وحدات خطية.

تحول طبقة الإدخال متجه الإدخال إلى الوحدات المخفية التي تشكل استجابة محصورة لنمط الإدخال. تجهزنا بمستويات التنشيط لوحدات الإخراج بإشارة الاقتراب لمتجه الإدخال إلى التصنيف.

يمر التدريب بمرحلتين، حيث تستخدم تقنية العنقدة غير المُرشَدة (unsupervised clustering technique) للطبقة المخفية، بينما يطبق التدريب المُرشَد (supervised) على وحدات طبقة الإخراج[3].

العقد في الطبقة المخفية تنفذ بواسطة الدالة الأساسية التي تعمل على منطقة محصورة من حيز الإدخال. وذلك باعتماد المعادلة الآتية[5]:

$$a\,l_i = radbas\ (\left\| I_i W_{1,1} - p \right\| b\,l_i) \qquad \cdots\cdots \qquad (2)$$

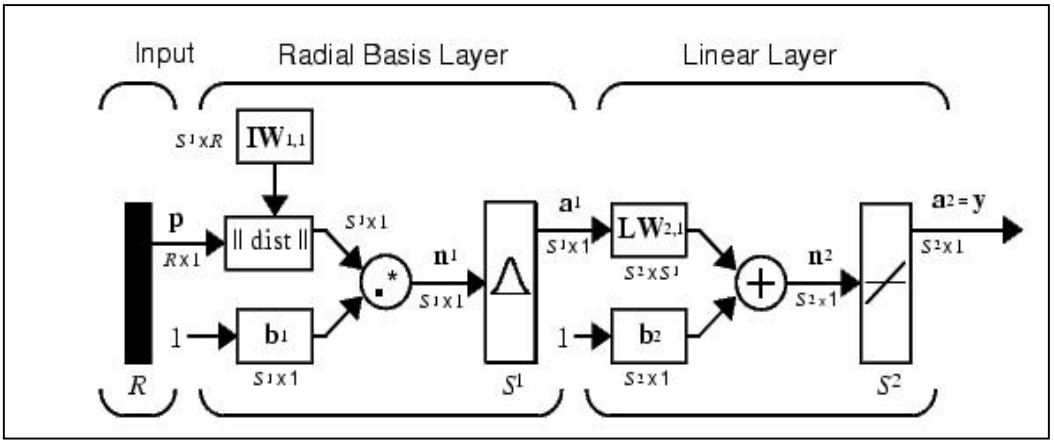
حيث ان:- b: مصفوفة الـ basis. p: مصفوفة الإدخال. $I_iW_{1,1}$: مصفوفة الوزن للطبقة المخفية.

ومن ثم العقد في طبقة الإخراج تنفذ بواسطة الدالة الخطية التي تعمل على منطقة محصورة من حيز الإخراج. وذلك باعتماد المعادلة الآتية[5]:-

$$a2 = purelin\ (LW_{2,1}a_1 + b_2) \qquad \cdots\cdots \qquad (3)$$

حيث ان:- b: مصفوفة الـ basis. LW2,1: مصفوفة الوزن لطبقة الإخراج.

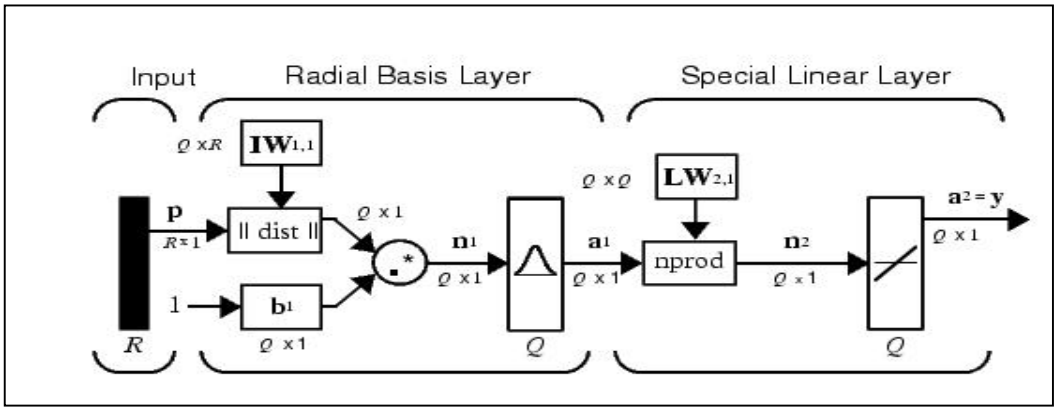
ثم يتم تحسين الشبكة بإضافة عقد انحياز (Bias node) إلى طبقة الإدخال والطبقة المخفية ويتم تغيير الوزن لهذه العقد كما هو الحال في بقية العقد المكونة للشبكة عدا قيمة الإدخال لعقدة الانحياز دائما تكون +1[3].



الشكل (1) التركيب العام لشبكة الدالة الأساس الشعاعية.

4- شبكة الارتداد العصبية العامةGeneral Regression Neural Network

هي عبارة عن هندسة شبكة عصبية معمارية تستخدم في حل مسائل تقريب الوظيفة، عملية التدريب هي مشابهة لعملية إيجاد سطح في فضاء متعدد الأبعاد، يجهز أفضل ملاءمة للبيانات المدربة. التعميم يعني استخدام السطح المتعدد الأبعاد لتوليد بيانات الاختبار [6]. الشكل(2) يوضح التركيب العام لشبكة الارتداد العصبية العامة[5].



الشكل (2). التركيب العام لشبكة الارتداد العصبية العامة.

حيث ان:- Q = تمثل عدد العصبونات في الطبقة الاولى وتمثل عدد العصبونات في الطبقة الثانية. وتمثل ايضا عدد ازواج (الادخال / الاخراج). R = تمثل عدد عناصر متجه الادخال .

وكما مبين بالشكل السابق فإن شبكة GRNN تتكون من ثلاث طبقات من العقد العصبية، كل طبقة لديها دور مختلف عن الاخرى :

1- طبقة الادخال (Input Layer): حيث يتم تطبيق الادخالات.
2- طبقة مخفية (Hidden Layer): حيث يتم تطبيق التحويل اللاخطي على البيانات القادمة من منطقة الادخال الى المنطقة المخفية. وفي اغلب التطبيقات تكون المنطقة المخفية ذات بعدية عالية.
3- طبقة الاخراج الخطية(Output Layer): حيث يتم انتاج الاخراج.

ان الطبقة الاولى لها خلايا عصبية بقدر ما هنالك من متجهات الادخال والاخراج فيP وبشكل محدد، فإن أوزان أول طبقة هي قيم 'P وقيمة المتحيز"bias" b1 هي متجه عمودي قيم كل عناصرها 0.836/spread ،وممكن للمستخدم ان يختار قيمة محددة للانتشار spread.

كل ادخال موزون لعصبون هو المسافة بين متجه الادخالP ومتجه الاوزان الخاص به $IW_{1,1}$، يحسب عن طريق معادلة إيجاد المسافة الاقليدية Euclidean distance كما في المعادلةالاتية:

$$D = \sqrt{\sum (X - Y)^2} \qquad \cdots \cdots \qquad (4)$$

ثم يتم تطبيق عملية الضرب النقطي على هذا الادخال الموزون للعصبون مع متجه الـ(bias) لينتج عصبون الادخال للطبقة المخفية (n1) الذي يدخل على دالة التنشيط (radbas) وذلك بالاعتماد على المعادلة (5) لينتج اخراجا للطبقة المخفية (a1) [5].

$$a_i^l = radbas\left(\left\| I_i W_{1,1} - p \right\| b_i^l\right) \quad \cdots\cdots \quad (5)$$

al_i هي عنصر في a1 حيث $liW_{1,1}$ متجه يتكون منْ الصف i من المتجه IW1,1 .

a1 سيدخل على الـ (nprod) الذي يقوم بوظيفة الضرب الاعتيادي بين متجه اخراج الطبقة المخفية وبين صف من مصفوفة اوزان طبقة الاخراج الخطية لتنتج متجه(n2) يدخل على الدالة الخطية، وذلك بالاعتماد على المعادلة الآتية [5]:

$$a2 = purelin(n2) \quad \cdots\cdots \quad (6)$$

ثم يتم تحسين الشبكة بإضافة عقد انحياز (Bias node) الى طبقة الادخال ويتم تغيير الوزن لهذه العقد كما هو الحال في بقية العقد المكونة للشبكة عدا قيمة الادخال لعقدة الانحياز دائما تكون 1+ [2].

ان الانتشار كلما كان كبيرا، زاد حجم المنطقة حول متجه الادخال ، حيث ان عصبونات الطبقة الاولى ستستجيب الى عصبونات اخراج محددة .

لذلك إذا كان ألـ spread صغيار، فستكون نتائج دالة الاساس الشعاعي دقيقة جدا، لكي تكون العصبونات مع متجه الوزن القريبة الى الادخال تمتلك إخراجا أكبر من غيرها من العصبونات.

وبما أنه spread يكون كبيرا مع الوقت، فإن مدى الشبكة سيكون اكثر نعومة وعدة عصبونات ستستجيب إلى متجه الادخال ثم ستتصرف الشبكات وكأنها تأخذ المعدلات الموزونة بين متجهات الـTargetالتي تصميم متجهات ادخالها قريب جداً إلى متجهات الادخال الجديدة.

وكلما كبر ال spread زاد عدد ال Neurons المساهِمة بألـ average وستكون النتائج التي تستخرجها دالة الشبكة العصبية اكثر نعومة [6].

5- النظام المقترح

النظام المقترح يتألف من جزأين، الجزء الأول يمثل العمليات التي تجرى عند المرسل لأجل إخفاء الرسالة السرية، أما الجزء الثاني فيمثل العمليات التي يجريها المستلم لاسترجاع الرسالة السرية.

5-1- الطريقة المعتمدة عند المرسل: هناك عدة خطوات يجب إتباعها عند المرسل.

5-1-1- تهيئة الغطاء والصورة المراد إخفاؤها عند المرسل:

في هذا البحث استخدمت الصور الملونة غطاء ويمكن أن تكون الصورة المستخدمة من نوع (bmp) أو (jpg). اما الصورة المراد اخفاؤها (message) فقد استخدمت صور ملونة من نوع (bmp) حجمها ربع حجم الصورة الغطاء (cover)، ونقوم بتوزيع bits الصورة (message) داخل مصفوفة صفرية تكون بنفس إبعاد الصورة (cover)، وتكون عملية توزيع bits عند المرسل وقبل القيام بعملية الإخفاء ثم يعاد تجميع هذه bits عند المستلم بعد فك الإخفاء.

5-1-2- عملية توزيع الـ bits على المصفوفة الصفرية:

يقوم النظام بتكوين مصفوفة صفرية إبعادها بنفس إبعاد الصورة الغطاء(cover) وتوزيع (bits) للصو ة (message) على المصفوفة الصفرية، لجعل إبعاد الصورة (message) بنفس إبعاد الصورة (cover) وذلك لان حجم الصورة (message) ربع حجم الصورة (cover)، إي إن كل (2bits) من الصورة (message) يتم اخفاؤها داخل (8 bits) من المصفوفة الصفرية.

يتم توزيع الصورة المراد اخفاؤها (message) على المصفوفة الصفرية، بحيث يتم توزيع bits كل (byte) من الصورة المراد اخفاؤها (message) إلى (4 bytes) من المصفوفة الصفرية، بحيث يحصل كل (byte) من المصفوفة الصفرية على 2bit فقط ليتم بعد ذلك جمعه مباشرة مع (cover) لغرض الإخفاء.

5-1-3- الأسلوب المعتمد في إخفاء البيانات:

تنفذ الخوارزمية المستخدمة في عملية الإخفاء في هذا النظام بتطبيق عملية الـ (XOR) بين اخر (2bit) من كل byte من الصورة (cover) والمصفوفة الصفرية. ويمكن توضيح تطبيق عملية XOR لأجل الإخفاء في هذا البحث بأخذ تطبيق رياضي كما موضح في الشكل (3).

	0	0	0	0	0	0	1	0	← بايت من متجه المصفوفة الصفرية
	0	0	1	0	1	1	0	0	← بايت من متجه الغطاء
XOR	0	0	1	0	1	1	1	0	← الناتج سيكون بايت من متجه (stego -cover)

الشكل (3) تطبيق عملية XOR لأجل الإخفاء.

5-1-4- طريقة عمل شبكة RBF و GRNN عند المرسل:

الادخال لشبكة RBF او GRNN هو الصورة الغطاء (cover) والذي يعتبر (X)، والهدف(target) لشبكة RBF او GRNN هو الصورة المضمنة (stego-cover) والذي يعتبر(Y)، بالاعتماد على معادلات التدريب سوف يتم اجراء عملية التدريب ومن ثم الحصول على الوزن النهائي، عندها سوف يتم إرسال الوزن مع الغطاء (cover) إلى الطرف الثاني (المستلم) لاستخدامه في عملية استرجاع الصورة التي تم اخفاؤها. وان هذه الشبكة تتكون من طبقتين، الطبقة الخفية (hidden layer) وطبقة الاخراج.

في هذه المرحلة سوف تكون الأوزان التي تم الحصول عليها لإرسالها إلى المستلم غير مفهومة لأي مترصد، لذلك فهي تعتبر مرحلة مهمة من مراحل التشفير.

5-2- طريقة الاسترجاع عند المستلم: هناك عدة خطوات يجب إتباعها عند المستلم لاسترجاع البيانات المخفية.

5-2-1- طريقة عمل شبكة RBF و GRNN عند المستلم:

بعد أستلام الأوزان (weights) والصورة (cover) من المرسل، تقوم شبكة RBF او GRNN باستخلاص الصورة المخفية، وذلك لاستخراج الصورة المضمنة (stego-cover) من الشبكة. هذه المرحلة تعتبر عملية فك التشفير، وذلك لأن الاوزان التي تم الحصول عليها لإرسالها إلى المستلم سوف تكون غير مفهومة لأي مترصد، لذلك فهي تعتبر مرحلة مهمة من مراحل التشفير، وعندما يقوم المستلم عن طريق شبكة RBF او GRNN بأستلام الوزن الذي يعتبر تشفير الصورة المضمنة واستخراجا (stego-cover)، اي عملية فك التشفير بتسلم الصورة المضمنة الى خوارزمية LSB.

عند المستلم شبكة RBF او GRNN لا تقوم بعملية التدريب لان الوزن قد تم استلامه من المرسل(ثابت)، فضلا عن انه شبكة RBF عند المستلم لا تحتوي على هدف(target) لأنه عند المستلم تقوم شبكة RBF او GRNN بعملية الاختبار(testing) فقط.

5-2-2- عملية فك الإخفاء عند المستلم (التحليل):

يقوم النظام بتطبيق عملية ألـ (XOR) بين الغطاء والصورة المضمنة(stego-cover) فينتج المصفوفة الصفرية التي تحوي في أول 2bits من كل byte فيها على بتات الصورة المرسلة. العملية موضحة في الشكل (4).

بايت من متجه (stego -cover) ←	0	0	1	0	1	1	1	0
بايت من متجه الغطاء ←	0	0	1	0	1	1	0	0
بايت من متجه المصفوفة الصفرية ←	0	0	0	0	0	0	1	0
XOR								

الشكل (4). تطبيق عملية XOR لأجل تحليل الإخفاء.

ومن ثم القيام بعملية تجميع الـ bits التي تم نشرها داخل المصفوفة الصفرية مسبقاً(عند المرسل) لاستخراج الصورة المخفية message.

6- النتائج العملية:

أ- الصورة الغطاء (cover) التي تمت تهيئتها لإخفاء الرسالة فيها موضحة في الشكل(5).

الشكل (5): الصورة الغطاء(cover).

ب- الصورة المراد اخفاؤها (الرسالة)، التي تمت تهيئتها لإخفائها ضمن الصورة الغطاء موضحة في الشكل(6).

الشكل (6): الصورة المراد إخفاؤها

جـ- بعد إجراء عملية الإخفاء سوف يتم الحصول على الصورة الغطاء (cover) وبداخلها الصورة (message)، وتدعى الغطاء المضمن (stego-cover).

د- بعدها يتم فك عملية الإخفاء، ليتم الحصول على الصورة (message) الأصلية فقط التي تم اخفاؤها سابقاً داخل الصورة الغطاء (cover).

أ. باستخدام GRNN. ب. باستخدام RBF.

الشكل (7): الغطاء المضمن المكون عند المستلم من إدخال الصورة الغطاء إلى الشبكة العصبية.

يجب ملاحظة ان المرسل سوف يرسل (Cover) إلى المستلم مرة واحدة فقط وعندها سوف يحتفظ المستلم بال (Cover) لعدد غير محدود من الرسائل (messages). وكلما أراد المرسل إرسال (message) يرسل فقط الأوزان (Weights) عبر قنوات مغطاة من دون معرفة المتطفلين. وعندها سوف يقوم المستلم عن طريق (Cover) الذي سبق ان استلمه مع الوزن الذي سوف يتم الحصول عليه مؤخراً بفك الإخفاء والحصول على (stego-cover) الشكل (7)، ومن ثم الحصول على الرسالة كما هو موضح في الشكل (8). ومن الجدير بالذكر انه يمكن ارسال الغطاء بقناة عادية والأوزان بقناة مغطاة.

أ. باستخدام GRNN.

ب. باستخدام RBF.

الشكل (8): الرسالة المستخلصة بعد الإخفاء.

فائدة استخدام (stego-cover) قريبة من (Cover) بحيث لا يمكن اكتشاف ان فيها بيانات مخفية بالعين المجردة مما يصعب على المتطفل اكتشاف البيانات المخفية حتى في حالة حصوله على (Cover) والأوزان. فضلا عن انه يفضل استخدام صورة كثيرة التفاصيل بالنسبة (Cover)، بحيث لا يكون فيها أي عمودين متشابهين لتجنب حصول إرباك للشبكة العصبية بسبب وجود متجهي مدخلات متشابهين لهما أهداف مختلفة أو العكس أي متجهي مدخلات مختلفين لهما أهداف متشابهة.

7- مناقشة النتائج:

استخدمت شبكة دالة الأساس الشعاعي في [1] لإنجاز التشفير بعد إخفاء البيانات في الصور عن طريق إزاحة الخليتين الثنائيتين الأقل أهمية من الغطاء ووضع بيانات الرسالة السرية مكانهما، أما في هذا البحث فقد استبدلت طريقة الازاحة بعملية XOR المنطقية، إذ تجري عملية XOR بين البيانات السرية وبيانات الغطاء وذلك لتكون البيانات الناتجة أقرب إلى الغطاء فتكون أصعب على محلل الإخفاء.

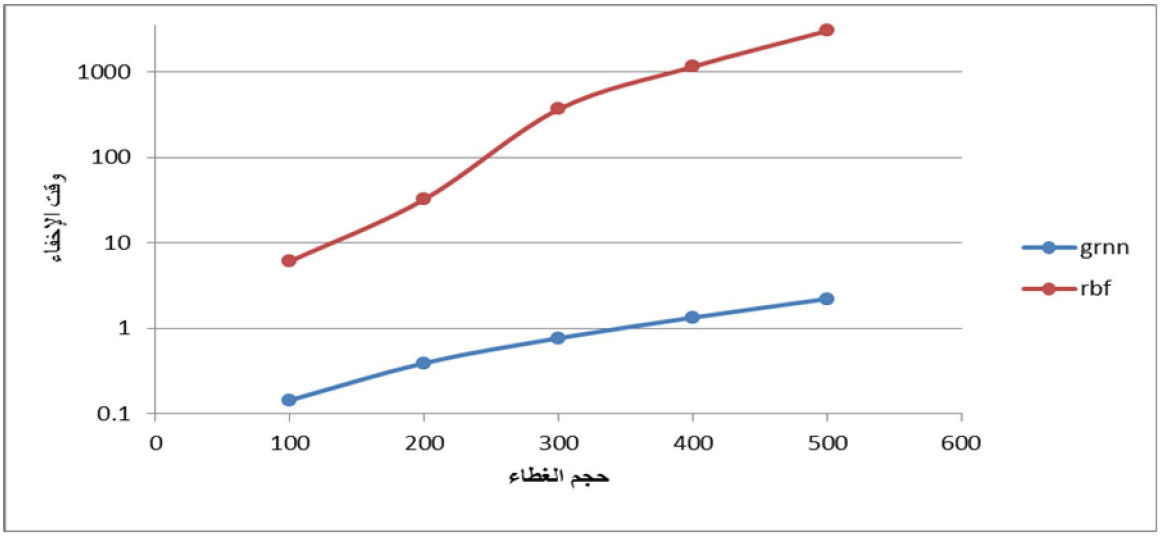
كما استخدمت شبكة الارتداد العصبية العامة لتنفيذ العمل للاستفادة من سرعتها في التدريب مقارنة بشبكة دالة الأساس الشعاعي وكذلك الدقة العالية في إخراج النتائج المتوقعة والجدول (1) يقارن بين أداء كل من الشبكتين من ناحيتي السرعة والدقة.

من الجدول (1) يتبين أن وقت التدريب في حالة استخدام شبكة دالة الأساس الشعاعي يزداد على أساس لوغارتمي بازدياد حجم الغطاء على النقيض منه في حالة استخدام شبكة الارتداد العصبية العامة، إذ تكون الزيادة في وقت التدريب زيادة منتظمة وكما موضح في الشكل (9). أما وقت الاسترجاع فلا يكاد يلاحظ أي فرق في الوقت المستغرق للاسترجاع سوى في حالة حجم الغطاء 500 * 500 والشكل (10) يظهر مقارنة لوقت الاسترجاع.

الجدول (1) مقارنة ما بين أداء شبكتي RBF و GRNN.

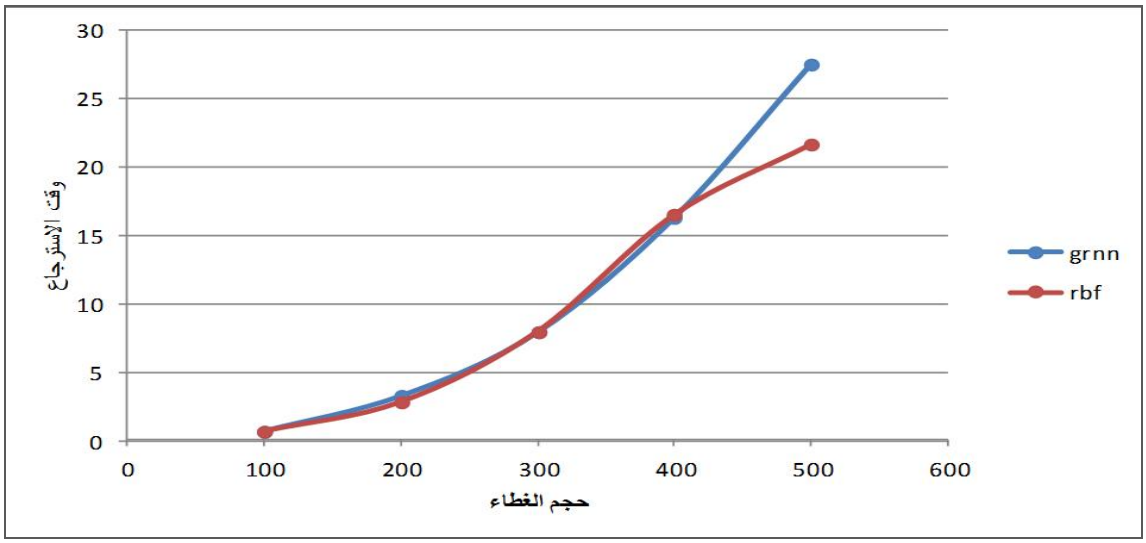
الغطاء المتضمن	أبعاد الغطاء	الشبكة	وقت الإخفاء بالثواني	اسم الرسالة المسترجعة	وقت الاسترجاع بالثواني	MSE	PSNR
stego_grn1	100*100	grnn	0.1445	extracted_grn1	0.7183	0	Inf
stego_rbf1	100*100	rbf	6.0744	extracted_rbf1	0.7143	0	Inf
stego_grn2	200*200	grnn	0.3928	extracted_grn2	3.2806	0	Inf
stego_rbf2	200*200	rbf	32.1615	extracted_rbf2	2.8538	0	Inf
stego_grn3	300*300	grnn	0.7678	extracted_grn3	7.9337	0	Inf
stego_rbf3	300*300	rbf	363.8287	extracted_rbf3	8.0020	0.1408	4.6183e+005
stego_grn4	400*400	grnn	1.3370	extracted_grn4	16.3061	0	Inf
stego_rbf4	400*400	rbf	1.1449e+003	extracted_rbf4	16.5352	0.1158	5.6177e+005
stego_grn5	500*500	grnn	2.2153	extracted_grn5	27.5253	0	Inf
stego_rbf5	500*500	rbf	3.0026e+003	extracted_rbf5	21.6694	0.1398	4.6523e+005

أما بالنسبة للدقة فيلاحظ أنه لا يوجد فقدان في بيانات الرسالة المرسلة عند استخدام شبكة الارتداد العصبية العامة، لكن عند استخدام شبكة دالة الأساس الشعاعي فيوجد فقدان لبعض البيانات المرسلة في الأحجام الكبيرة للغطاء و إن كانت البيانات المفقودة قليلة.



الشكل (9): مقارنة ما بين الوقت المستغرق للإخفاء باستخدام شبكتي RBF وGRNN.

هذه الطريقة تتضمن مستويين من الحماية، المستوى الأول يمثل إخفاء الرسالة في الغطاء لتكوين صورة مضمنه (stego-cover)، والمستوى الثاني يمثل تشفير الصورة المضمنة باستخدام الشبكة العصبية (RBF) أو (GRNN) باعتبارها هي الهدف (target) والصورة الغطاء هي الإدخال إلى الشبكة، عندها يتم تكوين أوزان تمثل البيانات المشفرة، التي تستخدم فيما بعد عند المستلم مع الغطاء لإيجاد البيانات الأصلية.



الشكل (10). مقارنة ما بين الوقت المستغرق للاسترجاع باستخدام شبكتي RBF وGRNN.

8- الاستنتاجات:

يمكن إخفاء حجم كبير من البيانات دون التأثير في ألوان الصورة المرسلة إلى المستلم إذ يرسل الغطاء،و عند استرجاع الرسالة (message) تسترجع غالباً بدون فقدان لبيانات الرسالة المرسلة على الرغم من حجمها الكبير نسبة إلى الغطاء.

إن تطبيق عملية XOR بدلاً من التصفير في الاخفاء زاد من قوة امنية البيانات. واستخدام الشبكات العصبية أعطى أمنية عالية في الإخفاء. لكن إجراء عملية التدريب للشبكة العصبية في كل مرة يجعل عملية الإخفاء تستغرق وقتاً طويلاً خاصة بازدياد أحجام صور الغطاء والرسالة السرية، لكنه في الوقت ذاته يزيد من أمنية الإخفاء وقوتها.

يلاحظ من الجدول (1) أن شبكة GRNN أفضل من شبكة RBF من ناحية سرعة الإخفاء، وذلك لتمتعها بسرعة عالية في مرحلة التدريب. وكذلك من ناحية الدقة في استرجاع البيانات خاصة عند استخدام الصور ذات الأحجام الكبيرة.

9- المصادر

1. محمد خضر، عبد الستار. الزبيدي، لهيب محمد. الحيالي، عامرة استقلال. (2010): "عملية إخفاء واسترجاع بيانات مشفرة بطريقة LSB في صورة باعتماد شبكة RBF" . جامعة الموصل. مجلة الرافدين لعلوم الحاسوب والرياضيات.

2. A., Muhalim M., (2003), “Information Hiding Using Steganography”, University Technology Malaysia.
3. Alex Alexanderidis, Haralambos Sarimveis, George Bavas, (2010) "Modeling of Continuous Digesters Using Adaptive RBF Neural Networks Models", National Technical University of Athens, School of Chemical Engineering.
4. Hopgood Adrian A. (2001) " Intelligent Systems for Engineers and Scientists". CRC Press, 2nd ed..
5. Howared D., Mark B., (2008), ”Neural Network toolbox user’s”, The mathworks.
6. Kasabov Nikola K. (1998) " Foundations of Neural Networks, Fuzzy Systems, and Knowledge Engineering". A Bradford Book, 2nd Printing.

7. T. Filler, J. Judas, and J. Fridrich, (2011), "Minimizing Additive Distortion in Steganography Using Syndrome-Trellis Codes", IEEE Transactions on Information Forensics and Security.

8. W. Guohua, (2008), "A Fast Audio Digital Watermark Method Based on Counter-Propagation Neural Net Works", Hangzhou Dianzi University Institute of Graphics and Image Hangzhou, Chin 9.