المجلة العراقية للعلوم الإحصائية (24) 2013

ص ص[131-143]

إخفاء الصور الرقمية الملونة في ملفات الصوت والفيديو باستخدام الشبكات العصبية

عامرة استقلال بدران *

الملخص

في هذا البحث استخدمت شبكة GRNN لإخفاء صورة داخل ملف غطاء، وقد استخدم نوعان من ملفات الغطاء هما الملف الصوتي و الفيديو. وطبق الإخفاء باستخدام إحدى خوارزميات الإخفاء وهي (Least Significant Bit (LSB)) وذلك بتطبيق عملية الـ (XOR) بين آخر (2bit) من كل byte من الغطاء (cover) و2bit من الرسالة لإنتاج الغطاء المضمن (stego_cover)، الذي يدخل مع الغطاء (cover) على 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(messages). وكل رسالة يتم إخفاؤها سوف يتم إرسال الوزن (weight) فقط، والذي يعتمد مفتاحا، عندها يقوم المستلم باستخدام الغطاء مع الوزن الذي تسلمه لفك الإخفاء، وبذلك فأن 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 (GRNN) باعتبارها هي الهدف (target)و الغطاء هو الإدخال إلى الشبكة، عندها يتم تكوين أوزان تمثل البيانات المشفرة. وبعد ذلك بإمكان المستلم عن طريق شبكة (GRNN) من فك الإخفاء والحصول على الصوت المضمن أو ملف الفيديو المضمن ومن ثم الحصول على الرسالة. وقد استخدمت لغة (Matlab R2010a) لانجاز هذا البحث.

Hiding Colored Digital Images in Audio and Video Files Using Neural Networks

Abstract

In this paper GRNN is used to hide an image into a cover file, Audio and video files are used as cover files in this work. The hiding was applied using one of concealment algorithm that is (Least Significant Bit (LSB)) by applying (XOR) operation between the last (2bits) of each byte of the image (cover) and 2bits of the message to produce the

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

تاريخ استلام البحث 2012/10/7 ——— **تأريخ القبول** 2013/5/5

(stego_cover), which feed with the cover to 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, this method includes two levels of security. The first one is hiding the message in the cover to produce embedded cover (stego-cover). The second one is ciphering the embedded cover using GRNN Neural Network. This Network is considered as a target and the input to the Neural Network is the cover. Then the weights, which represent the encrypted information, are reconstructed. The recipient can use GRNN Network to unhide the message by having the embedded cover (stego-cover) then the message. Matlab R2008a was used in this paper.

1- المقدمة

يهدف هذا البحث إلى المحافظة على سرية البيانات وعدم اطلاع المتطفل عليها وسهولة وصول المعلومة من المرسل إلى المستقبل من دون انتهاك أمنيتها، واحد أهم الطرائق لتحقيق أمنية المعلومات هو إخفؤ ها عن أعين المتطفلين حيث يتم إخفاء البيانات داخل بيانات أخرى (cover) بطريقة لا تثير إية شبهة أو شك يؤدي إلى كشف هذا الإخفاء[11].

في هذا البحث وقد استخدمت خوارزمية (LSB) للإخفاء لبساطتها وسهولة فهمها وتطبيقها، ويمكن استخدام أية خوارزمية أخرى للإخفاء بحسب ما يتوافق مع الغرض المستخدم له. فضلا عن تطبيق عملية XOR من اجل تجنب فقدان البيانات الموجودة في الغطاء.

واستخدمت الشبكات العصبية الاصطناعية للمساعدة في إتمام عملية الإخفاء وفك الإخفاء ولإضافة درجة اكبر من الصعوبة لفك الإخفاء من قبل المتطفلين، وقد تم استخدام الشبكتين العصبيتين (GRNN) لاحتوائهما على خاصية استرجاع البيانات بصورة صحيحة.

2- الأعمال السابقة:

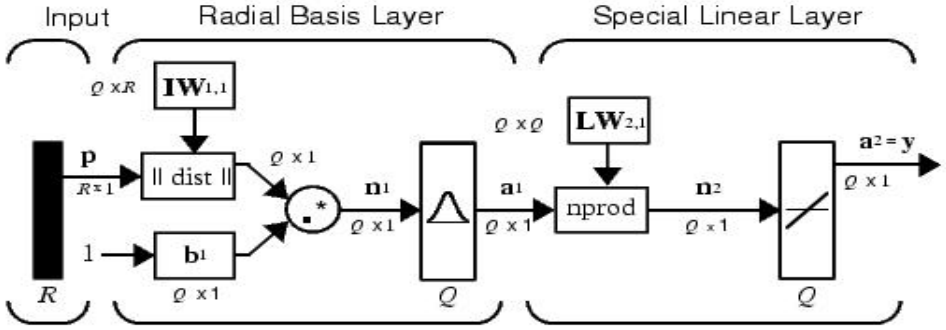
في البحث [4] أقترحت طريقة إخفاء لتضمين البيانات في الصورة الغطاء عن طريق تضمين إشارة ضوضاء ضعيفة بتوزيع احتمالي محدّد لكنه اعتباطي لتوفير المرونة للمستخدم لإبداء التشويه الناتج من التضمين كالضوضاء الناتج من أداة استملاك الصورة. وفي البحث [5] يحاول الباحثون

تمكين المرسل من إرسال البيانات المخفية من دون إشراك تغييرات التضمين في الرسالة، وكذلك اقترحوا طريقة مختلفة مستندة إلى الرموز الخطيّة العشوائية على الكتل الصغيرة بهدف تقليل عدد تغييرات التضمين. أما في البحث [10] فاقترح الباحثون طريقة إخفاء جديدة تحاول عدم إظهار أية تغييرات ناتجة من عملية التضمين بهدف جعل الإخفاء غير مرئي وذلك عن طريق إجراء تعديلات مناسبة على الإحصاءات المتأثرة بعملية التضمين.

واستخدمت في البحث [6] شبكة GRNN في عملية الكبس وفكه وقد استخدمت هذه الطريقة لان هذه التقنية تقدم ذاكرة خزنيه وبوقت اقل لنقل البيانات. أما في البحث [7] فقد اجريت عملية مقارنة فعالة لحماية الملكية عن طريق إخفاء البيانات الرقمية في القزحية لإغراض التوثيق. أما في البحث [3] فتم إجراء إخفاء واسترجاع بيانات مشفرة بطريقة LSB في صورة باعتماد شبكة RBF ولكن من دون تطبيق عملية XOR.

3- شبكة الارتداد العصبية العامة General Regression Neural Network

هي عبارة عن شبكة عصبية تستخدم في حل مسائل تقريب الوظيفة، عملية التدريب و هي مشابهة لعملية إيجاد سطح في فضاء متعدد الأبعاد، يجهز أفضل تلاؤم للبيانات المدربة.ويعني التعميم استخدام السطح المتعدد الأبعاد لتوليد بيانات الاختبار [6].و الشكل(1) يوضح التركيب العام لشبكة الارتداد العصبية العامة[8].



الشكل(1): يوضح التركيب العام لشبكة الارتداد العصبية العامة

R = تمثل عدد عناصر متجه الإدخال.

Q = تمثل عدد العصبونات في الطبقة الأولى وتمثل عدد العصبونات في الطبقة الثانية.

وتمثل أيضا عدد أزواج (الإدخال / الإخراج)

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

1- طبقة الإدخال (Input Layer): حيث يتم تطبيق الإدخالات.

2- طبقة مخفية (Hidden Layer): حيث يتم تطبيق التحويل اللاخطي على البيانات القادمة من منطقة الإدخال إلى المنطقة المخفية. وفي أغلب التطبيقات تكون المنطقة المخفية ذات بعدية عالية.

3- طبقة الإخراج الخطية(Output Layer): حيث يتم إنتاج الإخراج.

إن الطبقة الأولى لها خلايا عصبية بقدر ما هنالك من متجهات الإدخال والإخراج فيP وبشكل محدد، فإن أوزان أول طبقة هي قيم 'P وقيمة المتحيز b1 هي متجه عمودي قيم كل عناصرها 0.836/SPREAD، وممكن للمستخدم أن يختار قيمة محددة للانتشار [8] SPREAD.

كل إدخال موزون لعصبون هو المسافة بين متجه الإدخالP ومتجه الأوزان الخاص به IW1,1 ، يحسب عن طريق معادلة إيجاد المسافة الاقليدية Euclidean distance كما في المعادلة (1):

$$D = \sqrt{\sum (X - Y)^2} \qquad \cdots\cdots \qquad (1)$$

ثم يتم تطبيق عملية الضرب النقطي على هذا الإدخال الموزون للعصبون مع متجه الـ(bias) لينتج عصبون الإدخال للطبقة المخفية (n1) الذي يدخل على دالة التنشيط (radbas) لينتج إخراجا للطبقة المخفية (a1) وذلك بالاعتماد على المعادلة (2) الآتية[8]:

$$a_i^1 = radbas\ (\left\| I_i W_{1,1} - p \right\| b_i^1) \qquad \cdots\cdots \qquad (2)$$

al_i هي عنصر في a1 حيث $I_iW_{1,1}$ متجه يتكون منْ الصف i من المتجه $IW_{1,1}$. حيث a1 سيدخل على الـ (nprod) الذي يقوم بوظيفة الضرب الاعتيادي بين متجه إخراج الطبقة المخفية وبين صف من مصفوفة أوزان طبقة الإخراج الخطية لتنتج متجه(n2) يدخل على الدالة الخطية ، وذلك بالاعتماد على المعادلة (3) [8]:

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

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

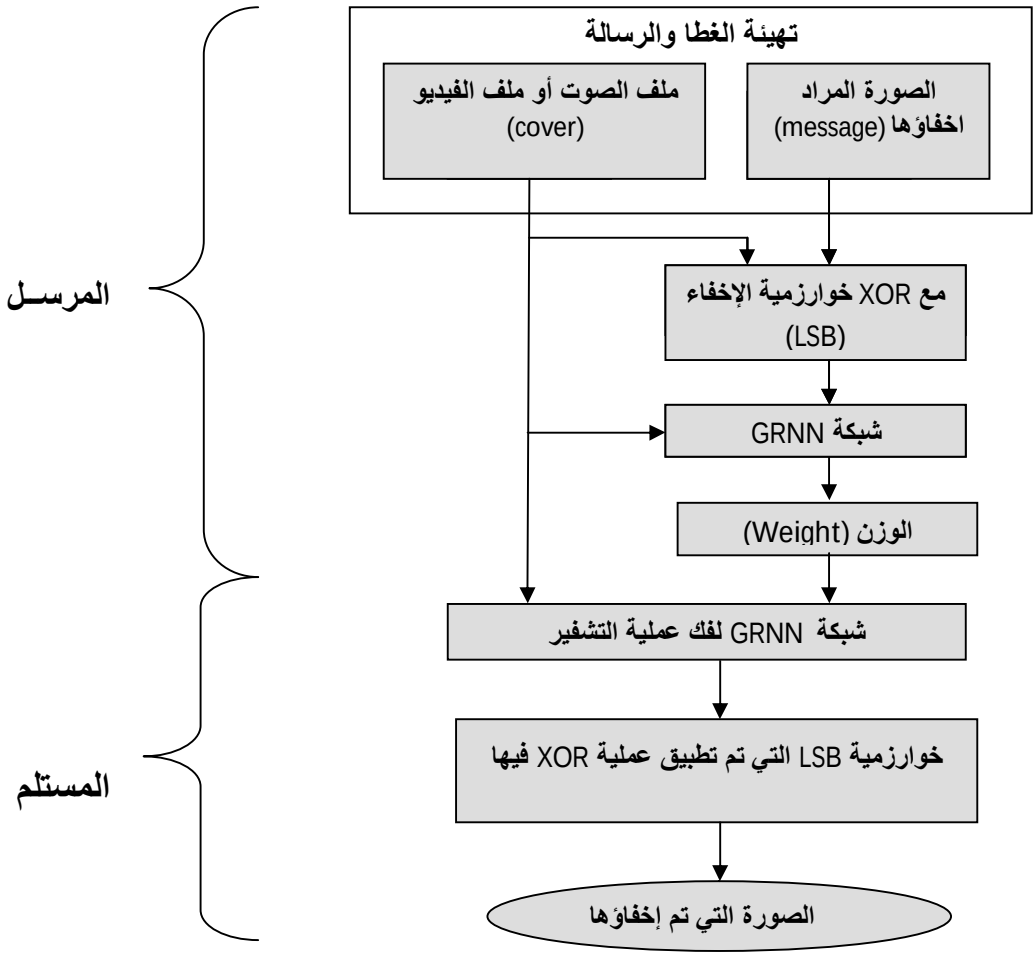
و كلما كان الانتشار كبيرا، زاد حجم المنطقة حول متجه الإدخال ، حيث إن عصبونات الطبقة الأولى ستستجيب إلى عصبونات إخراج محددة. لذلك إذا كان ألـ SPREAD صغيرا، فستكون نتائج دالة الأساس الشعاعي دقيقة جدا، لكي تكون العصبونات مع متجه الوزن القريبة إلى الإدخال تمتلك إخراجا أكبر من غيرها من العصبونات[8][9].

وبما أنه SPREAD يكون كبيرا مع الوقت، فإن مدى الشبكة سيكون أكثر نعومة وعدة عصبونات ستستجيب إلى متجه الإدخال ثم ستتصرف الشبكات وكأنها تأخذ المعدلات الموزونة بين

متجهات الـ Target التي يكون تصميم متجهات إدخالها قريبا جداً إلى متجهات الإدخال الجديدة. كبر الـ SPREAD كلما زاد عدد الNeurons المساهِمة بألـaverage وستكون النتائج التي تستخرجها دالة الشبكة العصبية أكثر نعومة[8].

مجموعة كل البيانات المتوافرة تكون مقسمة علما مجموعتين منفصلتين: مجموعة التدريب ومجموعة الاختبار. مجموعة الاختبار غير مشتركة في مرحلة التدريب للشبكات العصبية وتستخدم في تقييم اداء النماذج. إن ترتيب نماذج الشبكة العصبية يتم تحديده حسب طبيعة المشكلة المطلوب حلها[6].

4- المخطط الصندوقي للطريقة المقترحة تم توضيحها في الشكل (2).



الشكل(2): يوضح المخطط الصندوقي للخوارزمية المقترحة

5- تهيئة الغطاء والرسالة :

5-1- تهيئة الغطاء (الملف الصوتي أو ملف الفيديو) (cover):

هذا النظام سوف يستخدم نوعين من الغطاء: ملف صوتي من نوع WAV، وهي نوعية شائعة الاستخدام وقد يكون هذا النوع من ملفات الصوت مكبوسا أو غير مكبوس، ألا أن حجمه يكون كبيرا حتى في حالة كونه مكبوساً، حيث يوفر هذا الملف (نسب تعيان مختلفة، عددا مختلفاً من القنوات (Channel)، إتباع عدد من خوارزميات الكبس المختلفة)[2].

أما بالنسبة للنوع الثاني من الغطاء فهو ملف فيديو، ملف الفيديو المستخدم هو من نوع AVI ، و ان نوع الكبس المستخدم هو Cinepak لأنها توفر سرعة عالية في تشغيل الفيديو[1].

5-2- تهيئة الصورة المراد إخفؤ ها (message) :

يفضل ان تكون الصورة المراد إخفؤ ها (message) صورة ملونة ويفضل أن يكون حجمها ربع حجم الغطاء (cover) أو اقل، لأنه إذا كان حجم الصورة المراد إخفؤ ها (message) أكبر من ربع حجم (cover) فعندها سوف تكون نسبة التشوه اكبر إذ يتعين عند ذلك إخفاء أكثر من 2bits في كل byte من الغطاء، لذلك سيتم اختيار الصورة المراد إخفؤ ها بحيث تكون ربع حجم بيانات الملف الصوتي (cover) أو اقل ونقوم بتوزيع bits الصورة داخل مصفوفة صفرية تكون عبارة عن متجه طوله بطول الملف الصوتي (cover) وتكون عملية توزيع ألـ bits عند المرسل وقبل القيام بعملية الإخفاء ثم يعاد تجميع هذه ألـ bits عند المستلم بعد فك الإخفاء. وكذلك الحال عند الإخفاء في الفيديو مع ملاحظة إن الإخفاء في الفيديو يكون لأطر معينة. وقد استخدمت في هذا البحث صور من نوع bmp كـ (message) ويمكن استخدام أي نوع من أنواع الصور ايضا على شرط الحصول على القيم اللونية بأية صيغة كانت.

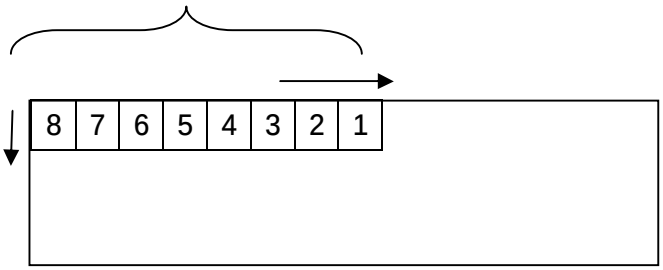
6-1- الطريقة المعتمدة عند المرسل:

هناك عدة خطوات يجب إتباعها عند المرسل.

6-2- تهيئة الصورة المراد إخفؤ ها عند المرسل:-

إن الغطاء المستخدم يمكن أن يكون ملف صوت أو فيديو. عندما يكون الغطاء ملف صوت عندها يقوم النظام بتكوين مصفوفة صفرية ذات بُعد واحد، أي أبعادها بنفس أبعاد الملف الصوتي (cover) وتوزيع ألـ (bits) للصورة ألـ(message) على هذه المصفوفة الصفرية، بحيث أن كل (2bits) من الصورة يتم إخفؤ ها داخل (8bits) من المصفوفة الصفرية، ومن ثم سيتم توزيع كل (byte) من الصورة

على (4bytes) من ملف الغطاء الصوتي. وعملية توزيع bits الصورة المراد إخفاؤ ها داخل المصفوفة الصفرية يكون بالشكل(3) الاتية:



((3)-أ) الصورة (message)

0	0	0	0	0	0	2	1	0	0	0	0	0	0	4	3	0	0	0	0	0	0	6	5	0	0	0	0	0	0	8	7	0	0	0	0	0		2	1	0	0	0

((3)-ب) المصفوفة الصفرية

الشكل(3) : عملية توزيع bits

أما إذا كان الغطاء هو ملف فيديو عندها إذا كان حجم الصورة المراد إخفاؤ ها (message) اكبر من ربع حجم الإطار(frame) فعندها سوف توزع الصورة على أكثر من إطار، لذلك سوف نختار الصورة (message) بحيث تكون ربع حجم الإطار(frame) ويتم توزيع bits الصورة (message) داخل مصفوفة صفرية تكون عبارة عن مصفوفة ثنائية بنفس إبعاد حجم الإطار(frame)، وتكون عملية توزيع bits عند المرسل وقبل القيام بعملية الإخفاء ثم يعاد تجميع هذه bits عند المستلم بعد فك الإخفاء.

6-5- الأسلوب المعتمد في إخفاء البيانات:

الخوارزمية المستخدمة بعملية الإخفاء في هذا النظام هي خوارزمية البت الأقل أهمية، طريقة عمل خوارزمية (LSB) هي أن يتم التعامل مع كل (byte) من الصورة (cover). وذلك بتطبيق عملية الـ (XOR) بين آخر (2bit) من كل byte من الصورة (cover) والمصفوفة الصفرية.

6-6- طريقة عمل شبكة GRNN عند المرسل:

الإدخال لشبكة GRNN هو الغطاء (cover)، والهدف(target) لشبكة GRNN هو الغطاء المضمن (stego-cover)، سوف يتم إجراء عملية التدريب ومن ثم الحصول على الوزن النهائي، عندها سوف يرسل الوزن مع الغطاء(cover) إلى الطرف الثاني (المستلم) لاستخدامه في عملية

استرجاع الصورة التي تم إخفاؤها. وان هذه الشبكة تتكون من طبقتين، الطبقة الخفية(hidden layer) وطبقة الإخراج.

6-7- **الأوزان** (Weights):

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.

7-1- **الطريقة المتبعة عند المستلم**: هناك عدة خطوات يجب إتباعها عند المستلم.

7-2- **طريقة عمل شبكة** GRNN **عند المستلم**:

بعد تسلم الوزن (weight) و(cover) من المرسل، تقوم شبكة GRNN باستخراج الغطاء المضمن (stego-cover)، الذي نستخرج منه الصورة المخفية.

هذه المرحلة تعتبر عملية فك التشفير، وذلك لان الأوزان 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 GRNN بتسلم الوزن الذي يعتبر تشفير واستخراج الغطاء المضمن (stego-cover)، آي عملية فك التشفير وإرسال الغطاء المضمن إلى خوارزمية LSB.

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

7-3- **عملية فك الإخفاء عند المستلم (التحليل)**:

يقوم النظام بتطبيق عملية ألـ (XOR) بين الغطاء والغطاء المضمن(stego-cover) فينتج المصفوفة الصفرية التي تحتوي في أول 2bits من كل byte فيها على bits الصورة المرسلة. ومن ثم القيام بعملية تجميع الـ bits التي تم نشرها داخل المصفوفة الصفرية مسبقاً(عند المرسل) لاستخراج الصورة المخفية message.

8- **النتائج العملية**:

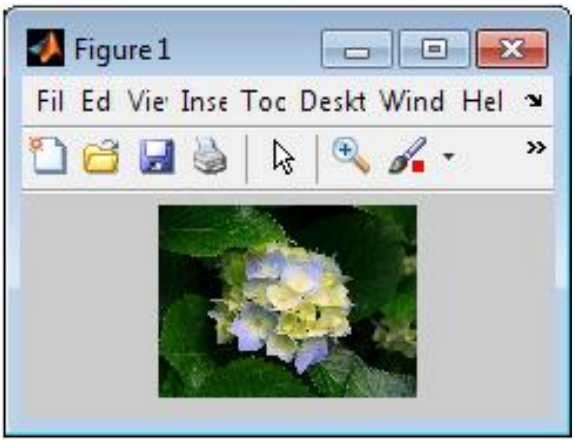
أ- تهيئة ملف صوتي من نوع (wav.) أو ملف فيديو من نوع (avi.) يمثل ملف الغطاء الذي سوف يتم إخفاء الصورة داخله.

ب- الصورة المراد اخفاؤها (message)، التي تمت تهيئتها لإخفائها داخل الملف الغطاء (cover)، كما هو موضح في الشكل(4).

الشكل (4): الصورة (message)

جـ- بعد إجراء عملية الإخفاء سوف يتم الحصول على ملف الغطاء (cover) وبداخله الصورة (message)، وتدعى الغطاء المضمن (stego-cover). بعد هذه العملية يتم خزن الأوزان الناتجة من (stego-cover) لاستخدامها في عملية التحليل.

د- بعدها يتم فك عملية الإخفاء عند المستلم، ليتم الحصول على الغطاء المضمن ومن ثم الحصول على الصورة الأصلية (message) التي تم اخفاؤها سابقاً داخل ملف الغطاء (cover)، كما هو موضح في الشكل(5).



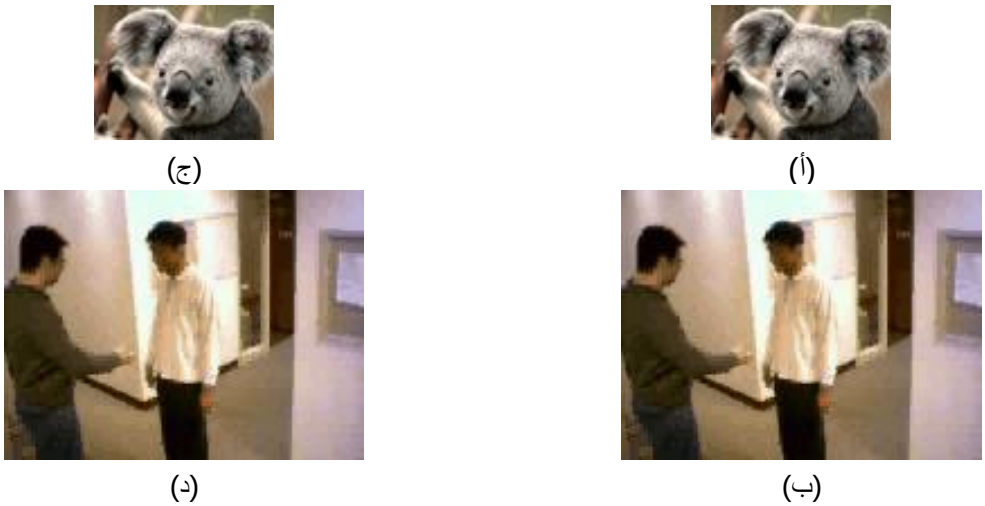
الشكل(5): الصورة (message) بعد عملية فك الإخفاء

يجب ملاحظة إن 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 الوزن (Weight) عبر قنوات مغطاة دون معرفة المتطفلين. وعندها سوف يقوم المستلم عن طريق (Cover) الذي سبق أن استلمه مع الوزن الذي سوف يتم الحصول عليه مؤخراً بفك الإخفاء والحصول على (stego-cover) ومن ثم الحصول على (message). ومن الجدير بالذكر انه يمكن إرسال (Cover) بقناة عادية و(Weight) بقناة مغطاة إذا رغب المرسل في. يجب ملاحظة ان عدد الإدخالات بعدد اسطر (Cover)، وعدد الاخراجات بعدد اسطر (stego-cover).

عدد أزواج التدريب لشبكة GRNN هي بعدد أعمدة (Cover) و(stego-cover)، ويجب أن يكونا متساويين.

فائدة استخدام (stego-cover) قريبة من (Cover) بحيث لا يمكن اكتشاف إن فيها بيانات مخفية بالعين المجردة مما يصعب على المتطفل اكتشاف البيانات المخفية حتى في حالة حصوله على (Cover) والأوزان.فضلا انه يفضل استخدام صورة كثيرة التفاصيل بالنسبة (Cover)، بحيث لا يكون فيها أي عمودين متشابهين. والشكل (6) يستعرض مثالاً لصورة (message) وفيديو (Cover) قبل وبعده الإخفاء.



(أ) (ج)

(ب) (د)

الشكل(6): مثال لإخفاء صورة في فيديو. أ. الصورة (message) قبل الإخفاء. ب. لقطة من الفيديو (Cover) قبل الإخفاء. ج. (أ) بعد الإخفاء. د. (ب) بعد الإخفاء.

8- مناقشة النتائج:

تم إيجاد نتائج (PSNR) لـ(25) مثال للصوت كغطاء و(10) أمثلة للفيديو وتم حساب (Mean Square Error (MSE)) وكانت النتيجة انه تم استرجاع جميع البيانات المشفرة بفقدان قليل، والجدول

(1) يستعرض متوسط PSNR وMSE للطريقة المقترحة في هذا البحث والبحث [3] من أجل المقارنة.

هذه الطريقة تتضمن مستويين من الحماية، المستوى الأول يمثل إخفاء الرسالة في الغطاء لتكوين ملف غطاء مضمن (stego-cover)،و المستوى الثاني يمثل تشفير الغطاء المضمن باستخدام الشبكة العصبية (GRNN) باعتبارها هي الهدف (target) والملف الغطاء هو الإدخال إلى الشبكة، عندها يتم تكوين أوزان تمثل البيانات المشفرة، التي تستخدم فيما بعد عند المستلم مع الغطاء لإيجاد البيانات الأصلية.

الجدول (1): مقارنة نتائج الطريقة المقترحة في هذا البحث مع البحث [3].

نوع الغطاء	الطريقة المقترحة في هذا البحث		البحث [3]	
	MSE	PSNR	MSE	PSNR
الصوت غطاءً	0.0738	8.81E+05	0.0894	7.27E+05
الفيديو غطاءً	0.1343	4.84E+05	0.1398	4.65E+05

9- الاستنتاجات:

1. يمكن إخفاء بيانات حجمها ربع حجم الغطاء (cover) دون ملاحظة تغيرات تذكر في ألوان الغطاء.
2. عند استرجاع الرسالة (message) تسترجع بفقدان قليل للبيانات.
3. تزداد التشوهات في الصورة المسترجعة بزيادة حجم الصورة وتعدد ألوانها.
4. يجب إرسال أوزان الشبكة عبر قنوات مغطاة (covert channels) لضمان وصولها إلى المستلم من دون علم المهاجمين (attackers).
5. عملية الإخفاء والاسترجاع سريعة نسبياً على الرغم من وجود عملية تدريب الشبكة العصبية في مرحلة الإخفاء.
6. استخدام الشبكات العصبية أعطى أمنية عالية في الإخفاء.

10- المصادر

1. ثابت، نادية معن، (2002)، "محرر فيديو الـ AVI "، رسالة ماجستير، جامعة الموصل، قسم علوم الحاسوب، كلية علوم الحاسوب والرياضيات.

2. قدّو، سجى جاسم، (2004)، "كبس الصوت بواسطة استخلاص الخواص"، رسالة ماجستير، جامعة الموصل، قسم علوم الحاسوب، كلية علوم الحاسوب والرياضيات.
3. 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، المجلد 7، العدد3. ص199-ص208.
4. Fridrich Jessica, M. Goljan, (2003), "Digital Image Steganography Using Stochastic Modulation", Proc. SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents V, vol. 5020, Santa Clara, California, pp. 191-202.
5. Fridrich Jessica, M. Goljan and D. Soukal, (2005) "Steganography via Codes for Memory with Defective Cells", 43rd Conference on Coding, Communication, and Control, Sep 28-30.
6. H. Dr. Safwan Omer, M. Susan Hassan, (2010), "General Regression Neural Network Application for Dynamic data Compression and Decompression", University of Mosul, Al-Rafidain journal of computer sciences and mathematics, vol7, no.3.
7. Hassanien, Aboul Ella, Ajith Abraham, Crina Grosan, (2008), "Spiking neural network and wavelets for hiding iris data in digital images", © Springer-Verlag.
8. Howared D., Mark B., (2010),"Neural Network toolbox user's", the mathworks.
9. Huang J. Shimizu A. (2002), "Robust Face Detection Using A Modified Radial Basis Function Network", IEICE Trans. ,Inf. & Syst. Vol E85-D,No 10.
10. K. Solanki, K. Sullivan, U. Madhow, B. S. Manjunath, and S. Chandrasekaran, (2006), " Provably Secure Steganography: Achieving

Zero K-L Divergence Using Statistical Restoration", in Proceedings of ICIP.

11. L. Y. Por, T. F. Ang, B. Delina, (2008), "WhiteSteg: A New Scheme in Information Hiding Using Text Steganography", Computer Science and Information Technology, University of Malaya.no.6, Volume 7, p735-p745.
ww.w.softcomputing.net/abo-sc.pdf.