# Encrypted Data Hiding & Retrieval of an Image using LSB Based on RBF Network

Amera Istiqlal Badran
amera_istiqlal@uomosul.edu.iq
College of Computer Science and Mathematics
University of Mosul

Abdulsattar M. Khidhir
abdulsattarmk@ntu.edu.iq
Northern Technical University

laheeb Mohammed Ibrahim
Laheeb_alzubaidy@yahoo.com
College of Computer Science and Mathematics
University of Mosul

Received on:2010/9/15 Accepted on:2010/11/10

## ABSTRACT

In this paper an image is hidden in another image using one of the hiding algorithms (Least Significant Bit) to produce the stego-cover image which used as an input with the cover to Radial basis function Network 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 include 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. This Network 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. The recipient can use RBF Network to unhide the message by having the stego-cover image then the message.

Matlab R2008a was used in this paper.

**Keywords:** Encryption, LSB algorithm , RBF Network.

## عملية إخفاء واسترجاع بيانات مشفرة بطريقة LSB في صورة باعتماد شبكة RBF

عامرة استقلال بدران
كلية علوم الحاسوب والرياضيات
جامعة الموصل

عبد الستار محمد خضر
الجامعة التقنية الش مالية

لهيب محمد إبراهيم
كلية علوم الحاسوب والرياضيات
جامعة الموصل

تاريخ استلام البحث:٢٠١٠/9/15 تاريخ قبول البحث:٢٠١٠/١١/10

## الملخص

في هذا البحث تم إخفاء صورة داخل صورة أخرى باستخدام إحدى خوارزميات الإخفاء وهي (Least Significant Bit (LSB)) لإنتاج الصورة (stego_cover)، التي تدخل مع الغطاء (cover) على شبكة دالة الأساس ألشعاعي (Radial Basis Function Network (RBF))لاستخراج الوزن.

يتم إرسال الغطاء لمرة واحدة إلى المستلم ويمكن أن يحتفظ به لعدد غير محدود من الرسائل (messages). ولكل رسالة يتم إخفاءها سوف يتم إرسال الوزن (weight) فقط، والذي يرسل كمفتاح إلى المستلم, عندها يقوم المستلم باستخدام الغطاء مع الوزن الذي استلمه لفك الإخفاء، وبذلك فأن 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) باعتبارها هي الهدف (target) والصورة الغطاء هي الإدخال إلى الشبكة، عندها يتم تكوين أوزان والتي تمثل البيانات المشفرة. وبعد ذلك بإمكان المستلم عن طريق شبكة (RBF) من فك الإخفاء والحصول على الصورة المضمنة (stego-cover) ومن ثم الحصول على الرسالة.

ولقد تم استخدام لغة (Matlab R2008a) لانجاز هذا البحث.

**الكلمات المفتاحية:** تشفير، خوارزمية LSB، شبكة RBF.

## 1- المقدمة:

يهدف هذا البحث إلى المحافظة على سرية البيانات وعدم اطلاع المتطفل عليها وسهولة وصول المعلومة من المرسل إلى المستقبل بدون انتهاك أمنيتها, واحد أهم الطرائق لتحقيق أمنية المعلومات هو إخفاءها عن أعين المتطفلين حيث يتم إخفاء البيانات داخل بيانات أخرى (cover) بطريقة لا تثير إي شبهة أو شك يؤدي إلى كشف هذا الإخفاء[1][2] .

تم استخدام الشبكات العصبية الاصطناعية للمساعدة في إتمام عملية الإخفاء وفك الإخفاء ولإضافة درجة اكبر من الصعوبة لفك الإخفاء من قبل المتطفلين، وقد تم استخدام الشبكة العصبية (RBF) لاحتوائها على خاصية استرجاع البيانات بصورة صحيحة.

## 2- الأعمال السابقة:

في البحث[3] تم أجراء عملية أخفاء للبيانات بدون تضمين البيانات وذلك عن طريق تدريب شبكة عصبية على إيجاد البيانات المخفية من خصائص مختارة من الصورة الغطاء بعد تحويلها إلى مجال الألوان (Ycbcr). أما في البحث [4] تم استخدام طريقة سريعة للعلامة المائية الرقمية السمعية بالاعتماد على شبكة Counter-Propagation العصبية. أما في البحث [5] تم كشف البيانات باستخدام معاملات Wavelet لصورة متضمنة للبيانات (stego-cover) وتدريب الشبكة العصبية عليها.

### 3-1- شبكة دالة الأساس الشعاعي(Radial Basis Function Network)

وتعد أكثر الشبكات استخداماً وهي أيضاً شبكة ذات تغذية أمامية لكن بطبقة مخفية واحدة. و(RBF) هي شبكة بطبقتين، لا تتم في طبقة الإدخال أية معالجة ثم الطبقة المخفية حيث تتم فيها المعالجة والطبقة الأخيرة حيث ينجز مجموع موزون مع إخراج خطي. وحدات إخراج شبكة RBF تشكل تركيب خطي لدوال أساسية احتسبت بواسطة الوحدات المخفية[6] .

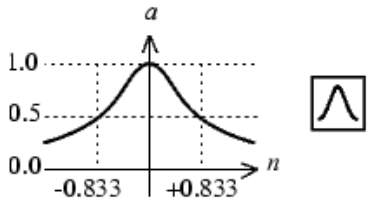
الدوال الأساسية في الطبقة المخفية تنتج استجابة محصورة في منطقة محددة للإدخال وهذه المنطقة لها مركز. وهذه الاستجابة تعد قيم إدخال خاصة ولها أعلى قيمة إخراج، وقيمة الإخراج هذه تصبح بمثابة قيم الإدخال وتنطلق من هذه النقطة[7].

الدالة الأساسية نشير إليها كدالة 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[8].

تأخذ الدالة شكل الجرس (bell shape) ، يعد التوزيع الطبيعي من التوزيعات المهمة والأكثر استخداماً لان معظم الصفات البيولوجية والاجتماعية وغيرها من الصفات المهمة يكون توزيعها مشابهاً للتوزيع الطبيعي أو مقارباً له وكذلك سهولة اختبار التوزيع وإمكانية تحويل توزيعات كثيرة إلى التوزيع الطبيعي. وهذه الدالة لها أعلى قيمة في نقطة المركز ثم تتناقص باتجاه الخارج[9][10]. دالة التنشيط لشبكة RBF هي (radial basis)، وكما موضح في المعادلة التالية[11]:

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

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 إخراج مطابق للمدخلات بمسافة متساوية عن مركز كاوس وهذا ما يدعى بـ Radial basis [6][7]. والشكل رقم (1) يوضح فيه دالة التنشيط (radbas) [11].




**الشكل(1): يوضح فيه دالة التنشيط**

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 شبكات RBF يمكن أن تكون متعددة المخرجات.

تحل شبكات RBF كثيراً من المشاكل وهي مفيدة للاستخدام في المسائل الآتية:

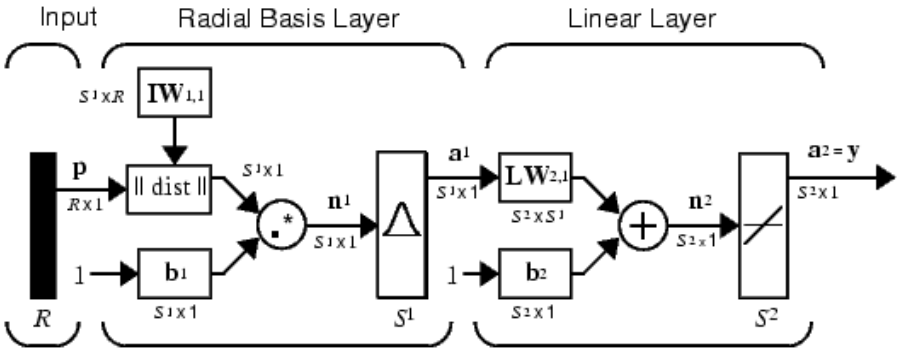
أ- التقريب الدالي Function Approximation.

ب- التصنيف Classification.

ج- موديلات الأنظمة الديناميكية والسلاسل الزمنية[6].

**3-2-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. كما هو موضح في الشكل رقم(2).




**الشكل(2): يوضح فيه عمل شبكة RBF**

R:عدد العناصر في عمود الإدخال.

$S^1$:عدد العصبونات في الطبقة الأولى.

$S^2$:عدد العصبونات في الطبقة الثانية.

P: مصفوفة الإدخال.

$IW^{1,1}$: مصفوفة الوزن للطبقة المخفية.

$b^1,b^2$: مصفوفة الـ basis.

$LW^{2,1}$: مصفوفة الوزن لطبقة الاخراج.

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[6].

العقد في الطبقة المخفية تنفذ بواسطة الدالة الأساسية التي تعمل على منطقة محصورة من حيز الإدخال. وذلك باعتماد المعادلة الآتية[11]:

$$a_i^1 = radbas(\|IW_{1,1}^i - p\| b_i^1) \quad \ldots(2)$$

ومن ثم العقد في طبقة الإخراج تنفذ بواسطة الدالة الخطية التي تعمل على منطقة محصورة من حيز الإخراج. وذلك باعتماد المعادلة الآتية[11]:-

$$a_2 = purelin(LW_{2,1}a_1 + b_2) \quad \ldots(3)$$

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 +6[1].

في هذا النظام توجد لدينا صورتين الصورة الغطاء و message:-

**4-الصورة الغطاء (cover):**

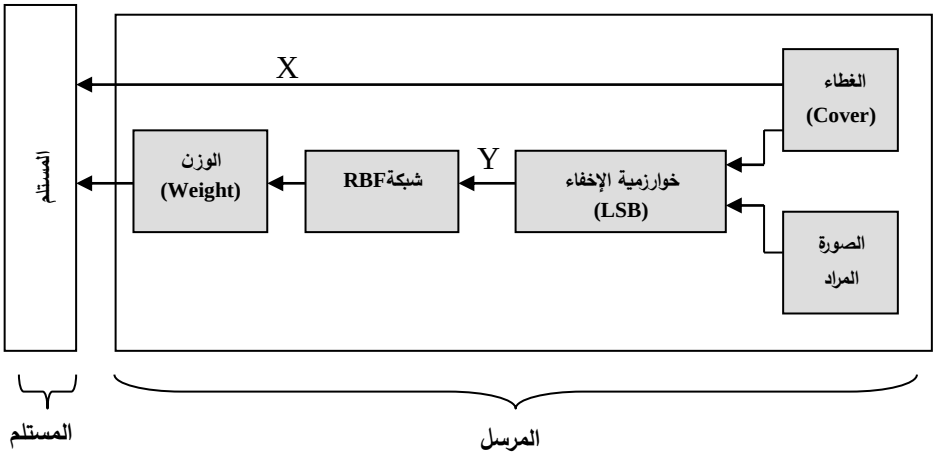
في هذا البحث تم استخدام صورة ملونة تتكون من ثلاث طبقات (R,G,B)، ممكن إن تكون الصورة المستخدمة من نوع (bmp) أو (jpg)، لكن يجب إن تكون عند خزنها من نوع بدون فقدان مثل (bmp) وليس من النوع الذي فيه كبس بفقدان (Lossy Compression) مثل(jpg) [1].

**5- الصورة المراد إخفاءها (message):**

الصورة المراد إخفاءها (message) يفضل إن تكون صورة ملونة من نوع (bmp) ويفضل إن يكون حجمها ربع حجم الصورة الغطاء (cover)، لأنه إذا كان حجم الصورة المراد إخفاءها (message) اكبر من ربع حجم (cover) فعندها سوف تكون نسبة التشوه اكبر، لذلك سوف نختار الصورة (message) بحيث تكون ربع حجم الصورة (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.

**6- الطريقة المعتمدة عند المرسل :**

هناك عدة خطوات يجب إتباعها عند المرسل، وكما هو موضح في الشكل (3).

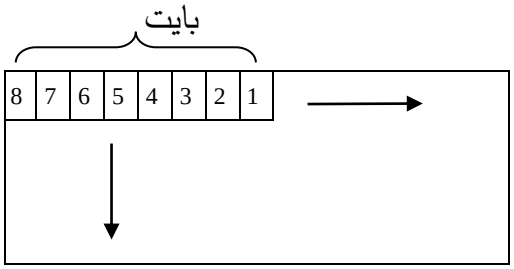



**الشكل (3): مخطط خوارزمية الإخفاء**

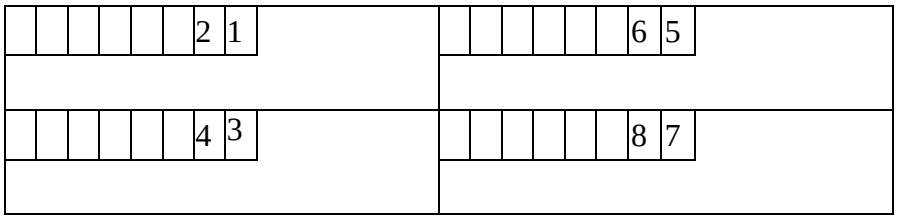
**6-1- تهيئة الصورة عند المرسل:**

يقوم النظام بتكوين مصفوفة صفرية إبعادها بنفس إبعاد الصورة الغطاء(cover) وتوزيع (bits) للصورة (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 إخفاءها داخل (8 bits) من المصفوفة الصفرية.

يتم توزيع الصورة المراد إخفاءها (message) على المصفوفة الصفرية، بحيث يتم توزيع bits كل (byte) من الصورة المراد إخفاءها (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، وكما هو موضح في الشكل (4).




**الشكل(4-أ): الصورة message**




**الشكل(4-ب): المصفوفة الصفرية**

**الشكل(4):عملية توزيع الـ bits**

**6-2- 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 بتصفير أقل (2bit) في أول (byte) من الصورة والتي تدعى (LSB) [1][2].

ثم يتم دمج المصفوفة الصفرية الموزع فيها الصورة المراد إخفاءها (message) مع الصورة الأصلية (cover) بعد تصفير آخر (2bits) من كل (byte) لإنتاج (stego-cover).

في هذا البحث تم استخدام خوارزمية (LSB) للإخفاء لبساطتها وسهولة فهمها وتطبيقها، ويمكن استخدام أية خوارزمية أخرى للإخفاء بحسب ما يتوافق مع الغرض المستخدم له.

**6-3- طريقة عمل شبكة RBF عند المرسل:**

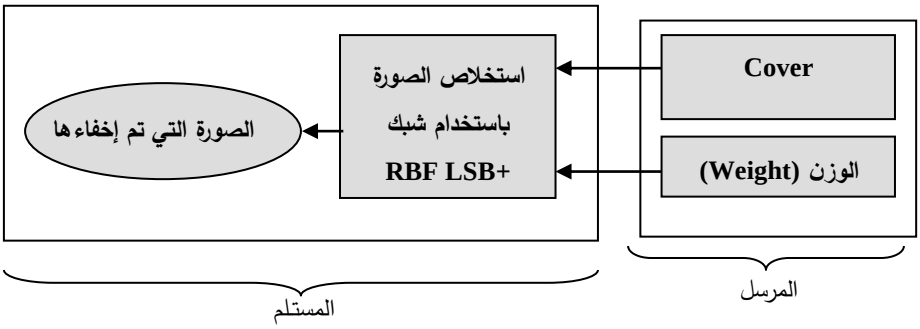
المدخل الأول لشبكة RBF هو الصورة الغطاء (cover) والذي يعتبر (X)، والمدخل الثاني لشبكة RBF هو (stego-cover) والذي يعتبر(Y)، سوف يدخل (X) و(Y) على شبكة RBF لإنتاج الوزن (التدريب) وذلك بالاعتماد على المعادلتين على التوالي (2) و(3)، ويتم إرسال الوزن و(cover) إلى الطرف الثاني (المستلم) لاستخدامه في استخراج الصورة (stego-cover).

**6-4- الأوزان (Weights):**

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

**7- الطريقة المتبعة عند المستلم :**

هناك عدة خطوات يجب إتباعها عند المستلم، وكما هو موضح في الشكل (5).




**شكل(5): مخطط خوارزمية فك الإخفاء**

**7-1- طريقة عمل شبكة RBF عند المستلم:**

بعد استلام الوزن (weight) والصورة (cover) من المرسل، تقوم شبكة RBF باستخلاص الصورة المخفية وذلك بالاعتماد على المعادلتين على التوالي (2)و(3)، وذلك لاستخراج الصورة (cover) من الشبكة.

**7-2- عملية فك الإخفاء عند المستلم (التحليل):**

عند إجراء عملية فك الإخفاء يتم طرح الصورة (stego-cover) من الصورة (cover) لإنتاج الصورة (message)، ثم يعاد تجميع التوزيع للصورة الناتجة من عملية الطرح.

**8- النتائج العملية:**

أ- الصورة الغطاء (cover) التي تم تهيئتها لإخفاء الصورة (message) داخلها، كما هو موضح في الشكل(6).

**الشكل (6): الصورة الغطاء(cover)**

ب- الصورة المراد إخفاءها (message)، التي تم تهيئتها لإخفائها داخل الصورة الغطاء (cover)، كما هو موضح في الشكل(7).

**الشكل (7): الصورة (message)**

جـ- بعد إجراء عملية الإخفاء سوف يتم الحصول على الصورة الغطاء (cover) وبداخلها الصورة (message)، وتدعى (stego-cover) كما هو موضح في الشكل (8).

**الشكل (8): نافذة الصورة (cover) مع الصورة (message) بعد عملية الإخفاء (stego-cover)**

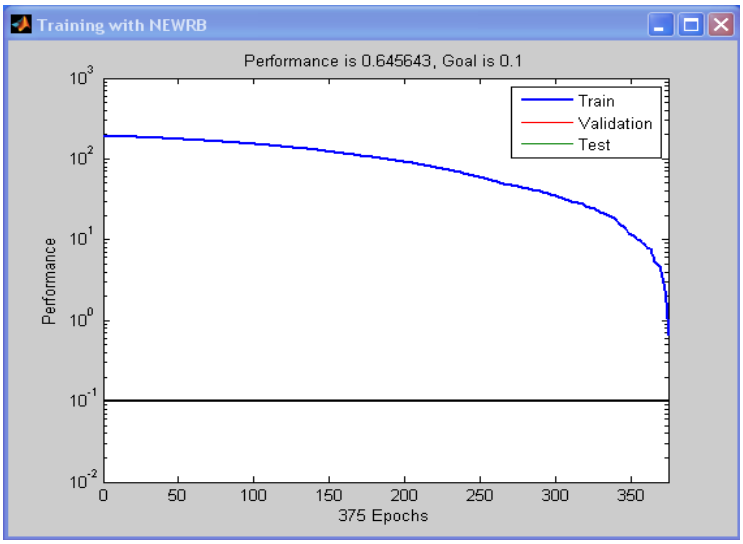
د- خزن الوزن (weight) الناتج من (stego-cover).

هـ- بعدها يتم فك عملية الإخفاء, ليتم الحصول على الصورة (message) الأصلية فقط التي تم إخفاءها سابقاً داخل الصورة الغطاء (cover)، كما هو موضح في الشكل(9).

**الشكل(9): الصورة (message) بعد عملية فك الإخفاء**

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 الوزن (Weight) عبر قنوات مغطاة بدون معرفة المتطفلين. وعندها سوف يقوم المستلم عن طريق (Cover) الثابت الذي سبق ان 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 ارسال (Cover) بقناة عادية و(Weight) بقناة مغطاة إذا رغب المرسل بذلك.

ويجب ملاحظة انه عدد الإدخالات بعدد اسطر (Cover)، وعدد الاخراجات بعدد اسطر (stego-cover). عدد أزواج التدريب لشبكة RBF هي بعدد أعمدة (Cover) و(stego-cover)، ويجب ان يكونا متساويين، الشكل رقم (10) يوضح فيه عملية التدريب لشبكة RBF.




**الشكل(10): يوضح عملية التدريب لشبكة RBF**

فائدة استخدام (stego-cover) قريبة من (Cover) بحيث لا يمكن اكتشاف ان فيها بيانات مخفية بالعين المجردة بحيث يصعب على المتطفل اكتشاف البيانات المخفية حتى في حالة حصوله على (Cover) والأوزان. بالإضافة إلى انه يفضل استخدام صورة كثيرة التفاصيل بالنسبة (Cover)، بحيث لا يكون فيها أي عمودين متشابهين.

**9- مناقشة النتائج:**

تم إيجاد نتائج (PSNR) لـ(50) مثال وتم حساب(Mean Square Error (MSE)) وكانت النتيجة انه تم استرجاع جميع البيانات المشفرة بدون فقدان.

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) باعتبارها هي الهدف (target) والصورة الغطاء هي الإدخال إلى الشبكة, عندها يتم تكوين أوزان والتي تمثل البيانات المشفرة، التي تستخدم فيما بعد عند المستلم مع الغطاء لإيجاد البيانات الأصلية.

**10- الاستنتاجات:**

أ- يمكن إخفاء حجم كبير من البيانات دون التأثير على ألوان الغطاء.

ب- عند استرجاع الرسالة (message) تسترجع بدون فقدان.

ج- استخدام الشبكات العصبية أعطت أمنية عالية في الإخفاء .

***المصادر***


[1]. برزنجي, فوزي, (2008)، "إخفاء البيانات داخل الصورة"، جامعة السليمانية، العراق.
WWW.boosla.com .

[2]. A., Muhalim M., (2003), "Information Hiding Using Steganography", University Technology Malaysia.

[3]. K. Naoe, Takefuji, (2008), "Damage less Information Hiding using Neural network on Ycbcr Domain", IJCSNS, Vol 8 No. 9, September.

[4]. 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.

[5]. D. Jennifer, B. Clifford, (2005), "An Artificial Neural Network for Wavelet Steganalysis", Lowa State University, Ames Iowa, 50011.

[6] . حسن، سوزان، (2007)، "استخدام الشبكتين العصبيتين الاصطناعيتين شبيهة نيوتن ودالة الأساس ألشعاعي في تشخيص مرض خلع الورك الولادي"، جامعة تكريت.

[7]. Patterson D. (1996), "Artificial Networks", Singapore, Prentice Hall.

[8]. الراوي، د.خاشع محمود (1984)، "المدخل إلى الإحصاء"، مطابع جامعة الموصل.

[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]. Pao, Y.H., (1998), "Adaptive Pattern Recognition And Neural Networks", Wesley Publishing Company, Inc. New York.

[11]. Howared D., Mark B., (2008), "Neural Network toolbox user's", The mathworks.