إخفاء الصور باستخدام الطرق الذكائية

شهلة حازم احمد خروفة

قسم العلوم الأساسية ، كلية طب الأسنان ، جامعة الموصل ، الموصل ، العراق

(تاريخ الاستلام: 2 / 9 /2010 ---- تاريخ القبول: 27 / 9 /2011)

الملخص

الإخفاء وسيلة قديمة، ظل يستخدمها الإنسان كلما أراد ألا يصل ما يخفيه أيدي الاخرين أو أعينهم، ولقد تطور هذا الأسلوب إلى علم وفن راقيين، غير أن العلم الحديث يزيد كل يوم من تعقيد عملية الإخفاء. إن حماية البيانات تمثل أول حقل من حقول تقنية المعلومات، وا ِخفاء المعلومات يمثل نوع من المعالجة يستخدم لإخفاء البيانات (نص، صورة، صوت) في صيغ متعددة من الأوساط مثل نص، صورة، صوت، أما عملية التحقق من وجود الإخفاء فيتم من خلال تحليل الحاملات المشكوك فيها أو تخمين المعلومات المخفية المحتمل وجودها عن طريق ملاحظة البيانات المتولدة أو بالاعتماد على خوارزميات الإخفاء.

في هذا البحث تم اقتراح طريقتين لإخفاء الصور ذات التدرج الرمادي، في الطريقة الأولى تم استخدام صورتين: الصورة الأولى استخدمت للتضمين والصورة الثانية استخدمت كغطاء ليتم الحصول وسط الستيكو. أما الطريقة الثانية فقد تم اقتراح طريقة لإخفاء الصورة الأصلية (المدخلة) والحصول على وسط الستيكو. تم في الطريقتين استخدام طريقة جيدة و ذكية لتحديد قيمة المفتاح باستخدام الشبكات العصبية الاصطناعية كما تم استخدام شبكة Generalized Regression Neural Network(GRNN)لتحديد قيمة المفتاح نظراً لما تتميز به الشبكات العصبية من إعطاء طريقة مناسبة لتمثيل العلاقات بين معطيات المسألة المطلوب حلها بشكل مختلف تماماً عن الطرق المتبعة في البرمجة التقليدية. تم عمل برنامج بلغة Matlab (Version 6.5) لتنفيذ العمل.

المقدمة:

يعرف أمن المعلومات بأنه العلم الذي يبحث في نظريات وستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها ومن زاوية تقنية، هو الوسائل والأدوات والإجراءات اللازم توفرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية. أن الأهداف الرئيسية لحماية المعلومات هي: منع تسرب أو سرقة أو تزوير المعلومات،ومنع الأعمال غير الشرعية لتدمير أو تشويه المعلومات، وحماية الحقوق الشرعية للمواطنين للمحافظة على الأسرار الشخصية وسرية المعلومات الشخصية للفرد [1]. أما إخفاء المعلومات فيعني إخفاء المعلومات في معلومات أخرى بريئة المظهر ولا تجلب الانتباه، وتعتمد في تنفيذها على الغريزة في توظيف التقنية قبل المنطق الرياضي[1]. الشيء المهم في هذه التقنية أنها غير ملفتة للنظر إضافة إلى مرونتها في استخدام كافة الوسائط لغرض الإخفاء [2]، حيث يمكن إخفاء الرسالة السرية بكافة أشكالها (نص، صورة، صوت) داخل أوعية معلومات تمتلك خصائص مختلفة (نص، صورة، صوت، وسائط متعددة)[4] [3] [1].

يعتبر علم الإخفاء علم قديم جداً ، ويعتمد على إرسال المعلومات بطريقة خفيه. بدأ هذا العلم في عهد الإغريق (في حدود 700 سنة) قبل الميلاد، وذلك بكتابة الرسائل السرية على الأحجار أو الجلود وا ِخفائها في بطون الحيوانات، ومن ثم إرسالها إلى الجهة المقصودة بعد اتفاق مسبق بين الطرفين. كذلك حلق شعر الرأس وكتابة الرسالة السرية وبعد نمو الشعر يرسل الشخص إلى الجهة المقصودة [5]، أما في عصر الحاسبات عصرنا هذا فقد تعددت وسائل الاتصالات بين الناس، كالهاتف و الفاكس و شبكات الحاسبات و أجهزة الراديو إلى آخر ما هنالك من وسائل و أجهزة تخاطب وبالرغم من ذلك يبقى الهاجس هو الحفاظ على خصوصية المعلومات المتبادلة. كل وسيلة من وسائل الاتصال يجب أن تؤمن الحد الأدنى من سرية المعلومات المتبادلة، و الطرف الذي ترسل له الرسالة يجب أن يكون الوحيد الذي يستطيع أن يقر أ أو يسمع هذه الرسالة و يفسرها. لذا يجب استعمال وسائط اتصال تؤمن قنوات اتصال ذات مستوى أمان عال جداً لا يمكن اختراقها من قبل أي كان للاطلاع على الرسائل أو الصور المغطاة. إن عملية الإخفاء يجب أن تكون قوية في مواجهة أية محاولات لكسرها[6].

من المعلوم أن الصور تلعب دوراً مهماً في حياة البشر، لهذا السبب يمكن استخدام الصور كمواد للغطاء للاتصالات المخفية. والصور هي عبارة عن مصفوفة من الأرقام والتي تمثل شدة الإضاءة في نقاط مختلفة من الصورة. وتعتبر الصور ذات التدرج الرمادي مثالاً جيداً للإخفاء وذلك لان القيم اللونية تتغير بصورة تدريجية وهذا مما يزيد قدرة الصورة على الإخفاء. وتعطي الصور ذات التدرج الرمادي أفضل النتائج لبعض تطبيقات الستيكانوكرافي حيث أن كون الصورة حاوية على كثير من الأشياء تجعلها مملوءة وبالتالي تؤمن غطاءً جيداً للإخفاء أما الصورة المتضمنة فمن الصعوبة ملاحظتها[7].

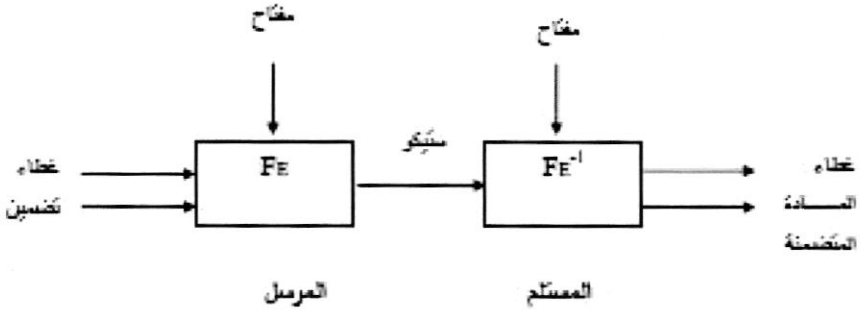
في هذا البحث تم اقتراح طريقتين لإخفاء الصور ذات التدرج الرمادي، في الطريقة المقترحة الأولى تم استخدام صورتين الصورة الأولى استخدمت للتضمين والصورة الثانية استخدمت كغطاء، أما في الطريقة المقترحة الثانية فتم إخفاء الصورة الأصلية.

ISSN:1813 – 1662

ستيكانوكرافي:

من المواضيع المهمة والرئيسية لإخفاء المعلومات ويقصد به إخفاء المعلومات (أو الصورة) داخل معلومات أخرى (أو صورة أخرى) [8].

النموذج العام لإخفاء البيانات في بيانات أخرى يمكن وصفه كما يلي: البيانات المتضمنة أو المطمورة (Embedded data) هي الرسالة (أو الصورة) التي يرغب الشخص بإرسالها بصورة سريةو عادة ما تخفى في رسالة بريئة يشار إليها غطاء (غطاء نص cover text أو غطاء صورة cover image أو غطاء صوت cover Audio) حسب الملائمة وينتج وسط ستيكو(Stego). يستخدم مفتاح ستيكو للسيطرة على عملية الإخفاء، وقد تم في هذا البحث استخدام شبكة Generalized Regression Neural Network (GRNN) لتحديد قيم المفتاح [10] [9]. الشكل (1) يوضح عملية التضمين العامة.



الشكل رقم (1) يوضح نموذج التضمين

حيث أن:

FE: دالة ستيكانوكرافي " تضمين "

FE^{-1}: دالة ستيكانوكرافي "استخلاص "

غطاء: غطاء البيانات (أو غطاء الصورة) التي تخفى فيها البيانات المتضمنة (أو الصورة المتضمنة)

تضمين: الرسالة (الصورة) المراد إخفائها (تضمينها)

المفتاح: معامل إلى FE

ستيكو: بيانات الغطاء مع الرسالة المخفية

يمثل الإدخال غطاء البيانات (أو الصورة) التي لم يتم معالجتها، وتضمين تمثل الرسالة (أو الصورة) المراد إخفائها في الغطاء من خلال دالة FE، تسمى البيانات الناتجة ستيكو والتي تحوي على الرسالة المخفية (أو الصورة المخفية) اما عملية FE^{-1} فتعمل على استرجاع البيانات المتضمنة[13][12][11].

يجب إن يكون الغطاء في الإدخال والإخراج هو نفسه وكذلك بالنسبة إلى الرسالة السرية (أو الصورة السرية)[15][14].

الشبكة العصبية الصناعية :

هي عبارة عن نظام لمعالجة البيانات بشكل يحاكي و يشابه الطريقة التي تقوم بها الشبكات العصبية الطبيعية للإنسان أو للكائن الحي (أي النظام العصبي البشري)، والشبكة العصبية الاصطناعية عبارة عن هيكل ذو بناء متوازي المعلومات يتكون هذا الهيكل من وحدات معالجة تقوم بمعالجة المعلومات وتدعى بالعصبونات أو عناصر المعالجة، وتمر الإشارات بين العصبونات عبر خطوط ربط، كما يرفق كل خط ربط بوزن معين وهو رقم يضرب مع الإشارات الداخلة، كما يطبق على كل عصبون دالة تفعيل ليتم تحديد إشارة الإخراج الناتجة منها [16].

الشبكات العصبية الاصطناعية هي جملة من الإجراءات الأساسية التي تمكن عند إدماجها فيما بينها من القيام بعمليات معينة يطلبها المستفيد عند الحاجة. لذلك من الضروري للمستفيدين من خدمات الشبكات العصبية القيام بعمليات أولية لتدريب الشبكة تدريجيا حتى تتمكن في النهاية من الاستجابة لكل مطالبهم. وتتم هذه التدريبات في شكل تلقينات متكررة للتصرفات المطلوبة من قبل الشبكة من خلال برامج مختصة تتولى السهر على ضمان تطابق تصرفات الشبكة مع متطلبات صاحبها، والشبكات العصبية الاصطناعية ذات استخدامات واسعة جداً في معالجة الصور وذلك لما تقدمه من كفاءة عالية في العمليات الحسابية بالإضافة إلى أسلوب عملها المتوازي[17] مما يجعلها مناسبة لتستخدم في تمييز الكلام ومعالجة الإشارة وتمييز الصوت والطب والعديد من المجالات الأخرى، ويعد حقل دراسة الشبكات العصبية الاصطناعية حقل متشعب جداً من ناحيتي التطوير والتطبيق. [18]

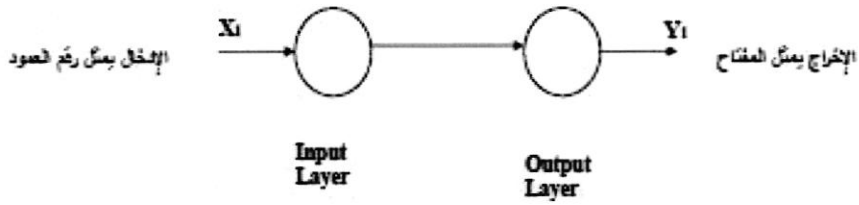
Generalized Regression Neural Network(GRNN):

هي نوع من Radial Basis Network وتستعمل دوال تقريبية. وتتكون هذه الشبكة من طبقة الإدخال والتي تحوي على خلية عصبية وتقوم باستلام المعلومات من العالم الخارجي. تنساب البيانات من طبقة الإدخال إلى طبقة الإخراج [20][19].

شبكة (GRNN) تمتلك صفات عديدة وهي: هذه الشبكة تمتلك صفة التغذية الأمامية (Feed forward) أي أن اتجاه الإشارة الداخلة إلى الشبكة يكون إلى الأمام ومن ثمة فان الإشارة الخارجة من أي خلية تعتمد على الإشارة الداخلة فقط. تدريب الشبكة يتم عن طريق مشرف أي التدريب بإشراف (Supervised Training) وهذا يتطلب وجود زوج من متجه الإدخال ومتجه الإخراج المتوقع[21].

ISSN:1813 – 1662

في هذا البحث تم استخدام شبكة(GRNN)لتحديد قيمة المفتاح نظراً لما تتميز به هذه الشبكة من دقة وسرعة في الحصول على النتائج [22]. الإدخال إلى الشبكة يتمثل برقم العمود (وهو من 1 إلى 100)، أما الإخراج فيمثل قيمة المفتاح (وهو 1 أو 0) كما مبين في الشكل رقم (2). في حالة كون قيمة المفتاح 1 معناها في الطريقة المقترحة الأولى إجراء عملية التبديل بين صورة التضمين وصورة الغطاء، أما في حالة كون قيمة المفتاح 0 فتبقى صورة التضمين وصورة الغطاء كما هي أي بدون إجراء عملية التبديل. أما في حالة كون قيمة المفتاح تساوي 1 معناها في الطريقة المقترحة الثانية إجراء عملية قلب البت الثامن (MSB)، أما في حالة كون قيمة المفتاح 0 فتبقى الصورة كما هي أي بدون إجراء عملية القلب.



الشكل رقم (2) يوضح شبكة GRNN

الطريقة المقترحة الأولى:

تخفيض الصورة هي تقنية ستيكانوكرافي [23] تم استخدامها في هذا البحث لتبادل الصور المغطاة. وتخفيض الصورة هي حالة خاصة من نظام التعويض التي تعمل فيه الصور كرسالة سرية وغطاء حيث يتم إعطاء صورة غطاء وصورة سرية بأبعاد متساوية [25][24]، وتم استخدام طريقة ذكائية لتحديد قيمة المفتاح، حيث تم استخدام شبكة GRNN، وفي حالة كون القيمة الناتجة من الشبكة تساوي واحد فإن المرسل يغير البتات الأقل أهمية الأربعة لقيم اللون الرصاصي لصورة الغطاء مع البتات الأكثر أهمية الأربعة للصورة السرية أما في حالة كون القيمة الناتجة من الشبكة تساوي صفر فتبقى الصور كما هي أي بدون إجراء عملية التبديل. ويتم الحصول على وسط الستيكو والذي يمثل الصورة الأصلية وصورة الغطاء بعد إجراء عملية التبديل، أما المستلم وبالاعتماد على المفتاح الناتج من الشبكة يستخلص البتات الأقل أهمية الأربعة من صورة الستيكو، من خلال الحصول على البتات الأكثر أهمية للصورة السرية. ويتم استعمال أربعة بتات كافية لتحويل تقريب قوي إلى الصورة السرية.

الخوارزمية المقترحة الأولى:

1- إدخال اسم صورة التضمين وصورة الغطاء
2- قراءة صورة التضمين وصورة الغطاء
3- جعل الصورتين بنفس الحجم (عدد الصفوف يساوي 100 وعدد الأعمدة يساوي 100)
4- عرض صورة التضمين وصورة الغطاء
5- تحويل القيم اللونية للصورتين إلى النظام الثنائي
6- ندرب شبكة GRNN على الإدخال والإخراج (الإدخال يمثل رقم العمود والإخراج يكون واحد أو صفر ويتم خزنه في المتغير n)
7- j=1 (j يمثل رقم العمود)
8- i=1 (i يمثل رقم الصف)
9- نختبر شبكة GRNN على الإدخال والإخراج، إذا كان n يساوي صفر الانتقال إلى الخطوة الثالثة عشر
10- إجراء عملية تبديل بين البتات الأربعة الأقل أهمية لصورة الغطاء مع البتات الأربعة الأكثر أهمية لصورة التضمين
11- زيادة قيمة المتغير i بمقدار واحد
12- يتم فحص قيمة المتغير i إذا كان اقل أو يساوي 100 يتم الانتقال إلى الخطوة العاشرة
13- زيادة قيمة المتغير j بمقدار واحد
14- يتم فحص قيمة المتغير j إذا كان اقل أو يساوي 100 يتم الانتقال إلى الخطوة التاسعة
15- تحويل القيم اللونية للصورتين إلى النظام العشري
16- يتم الحصول على وسط الستيكو ويتم عرض الصورتين بعد الإخفاء
17- تحويل القيم اللونية للصورتين إلى النظام الثنائي
18- ندرب شبكة GRNN على الإدخال والإخراج (الإدخال يمثل رقم العمود والإخراج يكون واحد أو صفر ويتم خزنه في المتغير n)
19- j=1 (j يمثل رقم العمود)
20- i=1 (i يمثل رقم الصف)
21- نختبر شبكة GRNN على الإدخال والإخراج، إذا كان n يساوي صفر الانتقال إلى الخطوة الخامسة والعشرون
22- إجراء عملية تبديل بين البتات الأربعة الأقل أهمية لصورة الغطاء مع البتات الأربعة الأكثر أهمية لصورة التضمين
23- زيادة قيمة المتغير i بمقدار واحد
24- يتم فحص قيمة المتغير i إذا كان اقل أو يساوي 100 يتم الانتقال إلى الخطوة الثانية والعشرون
25- زيادة قيمة المتغير j بمقدار واحد
26- يتم فحص قيمة المتغير j إذا كان اقل أو يساوي 100 يتم الانتقال إلى الخطوة الواحدة والعشرون

27- تحويل القيم اللونية للصورتين إلى النظام العشري
28- عرض الصورتين الناتجتين

الطريقة المقترحة الثانية:

تم اقتراح طريقة جديدة لتبادل الصور. حيث يتم إدخال الصورة المراد إخفائها ويتم قراءتها، وتم استخدام طريقة ذكائية لتحديد قيمة المفتاح، حيث تم استخدام شبكة GRNN ، وفي حالة كون القيمة الناتجة من الشبكة تساوي واحد فإن المرسل يعمل على قلب قيمة البت الثامن أي (MSB) (إذا كان واحد يصبح صفر وبالعكس)، أما في حالة كون القيمة الناتجة من الشبكة تساوي صفر فتبقى الصورة كما هي أي بدون إجراء عملية القلب. ويتم الحصول على وسط الستيكو والذي يمثل الصورة الأصلية بعد إجراء عملية القلب، أما المستلم وبالاعتماد على المفتاح الناتج من الشبكة يستخلص الصورة الأصلية.

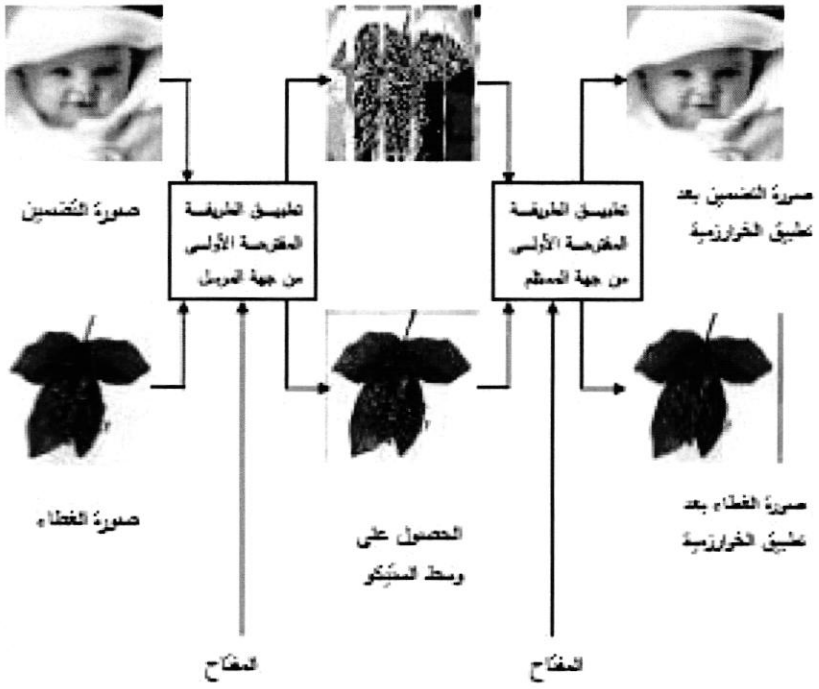
الخوارزمية المقترحة الثانية:

1- إدخال اسم الصورة
2- قراءة الصورة
3- إيجاد حجم الصورة
4- عرض الصورة الأصلية
5- تحويل القيم اللونية للصورة إلى النظام الثنائي
6- ندرب شبكة GRNN على الإدخال والإخراج (الإدخال يمثل رقم العمود والإخراج يكون واحد أو صفر ويتم خزنه في المتغير n)
7- j=1 (j يمثل رقم العمود)
8- i=1 (i يمثل رقم الصف)
9- نختبر شبكة GRNN على الإدخال والإخراج، إذا كان n يساوي صفر الانتقال إلى الخطوة الثالثة عشر
10- إجراء عملية قلب البت الثامن (MSB) في حالة كونه يساوي واحد نجعله صفر وبالعكس
11- زيادة قيمة المتغير i بمقدار واحد
12- يتم فحص قيمة المتغير i إذا كان اقل أو يساوي 100 يتم الانتقال إلى الخطوة العاشرة
13- زيادة قيمة المتغير j بمقدار واحد
14- يتم فحص قيمة المتغير j إذا كان اقل أو يساوي 100 يتم الانتقال إلى الخطوة التاسعة
15- تحويل القيم اللونية للصورة إلى النظام العشري
16- يتم الحصول على وسط الستيكو ويتم عرض الصورة بعد الإخفاء
17- تحويل القيم اللونية للصورة إلى النظام الثنائي
18- ندرب شبكة GRNN على الإدخال والإخراج (الإدخال يمثل رقم العمود والإخراج يكون واحد أو صفر ويتم خزنه في المتغير n)
19- j=1 (j يمثل رقم العمود)
20- i=1 (i يمثل رقم الصف)
21- نختبر شبكة GRNN على الإدخال والإخراج، إذا كان n يساوي صفر الانتقال إلى الخطوة الخامسة والعشرون
22- إجراء عملية قلب البت الثامن (MSB) في حالة كونه يساوي واحد نجعله صفر وبالعكس
23- زيادة قيمة المتغير i بمقدار واحد
24- يتم فحص قيمة المتغير i إذا كان اقل أو يساوي 100 يتم الانتقال إلى الخطوة الثانية والعشرون
25- زيادة قيمة المتغير j بمقدار واحد
26- يتم فحص قيمة المتغير j إذا كان اقل أو يساوي 100 يتم الانتقال إلى الخطوة الواحدة والعشرون
27- تحويل القيم اللونية للصورة إلى النظام العشري
28- عرض الصورة الناتج

تنفيذ الطريقة المقترحة الأولى:

تم عمل برنامج بلغة Matlab لتنفيذ الطريقة المقترحة الأولى، حيث تم إدخال صورة للتضمين وصورة أخرى للغطاء لاحظ الشكل رقم (3) وكان حجم كل صورة (100 صف و100 عمود)، وتم استخدام شبكة GRNN لتحديد قيمة المفتاح (الإدخال إلى الشبكة يمثل رقم العمود والإخراج يمثل قيمة المفتاح وهو 1 أو 0) ، في حالة كون قيمة المفتاح 1، فإن المرسل يغير البتات الأقل أهمية الأربعة لصورة الغطاء مع البتات الأكثر أهمية الأربعة لصورة التضمين وتم ملاحظة أن التغير في القيم اللونية لصورة التضمين كانت واضحة وذلك لأنه يتم تبديل القيم اللونية الأربعة الأكثر أهمية ، أما التغير في القيم اللونية لصورة الغطاء فهي قليلة وغير واضحة وذلك لأنه يتم تبديل القيم اللونية الأقل أهمية ويتم الحصول على وسط الستيكو، أما المستلم يعمل على فحص قيمة المفتاح، في حالة كون قيمة المفتاح 1، فان المستلم يغير البتات الأربعة الأقل أهمية لصورة الغطاء الناتجة في الوسط ستيكو مع البتات الأربعة الأكثر أهمية لصورة التضمين في الوسط ستيكو. ويتم الحصول على صورة التضمين وصورة الغطاء،كما مبين في الشكل رقم (4) والشكل رقم (5) الذي يبين تنفيذ الخوارزمية على أول قيمة لونية.المفتاح المستخدم في هذا التنفيذ كانت قيمته:

(1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 1 1 1 1 1 1 1
1 1 1 1 1 1 1 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 1 1 1 1 1 1
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0)



الشكل رقم (3) يبين الطريقة المقترحة الأولى

123	180	175	------
180			
175			

صورة الغطاء قبل تطبيق الطريقة المقترحة الأولى
100 صف و 100عمود

164	167	168	------
194			
186			

صورة التضمين قبل تطبيق الطريقة المقترحة الأولى
100 صف و 100عمود

122	186	170	------
188			
171			

صورة الغطاء بعد تطبيق الطريقة المقترحة الأولى 100 صف و 100 عمود

180	71	248	------
66			
250			

صورة التضمين بعد تطبيق الطريقة المقترحة الأولى 100 صف و100 عمود

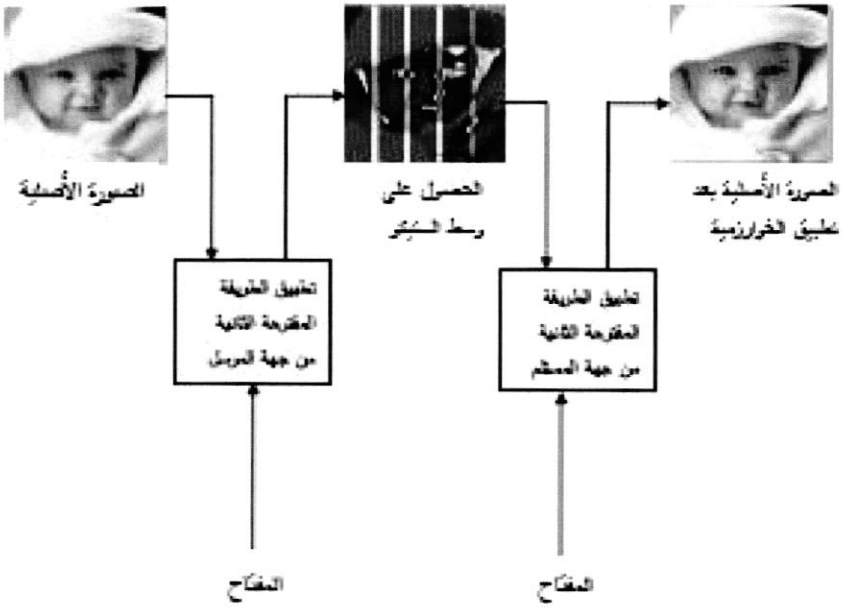
شكل رقم (4) يبين القيم اللونية للصورتين قبل وبعد تنفيذ الخوارزمية

شكل رقم (5) يبين تنفيذ الخوارزمية المقترحة الأولى على أول قيمة لونية

تنفيذ الطريقة المقترحة الثانية:

تم عمل برنامج بلغة Matlab لتنفيذ الطريقة المقترحة الثانية، حيث تم إدخال الصورة الأصلية لاحظ الشكل رقم (6)، وكان حجم الصورة (100 صف و100 عمود)، وتم استخدام شبكة GRNN لتحديد قيمة المفتاح (الإدخال إلى الشبكة يمثل رقم العمود والإخراج يمثل قيمة المفتاح وهو 1 أو 0)، في حالة كون قيمة المفتاح 1، فان المرسل يعمل على قلب قيمة البت الثامن (إذا كان 1 يصبح 0 وبالعكس) ويتم الحصول على وسط المستيكو، أما المستلم يعمل على فحص قيمة المفتاح، في حالة كون قيمة المفتاح 1، فانه يعمل على قلب قيمة البت الثامن (إذا كان 1 يصبح 0 وبالعكس) ويتم الحصول على الصورة الأصلية ،كما مبين في الشكل رقم (7) والشكل رقم (8) الذي يبين تنفيذ الخوارزمية على أول قيمة لونية. المفتاح المستخدم في هذا التنفيذ كانت قيمته:

(1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
0 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 1 1 1 1 1 1
1 1 1 1 1 1 1 1 1 1 1 1 1 0)



شكل رقم (6) يبين الطريقة المقترحة الثانية

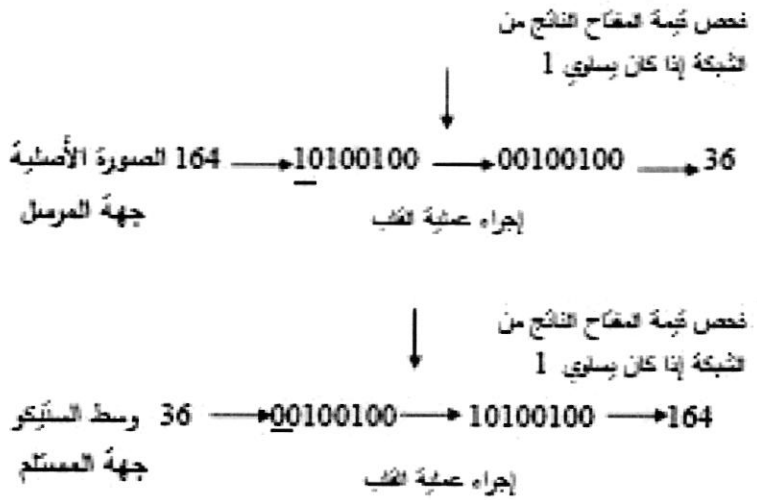
164	167	168	———
194			
186			

الصورة الأصلية قبل تطبيق الطريقة المقترحة الثانية
100 صف و 100 عمود

36	39	40	———
66			
58			

الصورة الأصلية بعد تطبيق الطريقة المقترحة الثانية
100 صف و 100 عمود

الشكل رقم (7) يبين القيم اللونية للصورة الأصلية قبل وبعد تطبيق الخوارزمية المقترحة الثانية



الشكل رقم (8) يبين تنفيذ الخوارزمية المقترحة الثانية على أول قيمة لونية

ISSN:1813 – 1662

المناقشة:

يعد إخفاء المعلومات من المواضيع المهمة والرئيسية للمحافظة على سرية المعلومات (نص، صورة، صوت). لذا تم اقتراح طريقتين لإخفاء الصور ذات التدرج الرمادي للمحافظة على سرية الصور المرسلة كما تم استخدام الشبكات العصبية الاصطناعية واستخدمت شبكةGeneralized Regression Neural Network نظراً لما تتميز به هذه الشبكة من دقة وسرعة في الحصول على النتائج مقارنة مع الطرق التقليدية التي تحتاج وقت وزمن طويل. تم عمل برنامج بلغة ماتلاب لتنفيذ العمل وذلك لإمكانات هذه اللغة في التعامل مع المسائل الرياضية والحاسوبية. الطريقة المستخدمة الأولى تكون أدق في الإخفاء من الطريقة الثانية وذلك لأنه تم تبديل أربع بتات، والطريقة الثانية تحتاج إلى وقت اقل في التنفيذ مقارنة مع الطريقة الأولى وذلك لأنه تم التعامل في الطريقة الثانية مع صورة واحدة.

الاستنتاجات:

هناك طرق متعددة لإخفاء المعلومات عرفت عبر التاريخ، ومنها على سبيل المثال كتابة الرسائل بالحبر الخفي أو باستخدام طرق أخرى مثل سائل الليمون أو غيره من الأحبار الخفية. وقد تطور هذا العلم تطوراً كبيراً في الوقت الحاضر نظراً لما له من أهمية كبيرة في الحفاظ على سرية المعلومات.

وتم في هذا البحث اقتراح طريقتين لإخفاء الصور ذات التدرج الرمادي، في الطريقة المقترحة الأولى يتم إدخال صورتين، الصورة الأولى استخدمت كصورة للتضمين والصورة الثانية استخدمت كصورة غطاء وبعد تطبيق الخوارزمية المقترحة الأولى على الصورتين، تم ملاحظة أن التغير في القيم اللونية لصورة التضمين كانت واضحة وذلك لأنه تم تبديل القيم اللونية الأربعة الأكثر أهمية (MSB)، أما التغير في القيم اللونية لصورة الغطاء فانه قليل وغير ملاحظ وذلك لأنه تم تبديل القيم اللونية الأربعة الأقل أهمية (LSB)، أما في الطريقة المقترحة الثانية فيتم إدخال صورة واحدة أصلية وتم إخفائها، حيث تم قلب قيمة البت الثامن في الصورة الأصلية (إذا كانت قيمة البت 1 تقلب إلى 0 وبالعكس) بالاعتماد على قيمة المفتاح ونلاحظ أن عملية قلب البت كان له تأثير على تغير القيمة اللونية للصورة الأصلية.

وتم في الطريقتين استخدام طريقة ذكائية لتحديد قيمة المفتاح حيث تم استخدام الشبكات العصبية الاصطناعية، وتم اختيار شبكة (GRNN)نظراً لما تتميز به الشبكات العصبية من سرعة عالية في معالجة البيانات كما تتميز بقدرتها على التعامل مع أنماط مختلفة من البيانات مما يجعلها مناسبة لكثير من التطبيقات المختلفة إذ أعطت حلولاً ذات كفاءة عالية في الكثير من المجالات.

المصادر:

1- Ibrahim, Ahmed and Arwa zabian, (2009), "Algorithm for text hiding in digital image for information security", IJCSNS International Journal of computer science and network security, Vol. 9, No. 6, P:1-7.

2- Prasad, M. Siaram and S. Naganjaneyu, (2009), "A Novel information hiding technique for security by using image steganography", Journal of theoretical and applied information technology, P: 1-5.

3- Baragada, Sambasiva and S. Ramkrishna, (2009), "Polynominal discriainant radial basis function for steganalysis", IJCSNS International Journal of computer science and network security, Vol. 9, No. 2, P:1-10.

4- Rao, T. Venkat Narayana and A. Govardhan, (2009), "Comparative study of visible reversible watermarking algorithms image security paradigm", International Journal of Engineering studies, Vol. 1, No. 3, P: 193-206.

5- Devi, T. H and H. S. Manjunatha, (2009), " Detecting original image using histogram, DFT and SVM", International Journal of Recent Trends in Engineering Vol. 1, No. 1, P: 367-371.

6- Kao, Chuan and Ren Juunn Hwang, (2005), "Information hiding in lossy compression gray scale image", Tarnkang Journal of science and Engineering, Vol. 8, No. 2, P: 99-108.

7- Spisak , Matthew D., (2004), "An Analysis of perturbed quantization steganography in the spatial domain", AFIT GIA ENG, P: 1-129.

8- Rabah, Kefa (2004), "Steganography the art of hiding data", Information Technology Journal 3, P: 245-269.

9- Naoe, Kensuke and oshiyasu Takeuji, (2008), "Damageless information hiding using neural network on ycbcr domain", IJCSNS International Journal of computer science and network security, Vol. 8, No. 9.

10- Tadiparti, Goalakrishna and Toshiyuki Sueyoshi, (2006), "Steganim a novel information hiding technique using animations", Engineering Letters, P: 1:11.

11- Al Toani, Ahmad T. and Abdulla M., (2009), "A Novel steganographic method for gray level images", International Journal of computer, P: 1-6.

12- Leng, Chiewkang and Jane Labadin (2008), "Steganography DCT coefficients reparation technique in JPEG image", International Journal of digital content technology and its applications, Vol. 2, No. 2, P: 1-7.

13- Davidson, Jennifer and Clifford Bergman, (2005), "An Artificial neural network for wavelet steganalysis", The International Society for optical Engineering, Vol. 5916, P:1-10.

14- Bhattacharyya, Debnat and Arpita Roy, (2009), "Receiver compatible data hiding in color image", International Journal of advanced science and Technology Vol. 6, P: 1-10.

15- Hassanien, Aboul Ella and Ajith Abraham, (I2008), "Spiking neural network and wavelets for

hiding iris data in digital images", Soft Compute DOI.
16- Vesely, A., (2003), "Neural networks in data mining",AGRIC. ECOM-CZECH, P: 427-431.
17- Mitra, Sushmita , (2002), "Data mining in soft computing framework a survery", IEEE, Vol. 13, No. 1.
18- Sajda, Paul, (2002), "Learning contextual relationships in mammograms using a hierarchical pyraid neural network", IEEE, Vol. 21, No. 3.
19- Baragada, Sambasiva Rao and S. Ramakrishna, (2001), "Implementation of radial basis function neural network for image steganalysis", International Journal of computer science and security, vol. 2
20- Medler, David A., (1998), "A Brief history of connectionism", Neural Computing surveys, P: 18-72.
21- Koutsoyiannis, Demetris, (2007), "Discussion of generalized regression neural networks for evapotran spiration modelling", Journal dessciences Hydrologques, P:832-839.
22- Al-Daoud, Essam, (2009), "A Comparison between three neural network models for classification problems", Journal of Artificial Intelligence 2, P: 56-64.
23- Sabeti, Vajiheh and Shadrokh Samavi, (2009), "Steganalysis of embedding in difference of image pixel pairs by neural network", Journal of Information security , Vol. 1, No. 1, P:17-26.
24- Potdar Vidyasagarand and Elizabeth Chang, (2004), "Visibly Invisible : cipher text as a steganographic carrier", International network conference, P: 1-8.
25- Zhong, Shangping and Xin Fan, (2009), "Steganalysis against equivalent transformation based steganographic algorithm for PDF files", International Symposium on information processing, P: 75-78.

Hiding images using clever methods

Shahla H. Ahmad Karruffa
College Of Dentistry , Mosul University , Mosul , Iraq

(Received: 2 / 9 / 2010 ---- Accepted: 27 / 9 / 2011)

Abstract

Hiding, is an ancient method that the human kept on using it so that no one can see or steal his precious things, this method was developed to be a science of considual value. The modern science, day by day, increases the hiding process with sophistication. Protecting data is considered to be the first of the information technology fields. Hiding data is considered to be a type of processing which is used in concealing data (text, image, audio) in different format of media such as text, image, audio. As for getting sure of an hidden files, it is done by analyzing the doubtable factors or by guessing the hidden information that may exist by noting the generated data or by depending on the hiding algorithms.

In this research, two methods were suggested to hide the gray images. In the first method: two images were used, the first was used for guessing while the second was used for covering and the stego can be obtained. The second method was possible in suggesting a way to hide the original image and obtain the stego. With both methods, it was possible to use a clever method to identify the key value such as artificial neural networks, also Generalized Regression Neural Network (GRNN) was used to identify the key value. The neural networks are well-Know way of providing a suitable method to represent the relations between the outputs of the given problem that is to be analyzed in a way so different from that ways used in the traditional programming. A Matlab (version 6.5) program was programmed to perform this task.