

نظام العلامة المائية المهجن ذكائيا

فردوس عدنان عبد القادر شهباء إبراهيم خليل ندى نعمت سليم
كلية علوم الحاسوب والرياضيات
جامعة الموصل

تاريخ استلام البحث: ٢٠١٠/٣/١٦

تاريخ قبول البحث: ٢٠١٠/٨/١٦

ABSTRACT

As a result of the development in data transfer technology a cross multimedia and internet, it has become possible to access and copy these information in unauthentic manner . This leads to penetrate digital multimedia security problem.

In this research a hybrid method is designed to protect product from unauthentication access using watermark technique with digital images, these images represent the important part in information systems and many applications. The method indicates hiding the watermark in both spatial and frequency domains using Artificial Intelligent techniques, such as neural networks and genetic algorithms by dividing the watermark depending on the important information contents. The basic important part hides in frequency domain and the second part in spatial domain using *Discreet Cosine Transform DCT* and *Least Significant Bit LSB*.

The method efficiency is measured using *Peak Signal –to-Noise Ratio PSNR* and *Normalized Correlation Coefficient NC* , Also many attacks is used to measured the watermark robustness and feasibility.

المخلص

نتيجة للتطورات الحاصلة في تقنيات نقل المعلومات والبيانات عبر الأوساط المتعددة وعلى شبكة الانترنت أصبح بالإمكان الوصول ونسخ هذه المعلومات والبيانات بأسلوب غير مخول وهذا يؤدي إلى مشكلة اختراق أمنية الوسائط الرقمية.

تم في هذا البحث تصميم طريقة مهجنة لحماية المنتج من الوصول غير المخول باستخدام تقنية العلامة المائية مع الصور الرقمية حيث تمثل هذه الصور الجزء الأساسي لأنظمة المعلومات والعديد من التطبيقات , تتضمن الطريقة إخفاء العلامة المائية في المجال المكاني وفي المجال الترددي باستخدام التقنيات الذكائية التي تتكون من الخوارزميات الجينية والشبكات العصبية عن طريق تقسيم العلامة المائية وحسب أهمية المعلومات التي تتضمنها, وتتلخص الطريقة بإخفاء وتضمين الجزء الأساسي والمهم من العلامة المائية في المجال الترددي وإخفاء الجزء الثاني في المجال المكاني باستخدام طريقة التحويل الجيب تمام *Discreet Cosine Transform DCT* وطريقة الـ *Least Significant Bit LSB* .

تم قياس كفاءة الطريقة بحساب قيم الـ *Peak Signal –to-Noise Ratio PSNR* ومعامل الارتباط *Normalized Correlation Coefficient NC* وكذلك استخدام مجموعة من الهجمات لقياس مرونة وصلابة العلامة المائية.

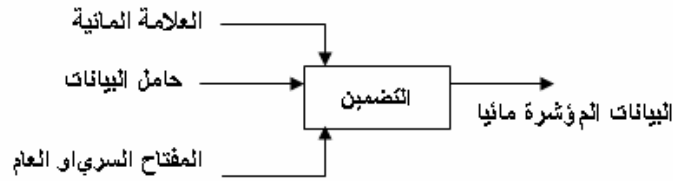
1-مقدمة:

أصبح الحاسوب الشخصي شائع جدا ومنتشر بصورة كبيرة وأصبح من السهل استنتاج وإنتاج الصور وأفلام الفيديو والنص والصوت بسرعة وبكلفة قليلة وبالإمكان توزيع هذه الملفات بسرعة بسبب توفر الانترنت في معظم المساكن ويعتبر التوسع في الشبكة العنكبوتية العالمية هو المسؤول عن الزيادة الكبيرة في قرصنة الوسائط. لهذا أصبح من المهم الكشف فيما إذا كان الملف أصلي وكذلك لمن تعود النسخة الأصلية إذ يمانع الناشرون من توزيع المواد الكترونيا لذلك فإنهم يرغبون بطريقة لاستخدام التوقيع الالكتروني لمنتجاتهم لأسباب حقوق الطبع. تم تعريف حق الطبع للصور الرقمية على انه عملية إثبات حقوق الملكية الفكرية بالقانون ضد إعادة الإنتاج غير المخول به أو معالجة أو تحويل أو بث الصور الرقمية، ولتحديد المؤلف الأصلي لملف مع قوانين حقوق الطبع تم استخدام تقنية تعرف بالتأشير المائي *watermarking* ويشار لها كعلامة مائية رقمية.[1]

تتضمن العلامة المائية التقليدية علامات صغيرة مرئية على ورقة لضمان أصولها، ومن الأمثلة على هذا وجودها في الصكوك الحكومية والمستندات الرسمية والنقود الورقية. تم تحويل وتحديث هذه الطريقة لتلائم الصور الرقمية وأفلام الفيديو والصوت والنص الرقمي.[3,4,5]

تشارك جميع طرق التأشير المائي بنفس كتل البقاء العامة. " نظام تضمين العلامة المائية *Watermark embedding* ونظام استرجاع العلامة المائية *watermark recovery*."

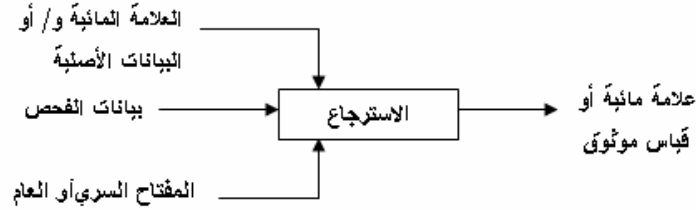
يوضح الشكل(1) العملية العامة لتصنيف العملية المائية، الإدخال إلى المخطط هو العلامة المائية، بيانات الغطاء ومفتاح اختياري سري أو عام.[9,17]



الشكل(1): المخطط العام للتأشير المائي الرقمي

يمكن أن تكون العلامة المائية بأي طبيعة مثل (عدد، نص، صورة) وقد يستخدم المفتاح لغرض الأمانة، التي هي منع المجموعات غير المخولة من استرجاع ومعالجة العلامة المائية. يكون الإخراج لمخطط التأشير المائي هو البيانات المؤشرة مائيا.

أما عملية استرجاع العلامة المائية فهو موضح بالشكل (2). نلاحظ أن الإدخال إلى المخطط هو البيانات المؤشرة مائيا، المفتاح السري أو العام واعتمادا على الطريقة، البيانات الأصلية و/أو العلامة المائية الأصلية. يكون الإخراج أما العلامة المائية المسترجع ، أو بعض أنواع القياس الموثوق مؤشر التشابه مع العلامة المائية في الإدخال الواجب تقديمها في البيانات.[7,8]



الشكل (2): المخطط العام لاسترجاع العلامة المائية

يهدف البحث إلى تصميم نظام العلامة المائية المهجن للصور الرقمية. تتضمن التقنية المهجنة استخدام طريقتين لإخفاء العلامة المائية، الطريقة الأولى تستخدم المجال المكاني والطريقة الثانية تستخدم المجال الترددي في الإخفاء ويتم تحديد مواقع الإخفاء باستخدام طرق التقنيات الذكائية. أن طريقة تقسيم العلامة المائية إلى جزئين لغرض إخفائها في المجال المكاني والمجال الترددي تعتمد على المستخدم وكذلك على أهمية المعلومة التي تتضمنها العلامة المائية.

2- الاعمال السابقة

قدم الباحثون R. Schyndel ، A. Trikel و C. Osborne طريقة لتضمين العلامة المائية في المجال المكاني وهي Least Significant Bit LSB أي الخلية الأقل أهمية حيث قاموا بتضمين بيانات العلامة المائية في LSB لبعض النقاط الضوئية للصورة الأصلية (الغطاء) [18].

في البحث الموسوم " DCT Doomain Watermarking Techniques for Still Images: Detector Performance Analysis and a New Structure " تم اقتراح طريقة تضمين باستخدام DCT حيث تم التضمين في حزمة بيانات الـ DCT ما عدا في قيمة DC وكانت عملية التضمين بجمع قيمة من قيم العلامة المائية مع قيمة من قيم الـ DCT [11].

قام الباحثان Tapio Seppanen و Nedeljko Cvejic ببحثهما الموسوم " Increasing Robustness of LSB Audio Steganography Using a Novel Embedding Method " بتقديم طريقة جديدة وقوية لاجراء عملية تضمين علامة مائية في ملف audio باعتماد الخانات العالية المستوى ضمن القيمة المعينة من قيم الملف وتم الحصول على نتائج جيدة وذلك بعد تطبيق الطريقة من قبل الباحثان على مجموعة كبيرة من انواع الموسيقى pop, rock, techno, jazz من دون حدوث تغيير مؤثر على بيانات الملف [16].

كما قدم الباحثان A. Golikeri و P. Nasiopoulos طريقة قوية لتضمين العلامة المائية باستخدام الـ DCT حيث تم تقسيم الصورة الغطاء الى مقاطع حجم كل مقطع 16×16 ومن ثم حساب قيمة الـ energy لكل مقطع واختيار المقاطع الصورية التي تمتلك أعلى قيم للـ energy واخذ اول ثمان قيم AC من هذه المقاطع ذات الحجم 16×16 وتضمين العلامة المائية فيها [2].

قدم البحث الموسوم " Robust Digital Watermarking Based Falling-off-Boundary in Corners Board MSB₆ Gray Scale Images " طريقة جديدة لتضمين العلامة المائية في صور رمادية

ضمن الخانة السادسة من النقطة الضوئية المختارة بطريقة تقليدية وحيث أنه تم التضمن بالخانات من خانة رقم 1 الى خانة رقم 8 ومن ثم المقارنة بينهم واتضح أنه عند التضمن ضمن MSB_6 أفضل الجميع [12].

3- تقنيات الذكاء الاصطناعي

شهد العالم في الآونة الأخيرة تطوراً كبيراً في ميادين الحياة، ومع هذا التطور ازدادت الصعوبات التقنية مما أدى إلى عدم القدرة على حلها باستخدام البرمجة التقليدية، وأدى بعد ذلك الى دفع الباحثين إلى التعمق في إيجاد خوارزميات وطرائق جديدة تساعد على الحل المناسب والأفضل للمسائل المعقدة إذ تم التوصل إلى بناء بنيات برمجية ذكية. تعد الخوارزمية الجينية أحد أساليب الذكاء الاصطناعي ، إذ برزت أهمية استخدام هذا الأسلوب في حل مسائل معقدة (كبيرة الحجم تمتلك كمّاً هائلاً من الحلول البديلة) خلال زمن مناسب، والحل الناتج من تطبيق الخوارزمية الجينية يكون في أغلب الأحيان حلاً قريباً إلى المثالي، ويؤمن هذا الأسلوب عند تطبيقه بحثاً ذكياً بين عدد هائل من الخطط البديلة. كذلك تعد الخوارزمية الجينية واحدة من خوارزميات البحث العامة المعتمدة على آلية الانتقاء الطبيعي ونظام الجينات الطبيعية. [15]

أما التقنية الأخرى من تقنيات الذكاء الاصطناعي فهي الشبكات العصبية. نشأ الاهتمام بالشبكات العصبية *Neural Network* من الخصائص المهمة الموجودة فيها وقدرتها على تجاوز محددات الحل التقليدي ، ومن خصائص الشبكات العصبية الاصطناعية خاصية التوازي وقدرتها على التكيف والتنظيم الذاتي ، حيث أن الشبكات العصبية توفر قدرات معالجة موثوق بها فضلاً عن قابليتها على التكيف من خلال تعديل أوزان ارتباط خلاياها ، كذلك تمتلك خاصية تقسيم الذاكرة حيث إن كل خلية من خلايا الشبكة العصبية تحتوي على وحدة ذاكرة خاصة بها تقوم بخزن الحقائق ، لذا فإن فقدان احد العناصر لا يسبب فقداناً لجميع البيانات المخزونة . تلك الخصائص جعلت من استخدام الشبكات العصبية مناسبة في كثير من المجالات التطبيقية ، كاستخدامها في معالجة الصوت والصور الرقمية وتمييز الأنماط . . الخ. ولذلك كان من الضروري التوجه إلى الشبكات العصبية الاصطناعية *Artificial Neural Networks* التي تعد من التطبيقات المهمة في مجال الذكاء الاصطناعي إذ اعتمدت على أسس بيولوجية في محاولة محاكاة السلوك البشري. [19,6]

تم في هذا البحث تصميم طريقة لتوليد المفتاح السري لتحديد مجموعة مواقع الغطاء *byte* المستخدم في تضمين واسترجاع العلامة المائية باستخدام شبكة *Kohonen* ، وتوليد المفتاح السري لتحديد مواقع النبضات *Bits* في الغطاء المراد إخفاء داخلها باستخدام الخوارزمية الجينية.

4- وصف خوارزميات البحث

4-1 تضمين العلامة المائية داخل الصورة الرقمية

إن الطريقة المهجنة المستخدمة في تضمين العلامة المائية داخل الصورة الرقمية تستخدم المجالين الزماني والمكاني وتتلخص بثلاث مراحل :

1. تقسيم العلامة المائية W إلى جزأين $w_1 + w_2$.
2. يتم تضمين الجزء الأول من العلامة المائية w_1 في المجال المكاني *Spatial domain* .
3. يتم تضمين الجزء الثاني من العلامة المائية w_2 في المجال الترددي *domain Frequency* .

4-1-1 تقسيم العلامة المائية

إن العلامة المائية هي صورة رقمية ممثلة بالنظام الثنائي *Binary Image* تعتمد طريقة تقسيم العلامة المائية على الشخص المضمن للعلامة وأهمية المعلومات والتطبيق وقد تم في هذا البحث تقسيم العلامة المائية حسب الصورة المبينة في الشكل (3):

العلامة المائية الأصلية W 

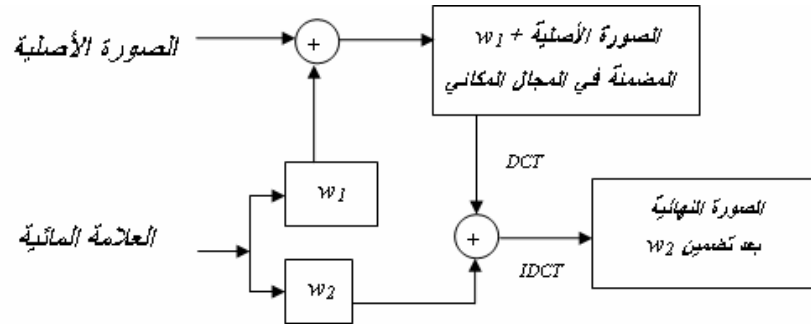
الجزء الأول من العلامة المائية الجزء الثاني من العلامة المائية

 W_2 W_1

الشكل (3): تقسيم العلامة المائية

4-2 خوارزمية التهجين لتضمين العلامة المائية في الصورة الرقمية

الشكل (4) يوضح خوارزمية التضمين المهجنة .



الشكل (4): خوارزمية التضمين المهجن

نتلخص خوارزمية التضمين بالخطوات التالية:

1. قراءة الصورة الرقمية التي بحجم $n \times n$ وتحميلها إلى الذاكرة.
2. قراءة العلامة المائية التي بحجم $m \times m$ وتحميلها إلى الذاكرة.
3. تقسيم العلامة المائية إلى جزئين الجزء الأول w_1 ذات الحجم $m_1 \times m_1$ والجزء الثاني w_2 ذات الحجم $m_2 \times m_2$.
4. توليد المفتاح السري k_1, k_3 لتحديد مجموعة مواقع الغطاء Bytes المراد الإخفاء داخلها باستخدام تقنية شبكة *kohonen* العصبية ، حيث تم بناء شبكة *kohonen* العصبية الاصطناعية لنقوم بهذا الغرض وذلك باتباع الخطوتين التاليتين .

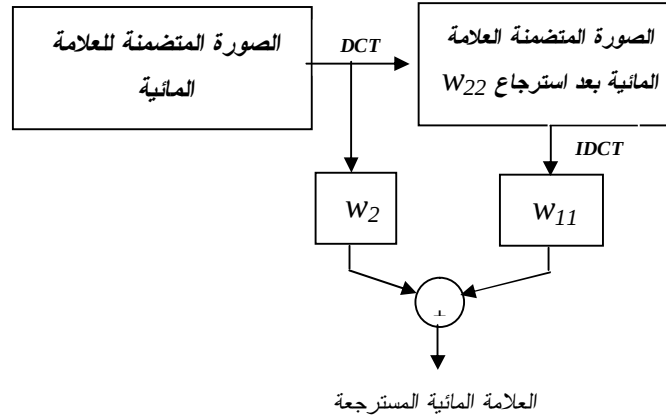
♦ توليد أوزان عشوائية وتثبيتها على الشبكة كأوزان إبتدائية.

- ◆ الاعتماد على بيانات الصورة الغطاء لتوليد المفتاح السري لتحديد مجموعة مواقع الغطاء bytes المراد الاخفاء داخلها وذلك بإدخال قيمة تلو قيمة من بيانات الغطاء الى شبكة kohonen والنتاج هو قيمة من قيم المفتاح والذي يمثل الخلية الفائزة winner node وذلك بعد تدريب الشبكة بعدد من الخطوات . حيث كان عدد خلايا طبقة الاخراج هي 256 خلية وذلك لان ابعاد الصورة الغطاء كان 256×256 لكي لا ينتج موقع خارج حدود الغطاء.
- 5. توليد المفتاح السري k_2, k_4 لتحديد المواقع المراد الإخفاء فيها النبضات Bit بالغطاء باستخدام تقنية الخوارزمية الجينية. بعد تحديد حجم المجتمع الممثل بحجم العلامة المائبة المطلوب تضمينها ضمن الغطاء المختار تم تنفيذ الخوارزمية الجينية على جميع الافراد المحددة للحصول على المفتاح السري الذي يمثل المواقع المراد التضمين فيها أي bit وتم اعتماد التقاطع crossover ذو نقطة القطع الواحدة وبالنسبة للطفرة mutation تم اختيار عكس قيمة الجين لاجراء عملية الطفرة على افراد المجتمع المتولد ومن ثم تم الحصول على المفاتيح السرية لمواقع الـ bit المراد التضمين بها في المجالين المكاني والتردد بعد 100 جيل وكان أفضل حل.
- 6. تضمين العلامة المائبة w_1 في المجال المكاني بالاعتماد على المفتاح السري $k_1 + k_2$ باستخدام طريقة LSB .
- 7. تحويل الصورة الناتجة من عملية التضمين في المرحلة الأولى إلى المجال الترددي باستخدام تحويل جيب التمام DCT .
- 8. يتم تضمين الجزء الثاني من العلامة المائبة w_2 في بيانات الصورة وهي بالمجال الترددي باستخدام المفتاح السري k_3 و k_4 .
- 9. يتم تحويل الصورة من المجال الترددي إلى المجال المكاني بعمل IDCT .

4-3 خوارزمية التهجين لاسترجاع العلامة المائبة المضمنة

- إن عملية استرجاع العلامة المائبة من الصورة هي العملية المعاكسة لعملية التضمين حيث يكون الإدخال هنا هو الصورة المتضمنة للعلامة المائبة والإخراج لهذه العملية سيكون هو العلامة المائبة المسترجعة ، الشكل (5) يوضح خوارزمية الاسترجاع المهجن.
- إن عملية الاسترجاع تتلخص بمرحلتين:-
- a- مرحلة استرجاع العلامة المائبة من المجال الترددي للحصول على الجزء الثاني w_2 من العلامة المائبة.
 - b- مرحلة استرجاع العلامة المائبة من المجال المكاني للحصول على الجزء الأول w_1 من العلامة المائبة.
- خوارزمية استرجاع العلامة المائبة تتم باستخدام الخطوات التالية:-
- 1- يتم تحويل الصورة المضمنة من المجال المكاني إلى المجال الترددي.
 - 2- يتم استرجاع الجزء الثاني من قيمة العلامة المائبة بالاعتماد على المفتاح السري k_3 و k_4 و خزنها في w_{22} .
 - 3- تحويل الصورة بعد عملية الاسترجاع من المجال الترددي إلى المجال المكاني.

- 4- استرجاع الجزء الأول من قيمة العلامة المائية بالاعتماد على المفتاح السري k_1 والمفتاح السري k_2 و تخزينها في w_{11} .
- 5- يتم دمج الجزء الأول من العلامة المائية w_{11} مع الجزء الثاني w_{22} للحصول على العلامة المائية كاملة.
- 6- يتم عرض العلامة المائية المسترجعة.
- 7- يتم حساب درجة الترابط بين العلامة المائية الأصلية والعلامة المائية الناتجة من الاسترجاع.



الشكل (5): خوارزمية الاسترجاع المجهن

5- حساب نسبة الخطأ والتطابق

يتم حساب نسبة الخطأ بين الصورة الأصلية والصورة المتضمنة للعلامة المائية عن طريق حساب قيمة $PSNR$ Peak Signal –to-Noise Ratio باستخدام القانون التالي: [13,10]

$$PSNR = 10 \cdot \log_{10} \left(\frac{255^2}{MSE} \right) dB \quad \dots (1)$$

$$MSE = \frac{1}{n \cdot n} \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} (I(i, j) - I_w(i, j))^2 \quad \dots (2)$$

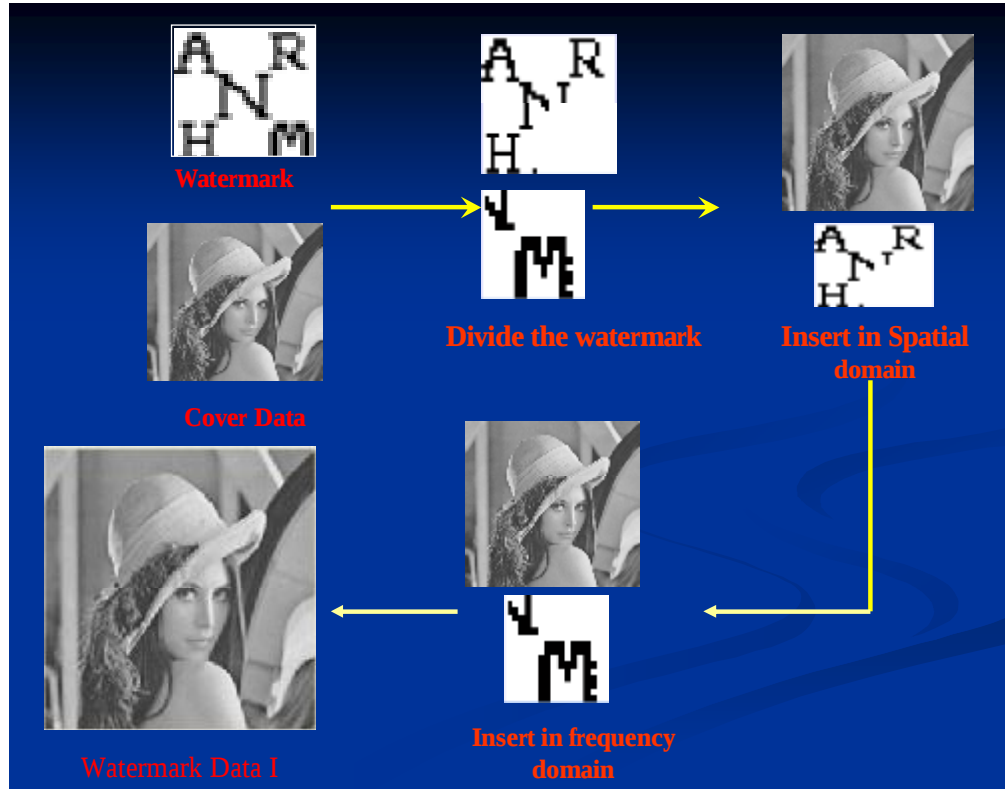
حيث إن $I(i, j)$ تمثل الصورة الأصلية و $I_w(i, j)$ تمثل الصورة المتضمنة للعلامة المائية، كذلك ممكن حساب نسبة الخطأ بين العلامة المائية الأصلية والعلامة المسترجعة باعتماد نفس المعادلات اعلاه ، يجب أن تكون العلامة المائية المسترجعة مشابهة للعلامة المائية الأصلية ويتم حساب نسبة التطابق من خلال حساب معامل الارتباط $Normalized Correlation Coefficient$ وحسب المعادلة التالية: [13,14]

$$NC = \frac{\sum_{i=1}^{M1} \sum_{j=1}^{M2} w(i, j) w^*(i, j)}{\sqrt{\sum_{i=1}^{M1} \sum_{j=1}^{M2} w(i, j)^2 \sum_{i=1}^{M1} \sum_{j=1}^{M2} w^*(i, j)^2}} \quad \dots (3)$$

حيث إن $w(i, j)$ تمثل العلامة المائية الأصلية و $w^*(i, j)$ تمثل العلامة المائية المسترجعة .

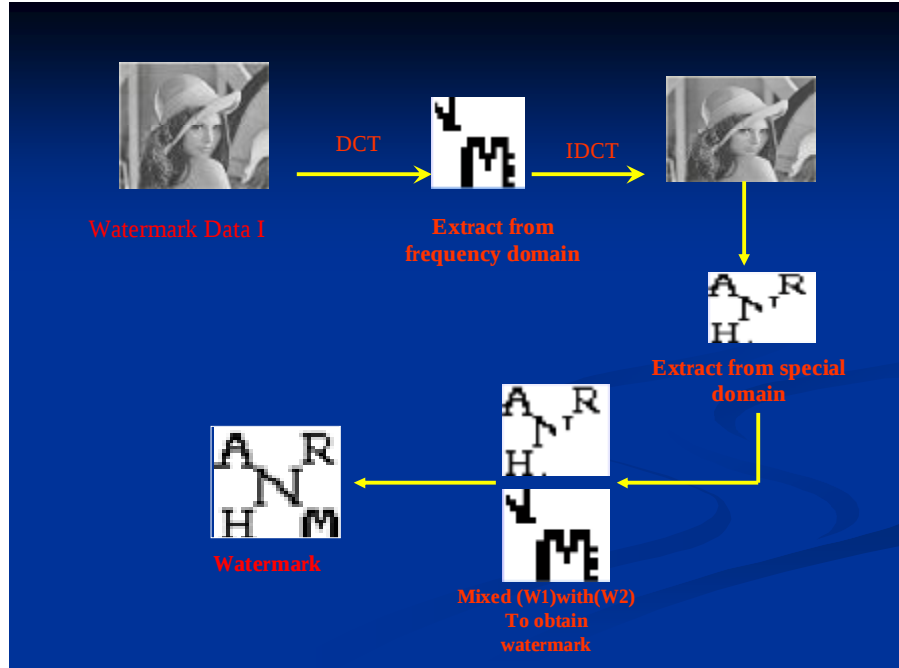
6- نتائج عملية التضمين والاسترجاع

تم اعتماد صورة *Lena* ذات التدرج الرمادي القياسية بأبعاد 256×256 كغطاء للعلامة المائية. أما بالنسبة للعلامة المائية فقد تم استخدام علامة مائية رقمية وهي عبارة عن صورة ثنائية بأبعاد 32×32 . تم في هذا البحث تقسيم العلامة المائية إلى جزأين حيث تم تضمين الجزء الأول من العلامة المائية في المجال المكاني والجزء الثاني من العلامة المائية تم تضمينه في المجال الترددي. و الشكل (6) التالي يوضح شاشة النتائج لعملية تضمين العلامة المائية بحجم 32×32 داخل الصورة *Lena* ذات التدرج الرمادي وبحجم 256×256 .



الشكل (6): يوضح شاشة النتائج لعملية تضمين للعلامة المائية

الشكل (7) التالي يوضح شاشة النتائج لعملية الاسترجاع للعلامة المائية من الصورة *Lena* ذات التدرج الرمادي.

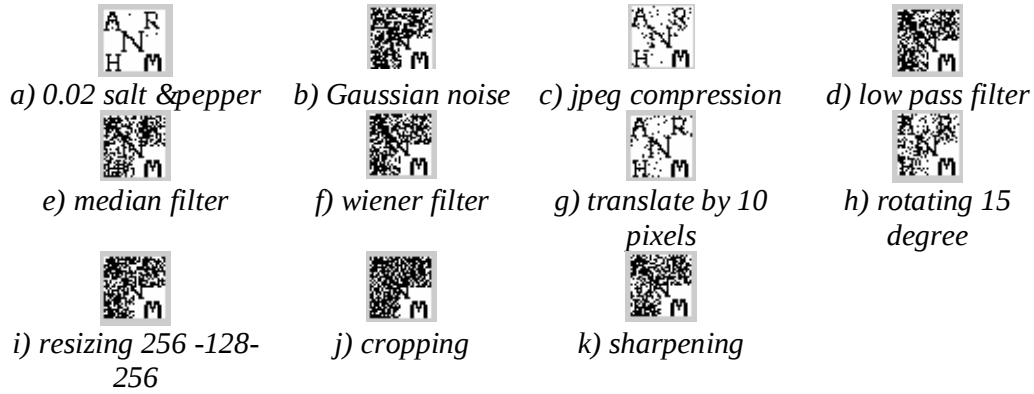


الشكا

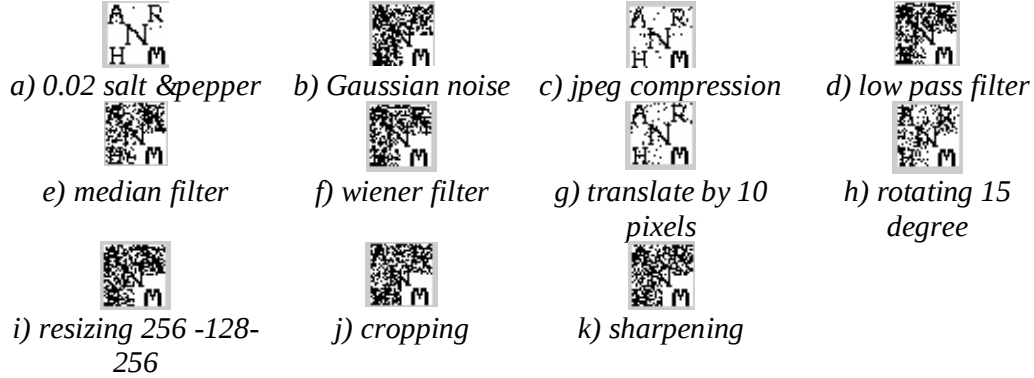
يتم حساب معامل الارتباط *Normalized correlation coefficients* لقياس مدى ترابط العلامة المائية المسترجعة والعلامة المائية الأصلية وتكون قيمة هذا المعامل في المجال $[-1,1]$. حيث تم حساب درجة الترابط بين العلامة المائية الأصلية والعلامة المائية الناتجة من الاسترجاع لصورة *Lena* وكانت مسلوية للواحد وهذا يدل على أن العلامة المائية استرجعت بشكل ممتاز وبدون أي نقص أو تشويه. كما تم حساب نسبة التشوه للغطاء المستخدم بعد تضمين العلامة المائية فيه عن طريق *PSNR* وهي اختصار لـ *Peak Signal to-Noise Ratio* وكانت قيمتها 70.672674 بالطريقة الأولى وكانت قيمتها 71.731943 بالطريقة الثانية المستخدمة المفاتيح الذكائية.

لاختبار قوة ومتانة نظام تضمين العلامة المائية المستخدم في هذا البحث تم توجيه وإدخال بعض التأثيرات التي تؤثر على الصورة حيث هنالك أنواع مختلفة من الهجمات في العلامات المائية والتي تعتمد على الهدف أو الغرض من الهجوم على الصورة التي تحتوي على العلامة المائية، بالنسبة للهجمات العدائية التي تحصل خلال إجراء عمليات معالجة الصور الشائعة التي يكون الهدف منها هو إضافة تشويه إلى العلامة المائية بالترتيب لإرجاع العلامة المائية بصورة غير مقروءة إي لا يمكن قراءتها أو اكتشافها ومن هذه الهجمات كبس الصور بفقدان، وإضافة ضوضاء لعمل تشويه بالصورة ، وتمرير الصورة على عدد من المرشحات منها مرشح تمرير الترددات الواطئة ومرشح تمرير الترددات العالية والمرشح المعدل والوسيط ، وكذلك تغيير حجم الصورة وتحويلها وعمل قطع لجزء من الصورة والخ من التحويلات التي تتم على الصورة المضمنة داخلها العلامة المائية لغرض تشويهها والتي يكون القصد منها تقليل قوة العلامة المائية وعدم استرجاعها بصورتها الأصلية. تم في هذا البحث تسليط مجموعة من الهجمات على الصورة المضمنة فيها العلامة المائية مثل عمل تصغير للصورة وإضافة ضوضاء من نوع كاوسين وضوضاء الملح والفلفل ، وكذلك كبس الصورة بنوعية *jpg*

أظهرت النتائج أن الخوارزمية المستخدمة في عملية التضمين والاسترجاع قوية ضد عملية الكبس، وتميرير الصورة على مرشح الترددات الواطئة، والمرشح الوسيط، تغيير حجم الصورة وتزحيف وتدوير الصورة وكذلك تمرير الصورة على مرشح *wiener* والشكلان (8) و (9) يوضحان العلامة المائية المسترجعة بعد تسليط بعض التأثيرات على الصورة المضمنة للعلامة المائية بطريقتين الأولى باستخدام مفتاح سري تقليدي والأخرى باستخدام مفتاح سري ذكائي.



الشكل (8) يمثل العلامة المائية المسترجعة بعد تسليط الهجمات عليها بطريقة استخدام مفتاح سري تقليدي



الشكل (9) يمثل العلامة المائية المسترجعة بعد تسليط الهجمات عليها بطريقة استخدام مفتاح سري ذكائي

والجدولان (1) و (2) يوضحان النتائج التي تم التوصل إليها بعد تعريض الصورة المضمنة للعلامة المائية لبعض الهجمات حيث تم حساب درجة الترابط بين العلامة المائية الأصلية والعلامة المائية المسترجعة وحساب قيمة PSNR أيضاً.

جدول (1) معامل الارتباط *Normalized Correlation Coefficient* ونسبة التشوه *PSNR* بين العلامة

المائية المسترجعة والعلامة المائية الأصلية باستخدام مفتاح سري تقليدي

<i>Attack</i>	<i>Normalized Correlation Coefficient</i>	<i>PSNR</i>
Cropping	0.710482	52.063800
Gaussian noise	0.769484	52.906259
Jpg compression	0.962356	60.309886
Low pass filter	0.771037	52.931806
Median filter	0.810369	53.654984
Resizing	0.762456	52.793123
Salt and pepper noise	0.996406	70.452291
Sharpening	0.785637	53.182303
Translate	0.967164	60.909866
Rotating	0.883799	55.609292
Wiener filter	0.771812	52.944636

جدول (2) معامل الارتباط *Normalized Correlation Coefficient* ونسبة التشوه *PSNR* بين العلامة

المائية المسترجعة والعلامة المائية الأصلية باستخدام مفتاح سري ذكائي

<i>Attack</i>	<i>Normalized Correlation Coefficient</i>	<i>PSNR</i>
Cropping	0.779523	53.075065
Gaussian noise	0.777217	53.035523
Jpg compression	0.972208	61.606225
Low pass filter	0.787917	53.223211
Median filter	0.825723	53.984987
Resizing	0.774133	52.983355
Salt and pepper noise	0.996406	70.452291
Sharpening	0.787158	53.209532
Translate	0.967164	60.909866
Rotating	0.883799	55.609292
Wiener filter	0.792458	53.306199

بالنسبة لقيمة معامل الارتباط كلما اقتربت من الواحد هذا يعني ان العلامة المائية استرجعت بأفضل شكل ومن الجدولين 1 و 2 نلاحظ أنه قيم معامل الارتباط تكون أفضل عند استخدام مفتاح سري ذكائي عن ما هو عليه عند استخدام مفتاح تقليدي، حيث عند عمل *cropping* للصورة المضمنة بها العلامة المائية ومن ثم استخلصت العلامة المائية وحسب لها معامل الارتباط لوحظ أنه عند استخدام مفتاح ذكائي كانت قيمته أفضل وهي 0.779523 في حين عند استخدام مفتاح تقليدي كانت قيمة 0.710482 وكذلك قيمة *PSNR* كانت 53.075065 بالذكائي (وهذا يعني أن العلامة المائية المسترجعة مطابقة للأصلية أو مشابهة لها جداً) بينما بالتقليدي كانت قيمته أقل وهي 52.063800 وهكذا بالنسبة لباقي الهجمات.

7- الاستنتاجات:

تعتبر الطريقة المعتمدة في البحث لإخفاء العلامة المائية من طرق الإخفاء القوية والجيدة إذ أنها تمكننا من:

- استخدام العلامة المائية بحجم اكبر من الحجم المستخدم في الطرق الأخرى لأنها تستخدم الإخفاء في المجال المكاني والمجال الترددي . إذ تعتمد الطريقة على تقسيم العلامة المائية إلى جزئين وإخفاء الجزء الأول في المجال المكاني والجزء الثاني في المجال الترددي .
- يمكن إخفاء المعلومات المهمة (الجزء المهم من العلامة المائية) في المجال الترددي وإخفاء الجزء الأقل أهمية في المجال المكاني وهذا يجعل من الصعوبة التعرف على العلامة المائية واختراقها والوصول غير المخول لها.
- تميزت الخوارزمية بالقوة والمتانة تجاه معظم التهديدات التي تتعرض لها العلامة المائية في محاولة لتغييرها وإزالتها .
- باستخدام طريقة الخوارزمية الجينية في توليد المفتاح السري تم الحصول على نتائج وقيم جيد جداً بعد الجيل المائة.
- كما تميزت العلامة المائية المضمنة بكونها غير مدركة في الصورة المضمنة وتضمينها لا يسبب أي تشوه أو تغير في الصورة الحاملة لها.
- تم الحصول على نتائج كفاءة لقيم $PSNR$ ومعامل الارتباط NC .

المصادر

- [1] د.علاء حسين الحمامي ومحمد علاء الحمامي, (2008) ، "إخفاء المعلومات الكتابية المخفية والعلامة المائية"، مكتبة الجامعة، الشارقة.
- [2] A. Golikeri, P. Nasiopoulos,(2004), "A Robust DCT energy based watermarking scheme for images", Canada.
- [3] AL-Hamami A.H.,Hilal M. Yousif & Jawal M.A., (2002),"Watermarking JPEG bit Stream Images", First Conference on Information Hiding, AL-Rafidain University College Magazine, No., pp. 34-47, Baghdad, Iraq.
- [4] AL-Hamami, AH & Ziad Tariq, (2003),"An algorithm for watermarking digital images In the wavelet transform domain",second conference on information hiding, AL-Rafidian university college magazine,No. 10, Iraq.
- [5] Allan M. Bruce, November 2nd,(2001),"A Review of digital watermarking", Department of Engineering, university of Aberdeen,Scotland,.
- [6] Bramer M. and Devedzic V., (2004), " Artificial Intelligence Applications and Innovations, International Federation for information processing, Boston.
- [7] Cox Ingemar J., Kilian Joe, Leighton Tom,and shamon Talal, (1996),"A secure, Robust watermark for multimedia", information hiding: First International workshop, proceeding, vol. 1174 of lecture notes in computer science, springer, pp. 185-205
- [8] Edin Muharemagic and Borko Furht, (2004), " Multimedia security: watermarking techniques", Department of computer science and engineering, Florida Atlautic university, USA,.
- [9] Fernando Perez-Gonzales and Juan R. Hernandez,(2003)," A Tutorial on digital watermarking", Dept. Of Communication vigo university , spain, project TIC-96-0500-C10-10,.
- [10] H. Seddik, M. Sayadi, F. Fnaiech, and M. Cheriet, (2007), "New multi-domains image watermarking method based on multi-watermarks embedding and neural network segmentation, Applied mathematical sciences, vol. 1, no. 39, pp. 1927-1939.
- [11] J. R. Hernandez , M. Amado and F. Perez-Gonzalez, " DCT Doomain Watermarking Techniques for Still Images: Detector Performance Analysis and a New Structure", in IEEE Trans. on Image processing, 9(1), pp. 55-68.
- [12] M. Aliwa, T. El_Tobely, M. Fahmy, M. El Said Nasr and M. Abd El_Aziz, , August (2009), " Robust Digital Watermarking Based Falling-off-Boundary in Corners Board MSB₆ Gray Scale Images", IJCSNS International Journal of Computer Science and Network Security, VOL. 9 No. 8.
- [13] M. Ketcham, and S. Vongpradhip ,(2007), "Intelligent Audio Watermarking using Genetic Algorithm in DWT Domain", International Journal of Intelligent technology, vol. 2, no. 2, pp. 135-140.
- [14] M. Shen, X. Zhang, L. Sun, P. Beadle and F. Chan, (2003), "A method for digital image watermarking using ICA",4th International symposium on

- independent component analysis and blind signal separation(ICA2003), Nara,Japan.
- [15] Mitchell, M., (1996), “ An Introduction to Genetic Algorithms “, MIT press, London.
- [16] N. Cvejic, T. Seppanen, (2004),"Increasing Robustness of LSB Audio Steganography Using a Novel Embedding Method", Proceedings of the International conference on information Technology: Coding and Computing, IEEE,.
- [17] Nedeljno Cvejic, (2004), " Algorithms for Audio watermarking and steganography", Academic dissertation , university of Oulu,.
- [18] R. Schyndel , A. Trixel and C. Osborne, (1994), " A Digital Watermark", Proc. ICIP,.
- [19] Zurada J. M., (1994) Introduction to Artificial Neural Systems, Jaico Publishing House, Mumbai.