العدد الواحد والعشرون
تاريخ الإصدار: 2 – تموز – 2020 م
www.ajsp.net
ISSN: 2663-5798

"خوارزمية مطورة للعلامة المائية بإستخدام الخريطة المقطعة"

إعداد الباحثة:

فدوى عبد اللطيف صافيه

إشراف:

د.زكريا زكريا [1] ، د.ناصر أبو صالح[2]

1- قسم الرياضيات- كلية العلوم - جامعة البعث

2- قسـم البرمجيات - كلية الهندسة المعلوماتية - جامعة البعث

العدد الواحد والعشرون
تاريخ الإصدار: 2 – تموز – 2020 م
www.ajsp.net
ISSN: 2663-5798

الملخص:

مع ظهور الانترنت أصبح بإمكان مؤلفي الوسائط الرقمية توزيع أعمالهم بجعلها متاحة على صفحات الويب أو بمنتديات النقاش العامة. الشخص الذي يملك الصلاحية بالدخول إلى الصفحات أو المنتديات يستطيع نسخ هذه الوسائط و تعديلها و الحصول على نسخة مطابقة تماماً للأصل. إن استخدام الوسائط الرقمية أظهرت مشاكل متعددة منها كيف يمكن للمؤلفين ضمان حقوق الملكية لأعمالهم. و تم تضمين الوسائط المتعددة بمعلومات إضافية لحماية الوسائط قبل توزيعها.

في هذا البحث تم اقترح طريقة جديدة لتضمين العلامة المائية في الصور من أي نوع، تم اقتراح خوارزمية محسنة وهي تقطيع بيانات العلامة المائية (Datas) إلى كتل(Blokes) بتقنية البزل الخريطة المقطعة. ثم طبقت خوارزمية الخلية الثنائية الأقل أهمية LSB (Least Significant Bit) من أجل الإخفاء. و للحصول على نتائج أفضل تم استخدام خوارزمية الحيتان من أجل تحديد الموضع الأمثل للإخفاء.

فعالية الخوارزمية المقترحة تأتي من خلال حصولنا على القيمة المثلى لذروة الإشارة إلى الضجيج PSNR (Peak Signal to Noise Ratio) و ذلك بتحديد الموقع الأفضل للإخفاء و كذلك قيمة متوسط مربع الخطأ MSE (Mean Square Error). ومقارنة النتائج بين خوارزمية LSB بالطرق القياسية و خوارزميتنا المقترحة.

النتائج التي حصلنا عليها تدل على كفاءة و قوة الخوارزمية المقترحة حيث تتميز بالمتانة لمقاومتها العديد من الهجمات التي نفذت على الصورة.

تم اعتماد على بيئة فيجول استديو 2016 وذلك لاحتوائها على دوال ذات كفاءة عالية تتعامل مع الخوارزمية المقترحة.

الكلمات المفتاحية: – العلامة المائية – الصور الرقمية – المواراة – الخانة الأقل أهمية – المخزن الثنائي – البزل – متوسط مربع الخطأ – ذروة الإشارة إلى الضجيج.

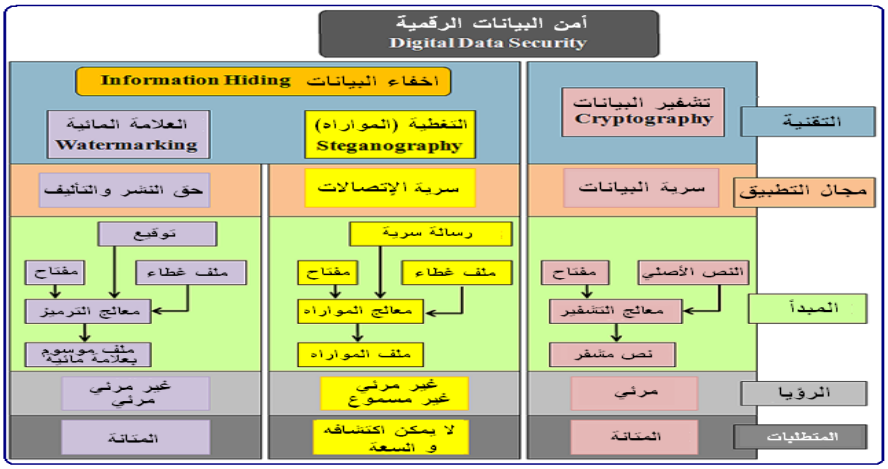
1-المقدمة Introduction:

يعتبر علم أمن البيانات الرقمية واحداً من أهم أركان الثورة المعلوماتية، نشأ كنتيجة مباشرة لها، وتطور معها. فقد أَمّن لها الحماية الضرورية في مواجهة المخاطر العديدة التي صادفتها خلال مسيرتها الحافلة بالإنجازات الكبيرة والتطورات المتلاحقة المتسارعة بصورة لم تعهدها أي من الثورات العلمية السابقة. يتألف نظام أمن البيانات الرقمية من تقنيتين:

1- تقنية تشفير البيانات Encryption.
2- تقنية إخفاء البيانات Information Hiding، وتتضمن:
أ- التغطية (المواراة) Steganography. ب- العلامة المائية Watermarking.

العدد الواحد والعشرون
تاريخ الإصدار: 2 – تموز – 2020 م
www.ajsp.net
ISSN: 2663-5798

يبين الشكل (1) مخططاً عاماً لأمن البيانات الرقمية، الذي يُوضح التقنيات المستخدمة ومجالات تطبيقها.



الشكل (1) المخطط العام لأمن البيانات الرقمية

2- هدف البحث و أهميته Research objectives and its importance:

إن من أعظم فوائد شبكة الإنترنت التي تمتد عبر كل أنحاء العالم هو سهولة نشر المعلومات و نقلها عبر الشبكة، لكن في نفس الوقت تعد هذه أكبر نقطة ضعف للإنترنت، حيث يمكن نسخ المعلومات و سرقة حقوق ملكيتها بسهولة كبيرة. و أي شخص يريد نشر معلومات عبر الإنترنت يرغب بحفظ معلوماته من السرقة أو من التخريب. قانونياً يجب أن يملك هذا الشخص حقوق ملكية مصدقة من قبل شخص نزيه (قاضي مثلاً) لتأكيد أن هذه المعلومات ملكه و ليست ملكاً لشخص آخر. الكتّاب، المصورون، الموسيقيون، الفنانون و غيرهم من المبدعين هم أكثر من استفاد من الإنترنت لنشر مؤلفاتهم و توزيعها حول العالم، لكن كثيراً ما تتعرض مؤلفاتهم للسرقة من قبل القراصنة حيث أنه من السهل جدا نسخ الملفات سواء كانت نصية أو سمعية أو

مرئية و طبعاً هذا النسخ يتم دون موافقة المالك الحقيقي للبيانات.

و مع ظهور التقنيات الحديثة تم تزويد هؤلاء المؤلفين بأسلحة جديدة و ثمينة في معركتهم لفرض القانون العالمي على الإنترنت.

و يوجد عدة حالات نحتاج فيها لحماية المنتج:

- ❖ خلال مرحلة الإنتاج نستخدم Access Control لمنع الآخرين من سرقة هذا المنتج.
- ❖ خلال عملية التوزيع لهذا المنتج في وسط غير موثوق (عبر الإنترنت مثلاً) يمكن أن نستخدم التشفير.

الحالة الأولى: في حال كان الطرف الأخير موثوق (Trusted End System)، فقط يتم تسليم المنتج لطرف موثوق و هذا الطرف لن ينشر البيانات و يسمح له باستخدامها فقط بالطرق التي دفع لأجلها.

الحالة الثانية: الطرف الأخير غير موثوق، عندما يستلم هذا الطرف المنتج بصيغة رقمية فربما يقوم بنسخه أو بالتلاعب به بطرق مختلفة.

في الحالة الأولى يوجد ما يشبه العقد و الذي يحوي شروط استخدام المنتج، لكن هل سيقبل الزبون بهذا العقد؟ مثلاً قد نفرض عليه Video Player معين يمنع نسخ الملفات... و لكن هذا سيسبب الحد من خيارات الزبون في وقت يوجد فيه عالم من الخيارات غير المحدودة.

و في حال وصلت البيانات لطرف غير موثوق فإننا نكون قد فتحنا الباب لعمليات النسخ و التعديل. أحد هذه العمليات مثلاً التلاعب بملاحظات حقوق النشر المرئية وإزالتها عن المنتج.

كلا الحالتين تبدو غير مرضية و هنا يأتي دور Watermarking.

Digital Watermarking: تقنية سمحت للمالكين الأصليين بحفظ حقوق الملكية لأعمالهم و مؤلفاتهم عبر إضافة معلومات مخفية عن العين البشرية.

و بدمج هذه التقنية مع خدمات التعقب الجديدة التي تطرحها بعض الشركات أصبح من الممكن (نظرياً) تعقب كل النسخ غير القانونية للصور أو ملفات الموسيقا وغيرها... عبر الانترنت، و اتخاذ الإجراءات القانونية و القضائية المناسبة.و بهذا أصبح من الممكن تأمين بيئة مناسبة للإبداع و الابتكار مع ضمان عدم سرقة هذه الإبداعات.

3- تقنية العلامة المائية الرقمية Digital Watermark (Vidyasagar M. , 2005):

Digital Watermarking هي تقنية تسمح للمستخدم بإخفاء ملاحظات عن حقوق الملكية أو

رسائل إثبات في ملفات الصوت الرقمية أو ملفات الفيديو أو الصور أو الملفات النصية.

الرسالة المخفية عبارة عن مجموعة بتات تصف معلومات متعلقة بالبيانات الأصلية أو تتعلق

بمالك هذه البيانات (الاسم، العنوان، الشعار ...).

أخذت هذه التقنية اسمها من العلامة المائية التي توضع على ورقة أو على عملة ورقية و التي توضع كمقياس لمنع التزوير.

Digital Watermarking هي شكل من أشكال فن الإخفاء Data Hiding حيث يتم إخفاء معلومات ضمن الرسالة دون علم الطرف الذي سيستخدمها فيما بعد.

و إضافة هذه المعلومات المخفية لا تعيق استخدام البيانات الأصلية لكنها تزودنا بآلية لمعرفة المالك الأصلي و لمنع تزييف البيانات الأصلية (Johnson N. , 1999) .

4- أنواع Watermarking:

يوجد عدة تصنيفات لـ Watermark (Kwitt R. , 2009) نذكر منها:

- Visible watermark تكون العلامة ظاهرة للعين المجردة و مرئية.

- Invisible watermark تكون العلامة غير ظاهرة للعين، و عندما تكون ملكية البيانات في موضع مساءلة يتم إظهار الـ Watermark لتحديد مالكها الأصلي. و نحتاج لهذا النوع بسبب أن توزيع البيانات الرقمية أصبح يتم بسرعة أكبر و تطور التقنيات سمح بإنشاء نسخ طبق الأصل عنها.

و بعكس الـ Watermark المطبوعة على الورق و التي يجب أن تكون ظاهرة و واضحة فإن Watermark الرقمية ممكن أن تكون غير مرئية و في حالة الملفات الصوتية يجب أن تكون غير مسموعة بالنسبة للأذن البشرية (Gonzalez & Woods , 2007) .

5- متطلبات Watermarking:

تبعاً للتطبيق الذي يستخدم به الـ Watermark و الهدف منه تظهر متطلبات مختلفة و متعددة، لكن أشهر المتطلبات و التي يجب تحقيقها في كل التطبيقات هي:

Imperceptibility (الجاذبية): وهي من أكثر المتطلبات شيوعاً وهي مستقلة عن الغرض من التطبيق و المقصود بها أنه بعد إضافة الـ Watermark فإن دقة المحتوى الأصلي لا تتغير و تبقى التعديلات التي تحدث دون العتبة المحسوسة بحيث لا يتم إدراك وجودها.

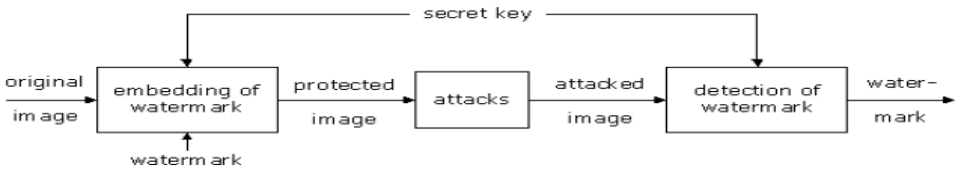
- Robustness (المتانة): و هي قدرة الـ Watermark على مقاومة التشويه الذي قد يطرأ على البيانات، سواء كان هذا التشويه لأسباب غير مقصودة أو بهدف التخريب و الأذى. و تعتبر المتانة ميزة من ميزات Watermark أكثر من كونها مطلباً، و لتحقيق هذه الميزة نستخدم التكرار (Redundancy) أي نكرر Watermark عدة مرات في الملف بحيث يصعب إزالتها كلها و نبقى قادرين على كشفها من أصغر جزء من البيانات (يجب أن تكون Watermark أصغر ما يمكن).
- Security(الأمن): تكون الـ Watermark آمنة في حال كانت الخوارزميات المستخدمة لتضمينها أو لكشفها من الملف الأصلي معروفة و مع ذلك لا يمكن لطرف غير مرخص كشف الـ Watermark أو إزالتها، و يتم تحقيق هذا المطلب باستخدام مفاتيح التشفير.
- Transparency(الشفافية): و تتعلق بحساسية العين البشرية و يقصد بها ألا تسبب Watermark ضياع في الدقة.
- Complexity (التعقيد): يقصد به الوقت و الجهد المطلوبين لتضمين Watermark ولاسترجاعها و هذه الخاصية مهمة جداً عند التعامل مع تطبيقات الزمن الحقيقي(Real-time).
- PayLoad (السعة): يقصد بها عدد بتات المعلومات التي يمكن إضافتها و تتعلق أيضاً بإمكانية تضمين أكثر من Watermark في نفس الملف وعلى التفرع) (Meerwald & Uhl , 2008 (Vidyasagar M. , 2005) .

6- كيف تعمل تقنية Watermarking ؟

تستخدم تقنية Watermarking حقيقة أن العين البشرية تملك قدرة محدودة على ملاحظة الاختلافات. لذا فإن تعديلات بسيطة على قيم لون ما في صورة مثلاً، تصحح لا شعوريا في العين لكي لا يلاحظ المراقب أي فرق.

العدد الواحد والعشرون
تاريخ الإصدار: 2 – تموز – 2020 م
www.ajsp.net
ISSN: 2663-5798

الشكل التالي يوضح مراحل تضمين Watermark (Nikola & Pitas , 2003):



الشكل (2) مراحل تضمين Watermark

يقوم صاحب البيانات الأصلية بإنشاء Watermark مناسبة و التي يمكن تضمينها ضمن البيانات و لضمان سرية الـ Digital Watermark المضمنة يستخدم مفتاح سري أو أكثر من مفاتيح التشفير. لإضافة Watermark للبيانات الأصلية يتم معالجة Watermark مع مفتاح public أو private بالإضافة للبيانات الأصلية باستخدام خوارزمية watermarking.

و لكشف الـ Watermark فإن الشخص المرخص له يحتاج فقط لـ Watermark أو البيانات الأصلية (حسب نوع نظام WM المستخدم)، مع وجود المفتاح المستخدم وبيانات الفحص، كل هذه المدخلات تعالج من قبل برنامج كشف Watermark لاستخلاصها (extract)، و يعطي مقياس ثقة بهذه البيانات (confidence measure)، هذا المقياس يحدد درجة قرب الـ Watermark الأصلية إلى الـ Watermark الناتجة عن عملية الكشف (Kwitt R. , 2009)

.(Liu & Dong 2007)

7- طرق تضمين العلامة المائية في الصور الرقمية: يمكن تصنيف هذه الطرق إلى قسمين:

أ. تضمين في المجال المكاني حيث تضاف العلامة المائية على الصورة مباشرة ويسمى هذا النوع بـ تعديل المطال mplitude modulation مثال على هذا النوع طريقة LSB التي تحمل العلامة المائية على البت الدنيا (Vidyasagar M.,2005). حديثاً تم استخدام البت العلوية MSB لتضمين العلامة المائية المرئية (Tsai & Chang,2010). تتصف طرق إضافة العلامة المائية في المجال المكاني بسهولة التحقيق ولكنها تعتبر هشة لا تقاوم الضجيج لعدة أنواع من الهجومات.

ب. من أجل الحصول على تقنيات أفضل, ظهرت طرق تعتمد إضافة العلامة المائية في مجالات التحويل. تم إضافة العلامة المائية باستخدام تحويل التجب المتقطع DCT (Vidyasagar M., 2005) (Liu & Dong,2007). كما تم إضافة العلامة المائية باستخدام تحويل الموجي المتقطع DWT (Kwitt & Meerwald,2008) حيث لاقى هذا التحويل إقبالاً واسعاً بسبب خاصية التحليل المتعدد الدقة.

العدد الواحد والعشرون
تاريخ الإصدار: 2 – تموز – 2020 م
www.ajsp.net
ISSN: 2663-5798

8- تقنية الإخفاء باستخدام الخانة الأقل أهميةLSB (Least Significant Bit):

سوف نستخدم هذه التقنية وهي من الطرق ذات التطبيق الواسع في الإخفاء، و عملية استخدام

هذه التقنية تعتمد على الخانة الأقل أهمية في بيكسل معين لتخزين المعلومة التي نريد إخفائها ضمن الصورة (Johnson N. , 1999) بعد استخدام خوارزميتنا المقترحة.

9- تقنية كشف الإخفاء Detection: توجد ثلاثة أنواع من الكشف وهي(Cox I. 2008):

9-1: الكشف الحسي (Sensational Detection): يعتمد على الحواس وهو نوعان:

1- الكشف البصري (Visual Detection): يصلح هذا النوع لكشف المواراة في ملفات الصور أو الفيديو، وذلك بالاعتماد على حاسة البصر في كشف أية تشوهات أو تغييرات تبدو

غير طبيعية في الصور أو عروض الفيديو.

2- الكشف السمعي (Auditory Detection): يصلح لكشف المواراة في ملفات الصوت،

وذلك بالاعتماد على حاسة السمع في كشف أي ضجيج أو خلل في تواترات الصوت أو في

شدته من الضروري عند اعتماد هذه الطريقة الانتباه لفروق بين الناس في رهافة قدراتهم الحسية.

9-2: الكشف البنيوي (Structural Detection):

تتغير في بعض الأحيان بنية الملف الحامل المستخدم للمواراة عند إخفاء معلومات فيه، و كشف

هذا التغير في بنية الملف يساعد في كشف المعلومات المخبأة.

9-3: الكشف الإحصائي (Statistical Detection):

في هذا النمط يتم الكشف عن المعلومات المخبأة عن طريق الصيغ والمعادلات الرياضية التي تساعد على تحديد وجود هذه المعلومات، بشكل عام تكون بنية الملف الحاوي على المعلومات السرية أكثر عشوائية من الملفات العادية.

تم استخدام عدة مقاييس للدراسة (Manmeet Gurmoha, 2011) وهي:

أ- متوسط مربع الخطأ(MSE) Mean Square Error :

متوسط مربع الخطأ يعطى بالعلاقة الرياضية التالية:

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(f_{ij}-g_{ij})^2$$

حيث: M,N : هما الصف والعمود بالنسبة للملف.

f_{ij} : هي الوحدة الصورية من ملف الغطاء.

g_{ij} : هي الوحدة الصورية من ملف المواراة.

ب- معدل الإشارة إلى الضجيج Signal to Noise Ratio (SNR) :

معدل الإشارة إلى الضجيج تمثل بقيمة محصورة بين 0 و100 و هي العلاقة بين ملف الغطاء W وملف المواراة $\hat{W}$ ويعطى بالعلاقة الرياضية التالية:

$$SNR(W,\hat{W}) = 10 \cdot log_{10} \cdot \frac{\sum_{i=1}^{N} W_i^2}{\sum_{i=1}^{N}(W_i - \hat{W}_i)^2}$$

ج- ذروة الإشارة إلى الضجيج Peak Signal to Noise Ratio(PSNR) :

ذروة الإشارة إلى الضجيج تمثل بقيمة محصورة بين 0 و100 وهي العلاقة بين ملف الغطاء $f(m,n)$ وملف المواراة $\tilde{f}(m,n)$ ويعطى بالعلاقة الرياضية التالية:

$$PSNR = 20 \cdot log_{10} \cdot \left[\frac{255}{RMSE}\right]$$

$$RMSE = \sqrt{\frac{1}{M \cdot N}\sum_{i=1}^{M}\sum_{j=1}^{N}\left[\tilde{f}(m,n) - f(m,n)\right]^2}$$

د- معامل الارتباط المعياري Normalized Correlation :

معامل الارتباط تمثل بقيمة محصورة بين 0 و1 وهي العلاقة بين ملف الغطاء W وملف المواراة $\hat{W}$ ويعطى بالعلاقة الرياضية التالية:

$$\rho(W,\hat{W}) = \frac{\sum_{i=1}^{N} W_i \hat{W}_i}{\sqrt{\sum_{i=1}^{N} W_i^2}\sqrt{\sum_{i=1}^{N} \hat{W}_i^2}}$$

10- طريقة العمل المقترحة Proposed Method:

تم الاعتماد على طريقة الخانة الأقل أهمية LSB بحيث يتم الإخفاء في البت الأقل أهمية، وبهذه الطريقة لا نستطيع تمييز الفرق بين الصورة مع العلامة المائية قبل وبعد الاخفاء بالعين

المجردة، قمنا بتقطيع ملف العلامة المائية المراد اخفائه و هذه القطع تم توزيعها بوضع القطع

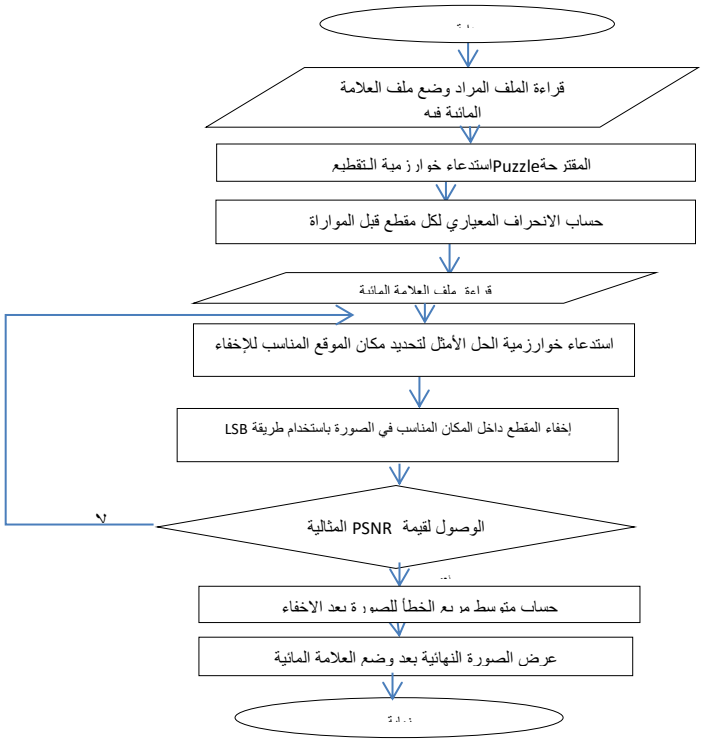
العدد الواحد والعشرون
تاريخ الإصدار: 2 – تموز – 2020 م
www.ajsp.net
ISSN: 2663-5798

في المكان المناسب بالاعتماد على طريقة الخريطة المقطعة (Elgamal & Mustafa , 2007)

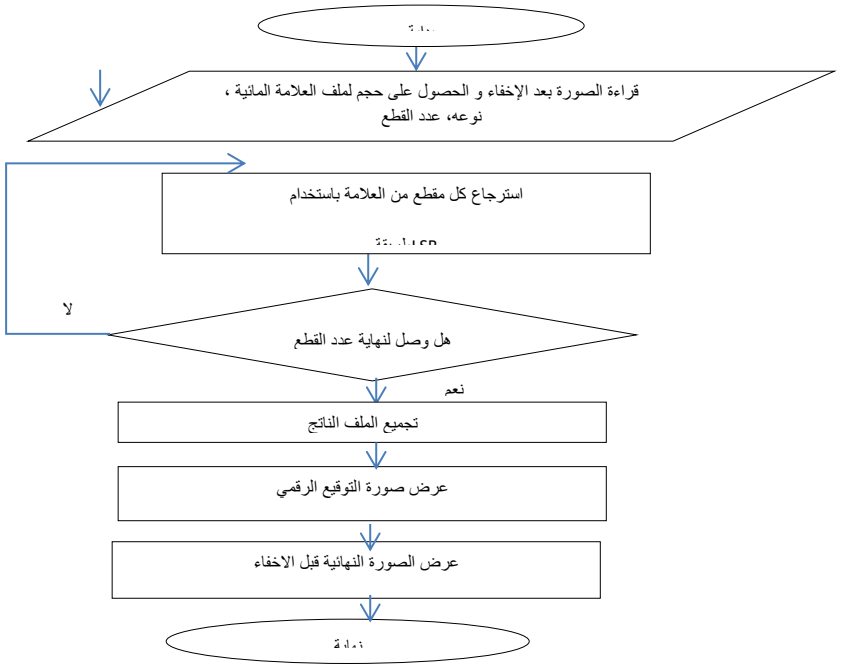
فيما يلي سوف نشرح تقنيتين تم استخدامهم في الخوارزمية المقترحة وهما تقنية المخزن الثنائي

Binary Store و تقنية تقطيع الملف Puzzle:

1- **تقنية المخزن الثنائي (Binary Store)** التي تهدف لتنظيم عملية تخزين البايتات ملف العلامة المائية المراد مواراته وسميت المخزن الثنائي كناية عن مصفوفة البايتات للملف العلامة المائية المراد مواراته بعد تحويله إلى بايتات و ذلك لتشكل هيكلية بناء خاصة يمكن من خلالها معرفة نوع ملف العلامة المائية المخزن وحجمه ورقم الصفحة في حال قمنا بتوزيعه على طريقة الخريطة المقطعة أي Puzzle و ذلك لإعادة تجميعه لاحقاً. فيما يلي مخطط الكتابة و القراءة للمخزن الثنائي لملف العلامة المائية المراد إخفائه في الشكلين (3 و 4)



الشكل (3) مخطط خوارزمي كتابة المخزن الثنائي Binary Store Write



الشكل (4) مخطط خوارزمي قراءة المخزن الثنائي Binary Store Read

بناء على المخطط السابق الخوارزمية المقترحة تعتمد على الإجرائيين الأساسيين التاليتين:

أ- **إجرائية الجمع Compile:** تعتمد هذه الاجرائية على تجميع أجزاء المخزن الثنائي بعد إعطائه البارامترات اللازمة لملف وهي اسم الملف وحجمه و بالتالي يعطينا مصفوفة بايتات فيها جميع خصائص الملف المخزن.

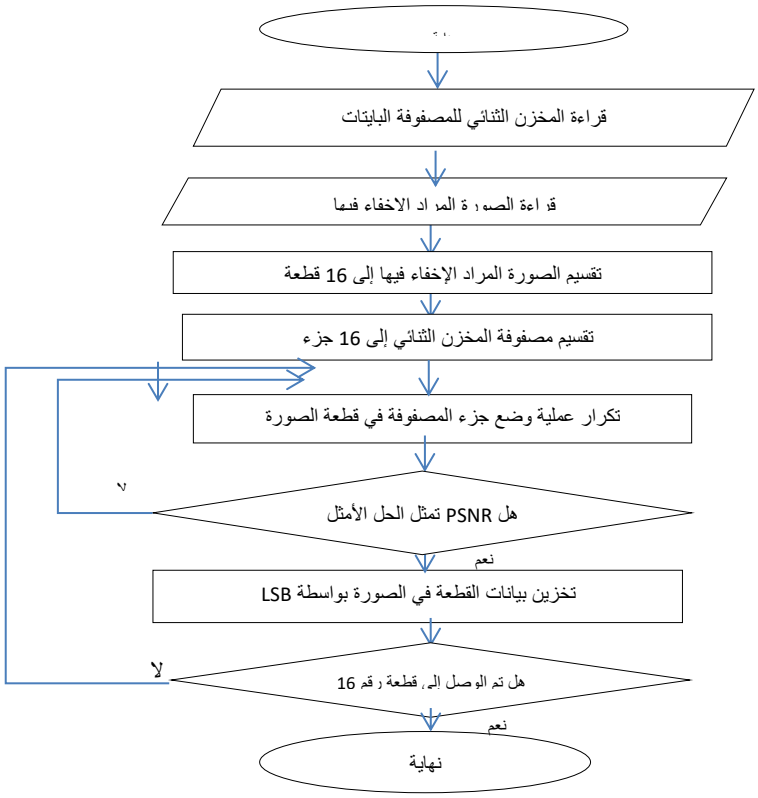
ب- **إجرائية الاستخراج Extract:** تعتمد هذه الإجرائية على استخراج خصائص الملف المخزن وهي نوعه و حجمه (Gurpreet & Supriya , 2013).

2- **تقنية تقطيع الملف Puzzle** : الإخفاءباستخدام تقنية البت الأقل أهمية LSB القياسية

حسب الطرق السابقة للباحث اليزوكا(EL-Zouka,H.) وطريقة الباحث هاشينك (sing,C) تسمح بإخفاء البايتات ببساطة دون تحديد لمكان المواراة أما الطريقة المقترحة في بحثنا عملية الإخفاء تعتمد على استخدام تقنية الإخفاء بشكل أمثل أي تحديد المكان الأمثل بعد تقطيع ملف العلامة المائية المراد إخفائه إلى أجزاء و كذلك تقسيم الصورة المراد الإخفاء فيها إلى قطع بالاعتماد على خريطة التقطيع ومن ثم اختيار المكان الأمثل أي القسم الأقل تضرراً في الصورة المستهدفة، بحث تكون PSNR أفضل في القسم الذي ستحفظ فيه البايتات وتختلف هذه الخريطة باختلاف المحتوى نفسه أي كلما تم تغيير المحتوى تتغير طريقة التوزيع.

يمثل الشكل (6) مخطط عمل خريطة التقطيع Puzzle يتم قراءة بايتات ملف العلامة المائية المراد إخفائه التي تم الحصول عليها من تقنية المخزن الثنائي و وضعه في مصفوفة ثم نقوم بقراءة الصورة المراد الإخفاء فيها و نقوم بتقسيم الصورة إلى 16 قطعة و كذلك تقسيم المصفوفة إلى 16 جزء بعد ذلك يتم تحديد كل جزء من المصفوفة في الموقع الأمثل من الصورة و ذلك من خلال الحصول على PSNR الأفضل (Hajjara S. , 2009) .

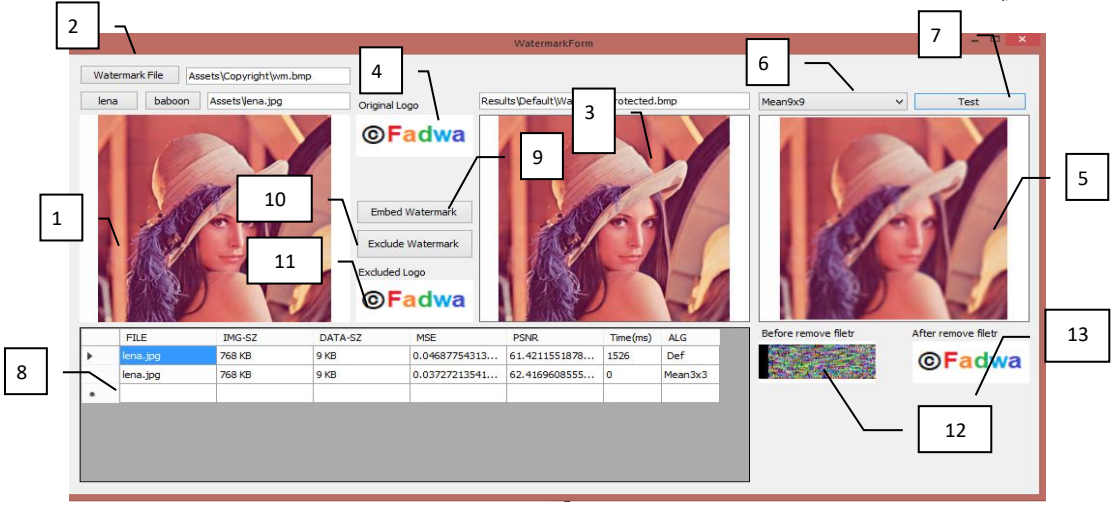
العدد الواحد والعشرون
تاريخ الإصدار: 2 – تموز – 2020 م
www.ajsp.net
ISSN: 2663-5798



الشكل (5) مخطط خوارزمي عمل خريطة التقطيع Puzzle

11- طريقة العمل على الخوارزمية المقترحة:

يوضح الشكل (6) تنفيذ الخوارزمية المقترحة باستخدام بيئة فيجول استديو اصدار 2016 على حاسب شخصي معالجه Cor i5 و ذاكرة 8 غيغا بايت، تم اختبار الخوارزمية المقترحة على ملفات صور Lena و Baoon و أي ملف نريد مع مقارنتها مع الطريقة القياسية للموراة بتقنية LSB.



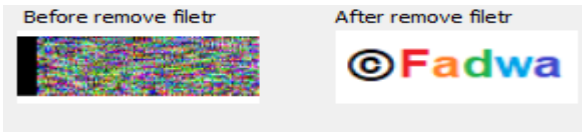
الشكل (6) واجهة تصميم عمل الخوارزمية المقترحة منفذة بيئة فيجول استوديو

العدد الواحد والعشرون
تاريخ الإصدار: 2 – تموز – 2020 م
www.ajsp.net
ISSN: 2663-5798

11-1 شرح المخطط :

في الشكل السابق الصورة رقم (1) تمثل الصورة الأصلية التي نريد الإخفاء فيها والصورة رقم (2) تمثل اسم الملف المراد الإخفاء فيه أي ملف نريد من خلال اختياره أما الصورة رقم (3) تمثل الصورة الناتجة مع ملف العلامة المائية التي تم إخفائه والصورة رقم (4) تمثل ملف العلامة المائية والصورة رقم (5) تمثل الصورة الناتجة مع العلامة المائية بعد تطبيق هجوم عليها والصورة رقم (6) تمثل أنواع الهجومات التي يمكن تطبيقها على الصورة التي تحوي العلامة المائية و الصورة رقم (7) تمثل زر الهجوم على الصورة حسب نوع المختار من القائمة والصورة رقم (8) تمثل نتائج تنفيذ الخوارزمية والصورة رقم (9) تمثل تنفيذ الإخفاء حسب الطريقة المقترحة والصورة رقم (10) تنفيذ استخراج العلامة المائية حسب الطريقة المقترحة الصورة رقم (11) تمثل العلامة المائية المستخرجة من الصورة والصورة رقم (12) تمثل العلامة المائية بعد تنفيذ الهجوم، الصورة رقم (13) تمثل العلامة المائية بعد تنفيذ الهجوم بعد إزالة الفلتر. بعض الصور في الشكل السابق غير واضحة سيتم توضيح الصورة ذات الأرقام (5 و 6 و 7 و 12 و 13) لأهميتها عملية الهجوم.

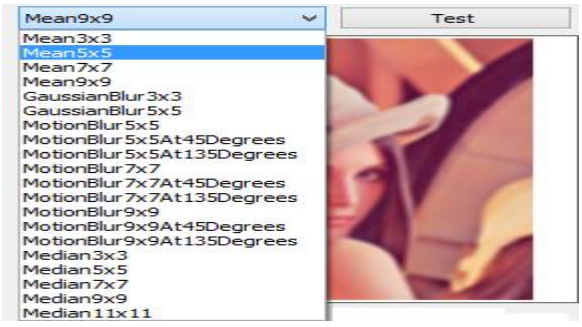
11-2 العلامة المائية : يمثل القسم (12 و 13):



الشكل (7) العلامة المائية مع الهجوم قبل ازالة الفلتر و بعد ازالة الفلتر

الجزء اليساري يمثل العلامة المائية بعد تنفيذ الهجوم قبل إزالة الفلتر التي تم استخراجها من الصورة التي تم الإخفاء فيها هذه العلامة المائية أو الجزء اليميني يمثل العلامة المائية بعد تنفيذ الهجوم بعد إزالة الفلتر التي تم استخراجها من الصورة التي تم الإخفاء فيها هذه العلامة المائية.

11-3 الهجوم: يمثل القسمين (5 و 6 و 7)



الشكل (8) أنواع الهجوم التي يمكن تنفيذها على الصورة

العدد الواحد والعشرون
تاريخ الإصدار: 2 – تموز – 2020 م
www.ajsp.net
ISSN: 2663-5798

الجزء اليساري يمثل أنواع الهجومات التي يمكن تطبيقها على الصورة التي تحوي العلامة المائية اليسار أو الجزء اليميني يظهر كيف تم تطبيق الهجوم على الصورة و كيف اصبحت بعد تنفيذ أي هجوم بعد ضغط على زر.

4-11 نتائج التنفيذ: يمثل القسم (8):

بعد تنفيذ البرنامج يتم اختيار اسم ملف المراد الإخفاء فيه من خلال الضغط على الزر Watermark File يتم اختيار أي ملف نريد وضع علامة مائية له و هي الشعار الموجود في الصورة رقم (4) و يوجد زرين وهما لصور ثابتة حيث تم اختبار صورتين وهما Lena و Baboon بعد ذلك نضغط على الزر Embed Watermark فتظهر النتائج في جدول عبارة عن اسم ملف الذي تمت الإخفاء فيه و حجمه و حجم بيانات ملف المراد مواراته ثم يتم حساب كلاً من : MSE و PSNR و زمن التنفيذ و نوع الهجوم المنفذ على الصورة، الجدول (1) يمثل نتائج الإخفاء بالطريقة القياسية و الطريقة المقترحة بخوارزميتنا مع تنفيذ عدة هجومات على الصورة التي تحتوي العلامة المائية المقترحة من أجل الصورة Lena.jpg.

File	Size	Data	MSE	PSNR	Alg
lena.jpg	768 KB	9 KB	0.0468775431315104	61.4211551878766	Def
lena.jpg	768 KB	9 KB	0.0372721354166667	62.4169608555148	Mean3x3
lena.jpg	768 KB	9 KB	0.0346946716308594	62.7281757942007	Mean5x5
lena.jpg	768 KB	9 KB	0.0327987670898438	62.9722284203858	Mean7x7
lena.jpg	768 KB	9 KB	0.031646728515625	63.1275153943859	Mean9x9
lena.jpg	768 KB	9 KB	0.040740966796875	62.0304903012703	GaussianBlur3x3
lena.jpg	768 KB	9 KB	0.0350240071614583	62.6871452784262	GaussianBlur5x5
lena.jpg	768 KB	9 KB	0.0296249389648438	63.4142289660954	MotionBlur5x5
lena.jpg	768 KB	9 KB	0.0364507039388021	62.5137444100444	MotionBlur5x5At45Degrees
lena.jpg	768 KB	9 KB	0.03692626953125	62.4574492551118	MotionBlur5x5At135Degrees
lena.jpg	768 KB	9 KB	0.029687245686849	63.4051045422811	MotionBlur7x7
lena.jpg	768 KB	9 KB	0.0347124735514323	62.7259479901262	MotionBlur7x7At45Degrees
lena.jpg	768 KB	9 KB	0.0348040262858073	62.7145087288219	MotionBlur7x7At135Degrees
lena.jpg	768 KB	9 KB	0.0293858846028646	63.4494159206012	MotionBlur9x9
lena.jpg	768 KB	9 KB	0.0334294637044271	62.8895095143287	MotionBlur9x9At45Degrees

lena.jpg	768 KB	9 KB	0.0331738789876302	62.9228410477114	MotionBlur9x9At135Degrees
lena.jpg	768 KB	9 KB	0.0970751444498698	58.2597231540996	Median3x3
lena.jpg	768 KB	9 KB	0.193364461263021	55.2670370340439	Median5x5
lena.jpg	768 KB	9 KB	0.268971761067708	53.8337367438311	Median7x7
lena.jpg	768 KB	9 KB	0.364087422688802	52.5187468427177	Median9x9
lena.jpg	768 KB	9 KB	0.411692301432292	51.9850761501868	Median11x11

الجدول (1) نتائج الخوارزمية المقترحة لإخفاء العلامة المائية لصورة lena.jpg

يتم إعادة تنفيذ ما سبق و لكن بتغيير الصورة فتظهر النتائج في جدول رقم (2) يمثل نتائج الإخفاء بالطريقة القياسية و الطريقة المقترحة بخوارزميتنا مع تنفيذ عدة هجومات على الصورة التي تحتوي العلامة المائية المقترحة من أجل الصورة Baboon.jpg.

File	Size	Data	MSE	PSNR	Alg
baboon.jpg	55 KB	9 KB	0.0470682779947917	61.4035205104739	Def
baboon.jpg	55 KB	9 KB	0.0375111897786458	62.3891952156107	Mean3x3
baboon.jpg	55 KB	9 KB	0.0347709655761719	62.7186360982858	Mean5x5
baboon.jpg	55 KB	9 KB	0.0328025817871094	62.971723338706	Mean7x7
baboon.jpg	55 KB	9 KB	0.0318590799967448	63.0984713046074	Mean9x9
baboon.jpg	55 KB	9 KB	0.0405082702636719	62.0553666201858	GaussianBlur3x3
baboon.jpg	55 KB	9 KB	0.0352999369303385	62.6530643142429	GaussianBlur5x5
baboon.jpg	55 KB	9 KB	0.0294596354166667	63.4385299302218	MotionBlur5x5
baboon.jpg	55 KB	9 KB	0.0369962056477865	62.4492317600981	MotionBlur5x5At45Degrees
baboon.jpg	55 KB	9 KB	0.0368372599283854	62.4679304233547	MotionBlur5x5At135Degrees
baboon.jpg	55 KB	9 KB	0.0297228495279948	63.3998991799468	MotionBlur7x7
baboon.jpg	55 KB	9 KB	0.0347480773925781	62.7214958074446	MotionBlur7x7At45Degrees
baboon.jpg	55 KB	9 KB	0.0347913106282552	62.716095714449	MotionBlur7x7At135Degrees
baboon.jpg	55 KB	9 KB	0.029839833577474	63.3828396420489	MotionBlur9x9
baboon.jpg	55 KB	9 KB	0.0332552591959635	62.9122002373494	MotionBlur9x9At45Degrees
baboon.jpg	55 KB	9 KB	0.0332361857096354	62.9146918391192	MotionBlur9x9At135Degrees

baboon.jpg	55 KB	9 KB	0.113043467203776	57.5983489139422	Median3x3
baboon.jpg	55 KB	9 KB	0.297813415527344	53.3913610345488	Median5x5
baboon.jpg	55 KB	9 KB	0.625255584716797	50.1702278137564	Median7x7
baboon.jpg	55 KB	9 KB	1.03094863891602	47.9984333126915	Median9x9
baboon.jpg	55 KB	9 KB	1.62504704793294	46.0221442179186	Median11x11

الجدول (2) نتائج الخوارزمية المقترحة لإخفاء العلامة المائية لصورة Baboon.jpg

يتم إعادة تنفيذ ما سبق و لكن بتغيير الصورة فتظهر النتائج في جدول رقم (3) يمثل نتائج الإخفاء بالطريقة القياسية و الطريقة المقترحة بخوارزميتنا مع تنفيذ عدة هجومات على الصورة التي تحتوي العلامة المائية المقترحة من أجل الصورة ab.jpg.

File	Size	Data	MSE	PSNR	Alg
ab.jpg	127 KB	9 KB	0.0178028549382716	65.6259070774352	Def
ab.jpg	127 KB	9 KB	0.0136241319444444	66.7877151991904	Mean3x3
ab.jpg	127 KB	9 KB	0.0122622492283951	67.2451022201612	Mean5x5
ab.jpg	127 KB	9 KB	0.0119150270061728	67.3698532982802	Mean7x7
ab.jpg	127 KB	9 KB	0.0114091435185185	67.5582731760154	Mean9x9
ab.jpg	127 KB	9 KB	0.0143764467592593	66.5542880051864	GaussianBlur3x3
ab.jpg	127 KB	9 KB	0.0123109567901235	67.2278855387296	GaussianBlur5x5
ab.jpg	127 KB	9 KB	0.0109206211419753	67.7483302003943	MotionBlur5x5
ab.jpg	127 KB	9 KB	0.0128288966049383	67.0489105593442	MotionBlur5x5At45Degrees
ab.jpg	127 KB	9 KB	0.0130116705246914	66.9874730311638	MotionBlur5x5At135Degrees
ab.jpg	127 KB	9 KB	0.0108897569444444	67.7606217430447	MotionBlur7x7
ab.jpg	127 KB	9 KB	0.0120683834876543	67.3143125890705	MotionBlur7x7At45Degrees
ab.jpg	127 KB	9 KB	0.0121397569444444	67.2887036924756	MotionBlur7x7At135Degrees
ab.jpg	127 KB	9 KB	0.010697337962963	67.8380464410166	MotionBlur9x9
ab.jpg	127 KB	9 KB	0.0115060763888889	67.5215310788599	MotionBlur9x9At45Degrees
ab.jpg	127 KB	9 KB	0.0115340470679012	67.5109864152946	MotionBlur9x9At135Degrees
ab.jpg	127 KB	9 KB	0.0193774112654321	65.2578460405789	Median3x3

العدد الواحد والعشرون
تاريخ الإصدار: 2 – تموز – 2020 م
www.ajsp.net
ISSN: 2663-5798

ab.jpg	127 KB	9 KB	0.0226374421296296	64.5825300777504	Median5x5
ab.jpg	127 KB	9 KB	0.0251253858024691	64.1296762175889	Median7x7
ab.jpg	127 KB	9 KB	0.0260185185185185	63.9779779644978	Median9x9
ab.jpg	127 KB	9 KB	0.0279827353395062	63.6619019593045	Median11x11
ab.jpg	127 KB	9 KB	0.0136241319444444	66.7877151991904	Mean3x3

الجدول (3) نتائج الخوارزمية المقترحة لإخفاء العلامة المائية لصورة ab.jpg

12- الفرق بين الطريقة المقترحة والطريقة الواردة في المرجع(Hajjara S. , 2009) :

1- الطريقة المقترحة تستخدم فلاتر موجودة بالشكل (8) بينما الطريقة الواردة في المرجع(Hajjara S, 2009) تستخدم فلاتر محددة.

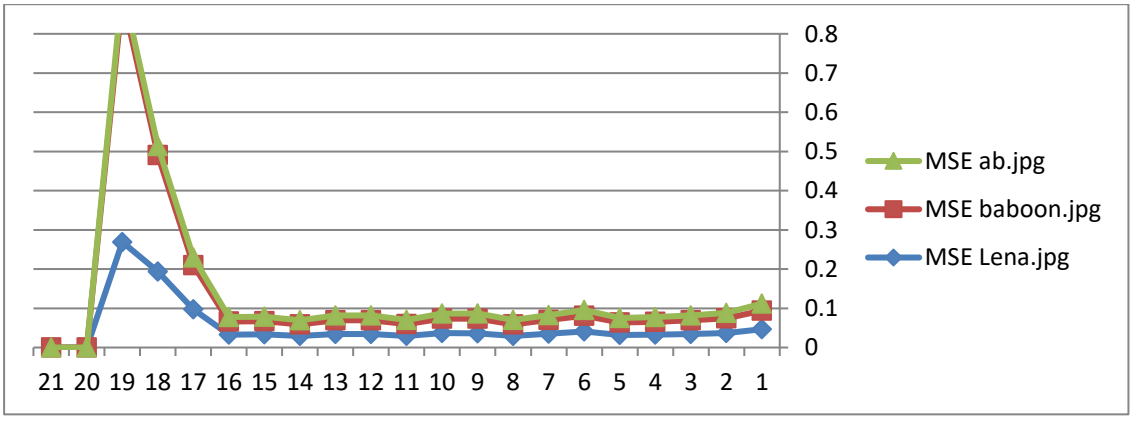
2- الطريقة الواردة في المرجع(Hajjara S, 2009) تضمن العلامة المائية عن طريق توليد ضجيج عشوائي (pseudo-random noise) للنقاط التي تقابل معالم الصورة foreground. بينما في الطريق المقترحة التضمين في الأماكن التي تقلل التشويه أقل ما يمكن.

3- في مرحلة الاستخراج نحتاج إلى الصورة المضيفة والصورة المتضمنة للعلامة المائية بينما في الطريقة الواردة في المرجع (Hajjara S, 2009) نحتاج فقط إلى الصورة المتضمنة للعلامة المائية.

13- نتائج البحث Research Results:

13-1 من خلال حساب MSE:

من خلال النتائج بالجدولين (1) و (2) و (3) يتضح أن الخوارزمية المقترحة الحصول على قيمة أعلى لمتوسط مربع الخطأ MSE والتي يمكن مقارنتهما معاً من خلال المخطط البياني رقم (1) لكل صور.



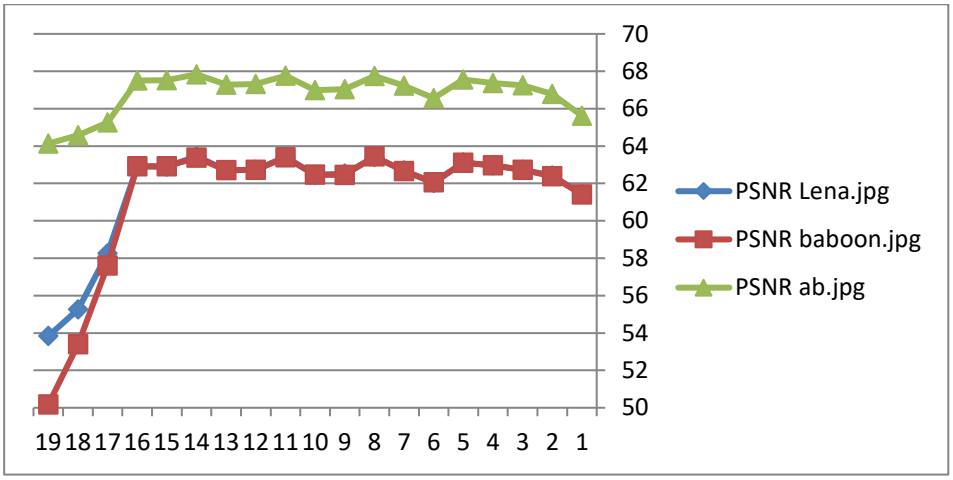
مخطط(1) متوسط مربع الخطأ MSE للصور الثلاثة مقارنة مع القيمة الافتراضية

بالمقارنة مع النتائج نلاحظ:

ارتفاع قيمة متوسط مربع الخطأ MSE بعد تطبيق للخوارزمية المقترحة كما هو موضح بالجداول رقم (1 و 2 و 3).

13-2 من خلال حساب PSNR:

من خلال النتائج بالجدولين (1) و (2) و (3) يتضح أن الخوارزمية المقترحة تقوم بتحسين قيمة معدل طاقة الإشارة إلى الضجيج PSNR ليكون الحل الأمثل والتي يمكن مقارنتهما معاً من خلال المخطط البياني رقم (2) لكل صور.



مخطط(2) معدل طاقة الإشارة إلى الضجيج للصور الثلاثة مقارنة مع القيمة الافتراضية

بالمقارنة مع النتائج نلاحظ:

انخفاض ذروة الإشارة إلى الضجيج PSNR يعني أن متوسط الخطأ بين الصورة الأصلية والصورة التي أعيد بناؤها منخفض جدًا. وهذا يعني أنه تم استعادة بشكل صحيح. من ناحية أخرى فإن جودة الصورة المستعادة أفضل رغم تعرضها لهجوم.

13-3 مقاومة الهجومات:

تم استخدام الصورة المضيفة lena.jpg(768 kb) الشكل (9).

الشكل (9) الصورة المضيفة lena.jpg

العدد الواحد والعشرون
تاريخ الإصدار: 2 – تموز – 2020 م
www.ajsp.net
ISSN: 2663-5798

العلامة المائية صورة (9 kb) wm.bmp الشكل (10).

الشكل (10) العلامة المائية

وكذلك تم استخدام الصورة المضيفة (55 kb)baboon.jpg الشكل (11).

الشكل (11) الصورة المضيفة baboon.jpg

وكذلك تم استخدام الصورة المضيفة (127 kb)ab.jpg الشكل (12)

الشكل (12) الصورة المضيفة ab.jpg

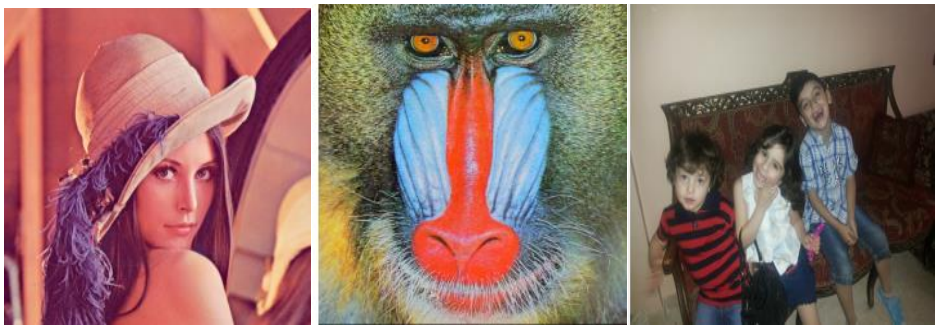
تم تعريض الصورة المتضمنة للعلامة المائية بالطريقة المقترحة و بالطريقة الواردة بالمرجع(Hajjara S, 2009) لعدة هجمات: ضجيج من النوع Gaussian(0,0.0001) و ضجيج من النوع Salt& pepper(0.01). تم حساب PSNR ليوضح العلاقة بين الصورة المتضمنة للعلامة المائية والصورة المتضمنة للعلامة المائية المضجة، وحساب PSNR ليوضح العلاقة بين العلامة المائية المضمنة والعلامة المائية المستخرجة. وحصلنا على نتائج الطريقة المقترحة الموضحة بالجداول(1 و 2 و 3) ونتائج الطريقة الواردة

العدد الواحد والعشرون
تاريخ الإصدار: 2 – تموز – 2020 م
www.ajsp.net
ISSN: 2663-5798

بالمرجع(Hajjara S, 2009) الفروقات بين الطريقتين حيث نلاحظ أن طريقتنا المقترحة أفضل من الطريقة الواردة في المرجع (Hajjara S, 2009).

13-4 أثر الصورة المضيفة:

لتقييم الطريقة المقترحة تم استخدام عدة صور مضيفة من النوع jpg و حجوم متساوية منها موضحة في الشكل (13) وتم تضمين كل منها العلامة المائية السابقة الشكل (10).



lena.jpg baboon.jpg ab.jpg

الشكل (13) أثر الصور المضيفة

تم تعريض الصور المتضمنة العلامة المائية لهجمات متعددة تبين أن الطريقة المقترحة تعمل بشكل جيد بالنسبة للصور من نفس الحجم.

13-4 أثر العلامة المائية:

تم استخدام علامة مائية أخرى توقيع بحجم 9 kb من النوع bmp وتم تعريض الصورة المتضمنة العلامة المائية إلى هجمات متنوعة وحصلنا على النتائج التالية الشكل (14):

lena.jpg baboon.jpg ab.jpg

الشكل (14) العلامة المائية المستخرجة بعد تعرضها لهجمات مختلفة

نلاحظ كلما ازداد حجم الملف المضيف للعلامة المائية كلما نقص التشويه في الصورة المتضمنة للعلامة المائية وبالتالي ازداد قدرته على المقاومة الهجمات.

14- الخاتمة والتطورات المستقبلية Conclusion and future developments:

قدمنا في هذا البحث خوارزمية جديدة لتضمين العلامة المائية باستخدام تقنية LSB المطورة و لتقييم هذه الطريقة قمنا بتحقيقها باستخدام بيئة فيجول استديو 2016 وتعاملنا مع صور من النوع من أي نوع. تتميز هذه الطريقة بالمتانة ومقاومتها للعديد من الهجمات، كما قدمنا دراسة عن أثر الصورة المضيفة وأثر العلامة المائية.

وفي المستقبل تطبيق الخوارزمية المقترحة على وسائط أخرى مثل ملفات الصوت والفيديو.

15- المراجع:

.Johnson N. (1999) An Introduction to Watermark Recovery from Images, held in San Diego, February9-13

(Et Al.) (2005) A Survey of Digital Image Watermarking Techniques",3rd, International .Vidyasagar M Conference on Industrial Informatics(INDIN),IEEE.

.(Et Al.)(2008)Digital Watermarking and Steganography",(Second Edition), Morgan Kaufmann .Cox I

(Et Al.)(2009)Color-Image Watermarking Using Multivariate Power-Exponential Distribution, IEEE. .Kwitt R

Meerwald P. & Uhl A. (2008) Scalability evaluation of blind spread spectrum image watermarking, Springer Verlag.

Kwitt R. & Meerwald P.(2008) A Lightweight Rao-Cauchy Detector for Additive Watermarking in the DWT-Domain,Vol.8,P22–23.

Liu W& Dong L.(2007) Optimum detection for spread-spectrum watermarking that employs self-masking. IEEE Transactions on Information Forensics and Security,Vol.2(4),P645–654.

Nikola A. & Pitas I.(2003) Asymptotically optimal detection for additive watermarking in the DCT and DWT domains, IEEE Transactions on Image Processin,Vol.12(5),P563–571.

Merhav N. & Sabbag E.(2008) Optimal watermark embedding and detection strategies under limited detection resources, IEEE Transactions on Information Theory,Vol.54(1),P255–274.

Gonzalez R. & Woods R.(2007) Digital Image Processing, Prentice Hall, USA.

Tsai H. & Chang L.(2010) Secure reversible visible image watermarking with authentication, Signal Processing: Image Communication,Vol.25,P10-17.

Hajjara S. (Et Al) (2009) Digital Image Watermarking Using Localized Biothogonal Wavelets, European Journal Of Scientific Research,Vol.26,P594-608.

& Mustafa A.(2007) A Proposed Algorithm For Steganography In Digital Image Based on Least .Elgamal A 2,P752–767..Significant Bit, Research Journal Specific Education, Vol
Gurpreet S. & Supriya A.(2013)A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security, International Journal of Computer Applications, Vol.67,P33-38.

العدد الواحد والعشرون
تاريخ الإصدار: 2 – تموز – 2020 م
www.ajsp.net
ISSN: 2663-5798

Manmeet K. & Gurmohan S.(2011) Comparison of Tacit Encryption Algorithm With Various Encryption Algorithms, International Journal of Electronics and Computer Science Engineering, Vol.1,P741-750.

"An Algorithm Developed For the Watermark Using the Cut Map"

Author: Fadwa A. Safiah[(1)] ;

Supervisor: Dr Z. Zakriah[(1)] and Dr N. Abo Salah[(2)]

1- Department of Mathematics -Faculty of Science -University of AL-Baath

2- Department of Fundamental Sciences, Faculty of Engineering, University of AL-Baath

Abstract:

With the advent of the Internet, you can compose digital media by distributing their works by making them available on web pages or public discussion forums. A person who has the authority to access pages or forums can copy and modify these media and obtain a copy that is completely identical to the original. The use of digital media for multiple problems including how authors can guarantee the property rights of their works. The multimedia was included with additional information to protect the media before it was distributed.

In this paper, a new method has been proposed to include the watermark in images of any kind. An improved algorithm has been proposed which breaks the data of the watermark (Datas) into blocks (Blokes) with the technique of cutting the map. Then the LSB (Least Bit Bit) algorithm was applied for masking. For better results, the whale algorithm was used to determine the optimal placement of concealment.

The effectiveness of the algorithm comes from obtaining the optimum value of peak signal-to-noise (PSNR) (peak-to-noise ratio), thereby determining the best location for concealment, as well as the value of the mean square error MSE (mean square error). And compare the results between the LSB algorithm by standard methods and our stated algorithm.
The results obtained are indicative of the efficiency and robustness of the algorithm, as it is characterized by its durability due to its resistance to many attacks carried out on the image.

It was adopted on the Visual Studio 2016 environment because it contains highly efficient functions dealing with the proposed algorithm.

Keywords: - Least - Binary Store - Puzzle - Mean Watermark - Digital imagery - Steganography- Significant Bit Square Error - Peak Signal to Noise Ratio.