مجلة جامعة تشرين للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (40) العدد (3) 2018
Tishreen University Journal for Research and Scientific Studies - Engineering Sciences Series Vol. (40) No. (3) 2018

بناء مخطط مصادقة الصور الرقميّة
باستخدام تقنيات إخفاء المعلومات و البعثرة الادراكية

د. رياض ضاهر *
إيهاب عيسى صالح **

(تاريخ الإيداع 24 / 9 / 2017. قُبِل للنشر في 30/ 4 / 2018)

□ ملخّص □

اكتسبت تقنيات التوثيق للصور الرقمية في الآونة الأخيرة اهتماما كبيرا نظرا لأهميتها بالنسبة لعدد كبير من تطبيقات الوسائط المتعددة، و بشكل عام تنتقل الصور الرقمية عبر أوساط غير آمنة كالأنترنت و شبكات الحواسيب بأنواعها المختلفة، و قد يتطلب التطبيق وجود تأمين مستوى عال من الأمن مثل التطبيقات العسكرية و الطبية و بالتالي يجب أن تكون الصور محمية ضد محاولات تعديل محتواها، مثل هذه التعديلات قد تؤدي إلى التأثير على القرارات المرتبطة بهذه الصور.

تم في هذا البحث اقتراح مخططاً عاماً لضمان امن تبادل الصور الرقمية المتبادلة بالاعتماد على تقنيات إخفاء المعلومات(التورية) و البعثرة الادراكية الصور الرقمية و في مرحلة الاختبار النهائي تم دراسة مدى مقاومة المخطط المقترح لعمليات التعديل مثل تطبيق ضغط الصورة وفق مستويات مختلفة و تغيير مستوى التباين و السطوع للصورة، و تم الاعتماد على حساب نسبة التطابق بين بتات شعاع البعثرة الأصلي للصورة وبتات شعاع البعثرة الذي تم تضمينه بها من أجل تحليل نتائج الاختبارات المطبقة، و بالمحصلة حصلنا على نسبة تطابق شبه مثالية حتى بعد تطبيق ضغط الصورة أو تغيير مستوى السطوع لها(ما يقارب 99.9%)، بينما انخفضت نسبة التطابق بشكل ملحوظ مع زيادة مستوى التباين للصورة(ما يقارب 94%).

الكلمات المفتاحية :التورية، التوقيع الرقمي، البعثرة الادراكية للصورة، البعثرة الكريبتوغرافية، المجال الترددي

* **أستاذ مساعد، قسم هندسة الحاسبات و التحكم الآلي، كلية الهندسة الميكانيكية و الكهربائية، جامعة تشرين، اللاذقية، سورية**
** **طالب دراسات عليا(ماجستير هندسة حاسبات)، قسم هندسة الحاسبات و التحكم الآلي، كلية الهندسة الميكانيكية و الكهربائية، جامعة تشرين، اللاذقية، سورية.**

مجلة جامعة تشرين للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (40) العدد (3) 2018
Tishreen University Journal for Research and Scientific Studies - Engineering Sciences Series Vol. (40) No. (3) 2018

Building Scheme Of Digital Image Authentication Using Steganography & Perceptual Hashing Techniques

[*]Dr. Reyad Daher
[**] Ehab Issa Saleh

(Received 24 / 9 / 2017. Accepted 30 / 4 / 2018)

□ ABSTRACT □

Recently، digital image authentication technologies have gained much attention because of their importance in many multimedia applications. In general digital images are transmitted over unsaved media such as the internet and many types of computer networks. Applications may require a large amount of safety such as military applications and medical applications. Therefore the digital images must be protected against any modifications، which may lead to influence the decisions that associated with them.
In this paper، a general scheme based on Steganography & Perceptual Image Hashing techniques was proposed to enhance the security of digital image transmission. In the final test stage, we checked the accuracy of the proposed scheme against potential modifications was studied, by applying different levels of compression and changing the contrast & brightness level of the image. For analyzing the final results, we computed the matching ratio between the original hash vector and the embedded hash vector. As a result، we achieved a near perfect match ratio even after applying the image compression level or changing its brightness level (approximately 99.9%), while the match ratio decreased significantly with the increase of the contrast level of the image (approximately 94%).

Keywords:
Steganography، Digital Signature, Perceptual Image Hashing, Cryptographic Hashing، Frequency Domain

[*] **Associated Prof ،Department Of Computers And Automatic Control Engineering، Faculty Of Mechanical And Electrical Engineering، Tishreen University، Lattakia، Syria.**
[**] **Postgraduate Student(Master In Computers Engineering)، Department Of Computers And Automatic Control Engineering، Faculty Of Mechanical And Electrical**

مقدمة:

يحاكي التوقيع الرقمي التوقيع اليدوي المنفذ بواسطة قلم الحبر على الوثائق الورقية، بينما يتم توليد التوقيع الرقمي بواسطة الوسائل الالكترونية المتعددة مثل الحواسيب و أجهزة الهاتف المحمول. إن التوقيع الرقمي عبارة عن ترميز ناتج عن تنفيذ توابع رياضية على ملف معين و من ثم يتم عملية الحاق الترميز بالملف و إرساله و تستخدم من قبل المستقبل للبرهان على أصالة و موثوقية و صحة الرسالة المرسلة مما يعطي المستقبل سبباً في الاعتقاد ان الرسالة صحيحة و أن المرسل لا يمكنه انكار إرسالها أو أنها لم يتم تعديلها أو تغييرها أثناء الارسال، و تعتبر عملية تزوير التوقيع الرقمي أصعب من تزوير التوقيع اليدوي.

يستخدم التوقيع الرقمي بشكل عام من أجل تصديق الرسائل ذات القيمة المادية او المعنوية مثل تصديق الفواتير و الأرصدة المصرفية و يمكن استعمالها لتوزيع الحزم البرمجة أو البريد الالكتروني و كشف حالات التزوير أو وجود تعديل للبيانات من قبل أشخاص غير مخولين أو وسائل غير معروفة.

يمكن مصادقة الرسالة و التحقق من وصولها سليمة بعدة طرق، منها[7]:

1- طريقة المصادقة بواسطة التشفير بالمفتاح المتناظر.
2- طريقة المصادقة بواسطة التشفير بالمفتاح العام.
3- طريقة المصادقة بواسطة توابع البعثرة (Hash function).

تمتلك ملفات الوسائط المتعددة خصوصية معينة عند استخدامها مع مخططات التوقيع الرقمي العامة، حيث يمكن لنفس الملف أن يتملك أكثر من تمثيل رقمي على الحاسب أو الشبكة و السبب يعود إلى أن هذه الملفات تمر بمراحل تبادل مختلفة بين شبكات الحاسوب أو شبكت الانترنت، و التي قد يؤدي إلى وجود ضجيج متداخل أو تطبيق مستويات معينة من عمليات الضغط، مما يؤثر على المكون الرقمي للملف المتبادل لكنه يحافظ في نفس الوقت على المتطلبات الأدنى لجودته، انطلاقاً من هذه الحقيقة ظهرت عدة اقتراحات على تعديل مخططات المصادقة التي تستخدم توابع البعثرة الكريبتوغرافية في بنيتها، حيث إن مثل توابع البعثرة هذه تعطي على خرجها قيمة فريدة للملف المراد الحفاظ على تكامليته و تعديل أي بت من التمثيل الرقمي لهذا الملف سيؤدي إلى تشكيل قيمة بعثرة مختلفة و بالتالي لا يمكن الاستفادة من مثل توابع البعثرة هذه في بناء مخطط يحقق تكاملية و أصالة ملفات الوسائط المتعددة عامة و الصور الرقمية على وجه التحديد. من مبين الاقتراحات ظهر ما يسمى بتوابع البعثرة الادراكية أو البعثرة الادراكية للصور (*Perceptual Image Hashing*) و التي تهدف إلى استخلاص قيمة بعثرة فريدة لملف الصورة يتم استخلاصها من المعلومات التي يحملها ملف الصورة بدلاً من التمثيل الرقمي لها، كما هو الحال بالنسبة إلى توابع البعثرة الكريبتوغرافية.

المشكلة العلميّة للبحث:

يتم تراسل الصور الرقمية عبر وسط غير آمن مثل شبكات الانترنت، لذا من المحتمل أن تتعرض الصورة لمحاولات التحريف أو التعديل و التي قد يكون أحد أهدافها تغير الملكية الأصلية لصاحب الصورة، لذلك لابد من استنباط مخططات و وسائل تعمل على استرجاع الصورة الأصلية و اثبات ملكيتها. ظهرت العديد من الاقتراحات و المخططات التي تهدف إلى اثبات ملكية الصورة و كان منها استخدام علامات مائية مرئية، إلا أنها لم تصمد أمام العديد من الأدوات البرمجية التي تعمل على إزالتها.

أهمية البحث و أهدافه:

يهدف البحث إلى بناء مخطط توقيع عام للصور الرقميّة يعمل على استخلاص شعاع بعثرة مميز للصورة و من ثم إخفاءه ضمنها بالاعتماد على خوارزميات الاخفاء ضمن الصور الرقميّة، و أن يحافظ المخطط على المتطلبات الأدنى لجودة الصورة مع دراسة الأثر الذي يمكن أن تتركه عمليات تحسين الصورة على شعاع البعثرة المُضمن ضمن الصورة، كالتحكم بمستوى التباين أو سطوع الصورة أو الأثر الناتج عن تطبيق ضغط الصورة بنسب معينة.

طرائق البحث و مواده:

بدأ هذا البحث بدراسة أسلوب التوقيع الرقمي للصور و آلية استخلاص شعاع بعثرة ثابت و مستقر و التعرف على خصائص شعاع البعثرة المستخلص و مدى تأثره بعمليات ضغط الصورة أو تحريفها، و في المرحلة التالية تم التطرق إلى تقنيات الاخفاء ضمن الصور الرقميّة و الفرق بينها و تحديد أسلوب الإخفاء الأفضل، و في نهاية البحث تم اختبار مخطط الاخفاء المقترح و فق عدد من المعايير وهي :

1- دراسة أثر ضغط الصورة بنسب مختلفة على شعاع البعثرة المُضمن، حيث يمكن أن تتعرض الصورة أثناء تبادلها ضمن شبكات الحاسب أو الانترنت إلى عمليات ضغط متعددة تهدف بشكل أساسي إلى ضمان جودة عملية النقل بشكل فعال خاصة مع الصور الرقمية التي تتطلب حجم تخزين كبير، و يهدف هذا الجزء من الدراسة إلى إظهار أداء مخطط الاخفاء المتبع من خلال مقارنة قيمة شعاع البعثرة الأصلي للصورة و شعاع البعثرة الذي تم إخفاءه ضمنها، و في هذه الدراسة سيتم تطبيق مخطط الاخفاء على الصورة و من ثم حفظها بعد تطبيق مستويات ضغط مختلفة و هي (75%، 50%، 25%).

2- دراسة أثر تغيير مستوى التباين و السطوع على قيمة شعاع البعثرة المضمن، حيث تتيح العديد من محررات الصور إمكانية تغيير مستوى التباين للصورة أو تفتيح سطوعها و تغميقه، وغالبا ما تتحسّن الصور باستخدام هذه الميزة. وقد أتاحت التطورات الأخيرة طرق عديدة للتعديل أكثر ذكاءً، حيث يتم تغيير قيم بكسل واحد محدد وجعله أقل أو أعلى من مستوى لمعان الصورة ككل وبالتالي زيادة سطوع الظلال قليلاً دون التأثير على بقية الصورة. عملية التحويل والتغيير المحدد هذه يمكن أن تختلف من محرر إلى محرر.

عند دراسة أثر تغيير سطوع الصورة على شعاع البعثرة المُضمن تم اعتماد الصيغة التي يستخدمها محرر الصور (جَنو) لمعالجة الصور (GNU Image Manipulation Program) و هي كالتالي [10]:

$$New_{Value} = \begin{cases} Old_{Value} + (1 - Old_{Value}) \times \beta. & \beta < 0 \\ Old_{Value} \times (1 + \beta) & \beta > 0 \end{cases} \quad (1)$$

يعبر المتغير *New_Value* عن القيمة الجديدة للبيكسل بعد تغيير مستوى السطوع له، حيث أن قيمته السابقة تكون قيمة المتغير *Old_Value* و يجب أن يمتلك قيمة حقيقية محصورة بالمجال [0 1]، أما بالنسبة إلى المعامل β فهو يحدد مقدار زيادة سطوع الصورة أو انقاصه و قيمه محصورة بالمجال [1 -1]، و من أجل انقاص سطوع الصورة يتم اختيار قيم β سالبة، بينما من أجل زيادة سطوع الصورة يتم اختيار قيم β موجبة، و من أجل β= 0 لن يتم تعديل مستوى سطوع الصورة و في هذه الدراسة تم استخدام القيم التالية للمعامل β :(0.75-،0.5-،0.25-، 0.25،0.5،0.75)، و تم تطبيق الصيغة السابقة على جميع بكسلات الصورة من أجل جميع هذه القيم.

أما بالنسبة إلى دراسة أثر تغيير مستوى التباين للصورة فتم اعتماد الصيغة التالية [5] :

$$New\_Value = (Old\_Value)^{\gamma} \quad (2)$$

يتم زيادة تباين الصورة أو انقاصه من خلال التحكم بقيم γ، و من أجل القيم التي تزيد عن 1 يتم زيادة مستوى التباين أما من أجل القيم الأقل من العدد 1 يتم انقاص مستوى التباين للصورة، وفي هذه الدراسة تم استخدام القيم(0.5،0.8 ، 1.2،3) و المستخدمة في الدراسة [5].

و من أجل دراسة الأثر الاحصائي لعمليه تضمين شعاع البعثرة ضمن الصورة تم الاعتماد على حساب معامل الترابط المعياري(NC) Normalization Correlation . حيث يعتبر معامل الترابط المعياري مقياسا لمدى التشابه بين متغيرين مستقلين، يقيس هذا المعامل الفرق بين الصورة الأصلية و الصورة الناتجة عن عملية الإخفاء و يعطى بالعلاقة التالية [9]:

$$NC = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \left(C(i,j) \times S(i,j) \right) / \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \left(C(i,j) \right)^2 \quad (3)$$

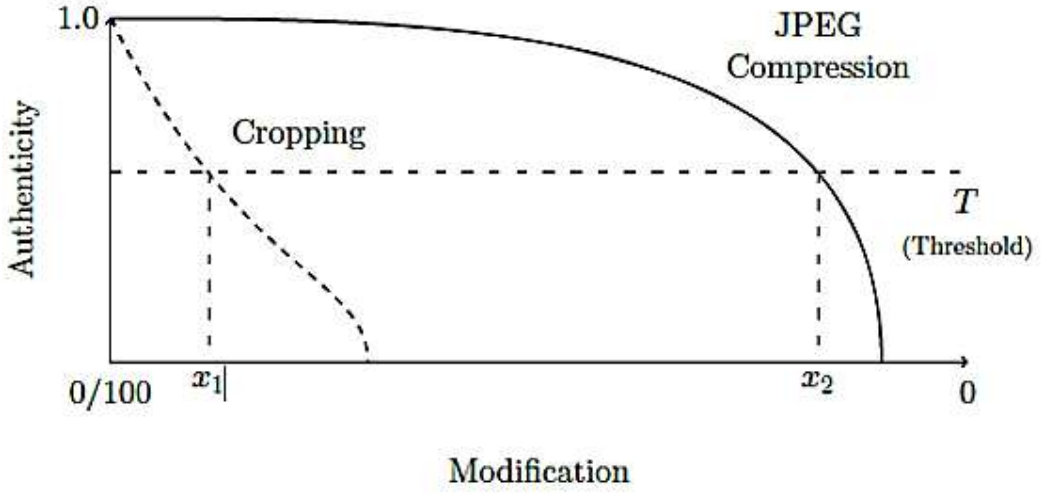
عملياً، كلما اقتربت قيمة الترابط المعياري من الـ 1 كلما كان الفرق بين الصورتين C و S قريب جداً و بالتالي لا يكون لخوارزمية الإخفاء الكثير من التأثير على المعطيات الرقمية للصورة.

تم استخدام نسخة برنامج MATLAB 7.12.0 (R2011a) من أجل تحقيق المخطط برمجيّا و اجراء الاختبارات المناسبة على الصورة الموقعة.

1- تقنيات إثبات ملكية الصورة و تكامليتها :

إن الأسلوب المعتمد في تأمين تكاملية الملف الرقمي يعتمد بشكل أساسي على طبيعة هذا الملف، فعند حديثنا عن الملفات التنفيذية المستخدمة في توزيع حزم البرمجيات يكون من المهم جداً أن يحدث تطابق بين جميع بتات هذا الملف مع النسخة الأصلية له، و في مثل هذه الحالة يتم استخدام أساليب مصادقة الرسائل و التوقيع الرقمي التي تتضمن استخدام توابع البعثرة الكريبتوغرافية و التي تعطي على خرجها قيمة فريدة، إلا أنه عند تعاملنا مع الصور الرقمية فلا يمكننا الاعتماد على مثل أساليب مصادقة الرسائل هذه وذلك لأن نفس الصورة يمكن أن تمتلك أكثر من تمثيل رقمي على الحاسب و بنفس الوقت فإن جميع هذه التمثيلات متطابقة عند قيامنا بمقارنة مرئية لها. يعود اختلاف تمثيل الصورة إلى مرورها بعمليات معالجة الصورة كأن نقوم بتطبيق ضغط للصورة وفق مستويات معينة، جميع عمليات المعالجة هذه ستؤدي إلى حصولنا في كل مرة على تمثيل رقمي مختلف للصورة، لذا فإن الاعتماد على توابع البعثرة الكريبتوغرافية في تأمين أصالتها غير مجدي.

ظهر مؤخراً اهتماما واسع بتوابع البعثرة الادراكية (*Perceptual Hash Function*) و المستخدمة مع الوسائط المتعددة كملفات الصور الرقمية أو ملفات الصوت، إن هذه التقنية تهدف بشكل رئيسي إلى استخلاص سمات مميزة لملفات الوسائط المتعددة و من ثم يتم حساب قيمة بعثرة تعتمد على هذه السمات[1]، و يتم التحقق من أصالة و تكاملية الملف من خلال عملية مقارنة بين قيمة البعثرة الأصلية و القيمة الجديدة له و القرار النهائي يعتمد على عتبة مختارة تحدد فيما إذا كان الملف قد تعرض للتحريف أم لا، و كمثال على ذلك يبين الشكل(1) العلاقة بين أصالة الصورة و التعديلات المطبقة على الصورة من ضغط و قص[2]. تعبر العتبة T عن القيمة التي يمكن اعتبار الصورة غير موثوقة في حال تجاوزها، بالنسبة لعملية القص x1 و لعملية الضغط x2.



الشكل(1): العلاقة بين أصالة الصورة و بين عملية ضغطها و قصها.

تتعدد وسائل و تقنيات استخلاص قيمة بعثرة إدراكية لملف الوسائط المتعددة و جميعها يهدف إلى استخلاص قيمة بعثرة فريدة تعتمد على المعلومات التي يحملها الملف أكثر من اعتمادها على التمثيل الرقمي لهذه المعلومات على الحاسب [2]. على سبيل المثال يمكن استغلال المعلومات التي تحملها حواف الصورة في المجال الفراغي لها في توليد قيمة بعثرة فريدة لها بالاعتماد على فرضية أنه لا يمكن لصورتين مختلفتين أن تمتلكان نفس المعلومات التي تمثلها حواف الصورة، و تعتبر عملية استخلاص توقيع الصورة بالاعتماد على قيمة المتوسط الحسابي لعلب الصورة من تقنيات البعثرة الإدراكية للصور و التي تهدف إلى الحصول على توقيع مستقر و ثابت لا يتأثر بعمليات تحسين الصورة، تتلخص فكرة استخلاص توقيع للصورة باستخدام خوارزمية قيمة المتوسط الحسابي لعلب الصورة بإيجاد صورة مصغرة عن الصورة الأصلية يتم اعتماده كقيمة بعثرة تحتوي على خصائص الصورة الأصلية و لا تتغير قيمة هذه البعثرة عبر عمليات تحسين الصورة كتغيير مستوى التباين أو مستوى السطوع أو تطبيق الضغط بنسب مختلفة.

يمكن تلخيص خطوات القيام بهذه الطريقة عبر النقاط التالية:

1- تحويل الصورة الأصلية إلى صورة ذات تدرجات رمادية.

2- إعادة تحجيم الصورة الناتجة عن المرحلة السابقة إلى حجم محدد من قبل المستخدم على أن تكون أبعاد الحجم الجديد متساوية.

3- تقسيم الصورة التي تم تحجيمها إلى علب متجاورة، أبعاد العلبة الواحدة يتم تحديدها من قبل المستخدم و يعبر مع حجم الصورة التي تم تحجيمها عن طول الشعاع الذي يعبر في النهاية عن قيم بعثرة الصورة الأصلية.

4- إيجاد قيمة المتوسط الحسابي لكل علبة من علب الصورة، و ليكن رمزها Mi، بحيث يعبر i عن ترتيب العلب.

5- بعد إيجاد قيم المتوسط الحسابي يتم إيجاد القيمة المتوسطة لهذه القيم و لتكن Md .

6- القيام بمقارنة بين القيمة المتوسطة Md و بين قيم المتوسط الحسابي Mi، و توليد بتات شعاع البعثرة الادراكية و فق العلاقة التالية[2]:

$$hashVec(i) = \begin{cases} 1 & Mi \geq Md \\ 0 & Mi < Md \end{cases} \qquad (4)$$

تكمن فعالية هذه الخوارزمية في إمكانية اختيار حجم شعاع البعثرة المناسب و بالتالي اختيار الدقة المطلوبة حسب التطبيق المستخدم في مخطط المصادقة ففي حال التطبيقات القوية التي تتطلب دقة عالية للتوقيع يمكن استخدام حجم شعاع البعثرة ليكون 1024 بت و هنا يتم التحكم بأبعاد الصورة بعد إعادة تجميعها ليكون 512 × 512 بينما يكون حجم العلبة المستخدم هو 16 × 16، و كمثال على ذلك يظهر في الشكل(2) الفرق بين تعدد حجوم شعاع البعثرة من أجل الصورة الظاهرة في نفس الشكل حيث نلاحظ أن زيادة حجم الشعاع يزيد من عدد المعلومات التي يحملها الشعاع عن الصورة الأصلية، ومن ناحية أخرى من أجل التطبيقات التي لا تتطلب دقة عالية يمكن فقط تغيير حجم العلبة ليصبح 32 × 32 و بعد تطبيق الخوارزمية يصبح حجم الشعاع 16 × 16 أي 256 بت. يجب التنويه أن زيادة حجم الشعاع يمكن أن يزيد من حجم المساحة التي سيتم حجزها من الصورة المضيفة لتضمين بتات الشعاع و الذي يمكن أن يؤثر على جودة الصورة المضيفة بعد تطبيق عملية الاخفاء لشعاع البعثرة، لذا يمكننا إيجاد حجم شعاع متوسط الحجم يعطي نتائج مقبولة و فعالة كأن يكون 32 × 16 أي 512 بت ويكون مناسباً لعملية التضمين ضمن الصورة من حيث مساحة التخزين، و تم اعتماد هذا الحجم عند بعض أشهر توابع البعثرة الكريبتوغرافية كـ-SHA 512 و MD5.

الشكل(2)، استخلاص شعاع بعثرة بحجوم مختلفة للصورة.

يبين الشكل(3) المخطط التدفقي لخوارزمية استخلاص شعاع البعثرة المستخدمة في هذا البحث، و نلاحظ الأبعاد الجديدة تم اختيارها للصورة و حجم العلبة المختار، ومن أجل جميع علب الصورة يتم تطبيق العلاقة(4) لنصل في النهاية إلى شعاع البعثرة الادراكية المستخلص من الصورة الأصلية.

الشكل(3)، مخطط تدفقي يبين تسلسل خطوات استخلاص شعاع البعثرة الخاص بالصورة .

تعتبر خوارزمية استخلاص قيمة البعثرة باستخدام القيمة المتوسطة من أسرع الخوارزميات المستخدمة في مجال التوقيع الرقمي للصور و تتميز بالبساطة و بإمكانية تحقيقها برمجياً بسهولة و تعطي نتائج دقيقة حتى في حال تطبيق ضغط على الصورة، و يبين الشكل(4) شعاع البعثرة المستخرج من الصورة الأصلية بحجم (**32** × **16**) بعد تطبيق الضغط على الصورة بنسب متعددة.

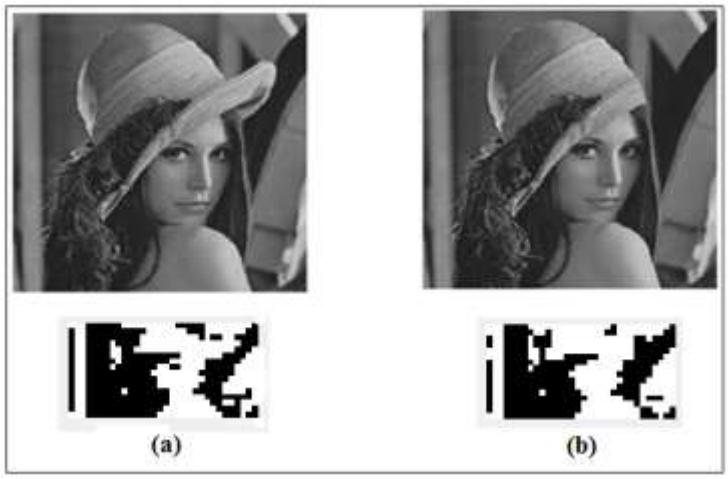
الشكل(4)، قيم شعاع البعثرة للصورة بعد ضغطها بنسب متعددة.

و بالنظر إلى الشكل السابق نلاحظ ان شعاع البعثرة قد حافظ على قيمه دون فقد في البيانات إلا في حال تجاوز نسبة الضغط 50%، حيث أدت عملية الضغط إلى فقدان جزء بسيط من البيانات. تم حساب الفرق بين شعاع البعثرة للصورة الأصلية (مستوى الضغط 0%) و شعاع البعثرة لنفس الصورة عند كل مستوى من مستويات الضغط و تم التعبير عن قيمة هذا الفرق و فق نسبة مئوية تحدد مقدار التطابق بين بتات الشعاعين وحصلنا على النتائج المبينة في الجدول(1).

الجدول(1): نسبة التطابق بين شعاع البعثرة الأصلي للصورة و شعاع البعثرة لنفس الصورة عند كل مستوى من مستويات الضغط

نسبة الضغط	نسبة التطابق
%0	%100
% 25	% 100
%50	% 99.8
%75	%99.8

أما بالنسبة للأثر الذي يمكن أن تتركه عمليه تحريف أو تعديل جزء من الصورة الأصلية، فيمكن ملاحظته من الشكل(5) الذي يبين الفرق بين الصورة الأصلية و الصورة بعد تحريف محتواها و مدى الاختلاف بين شعاعي البعثرة لكلا الصورتين، و بالحساب تبين ان نسبة التطابق بين الشعاعين هي 91.6% و نلاحظ أن إزالة جزء من محتوى الصورة الأصلية يؤدي إلى ضياع جزء من شعاع البعثرة الأصلي لها.



الشكل(5)،(a) : الصورة الأصليّة، (b) الصورة بعد التحريف بمحتواها.

عند تطبيق عملية اقتصاص لجزء من محتوى الصورة حصلنا على تغيرات كبيرة في شعاع البعثرة الجديد، و نسبة التطابق المحسوبة 86.71% و كما يظهر في الشكل(6) يمكننا استنتاج أن عمليات القص على الصورة تترك تأثيراً أكبر من غيرها على قيم شعاع البعثرة الأصلي لها، ويكون ذلك بنسب متفاوتة و حسب كبر الجزء الذي تم قصه من الصورة الأصلية.

الشكل(6)،(a) : الصورة الأصليّة، (b) الصورة بعد قص أجزاء منها.

يتبين لنا من الأشكال السابقة أن شعاع البعثرة المستخلص من الصورة باستخدام القيمة المتوسطة لا يتأثر بعمليات ضغط الصورة، إلا أن تعديل أو قص أجزاء من الصورة سيؤدي إلى توليد شعاع بعثرة جديد قيمته مختلفة بشكل كبير عن شعاع البعثرة الأصلي للصورة.

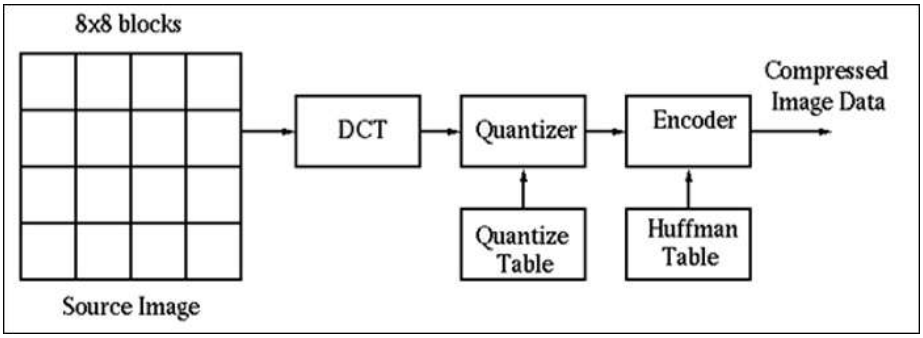
2- إخفاء شعاع البعثرة ضمن الصورة:

تعدد أساليب تضمين أو إخفاء الرسائل ضمن الصور الرقمية و بشكل عام يمكننا إخفاء بيانات ضمن الصورة في مجالين هما المجال الفراغي و المجال الترددي للصورة[3]، و يقصد بالمجال الفراغي المجال الذي يتم تمثيل بكسلات الصورة على شكل قيم عددية تعبر عن الكثافة اللونية لهذه البكسلات و يشار إلى هذا المجال بالمجال الزمني عند تعاملنا مع الإشارات الرقمية، ويمكننا إخفاء بتات الرسالة السرية ضمن هذا المجال باستخدام تقنية البتات الأقل أهمية(LSb) ، ومن ناحية أخرى يمكننا أيضاً تمثيل الصورة رياضيّاً بعد تحويلها إلى مجال نقل آخر غير المجال

الفراغي كالمجال الترددي، و يوجد العديد من التحويلات الرياضيّة التي تنقل الإشارة من مجالها الفراغي إلى المجال الترددي، و تعتبر عملية إخفاء الرسالة ضمن المجال الترددي للصورة أكثر أماناً و مقاومة لعمليات التحسين التي يمكن أن تمر بها الصورة[6]، بينما تعتبر عملية الاخفاء ضمن المجال الفراغي للصورة أكثر حساسية لأي تغيرات تطرأ على الصورة طالما أن قيم البكسلات تتأثر بشكل مباشر مما يؤثر على بتات الرسالة التي تم تضمينها ضمن خاناتها الأقل أهمية، و هذا ما يجعل التضمين في المجال الترددي للصورة له أفضلية على المجال الفراغي و يدخل بشكل مباشر في بناء مخطط إخفاء توقيع الصورة في هذا البحث، وبشكل عام يوجد عدة تحويلات تنقل الصورة من المجال الفراغي إلى المجال الترددي منها:

1. التحويل التجيب المتقطع Discrete Cosine Transform(DCT)
2. تحويل المويجة المتقطّع Discrete Wavelet Transform (DWT)

وكما ذكرنا سابقاً فإن الميزة الأساسية للإخفاء ضمن المجال الترددي للصورة هي تفادي عمليات الضغط المتكررة التي يمكن أن تمر بها الصورة، هذه الميزة تم استغلالها من مخطط ضغط الصورة القياسي JPEG و المبين في الشكل (7) بحيث إن أي عملية إخفاء يجب أن تتم قبل مرحلة التكميم(Quantizer) و التي تصبح فيها أغلب المعاملات ذات التردد الأعلى ذات قيمة صفرية مما يقلل من عدد البتات اللازمة لترميزها في مرحلة الترميز(Encoding)، و بالتالي تقليل حجم تخزين الصورة مع المحافظة قدر الإمكان على جودتها.



الشكل(7): مخطط الضغط القياسي المستخدم في صيغ الصور JPEG.

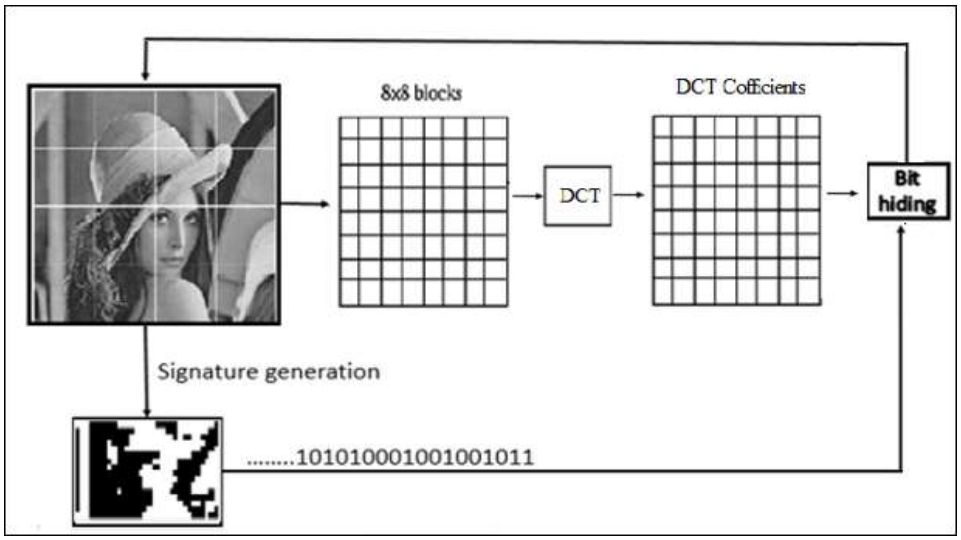
يبين الجدول (2) قيم مصفوفة التكميم(Quantize Table) و التي سيتم تقسيم جميع معاملات التحويل (DCT) عليها، قيم هذه المصفوفة اختيرت بعناية بحيث تصبح أغلب قيم معاملات التحويل ذات التردد الأعلى معدومة و بالتالي يسهل ترميزها باستخدام أحد المرمزات كترميز هوفمان.

الجدول(2): مصفوفة التكميم Q المستخدمة في مخطط الضغط القياسي لـJPEG

$$\begin{bmatrix} 16 & 11 & 10 & 16 & 24 & 40 & 51 & 61 \\ 12 & 12 & 14 & 19 & 26 & 58 & 60 & 55 \\ 14 & 13 & 16 & 24 & 40 & 57 & 69 & 56 \\ 14 & 17 & 22 & 29 & 51 & 87 & 80 & 62 \\ 18 & 22 & 37 & 56 & 68 & 109 & 103 & 77 \\ 24 & 35 & 55 & 64 & 81 & 104 & 113 & 92 \\ 49 & 64 & 78 & 87 & 103 & 121 & 120 & 101 \\ 72 & 92 & 95 & 98 & 112 & 100 & 103 & 99 \end{bmatrix}$$

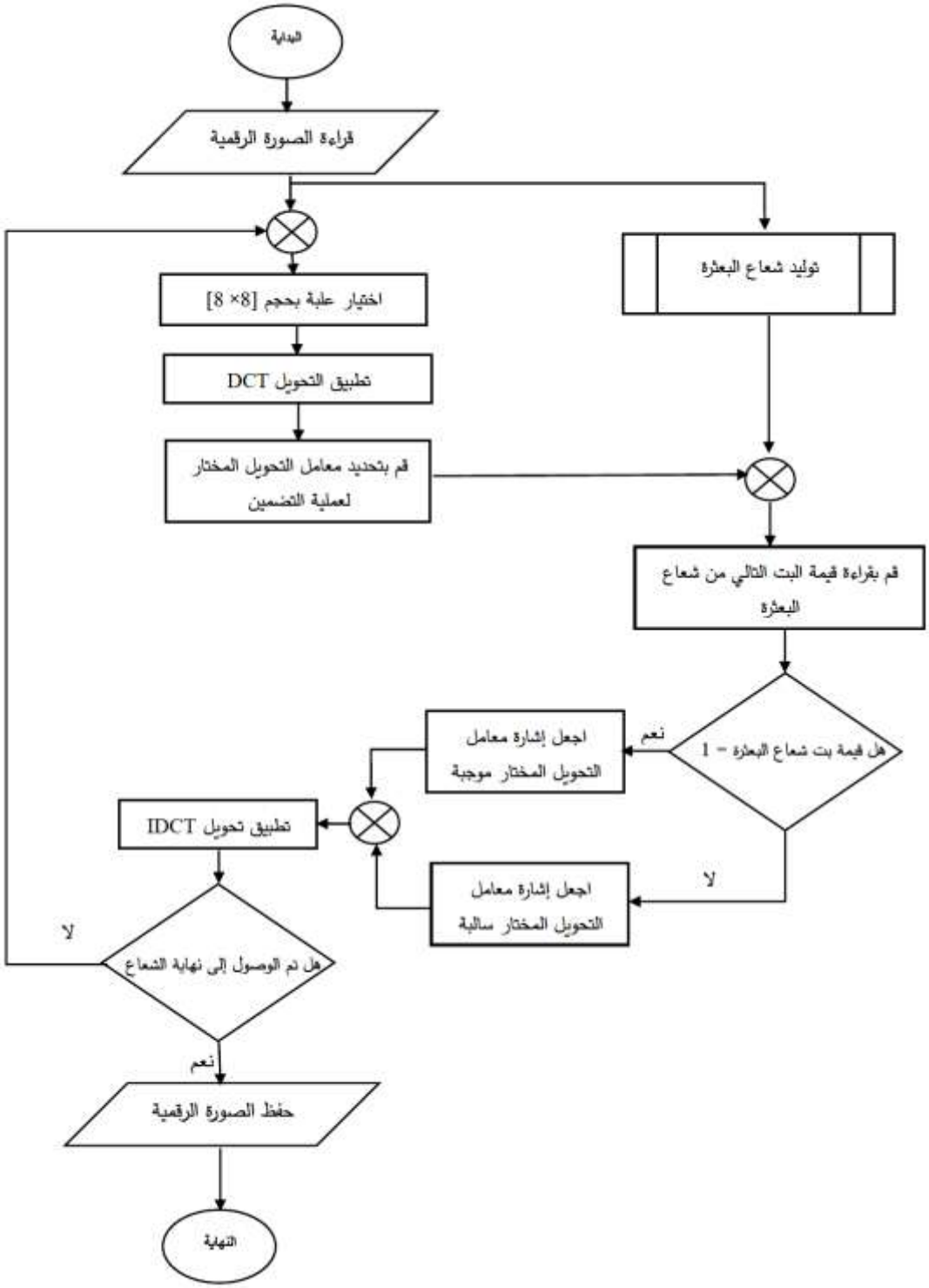
إن مخطط إخفاء التوقيع الرقمي في هذا البحث مشابه لمخطط الضغط القياسي، و يبين الشكل(8) مخطط إخفاء شعاع البعثرة الادراكية للصورة ضمن مجالها الترددي، ففي البداية يتم تقسيم الصورة إلى علب متجاورة حجم كل علبة

هو (8 × 8) و من ثم يتم اجراء تحويل DCT على العلبة، والمصفوفة الناتجة عن هذا التحويل هي بنفس حجم العلبة الأصليه.



الشكل(8): مخطط إخفاء شعاع البعثرة للصورة.

أما بالنسبة إلى آلية إخفاء بتات شعاع البعثرة للصورة ضمن معاملات التحويلDCT فيكون بطريقة تغيير إشارة المعامل حسب قيمة البت المراد اخفاؤه، فمثلاً إذا أردنا إخفاء البت ذو القيمة '0' يمكن جعل المعامل ذو قيمة سالبة بينما إذا اردنا إخفاء البت ذو القيمة '1' يمكن جعل المعامل ذو قيمة موجبة، عملية تغيير إشارة المعامل تتم من أجل جميع علب الصورة، حتى نهاية جميع بتات شعاع البعثرة. يبين الشكل(9) المخطط التدفقي لمخطط إخفاء شعاع البعثرة المتبع في هذا البحث.



الشكل(9)، مخطط تدفقي يبين تسلسل خطوات اخفاء شعاع البعثرة الخاص بالصورة .

وقد تبين بالتجريب أن قيم المعاملات القريبة من الصفر يمكن أن تتذبذب إشارتها بين الموجب و السالب مع عمليات التكميم المختلفة للمعاملات، و لكي نحافظ على إشارة المعامل القريب من 0 سيتم اعتماد ثابت k يضاف قيمته إلى قيمة المعامل بعد تغيير إشارته، أما بالنسبة إلى الثابت K الذي يجب اضافته إلى كل معامل فيمكن استنتاج قيمته من

مصفوفة التكميم **Q** بحيث ان ***K*** تأخذ قيمته من مصفوفة التكميم حسب المعامل المختار لعملية التضمين و ذلك بالاعتماد على أسلوب الضغط المتبع في مخطط ضغط الصورة القياسي JPEG.

إن الهدف الأساسي من إضافة قيمة ***K*** وفق الطريقة السابقة هو المحافظة على إشارة المعامل حتى بعد تطبيق عملية التكميم و بالتالي يتم المحافظة على قيمة بت شعاع البعثرة الذي تم إخفاؤه حتى بعد تطبيق عمليات ضغط متعددة للصورة.

النتائج و المناقشة:

بعد تطبيق مخطط إخفاء التوقيع الرقمي على الصورة المبينة في الشكل(2) و باختيار حجم شعاع البعثرة (32 × 16)، لم تترك عملية الاخفاء أثراً يمكن ملاحظته عند المقارنة مع الصورة الأساسية، و الشكل(10) يبن الصورتين الأساسية و الصورة بعد إخفاء شعاع البعثرة باستخدام مخطط الاخفاء المقترح.

الشكل(10): (a): الصورة الأصليّة،(b): الصورة بعد تضمين شعاع البعثرة.

و بعد حساب معامل الترابط المعياري المعطى في العلاقة(3) من أجل الصورتين(a) و (b) من الشكل(10) حصلنا على القيمة NC=0.9999998 ونلاحظ مدى اقتراب القيمة من القيمة المثالية(NC=1) و الذي يشير بدوره إلى التشابه الكبير بين الصورتين.

و بشكل عام لا يمكننا الاعتماد على نتائج اختبار صورة واحدة من أجل تقييم كامل مخطط المصادقة المقترح، ومن أجل الحصول على نتائج أكثر موثوقية قمنا بتطبيق المخطط على عينة من الصورة(ما يقارب 1000 صورة) مختلفة في المقاسات و الصيغ و الحجم، و نبين فيما يلي النتائج التي حصلنا عليها من أجل كل عملية اختبار مطبقة على الصور.

1- دراسة أثر تطبيق ضغط الصورة على شعاع البعثرة المُضمن

بالنسبة إلى أثر تطبيق عملية الضغط على الصورة بعد تضمين شعاع البعثرة فيمكن ملاحظته من الشكل(11)، و الذي يبين ناتج تطبيق نسب مختلفة من الضغط على الصورة بعد تضمين توقيعها باستخدام مخطط إخفاء التوقيع المتبع في هذا البحث، و نلاحظ مدى مقاومة شعاع البعثرة المُضمن لعمليات ضغط الصورة.

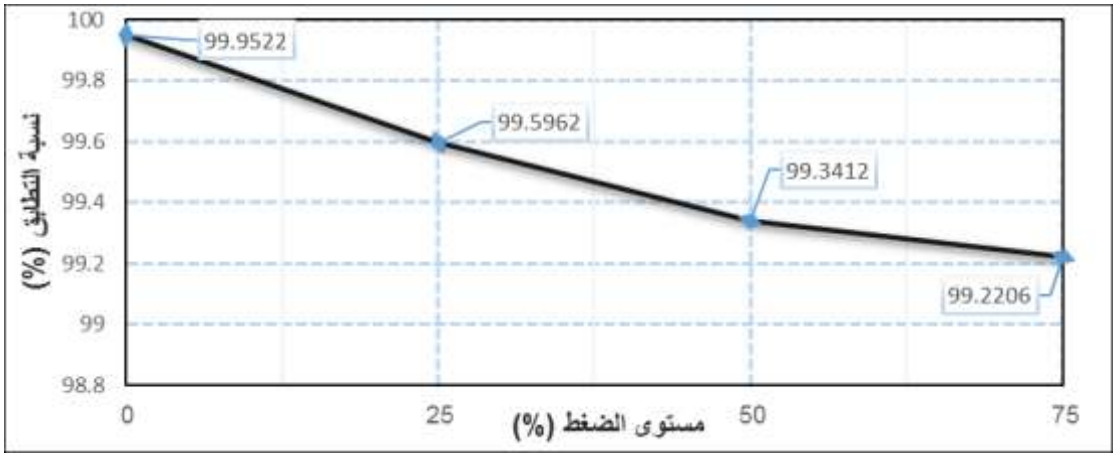
الشكل(11): أثر تطبيق ضغط للصورة بنسب مختلفة على شعاع البعثرة المُضمن.

و كما ذكرنا فإن عملية ضغط الصورة قد تؤثر على شعاع البعثرة المستخلص منها كما هو مبين في الشكل(4) لذا قد لا نحصل على نسبة تطابق مثالية بين شعاع البعثرة الأصلي و بين شعاع البعثرة المُضمن، و يتضمن الجدول(3) نسبة تطابق شعاع البعثرة المُضمن ضمن الصورة مع شعاع البعثرة الأصلي عند كل نسبة ضغط مطبقة.

الجدول(3): نسبة التطابق بين شعاع البعثرة المُضمن و شعاع البعثرة الأصلي للصورة بعد إجراء ضغط للصورة بنسب مختلفة.

نسبة الضغط	نسبة التطابق
% 0	% 100
% 25	% 100
%50	% 99.8
%75	%99.8

ومن أجل عينة الصور التي تم اختبارها تم حساب قيمة المتوسط الحسابي لنسبة التطابق المحسوبة لهذه الصور عند كل مستوى من مستويات الضغط، حيث يظهر في الشكل(12) العلاقة بين نسبة التطابق المحسوبة و بين مستويات ضغط مختلفة لضغط الصورة.



الشكل(12): نسبة التطابق بين شعاع البعثرة المُضمن و شعاع البعثرة الأصلي لعينة الصور المختبرة عند نسب مختلفة من الضغط .

يتبين من الشكل السابق انخفاض نسبة التطابق بين شعاع البعثرة المُضمن و شعاع البعثرة الأصلي للصورة بشكل متناسب مع زيادة مستوى الضغط المختار، و بالتدقيق في قيم نسب التطابق نلاحظ أن المعدل لم يتجاوز النسبة 99% من اجل أقصى مستوى ضغط طُبق على الصورة.

2- دراسة أثر تعديل مستوى التباين على شعاع البعثرة المُضمن

عند قيامنا بتعديل مستوى التباين للصورة بعد تضمين شعاع البعثرة وفق درجات و نسب مختلفة حصلنا على النتائج المبينة في الشكل(13)، و نلاحظ أن زيادة مستوى التباين بشكل كبير أدى إلى ضياع جزء من قيمة شعاع البعثرة المُضمن.

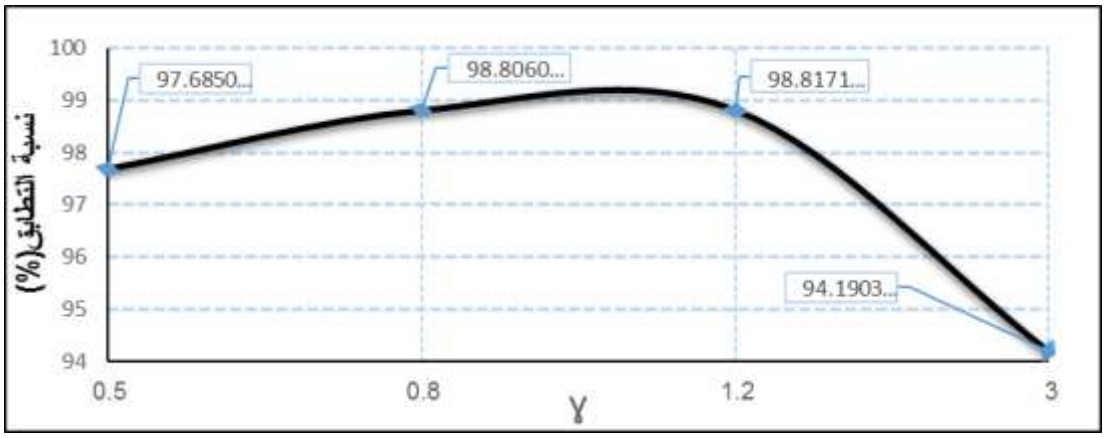
الشكل(13): أثر تغيير مستوى التباين عند قيم مختلفة للمعامل γ على شعاع البعثرة المُضمن ضمن الصورة.

وبشكل مشابه لأثر ضغط الصورة، لم نحصل على تطابق مثالي بين شعاع البعثرة المُضمن و شعاع البعثرة المستخلص باستخدام خوارزمية القيمة المتوسطة و يبين الجدول(4) نسب التطابق بين الشعاعين بعد تغيير مستوى التباين للصور الموقعة.

الجدول(4): نسبة التطابق شعاع البعثرة المُضمن و شعاع البعثرة الأصلي للصورة بعد تغيير مستوى التباين بنسب مختلفة.

مستوى التباين(γ)	نسبة التطابق
1	%100
0.5	%97.46
0.8	%99.41
1.2	99.61
3	% 93.16

أما بالنسبة إلى العلاقة بين نسبة التطابق المحسوبة و بين تغيير مستوى التباين من اجل عينة الصور المختبرة فيمكن ملاحظته من الشكل(14)، حيث إن تغيير مستوى التباين للصور الموقعة وفق قيم مختلفة للمعامل γ أدى إلى انخفاض نسبة التطابق خاصة عند زيادة قيم المعامل γ (زيادة مستوى التباين).



الشكل(14): نسبة التطابق عند قيم مختلفة للمعامل γ لعينة الصور المختبرة.

3- دراسة أثر تعديل مستوى السطوع على شعاع البعثرة المُضمن

أما بالنسبة لتعديل مستوى السطوع للصورة وفق درجات و نسب مختلفة فقد حصلنا على النتائج المبينة في الشكل(15)، و نلاحظ أننا حصلنا على نتائج أفضل بالمقارنة مع عملية تغيير مستوى التباين للصورة الموقعة.

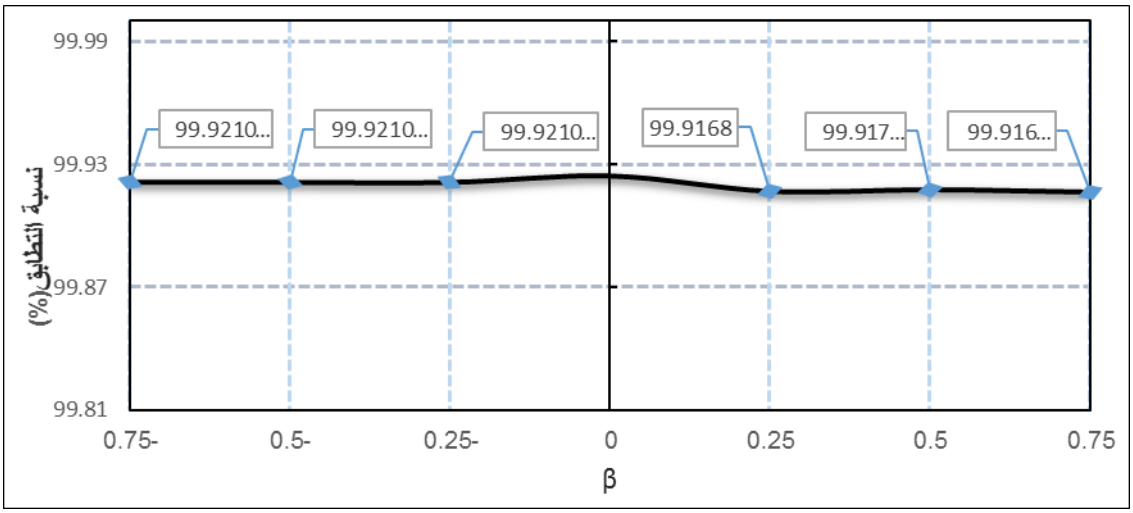
الشكل(15): أثر تغيير سطوع الصورة عند قيم مختلفة للمعامل β على شعاع البعثرة ضمن الصورة.

ويبين الجدول(5) نسب التطابق بين شعاع البعثرة المُضمن و شعاع البعثرة الأصلي بعد تعديل سطوع الصورة الموقعة، ونلاحظ أن تغيير السطوع بنسب متزايدة أدت إلى انقاص نسبة التطابق بين الشعاعين بشكل أكبر، و هذا يعود إلى أثر تغيير السطوع على ملامح الصورة بحيث أدت إلى تغيير بسيط في قيمة شعاع البعثرة الأصلي(المستخلص من الصورة) و المحسوب من خوارزمية القيمة المتوسطة.

الجدول(5): نسبة التطابق بين شعاع البعثرة المُضمن و شعاع البعثرة الأصلي للصورة بعد تغيير سطوع الصورة بنسب مختلفة.

مستوى السطوع (β)	نسبة التطابق
0	%100
0.25	%98.6
0.5	%97
−0.25	%99.8
−0.5	%99.4

و من أجل عينة الصور التي تم اختبارها يظهر في الشكل(16) نسبة التطابق المحسوبة عند مستويات مختلفة لسطوع الصور الموقعة، و بالمقارنة مع الشكل(14) نلاحظ أننا قد وصلنا إلى نتائج أفضل و شبه مثالية بالنسبة إلى زيادة مستوى السطوع أو انقاصه.



الشكل(16): نسبة التطابق عند قيم مختلفة للمعامل β لعينة الصور المختبرة.

الاستنتاجات و التوصيات:

بالنظر إلى النتائج التي توصلنا إليها في المخططات و الجداول السابقة، يمكننا تلخيص النقاط التالية:

1- إن التوقيع الرقمي للصور الرقمية يختلف عن التوقيع المستخدم لباقي الملفات الرقمية نظراً لعمليات المعالجة التي يمكن أن تمر بها الصورة بين الأطراف المتبادلة و التي لا يمكن ادراجها ضمن محاولات التعديل غير المشروع بالصورة.

2- قوة مخطط إخفاء التوقيع المُقترح تكمن في المحافظة قدر الإمكان على قيمة شعاع البعثرة المُضمن ضمن الصورة في وجه عمليات الضغط أو تحسين التباين و شدة الإضاءة للصورة.

3- بعد تطبيق الاختبارات السابقة حصلنا على نسبة تطابق شبه مثالية حتى بعد تطبيق ضغط الصورة أو تغيير مستوى السطوع لها، بينما انخفضت نسبة التطابق بشكل ملاحظ مع زيادة مستوى التباين للصورة.

4- من أجل الحصول على نسبة تطابق مثالية بين شعاع البعثرة المُضمن و شعاع البعثرة الأصلي للصورة يمكننا تقييد المستخدم باستخدام صيغ الصور التي لا يتم ضغطها(png.) أو تحديد عتبة محددة لا يجب تجاوزها عند اختبار مقدار التطابق بين الشعاعين.

5- بالنسبة إلى حالات التعديل أو التحريف التي يمكن أن تواجهها الصورة الموقَّعة نكون هنا أما احتمالين إما أن يكون التعديل قد غير من التوقيع الأصلي للصورة و بالتالي لن يحصل تطابق مع التوقيع الذي تم تضمينه، أو أن يسبب التعديل ضياع في بعض قيم التوقيع المُضمن على فرض حدث التعديل ضمن مناطق تضمين التوقيع و بالتالي لن يتطابق التوقيع الأصلي للصورة مع التوقيع المُضمن و سيكتشف وجود تعديل حدث للصورة.

6- يمكننا نشر بتات شعاع البعثرة على كامل الصورة من أجل تفادي الحالات التي يبقى فيه التوقيع الجديد للصورة متطابق مع التوقيع المُضمن حتى بعد وجود تحريف متعمد على الصورة.

7- إن بساطة خوارزمية استخلاص التوقيع باستخدام المتوسط الحسابي لبلوكات الصورة يجعها سهل التحقيق برمجيّاً ضمن تطبيقات الأجهزة المحمولة أو الماسحات الضوئية.

المراجع

1- SCHNEIDER، M. ; CHANG، S.F: *A robust content based digital signature for image authentication*. In Proceedings of the International Conference on Image Processing (ICIP)، IEEE ،vol. 3، Sept. 1996، 227-230.

2- ZAUNER،C، *Implementation and Benchmarking of Perceptual Image Hash Functions*(Master Thesis)، Austria،2010.

3- GHOSHAL،N; MANDAL،J. *Image Authentication Technique in Frequency Domain based on Discrete Fourier Transformation.* ICCS journal، India،2010،144-150.

4- MOUSAVI،S.M. *Image Authentication Scheme using Digital Signature and Digital Watermarking*. IJCEM، Iran، Vol. 16، 2013، 59-63.

5- KANNAMMAL،A; RANI،S. *Authentication of DICOM Medical Images using Multiple fragile watermarking Techniques in Wavelet Transform Domain.* IJCSI journal، India، Vol. 8، No .1، *2011،181-189.*

6- NOSRATI،M; KARIMI،R; HARIRI،M. *An introduction to steganography methods. WAP* journal، *Iran، Vol.1،No .1، 2011،191-195.*

7- د. رياض ضاهر، *أمن المعلومات*، منشورات جامعة تشرين، 2014

8- محمد، نادية معن. *الإخفاء الفوضوي للصور باستخدام DCT & DWT*، مجلة الرافدين لعلوم الحاسوب و الرياضيات، العراق- جامعة الموصل، المجلد(10)، العدد(3)،2013، 61-73.

9- متراس، بان أحمد حسن ; عبو، أديبة خالد. *الإخفاء ضمن سلسلة(DNA) باستخدام مفتاح سري يعد بزرة (seed) لمولد أرقام عشوائية*، المجلة العراقية للعلوم الإحصائيّة، العراق، العدد الخامس و العشرون، 2013، 430-440

10- GIMP source code for brightness and contrast image filtering. [online], June 2017 <https://github.com/piksels-and-lines-orchestra/gimp/blob/master/app/base/lut-funcs.c>