Analyzing the System Performance for Compression Encrypted Images Using Hybrid DWT-DCT-DST Compression Algorithm

Dr. Al-Samawal SALEH*
Dr. Sadek Ali**
Kholod SARHAN***

(Received 12 / 1 / 2020. Accepted 2 / 6 / 2020)

□ ABSTRACT □

Recently, the field of multimedia and network technologies has developed greatly. With this development, the information security has become the most important part of multimedia-based system when the data is transmitted over the network. If encryption is not applied, the information may be stolen. on the other hand, Image compression is also essential where images need to be stored, transmitted or viewed quickly and efficiently. Therefore, there is a need for a system that applies encryption before the image compression.

In this research, we propose an encryption method that is operated with Arnold transform and image compression algorithm using Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT) and Discrete Sine Transform (DST) that can be used efficiently to compress the encrypted image. To achieve our goal, we used several normal and medical images. We conducted a performance test for (6) different types of mother wavelets, in order to select the optimal mother wavelet that achieves the best compression ratio and maintains best quality of the reconstructed image. We evaluated the results using Peak Signal to Noise Ratio (PSNR), Compression Ratio (CR) and Root Mean Square Error (RMSE) parameters. In order to have a visual perception, subjective evaluation of the images have been conducted. The simulation was performed using MATLAB. The results showed that (bior3.9) achieved the best quality of the reconstruction image. The proposed algorithm achieved good results for compression and quality of medical images.

Keywords: Encryption, Compression, Permutation, Discrete Wavelet Transform, Discrete Cosine Transform, Discrete Sine Transform, High frequency minimization.

*Professor, Department of Communication and Electronics, Faculty of Mechanical and Electrical Engineering, Tishreen University, Latakia, Syria.

**Associate Professor, Department of Communication and Electronics, Faculty of Mechanical and Electrical Engineering, Tishreen University, Latakia, Syria.

***Master Student, Department of Communication and Electronics, Faculty of Mechanical and Electrical Engineering, Tishreen University, Latakia, Syria.

تحليل أداء نظام ضغط الصور المشفرة باستخدام خوارزمية ضغط هجينة معتمدة على التحويلات المويجي والتجيبي والجيبي المتقطعة

د. السموءل صالح*

د. صادق علي**

خلود سرحان***

(تاريخ الإيداع 12 / 1 / 2020. قُبِل للنشر في 2/ 6 / 2020)

□ ملخّص □

تطور مجال الوسائط المتعددة وتقنيات الشبكات بشكل كبير مؤخراً. مع هذا التطور، أصبح أمن المعلومات يمثل الجزء الأكثر أهمية في النظام المعتمد على الوسائط المتعددة عند إرسال المعطيات عبر الشبكة. إذا لم يطبق التشفير قد يكون هناك إمكانية لسرقة المعلومات. من جهة ثانية، فإن ضغط الصور ضروري أيضاً حيث تحتاج الصورة لأن تخزن، وترسل، وتعرض بسرعة وفعالية. لذلك، يوجد حاجة لنظام يطبق التشفير قبل ضغط الصورة.

نقترح في هذا البحث طريقة لتشفير الصور تعتمد على تحويل أرنولد Arnold Transform، وخوارزمية لضغط الصور تعتمد على التحويل المويجي المتقطع Discrete Wavelet Transform (DWT) والتحويل التجيبي المتقطع Discrete Cosine Transform (DCT) والتحويل الجيبي المتقطع Discrete Sine Transform (DST) التي يمكن أن تستخدم بشكل فعال لضغط الصور المشفرة. لتحقيق أهدافنا استخدمنا عدة صور عادية وطبية. قمنا بإجراء اختبار أداء (6) أنواع من المويجات الأم، وذلك بغية اختيار المويجة الأم المثلى التي تحقق أفضل نسبة ضغط وتحافظ على أفضل جودة للصورة المستعادة. تم تقييم الأداء باستخدام بارامترات قمة نسبة الإشارة إلى الضجيج Peak Signal to Noise Ratio (PSNR) ونسبة الضغط Compression Ratio (CR) والجذر التربيعي لمتوسط مربع الخطأ Root Mean Square Error (RMSE). ومن أجل الحصول على الإدراك البصري، تم أيضاً إجراء التقييم الشخصي للصورة. تمت عملية المحاكاة باستخدام MATLAB. أظهرت النتائج أن المويجة (bior3.9) حققت أفضل جودة للصورة المستعادة. حققت الخوارزمية المقترحة نتائج جيدة من ناحية الضغط وجودة الصورة المستعادة بالنسبة للصور الطبية.

الكلمات المفتاحية: تشفير، ضغط، التبديل، التحويل المويجي المتقطع، التحويل التجيبي المتقطع، التحويل الجيبي المتقطع، تخفيض الترددات العالية.

* **استاذ، قسم هندسة الاتصالات والالكترونيات، كلية الهندسة الميكانيكية والكهربائية، جامعة تشرين، اللاذقية، سورية.**

** **أستاذ مساعد، قسم هندسة الاتصالات والالكترونيات، كلية الهندسة الميكانيكية والكهربائية، جامعة تشرين، اللاذقية سورية.**

*** **طالبة دراسات عليا (ماجستير)، قسم هندسة الاتصالات والالكترونيات، كلية الهندسة الميكانيكية والكهربائية، جامعة تشرين، اللاذقية سورية.**

مقدمة:

تطورت تقنيات الوسائط المتعددة multimedia والشبكات بشكل كبير مؤخراً. رافق هذا التطور نمواً متزايداً للحركية عبر شبكة الإنترنت، وتزايد متطلبات التخزين بشكل كبير. هذا يعني أن استخدام طرق فعالة لترميز الصور والفيديو لم يعد كافياً، بل أصبح من الضروري استخدام طرق ضغط فعالة لمعطيات الصور والفيديو مع الأخذ بعين الاعتبار الحفاظ على جودة عالية وتقليل حجم التخزين بشكل كبير. وبما أن المعلومات المرسلة عبر شبكة الإنترنت معرضة للهجمات أو الوصول من قبل أشخاص غير مخول لهم ذلك، فإن أمن المعلومات في نظام الوسائط المتعددة أيضاً يمثل جزء هام جداً في الإنترنت. يعتبر التشفير من الطرق الهامة المستخدمة لضمان حماية المعلومات من إساءة الاستخدام والتزوير، فإذا لم يطبق ستوجد إمكانية لسرقة المعلومات [1,2,6].

تشفير الصور هو تحويل الصورة إلى شكل غير مفهوم، لذلك تصبح غير قابلة للقراءة ويمكن أن ترسل بشكل آمن عبر الإنترنت. يتألف نظام ضغط الصور من عمليات تقود لضغط تمثيل الصورة وبالتالي تقليل المتطلبات الكلية للإرسال والتخزين [6]

في عالم اليوم المحوسب والمترابط بشكل كبير، أصبح أمن الصور والفيديو الرقمي ذو أهمية كبيرة في تطبيقات العرض التلفزيوني المدفوع والمؤتمرات الفيديوية السرية والتصوير الطبي وأنظمة التصوير العسكرية أو الصناعية ...، ولكن الإرسال الآمن للصور يحتاج تكلفة أكبر من حيث الزمن وعرض الحزمة والتعقيد [5]. فبالرغم من التقدم السريع في سعة التخزين الشاملة وسرعات المعالجات وأداء نظام الاتصالات الرقمي فإن سعة التخزين المطلوبة للمعطيات وعرض الحزمة المطلوب للإرسال يستمر في تجاوز إمكانية التقنيات المتاحة[1] .

عملياً، يشكل عرض الحزمة وتكاليف التخزين حدوداً قاسيةً على كمية المعطيات المرسلة عبر الإنترنت [5]. إذاً هذا النمو المتزايد للحركية ومتطلبات التخزين والأمن على الشبكة يعني أن خوارزميات ضغط المعطيات يمكن أن تملك أثر كبير على مراكز المعطيات، ويتعلق هذا الأثر بعرض الحزمة ومساحة التخزين الفيزيائية واستهلاك الطاقة [3].

جذب ضغط المعلومات المشفرة اهتمام الكثير من الأبحاث في السنوات الأخيرة، بحيث تعتمد الطريقة التقليدية للإرسال بشكل فعال وآمن على ضغط المعطيات أولاً وذلك لتقليل التكرار، ومن ثم تشفير المعطيات المضغوطة لإخفائها. ولكن في بعض التطبيقات، يحتاج المرسل لإرسال بعض المعطيات للمستقبل، ويأمل بالحفاظ على سرية المعلومات في مشغل الشبكة الذي يقدم موارد القناة من أجل الإرسال. يعني ذلك أنه ينبغي على المرسل أن يشفر المعطيات الأصلية، وقد يميل مزود الشبكة لضغط المعطيات المشفرة دون أي معرفة عن مفاتيح التشفير والمعطيات الأصلية. في جانب المستقبل، تستخدم توابع فك الضغط وفك التشفير لاستعادة الصورة الأصلية [6].

أهمية البحث وأهدافه:

ضغط المعطيات هو أحد مساحات البحث الأساسية في تطبيقات معالجة الصور والفيديو. ومع تطور تقنيات الحاسب والإنترنت، أصبح الكثير من المعلومات المعتمدة على الوسائط المتعددة ترسل عبر الأنترنت والشبكات اللاسلكية. في حال إرسال المعطيات بشكلها الخام فإنها تحتاج عرض حزمة كبير وتتطلب مساحة تخزين كبيرة، وبالنتيجة من المرغوب تمثيل المعلومات بعدد قليل من البتات وذلك باستخدام تقنيات ضغط المعطيات. بنفس الوقت، يجب أن تكون تقنية ضغط المعطيات قادرة على استعادة المعطيات بشكل جيد جداً. يمكن أن يحقق ذلك عبر خوارزميات ضغط وفك ضغط فعالة.

تعتبر خوارزمية DCT وكذلك DWT من الخوارزميات المستخدمة على نطاق واسع في عدة مجالات. يمتلك DCT خاصية ضغط عالية، ويتطلب مصادر حساب منخفضة. من جهة أخرى، DWT هو تحويل متعدد مستويات الدقة،

ويمكنه تحقيق نسب ضغط مختلفة بسهولة. أما بالنسبة لتحويل DST فهو تحويل قليل الاستخدام بالرغم من ميزاته القريبة جداً من ميزات تحويل DCT. وبالإضافة إلى ذلك، يستخدم في إزالة الضجيج من الصور.

وبما أن المعلومات المرسلة عبر شبكة الإنترنت معرضة للهجمات أو الوصول من قبل أشخاص غير مخول لهم بذلك، فإن أمن المعلومات في نظام الوسائط المتعددة أيضاً يمثل جزء هام جداً في الإنترنت. فهو المعايير والإجراءات المتخذة لمنع وصول المعلومات إلى أيدي أشخاص غير مخول لهم بالوصول إليها، وبالتالي ضمان صحة وموثوقية هذا الاتصال.

يعتبر التشفير من الطرق الهامة المستخدمة لضمان حماية المعلومات من إساءة الاستخدام والتزوير. ويعد التبديل طريقة جيدة للتشفير بحيث تتميز ببساطتها وسرعتها، ومن طرق التبديل المشهورة خريطة أرنولد التي تتميز بمستوى أمني عالٍ وبساطةٍ وسرعةٍ بالأداء.

نقدم في هذا البحث خوارزمية هجينة تتألف من مستوى واحد من 2_D DWT و1_D DCT يليه 1_D DST. الفائدة الأساسية من الجمع بين هذه التحويلات هي الحصول على نسبة ضغط عالية جداً مع الحفاظ على جودة استعادة الصورة. وسنطبق في البداية طريقة أرنولد Arnold لتشفير الصورة من أجل حماية المعلومات ورفع المستوى الأمني للخوارزمية. الهدف الأساسي من هذا البحث هو التحقق من أداء الخوارزمية الهجينة المقترحة في مجال واسع من تطبيقات الصور.

طرائق البحث ومواده:

طبقت خوارزمية التشفير والضغط وخوارزمية فك التشفير وفك الضغط على برنامج MATLAB إصدار R2014a. هو برنامج رائد في التطبيقات الهندسية والرياضية. يسمح بالتلاعب حسابياً بالمصفوفات، وبالرسم البياني للتوابع الرياضية، وبتنفيذ الخوارزميات المختلفة، وإنشاء واجهات المستخدم الرسومية، والتواصل مع البرامج المكتوبة بلغات أخرى مثل C و++C وجافا. يستخدم هذا البحث الإمكانيات الكبيرة التي يقدمها المحاكي في مجال معالجة الصورة. سنقوم بتنفيذ الخوارزمية المقترحة، وتحديد البارامترات المرغوب بدراستها، وصولا إلى إتمام عملية المحاكاة وإظهار النتائج ومقارنتها مع الدراسات السابقة لتحديد الخوارزمية الأفضل.

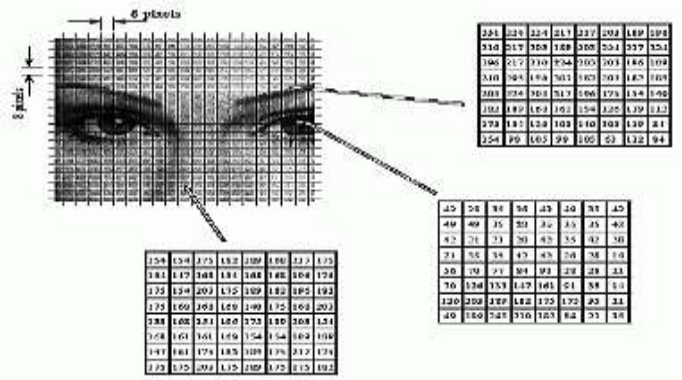
ضغط الصور Compression images

تقلل تقنيات الضغط من حجم المعطيات، والتي بدورها تتطلب عرض حزمة أقل وزمن إرسال أقل وتكلفة منخفضة. يعد ترميز التحويل transform coding من أبرز تقنيات الضغط. يعمل ترميز التحويل على نقل الصورة إلى مجال مختلف آخر (مثل المجال الترددي) ومن ثم ترمز معاملات التحويل الناتجة. تحاول تقنيات ترميز التحويل التقليل من الترابط الموجود بين بكسلات الصورة من خلال استثمار خاصية تركيز الطاقة في معاملات التحويل، وبالتالي فإن كمية كبيرة من الطاقة تتركز في جزء صغير من معاملات التحويل (غالباً تكون معاملات ذات ترددات منخفضة). يسمح لنا هذا بترميز الصورة بمعدل بت صغير بينما يتم الحفاظ على مستوى الجودة والوضوح من أجل التطبيق المعطى [11].

هذه التقنية تأخذ بالحسبان نظام الإدراك البصري للإنسان Visual Human System(VHS)، فالعين البشرية حساسة للترددات المنخفضة أكثر من الترددات العالية لذلك تخزن المعلومات الأكثر أهمية في المعاملات ذات الترددات المنخفضة والأقل أهمية في المعاملات ذات الترددات العالية. يوجد العديد من تراميز التحويل منها:

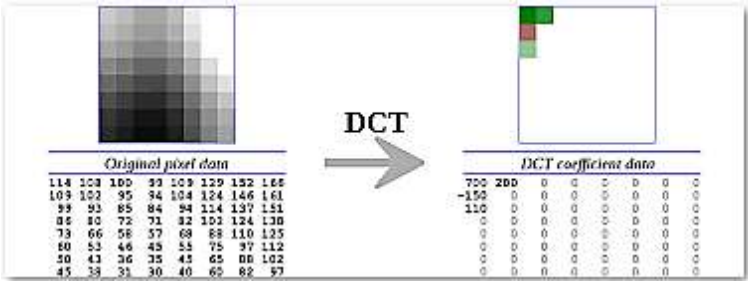
- **التحويل التجيبي المتقطع Discrete Cosine Transform(DCT):**

تحويل DCT تحويل بسيط، يمثل الصورة بعدد من الإشارات التجيبية ذات ترددات ومطالات مختلفة، وهو سهل التطبيق، ويتطلب حجم ذاكرة منخفض مقارنة مع غيره من أنواع التحويل. يقسم الصورة إلى بلوكات n×n (4×4, 8×8,16×16) كما هو مبين في الشكل(1)، ثم يطبق عليها التحويل لينقل الصورة من المجال المكاني إلى تمثيل مكافئ في المجال الترددي.



الشكل (1) مرحلة تقسيم الصورة إلى بلوكات في تحويل DCT

تُركَّز طاقة المعاملات المحولة حول الزاوية العليا اليسرى في مصفوفة المعاملات، بحيث توافق المعاملات في هذه الزاوية الترددات المنخفضة. يوجد قمة من الطاقة في هذه المنطقة (المركبة المستمرة DC)، وتنخفض قيم المعاملات بسرعة إلى الأسفل واليمين من المصفوفة بحيث تمثل هذه الزاوية الترددات العالية (المركبات المتناوبة AC) كما هو مبين في الشكل (2) [1] .



الشكل (2) مرحلة تطبيق تحويل DCT على بلوكات الصورة

إن هذه المعاملات غير مترابطة، هذا يعني أنه يمكن استبعاد المعاملات ذات القيم المنخفضة دون التأثير على جودة الصورة بشكل هام[1] .

- **التحويل المويجي المتقطع Discrete Wavelet Transform (DWT):**

ظهر هذا التحويل كتقنية حديثة في مجال معالجة الصورة. لإنجاز هذا التحويل يتم استخدام مجموعة من المويجات wavelets ذات أنواع مختلفة. فهو يستغل كلاً من الترابط المكاني والترددي للمعطيات من خلال توسيع (أو تقليص) وتمرير المويجة الأم على معطيات الدخل. يدعم تحليل متعدد المستويات Multi–Resolution للمعطيات [8].

مواصفاته مناسبة بشكل جيد من أجل ضغط الصور متضمنة إمكانية أخذ خصائص نظام الإدراك البصري للإنسان بالحسبان وإمكانيات ضغط الطاقة بشكل ممتاز[9].

يقسمDWT معلومات الصورة الأصلية إلى حزمة تقريبية وحزم تفصيلية كما هو مبين في الشكل (3). تُظهِر الحزمة التقريبية (LL) الاتجاه العام لقيم البكسلات، وتظهر الحزم التفصيلية الثلاثة (HL، LH،HH) التفاصيل العمودية والأفقية والقطرية في الصورة على التوالي. في أغلب الأحيان تكون هذه التفاصيل صغيرة جداً لذلك يمكن ضبطها إلى الصفر دون التأثير بشكل مهم على الصورة.

الشكل (3) تطبيق تحويل DWT على الصورة

- **التحويل الجيبي المتقطع Discrete Sine Transform (DST):**

تم إيجاد DST بشكل مشابه لتحويلي DCT و DWT، بحيث يملك بعض الميزات الجيدة من أجل معالجة الصورة وبشكل خاص من أجل إزالة ضجيج الصورة. يملك خاصية تمثيل متعدد المستويات مثل DWT، وهو تحويل سريع وبالتالي يحتاج زمن حساب منخفض. آلية عمل هذا التحويل مشابهة لآلية عمل تحويل DCT. يُستخدم تحويل DST لتمثيل الصورة بعدد من الإشارات الجيبية التي تملك مطالات وترددات مختلفة [10].

بالرغم من أن DST يملك العديد من الخصائص المشابهة لخصائص DCT، إلا أن انتشارDCT كان أوسع في مجال معالجة الصورة [10].

تشفير الصور Image encryption:

التبديل هي تقنية مفيدة جداً في عملية التشفير وذلك بسبب سهولة تنفيذها وسرعتها، والتبديل لا يعني تغيير قيم المعاملات بل تغيير مواقعها فقط [7]. تتم عملية التبديل من خلال تعيين أرقام متتالية لعناصر الصورة ومن ثم إعطاء ترتيب جديد لهذه العناصر بعد التبديل [6].

خريطة القطة للعالم أرنولد Arnold Cat's Map الكلاسيكية هي خريطة ثنائية البعد قابلة للعكس، وتطبق على صورة مربعة كما هو مبين في الشكل (4)، وتوصف بالمعادلات التالية:

$$X_{n+1} = X_n + aY_n mod(N) \quad (1)$$

$$Y_{n+1} = bX_n + (ab+1)Y_n mod(N) \quad (2)$$

$(X_n، Y_n)$ موقع البكسل في الصورة N×N

$(X_{n+1}، Y_{n+1})$ موقع البكسل بعد تطبيق Cat's Map

a,b بارامترات التحكم وهي أعداد صحيحة موجبة و تمثل المفاتيح

(a) الصورة الأصلية (b) الصورة المشفرة (c) الصورة المستعادة

الشكل (4) عملية تشفير وفك تشفير باستخدام Cat's Map

الخوارزمية الهجينة لضغط الصور المشفرة باستخدام التحويلات المويجي والتجيبي والجيبي المتقطعة

عملية تشفير وضغط المعطيات The Process of Data Encryption and Compression:

في البداية، نأخذ الصور بحجم 256×256. أولاً، نطبق خريطة القطة للعالم أرنولد Arnold's Cat Map على الصورة من أجل تبديل مواقع البكسلات والحصول على صورة مشفرة مبهمة الملامح.

ندخل الصورة المشفرة الناتجة إلى مرحلة الضغط التي تبدأ بمستوى واحد من تحويل 2_D DWT الذي يقسم الصورة إلى أربع حزم جزئية LL،LH، HL، HH . بعدها سنقوم بحذف حزم الترددات العالية LH،HL، HH . في هذه المرحلة نكون قد حققنا نسبة ضغط 75%. ثم نطبق تحويل 1_D DCT على كل سطر من المعاملات التقريبية LL، والذي يعطى وفقاً للمعادلة التالية [11]:

$$D_{dct}(i) = \frac{\sqrt{2}}{N} c(i) \sum_{x=0}^{N-1} LL(x) cos(\frac{(2x+1)i\pi}{2N}) \quad (3)$$

$$c(i) = \begin{cases} = 2^{-\frac{1}{2}} & if\ i = 0 \\ = 1 & if\ i > 0 \end{cases}$$

i=0, 1, 2… n−1 تمثل حجم أسطر الحزمة "LL".

D_{dct}معاملات DCT.

LL(x) معطيات الدخل.

تحويل 1_D DCT بدوره سيضغط المعلومات الأكثر أهمية في المعاملات الأولى من كل سطر والتي تمثل معاملات الترددات المنخفضة، بعدها نطبق تحويل 1_D DST على كل عمود من معاملات $D_{dct}(i)$ الناتجة. يعطى تحويل 1_D DST وفقاً للمعادلة التالية[4,9]:

$$D_{dst}(k) = \sum_{i=1}^{n} D_{dct}(x) \sin(\pi \frac{k*x}{n+1}) \quad (4)$$

K=1, 2…N حجم أعمدة الحزمة LL.

$D_{dct}(i)$ معطيات الدخل وهي معاملات DCT.

$D_{dst}(k)$ معاملات DST.

الفائدة الأساسية من استخدام DST في هذا السياق هي أنه يحافظ على جودة الصورة المرمزة من خلال الحفاظ على مكونات الترددات المنخفضة من $D_{dct}(i)$ وزيادة عدد الأصفار، بحيث يمكن أن تستبعد دون التخفيض في الجودة [4]. بعد تطبيقDST، نطبق تكميم على معاملات الترددات المرتفعة من المصفوفة المحولةD_{dst}. بهذه الطريقة، يعني التكميم

ضياع المعلومات غير المهمة فقط من المصفوفة، بحيث يُقَسم كل معامل في المصفوفة على العدد المقابل من مصفوفة التكميم وتقرب النتيجة إلى أقرب عدد صحيح. اقترحنا المعادلة التالية كجدول تكميم [2]:

$$Q(i,j) = Block + (i+j) \quad (5)$$

$$Q(i,j) = Q(i,j) * Scale \quad (6)$$

بحيث Block,...,2,1=i,j و Block,...,3,2,1.....2.0,1.0=Scale.

في المرحلة التالية، نقسم المصفوفة الناتجة إلى مصفوفة ترددات منخفضة Low Frequency ومصفوفة ترددات عالية عمودية Vertical High Frequency ومصفوفة ترددات عالية أفقيHorizontal High Frequency. بالنسبة لمصفوفة الترددات المنخفضة لا تضغط أكثر من ذلك، فقط نمثلها بعدد بتات أقل من خلال الترميز الرياضي. بينما، نضغط مكونات الترددات العالية الأفقية والعمودية باستخدام خوارزمية Minimized Matrix Size Algorithm (MMS). تطبق خوارزمية MMS لتخفيض حجم مصفوفة الترددات العالية بنسبة $2/3$. في البداية، تُحَول المصفوفة ثنائية البعد إلى مصفوفة أحادية البعد، ويتم تعريف ثلاث مفاتيح وضربها بثلاث معاملات متجاورة من مصفوفة الترددات العالية، ومن ثم تجمع القيم لإنتاج قيمة واحدة كما هو مبين في الشكل (5). تخزن القيم الناتجة في مصفوفة جديدة تدعى المصفوفة المصغرة (Minimized−Array). وقبل تطبيق هذه العملية تحسب الخوارزمية القيم المحتمل وجودها في مصفوفة الترددات العالية وتدعى Limited Data كما هو مبين في الشكل (6)، وكون هذه القيم خاصة بالصورة فلا يمكن استخدامها لإعادة بناء معاملات الترددات العالية لصورة أخرى [3]. لا تتعرض Limited Data لأي عملية ضغط بحيث ترسل في ترويسة الملف المضغوط وتستخدم مؤخراً من قبل خوارزمية فك الضغط [4].

تعطى خوارزمية MMS وفقاً للمعادلة التالية[4] :

$$Minimized\_Array_j = K_1 H_i + K_2 H_{(i+1)} + K_3 H_{(i+2)} \quad (7)$$

تُنتَج قيم المفاتيح من قبل خوارزمية مولد المفاتيح وفقاً للمعادلات التالية:

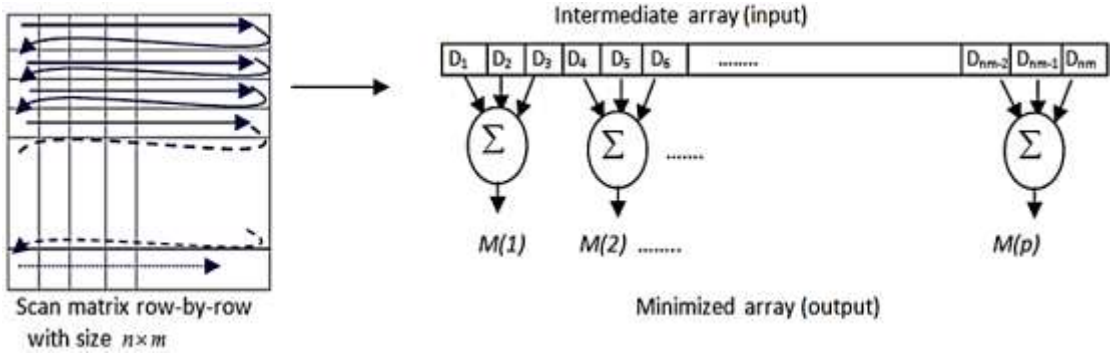
$$M = 2 * Max(H) \quad ; \quad (8)$$

$$K_1 = 1 \quad ; \quad (9)$$

$$K_2 = K_1 + M + Factor \; ; \quad (10)$$

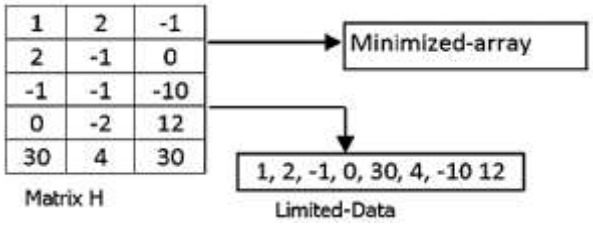
$$K_3 = Factor \times M(K_1 + K_2) \; ; \quad (11)$$

بحيث $\text{Factor} \geq 1$، $K_1 \geq 1$ هي قيم صحيحة. المعامل Factor هو معامل قياس لزيادة درجة الاختلاف بين المفاتيح الثلاث.



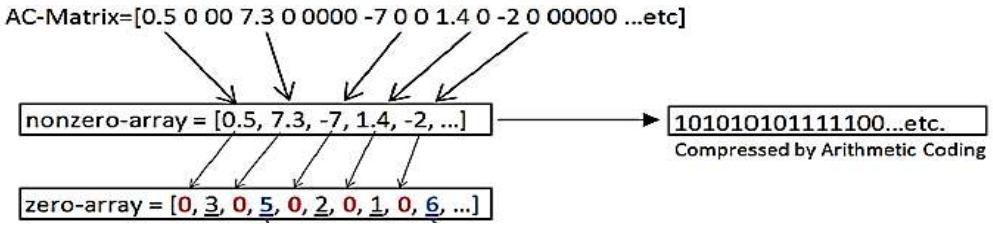
الشكل (5) تطبيق خوارزمية High−Frequency Minimization لضغط المعاملات D من المصفوفة

H (نمسح H سطر_ سطر من أجل الضغط)



الشكل (6) Limited Data

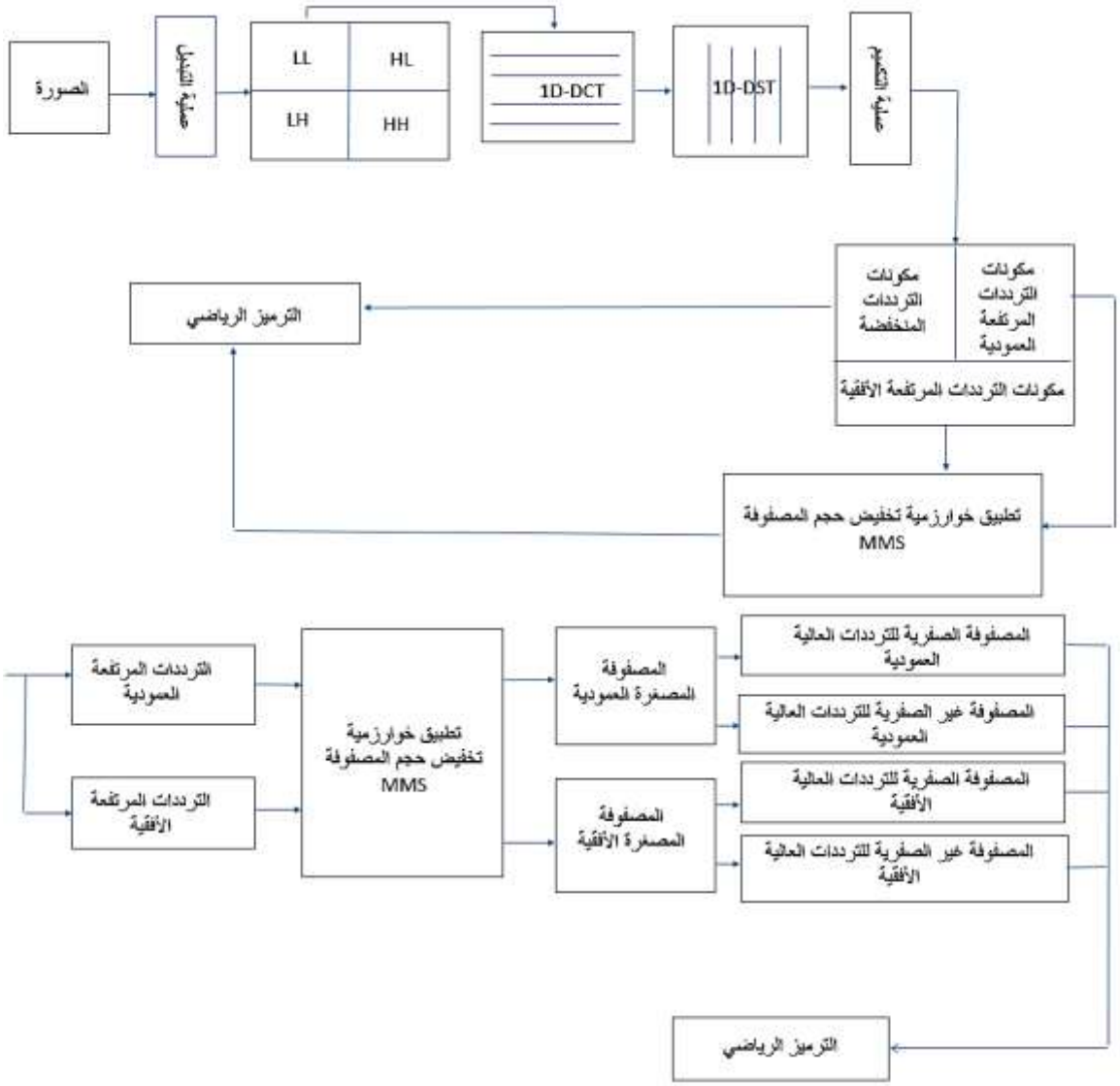
وبما أن مصفوفات الترددات العالية تحوي على كثير من القيم الصفرية مع القليل من القيم غير الصفرية. سنقوم بتقسيم كل مصفوفة من مصفوفات الترددات العالية إلى مصفوفة صفرية ومصفوفة غير صفرية كما هو مبين في الشكل (7) من أجل زيادة نسبة الضغط.



الشكل (7) تقسيم مصفوفة الترددات العالية إلى مصفوفة صفرية ومصفوفة غير صفرية

يمكن أن تحسب المصفوفة الصفرية بسهولة من خلال حساب عدد الأصفار بين كل قيمتين غير صفريتين. مثلاً نفترض المصفوفة AC=[0.5,0,0,0,7.3,0,0,0,0,0,−7]، ستكون المصفوفة الصفرية [0,3,0,5,0] بحيث تشير الأصفار إلى المعطيات غير الصفرية الموجودة في هذا الموقع من مصفوفة الترددات العالية الأصلية، وتشير الأرقام إلى عدد الأصفار بين كل قيمتين غير صفريتين متتاليتين. أما المصفوفة غير الصفرية تحتوي على القيم الموجبة والسالبة [0.5,7.3,−7].

وأخيراً، ندخل المصفوفات الصفرية وغير الصفرية إلى مرحلة الترميز الرياضي من أجل تمثيلها بعدد بتات أقل. تظهر خوارزمية التشفير والضغط المقترحة في الشكل (8).



الشكل (8) المخطط الصندوقي لخوارزمية التشفير والضغط المقترحة في بحثنا

عملية استعادة المعطيات The Process of Data Reconstruction:

يتم الحصول في عملية فك الضغط على سلسلة البتات الناتجة عن الترميز الرياضي. إذاً في الخطوة الأولى، نقوم بتطبيق فك الترميز الرياضي Arithmetic Decoding لنحصل على معطيات الترددات المنخفضة والمصفوفات الصفرية والمصفوفات غير الصفرية للترددات العالية. نقوم بدمج المصفوفة الصفرية والغير صفرية للترددات العالية العمودية لنحصل على المصفوفة العمودية المرمزة Codded Array Vertical، وندمج المصفوفة الصفرية والغير صفرية للترددات العالية الأفقية لنحصل على المصفوفة الأفقية المرمزة Codded Array Horizontal. بعد ذلك، نُدخِل المصفوفات المرمزة الأفقية والعمودية إلى خوارزمية البحث السريع Fast-Matching Search Algorithm(FMS) التي تعتمد على Limited Data والمصفوفة المصغرة Minimized Array والمفاتيح لتستعيد معطيات الترددات العالية الأصلية. بحيث يحوي الملف المضغوط معلومات حول مفاتيح الضغط k1،k2، k3 و Limited Data متبوعة بسلاسل

من معطيات الترددات العالية المضغوطة. لذلك، تلتقط خوارزمية FMS كل معطيات الترددات العالية المضغوطة وتقرأ قيم المفاتيح و Limited Data من أجل استعادة المعطيات الأصلية. نعين خوارزمية FMS عبر الخطوات التالية A و B [2]:

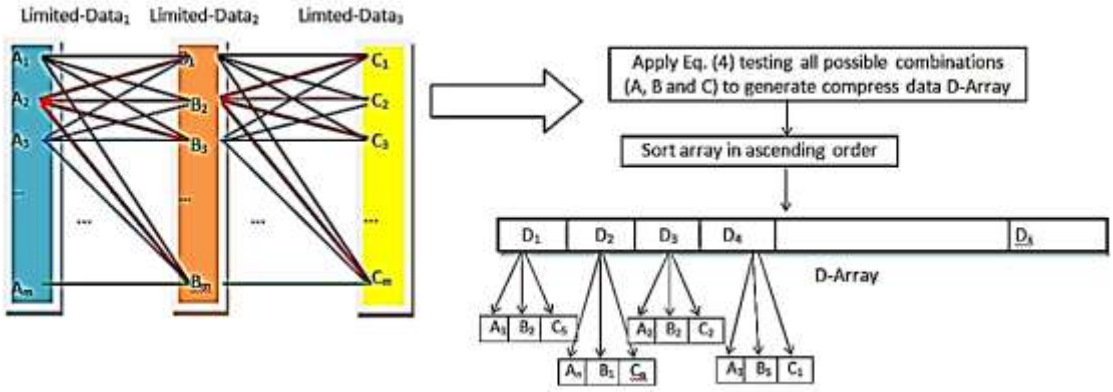
(A) بدايةً، يتم نسخ Limited Data في ثلاث مصفوفات منفصلة مع الأخذ بعين الاعتبار أننا سنستخدم مفاتيح الضغط. تلتقط الخوارزمية ثلاث عينات من المعطيات (واحدة من كل Limited Data)، وتطبق عليها المعادلة التالية:

$$D = k_1 * A_i + k_2 * B_j + k_3 * C_k \quad (12)$$

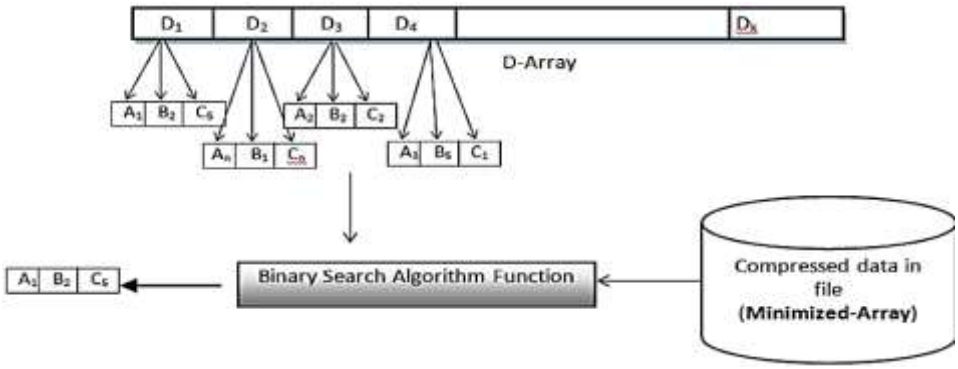
تحتوي مصفوفات Limited Data على نفس القيم A1=B1=C1، A2=B2=C2 وهكذا، ويتم حساب كل احتمالات الجمع كما هو مبين في الشكل (9)، ثم توضع النتائج في المصفوفة D [4].

كمثال على ذلك، نأخذ Limited Data$_1$= [A1 A2 A3]، Limited Data$_2$= [B1 B2 B3] و Limited Data$_3$= [C1 C2 C3]. ستحسب المعادلة (12) 27 مرة (3^3=27) بحيث تختبر كل احتمالات الجمع.

(B) خوارزمية البحث المستخدمة في طريقة فك الضغط هذه تدعى خوارزمية البحث الثنائي Binary Search Algorithm. تقارن هذه الخوارزمية كل قيمة من المصفوفة المصغرة Minimized Array مع عناصر المصفوفة D. إذا توافقت قيمتين، هذا يعني أنه تم إيجاد موقع العنصر المقابل والقيم A، B، C الموافقة لهذا العنصر هي المعطيات المفكوكة الضغط. لا توجد احتمالات "غير موافقة" لأن خوارزمية FMS تحسب كل احتمالات المعطيات المضغوطة كما هو مبين في الشكل (10).



الشكل (9) نسخ Limited Data من أجل خوارزمية FMS وتخمين كل احتمالات الجمع



الشكل (10) فك الضغط باستخدام خوارزمية البحث الثنائي

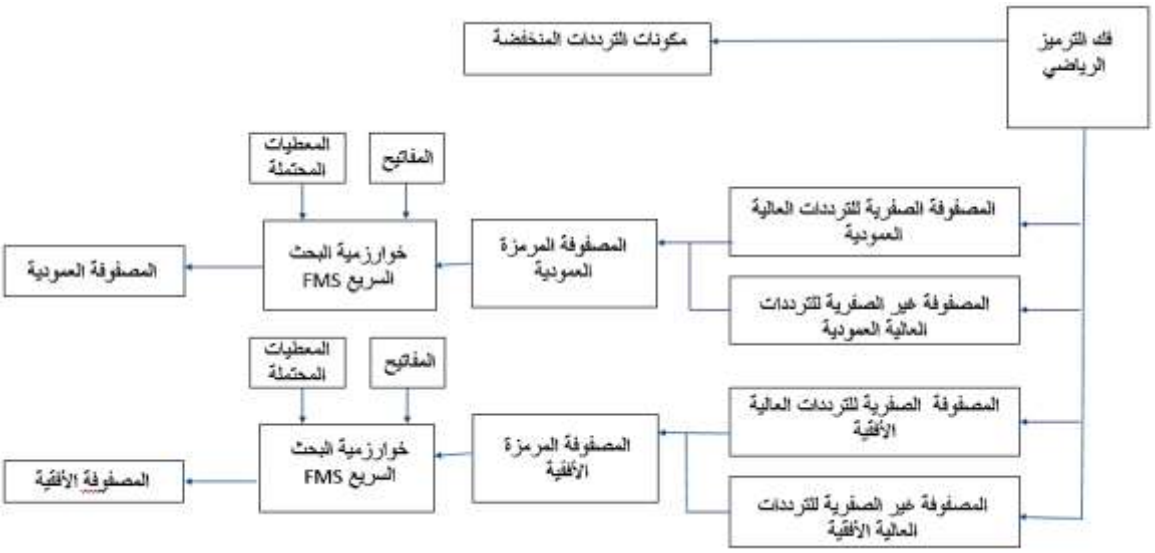
إذاً نحصل في هذه المرحلة على مصفوفات الترددات العالية الأفقية والعمودية، وحصلنا سابقاً على مصفوفة الترددات المنخفضة. نجمع المصفوفات الناتجة وندخلها إلى خطوة التكميم العكسي باستخدام جدول التكميم نفسه المستخدم في خوارزمية الضغط، ثم نطبق تحويل 1_D DST العكسي على المصفوفة الناتجة والتي تمثل مصفوفة معاملات DST. يعطى 1_D DST العكسي وفقاً للمعادلة التالية:

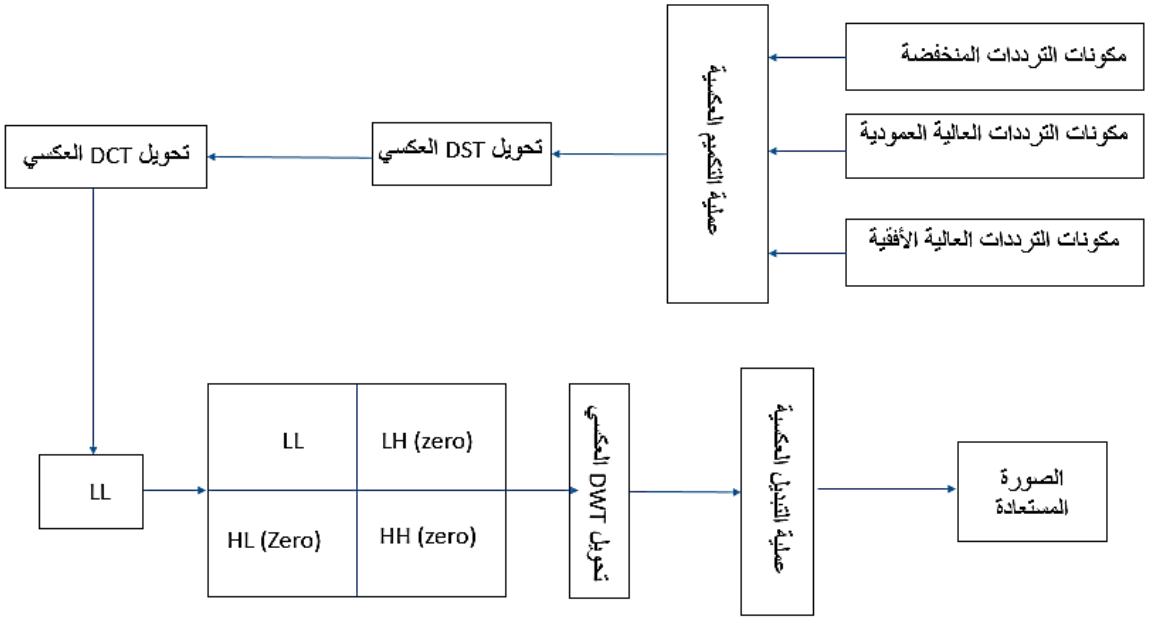
$$D_{dct}(i) = \frac{2}{N+1}\sum_{k=1}^{n} D_{dst}(k)\sin(\pi\frac{k*i}{n+1}) \quad (13)$$

نحصل على مصفوفة معاملات DCT، ثم نطبق عليها تحويل 1_D DCT العكسي الذي يعطى وفقاً للمعادلة التالية:

$$LL(x) = \frac{\sqrt{2}}{N}\sum_{i=0}^{N-1} c(i)D_{dct}\cos(\frac{(2x+1)i\pi}{2N}) \quad (14)$$

نحصل على حزمة الترددات المنخفضة LL المستعادة. أما بالنسبة لحزم الترددات العالية LH،HL، HH نضع فيها قيم صفرية، ثم نطبق عليها تحويل DWT العكسي فنحصل على الصورة المشفرة المستعادة، هنا نكون قد انتهينا من مرحلة فك الضغط. ندخل الصورة المشفرة المستعادة إلى عملية تبديل عكسي من أجل الحصول على الصورة المستعادة. تظهر خوارزمية فك الضغط والتشفير في الشكل (11).





الشكل (11) المخطط الصندوقي لخوارزمية فك الضغط وفك التشفير المقترحة في بحثنا

النتائج والمناقشة:

تم تطبيق الخوارزمية المقترحة على ثمانية صور ذات تدرج رمادي، أربعة صور عادية كما هو مبين في الشكل (12)، وأربعة صور طبية كما هو مبين في الشكل (16). كل هذه الصور لها نفس الحجم (256×256 بكسل) مع مستويات رمادية مؤلفة من 8bits. قمنا بتنفيذ الخوارزمية على برنامج MATLAB R2014a.

Lena Barbara Boat Mandrill

الشكل (12) الصور العادية التي أجري عليه الاختبار

تم تحليل النتائج باستخدام بارامترات التقييم الموضوعي، وهي قمة نسبة الإشارة إلى الضجيج Peak Signal to Noise Ratio (PSNR) ونسبة الضغط Compression Ratio (CR) والجذر التربيعي لمتوسط مربع الخطأ Root Mean Square Error (RMSE).

يستخدم الجذر التربيعي لمتوسط مربع الخطأ RMSE كمقياس لقياس التشتت بين الصورة الأصلية والصورة المستعادة [6]. تعطى المعادلة الممثلة لـ RMSE وفقاً لما يلي:

$$RMSE = \sqrt{\frac{1}{M\times N}\sum_{i=1}^{M}\sum_{j=1}^{N}(A_{i,j} - B_{i,j})^2} \quad (15)$$

بحيث A هي الصورة الأصلية وحجمها M×N.

Bهي الصورة المستعادة وحجمها M×N.

تمثل قمة نسبة الإشارة إلى الضجيج PSNR بالـ dB وفقاً للمعادلة التالية:

$$\mathrm{PSNR} = 10log_{10}\frac{I^2}{MSE} \quad (16)$$

بحيث I هي مستوى دقة بكسل الصورة المسموح. من أجل 8 بت بالبكسل

$$I = 2^8 - 1 = 255 \quad (17)$$

تعطى نسبة الضغط CR وفقاً المعادلة التالية:

$$\text{نسبة الضغط} = \frac{\text{المعطيات االمستبعدة}}{\text{المعطيات الأصلية}} \quad (18)$$

نقيم في عملنا عدة أنظمة مختلفة كما يلي:

النظام 1 يستخدم خوارزميتنا المقترحة

النظام 2 يستخدم التحويلين المويجي والتجيبي المتقطعة في مرحلة ضغط وفك ضغط الصورة المشفرة.

النظام 3 يستخدم التحويل التجيبي المتقطع في مرحلة ضغط وفك ضغط الصورة المشفرة.

النظام 4 يستخدم التحويل المويجي المتقطع في مرحلة ضغط وفك ضغط الصورة المشفرة.

بداية أجرينا اختبار للنظام المقترح من أجل اختيار المويجة الأم التي تحقق جودة أفضل للصورة المستعادة. نُظهِر النتائج الأفضل من كل نوع من المويجات الأم وفقاً للجدول (1)

الجدول (1) المويجات الأم الأفضل

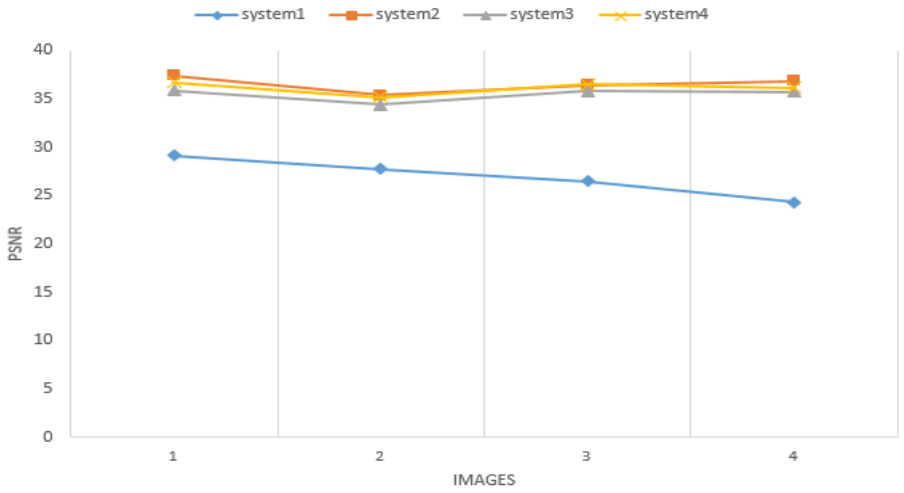
wavelets	PSNR
db7	28.9888
sym5	28.8632
coif3	28.81
rbio1.5	28.7186
bior3.9	29.1446
haar	26.3686

نلاحظ من الجدول (1) أن المويجة bior 3.9 حققت أكبر نسبة PSNR وبالتالي ستعطي أفضل جودة للصورة المستعادة.

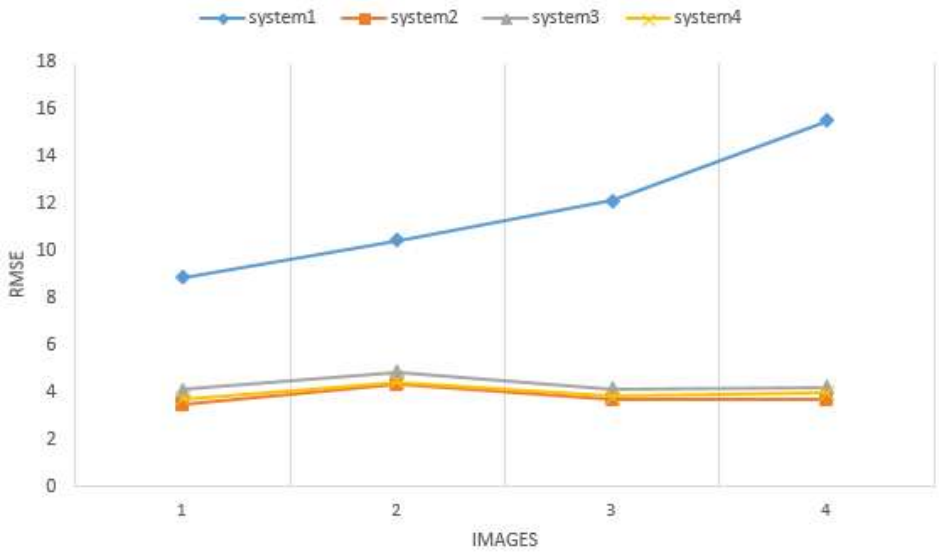
لاختبار أداء نظامنا نقارنه مع الأنظمة الأخرى. نقارن قيم PSNR وRMSE الناتج عن نظامنا المقترح والأنظمة الأخرى وفقاً للجدول (2). علماً أنه تم دراسة متوسط مربع الخطأ MSE Mean Square Error في الدراسات المرجعية، أما نحن أخذنا الجذر التربيعي لمتوسط مربع الخطأ RMSE Root Mean Square Error.

الجدول (2) مقارنة PSNR وRMSE من أجل الأنظمة الأربعة المدروسة

	الصور	نظام 1		نظام 2		نظام 3		نظام 4	
		PSNR(dB)	RMSE	PSNR(dB)	RMSE	PSNR(dB)	RMSE	PSNR(dB)	RMSE
1	Lena	29.1446	8.8983	37.3653	3.4866	35.8653	4.1207	36.7142	3.7370
2	Barbara	27.742	10.4578	35.3995	4.3477	34.3864	4.8856	35.1914	4.4531
3	Boat	26.4528	12.131	36.8370	3.6845	35.8070	4.1484	36.5209	3.8211
4	Mandrill	24.317	15.5128	36.8365	3.6848	35.7074	4.2319	36.1576	3.9843



الشكل (13) مقارنة PSNR من أجل الأنظمة الأربعة المدروسة



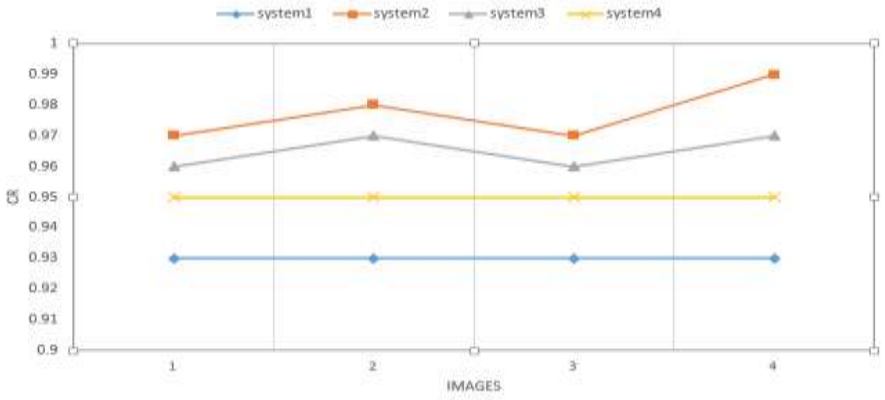
الشكل (14) مقارنة RMSE من أجل الأنظمة الأربعة المدروسة

نلاحظ من الجدول (2) والأشكال (13) و(14) أن نظامنا المقترح حقق نتائج PSNR أدنى وRMSE أعلى من الأنظمة الأخرى، وبالتالي فهو أقل مقاومة للضجيج، ويعطي جودة استعادة أدنى من الانظمة الأخرى.

ونقارن CR الناتجة عن نظامنا المقترح والأنظمة الأخرى وفقاً للجدول (3).

الجدول (3) مقارنة CR من أجل الأنظمة الأربعة المدروسة

	الصور	نظام 1	نظام 2	نظام 3	نظام 4
		CR	CR	CR	CR
1	Lena	0.93	0.97	0.96	0.95
2	Barbara	0.93	0.98	0.97	0.95
3	Boat	0.93	0.97	0.96	0.95
4	Mandrill	0.93	0.99	0.97	0.95



الشكل (15) مقارنة CR من أجل الأنظمة الأربعة المدروسة

نلاحظ من الجدول (3) والشكل (15) أن نظامنا المقترح حقق CR أدنى من الأنظمة الأخرى، وبالتالي يحتاج الملف المضغوط باستخدام نظامنا المقترح حجم في الذاكرة وعرض حزمة أكبر من الملف المضغوط باستخدام الأنظمة الأخرى. ولكن بالرغم من ذلك حجمه صغير يشكل 7% فقط من حجم الملف الأصلي.

نلاحظ من نتائج البارامترات (نسبة الضغط –قمة نسبة الإشارة للضجيج –الجذر التربيعي لمتوسط مربع الخطأ) أن نظامنا المقترح حقق نسبة ضغط وPSNR أدنى وRMSE أعلى من الأنظمة السابقة. بالرغم من ذلك، فإن نسبة الإشارة إلى الضجيج ضمن الحد المقبول، فاستطاعة الإشارة على الأقل أكبر ب 270 ضعف من استطاعة الضجيج.

الشكل (16) الصور الطبية التي أجري عليها الاختبار

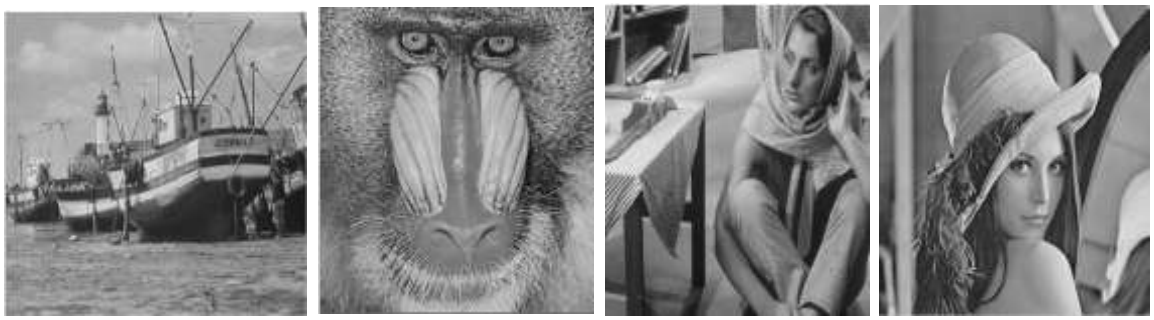
نحسب PSNR و CR و RMSE الناتجة عن تطبيق نظامنا المقترح على الصور الطبية وفقاً للجدول(4)

الجدول (4) CR و PSNR و RMSE الناتجة عن تطبيق نظامنا المقترح على الصور الطبية

	نظام 1			
	images	CR	PSNR	RMSE
1	skull	0.93	30.889	7.2793
2	bones	0.93	33.1002	5.6432
3	Rib cage	0.93	29.3471	8.6932
4	feet	0.93	27.4444	10.8223

نلاحظ من خلال تطبيق نظامنا على الصور الشعاعية الطبية أنه حقق نتائج أفضل من النتائج التي حصلنا عليها في الصور العادية، بحيث أعطى PSNR أعلى ومتوسط خطأ أقل، وهذا يعطينا جودة استعادة أفضل. السبب في ذلك هو أن نظامنا المقترح حقق إمكانية تركيز الطاقة في قيم الترددات المنخفضة للصور الشعاعية أفضل من الصور العادية مما ساهم في الحفاظ على المعلومات المهمة للصورة بشكل أفضل.

نجري التقييم الشخصي على الصور التي تم اختبارها، كما هو مبين في الشكل (17) والشكل (18).



(a) الصور العادية الأصلية

(b) الصور العادية المستعادة

الشكل (17) (a) الصور العادية الأصلية، (b) الصور العادية المستعادة من النظام المقترح

(a) الصور الطبية الأصلية

(b) الصور الطبية المستعادة

الشكل (18) (a) الصور الطبية الأصلية، (b) الصور الطبية المستعادة من النظام المقترح

نلاحظ من التقييم الشخصي للصور العادية أن الصور المستعادة تمتلك جودة جيدة. أما بالنسبة للصور الشعاعية الطبية نلاحظ أن جودة الاستعادة أفضل، فقد تم الحفاظ على معلومات الترددات المنخفضة المهمة في الصور وحذف معلومات الترددات العالية التي لا يدركها نظام الإدراك البصري للإنسان.

نجري اختبار زمن تنفيذ خوارزمية الضغط والتشفير على الصور المستخدمة في الاختبار، فنحصل على زمن تنفيذ وسطي 10.3ثانية. وبالنسبة لخوارزمية فك الضغط وفك التشفير نحصل على زمن تنفيذ وسطي 14.56ثانية. يعتبر هذا الزمن صغير بالنسبة لتنفيذ نظام ضغط وتشفير.

الاستنتاجات والتوصيات:

قمنا في هذا البحث بدراسة وتحليل أداء نظام التشفير والضغط المقترح الذي يعتمد على التحويلات DWT وDCT وDST ومقارنته مع عدة أنظمة أخرى (نظام هجيني يستخدم تحويلي DWT وDCT ونظام تقليدي يستخدم تحويل DWT فقط ونظام تقليدي يستخدم تحويلDCT فقط). أثبتنا من خلال نتائج المحاكاة على MATLAB ما يلي:

1. تحقيق نسبة ضغط CR أخفض من الأنظمة الأخرى.
2. تحقيق قمة نسبة الإشارة إلى الضجيج PSNR أخفض من الأنظمة الأخرى.
3. تحقيق متوسط مربع خطأ RMSE أعلى من الأنظمة الأخرى.
4. تقييم شخصي جيد جداً بالنسبة للصور الطبية، بحيث تم الحفاظ على التفاصيل المهمة في الصورة المستعادة وحذف التفاصيل التي لا يمكن إدراكها في نظام الإدراك البصري للإنسان.

5. تحقيق مستوى أمني عالي للمعلومات، بحيث لا يمكن فك ضغط الصورة إلا بالحصول على قيم المفاتيح التي استخدمت في عملية الضغط، ولكل صورة مفاتيح خاصة بها لا يمكن استخدامها لصور أخرى، وحتى لو تم الحصول على المفاتيح من قبل أشخاص غير مخول لهم سيتم الحصول على صورة مشفرة.

6. زمن التنفيذ الوسطي لخوارزمية الضغط والتشفير 10.3 ثانية، وزمن التنفيذ الوسطي لخوارزمية فك الضغط وفك التشفير 14.56 ثانية.

وبالنتيجة وبعد تحليل النتائج السابقة نوصي باستخدام نظام التشفير والضغط الذي اقترحناه في التطبيقات الأمنية بسبب المستوى الأمني العالي الذي يحققه وفي التطبيقات الطبية بحيث يحقق جودة تشخيص جيدة جداً. وفي المستقبل، يمكن أن يوسع النظام المقترح ليطبق على الصور الملونة.

References:

[1] SIDDEQ,M.M& RODRIGUES,M.A, "Anovel image compression algorithm for high resolution 3D reconstruction," *3D Research,* p. 17, 2014.

[2] SIDDEQ,M.M& RODRIGUES,M.A, "A Novel 2D Image Compression Algorithm Based on Two Levels DWT and DCT Transforms with Enhanced Minimize-Matrix-Size Algorithm for High Resolution Structured Light 3D Surface Reconstruction," *3D Research,* p. 35, 2015.

[3] SIDDEQ,M.M& RODRIGUES,M.A, "A novel high- frequency encoding algorithm for image compession," *EURASIP,* p. 17, 2017.

[4] SIDDEQ,M.M& RODRIGUES,M.A, "DCT and DST Based Image Compression for 3D Reconstruction," *3D research,* p. 19, 2017.

[5] SIDDEQ,M.M& RODRIQUES,M.A, "Applied sequential-search algorithm for compression-encryption of high-resolution structured light 3D data," *In: BLASHKI, Katherin and XIAO,Yingcai,(eds) MCCSIS,* pp. 195-202, 2015.

[6] KHUDHAIR,M.M, "An Efficient System for Encrypted Image by Using Hybrid DWT-DCT Compression Algorithm," *IJCSMC,* pp. 93-102, 2016.

[7] DUREJA,P& KOCHHAR,B, "Image Encryption Using Arnold's Cat Map and Logistic Map for Secure Transmission," *IJCSMC,* pp. 194-199, 2015.

[8] KHUDHAIR,M.M, "An Efficient Image Encryption Technique by Using Cascaded Combined Permutation," *IJCSIS,* pp. 576-588, 2016.

[9] PELAES,E.G& LANO,Y, "IMAGE CODING USING DISCRETE SINE TRANSFORM WITH AXIS ROTATION," *IEEE Transactions on Consumer Electronice,* pp. 1284-1290, 1998.

[10] MALIN,S& MONI,R.S, "Use of Discrete Sine Transform for A Novel Image Denoising Technigue," *IJIP,* pp. 204-213, 2014.

[11] MARTUCCI,S.A, "Symmetric Convolution and the Discrete Sine and Cosine Transforms," *IEEE TRANSACTIONS ON SIGNAL PRO CESSING,* pp. 1038-1051, 1994.