Hybrid hiding in multimedia files

Farah Tareq Mohammed
farahtarik@uomosul.edu.iq
College of computer science and mathematics
University of Mosul

Received on : 12 / 6 / 2011 **Accepted on : 3 / 10 /2011**

ABSTRACT

The principle of hybrid information hiding represented by process of information hiding message (multimedia files) embedded inside another message which is depended on hiding a certain media in another media using different domains (special domain, frequency domain) to provide protection and security for transformed data, this paper suggest an algorithm by using two different files first one compressed binary image, the compression method is run-length and hided this file inside the hostage media by use frequency domain which is represented by Discrete cosine transform (DCT), the second is text ciphered by Caesar method which is depended one secret key by using spatial domain.

The data has been retrieved with no error for both text and binary image after deciphering and decompress process completed; the value of normalization correlation factor for both of them is equal to one.

Key word: Run-length, DCT, PSNR, NC

الإخفاء الهجين في ملفات الوسائط المتعددة

فرح طارق محمد

كلية علوم الحاسوب والرياضيات ، جامعة الموصل

تاريخ استلام البحث: 2011/06/12 **تاريخ قبول البحث: 2011/10/03**

الملخص

يقوم مبدأ الإخفاء الهجين بعملية إخفاء رسالة متمثلة بإحدى ملفات الوسائط المتعددة داخل وسط أخر أو يعتمد على إخفاء وسط معين في وسط أخر باستخدام مجالين مختلفين (المجال المكاني والمجال الترددي) من اجل توفير حماية وأمنية للبيانات المنقولة.

لذا تم في هذا البحث اقتراح خوارزمية تعتمد على دمج المبدأين إذ تم استخدام ملفين مختلفين الأول يتمثل بملف صورة ثنائية مكبوسة باستخدام طريقة الـ run-length وإخفائها داخل وسط مضيف (الصورة الرمادية) باستخدام تحويل جيب تمام المتقطع Discrete cosine transform (DCT) (المجال الترددي) والثاني ملف نصي مشفر باستخدام طريقة قيصر (Caesar Cipher) المعتمدة على مفتاح سري باستخدام طريقة البت الأقل أهمية LSB للإخفاء بالمجال المكاني وقد تم استرجاع البيانات بصورة كاملة للملف النصي والصوري بعد عملية فك الشفرة والكبس وقد كانت قيمة معامل الارتباط التعياري لكليهما يساوي واحداً.

الكلمات المفتاحية: مجال الترددي، البت الاقل اهمية.

1. المقدمة:

خلال السنوات الماضية، أصبح أمن المعلومات محل اهتمام الباحثين لضمان نقل المعلومات بأمان من خلال الشبكة وخاصة شبكة الانترنت دون حدوث أي اختراق أو كشف لتلك المعلومات.

إن نتيجة التزايد المستمر لاستخدام الشبكة والحاسوب في الوقت الحاضر اثر بشكل كبير على ضرورة توفير إجراءات أمنية تعمل على إيصال المعلومة إلى الشخص المخول بشكل لا يبعث للشك والانتباه وتمنع المتطفل أو السارق من العبث بها أو تغيير محتواها لذا فان جميع التقنيات الأمنية سواء في مجال علم التشفير (cryptography) أو علم الخفاء (information hiding) تجري جميعها باتجاه واحد إلا وهو حماية البيانات والمعلومات من معرفة محتواها أو تغييرها وإيصالها إلى الشخص المخول بصورة صحيحة ومتكاملة.[2]

ومن الدراسات السابقة قام الباحث Babita Ahuji باستخدام خوارزمية تحويل الجيب تمام المتقطع (DCT) وخوارزمية البت الأقل أهمية (LSB) لإخفاء البيانات كل على حدة واستخدام نتائج كلتا الطريقتين ومقارنتها بتسليط أنواع مختلفة من الـ Attacks والباحث Jixin Lui اعتمد خوارزمية العلامة المائية الصوتية المتعددة الأغراض تم تقيمها بالاعتماد على مبدأ vector (quantization) الذي يعتمد على مجال تحويل الجيب تمام المتقطع أما الباحث .Mona M بتمثيل خوارزمية تعتمد على دمج طريقة الإخفاء باستخدام البت الأقل أهمية و تقنية الفلترة لتحسين الصورة. [4][8][9]

طرق الإخفاء :

هناك عدة طرائق لإخفاء المعلومات داخل الصور الرقمية في المجالين المكاني والترددي لذا فقد تم اعتماد المجال الترددي باستخدام تحويل جيب تمام المتقطع (DCT) في إخفاء صورة ثنائية مكبوسة بطريقة الـ Run-Length (وهي من الطرق الفعالة في كبس الصور بدون فقدان والتي يتم تمثيلها عن طريق توليد سلسلة متعاقبة من القيم التي تمثل طول كل مجموعة مستمرة من القيم (0), (1)) [5] داخل صورة رمادية حيث تم تقسيم الصورة الغطاء إلى مجموعة من الكتل (blocks) بحجم (4*4 pixels/block) وإيجاد قيمة الـDCT لها كما في المعادلة (1): [3][6]

$$B_{pq}=\alpha_p\,\alpha_q\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}A_{mn}\cos\frac{\pi(2m+1)p}{2M}\cos\frac{\pi(2n+1)p}{2N} \qquad \ldots(1)$$

where:

$$0 \le m \le M-1, \quad 0 \le n \le N-1$$

$$\alpha_p=\begin{cases}1/\sqrt{M} & P=0\\ \sqrt{2}/M & 1 \le p \le M-1\end{cases}$$

$$\alpha_q=\begin{cases}1/\sqrt{N} & q=0\\ \sqrt{2}/N & 1 \le q \le N-1\end{cases}$$

ثم يتم إخفاء bit واحد في كل block (4*4) وعن طريق الاتفاق بين المرسل والمستقبل تم تحديد المعاملات التي يتم استخدامها في عملية التضمين بحيث يضمن إن هذه المعلومات مخزونة في أقسام مهمة من الإشارة من اجل الحفاظ عليها ثم يجري تحويل جيب تمام المعاكس IDCT لكل block كما في المعادلة (2): [3][6]

$$A_{mn}=\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}\alpha_p\,\alpha_q\,B_{pq}\cos\frac{\pi(2m+1)p}{2M}\cos\frac{\pi(2n+1)p}{2N} \qquad \ldots(2)$$

where:

$$0 \le m \le M-1, \quad 0 \le n \le N-1$$

$$\alpha_p = \begin{cases} 1/\sqrt{M} & P=0 \\ \sqrt{2}/M & 1 \le p \le M-1 \end{cases}$$

$$\alpha_q = \begin{cases} 1/\sqrt{N} & q=0 \\ \sqrt{2}/N & 1 \le q \le N-1 \end{cases}$$

وقد تم أيضا اعتماد المجال المكاني في إخفاء النص داخل الصورة الرمادية الحاوية على الصورة الثنائية عن طريق استخدام LSB فعند الإخفاء في الصورة الرمادية يتم تحويل كل قيمة لونية إلى 8-bit وتغيير قيمة الـ bits الأقل أهمية لبيانات الرسالة المرسلةِ. [1][3][6]

2. الخوارزمية المقترحة:

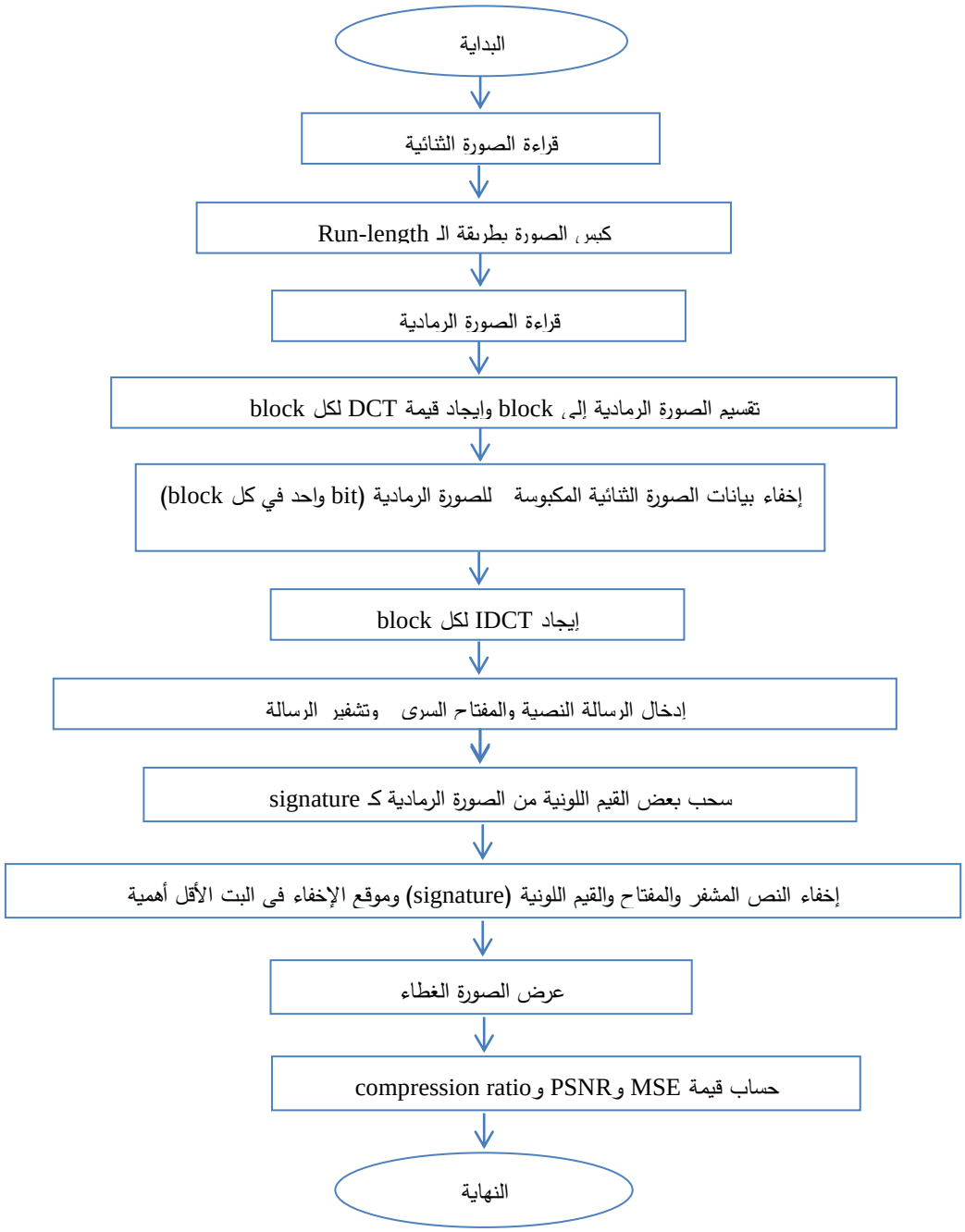
تم تمثيل فكرة العمل بخوارزميتين الأولى تمثل عملية إخفاء صورة ثنائية من نوع BMP (بأحجام (100x100),(150x150)) والتي تم كبسها باستخدام طريقة الـ Run-length داخل الصورة الرمادية بعد تحويلها (صورة الغطاء) إلى المجال الترددي باستخدام تحويل جيب تمام المتقطع DCT إذ تم تقسيم الصورة إلى كتل Blocks كل كتلة بحجم 4X4 pixels/Blocks وإخفاء بيانات الصورة الثنائية (المكبوسة) داخلها بحيث يتم إخفاء bit واحد في كل block في موقع يتم الاتفاق عليه من الطرفين بحيث يتم استرجاع البيانات بصورة صحيحة وبعد إيجاد تحويل جيب تمام المتقطع المعاكس IDCT يتم إخفاء نص مشفر بطريقة متغيرة Caesar (باستخدام مفتاح سري) في بعض القيم اللونية المتفق عليها من قبل الطرفين للصورة الرمادية (لتأكيد من وثوقية بيانات الصورة الغطاء) باستخدام المجال المكاني بطريقة LSB للإخفاء.

أما الخوارزمية الثانية فتمثل عملية استرجاع الصورة الثنائية والنص بصورة صحيحة إذ تم استرجاع القيم اللونية للصورة الرمادية والمفتاح السري وقيم النص المشفر من البت الأقل أهمية للصورة الغطاء وتم اختبار قيمة الـ signature للتأكد من صحة الملف ثم فك الشفرة للنص باستخدام المفتاح السري بعد ذلك يتم تقسيم الصورة الغطاء إلى مجموعة من blocks بنفس الحجم (4X4 pixels/blocks) وإيجاد قيمة DCT لكل كتلة ويتم استرجاع القيم التي تمثل بيانات الصورة الثنائية (المكبوسة) من المعاملات التي تم الاتفاق عليها ثم يتم فك الكبس واسترجاع الصورة الثنائية.

1.2 الخوارزمية (1) (الإخفاء):

لقد تضمنت خوارزمية الإخفاء قراءة صورة ثنائية (binary image) من نوع BMP بشكل مصفوفة ثنائية الأبعاد وبعد كبسها باستخدام طريقة الـ Run-Length تم قراءة صورة رمادية من نوع BMP والتي تمثل ملف الغطاء وتقسيمها إلى مجموعة من blocks بحجم 4X4 pixels/blocks وإيجاد قيمة DCT لكل block وإخفاء بيانات الصورة المكبوسة في مواقع المعاملات المتفق عليها إذ يتم إخفاء bit واحد في كل block ثم إيجاد قيمة تحويل الجيب تمام المتقطع المعاكس لها (blocks) أي تم الإخفاء في المجال الترددي. أما في المجال المكاني فقد تم إدخال بيانات الرسالة النصية وقيمة المفتاح السري و تشفيرها باستخدام طريقة قيصر Caesar method ثم تحويل البيانات الناتجة إلى مصفوفة أحادية بالنظام الثنائي وإخفائها في ملف الغطاء مع بعض القيم اللونية

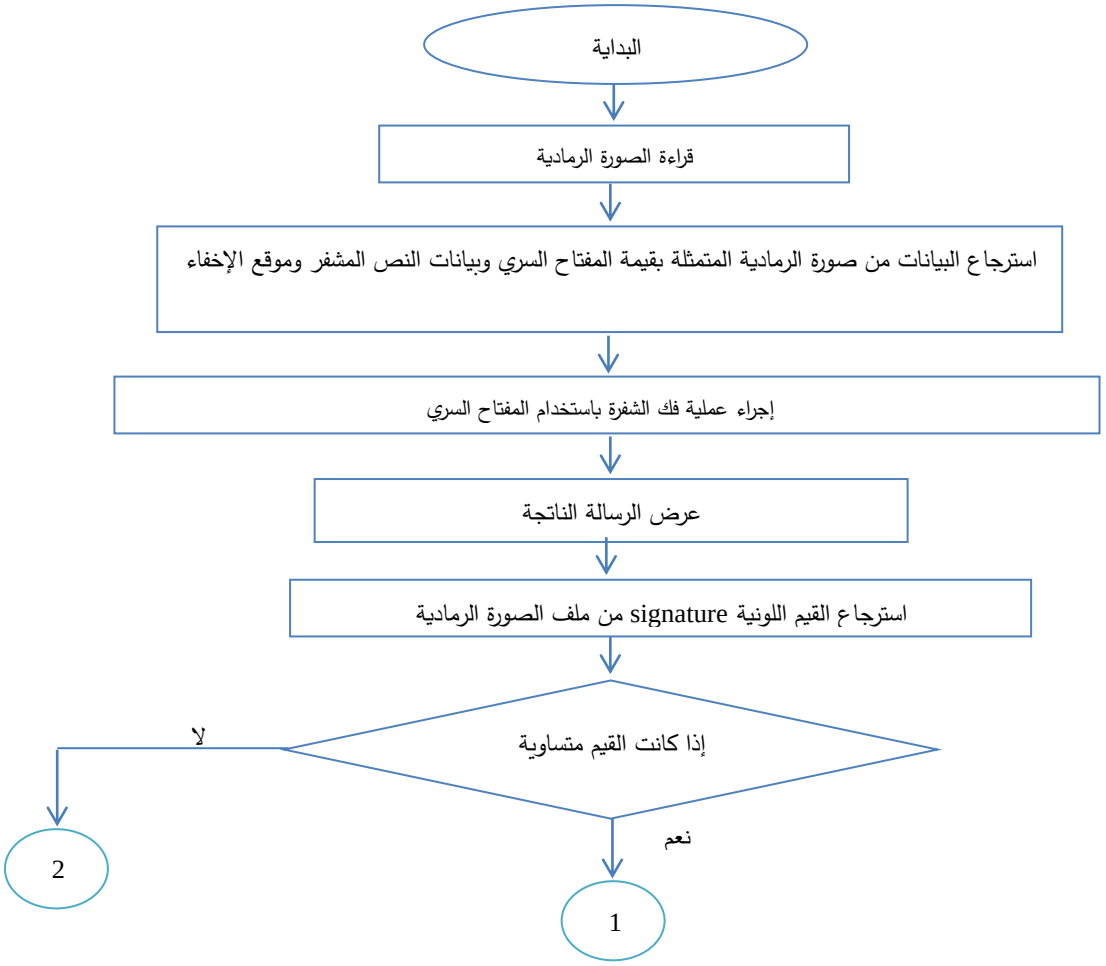
المأخوذة من ملف الغطاء كتوقيع لتأكيد الوثوقية وقيمة المفتاح السري في البت الأقل أهمية (الأولى والثانية) لملف الغطاء وللتأكد من دقة الصورة الرمادية بعد عرضها يتم حساب قيمة متوسط مربع الخطأ (MSE) و(PSNR) ونسبة الكبس للصورة الثنائية (compression ratio) كما موضح في المخطط الانسيابي (1)

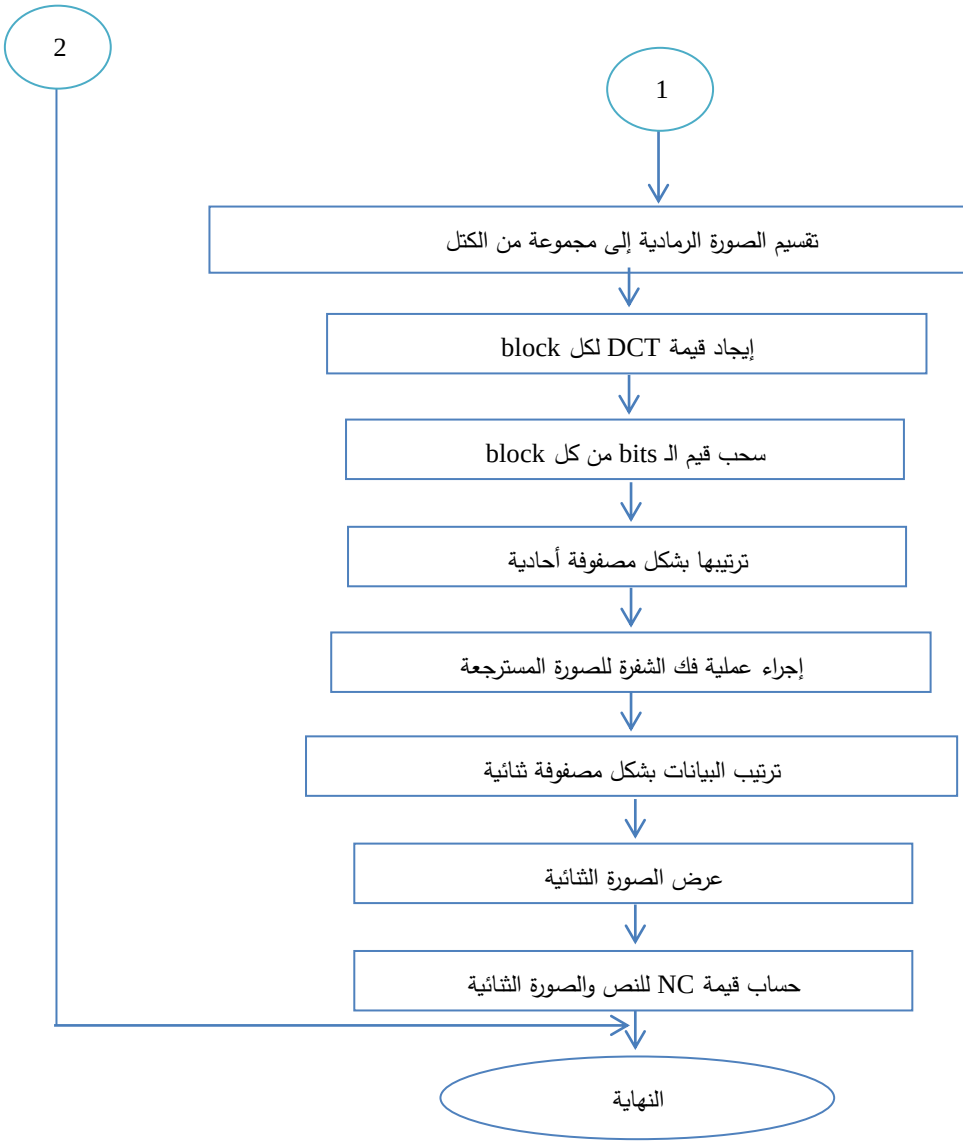


مخطط انسيابي (1). عملية الإخفاء

2.2 خوارزمية (2) (استرجاع الصورة الثنائية والرسالة النصية):

إن فكرة خوارزمية الاسترجاع تتمثل في قراءة صورة رمادية وسحب البيانات التي تم إخفائها في المجال المكاني (قيمة الـ signature والمفتاح السري بالإضافة إلى القيم التي تمثل بيانات الرسالة المشفرة) من البت الأقل أهمية (الأولى والثانية), يتم ترتيب قيم بيانات الرسالة المشفرة بشكل مصفوفة أحادية كل 8bit على حدة لاسترجاع قيم النص الأصلي بعد فك شفرة ثم يتم مقارنة القيم المستخدمة كـ signature مع القيم المسترجعة فإذا كانت القيم غير متساوية فهذا يعني إن ملف الغطاء خاطئ أما إذا كانت القيم متساوية فيتم تقسيم الصورة الغطاء إلى مجموعة كتل بحجم 4X4 pixels/blocks وحساب قيمة تحويل الجيب تمام المتقطع لها وسحب القيم المخزونة من كل كتلة بالاعتماد على الموقع المتفق عليه وخزن الناتج بشكل مصفوفة أحادية والتي يتم إجراء عملية فك الكبس عليها وترتيبها بشكل مصفوفة وعرضها بشكل صورة (الصورة الثنائية). وللتأكد من دقة البيانات المسترجعة يتم حساب قيمة معامل الارتباط التعياري (NC) للصورة الثنائية والرسالة النصية. وكما موضح في المخطط الانسيابي (2)





مخطط انسيابي (1). استرجاع الصورة الثنائية والرسالة النصية

3. النتائج:

إن النتائج المستحصلة من تطبيق فكرة العمل بعد تنفيذها على الصورة الرمادية إذ تم خزن صورة ثنائية مكبوسة بطريقة الـ Run–length والتي كانت بحجم يساوي ثلث حجم ملف الغطاء باستخدام تحويل جيب تمام المتقطع (DCT) حيث تم تقسيم الصورة الغطاء إلى مجموعة من الكتل (blocks) بحجم (4*4 pixels/block) ثم يتم إخفاء bit واحد من الصورة المكبوسة في كل block في المعاملات التي تم الاتفاق عليها ثم يتم إيجاد تحويل جيب تمام المعاكس IDCT لكل block بعدها يتم سحب بعض القيم اللونية من الملف الناتج كتوقيع لتأكيد وثوقية ملف الغطاء ثم يتم إدخال النص وتشفيره بطريقة قيصر التي تعتمد على إدخال مفتاح سري متفق عليه من الطرفين وإخفائه داخل الملف الناتج بالاعتماد على المجال المكاني للإخفاء باستخدام البتين الأقل أهمية LSB مع قيمة المفتاح والقيم الـ Signature في موقع متفق علية من الطرفين.

لقد تم استخدام مقياس متوسط مربع الخطأ (MSE) mean square error و(PSNR) Peak signal to noise ratio للتأكد من جودة الصورة الحاوية على البيانات المخفية (الصورة الثنائية المكبوسة مع النص المشفر وقيمة المفتاح وقيم الـ signature) كما موضح في المعادلة (3) (4)

$$MSE=1/M*N \sum_{i,j}(sw(i,j)-s(i,j))^2 \quad \ldots(3)$$

$$PSNR=20* Log10(255/\sqrt{\frac{1}{M*N}*\sum_i\sum_j(sw(i,j)-s(i,j))^2}) \quad \ldots(4)$$

أما للتأكد من دقة البيانات المسترجعة فقد تم اعتماد مقياس معامل الارتباط التعياري normalization correlation (NC) والموضح في المعادلة (5) وقد كانت النتائج بالنسبة للصورة الثنائية والنص المشفر وقيم الـ signature تساوي واحد (NC=1). [7][10]

$$NC=\sum_i sw(i)*s(i)\ /\ \sum_i\big(s(i)\big)^2 \quad \ldots(5)$$

حيث: sw: تمثل قيم المصفوفة التي تحتوي العلامة المائية, s:مثل قيم المصفوفة الأصلية, M: تمثل عدد الأسطر , N: تمثل عدد الأعمدة

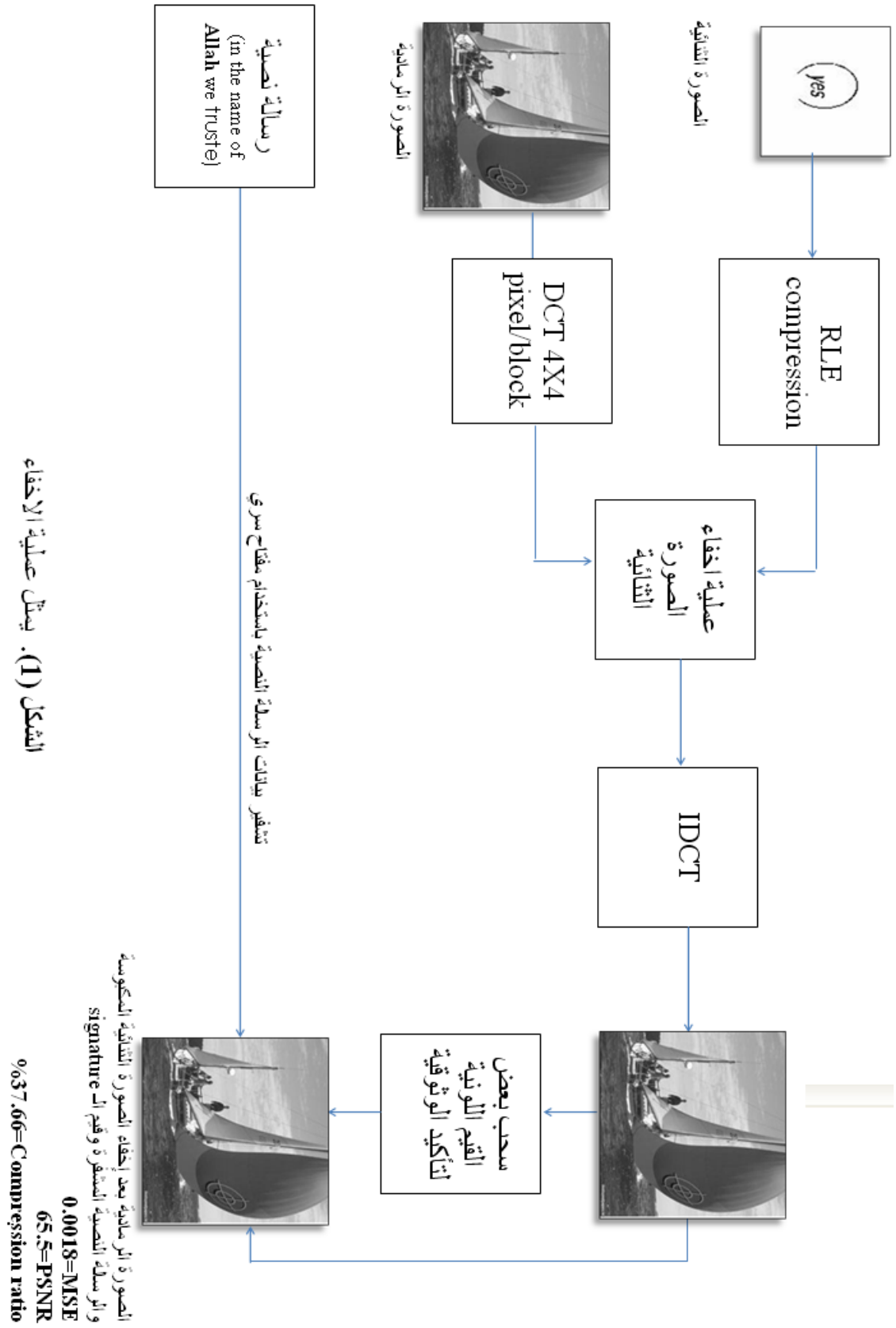
وقد كانت النتائج كما مبينة في الأشكال (1، 2، 3، 4) والجدول (1) والتي تمثل القيم الناتجة في حالة كون الملف الغطاء والملف المخفي (الصورة الثنائية) بالأحجام (420x420)، (150x150).

4. الاستنتاجات:

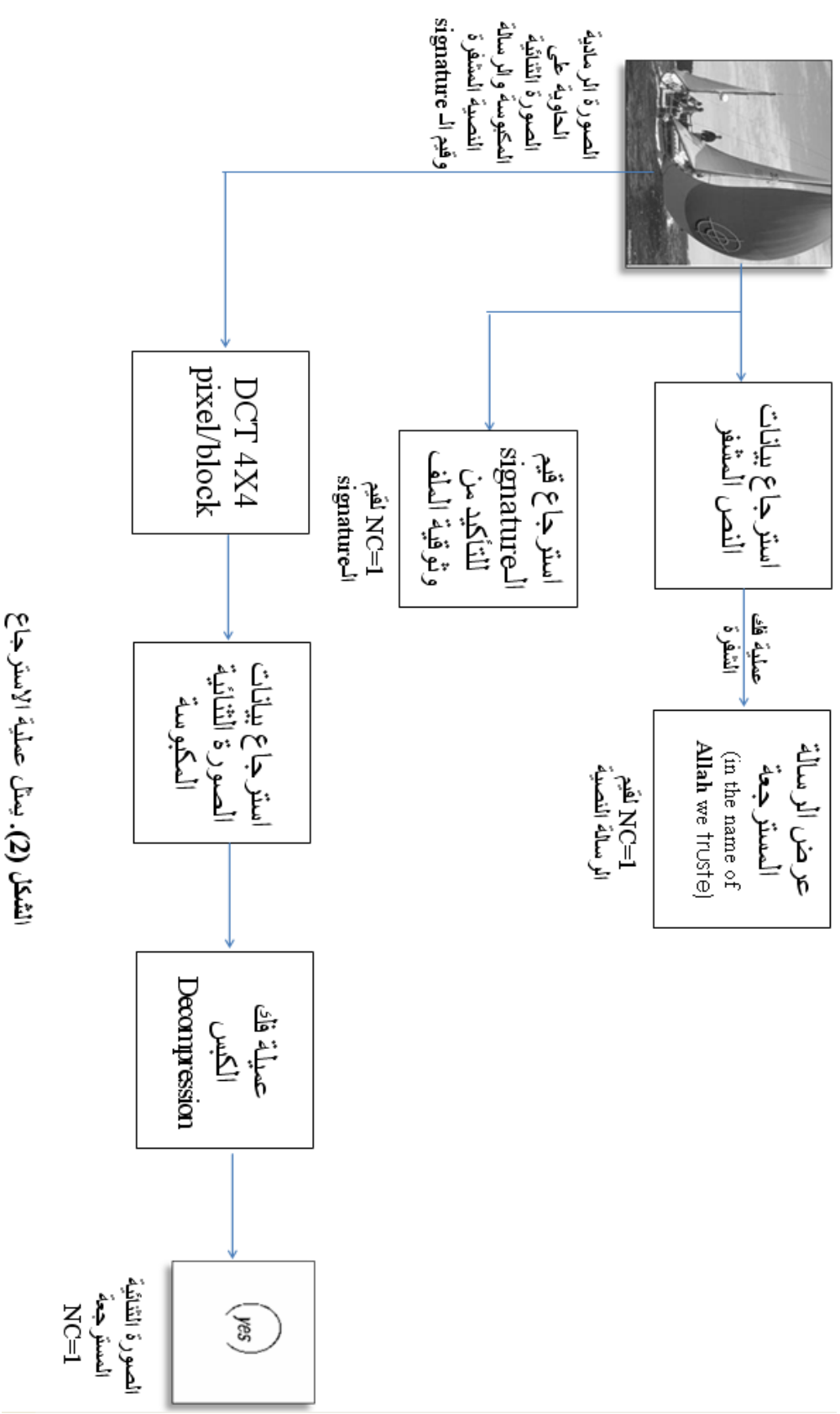
بعد تنفيذ الخوارزمية على عدة أنواع من الصور الثنائية المكبوسة والتي كانت بحجم أكثر من ثلث حجم الصورة الغطاء (حسب ما تم ملاحظته من تطبيق الخوارزمية) إن قيم معامل الارتباط التعياري تساوي واحداً للصورة الثنائية والرسالة النصية وقيم الـsignature أي متطابقة تماما مع القيم المدخلة وبنسبة تشويه غير مدركة وبالمقارنة مع استخدام الخوارزمية بدون كبس الصورة الثنائية فيجب أن يكون حجم ملف الغطاء يساوي أربعة أضعاف الملف المخفي (الصورة الثنائية) أي نحتاج لعملية الإخفاء بطريقة DCT ملف غطاء اكبر من حجم الملف المستخدم في هذه الخوارزمية أما بالنسبة لقيمة مربع الخطأ فقد تفاوتت بمدى بسيط جداً مما يدل على كفاءة الخوارزمية وجودتها في هذا التطبيق.

جدول (1)

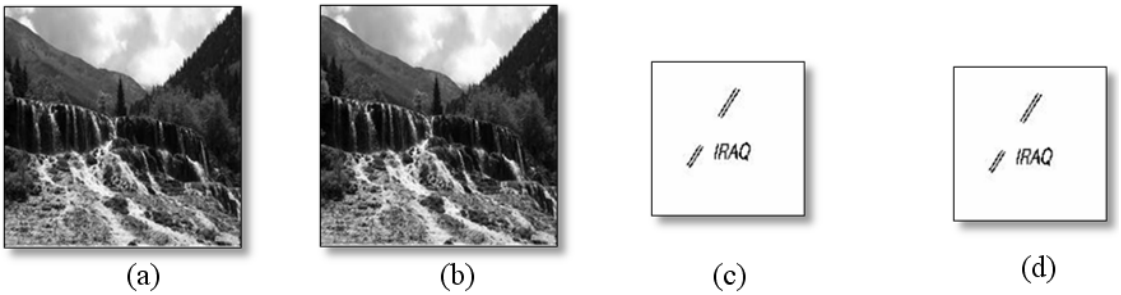
Figures	Compression ratio %	100-compression %	Test (size)	MSE	PSNR	NC
Figure(1)	25.94%	74.06%	36 char	0.0107	67.83	1
Figure(3)	26.56%	73.44%	34 char	0.0100	68.13	1
Figure(4)	22.33%	77.67%	48 char	0.0120	67.33	1



الشكل (1). يمثل عملية الإخفاء



الشكل (2). يمثل عملية الاسترجاع



الشكل (3)

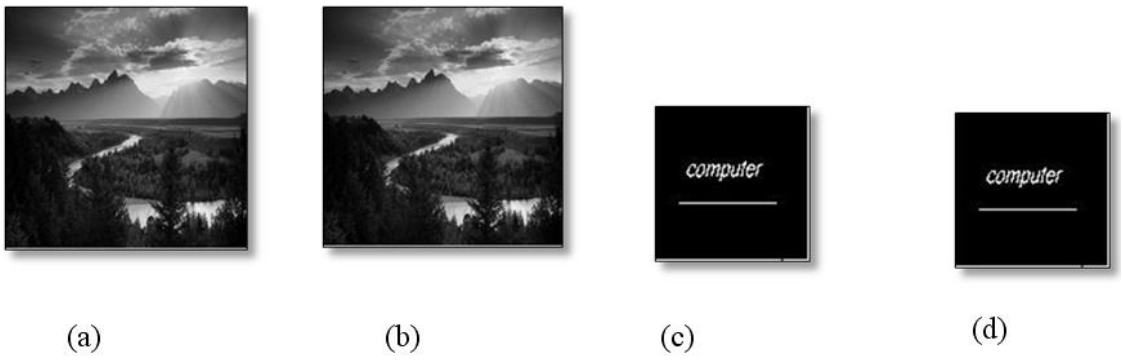
(a) الصورة الرمادية الأصلية

(b) الصورة الرمادية الحاوية على الصورة الثنائية المكبوسة والنص ((Iraq) we love our country)

(c) الصورة الثنائية الأصلية

(d) الصورة الثنائية بعد الاسترجاع

قيم الـ NC=1 لبيانات الصورة الثنائية و النص, MSE=0.0020



الشكل (4)

(a) الصورة الرمادية الأصلية

(b) الصورة الرمادية الحاوية على الصورة الثنائية المكبوسة والنص (university of Mosul-computer science)

(c) الصورة الثنائية الأصلية

(d) الصورة الثنائية بعد الاسترجاع

قيم الـ NC=1 لبيانات الصورة الثنائية و النص, MSE=0.

5. أعمال مستقبلية:

1. تطبيق الخوارزمية المقترحة على أنواع أخرى لملفات الوسائط المتعددة.
2. دمج أكثر من طريقة للإخفاء بالمجال الترددي لإخفاء أكثر من نوع من ملفات الوسائط المتعددة.

المصادر

[1] الحمامي, علاء حسين, محمد حسين, 2008، "إخفاء المعلومات الكتابة المخفية والعلامة المائية", مكتبة جامعة الشارقة ص 29-84-102.

[2] طه, دجان بشير, احمد سامي نوري, نجلاء بديع إبراهيم , 2010، "تشفير وإخفاء المعلومات في ملفات الانترنيت XML,HTML" كلية علوم الحاسبات والرياضيات, مجلة الرافدين لعلوم الحاسبات والرياضيات المجلد 7, العدد 1.

[3] Ajit Danti, Preethi Acharya, 2010, "Randomized embedding scheme Based on DCT coefficients for image steganography", JNN college of engineering recent trends in image processing and pattern recognition RTipp. P99.

[4] Babita Ahuja, Manpreet Kaur, May 2009, "high capacity filter based steganography", manar rachna college of engineering department of science Faridabad, India, international of recent trends in engineering, vol. 1, no. 1, pp 672.

[5] Gonzalez R. C., Woods R.E., 2008, "Digital image processing", university of Tennessee, third edition.

[6] H.B. Kekre, Archana Athawale, Pallavi. N. Halarmkar, July 2010, "increased capacity and high security for embedding secret message in transform domain using discrete cosine transform", journal of science engg. Of tech. mgt. vol. 2.

[7] Huajian Liu (2008), "digital watermarking for image content", Geboren in Shandong, China, p 47.

[8] Jixin Lui, Zherning Lu, 2009, "a multipurpose audio watermarking algorithm based on vector quantization in DCT domain", world academy of science, engineering and technology pp618.

[9] Mona M. El-Ghoneimy, 2008, " comarision between tow watermarking Algorithms using DCT coefficient and LSB replacement", associate professor, Elect. & comm. Dept., faculty of engineering, Cairouniversity, Journal of theoretical and Applied information technology, p 132.

[10] Teruya Minamolo, Kentaro Aoki, June 2010, "A blind digital image watermarking method using interval wavelet decom position", international journal of signal processing, image processing and pattern recognition, vol. 3, no. 2, department of information science, Saga university, Japan.