Chaotic Image Steganography using DCT and DWT

Nadia M. Mohammed
nadia.m.mohammed@uomosul.edu.iq
College of Computer Science and Mathematics
University of Mosul

Received on: 12/02/2012 **Accepted on: 28/06/2012**

ABSTRACT

The researchers was interest in the issue of security from long time ago even arrived to the current age (the digital age), and because of the importance of this topic and the challenges in it, so this work which included study and application of new algorithm is proposed to achieve a high level of security by encrypting the secret message (image) using the Logistic Chaotic function after the implementation of Discrete Wavelet Transform (DWT). In the next phase, it has been implemented the Discrete Cosine Transform (DCT) on the cover (image) and then hide the secret message within encrypted data in which the adoption of the principle of random Blocks which is determined by chaotic series.

Deliberately proposed algorithm to provide more of an advantage in it's work, provide ingreliability through data encryption, message security, and provided a very high degree of security through the adoption of the principle of random selected passages Chaotic, increasing the efficiency of the work of the algorithm and the degree of security.

After the application it must be the use of performance measurements, so the following was used (NC, BER, PSNR, MSE). The language was Matlab9.

Keywords: Chaotic, DWT, DCT.

الاخفاء الفوضوي للصور باستخدام DWT & DCT

نادية معن محمد

كلية علوم الحاسوب والرياضيات

جامعة الموصل، الموصل، العراق

تاريخ استلام البحث: 2012/02/12 **تاريخ قبول البحث: 2012/06/28**

الملخص

تتمتع مسألة السرية بأهتمام الباحثين منذ امد بعيد حتى وصلت للعصر الحالي (العصر الرقمي)، ولاهمية هذا الموضوع وكثرة التحديات الموجودة فيه كان هذا العمل الذي اشتمل على دراسة وتطبيق خوارزمية جديدة مقترحة لتحقيق مستوى عالٍ من السرية عن طريق تشفير الرسالة السرية (صورة) بأستخدام الدالة اللوجستية الفوضوية بعد تنفيذ Discrete Wavelet Transform (DWT). وفي المرحلة التي تليها تم تنفيذ (DCT) Discrete Cosine Transform على الغطاء (صورة) ومن ثم اخفاء بيانات الرسالة السرية المشفرة فيها باعتماد مبدأ Blocks العشوائية التي يتم تحديدها عن طريق السلسلة الفوضوية.

عمدت الخوارزمية المقترحة الى توفير اكثر من ميزة في عملها، إذ وفرت الوثوقية عن طريق تشفير بيانات الرسالة السرية، كما وفرت درجة سرية عالية جدا من خلال تبني مبدأ المقاطع العشوائية المختارة فوضوياً مما زاد في كفاءة عمل الخوارزمية ودرجة سريتها.

بعد التطبيق كان لابد من استخدام مقاييس كفاءة لبيان جودة العمل، حيث تم اعتماد (NC، BER، PSNR، MSE). اما اللغة فكانت Matlab9.

الكلمات المفتاحية: الفوضى، DWT، DCT.

1_المقدمة

ان مسائل امنية المعلومات اصبحت من الموضوعات الحساسة والمهمة جدا في حياة البشر بخاصة بعد انتشار الحكومات الالكترونية في معظم دول العالم، ومن هنا ظهر علم الاخفاء (Steganography) الذي يعد النظام الجديد والمتمم لعلم التشفير(Encryption) وقد استغرق وقتا طويلا في تناقل الرسائل السرية والمهمة عبر الشبكات والانترنت، كما يعد من طرائق الحماية التي تجعل البيانات المرسلة غير مرئية وذلك باخفاء رسائل معينة داخل غطاء معين.

ان الذي شجع ايضا على احياء وتطوير تقنية الاخفاء هو الانفجار الهائل في تقنية الحاسوب والاتصالات، والشئ المميز فيها انها تواكب التقنيات الحديثة. وان هذه التقنية لها استخداماتها في جميع الوسائط الحاسوبية من صور, نصوص, صوت وفيديو....الخ. [1]

2_دراسات سابقة

في [2007]، اقترح الباحث Peipei Liu واخرون طريقة جديدة للاخفاء باستخدام الخريطة الفوضوية، إذ قاموا اولا بتقسيم الصورة الغطاء الى مجموعة من المقاطع ذات حجم (8*8) ثم تنفيذ DCT على كل مقطع، واخيرا طمر الرسالة السرية ضمن المقاطع التي يتم تحديدها عن طريق الخريطة الفوضوية باستخدام الدالة اللوجستية. [2]

وفي [2009] قام الباحث Guang-ming Yang واخرون بتحسين طريقة الاخفاء (LSB) Least Significant Bitوذلك من خلال استخدام نظرية الفوضى ، إذ تم تحديد مواقع الـ bits التي سيتم الاخفاء فيها فوضويا باستخدام الدالة اللوجستية. [3]

3_مفاهيم عامة

في هذه الفقرة سيتم تقديم بعض المفاهيم والتوضيحات الخاصة بمفردات البحث:

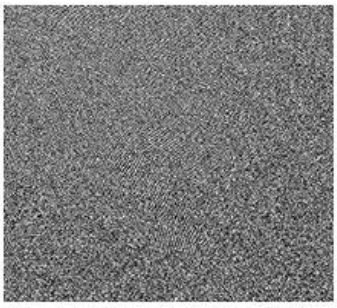
أ- **تحويل المويجة المتقطع Discrete Wavelet Transform (DWT)**

هو تحويل عام وقوي انتشر بشكل واسع في السنوات الاخيرة، ونجح باستخدمه في العديد من المجالات ابرزها مجال الصور، تتلخص الفكرة الاساسية في عمل تحويل المويجة بتقسيم الصورة الى 4 اجزاء (LL1,LH1,HL1,HH1), حيث يمثل (LL1) جزء التردد الواطئ، اما بقية الاجزاء فتمثل محتويات التردد العالي باتجاه قطري، عمودي او افقي، لاحظ الشكل (1). للحصول على المستوى الاخر لتحويل المويجة، سيتم تقسيم الجزء (LL1) الى 4 اجزاء اخرى وهكذا. ان سبب استخدام هذا التحويل يعود الى ميزته في الحصول على أنموذج مصغر للصورة الاصلية ولقد اعتمد التقسيم في البحث الى مرحلة واحدة فقط. [1][4]

الشكل (1): الصورة بعد تطبيق تحويل المويجة

ب- تحويل جيب التمام المتقطع Discrete Cosine Transform (DCT)

هو التحويل الأكثر شيوعًا نظرًا لفعاليته ومرونته، ويتم تطبيقه على عينات من الإشارة. ومن خصائصه أنه تتم تجزئة الصورة إلى"مقاطع" Blocks (NxN) ثنائية البعد بحيث تمثل Coefficients اي مصفوفة أخرى ثنائية البعد من معاملاتPixels NxN لاحظ الشكل(2). استخدم هذا التحويل في البحث نظرا لطبيعته في تقسيم الصورة الى مجموعة مقاطع (Blocks) تعود بالفائدة على الفكرة المرجوة في الاخفاء. [2]



الشكل (2): الصورة بعد تطبيق تحويل جيب التمام

ج- الفوضى (Chaos)

واحدة من السلوكيات التي تربط الانظمة غير الخطية والتي تحدث تطورا في القيم المحددة لنظام المعلومات، اذ عد اكتشاف هذا النظام العشوائي ثورة ادت الى العديد من القضايا المترابطة ونظرية الاستقرار وميزات هندسية جديدة وعروض لتمييز التواقيع. استخدمت الدالة الفوضوية أساساً لتطوير النماذج الرياضية واجتذبت العديد من الرياضيين بسبب الحساسية العالية للقيمة الابتدائية وتطبيقاتها لمشاكل الحياة اليومية. [4]

تم استخدام الدالة الفوضوية في تشفير واخفاء البيانات لما تمتاز به من خصائص: [5]

1. التعقيد العالي والتصرفات غير الخطية.
2. الحساسية المعتمدة على القيمة الابتدائية.

عند اعطاء قيمة ابتدائية لنظام معين فمن المعروف انه يمكن توقع الحالة المستقبلية للنظام الا انه في انظمة الفوضى فان توقع المدى البعيد يستحيل التنبؤ به. [6]

- **الدالة اللوجستية (Logistic Map)**

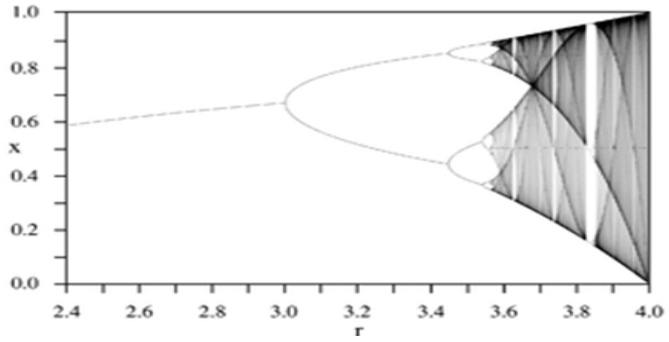
تمثل احد انواع الدوال الفوضوية والتي تم دراستها لاول مرة عام 1960. لوحظ اهتمام الكثير بها لما تمتاز به من خصائص، إذ ان القيم المحددة التي تنشئها هذه الدالة هي قيم عشوائية تماما في صيغتها (على الرغم من انها تقع ضمن حدود معينة)، وهذه القيم لاتتكرر حتى بعد عدد من الدورات، واهم صفة لهذه الدالة

هي حساسيتها للقيمة الابتدائية مما جعلها ذات اهمية عالية في مجال التشفير والاخفاء. اما التمثيل الرياضي للدالة فهو ممثل بالمعادلة التالية: [2][3]

$$X_{n+1} = \mu\,(1-X_n)\,X_n \quad \ldots(1)$$

حيث ان:

X_{n+1} عدد حقيقي يتراوح بين $(0, 1)$ $(0 \geq X_{n+1} \geq 1)$, وX_n تمثل القيمة الابتدائية، و(μ) قيمة موجبة تتراوح قيمتها بين $(0, 4)$ $(0 \geq \mu \geq 4)$. لاحظ الشكل (3): [4]



الشكل (3): الرسم البياني التشعبي لسلوك الدالة اللوجستية [4]

4_خوارزمية التشفير الفوضوي

وتستخدم لتشفير الرسالة السرية (Secret Image) وتتلخص بما يأتي: [5][7]

<u>الخطوة (1)</u>: قراءة الصورة السرية الثنائية (S') ذات حجم (m*m).

<u>الخطوة (2)</u>: اعطاء القيمة الابتدائية لكل من X_0 , μ (اللذين يعدان مفتاحا التشفير), $0 \geq X_0 \geq 1$، μ ə [5, 4, 3]، وهذه القيم (X_0، μ) لابد من الاتفاق عليها مابين المرسل والمستقبل قبل البدء بالعمل.

<u>الخطوة (3)</u>: استخدام المعادلة رقم (1) (معادلة الدالة اللوجستية) لتوليد سلسلة من الارقام الحقيقية (R) ذات حجم (m^2).

<u>الخطوة (4)</u>: تحويل السلسلة (R) الى سلسلة ذات ارقام ثنائية باستخدام المعادلة الآتية :

$$R'_k = \begin{cases} 0 & \text{if } R_k < 0.5 \\ 1 & \text{if } R_k > 0.5 \end{cases} \quad \ldots(2)$$

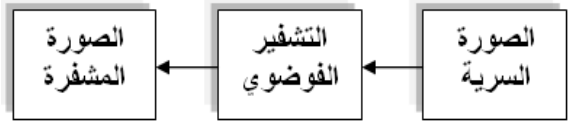
حيث ان k= 0,1,2 ,....., m^2.

<u>الخطوة (5)</u>: تشفير الصورة السرية (S') باستخدام المعادلة الآتية :

$$S''(i,j) = S'(i,j) \oplus R'_k \quad \ldots(3)$$

حيث ان :

$m-1 \geq i \geq 0$, $m-1 \geq j \geq 0$, $m^2-1 \geq k \geq 0$. لاحظ الشكل (4).



الشكل (4): تشفير الصورة السرية

5_الخوارزمية الفوضوية

ان الخوارزمية الفوضوية المستخدمة في الاخفاء ستنفذ كالاتي: [3][8]

الخطوة (1): اعطاء القيمة الابتدائية لـ X_0، والتي تمثل بذرة (seed) الدالة اللوجستية وتعد المفتاح الاول للاخفاء.

الخطوة (2): تنفيذ الدالة اللوجستية (المعادلة رقم (1)) لـ (n-1) من المرات لتكوين السلسلة الآتية:

$$X=\{ X_1, X_2, X_3,..... , X_{n-1}\}$$

إذ ان n تمثل طول الرسالة السرية.

الخطوة (3): ترتيب السلسلة الناتجة تصاعدياً لتكوين سلسلة جديدة ('X):

$$X'=\{ X'_0, X'_1, X'_2, X'_3,..... , X'_{n-1}\}$$

الخطوة (4): ايجاد موقع كل عنصر موجود في السلسلة (X) ضمن السلسلة ('X) لتكوين سلسلة التحويل (T) والتي تعد المفتاح الاخر للاخفاء :

$$T=\{ t_0, t_1, t_2, t_3,..... , t_{n-1}\}$$

ان السلسلة (T) التي تم تكوينها من هذه الخوارزمية (والتي ستحدد ارقام المقاطع (Blocks) المستخدمة في الاخفاء) ستحتوي على قيم تتراوح بين(n,1) مرتبة بشكل عشوائي وغير متسلسل.

6_خوارزمية الاخفاء المقترحة

ان خوارزمية الاخفاء المقترحة ضمن مجال DCT ستنفذ كالاتي:

الخطوة (1): قراءة الصورة الغطاء (C) ذات الحجم n*n.

الخطوة (2): قراءة الصورة السرية (S) ذات الحجم m*m.

الخطوة (3): تنفيذ DWT على الصورة السرية (S).

الخطوة (4): تحويل الصورة الناتجة الى صورة ثنائية ('S) ممثلة بالرمز (0,1).

الخطوة (5): تشفير الصورة السرية الناتجة باستخدام خوارزمية التشفير الفوضوي للحصول على الصورة المشفرة ("S).

الخطوة (6): تنفيذ DCT على الصورة الغطاء(C).

الخطوة (7): تقسيم الصورة الناتجة الى مجموعة من المقاطع (blocks) ذات حجم (3*3).

الخطوة (8): تكوين السلسلة الفوضوية (T) ذات الحجم n^2 (مفتاح الاخفاء الثاني) عن طريق تنفيذ الخوارزمية الفوضوية (للحصول على ارقام المقاطع (blocks) العشوائية بالاعتماد على قيم السلسلة (T)).

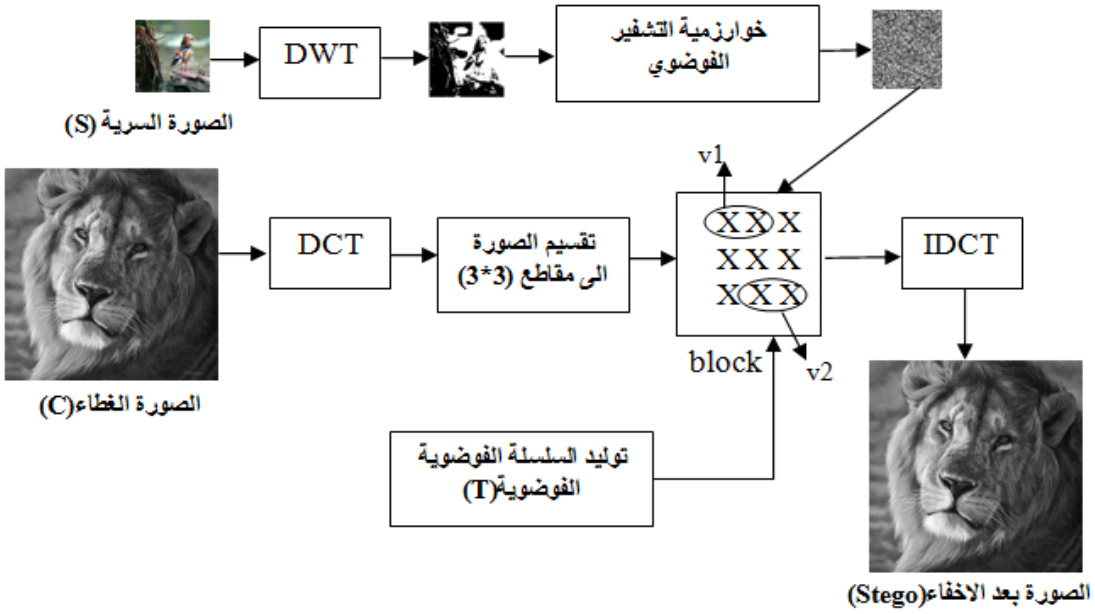
الخطوة (9): تنفيذ مايلي:

1. فحص الفرق بين مجموع كل نقطتين متجاورتين ضمن المقطع الواحد. حيث ان:
   v_1 يمثل مجموع اول نقطتين ، v_2 يمثل مجموع ثاني نقطتين.
2. تكرار النقطة (1) على مقاطع الصورة (blocks) المحددة من قبل السلسلة (T) والاحتفاظ بتسلسل النقاط التي تحقق اكبر فرق لاعتماده في الاخفاء.

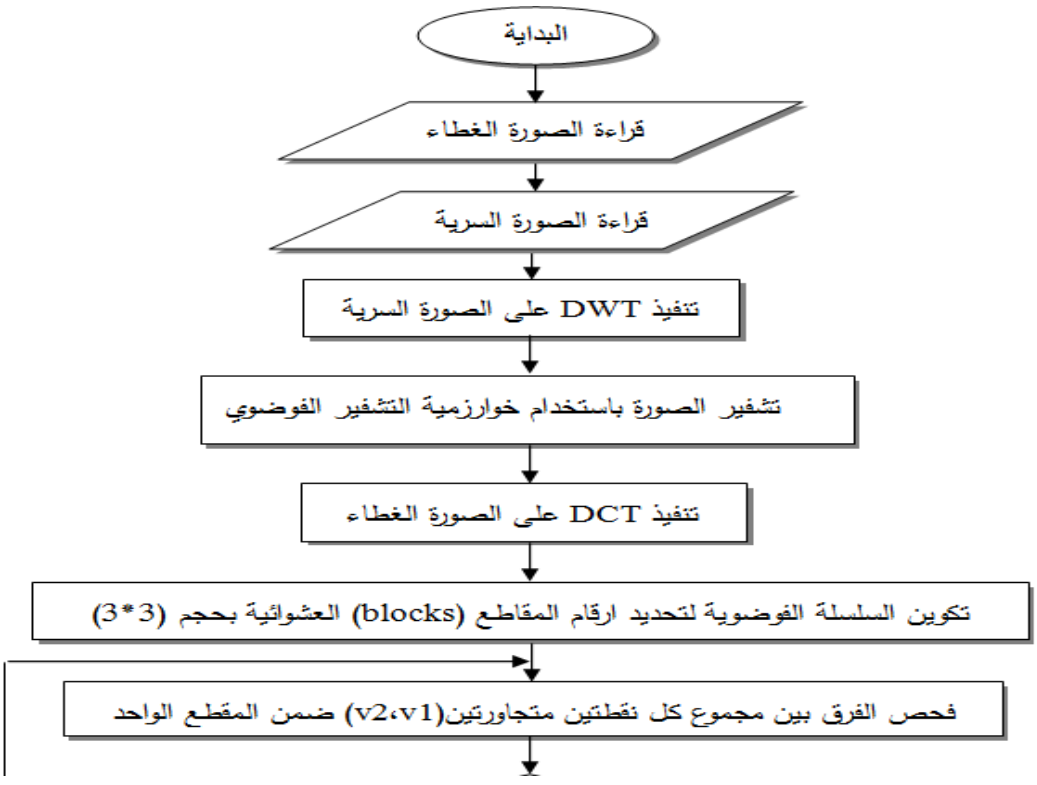
الخطوة (10): اعتماد الشرط التالي لتحديد قيمة الـ bit المخفية ضمن المقاطع (blocks) المختارة :

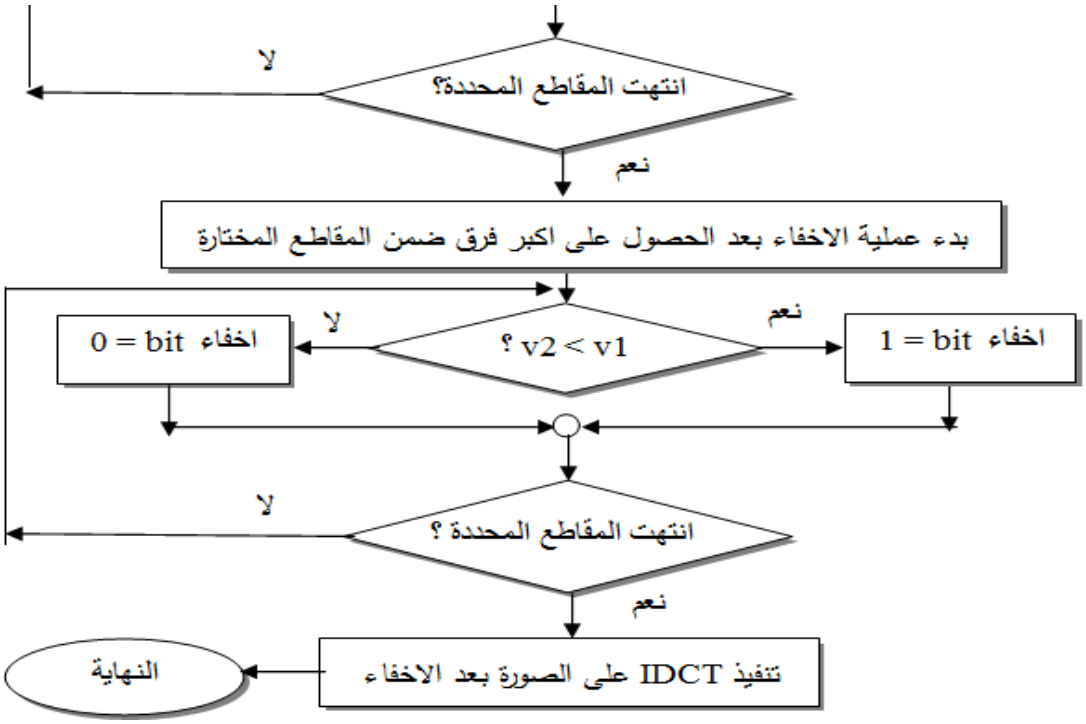
$$\begin{cases} \text{if} \quad v_1 > v_2 \longrightarrow 1 \\ \text{else} \longrightarrow 0 \end{cases} \qquad \ldots(4)$$

الخطوة (11): تنفيذ IDCT للصورة الناتجة للحصول على الصورة بعد الاخفاء (Stego Image). لاحظ الشكلين (5)و(6).



الشكل (5): مخطط خوارزمية الاخفاء المقترحة





الشكل (6): المخطط الانسيابي لخوارزمية الاخفاء المقترحة

7_خوارزمية الاسترجاع المقترحة

ان المرسل والمستقبل سيتفقان مسبقا على قيم (μ , X_0) الابتدائية المستخدمة في عمليتي التشفير والاخفاء وعلى تسلسل النقاط المحددة لمواقع الاخفاء وذلك عن طريق قناة مخفية ذات سرية جيدة. وان خوارزمية الاسترجاع ستنفذ كالاتي:

الخطوة (1): قراءة الصورة بعد الاخفاء (Stego) ذات الحجم n*n.

الخطوة (2): تنفيذ DCT على الصورة بعد الاخفاء (Stego).

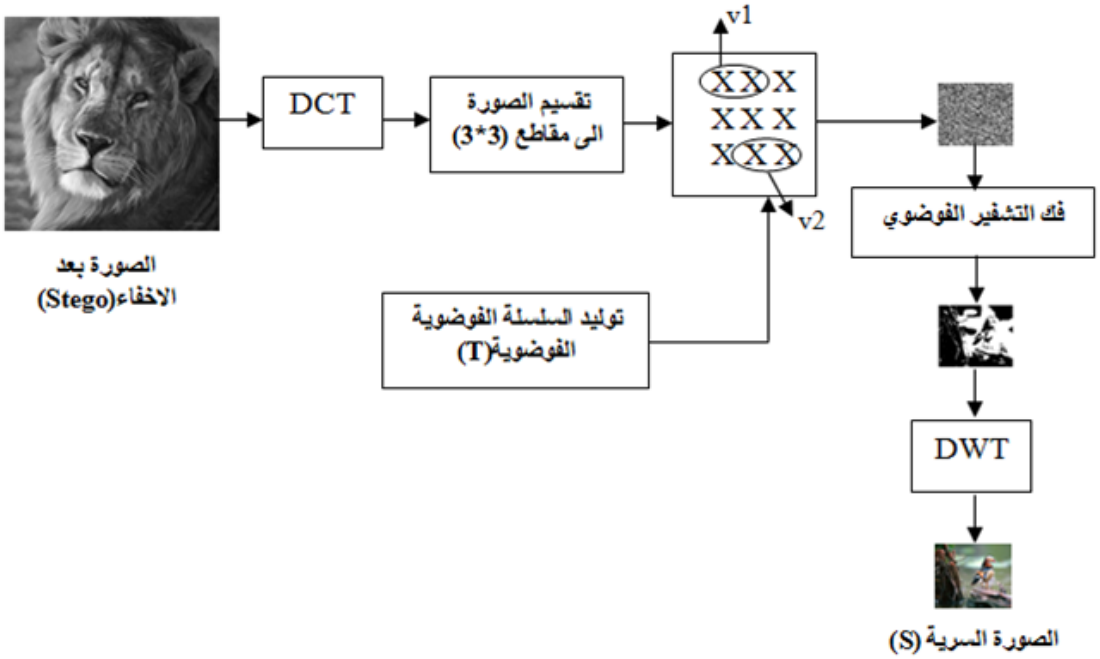
الخطوة (3): تقسيم الصورة الناتجة الى مجموعة من المقاطع (blocks) ذات حجم (3*3).

الخطوة (4): تنفيذ الخوارزمية الفوضوية (بالاعتماد على قيم (μ , X_0) المتفق عليها مسبقا) لتكوين السلسلة الفوضوية (T) ذات الحجم n2 (لتحديد المقاطع (blocks) العشوائية المستخدمة في الاخفاء).

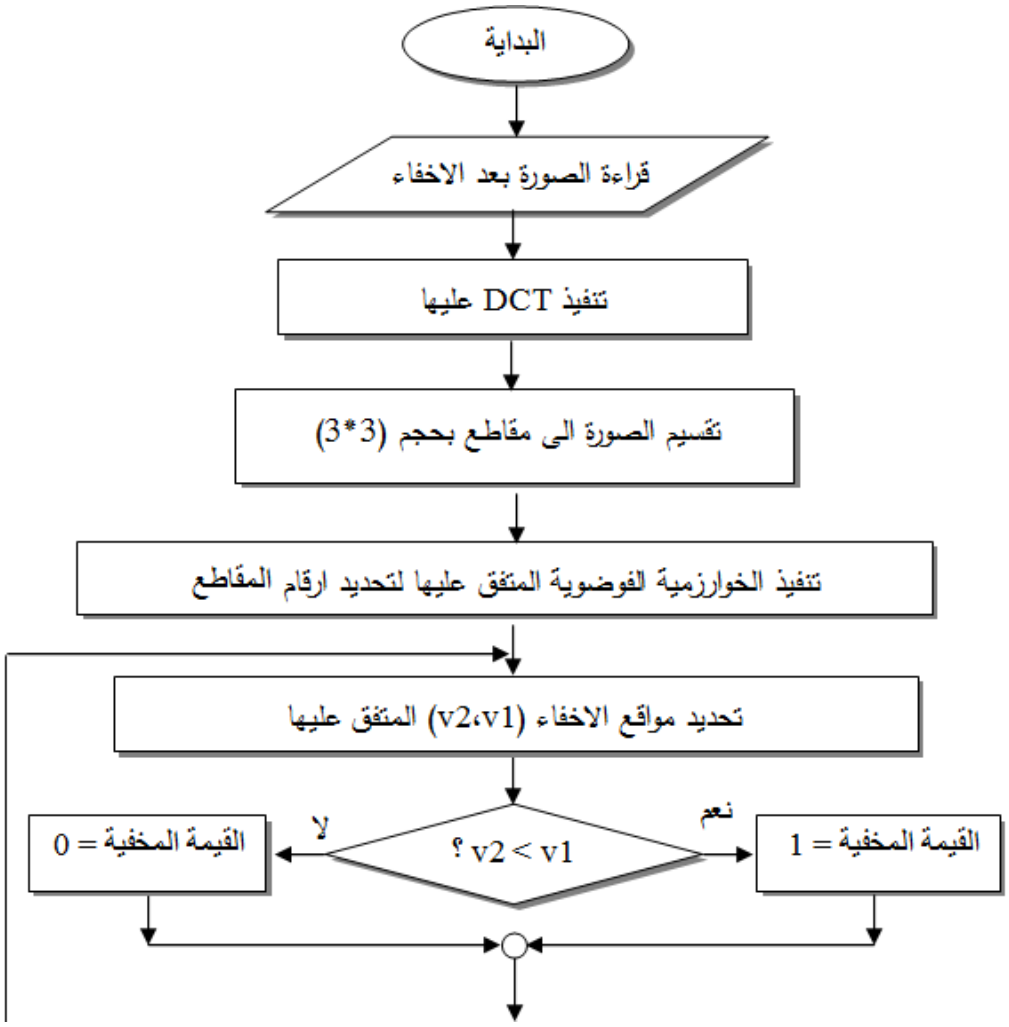
الخطوة (5): تحديد مواقع الاخفاء (v1,v2) (المتفق عليها مسبقا) ضمن مقاطع الاخفاء لاسترجاع الصورة السرية المشفرة بالاعتماد على الشرط (المعادلة (4)).

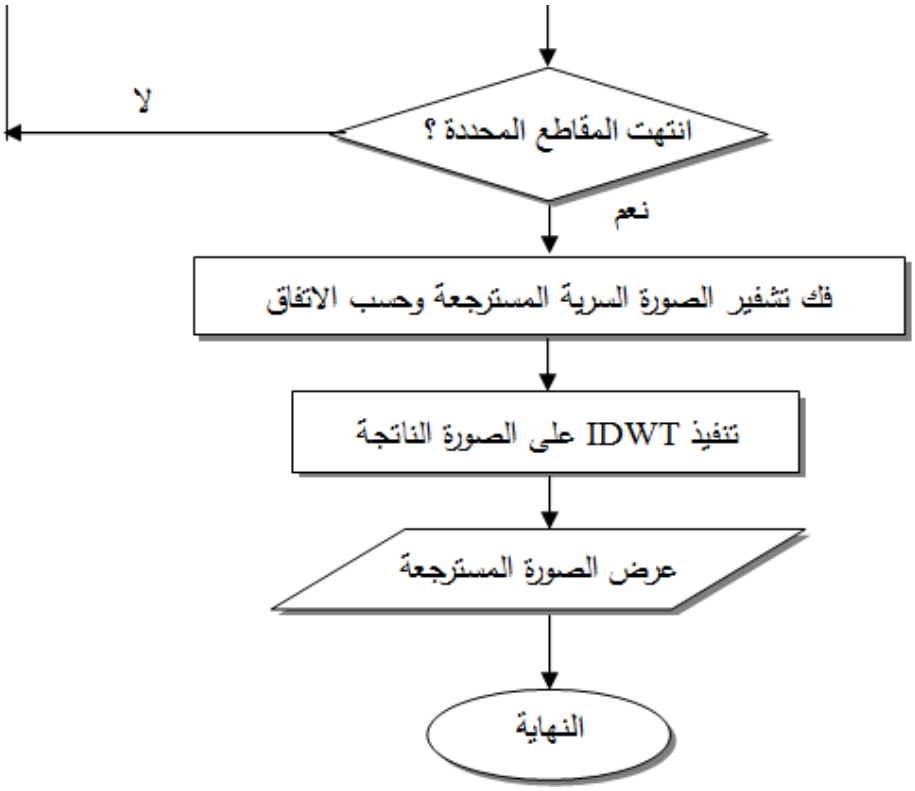
الخطوة (6): تنفيذ خوارزمية فك التشفير الفوضوي باستخدام قيم (μ , X_0) المتفق عليها مسبقا) لفك تشفير الصورة السرية.

الخطوة (7): تنفيذ IDWT على الصورة الناتجة.لاحظ الشكلين(7) و(8) .



الشكل (7): مخطط خوارزمية الاسترجاع المقترحة





الشكل (8): المخطط الانسيابي لخوارزمية الاسترجاع المقترحة

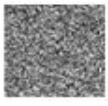
8_مثال تطبيقي

من النماذج التي استخدمت في تطبيق وتنفيذ الخوارزمية المقترحة هو المثال الآتي، حيث تم اعتماد صورة ذات حجم (1024*768) كصورة غطاء، وصورة ذات حجم (128*128) كصورة سرية. وكما موضح في الشكل(9).

الشكل (9): الصورة الغطاء و الصورة السرية

المرحلة الاولى (خوارزمية التشفير الفوضوي): سيتم فيها تشفير الصورة السرية باستخدام الدالة اللوجستية، بعد اختيار قيمة كل من:

$(0 \le X_0 \le 1)$ و$(3.5 \le \mu \le 4)$ واللذان يمثلان مفتاحي التشفير. والشكل(10) يمثل الصورة السرية المشفرة باستخدام $X_0=0.897$ و $\mu=4$.



الشكل (10): الصورة السرية المشفرة

المرحلة الثانية (الخوارزمية الفوضوية): سيكون ناتجها عبارة عن مجموعة ارقام صحيحة تمثل ارقام المقاطع (Blocks) العشوائية التي ستستخدم في عملية الاخفاء. لقد تم اختيار قيمة μ=4 ايضا(لانها تمثل اعلى فوضى)، وقيمة X0=0.698 (وهما يمثلان مفتاحي الاخفاء).

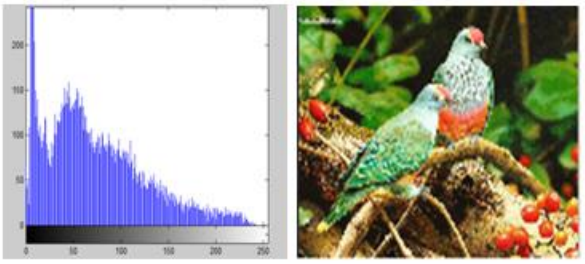
المرحلة الثالثة (خوارزمية الاخفاء): بعد تحديد مقاطع (Blocks) الاخفاء (ناتج المرحلة الثانية), سيتم فحص الفرق بين مجموع كل نقطتين متجاورتين (v2,v1) ضمن المقطع الواحد, فلو فرضنا ان قيمة النقطة الاولى =7.034 , قيمة النقطة الثانية = 9.872 , قيمة النقطة الثالثة = 8.275 و قيمة النقطة الرابعة = 7.324, ستكون قيم v1 و v2 كالاتي :

$$v1 = 7.034 + 9.872 = 16.906$$

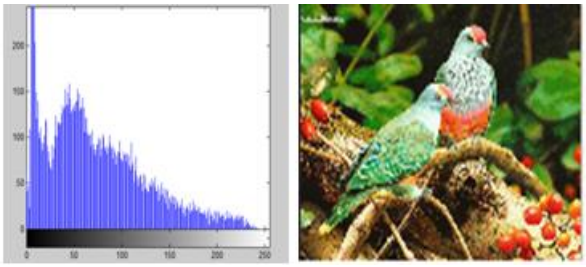
$$v2 = 8.275 + 7.324 = 15.599$$

بما ان v1 > v2 اذن سيتم اخفاء الـ 1 bit والا الـ 0 bit . علماً ان الاخفاء هنا هو منطقي اي بدون تغيير.

بعد تنفيذ خوارزمية الاخفاء المقترحة, ستبقى الصورة كما هي وبدون تغيير واضح للعيان مما يعني ان الخوارزمية لم تحدث اي تحطيم للصورة الغطاء لاحظ الاشكال(11)،(12).



الشكل(11): الصورة الغطاء والمدرج التكراري لها



الشكل (12): الصورة بعد الاخفاء(Stego) والمدرج التكراري لها

9_النتائج والمناقشة

لاثبات كفاءة الخوارزمية المقترحة تم تطبيق المقاييس الآتية:

- **Mean Sequare Error(MSE)**: وتحسب من القانون الآتي:

$$MSE=1/(N*M)* \sum^{n}_{i=1}\sum^{n}_{j=1} (C(i,j)-S(i,j))^{2} \quad \ldots(5)$$

علما ان :

M , N: تمثلان ابعاد الصورة, C: تمثل الصورة الغطاء, S: تمثل الصورة بعد الاخفاء.

- **Peak Signal to Noise Ratio(PSNR)**: وتحسب من القانون الآتي:

$$\mathbf{PSNR=10log_{10}[Cmax^2/MSE](in\ db)} \quad \ldots(6)$$

علما ان : Cmax هي اعلى قيمة لونية في الصورة.

- **NormalizeCorrelation(NC)**: تم حساب الفرق بين الصورة الاصلية(الغطاء) والصورة الناتجة بعد الاخفاء باستخدام القانون الآتية:

$$\mathbf{NC=\sum_i\sum_j C(i,j)S(i,j)/\sum_{i=1}^{n}\sum_{j=1}^{n}[C(i,j)]^2} \quad \ldots(7)$$

- **Bit Error Rate (BER)** : يقيس نسبة الخطأ للصورة المسترجعة (عدد الbits الخاطئة التي تم استرجاعها)

$$\mathbf{BER=(no.\ of\ wrong\ bit/no.\ of\ original\ bit)*}100 \quad \ldots(8)$$

الجدول (1) يمثل قيم المقاييس المستخدمة لعدد من الصور التي استخدمت في العمل:

الجدول (1): نتائج مقاييس الكفاءة

ت	اسم الصورة	ابعاد الصورة	MSE	PSNR	NC	BER
1	**Boat. png**	1024*768	0.019	61.821	0.88	0
2	**Flower.jpg**	800*600	0.012	65.876	0.94	0
3	**Fly. png**	1024*768	0.018	62.433	0.90	0
4	**Loin.jpg**	1024*768	0.011	66.215	0.98	0
5	**Horse.png**	800*600	0.016	63.611	0.91	0
6	**Car. jpg**	1024*768	0.021	59.765	0.86	0
7	**Rose.png**	800*600	0.013	65.210	0.93	0
8	**Water. jpg**	800*600	0.017	62.788	0.90	0
9	**Girl. png**	1024*768	0.020	60.900	0.87	0
10	**Baby. jpg**	800*600	0.022	58.662	0.84	0

تشير النتائج المثبتة في الجدول(1) ان الخوارزمية المقترحة قد نجحت في الحصول على:

MSE بقيم صغيرة جدا, PSNR بقيم عالية جدا, NC بقيم قريبة من 1 وBER بقيم = 0 مما يعني استرجاع كامل للرسالة السرية وهي النقطة الاهم.

10_الاستنتاجات

1. اثبتت النتائج قوة وكفاءة الخوارزمية المقترحة.
2. كان للفوضى الاثر الكبير في زيادة سرية الطريقة المقترحة وذلك من خلال حساسيتها للقيمة الابتدائية لدالة الفوضى المستخدمة (الدالة اللوجستية).
3. ان اي تغيير في القيم الابتدائية للدالة اللوجستية (μ , X_0) سيؤثر على السلسلة الفوضوية (T).
4. كانت الافضلية في التقسيم الى مجموعة من المقاطع(blocks) للحجم (3*3) وذلك لما يوفره من كبر حجم البيانات المخفية.
5. من خلال النتائج التجريبية، تبين ان استخدام DCT في الاخفاء لايؤدي الى تحطيم الصورة الغطاء وهذا ماعكسته قيم NC القريبة من 1 مما يعني التماثل الكبير بين الصورة قبل وبعد الاخفاء.

11_التوصيات

1. استخدام الكنتورليت بدلا من DWT.
2. استخدام دوال فوضوية اخرى مثل دالة Lorenz وRossler.
3. اعتماد اسلوب اخر للاخفاء بدلا من ايجاد الفرق بين مجموع النقاط المتجاورة مثلا طريقة اخفاء البت الاقل اهمية او المقارنة بين نقاط معينة.

المصادر

[1] Al-Ataby, Ali and Al-Naima, Fawzi, 2010, "A Modified High Capacity Image Steganography Technique Based on Wavelet Transform", The International Arab Journal of Information Technology, Vol. 7, No. 4.

[2] Liu, Peipei, Zhu, Zhongliang, Wang, Hongxia, Yan, Tianyun, 2007, "A Novel Image Steganography Using Chaotic Map and Visual Model", International Journal on Advances in Security, Vol.2, No.1.

[3] Yang, Guang-ming and Zhon, Yang, 2009, "LSB algorithm research based on chaos", 9th International Conference on Hybrid Intelligent System.

[4] القدو, سجى جاسم, سعيد, ميلاد جادر, عبد المجيد , ايلاف اسامة, 2010, "التشفير الفوضوي باستخدام مفتاح المقياس الحيوي ", مجلة الرافدين لعلوم الحاسوب والرياضيات المجلد (7) العدد(3).

[5] Mohammad, Shaimaa Sh.,2011,"Encryption and Hiding Water- -marking Using A Chaotic Modified Wavelet Transform",Raf. J. of Comp. & Math's,Vol. 8, No. 2.

[6] Toosizadeh, Saeeid, Mohammad, Seyyed and Farshchi, Reza, 2011, " High Secure Communication using Chaotic Double Compression Steganography Technique", International Journal of Research and Reviews in Computer Science (IJRRCS) Vol. 2, No. 2.

[7] Ahmad, Musheer and Alam, M. Shamsher, 2009, "A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping", International Journal on Computer Science and Engineering, Vol.2.

[8] Amirtharajan, Rengarajan, Rayappan, Joun, 2012, "An Intellgent Chaotic Embedding Approach to Enhance Stego_Image Quality", Information Sciences Vol.193., pages 115-124.