Using the Genetic Algorithm in Developing a Method for Steganography

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

Received on: 20/03/2012 **Accepted on: 28/06/2012**

ABSTRACT

This paper has developed a method for hiding in images, as it was first encrypt the secret message chaoticlly using the chaotic encryption algorithm and secondly execute the steganography in two phases, the first divide the cover image (.BMP, .PNG) to a group of sections (Blocks) with the diagonal sequence and make hiding using the cell of the least Significant Bit (LSB) within (Bytes) of certain randomly, and then using the Genetic Algorithm (GA) and working at the expense of Peak Signal to Noise Ratio(PSNR) for each section after the steganography and then get the best PSNR value of the optimal section (ie, a better distribution of the random sites). The second include a final for all sections (Blocks) depending on the results of the first stage and the best for a random distribution of sites (Bytes) according to the results of genetic algorithm.

Measures such as PSNR, BER, MSE and NC are used to prove the accuracy of the results and efficiency. The application implemented using Matlab 9.

Keywords: Genetic algorithm, LSB, BMP, PNG.

استخدام الخوارزمية الجينية في تطوير طريقة للإخفاء

نادية معن محمد

كلية علوم الحاسوب والرياضيات

جامعة الموصل، الموصل، العراق

تاريخ استلام البحث: 2012/03/20 **تاريخ قبول البحث: 2012/06/28**

الملخص

اشتمل البحث على تطوير طريقة للإخفاء في الصور، إذ تم أولا تشفير الرسالة السرية فوضويا باستخدام خوارزمية التشفير الفوضوي، وثانيا تطبيق الإخفاء على مرحلتين، الأولى تقسيم الصورة الغطاء (.BMP,.PNG) إلى مجموعة من المقاطع (Blocks) ذات تسلسل قطري وإجراء الإخفاء فيها بطريقة الخلية الثنائية الأقل أهمية Least Significant Bit (LSB) ضمن مواقع (Bytes) معينة وبشكل عشوائي، ثم باستخدام الخوارزمية الجينية Algorithm Genetic (GA) والتي تعمل على حساب Peak Signal to Noise Ratio (PSNR) لكل المقاطع بعد الإخفاء وبالتالي الحصول على أفضل قيمة للـ PSNR للمقطع المثالي(أي أفضل توزيع عشوائي للمواقع). أما الثانية فتشمل إجراء الإخفاء النهائي لجميع المقاطع (Blocks) بالاعتماد على نتائج المرحلة الأولى والخاصة بأفضل توزيع عشوائي للمواقع (Bytes) حسب نتائج الخوارزمية الجينية.

اعتمدت المقاييس PSNR، Bit Error Rate (BER) ، Mean Square Error (MSE) و Normalize Correlation (NC) لإثبات دقة النتائج وكفاءتها. أما التطبيق فنفذ باعتماد Matlab 9.

الكلمات المفتاحية: الخوارزمية الجينية، الخلية الثنائية الاقل اهمية، BMP، PNG.

1. المقدمة

منذ العهود القديمة كانت هناك حاجة ملحة لإيجاد وسائل سرية للحفاظ على أمنية الرسائل المرسلة وخصوصاً في وقت الحروب وظهرت هناك طرائق مختلفة في هذا المجال ولكن مع تطور وسائل الاتصال وتطور علم الحاسوب أصبحت هناك حاجة ملحة لإيجاد وسائل أكثر تطوراً لخدمة هذا الغرض فكان أن ظهر التشفير وبالرغم من كونه طريقة جيدة لحفظ المعلومات إلا انه سهل الاكتشاف ويمكن لأي متطفل التلاعب به فكانت الحاجة إلى تقنية أكثر تطورا وأكثر سرية وحفاظا على المعلومات وخصوصا مع ظهور وتطور شبكة الانترنيت لذا تم اللجوء إلى نظام الإخفاء الذي يعتمد على مبدأ أن الرسالة المرسلة تكون غير مرئية لأي شخص بواسطة إخفائها داخل إحدى وسائل الاتصال (الصوت، الصورة والنص، الفيديو) [1].

يمكن تعريف نظام الإخفاء على انه فن وعلم إخفاء المعلومات باستخدام ملف حامل لها (Host) بهدف منع أي متطفل خارجي من الشك بوجود رسالة مخفية داخل الملف الحامل، وهي وسيلة من وسائل الاتصال السري بأسلوب يخفي وجود الاتصال.

أن كلمة Steganography يرجع أصلها إلى اللغة اليونانية وتتكون من المقطعين Steganos وتعني المغطاة أما Graphy فتعني الكتابة أو الرسم والمعنى الحرفي لها الكتابة المغطاة Covered Writing [5]. وإن الفائدة المرجوة من نظام الإخفاء هي إمكانية استخدامه للنقل السري للرسائل من دون اكتشافها، وان استخدامه يعزز سرية الاتصالات الشخصية ويعد وسيلة مهمة للاتصال خصوصا عبر الانترنيت [7].

تطبق الخوارزمية الجينية بنجاح لإيجاد الحل المقبول (القريب إلى المثالي) في المسائل المتعلقة بالعلوم ومنها العلوم الطبية والهندسة والتجارة، حيث أنها اختصرت الكثير من الزمن والجهد المطلوب لدى مصممي الأنظمة والبرامج، وذلك من خلال إيجادها خوارزمية عامة يعتمد عليها في حل مختلف أنواع المسائل، بدلا من بناء خوارزمية خاصة لكل مسألة، مع مراعاة التغييرات اللازمة التي تتناسب مع خصوصية كل مسألة من حيث حجم ونوع البيانات المستخدمة وطبيعة دالة الهدف والقيود لكل مسألة [6].

تستخدم الدالة الفوضوية في تشفير البيانات لما تمتاز به من خصائص مثل التعقيد العالي والتصرفات الغير الخطية بالإضافة إلى الحساسية المعتمدة على القيمة الابتدائية. فعند إعطاء قيمة ابتدائية لنظام معين فمن المعروف انه يمكن توقع الحالة المستقبلية للنظام إلا انه في أنظمة الفوضى فان توقع المدى البعيد يستحيل التنبؤ به [9].

2. أعمال سابقة

أُستخدمت الخوارزمية الجينية (GA) في إخفاء المعلومات من قبل الباحثين، ففي عام (2010) اقترح الباحث .El-Zouka,H خوارزمية جينية تعمل على تقليل التشويه الحاصل في البيانات السرية المخفية في الصورة الغطاء وحققت نتائج تقارب (57%)[5]. وفي نفس العام اقترح .Hsing,C واخرون طريقة لاستبدال LSB ، حيث استخدموا فيها الخوارزمية الجينية للبحث عن الحلول التقريبية وسميت الطريقة باستبدال LSB التحولي [7]. وايضاً اقترح .Wang, Sh واخرون تقنية إخفاء جديدة بالاعتماد على الخوارزمية الجينية، حيث اعتمدت التقنية على الإخفاء في الـ LSB ومن ثم تحديث النقاط (التي تم الإخفاء فيها) جينيا مع الحفاظ على خواصها الاحصائية ليصعب اكتشافها [11]. اما في عام (2011) فقدم .Mohamed,M وآخرون دراسة لتطبيق تقنية هجينة للـLSB

باستخدام مفتاح استبدالي مثالي تم الحصول عليه من خلال الخوارزمية الجينية وذلك لتقليل التشويه الحاصل في الصورة وتحققت من خلالها نتائج جيدة (58%)[8].

وفي هذا البحث استخدمت الخوارزمية الجينية لتطوير طريقة LSB والحصول على توزيع عشوائي امثل للإخفاء وكانت النتائج التي الحصول عليها جيدة (68%).

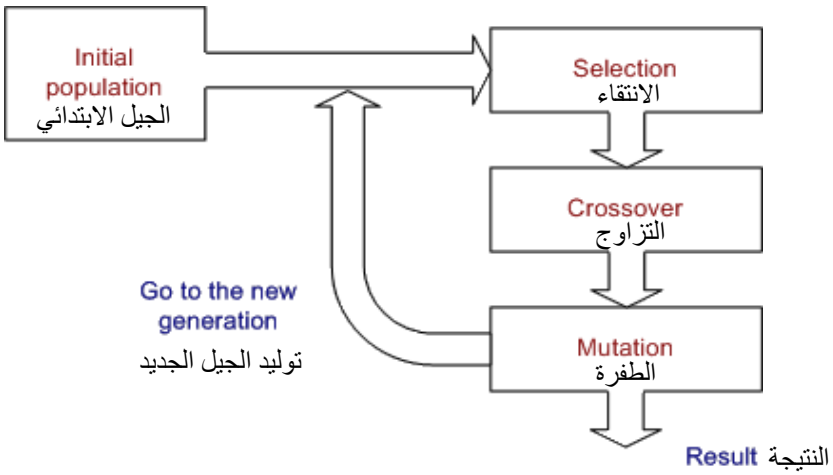
3. مفاهيم عامة

1.3 الخوارزمية الجينية

تعرف الخوارزمية الجينية بأنها خوارزمية ذكية يمكن استخدامها لإيجاد حل المسائل المعقدة وتحسينها، كما تعد من طرائق البحث الكفوءة المعتمدة على مبادئ الاختيار الطبيعي وعلم الوراثة، ابتكرها العالم هولاند (John Holland) عام 1975 في جامعة ميشيكان (University of Michigan) ، إذ نشر بحوثاً عديدة في هذا المجال ، وكان الهدف الأساسي منها بناء و تحسين العديد من الخوارزميات والبرمجيات والأنظمة باستخدام هذه الخوارزمية[8].

يتم حل المسائل المعقدة باستخدام الخوارزميات الجينية بتوليد مجتمع عشوائي يمثل مجموعة الحلول، كل حل تخصص له صلاحية (Fitness) معينة ترتبط مباشرة بدالة الهدف للمسألة المعينة، وبعدها يتم تعديل هذا المجتمع وتوليد مجتمع جديد من خلال تطبيق المعاملات الجينية: الانتقاء (Selection)، التزاوج (Crossover) والطفرة (Mutation) وبصورة متكررة وبالتتابع على أجيال هذا المجتمع لحين تحقق شرط التوقف[10].

إن المعاملات الجينية تعد الخطوات الأساسية للخوارزمية الجينية ، وهي خطوات ثابتة تختلف في أسلوب صياغتها وتطبيقها حسب المسألة أو مجال تطبيقها ، كما إن هذه الخطوات تكون مترابطة بعضها مع البعض الآخر، ولا يمكن تطبيق الخوارزمية على أية مسألة ما لم تطبق جميع هذه الخطوات وإلا تفقد الخوارزمية الجينية قيمتها وفائدتها في إيجاد أو تحسين الحل. لاحظ الشكل (1) [3]:



الشكل (1): المخطط العام للخوارزمية الجينية

2.3 الفوضى

واحدة من السلوكيات التي تربط الأنظمة غير الخطية والتي تحدث تطورا في القيم المحددة لنظام المعلومات، اذ عدّ اكتشاف هذا النظام العشوائي ثورة ادت الى العديد من القضايا المترابطة ونظرية الاستقرار وميزات هندسية

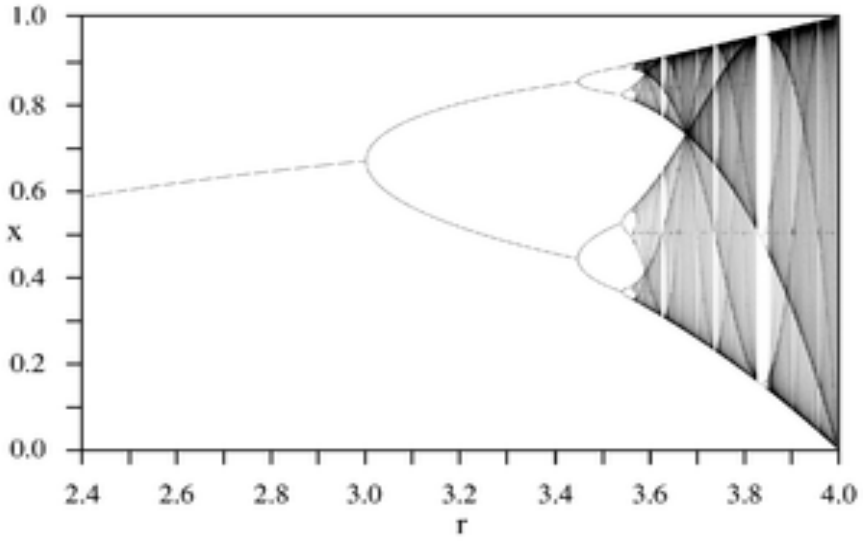
جديدة وعروض لتمييز التواقيع. استخدمت الدالة الفوضوية كاساس لتطوير النماذج الرياضية واجتذبت العديد من الرياضيين بسبب الحساسية العالية للقيمة الابتدائية وتطبيقاتها لمشاكل الحياة اليومية[2].

تمثل الدالة اللوجستية احد أنواع الدوال الفوضوية والتي تمت دراستها لأول مرة عام 1960. لوحظ اهتمام الكثير بها لما تمتاز به من خصائص، إذ ان القيم المحددة التي تنشأها 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. اما التمثيل الرياضي للدالة فهو ممثل بالمعادلة التالية [4]:

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

حيث ان:

X_{n+1} هي عدد حقيقي يتراوح بين (0, 1) وX_n تمثل القيمة الابتدائية، و(μ) قيمة موجبة تتراوح قيمتها بين (0, 4). لاحظ الشكل (2) [2]:



الشكل (2): الرسم البياني التشعبي لسلوك الدالة اللوجستية

3.3 الكتابة المغطاة في الصور

تعد الصور الرقمية من أكثر الوسائط المتعددة استخداما في الكتابة المغطاة بوصفها حاملا للبيانات السرية وذلك بسبب انتشارها الواسع على الإنترنت. ومن أكثر طرائق الإخفاء شيوعا في تضمين البيانات ضمن الصور الرقمية طريقة إدخال الخلية الثنائية الأقل أهمية (LSB)، إذ تستبدل الخلية الثنائية الأقل أهمية من كل نقطة ضوئية في الصور الرقمية بخلية ثنائية من البيانات السرية[1].

يمكن أن تستبدل الخلية الثنائية الأقل أهمية الأولى والثانية من النقاط الضوئية مع بقاء العين البشرية غير قادرة على تمييز الفرق بين الصورتين وهناك أشكال متعددة لهذه الطريقة إذ يمكن نشر الرسالة السرية بصورة عشوائية على الغطاء باستخدام مفتاح سري يعد بذرة (Seed) لمولد أرقام عشوائية أو يمكن اختيار بعض المناطق الأقل تأثراً بالتشوهات لتضمين البيانات في الصورة بالاعتماد على خصائص الرؤية للإنسان [7][8].

4. خوارزمية التشفير الفوضوي

تستخدم هذه الخوارزمية لتشفير الرسالة السرية (Secret Text) وتتلخص خطواتها بما يأتي[4][9] :

الخطوة (1): قراءة الرسالة السرية الثنائية ('S).

الخطوة (2): إعطاء القيمة الابتدائية لكل من X_0 , μ (اللذين يعدان مفتاحي التشفير)، بحيث ان:

X_0 ə (1,0) ، μ ə [4,3.5] ، وهذه القيم (X_0، μ) لابد من الاتفاق عليها مابين المرسل والمستقبل قبل البدء بالعمل.

الخطوة (3): توليد سلسلة أرقام حقيقية (R) بحجم (n) وحسب المعادلة (1).

الخطوة (4): تحويل السلسلة الناتجة الى سلسلة ارقام ثنائية باستخدام المعادلة الآتية:

$$R'_i = \begin{cases} 0 & \text{if } R_i < 0.5 \\ 1 & \text{if } R_i > 0.5 \end{cases} \quad \text{..... (2)}$$

الخطوة (5): تشفير الرسالة السرية ('S) باستخدام المعادلة الآتية:

$$S''(i) = S'(i) \oplus R'_i \quad \text{..... (3)}$$

حيث ان:

i= 0,1,2,....., n.

والشكل (3) يوضح عملية تشفير الرسالة السرية.

الشكل (3): تشفير الرسالة السرية

5. خوارزمية الإخفاء المطورة

في هذه الخوارزمية تم إخفاء النص المشفر فوضوياً ضمن الصورة الغطاء باستخدام طريقة LSB المطورة بعد تحديد خريطة الإخفاء العشوائي للمقطع المثالي (مفتاح الإخفاء) المحدد باستخدام GA. تم الاستفادة من الواجهة الخاصة بالخوارزمية الجينية الملحقة بلغة ماتلاب لتنفيذ عمل الخوارزمية الجينية بعد تحديد عملية الانتقاء من نوع انتقاء الأشكال المنتظمة stochastic uniform، التداخل من نوع التداخل الإبدالي المشتت scattered والطفرة من نوع adaptive feasible. وهنا خطوات خوارزمية الإخفاء المطورة:

1. قراءة الصورة الغطاء (C).
2. قراءة الرسالة السرية (S) (The Prophet Mohammed GBUY is My Teacher).
3. تحويل الرسالة السرية (S) إلى رسالة ثنائية ('S).
4. حساب طول الرسالة السرية الثنائية (n).
5. تشفير الرسالة السرية باستخدام خوارزمية التشفير الفوضوي.
6. تقسيم الصورة الغطاء (C) إلى 4 مقاطع(Blocks) بتسلسل قطري.
7. تقسيم كل مقطع من المقاطع السابقة إلى 4 مقاطع أخرى بنفس التسلسل القطري.
8. توليد أرقام عشوائية لتحديد مواقع (Bytes) الإخفاء.
9. إخفاء الرسالة السرية حسب المواقع (Bytes) المحددة عشوائيا في النقطة (8) ضمن المقاطع (Blocks) في الصورة الغطاء باستخدام طريقة الإخفاء في الخلية الثنائية الأقل أهميه (LSB).
10. تحديد المعاملات المستخدمة في الخوارزمية الجينية وكالآتي:

a. مجتمع ابتدائي من الأفراد، حيث يعد إنشاء الجيل الابتدائي نقطة الانطلاق في حل المسألة، وأن عملية بناء الجيل الابتدائي تمت بطريقة عشوائية (Randomly)، وقد تم اختيار عدد أفراد الجيل في هذه المسألة مساويا" لـ 16عنصر (عدد المقاطع (Blocks)) ، وطول الكروموسوم مساوياً لطول الرسالة السرية الثنائية (n).

b. دالة اللياقة (fitness function) للخوارزمية الجينية باعتماد معادلة PSNR [9]:

$$PSNR=10\log_{10}[Cmax^{2}/MSE] \quad .....(4)$$

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

إذ أن:

N,M : أبعاد الصورة الغطاء.

C ،ST : الصورة الغطاء قبل وبعد الإخفاء على التوالي.

Cmax: أعلى قيمة لونية في الصورة .

c. عملية الانتقاء من نوع انتقاء الأشكال المنتظمة stochastic uniform.

d. التداخل من نوع التداخل الابدالي المشتت scattered.

e. الطفرة من نوع adaptive feasible.

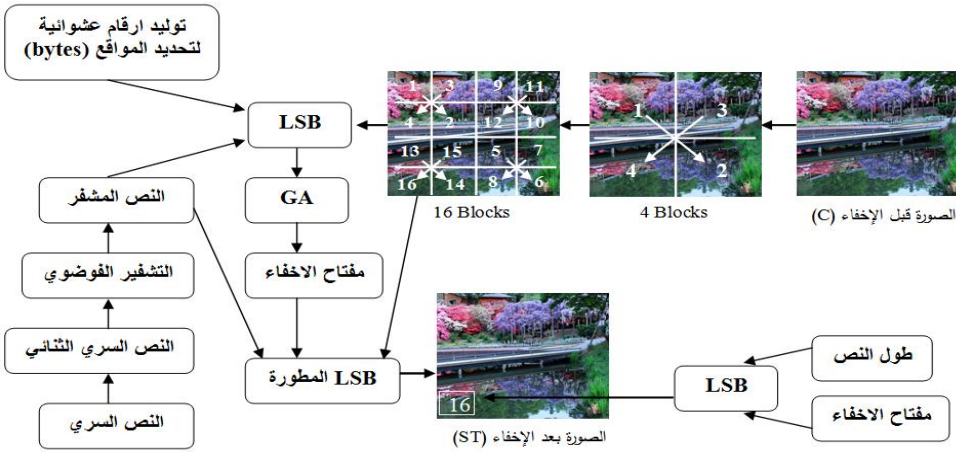
f. تعديل المجتمع الابتدائي وتوليد مجتمع جديد من خلال تكرار الخطوات (من b الى e) لحين تحقق شرط التوقف (الحد الأعلى لعدد الأجيال التي يتم توليدها للحل الأمثل =العدد 100 (نتيجة التجارب)).

11. اعتماد ناتج الخوارزمية الجينية المتمثل بأعلى قيمة (PSNR) للمقطع المثالي وحسب التوزيع العشوائي للمواقع (Bytes) المحددة فيه (مفتاح الإخفاء) سيجري الإخفاء بجميع المقاطع عداالمقطع الأخير(16).

12. إخفاء طول الرسالة السرية الثنائية ومفتاح الإخفاء في المقطع الأخير(16) باستخدام طريقة (LSB)، بحيث ان طول الرسالة السرية سيخفى في البت الأول من كل بايت، ومفتاح الإخفاء سيخفى في البت الثاني من كل بايت.

13. عرض الصورة بعد الإخفاء (Stego-image) .

الشكل (4) يوضح خطوات عمل خوارزمية الإخفاء المطورة على صورة رمادية (ROSE.BMP) :



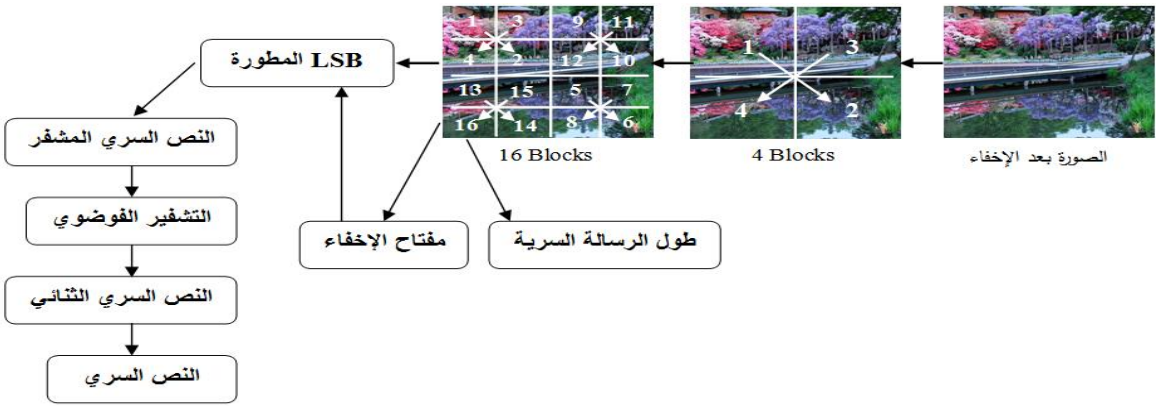
الشكل (4): مخطط خوارزمية الإخفاء المطورة

6. خوارزمية الاسترجاع المطورة

ان المرسل والمستقبل سيتفقان مسبقا على قيم (μ , X_0) الابتدائية المستخدمة في عملية التشفير، كما سيتفقان على موقع إخفاء كل من طول الرسالة السرية ومفتاح الإخفاء وذلك عن طريق قناة مخفية ذات سرية جيدة. وان خوارزمية الاسترجاع ستنفذ كالاتي:

1. قراءة الصورة بعد الإخفاء .
2. تقسيم الصورة الغطاء إلى 4 من المقاطع (Blocks) بتسلسل قطري.
3. تقسيم كل مقطع من المقاطع السابقة إلى 4 مقاطع (Blocks) وبتسلسل قطري ايضا.
4. استرجاع طول الرسالة السرية من المقطع (16) باستخدام طريقة (LSB).
5. استرجاع مفتاح الإخفاء (التسلسل العشوائي للمواقع (Bytes)) من المقطع (16) باستخدام طريقة (LSB).
6. استرجاع الرسالة السرية من مقاطع الصورة بالاعتماد على مفتاح الإخفاء .
7. فك تشفير الرسالة السرية المسترجعة باستخدام خوارزمية التشفير الفوضوي وبالاعتماد على قيم (μ , X_0) المتفق عليها مسبقا.
8. عرض الرسالة السرية المسترجعة.

والشكل (5) يوضح خطوات عمل خوارزمية الاسترجاع المطورة على صورة رمادية (ROSE.BMP):



الشكل (5): مخطط خوارزمية الاسترجاع المطورة

7. مثال تطبيقي

لتوضيح الفكرة المطبقة في هذا البحث، تم اعتماد الصورة (SS1.PNG) الموضحة في الشكل(6) كغطاء، والنص الآتي بوصفه نصاً سرياً: *When Iam wrong no one forget*

الشكل (6): الصورة الغطاء

- التشفير الفوضوي : وفيه إستخدمت الدالة اللوجستية بعد تحديد X_0=0.927 و μ= 4 وعدَهما مفتاحا التشفير للحصول على نص مشفر فوضوياً لاحظ الشكلين (7) و(8).

0	1	1	1	0	0	1	1
0	1	1	1	0	1	0	0
0	1	1	0	0	1	0	1
0	1	1	0	0	1	1	1
0	1	1	0	0	0	0	1
0	1	1	0	1	1	1	0
0	1	1	0	1	1	1	1
.....							

الشكل (7): النص السري الثنائي

1	1	1	0	1	0	0	0
1	0	1	0	0	1	0	0
1	0	0	1	0	0	1	0
0	1	1	1	0	1	0	1
0	1	0	0	1	1	0	0
0	0	0	0	0	1	0	1
0	0	0	1	1	0	1	1
.....							

الشكل (8): النص السري المشفر

- خوارزمية الإخفاء المطورة : وتشمل الآتي:

المرحلة الأولى :

1. تقسيم الصورة الغطاء إلى أربعة مقاطع بتسلسل قطري وإعادة العملية على كل مقطع لينتج 16 مقطعاً.
2. توليد أرقام عشوائية بعدد المواقع في كل مقطع. مثلاً:

(24،37،23،18،13،34،22،14،15،20،19،16،10،8،11،7،12،3،2،4،1،5،9،6).

3. تطبيق الإخفاء (LSB) لكل المقاطع.
4. تطبيق الخوارزمية الجينية (بالاستفادة من الواجهة الخاصة بالخوارزمية الجينية الملحقة بلغة ماتلاب) وإيجاد قيم PSNR للمقاطع. لاحظ الجدول(1).

الجدول (1): قيم PSNR لصورة (ROSE.BMP) بعد تطبيق GA

block	PSNR
1	32.5036
2	40.0348
3	50.1719
4	47.6298
5	31.8792
6	25.8971
7	37.7410
8	41.9170

block	PSNR
9	30.8819
10	44.2655
11	42.6103
12	**55.2106**
13	23.4237
14	54.2550
15	52.8794
16	53.3549

5. تحديد أعلى قيمة لل PSNR (55.2106).

6. تعديل المجتمع الابتدائي وتوليد مجتمع جديد من خلال إجراء الطفرة والتداخل لحين تحقق شرط التوقف (الحد الأعلى لعدد الأجيال التي يتم توليدها للوصول للحل الأمثل وهو العدد 100 (نتيجة التجارب)).
7. الحصول على أعلى PSNR (82.2950) للمقطع المثالي(14) (أفضل توزيع عشوائي للإخفاء واعتماده بوصفه مفتاح إخفاء للمرحلة النهائية). لاحظ الجدول(2).

الجدول (2): قيم PSNR النهائية لصورة (ROSE.BMP) بعد تطبيق GA

block	PSNR	block	PSNR
1	52.5046	9	40.8585
2	40.8788	10	47.2895
3	56.1678	11	42.9103
4	66.6246	12	77.2106
5	54.8762	13	43.4236
6	32.8956	**14**	**82.2950**
7	46.7410	15	70.8704
8	55.9170	16	74.3543

المرحلة الثانية :

إعتماد ناتج الخطوة السابقة (التوزيع العشوائي للإخفاء) لتنفيذ عملية الإخفاء في مقاطع الصورة.

ملاحظة: المقطع (16) لا يتم فيه الإخفاء مثل باقي المقاطع، بل يشتمل على مفتاح الإخفاء وطول النص السري.

- خوارزمية الاسترجاع المطورة : وتشمل الآتي:

1. تقسيم الصورة الغطاء إلى أربعة مقاطع بتسلسل قطري وإعادة العملية على كل مقطع لينتج 16 مقطعاً.
2. استرجاع مفتاح الإخفاء وطول النص السري من المقطع (16).
3. استرجاع النص السري المشفر بالاعتماد على مفتاح الإخفاء وباستخدام طريقة (LSB). لاحظ الشكل(9).

1	1	1	0	1	0	0
0	1	0	1	0	0	1
0	0	1	0	0	1	0
0	1	0	0	1	1	1
0	1	0	1	0	1	0
0	1	1	0	0	0	0
0	0	0	1	0	1	0

الشكل (9): النص السري المسترجع (المشفر)

4. فك تشفير النص السري المسترجع باستخدام التشفير الفوضوي بالاعتماد على قيم (X_0=0.927 و μ= 4) المتفق عليها مسبقاً بين المرسل والمستقبل للحصول على النص السري:

When I am wrong no one forget

8. مقاييس الكفاءة

استخدمت المقاييس التالية لقياس كفاءة الطريقة المطورة بالإضافة إلى مقياس نسبة الضوضاء بالصورة PSNR ونسبة الخطأ بالصورة MSE المذكورين سلفا [9]:

- **Normalize Correlation(NC)**: يستخدم لحساب الفرق بين الصورة الاصلية(الغطاء) والصورة الناتجة بعد الإخفاء وحسب المعادلة الآتية:

$$NC=\sum_i\sum_j C(i,j)ST(i,j)/\sum^{N}_{i=1}\sum^{M}_{j=1}[C(i,j)]^2 \quad .....(6)$$

- **Bit Error Rate (BER)** : يستخدم لقياس نسبة الخطأ (عدد الخلايا الخاطئة المسترجعة) وحسب المعادلة الآتية:

$$BER=(\text{no. of wrong bit/no. of original bit})*100 \quad .....(7)$$

الجدول الأتي يوضح النتائج النهائية بعد تنفيذ الطريقة المطورة على الصورة (ROSE.BMP):

الجدول (4): نتائج تنفيذ الطريقة المطورة على صورة (ROSE.BMP)

BER	NC	PSNR	MSE	Block
0	0.946	42.7036	0.029	1
0	0.961	50.1348	0.022	2
0	0.981	60.8719	0.015	3
0	0.992	67.5298	0.011	4
0	0.965	51.8792	0.021	5
0	0.975	55.8971	0.018	6
0	0.977	57.7810	0.017	7
0	0.957	46.9175	0.025	8
0	0.949	43.8819	0.028	9
0	0.972	54.2605	0.019	10
0	0.968	52.6103	0.020	11
0	0.987	64.2105	0.013	12
0	0.952	45.4233	0.026	13
0	0.998	68.2566	0.009	14
0	0.984	62.6794	0.014	15

ملاحظة (1) : **المقطع 16** استخدم لإخفاء طول الرسالة السرية ومفتاح الإخفاء.

ملاحظة (2) : بالإمكان تكوين مثل هذا الجدول لكل صورة من الصور المستخدمة.

من خلال النتائج الموضحة بالجدول تم الاستنتاج إلى أن قيمة BER الناتجة لجميع المقاطع كانت معظمها مساوية للصفر مما يعني استرجاع النص بالكامل وبشكل صحيح وبدون أي أخطاء. كما ان الصورة قبل وبعد الإخفاء لا تحوي أي تغيير واضح للعيان وهذا واضح من خلال قيم ال NC الموضحة بالجدول.

من خلال استخدام الخوارزمية الجينية تم تحديد المقطع المثالي للإخفاء وهو المقطع (14) ذو القيمة المثلى لـ PSNR (اكبر قيمة من بين قيمها).

أما بالنسبة لقيم MSE الموضحة بالجدول فكانت اغلبها قليلة، ويمكن ملاحظة ان اقل قيمة لـ MSE كانت للمقطع (14)(الذي يملك أعلى قيمة PSNR) .

9. الاستنتاجات

1- أثبتت النتائج قوة وكفاءة الطريقة المطورة.

2- تبين أن تشفير النص باستخدام خوارزمية التشفير الفوضوي يؤدي إلى زيادة سرية الطريقة المطورة وذلك من خلال حساسية الخوارزمية للقيمة الابتدائية لدالة الفوضى المستخدمة (الدالة اللوجستية).

3- تبين أن استخدام تقنية تقطيع الصورة إلى مقاطع بتسلسل قطري يؤدي إلى زيادة سرية الإخفاء وصعوبة الكشف عن المعلومات المخفية.

4- تم الحصول على قيمة مثلى لـ PSNR من خلال استخدام الخوارزمية الجينية (GA).

5- أن استخدام التداخل الابدالي من نوع (Scattered) والانتقاء من نوع (Stochastic uniform) والطفرة من نوع (Adaptive feasible) في الخوارزمية الجينية (GA) يؤدي الى الحصول على أفضل النتائج (قيمة مثلى لـ PSNR) اي (نسبة تشابه صورة الغطاء قبل وبعد الإخفاء).

6- تبين أن استخدام التشفير مع الإخفاء يؤدي إلى زيادة سرية الطريقة المطورة.

10. التوصيات

1- استخدام طرائق أخرى للتشفير كطريقة DES, RSA.

2- استخدام طرائق أخرى للإخفاء كطريقة DCT أو DWT.

3- استخدام تقنيات ذكائية أخرى في الإخفاء كالشبكات العصبية أو المنطق المضبب.

المصادر

[1] الحمامي ، علاء حسين،(2008) ، "إخفاء المعلومات الكتابة المخفية والعلامة المائية "، إثراء للنشر والتوزيع.

[2] 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)، الصفحة 186-187.

[3] بشير، غصون سالم، 2003، "استخدام الخوارزمية الجينية في مطابقة الصور"، رسالة ماجستير مقدمة إلى كلية علوم الحاسوب والرياضيات، جامعة الموصل.

[4] 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, No.1, page 47.

[5] El-Zouka, H.A, (2010), "Distortion Free Steganography System Based on Genetic Algorithm ", Journal of Information Hiding and Multimedia Signal Prossing . Vol. 1, No. 1, page 11.

[6] Gen, M. , (2000), " Genetic Algorithms and Engineering Optimization ", John Wiley and Sons, Inc.

[7] Hsing,C., Jeng,S., (2010), "Transforming LSB Substitution for Image-based Steganography in Matching Algorithms" , Journal of Information Science and Engineering .

[8] Mohamed, M., Al-Afari, F & Bamatraf, M., (2011), " Data Hiding by LSB Substitution Using Genetic Optimal Key permutation ", International Arab Journal of e-technology, Vol.2, No.1, pages 11-13.

[9] 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, pages 89-90.

[10] Rutkowski, L.S., (2010), "Artificial Intelligence and Soft Computing" Springer–Verlag Berlin .

[11] Wang, Sh., Yang, B. & Niu, X., (2010), " A Secure Steganography Method based on Genetic Algorithm ", Journal of Information Hiding and Multimedia Signal Prossing . Vol. 1 , No. 1, page 28.