DOI:

Hiding Encryption Text by DNA using Exploiting Modification Direction Algorithm

Mohammad S. Hashim ***Melad J. Saeed***
mohammad.csp85@student.uomosul.edu.iq *meladjader@uomosul.edu.iq*
Department of Computer Science
College of Computer Science and Mathematiics
University of Mosul, Mosul, Iraq

Received on: 10/01/2021 **Accepted on: 01/03/2021**

ABSTRACT

Local networks and the Internet increase day by day, and a large amount of information is transferred across these networks every day resulting in a dramatic increase in the information security threats.

Therefore, it was necessary to use the techniques that ensure the security and the confidentiality of the transferred information. Secret writing is a general term which is used to refer to the protection of information from attackers, and it includes two types of widely used technologies: cryptography and steganography.

The research has presented a security model that fulfils the requirements of confidentiality and safety of the data transferred between the parties of the communication process. This model includes two phases that aim to provide a high level of confidentiality and security for the secret text. New methods have been used to combine cryptography with steganography to attain a high level of secrecy and security where the secret text was encrypted in an innovative and modified way by encoding DNA (Deoxyribo Nucleic Acid) and hiding the resulting encrypted text inside images by means of EMD (Exploiting Modification Direction) method.

This method has been applied on a number of images and texts, and the measurement of PNSR (88.5382, 87.0293, 97.8257), MSE (0.000015, 0.000019, 0.00004), CO (0) and Q-Factor (0.3521,3458,0.3354) values in the resulting hidden images have been yielded good results.

Keywords: Networks, Information Security, Cryptography, Steganography, DNA.

إخفاء النص المشفر بطريقة الـ DNA باستخدام خوارزمية استغلال تعديل الاتجاه

محمد هاشم سلطان ***ميلاد جادر سعيد***
قسم علوم الحاسوب، كلية علوم الحاسوب والرياضيات
جامعة الموصل، الموصل، العراق

تاريخ استلام البحث: ٢٠٢١/٠١/١٠ **تاريخ قبول البحث: ٢٠٢١/٠٣/٠١**

الملخص

إنَّ الشبكات المحلية وشبكة الانترنت تزداد يوماً بعد يوم وينتقل فيما بين هذه الشبكات كم كبير من المعلومات كل يوم وتزداد معها تهديدات أمنية المعلومات على نحو كبير.

ولذلك كان لا بد من استخدام تقانات تعمل على حفظ أمن المعلومات المنقولة وسريتها؛ فالكتابة السرية هو مصلح عام يستخدم لحماية المعلومات من المهاجمين، ويشمل نوعين من التقانات المستخدمة على نحو واسع وهما: علم التشفير (Cryptography) وعلم الإخفاء (Steganography).

فقد قدم البحث أنموذجاً أمنياً يحقق متطلبات سرية وسلامة البيانات المتنقلة بين أطراف الاتصال؛ إذ يتضمن مرحلتين والتي تهدف إلى توفير مستوى عالٍ من السرية والأمنية للنص السري؛ إذ تم الدمج بين التشفير والإخفاء بطرائق جديدة وحديثة لعمل مستوى عالٍ من السرية؛ إذ شفر النص السري بطريقة مبتكرة ومحورة على تشفير الـ (الحمض النووي الريبوزي منقوص الاوكسجين) DNA ومن ثم إخفاء النص المشفر الناتج داخل الصور بالاعتماد على طريقة (استغلال تعديل الاتجاه)EMD .

نفذت هذه الطريقة على عدد من الصور والنصوص وقيست قيم (PNSR) و(MSE) و(CO) و(Q-Factor) على الصور الناتجة بعد الإخفاء، وحققت نتائج جيدة؛ إذ حُصل على قيم PSNR (88.5382, 87.0293, 97.8257) وقيم MSE (0.000015, 0.000019, 0.00004) أما قيم CO فكانت جميعها 0 ، وقيم Q-Factor (0.3521,0.3458,0.3354).

الكلمات المفتاحية: الشبكات، أمنية المعلومات، علم التشفير، علم الإخفاء، الحمض النووي الريبوزي منقوص الاوكسجين.

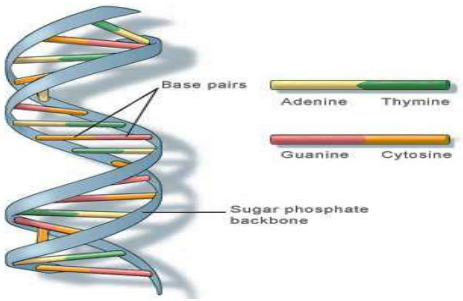
1. المقـــــــدمة:

لتوفير الأمنية للبيانات والمعلومات التي تنتقل بين المتصلين مع بعضهم البعض اعتمد على تقنيتين. الأولى هي التشفير "Encryption" والثانية الكتابة المغطاة أو ما تسمى بـ " steganography ". وكثير من المبتدئين في هذا العلم لا يميزون بين علم التشفير وعلم الإخفاء للمعلومات، معتقدين أنَّ كلا المصطلحين يعطي المعنى نفسه، في حين أنَّ كل مصطلح منهم يغطي علماً أو مجالاً خاصاً به [1]. فالتشفير هو عملية تحويل البيانات بواسطة مفتاح سري إلى بيانات غير مفهومة وبلا معنى، ولا يمكن إرجاعها إلى أصلها إلَّا عن طريق من يمتلك مفتاح التشفير، والبيانات المشفرة تكون موجودة، ولا نخفي أن هناك اتصالاً سرياً بين طرفين مما يدفع بالشخص غير المخول والمتطفل إلى اعتراض تلك البيانات أو محاولة فك هذا التشفير أو إلغائه [2]. ولا ننسى أن هناك بعضاً من الدول وضعت قوانين تقلل من استخدام طرائق التشفير أو منعها بصورة عامة لذلك تم التوجه إلى استخدام التقانة الثانية (الكتابة المغطاة) وذلك لإخفاء المعلومات المتبادلة بين الطرفين؛ لأنها تقوم بعملية تضمين بيانات سرية داخل بيانات أخرى بصورة لا يمكن كشفها بسهولة مما يخفي أصلاً وجود بيانات متناقلة بين الطرفين [4,3].

إنَّ التشفير صمم لحماية نوعين من البيانات وهما: أولاً البيانات الثابتة وثانياً البيانات أثناء النقل، وفي الحالة الأولى إذا كانت هناك حالة اختراق جهاز كمبيوتر أو محرك أقراص ثابت أو قاعدة بيانات فإنَّ التشفير في هذه الحالة يجعل البيانات غير قابلة للقراءة، وفي الحالة الثانية إذا كانت البيانات قيد النقل بين المتصفحات أو بين عنواني بريد الكتروني أو عند تحميل البيانات الشخصية إلى السحابة الالكترونية، وحدثت عملية اعتراض لهذه البيانات من قراصنة البيانات فإن التشفير يحافظ على أمان البيانات المتناقلة خلال هذه المراحل. [5]

نتيجة التطور الكبير في سلسلة الجينات سواء كانت بشرية أو حيوانية أو نباتية أدى إلى ظهور مصدر آخر للعشوائية ومناسب لتطبيقات الحوسبة، ويمكن ملاءمته لتنفيذها كخوارزمية للتشفير مع خوارزميات التشفير التقليدية،

وسميت هذه الخوارزمية بـ (التشفير المعتمد على الـ DNA) [6]؛ إذ تتصف تسلسلات الـ DNA الجينية الطبيعية بعشوائية في تسلسل قواعدها الكيميائية ويطلق عليها بالـ (نيكليوتيدات) وهي باختصار (الثايمين T) و (الأدنين A) و (الغوانين G) و(السيتوزين C) وهي عبارة عن سكريات خماسية تشكل الحمض النووي الريبي منقوص الأوكسجين أو ما يسمى بالـ (DNA) وكما موضح في الشكل (1) الذي يبين بنية ثلاثية الأبعاد لجزيء DNA والتي وضعها العالمان (Watson and crick) عام 1952، ونتجت عنه قاعدة بيانات جينية ضخمة من تسلسلات الـ DNA التي يمكن استخدام جزء منها في عملية التشفير [7] .



الشكل (1) البنية الفراغية لجزيء DNA [7]

بعد عملية السلسلة لجزيء الـDNA تخزن التسلسلات الناتجة رقمياً بالقراءة الضوئية للتسلسلات الحقيقية ومن ثم تحول إلى الشكل الرقمي وتحفظ في قواعد البيانات الجينية العامة، وتجري عملية تحويل تسلسلات الـ DNA إلى الصيغة الرقمية بقواعد التحويل بين رموز أو حروف الـDNA والترميز الثنائي ثم تنتج تسلسلات الـDNA من عملية السلسلة، وهي عملية تلي استخلاص الـDNA من خلايا الكائن الحي وقراءة تتالي النيكليوتيدات على شريط الـDNA وتسجيلها في ملف نصي وكما موضح في الشكل (2) [7] .

الشكل (2) تسلسلات الـ DNA [7]

أما بالنسبة إلى الترميز الثنائي لقواعد الـ DNA (النيكليوتيدات) الأربعة وهي (A-T-G-C) فتتم من خلال قواعد التحويل لتسلسلات الـ DNA إلى الصيغة الثنائية كما في الجدول رقم (1) والشكل رقم (3) [8].

الجدول (1) قواعد ترميز حروف الـ DNA ثنائياً [8]

Rule	1	2	3	4	5	6	7	8
11	T	T	A	A	C	C	G	G
10	G	C	G	C	A	T	A	T
01	C	G	C	G	T	A	T	A
00	A	A	T	T	G	G	C	C

تسلسل	A	T	G	A	G	....	C	T	G	A	G	T	A	C
المقابل	00	11	00	10	00	....	01	11	10	00	10	00	11	01

شكل رقم (3) ترميز تسلسل الـ DNA ثنائياً [8]

أما إذا أردنا تعريف فن الإخفاء بوصفه مصطلحاً حاسوبياً فهو يعني: "علم التضمين" وهو العلم الذي يهتم بإخفاء المعلومات الرقمية داخل وسيط الكتروني دون إحداث أي تشويه أو تعديل ملحوظ في هذا الوسيط، وقد تتضمن في الملفات التنفيذية للبرامج (executable file)، وفي عملية الإخفاء نحتاج إلى توفر عنصرين أساسيين مهمين وذلك لإتمام هذه العملية، وهما الأول هو الرسالة أو البيانات التي نريد أن نرسلها ونخفيها والثاني هو الغطاء (cover) المستخدم لإخفاء هذه البيانات أو الرسالة، تهدف تقانة فن التضمين إلى إخفاء البيانات داخل بيانات أخرى بطريقة لا تؤدي إلى التأثير في هذه الأخيرة، بحيث لا تثير أي شبهة أو شك قد يؤديان إلى كشف الحقيقة، والغرض من عملية الإخفاء هذه ألا يعلم المهاجم المحتمل عن وجود هذه البيانات، وبالتالي تحمى من القراءة أو التغير والتدمير عن طريق هذا المهاجم؛ لأنه لم يعلم بوجود شيء ما أصلاً فكيف يمكن لنا الاستفادة منها أو تدميرها، وهذا يعني أنّ فَن الاختزال ليس جزأً من فن التشفير، فالفرق بينهما كبير، وعلى سبيل المثال فإنَّ علم التشفير يترك أثراً واضحاً في معالم الرسائل المرسلة، ولا يتطّلب وسطاً ثانياً لإخفاء البيانات، ويمكن القول إنَّ التشفير هو تغير المعالم الظاهرة للنص المُرسَل بإحدى خوارزميات التشفير الكثيرة، بحيث يصعُب فهمها بعد تشفيرها، إلا عن طريق المرُسِل والمُستقبِل، بينما فن التضمين كعلم يتطلّب وسطاً ثانياً تخفى البيانات داخله، يشترط تغير معالم البيانات المُرسَلة، وهذا الذي يجعل هذه التقانة مختلفة عن التشفير (Cryptography)، [9].

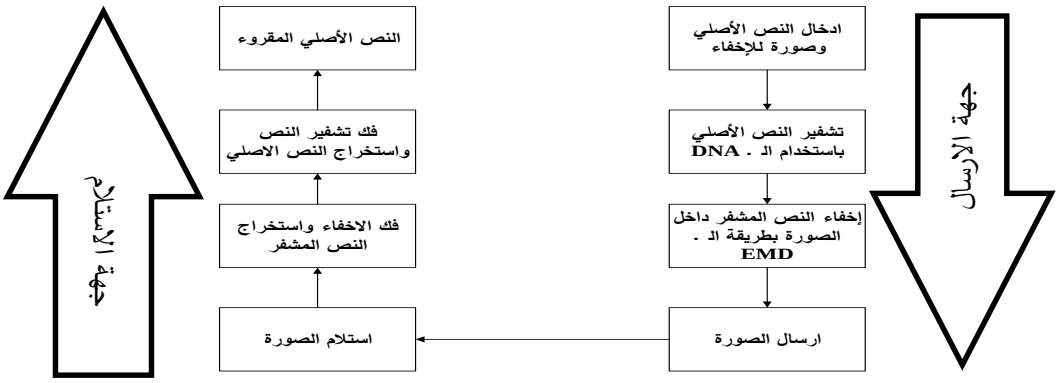
2. الدراسات السابقة:

من خلال قراءة مجموعة من البحوث والتطرق على الأساليب المستخدمة بها في التشفير والإخفاء فقد لوحظ العديد من التقانات والطرائق المختلفة التي اقترحها العديد من الباحثين، ففي عام 2006 اقترح كل من (Zhang and Wang) طريقة EMD بهدف الحد من التغيرات الحاصلة في الصورة أثناء عملية الإخفاء مقارنة مع LSB. [10] ثم قام كلٌّ من الباحثين (Zhang and Wang) في عام 2009 باقتراح طريقة للتشفير تعتمد على دمج مفاهيم الـ DNA وطرائق التشفير القياسية [11]. كذلك في عام 2010 قدم (K.Lin) وآخرون طريقة opt EMD التي تعتمد على تحليل العلاقة بين عدد البكسل n في المجموعة وكمية البيانات التي سوف تخفى داخل الصورة[12]. ثم قدم الباحث (ZHANG Y) وآخرون في عام 2011 طريقة لتشفير البيانات النصية وذلك باستخدام تسلسلات الـ (DNA) ذات أطوال كبيرة، وهذه التسلسلات تستخدم كحامل للبيانات وذلك في عملية فهرسة الـ (DNA) [13]، أما في عام 2013 فقد قدم الباحث (Kuo) وآخرون طريقة جديدة لتطوير خوارزمية الـ EMD من خلال إخفاء (n+1) من بتات الرسالة السرية في n من البكسل في الصورة بحيث البكسل يضاف له واحد أو ينقص منه أو تبقى بدون تغيير [14]. استمرت فكرة التطوير لطريقة الـ EMD الأصلية بحيث قدم الباحثان (Cheng and Wu) في عام 2014 طريقة لتحسين الـ EMD الأصلية بحيث تقوم هذه الطريقة بطمر رقمين سريين في بكسل واحدة في المجموعة؛ إذ يكون معدل الطمر في البكسل الواحدة في المجموعة مضاعفاً مقارنة مع الطريقة الأصلية [15]، كما قدم الباحث (Majid B) في عام 2013 دراسة اقترح فيها تشفير صورة بالاعتماد على نظرية الفوضوية (Chaos theory) وحسابات الـ DNA. [16]. قدم الباحث (Krishna Bhowal) وآخرون سنة 2019 أسلوب إخفاء المعلومات في الصوت الرقمي باستخدام عملية المعامل، وبناءً على

تقانة استغلال تعديل الاتجاه (Modeifide exploiting Modification Direction) mEMD المعدلة [17], وفي 2020 قدما الباحثان Z.Al-kateeb, M.Jader طريقة جديدة لإخفاء النص المشفر بطريقة الـ DNA باستخدام الدالة الفوضوية Chaotic function [18] ، ومن ثم قدمت الباحثة Ghada Hamed وآخرون في سنة 2020 بحثاً يقارن فيه بين أنواع إخفاء المعلومات القائمة على الـ (DNA) باستخدام معايير أمنية مهمة مع شرح استراتيجيات إخفاء المعلومات بالـ (DNA) وذلك للوصول إلى اقتراحات لمساعدة الباحثين على تقديم تقانات تعتمد على الـ (DNA) لتخزين البيانات بشكل آمن وبكفاءة أكثر وموثوقية أعلى [19] ، كما اقترح الباحث Qi Ke وآخرون سنة 2020 خوارزمية موازية ومحسنة وجديدة؛ إذ قام في هذا البحث بتغيير وظيفة خوارزمية الـ EMD الأصلية وإدخال معامل الأمان العشوائي لتحسين أمان الخوارزمية وسميت بخوارزمية إخفاء المعلومات المحسنة (Modified Parallel Exploiting Modification Direction) (MPEMD) [20]، كما قدم الباحث (Serdar Slolak) في سنة 2020 تقانة جديدة هجينة لإخفاء الصور بالاعتماد على البت الأقل أهمية (Least Significant Bit)(LSB) وخوارزمية الأرقام المعدلة (Enhanced Modiled Signed) (EMSD)؛ إذ تستخدم الخوارزمية مجموعة من البكسلات المتجاورة مع البتات الأقل أهمية في صورة الغلاف لإخفاء المعلومات السرية ونتجت الطريقة المقترحة قدرة عالية في التضمين للمعلومات السرية مع الحفاظ على جودة الصورة [21].

3. تصميم البرنامج:

يتضمن البرنامج المقترح العديد من العمليات والمراحل تهدف جميعها إلى توفير مستوى عالٍ من السرية والأمنية للنص السري المراد إرساله إلى الجهة المقابلة وبالتالي فمن الصعوبة على المتطفل معرفة النص الواضح والشكل (4) يوضح المخطط الصندوقي لآلية عمل البرنامج.



شكل (4) المخطط الصندوقي للبرنامج

4. خوارزمية تشفير DNA:

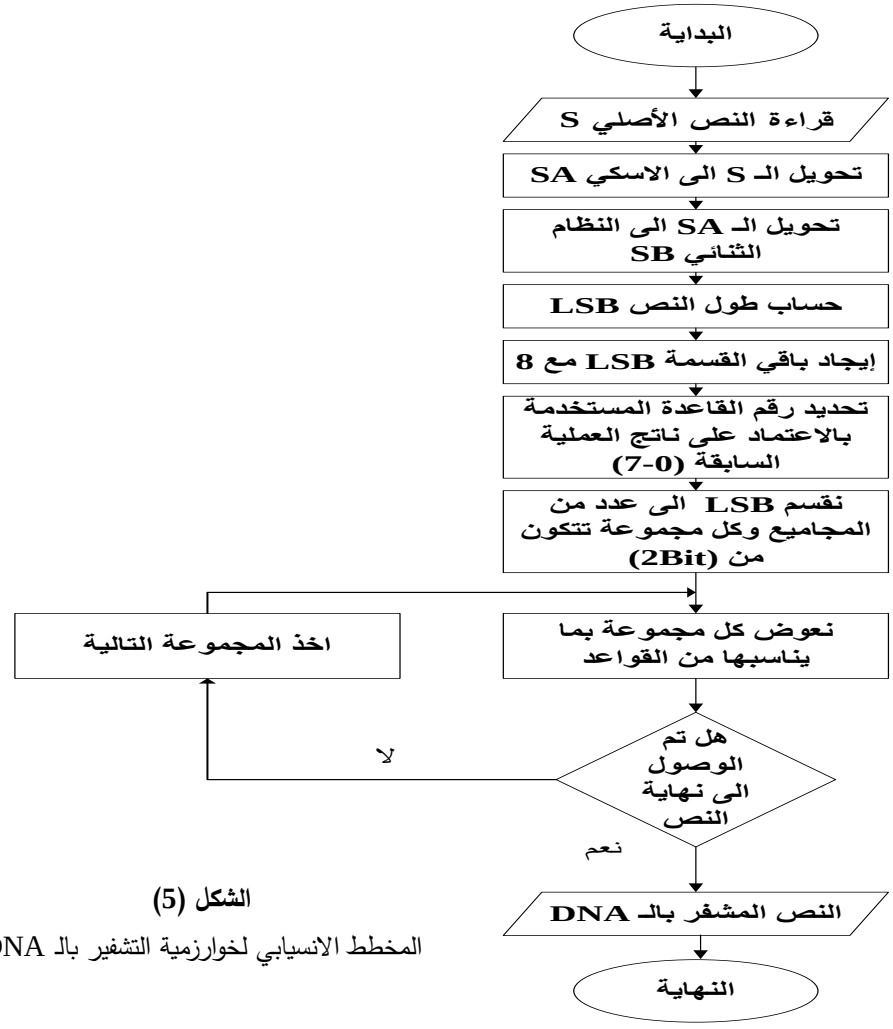
الإدخالات: النص الأصلي

الإخراجات: النص المشفر بالـ DNA

1. البداية
2. قراءة النص الأصلي وليكن S
3. تحويل حروف الـ S غلى الاسكي كود وليكن SA

4. تحويل الـ SA إلى النظام الثنائي وليكن SB
5. حساب طول النص (عدد المراتب الثنائية) وليكن LSB
6. إيجاد باقي قسمة الـ LSB مع 8
7. ناتج الخطوة السابقة يكون من (0 الى 7) وهو يمثل رقم القاعدة التي سوف تستخدم في التشفير بالاعتماد على الجدول رقم (1).
8. استبدال كل (2bit) من الـ LSB بما يقابلها من الجدول رقم (1)
9. هل تم الوصول إلى نهاية النص بالاعتماد على النقطة 5 إذا كانت نعم فينتقل إلى الخطوة رقم 12 إذا كانت النتيجة لا فنذهب إلى الخطوة رقم 9
10. استمرار الخطوة السابقة (9) الى نهاية النص الثنائي LSB
11. النهاية

توضح هذه العملية بالمخطط الانسيابي في الشكل (5)



الشكل (5)

المخطط الانسيابي لخوارزمية التشفير بالـ DNA

أما بالنسبة لخوارزمية فك الشفرة فتتضمن الخطوات نفسها ولكن بالاتجاه المعاكس.

5. خوارزمية الإخفاء EMD

الإدخالات: النص المشفر، صورة للإخفاء (cover image)

الإخراجات: الصورة بعد الإخفاء

1. البداية
2. قراءة النص المشفر وليكن M
3. حساب طول النص وخزنه بآخر بايت في الصورة وليكن ML
4. إدخال قيم الـ n التي تمثل حجم الـ Block الذي سوف تقطع الصورة بالاعتماد عليه
5. تحويل النص M إلى النظام الاسكي ومن ثم إلى النظام الثنائي وليكن MB
6. قراءة 8bit من النص MB وليكن BMB
7. تقسم الـ BMB إلى ثلاثة أجزاء

   الجزء الأول يتكون من 3bit ... ويرمز له d1

   الجزء الثاني يتكون من 3bit ... ويرمز له d2

   الجزء الثالث يتكون من 2bit ... ويرمز له d3
8. تقطيع الصورة إلى مجاميع على وفق قيمة الـ n
9. حساب قيمة المعادلة الآتية:

$K=(2n+1)$ .....(1)

10. تطبيق المعادلة الآتية:

$f = f(g1, g2, g3, \dots, gn) = \sum_{i=1}^{n}(g_i * i) mod\ k$ .....(2)

إذ إنَّ(g1, g2, g3,.....gn) تمثل قيم النقاط داخل المجموعة

n تمثل عدد النقاط داخل المجموعة

11. حساب قيمة S حسب المعادلة الآتية:

$S=d_i\text{-}f \bmod (2n+1)$ .....(3)

12. مقارنة قيمة S

- إذا كانت قيمة S>=n فإنَّ:

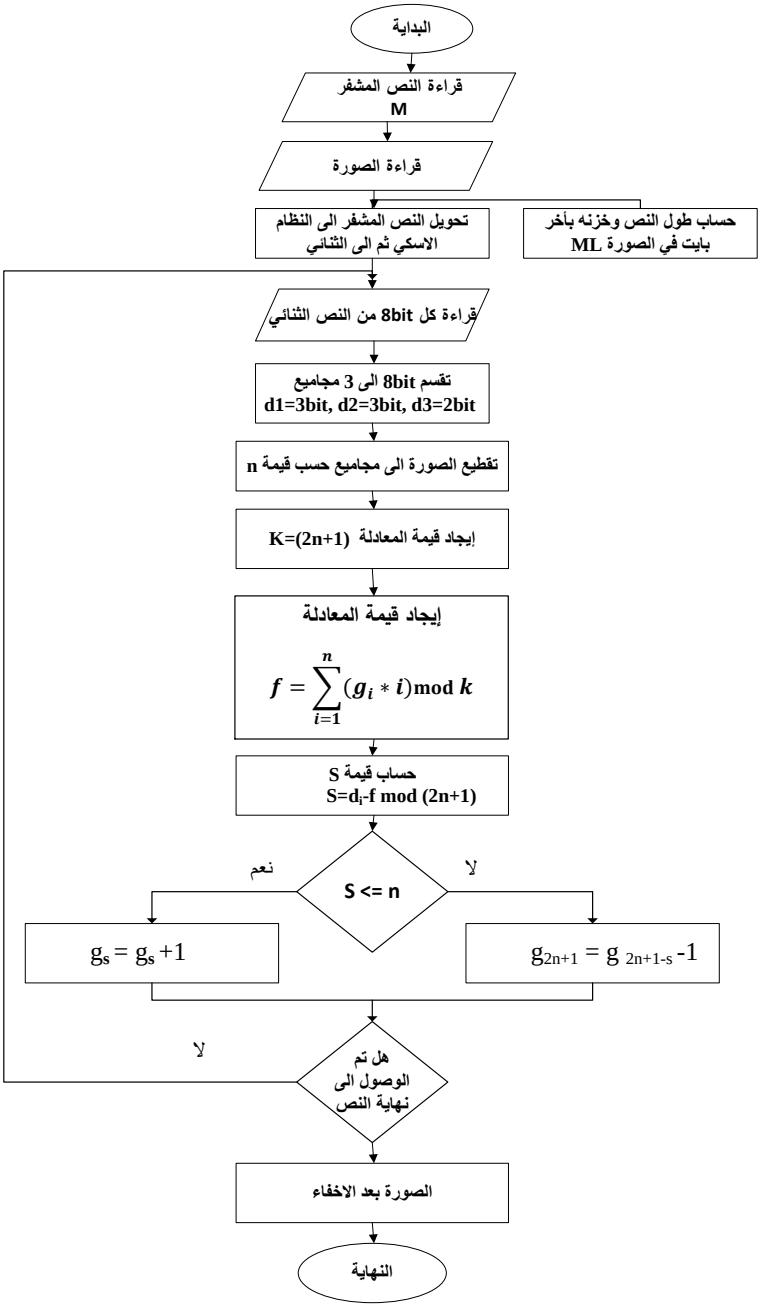
$g_s = g_s + 1$ .....(4)

- أمَّا إذا كانت قيمة S>n فإنَّ:

$g_{2n+1} = g_{2n+1-s} - 1$ .....(5)

13. هل تم الوصول إلى نهاية النص المراد إخفاؤه
    - لا ... الرجوع الى الخطوة رقم 6
14. النهاية

الشكل (6) يوضح المخطط الانسيابي لخوارزمية الإخفاء بالـ DNA

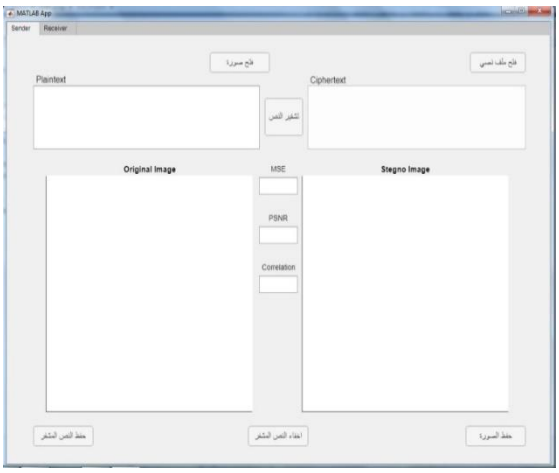


الشكل (6) المخطط الانسيابي لخوارزمية الاخفاء

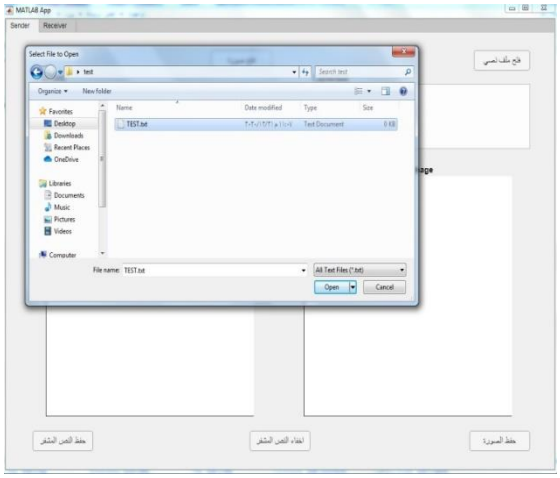
6. التطبيق العملي:

فيما يلي التطبيق العملي للبرنامج

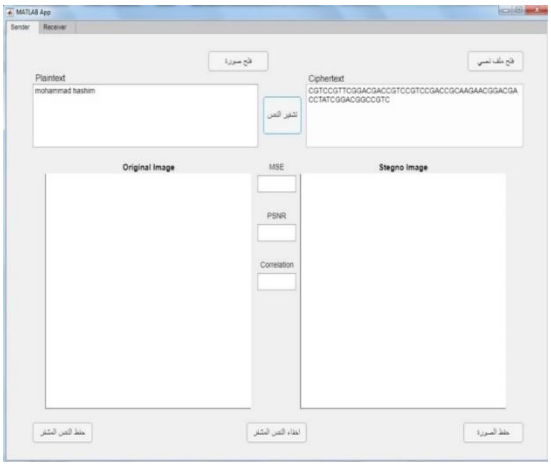
1. جهة الإرسال



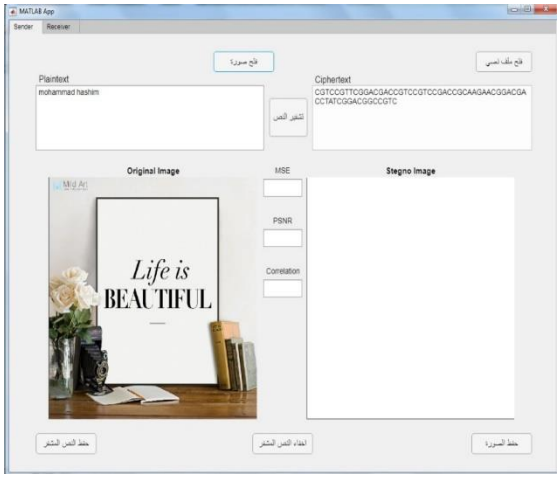
الشكل (7) النص الأصلي والمشفر



الشكل (8) النص الأصلي والمشفر

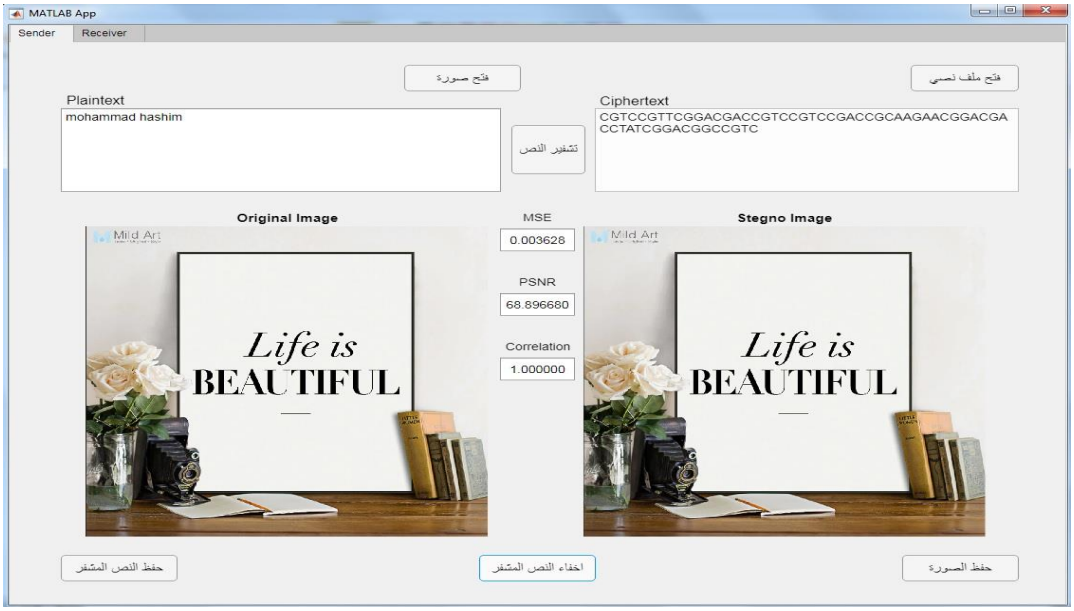


شكل (9) النص الاصلي والمشفر



شكل (10) صورة الغطاء

أما في جهة الاستقبال فتستلم الصورة ومن ثم يستخرج النص المشفر وتفك شفرته كما موضح بالشكل (11) كما حسبت قيم كل من Q_factor , Co ,MSE, PSNR وكانت النتائج جيدة كما موضح بالجدول (2)



الشكل (11) الصورة بعد الإخفاء

الجدول (2) جدول النتائج

Q-Factor	CO	MSE	PSNR	النص المشفر	النص الاصلي	الصورة بعد	الصورة قبل
0.3521	1.0000	0.000015	88.5382	CATCCGTTC GGACGACCG TCCGTCCGA CCGCAAGAA CAGACGACC GGACTATCG GCCGTC	Mohammad Hashim		
0.3458	1.0000	0.000019	87.0293	CATCCGTTC GGACGACCG TCCGTCCGA CCGCAAGAA CAGACGACC GGACTATCG GCCGTC	Mohammad Hashim		
0.3354	1.0000	0.00004	97.8257	CATCCGTTC GGACGACCG TCCGTCCGA CCGCAAGAA CAGACGACC GGACTATCG GCCGTC	Mohammad Hashim		

7. الاستنتاجات والتوصيات:

- يعطي البرنامج العملي الذي طبق في الرسالة نتائج مقبولة لعدة أنواع مختلفة من الإدخالات مثل النصوص والأرقام والرموز.
- نسبة التشوه والتأثير في الصورة قليلة جداً وذلك ما أثبت في القياسات (PSNR,MSE,CO, Q_factor) على الصورة بعد الإخفاء عند استخدام طريقة الـ EMD في الاخفاء.
- استخدام خوارزمية الـ DNA في التشفير تعدُّ كفوءة جداً عند استخدامها مع النصوص القصيرة وخاصةً إذا أردنا إخفاءها في صورة؛ وذلك بسبب أنَّ كلَّ حرف من النص الأصلي يتمثل بأربعة أحرف في النص المشفر بمعنى أنَّ حجم النص المشفر يكون أربعة أضعاف حجم النص الأصلي؛ لأنَّ خوارزمية التشفير بالـ DNA تعتمد على أربعة قواعد لتطبيقها، وهذا بالطبع سوف يأخذ نقاط كثيرة في الصورة ولهذا يفضل استخدام نصوص صغيرة الحجم.
- لوحظ أثناء تجربة وفحص البرنامج أنه كلما كانت الصورة ذات ألوان كثيرة ومشبعة أصبح التضمين والإخفاء أكثر كفاءة.

من خلال تطبيق الرسالة والحصول على النتائج السابقة يمكننا تقديم بعض المقترحات المستقبلية لتطوير العمل كاستخدام تقانات العشوائية chaotic في عدد من مراحل البحث لزيادة السرية وجعل النظام أكثر أماناً، وكذلك إمكانية دمج النظام مع الشبكات العصبية والمنطق المطبب للاستفادة من خصائصهما، وإضافة طرائق تشفير أخرى لجعل النص يمر بأكثر من مستوى من التشفير، وهذا يزيد من سرية النص ويجعله أكثر أماناً. كما أنه بالإمكان الاعتماد على الوسائط الأخرى في الإخفاء مثل الصوت والفيديو.

المصـــادر

[1] N. Provos and P. Honeyman, (2003), "Hide and Seek: An Introduction to Steganography", IEEE Security and Privacy Magazine, 1(3), 32- 44..

[2] S. Joshi and S. Nipanikar, "Implementation Of Exploiting Modification Direction (Emd) – A Steganography Technique Using Raspberry Pi", International Journal Of Current Engineering And Scientific Research (IJCESR),2(8),(2015).

[3] W. Kuo, J. Cheng and C. Wang, "Data Hiding Method With High Embedding Capacity Character", International Journal of Image Processing (IJIP), 3(6), (2010).

[4] الحمامي، علاء حسين ومحمد علاء، (2008)، "إخفاء المعلومات"، إثراء للنشر والتوزيع.

[5] كريم وعباس ، "2019"، تشفير المعلومات لضمان حمايتها ، الأرشيف العربي العلمي

[6] G. A, L. T and R. J, 2000, "Dna-based cryptography.,," DIMACS Series in Discrete Mathematics and Theoriti- cal Computer Science, p. 233–249, 54.

[7] A. Aich, A. Sen, S. R. Dash and S. Dehuri, 2015, "A Symmetric Key Cryptosystem Using DNA Sequence with OTP Key," Springer India, pp. 207 - 216.

[8] د.كندة سليمان ابوقاسم وتيسير عزت سليمان،2019، تشفير النصوص باستخدام OTP من تسلسلات DNA المولدة عشوائياً، مجلة جامعة تشرين .العلوم الهندسية المجلد(41) العدد(4).

[9] RajKumar, Yadav, et al, (2011), "Anew Image Steganography Approach For Information Security Using Gray Level Images In Spatial Domain", International Journal On Computer Science And Engineering (IJCSE), July.

[10] X. Zhang and S. Wang, 2006, "Efficient Steganographic Embedding by Exploiting Modification Direction", IEEE Communications Letters, 10(11),781-783.

[11] Zhang and Wang,2009,"DNA computing-based cryptography ", IEEE 978-1-4244-3867-9/09.

[12] K. Lin, w. Hong, J. Chen, T. Chen and w. Chiang, 2010, " Data Hiding by Exploiting Modification Direction Technique Using Optimal Pixel Grouping ", 2nd international Conference on Education Technology and Computer (ICETC).

[13] Y. ZHANG, Y. ZHU, Z. WANG and S. RICHARD, 2011, "Index-Based Symmetric DNA Encryption Algorithm," in 4th International Congress on Image and Signal Processing IEEE.

[14] W. Kuo and C. Wang, 2013," Data hiding based on generalized exploiting modification direction method", The Imaging Science Journal,61.

[15] Majid B,2013,"A novel text and image encryption method based on chaos theory and DNA computing", Springer Science Business Media B.V.

[16] C. Chang and H. Wu, 2014, "A Large Payload Information Hiding Scheme Using Two Level Exploiting Modification Direction", Tenth International

Conference On Intelligent Information Hiding And Multimedia Signal Processing IEEE.

[17] Debasree Chanda, Susanta Biswas, and Partha Sarkar,2019, An Efficient SteganographicApproach to HideInformation in Digital Audio using Modulus Operation The International Arab Journal of Information Technology, Vol. 16, No. 4.

[18] Z. Al-kateeb, M. Jader, 2020, " Encryption and hiding text using DNA coding and hyperchaotic system ", Indonesian Journal of Electrical Engineering and Computer Science, Vol. 19, No. 2, August 2020, pp. 766~774.

[19] Ghada Hamed, Mohammed Marey, Safaa Amin El-Sayed and Mohamed Fahmy Tolba,2020," Comparative Study for Various DNA Based Steganography Techniques with the Essential Conclusions about the Future Research", Faculty of Computer and Information Sciences,Ain Shams University,Cairo, Egypt.

[20] Qi Ke, Qinan Liao and Ruidong Pan,2020," An Improved EMD Parallel Steganography Algorithm", ICCSCT 2020 Journal of Physics: Conference Series 1621.

[21] SERDAR SOLAK,2020," High Embedding Capacity Data Hiding Technique Based on EMSD and LSB Substitution Algorithms", Digital Object Identifier 10.1109/ACCESS.2020.3023197 IEEE Access.