تشفير الصور الملونة باستخدام فهرسة تسلسلات DNA

د. كندة سليمان أبو قاسم [*]

تيســير عزت ســلمــان [**]

(تاريخ الإيداع 5 / 10 / 2020. قُبِل للنشر في 16/ 12 / 2020)

ملخّص

اعتمدت العديد من الدراسات على تقنيات مختلفة لتشفير الصور الملونة. تركز هذه الدراسة على استخدام تسلسلات DNA كمفاتيح تشفير وكذلك لغرض الفهرسة والتي بدورها ستستخدم لتغيير عناصر الصورة عند تشفير الصور الملونة. يتم في البداية الحصول على سلسلة HASH من تابع البعثرة لملف الصورة المراد تشفيرها، ثم ترميز تسلسل تابع البعثرة الناتج برموز DNA. الهدف من أخذ تابع البعثرة لملف الصورة المراد تشفيرها هو الحصول على حساسية عالية للمفتاح. تم تحويل ملف الصورة إلى الصيغة الثنائية ثم الترميز برموز DNA، وإجراء عملية تشفير للملف بالمفتاح من خلال عملية XOR. بعد الحصول على الملف المشفر تجري عملية تبادل لمواقع عناصر الصورة وذلك بالاستفادة من عملية فهرسة لثلاثة تسلسلات DNA. تم تقييم تشفير الصور من خلال عدة معاملات كالترابط بين البكسلات المتجاورة والانتروبية ومخطط الصورة (الهيستوغرام) ومقاومة الهجمات التفاضلية، وتبين أنه يمكن استخدام تسلسلات DNA العشوائية كمفاتيح تشفير وايضاً لأغراض الفهرسة عند تشفير الصور الملونة من خلال النتائج لمعاملات التقييم.

الكلمات المفتاحية: ترميز DNA، تشفير، معامل الترابط، الانتروبية، الهجمات التفاضلية.

[*] **أستاذ مساعد – قسم الحاسبات والتحكم الآلي – كلية الهندسة الميكانيكية والكهربائية – جامعة تشرين – اللاذقية – سورية.**
ki.abokassem@gmail.com

[**] **طالب دكتوراه –قسم الحاسبات والتحكم الآلي – كلية الهندسة الميكانيكية والكهربائية – جامعة تشرين – اللاذقية – سورية.**
tayseersalman2013@gmail.com

Encrypting Colored Images Using DNA Sequence Indexing

Dr. Kinda Abu Kassem [*]
Tayseer Izzat Salman [**]

(Received 5 / 10 / 2020. Accepted 16 / 12 / 2020)

□ ABSTRACT □

Many studies adopted different techniques to encrypt color images. This study will focus on using DNA sequences as encryption keys and for the purpose of indexing which will be used to change image elements positions for image encryption. At first HASH string is taken for the image file, the resulted HASH string is converted into DNA. The purpose of taking the hash function of the image file is to obtain a high key sensitivity. The image file is converted to binary format and then encoded with DNA codes. Encrypting of the file with the key through XOR process. After obtaining the encoded file, and pixel locations for the images by making use of three DNA sequences for the image files. Image encryption was evaluated by several factors such as the correlation between adjacent and entropy pixels, image layout, and resistance to differential attacks. It was shown that random DNA sequences could be used as encryption keys and for indexing purposes when encrypting colored images by the obtained results of the evaluation factors.

Keywords: DNA encoding, encryption, correlation coefficient, entropy, differential attacks.

[*] **Associate Professor, Department of Computer Engineering and Automatic Control, Faculty of Mechanical and Electrical Engineering, Tishreen University, Lattakia, Syria. ki.abokassem@gmail.com**

[**] **PhD student, Department of Computer Engineering and Automatic Control, Faculty of Mechanical and Electrical Engineering, Tishreen University, Lattakia, Syria.tayseersalman2013@gmail.com**

مقدمة:

تم استخدام ترميزات DNA في العديد من الدراسات الأبحاث إلا أنه لم تتم الاستفادة من الامكانات التي تؤمنها تسلسلات DNA العشوائية في عملية التشفير. تتألف تسلسلات DNA من أربع رموز A وC وG وT وكل من هذه الرموز عبارة عن سكر خماسي تسمى على الترتيب أدنين وسيتوزين وغوانين وتايمين. تتوالى هذه الرموز بشكل عشوائي ضمن التسلسل ويعتبر الجين مؤلفاً من تتالي عدة نيكليوتيدات بترتيب ما. من أجل ترميز البيانات برموز DNA يتم تحويل هذه البيانات سواء كانت نصية أو صور إلى الصيغة الثنائية ومن هنا يمكن ترميز هذه البيانات برموز DNA بالاعتماد على الجدول(1) وذلك من خلال إحدى قواعد الترميز. بعد عملية الترميز وتحويل البيانات إلى صيغة DNA يمكن إجراء عملية التشفير عليها.

الجدول 1: قواعد ترميز حروف DNA ثنائياً [1]

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

تم استعراض الدراسات المرجعية ذات الصلة بموضوع تشفير الصور بالاعتماد على تقنية DNA. حيث بدأ الاهتمام بحوسبة DNA عندما اكتشف ادلمان [2] بأنه يمكن استخدام تسلسلات DNA لحل المشاكل الحاسوبية المعقدة وذلك لقدرة DNA على التضاعف إلى عدة مليارات خلال زمن قصير وهذا ما جعل الباحثين يفكرون بحل المسائل بالاستفادة من المعالجة المتوازية لتسلسلات DNA. اقترح الباحثون في الدراسة [1] مخطط لتشفير الصور بالاعتماد على العشوائية وترميزات DNA. تتم عملية تباديل للصورة من خلال خلط البكسلات المتجاورة عمودياً وأفقياً بمساعدة الخريطة العشوائية المتصالبة CCM، بعد ذلك يتم تقسيم الصورة الناتجة إلى البتات الاقل أهمية والبتات الأكثر أهمية ومن ثم تقسم المجموعتان إلى كتل وترمز بتسلسل DNA. يتم تجميع الكتل الناتجة وتجرى عملية XOR للحصول على الصورة المشوشة والتي بدورها تخضع لعملية تباديل من خلال الخريطة العشوائية المكعبة للحصول على الصورة المشفرة النهائية.

قدمت الدراسة [3] خوارزمية لتشفير الصور بالاعتماد على العشوائية باستخدام خريطة عشوائية أحادية البعد، للخوارزمية أربع دورات وكل دورة تتضمن خمس خطوات: تقوم الخوارزمية بإدراج بكسل عشوائي في بداية كل سطر من الصورة الاصلية ثم فصل كل سطر إلى مصفوفة أحادية البعد وإجراء عملية تبديل لتغيير قيم البيانات في كل مصفوفة تم الحصول عليها بعد ذلك دمج كل المصفوفات الاحادية البعد في مصفوفة ثنائية البعد بناءً على موضع كل منها في مصفوفة الصورة الاصلية ثم تدوير المصفوفة ثنائية البعد بمقدار 90 درجة بعكس دوران عقارب الساعة. استخدمت الدراسة [4] مخطط يستخدم عملية تكرارية لتشفير تسلسل من البايتات والذي هو نسخة محولة من الصورة الاصلية ثنائية البعد. تم استخدام تابعين عشوائيين مستقلين، أحدهما لاجراء التباديل لمواقع البكسل والاخر لتغيير قيم الشدة الضوئية للبكسلات. اقترح الباحثون طريقة لتشفير الصور الملونة في الدراسة [5] باستخدام العشوائية ممثلة

بخريطة Zaslavsky العشوائية وذلك بتوليد تسلسلات عشوائية لإجراء عملية التباديل لبكسلات الصورة. قدمت الدراسة [6] طريقة لتشفير الصور الملونة باستخدام ترميزات DNA وتابع البعثرة SHA−256 والعشوائية ممثلة بنظام لورنتز. يتم في البداية توليد المفتاح من خلال أخذ قيمة البعثرة للصورة الملونة وينتج عن ذلك سلسلة نصية تستخدم لتوليد المفتاح وكذلك تستخدم لتحديث نظام لورنتز الذي بدوره يولد ثلاثة تسلسلات عشوائية من القيم الحقيقية. اقترحت الدراسة [7] طريقة جديدة لتشفير الصور بالاعتماد على العشوائية وترميز DNA ديناميكي. تستخدم الخوارزمية حساب قيمة البعثرة لتسلسل DNA تم أخذه من قاعدة البيانات الجينية العامة كقيمة ابتدائية للخريطة العشوائية مولدة فهرس عشوائي لتغيير مواقع بكسلات الصورة الاصلية بالترابط مع شبكة لتحقيق مستوى من التبديل العشوائي لمواقع البكسل. اعتمدت الدراسة [9] على العشوائية المولدة من نظام لورنتز بشكل مشابه للدراسة [6] لتشفير الصور الملونة بالاعتماد على تابع البعثرة SHA−512 ومفتاح تشفير من تسلسل DNA خارجي لزيادة فضاء المفاتيح.

طرائق البحث ومواده:

تم تقديم العديد من الدراسات الأبحاث [10] و [11] و[12] لتشفير الصور بدون استخدام DNA حيث استخدمت الخرائط العشوائية لتبديل مواقع البكسل للصورة. يعتمد التشفير في هذه الدراسات على استخدام الخرائط العشوائية التي تتصف بحساسيتها للشروط الأولية وبأنها قادرة على توليد تسلسلات عشوائية تستخدم لتبديل مواقع بكسلات الصورة الاصلية. كما اعتمدت عدة دراسات على استخدام مفهوم DNA من خلال ترميز الصورة برموز DNA بالإضافة إلى استخدام الخرائط العشوائية [9] و [13] و[14] و[15].

الأدوات لغة البرمجة Python 3.7 واستخدام المكتبات Numpy و CV2 و matplotlib وتسلسلات DNA من قواعد البيانات الجينية الع[1]امة حسب [8]. أما مجموعة البيانات فقد تم استخدام الصور القياسية (Lena, Baboon, Peper) كونها مستخدمة في معظم الدراسات المرجعية.

1. الخوارزمية المقترحة لتشفير الصور الملونة

قدمت كل من الدراستين [9] و [6] طريقة لتشفير الصور باستخدام العشوائية الناتجة عن نظام لورنتز، تعتمد الدراسة المقترحة في هذه الورقة على تقديم خوارزمية لتشفير الصور باستخدام ترميز DNA واستخدام مفتاح تشفير يتم استنتاجه من تابع البعثرة للصورة الاصلية SHA−512 حيث نحصل على مفتاح بطول 1024 بت. أما تبديل مواقع عناصر المصفوفات اللونية فيتم من خلال استخدام ثلاثة تسلسلات DNA عشوائية طول كل منها بحجم مصفوفة الصورة بالمستوى الرمادي. ويوضح الشكل (1) المخطط المقترح لتشفير الصور.

2.1. عملية التشفير وفق الطريقة المقترحة

يتم في البداية تفكيك الصورة الاصلية إلى مركباتها اللونية RGB وكل مركبة تمثل مصفوفة بالأبعاد n*m حيث n عدد الاعمدة و m عدد الاسطر وتتراوح قيم عناصر[1] كل مصفوفة ما بين 0 و255. بعد ذلك ترمز كل مصفوفة لونية برموز DNA من خلال تخطيط كل قيمة من قيم المصفوفة بمقابلها من أربع رموز DNA كما هو متبع في الدراسة [10] وبذلك تتشكل لدينا ثلاث مصفوفات مرمزة DNA كل عنصر منها يرمز باربع رموز DNA وبذلك يكون لدينا

[1]تمت الإشارة الى قيم المصفوفات اللونية الثلاث بالعناصر اللونية وليس بكسل لأن الصورة الملونة والمكونة من بكسلات قد تم تفكيكها الى ثلاث مصفوفات RGB توصف بأنها ذات تدرج رمادي وتتراوح قيم كل منها ما بين 0 و255 حيث أن البكسل يتكون من ثلاث عناصر لونية.

255 نمط من أنماط DNA لتوافق 255 قيمة، على سبيل المثال العنصر ذو القيمة 0 يكون ترميزه AAAA والعنصر ذو القيمة 255 يكون ترميزه TTTT. بعد الحصول على المصفوفات اللونية المرمزة DNA تجري عملية تشفير لها بواسطة المفتاح من خلال عملية XOR وبذلك نحصل على المصفوفات الثلاث المشفرة. أما عملية تغيير مواقع عناصر الصورة فتتم من خلال ثلاث تسلسلات DNA عشوائية كل منها بطول n*m*4 . يتم تحويل كل مصفوفة من المصفوفات اللونية الثلاث من مصفوفة ثنائية البعد إلى مصفوفة أحادية البعد. يتم ترتيب كل من تسلسلات DNAالثلاث أبجدياً ثم أخذ فهارس هذه التسلسلات على شكل مصفوفات أحادية البعد ثم استخدام هذه الفهارس لتغيير مواقع عناصر المصفوفات اللونية وذلك بتخصيص تسلسل لكل مصفوفة يوضح.

3.1. عملية فهرسة DNA

لتشفير الصور الملونة تستخدم ثلاثة تسلسلات DNA عشوائية، كل تسلسل لمصفوفة لونية واحدة. يتم اعتبار كل تسلسل على شكل مصفوفة أحادية يتم ترتيب عناصرها من الأكبر إلى أصغر أو بالعكس ثم أخذ فهارس كل من التسلسلات والتي ستستخدم كأدلة لعناصر المصفوفات اللونية لتغيير ترتيبها والحصول على المصفوفات اللونية المشفرة والمبدلة على سبيل المثال بفرض أنه يوجد تسلسل DNA الآتي الذي يستخدم لعملية الفهرسة:

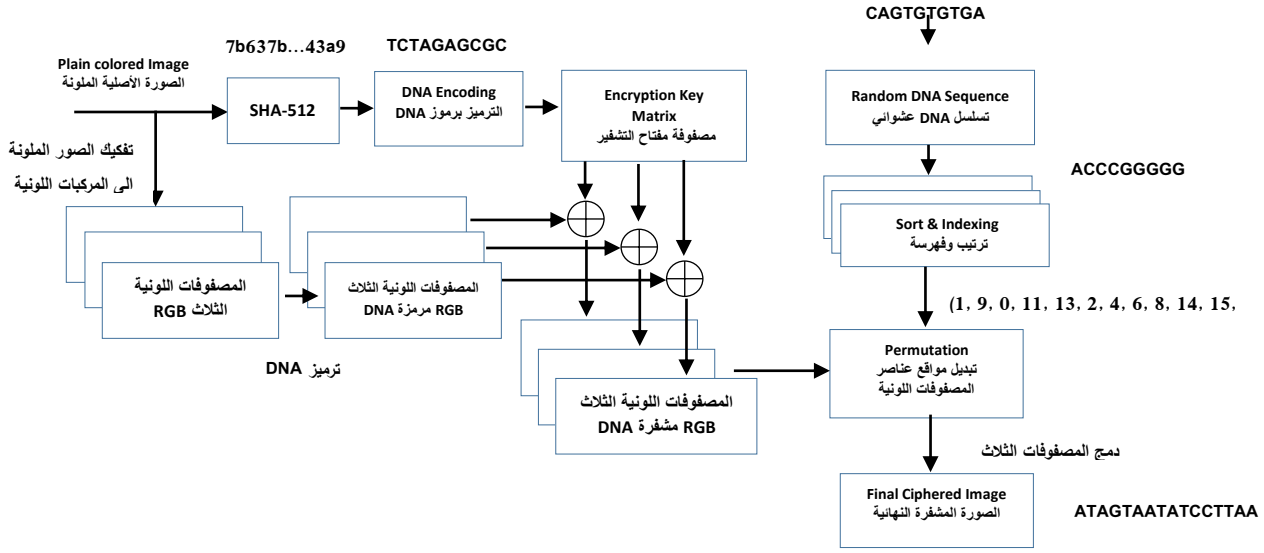
TGTCCAAACAGAAGAATCTCAAAAAGGTTCAATTGTGCTTTGGACAGCTTTGACTATTAGCCAC CACGCTGGCAAGAAAAACTCGTATGATCCGCCAATTATTCCGGCCTTCCTCTGGGGACCTTAACC CTAGTAGGATCTTGCCGGTATGGGATTGGAGTCAGAGTCCCGTAGTGCTCGAGATGCCGAATG GAAGTGAA

يتم تحويل هذا التسلسل إلى مصفوفة أحادية، ثم ترتيب هذا التسلسل تصاعدياً أو تنازلياً. وفي حالتنا هنا تم الترتيب تصاعدياً حيث تكون الفهارس idx الناتجة عن المصفوفة كما يلي:

(5, 6, 7, 9, 11, 12, 14, 15, 20, 21, 22, 23, 24, 30, 31, 43, 45, 52, 55, 58, 62, 65, 73, 74, 76, 77, 78, 79, 80, 86, 89, 96, 97, 100, 120, 125, 126, 131, 134, 137, 148, 153, 158, 162, 164, 172, 180, 182, 188, 189, 193, 194, 198, 199, 3, 4, 8, 17, 19, 29, 37, 44, 47, 53, 60, 61, 63, 64, 66, 68, 72, 81, 83, 91, 92, 94, 95, 103, 104, 107, 108, 111, 112, 114, 121, 122, 127, 128, 129, 139, 143, 144, 161, 167, 168, 169, 176, 178, 185, 186, 1, 10, 13, 25, 26, 34, 36, 41, 42, 46, 51, 59, 67, 70, 71, 75, 84, 88, 93, 105, 106, 116, 117, 118, 119, 132, 135, 136, 142, 145, 146, 150, 151, 152, 156, 157, 159, 163, 165, 170, 173, 175, 179, 181, 184, 187, 191, 192, 195, 197, 0, 2, 16, 18, 27, 28, 32, 33, 35, 38, 39, 40, 48, 49, 50, 54, 56, 57, 69, 82, 85, 87, 90, 98, 99, 101, 102, 109, 110, 113, 115, 123, 124, 130, 133, 138, 140, 141, 147, 149, 154, 155, 160, 166, 171, 174, 177, 183, 190, 196)

حيث أن كل رقم من الفهرس يعبر عن موقع حرف في تسلسل DNA المستخدم لعملية الفهرسة. وبما أن مواقع الفهارس أصبحت عشوائية نتيجة عملية ترتيب تسلسل DNA من الاصغر إلى الاكبر، تستخدم الفهارس الناتجة لتبديل مواقع عناصر المصفوفة المشفرة من خلال إجراء حلقة على عناصر المصفوفة اللونية المشفرة وتبديل مواقعها bx_s[i] bs[idx] = حيث bx_s[i] تمثل عنصر المصفوفة الجديدة الناتجة عن المصفوفة اللونية المشفرة[ ]bs بعد تبديل مواقع عناصرها بالاعتماد على الفهارس idx تكون النتيجة:

TCATAACCATATACGATAGCTGTAATCTCCGAGAATAAAGCAGACAAAATTTCTGAATCTTAGGATTATA AGATAATTAGAGATTTGAGCGAAGAGACTGGGGTTAATTGGGCAAAAATGCATGAATAGTCAGAAACT TGTGGTAAAACTAACACACTGATAAGTACTTCTTTAGGTGCTTCCCGGATTTAGACCGTTTA



الشكل (1): مخطط تشفير الصور المقترح باستخدام الترميز وفهرسة DNA

يمكن تلخيص عملية التشفير بالخطوات التالية:

1- قراءة الصورة الملونة وأخذ قيمة HASH لها.

2- تفكيك الصورة إلى المركبات اللونية RGB.

3- ترميز كل مصفوفة لونية برموز DNA حيث يرمز كل عنصر من عناصر المصفوفة باربع رموز من DNA.

4- ترميز القيمة الناتجة عن تابع HASH في الخطوة 1 برموز DNA واستخدامها بتشكيل مصفوفة المفتاح.

5- إجراء عملية التشفير باستخدام عملية XOR بين كل من المصفوفات اللونية ومصفوفة المفتاح بحيث تنتج ثلاث مصفوفات لونية مشفرة DNA.

6- استخدام ثلاثة تسلسلات DNA عشوائية من أجل عملية الفهرسة وتغيير مواقع عناصر المصفوفات اللونية الثلاث في 5 وأخذ فهارس تسلسلات DNA الثلاث بعد ترتيبها تصاعدياً.

7- تحويل كل من المصفوفات الناتجة في 6 إلى مصفوفات أحادية البعد.

8- استخدام الفهارس الثلاث الناتجة في 6 كفهارس للمصفوفات الاحادية البعد الناتجة في 7.

9- دمج المصفوفات الثلاث بعد إرجاعها إلى مصفوفات ثنائية البعد في مصفوفة واحدة وبذلك نحصل على المصفوفة المشفرة والمرمزة برموز DNA.

4.1. عملية فك التشفير

تتضمن عملية فك التشفير، خطوات معاكسة لعملية التشفير حيث تستقبل خوارزمية فك التشفير الصورة المشفرة النهائية والتي هي عبارة عن رموز DNA وفق المخطط (2). تتم عملية فك التشفير وفق الخطوات التالية:

1- تفكيك الصورة المشفرة الى المركبات اللونية الثلاث وتحويلها الى مصفوفات أحادية البعد.

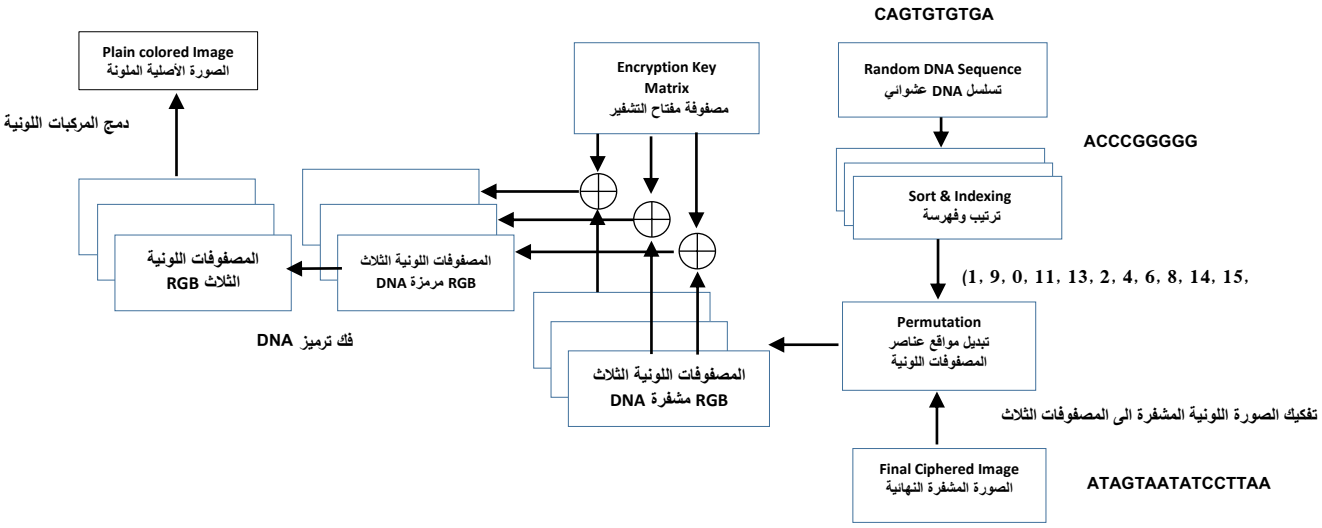
2- إعادة ترتيب مواقع عناصر المصفوفات الثلاث باستخدام الفهارس التي استخدمت في اثناء التشفير.

3- استخدام مصفوفة المفتاح لفك تشفير المصفوفات اللونية الثلاث باستخدام العملية XOR والحصول على المصفوفات اللونية المرمزة DNA.

4- فك ترميز المصفوفات الثلاث من روز DNA الى القيم من 0 الى 255.

5- تحويل المصفوفات اللونية الثلاث من أحادية البعد الى ثنائية الابعاد.

6- دمج المصفوفات اللونية الثلاث والحصول على الصورة الأصلية



الشكل (2) فك تشفير الصورة الملونة

2. تحليل الأمان لخوارزمية تشفير الصور

يتضمن تحليل الأمان للصور المشفرة عدة معايير أو اختبارات لتحديد مدى امان الطريقة المتبعة ومدى فعاليتها ضد الهجمات المختلفة مثل التحليل الإحصائي وهجوم البحث الشامل. تم استعراض معاملات الأمان وتطبيقها على الطريقة المتبعة ومقارنة النتائج مع الدراسات المرجعية ذات الصلة وذلك باستخدام نفس مجموعة البيانات التي استخدمتها تلك الدراسات من صور مرجعية قياسية (Lena وBaboon وPeppers). تشمل معايير الأمان التي تستخدم مع تشفير الصور على ستة معايير وهي معامل الترابط Correlation coefficient وفضاء المفتاح Key Space وحساسية المفتاح Key Sensitivity وانتروبية المعلومات Information Entropy ومخطط الصورة image Histogram ومعاملي الهجمات التفاضلية NCPR وUACI والتي سيتم استعراضها تباعاً:

2. 1. معامل الترابط Correlation coefficient:

تهدف عملية تحليل الترابط إلى دراسة مدى العلاقة بين نقاط البكسل المتجاورة في الصور الرمادية أو ذات التدرج الرمادي. كلما كان الترابط بين نقاط البكسل ضعيفاً في الصورة المشفرة كلما كان أداء خوارزمية التشفير أفضل[11] . يتم حساب معامل الترابط بين قيم البكسل المتجاورة وفق ثلاثة اتجاهات، الافقي Horizontal والعمودي Vertical والقطري Diagonal الشكل (3). ولحساب معامل الترابط تؤخذ مجموعة من النقاط العشوائية للصورة المشفرة ويحسب معامل الترابط بين نقطتي بكسل متجاورتين وفق المعادلات التالية [5]:

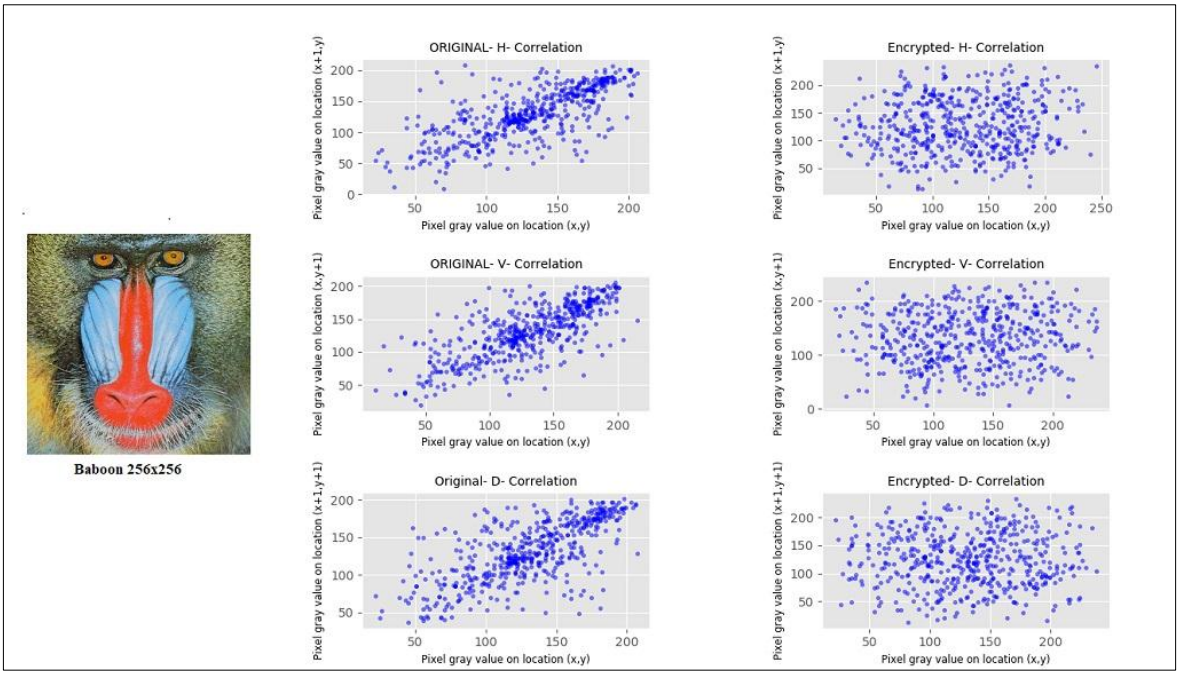
$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \quad (1)$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \quad (2)$$

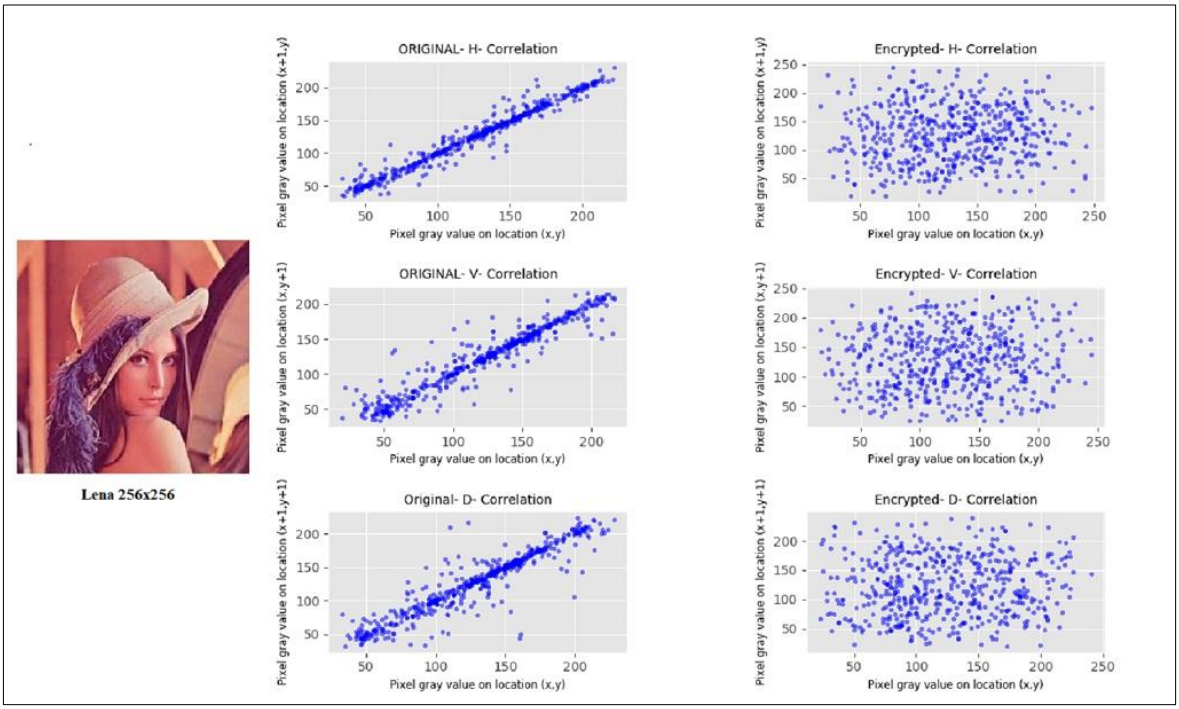
$$C_{covariance}(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \quad (3)$$

$$C_{r(x,y)} = \frac{C_{covariance}(x,y)}{\sqrt{D(x)\times D(y)}} \qquad (4)$$

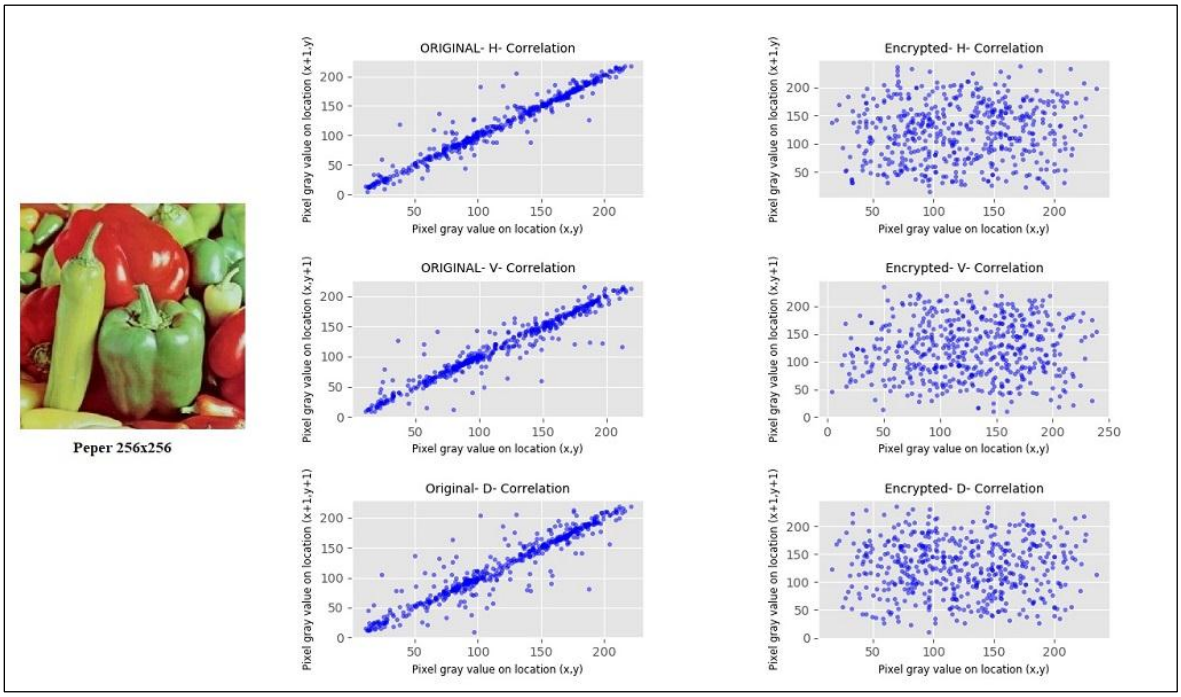
تمثل x,y القيم الرمادية للبكسلات المتجاورة، و N هي العدد الكلي للبكسلات التي تم اختيارها من الصورة و $C_{covariance}(x,y)$ معامل التغاير بينما $D(y)$ هو معامل التباين و $E(x)$ هو المتوسط و $C_{r(x,y)}$ هو معامل الترابط. يبين الشكل (3) مخطط الترابط للصورة القياسية (Baboon و Lena و House و Fruits) يوضح الجدول (5) قيم معامل الترابط لهذه الدراسة مقارنة مع الدراسات المرجعية التي اعتمدت الترميز DNA.



(a)



(b)



(c)

الشكل (3) علاقة الترابط Correlation بين نقاط البكسل للصورة الاصلية والصورة المشفرة بالنسبة للصور القياسية Baboon 256x256 (a) و Lena 256x256 (b) و Pepper 256x256 (c)

الجدول (2) قيم معامل الترابط Correlation coefficient
من أجل الصورة القياسية Lena 256x256

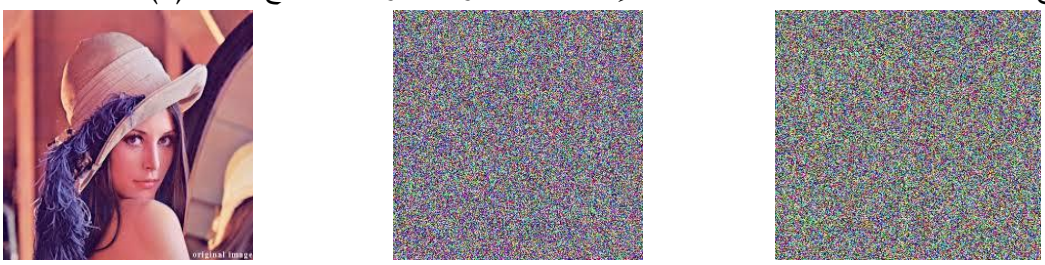
	الدراسة	معامل الترابط Correlation $C_{r(x,y)}$		
		الصورة المشفرة Encrypted Image		
		أفقي Horizontal	عمودي Vertical	قطري Diagonal
1	**المقترحة**	0.0011	0.0013	0.0010
2	[9]	0.0019	0.0027	0.0012
3	[12]	-0.0021	-0.0032	0.0037
4	[13]	0.0681	0.0845	-
5	[14]	0.0044	0.0034	0.0020
6	[15]	-000.1	0.0089	0.0091
7	[16]	0.0011	-0.0013	-0.0019
8	[17]	-0.0021	0.0009	0.0003

يأخذ الجدول رقم (2) قيم معاملات الترابط في ثلاثة اتجاهات، الأفقي والعمودي والقطري للصورة. حققت الطريقة المقترحة معاملات ترابط متقاربة مع الدراسات المرجعية وحققت نتائج أفضل من بعض الدراسات وأقل بمقدار بسيط من بعض الدراسات الأخرى حيث كلما قل معامل الترابط واقتربت قيمته من الصفر كلما كان أفضل لعملية التشفير [17]. إذا كان التعديل في متغير يؤدي إلى تغير في المتغير الآخر عندها يقال بأن المتغيرين مترابطان [18]. إذا انحرف

المتغيران بنفس الاتجاه أي أن الزيادة أو النقصان في أحدهما تؤدي إلى زيادة أو نقصان في المتغير الآخر عندها يقال بأن الترابط مباشر أو موجب. لكن إن انحرف المتغيران باتجاهين متعاكسين، بمعنى آخر زيادة أو نقصان في المتغير الأول قد أدت إلى نقصان أو زيادة في المتغير الثاني عندها يقال بأن معامل الترابط متنوع أو سالب كما في الدراسات [12] و [15] و [17] .

2.3. اختبار حساسية المفتاح

تشير حساسية المفتاح إلى أن تغييراً بسيطاً في مفتاح التشفير سيعطي مفتاحاً جديداً مختلفاً عن الأول وعند استخدام المفتاح الجديد المختلف بشكل بسيط لن يكون بالإمكان فك تشفير الصورة كما يوضح الشكل (4)



(a) (b) (c)

الشكل (4): اختبار حساسية المفتاح، (a) الصورة الاصلية و(b) الصورة المشفرة و(c) تمثل ناتج فك التشفير بمفتاح جرى تعديل بسيط عليه.

3.3. فضاء المفتاح

يشير فضاء المفتاح إلى عدد الاحتمالات التي يجب تجريبها للوصول إلى مفتاح أو مفاتيح التشفير المستخدمة وكلما كان هذا الرقم كبيراً كلما زادت مقاومة الهجمات من نوع البحث الشامل. المفتاح المستخدم في هذه الدراسة بطول 1024 بت يضاف اليه التسلسلات المستخدمة لعملية الفهرسة والتي هي بطول النص المشفر أو بحجم مصفوفة الصورة المشفرة nxm وبالتالي يكون فضاء المفاتيح المستخدم $2^{1024}x2^{nxm}$ أو $10^{308}x2^{nxm}$ حيث تختلف n و m حسب أبعاد الصورة المراد تشفيرها، كمثال صورة بالأبعاد 256x 256 ستنتج فضاء مفاتيح قدره $2^{1024}x2^{56536}$ أي 2^{66560} وهي قيمة كبيرة لاستخدامها في عملية البحث الشامل. يجب أن يكون فضاء المفاتيح بحدود $2^{100}\ bit$ من أجل متطلبات الأمان لمقاومة هجمات البحث الشامل [19] .

4.3. انتروبية المعلومات Information Entropy

يستخدم معيار انتروبية المعلومات لتقييم توزيع قيم البكسل الرمادية في الصورة. تكون قيمة الانتروبية عالية كلما كانت الصورة عشوائية أكثر. بمعنى آخر كلما كان التوزيع متساوى الاحتمال، كلما كان التشفير قادر على مقاومة الهجمات الإحصائية. القيمة النموذجية للانتروبية تكون 8 بالنسبة للصور ذات تدرج رمادي 255−0 ومشفرة بعشوائية حقيقية [10]. يبين الجدول (3) قيم الانتروبية للطريقة المقترحة بالمقارنة مع الدراسات المرجعية. تعطى الانتروبية بالعلاقة الرياضية التالية[17] :

$$H(X) = -\sum_{i=1}^{L} P(x_i) log_2 \mathrm{P}(x_i) \qquad (5)$$

$$\mathrm{P}(X = x_i) = \frac{1}{F} \qquad (6)$$

حيث (x_i) هي القيمة الرمادية و $\mathrm{P}(x_i)$ هو احتمال المستوى الرمادي (x_i)

الجدول (3): انتروبية المعلومات للصورة القياسية 255X255 Lena

Image /Reference	Entropy
(الصورة الاصلية) Plain Image	7.4477
الطريقة المقترحة [Proposed]	7.9983
[9]	7.9996
[10]	7.9976
[20]	7.9994
[21]	7.9970
[22]	7.9980
[23]	7.9975

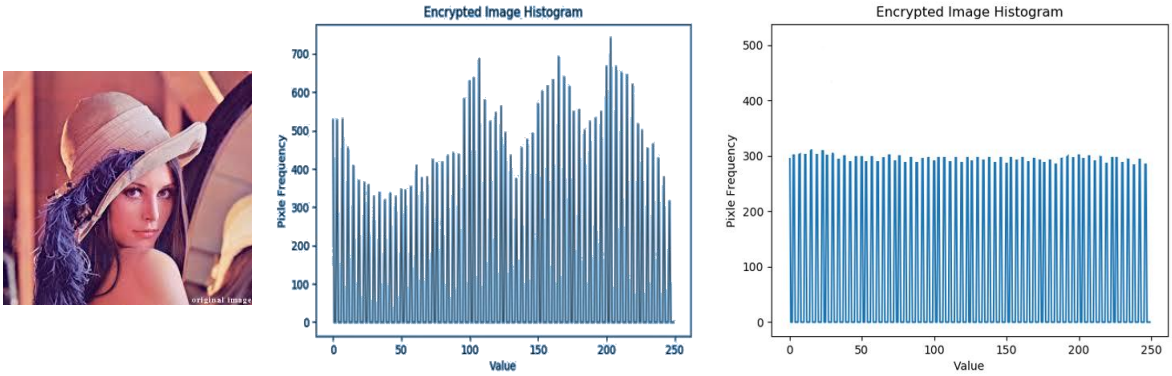
يُظهر الجدول (3)، قيم الانتروبية للصورة القياسية Lena 255x255 والتي لها قيمة انتروبية 7.4477 قبل التشفير وبعد التشفير بالطريقة المقترحة تصبح قيمة الانتروبية 7.9983 وهي قيمة قريبة من 8 ، القيمة النموذجية، أيضا أعطت قيم انتروبية أعلى من الدراسات [10] و [21] و [22] و [23].

5.3. تحليل الهيستوغرام Histogram analysis

يعطي تحليل الهيستوغرام في الشكل(5) فكرة عن فعالية التشفير ضد الهجمات الإحصائية. إذا كان المخطط بشكل توزيع متساوي الاحتمال لقيم البكسل الرمادية والتي تظهر على شكل مسطح، حيث يمكن للصور المشفرة التي لها مخطط مسطح مقاومة الهجمات الاحصائية بفعالية [24]. تعطى تباينات المخطط بالعلاقة الرياضية التالية [25]:

$$var(X) = \frac{1}{n^2}\sum_{i=1}^{n}\sum_{j=1}^{n}\frac{1}{2}(x_i - x_j)^2 \qquad (7)$$

حيث تمثل $X = \{x_0, x_1, x_2, \ldots . x_{255}\}$ شعاع قيم المخطط، و x_i و x_j هي أرقام نقاط البكسل التي قيمها الرمادية تساوي i و j على التوالي و n تعبر عن مستوى الرمادية. عندما تكون قيمة التباين صغيرة يكون التوزيع متساوٍ وهذا مناسب لصد الهجمات الاحصائية [25].



(a) (b) (c)

الشكل (5): المخطط Histogram للصورة الأصلية (b) وللصورة المشفرة (c)

6.3. الهجمات التفاضلية Differential Attacks

يقوم المهاجم في هذا النوع من الهجمات باختيار عدد محدد من الصور الاصلية بشكل عشوائي ثم يقوم بتشفيرها بواسطة خوارزمية التشفير المتبعة ويحصل على الصور المشفرة الموافقة. يتضمن التحليل التفاضلي المقارنة لأزواج من

الصور المشفرة والصور الأصلية بغية الحصول على علاقات تربط بين الصورة الأصلية والصورة المشفرة. في أسوأ الحالات يمكن للمهاجم الحصول على مفتاح التشفير مباشرة. لقياس مستوى مقاومة الهجمات التفاضلية نستخدم المعاملين NPCR (معامل تغير عدد البكسل) و UACI (معدل تغير الشدة الموحد) ويتم التعبير عن كل منهما بالعلاقتين التاليتين [23]:

$$NPCR = \frac{\sum_u D(i,j)}{m \times n} \times 100\% \qquad (8)$$

$$UACI = \frac{1}{m \times n}\left[\sum_{ij} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100\% \qquad (9)$$

تمثل C_1 الصورة المشفرة و C_2 الصورة المشفرة بعد تغيير القيمة الرمادية لأحد قيم البكسل في الصورة الأصلية. بينما تمثل m حجم السطر و n حجم العمود. تشير قيمة $NPCR$ إلى العلاقة بين الصورة الاصلية والصورة المشفرة، إذا كانت قيم البكسل متساوية والتي لها نفس الموقع في المصفوفتين المعبرتين عن الصورة الاصلية والصورة المشفرة تكون $D(i,j) = 0$ وإلا $D(i,j) = 1$. القيمة النموذجية للمعامل $NPCR$ هي 99.61% [26]. أما المعامل $UACI$ فيشير إلى متوسط الشدة بين صورتين والقيمة النموذجية للمعامل $UACI$ هي 33.46% [23]. يبين الجدول (4) قيم المعاملين NPCR و UACI التي تم الحصول عليها والمقارنة مع الدراسات الأُخرى والقيم النموذجية.

الجدول (4): قيم المعاملين NPCR و UACI بالنسبة للصورة القياسية Lena256*256

Ref	Proposed	[9]	[10]	[23]	[29]	[28]	[27]
NPCR	99.98	99.99	99.99	99.64	68.1731	99.5723	99.6378
UACI	33.576	33.76	33.76	33.63	31.7168	33.43	33.6875

يظهر الجدول (4) قيم المعاملين NPCR و UACI للطريقة المتبعة في هذه الدراسة والدراسات الأخرى التي اتبعت نهج مشابه حيث هناك تقارب في القيم للطريقة المتبعة مع الدراسات [9] و [10] وتفوق للطريقة المتبعة على الدراسات [23] و [28] و [27].

النتائج والمناقشة:

قدمت هذه المقالة طريقة جديدة لتشفير الصور الملونة بالاعتماد على عملية الفهرسة لتسلسلات DNA عشوائية، حيث تمت الاستفادة من عملية الفهرسة لتبديل مواقع عناصر المصفوفات اللونية للصورة الملونة قيد التشفير وذلك بدلاً من التسلسلات العشوائية التي تولدها الخرائط العشوائية التي تستخدم في الكثير من خوارزميات تشفير الصور. تم تقييم طريقة تشفير الصور بناءً على عدة معاملات وأعطت نتائج مقاربة في بعض المعاملات الانتروبية وبعض المعاملات كانت أفضل كمعامل الترابط وذلك بالمقارنة مع الطرق الاخرى الواردة في الدراسات المرجعية كما توضح الجداول أعلاه. أثبتت هذه الدراسة أنه يمكن استخدام تسلسلات DNA كمفاتيح وكذلك يمكن الاستفادة من الفهارس الناتجة عنها لتبديل عناصر مصفوفات الصورة الملونة للحصول على الصورة المشفرة.

الاستنتاجات والتوصيات:

تم تقديم طريقة جديدة لتشفير الصور الملونة من خلال استخدام فهرسة تسلسلات DNA عشوائية مأخوذة من قواعد البيانات الجينية العامة. يستخدم مفتاح تشفير من تسلسلات DNA وكذلك تستخدم الفهارس الناتجة لتغيير مواقع عناصر مصفوفات الصورة وبالتالي يجب توفر هذه الفهارس في طرفي التشفير وفك التشفير، يمكن العمل على إيجاد قاعدة بيانات من التسلسلات في طرفي الارسال والاستقبال وتطوير آلية لاختيار التسلسل أو التسلسلات التي ستستخدم في عملية التشفير وفك التشفير من خلال المزامنة بين المرسل والمستقبل لاختيار التسلسل لكن هذا يتطلب ضمان امان وسرية هذه التسلسلات. يمكن تطوير الطريقة التي تم استخدامها في هذه الورقة لتشفير النصوص والصوت والفيديو مستقبلاً.

References:

1. Ahmad Z, Umar H, Li C, Chen3 L. *A DNA-Based Security solution Using Aggregated Chaos Cross and Cubic Map*. The International Arab Journal of Information Technology. 2016; 13(6A): p. 873 - 878.
2. Adleman L. *Molecular Computation of Solutions to Combinatorial Problems*. Science. 1994; 266(5187): p. 1021-1023.
3. Zhou Y, Bao L, Chen P. *A new 1D chaotic system for image encryption.* Signal Processing 97; 2013. p. 171 - 182.
4. Yavuz E, Yazıcı R, Kasapba MC, Yamaç E. *A chaos-based image encryption algorithm with simple logical functions*. Elsevier. 2015;: p. 1- 13.
5. Hamza R, Titouna F. *A novel sensitive image encryption algorithm based on the Zaslavsky chaotic map*. Information Security Journal. 2016;: p. 1 -18.
6. Guesmi R, Farah M, Kachouri A, Samet M. *A novel chaos-based image encryption using DNA sequence operation and Secure Hash Algorithm SHA-2*. Springer Science+Business Media Dordrecht. 2015;: p. 1 -14.
7. Zhang X, Han F, Niu aY. *Chaotic Image Encryption Algorithm Based on Bit Permutation and Dynamic DNA Encoding*. Hindawi. 2017;: p. 1- 11.
8. Kinda AK, Tayseer IS. *Text encryption using OTP keys from randomly generated DNA sequences*. Tishreen University Journal. 2019; 41(4).
9. Kinda AK, Tayseer IS. *Securing Colour Image Based on DNA Encoding and Chaos*. International Journal of Computer Science Trends and Technology (IJCST). 2020; 8(2): p. 9.
10. Salman T, AboKassem K. *Securing Colour Image Based on DNA Encoding and chaos*. International Journal of Computer science trends and technology (IJCST). 2020; 8(2): p. 18 -26.
11. Tang Z, Yang Y, Xu S, Yu C, Zhang aX. *Image Encryption with Double Spiral Scans and Chaotic Maps*. Hindawi -Security and Communication Networks. 2019; 2019: p. 15.
12. Song C, Qiao Y. *A Novel Image Encryption Algorithm Based on DNA Encoding and Spatiotemporal Chaos. Entropy*. 2015;(17): p. 6954-6968.
13. Norouzi B, Seyedzadeh S, Mirzakuchaki S, Mosavi M. *A novel image encryption based on hash function with only two-round diffusion process*. Multimedia Syst. 2013; 20(1): p. 45–64.

14. Enayatifar R, Sadaei H, Abdullah A, Lee M, Isnin IF. *A novel chaotic based image encryption using a hybrid model of deoxyribonucleic acid and cellular automata*. Opt. Lasers Eng. 2015; 71: p. 33–41.
15. J Wu XL, Yang B. *Color image encryption based on chaotic systems and elliptic curve ElGamal scheme*. Signal Process. 2017; 141: p. 109–124.
16. Wang J. *A Color Image Encryption Using Dynamic DNA and 4-D Memristive Hyper-chaos*. IEEE Access. 2019; 7: p. 78367- 78379.
17. Wang X, Wang Y, Zhu X, Luo C. *A novel chaotic algorithm for image encryption utilizing one-time pad based on pixel level and DNA level.* Optics and Lasers in Engineering. 2020; 125: p. 1 -12.
18. S.C G, V.K K. *Fundamentals of Mathematical Statistics* New Delhi: Sultan Chand & Sons Educational Publications; 2001.
19. Song C, Qiao Y. *A Novel Image Encryption Algorithm Based on DNA Encoding and Spatiotemporal Chaos*. Entropy. 2015;(17): p. 6954-6968.
20. Jain A, Rajpal N. *A robust image encryption algorithm resistant to attacks using DNA and chaotic logistic maps*. Multimed Tools Appl. 2016; 75: p. 5455-5473.
21. Agarwal S. *A Chaotic Cryptosystem using Conjugate Transcendental Fractal Function*. I. J. Computer Network and Information Security. 2019; 2(1): p. 1-12.
22. Norouzi B, Mirzakuchaki S, Seyedzadeh SM, Mosavi MR. *A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process*. Multimedia tools and Applications. 2014;(71): p. 1469–1497.
23. Stalin S, Maheshwary P, Shukla PK, Maheshwari M, Gour B, Khare A. *Fast and Secure Medical Image Encryption Based on Non Linear 4D Logistic Map and DNA Sequences* (NL4DLM_DNA). Journal of Medical Systems. 2019; 267(43): p. 1-17.
24. Zhang CT. *Research on Image Encryption Based on DNA Sequence and Chaos Theory*. In Phys. Conf. Ser 1004 012023; 2018.
25. Xl C, Yr C, Lucie B. *A novel chaos based image encryption algorithm using DNA sequence operations*. Opt Lasers Eng. 2017; 88: p. 197 - 213.
26. Wang Y, Wong K, Liao X, Xiang T, Chen G. *A chaos-based image encryption algorithm with variable control parameters*. Chaos Solitons Fractals. 2009; 41(4): p. 1773-83.
27. LI X, Zhou C, Xu N. *A Secure and Efficient Image Encryption Algorithm Based on DNA Coding and Spatiotemporal Chaos*. International Journal of Network Security. 2018; 20(1): p. 110-120.
28. Li T, Yang M, Wu J, Jing X. *A Novel Image Encryption Algorithm Based on a Fractional-Order Hyperchaotic System and DNA Computing*. Hindawi. 2017;: p. 13.