مجلة جامعة فزان العلمية
Fezzan University scientific Journal
journal@fezzanu.edu.ly

ورقة مسحية لخوارزميات تشفير الصور الرقمية ومقاييس تقييمها

* خالد الحداد[1] ، لطفي عبدالصمد[2]
[1] قسم الهندسة الكهربائية والحاسوب ، كلية الهندسة القره بوللي، جامعة المرقب
[2] قسم الحاسوب، كلية الآداب والعلوم مسلاته، جامعة المرقب

الملخص

تعد تقنيات تشفير الصور ركيزة أساسية في الأمن السيبراني لحماية الوسائط المتعددة عبر الشبكات غير الآمنة، وشهد تبادل الصور الرقمية عبر شبكات الاتصالات المفتوحة نمواً هائلاً في الآونة الأخيرة، مما جعل حمايتها وضمان سريتها أمرا بالغ الأهمية في مجالات متعددة؛ مثل: الأمن السيبراني، الأنظمة العسكرية، والتطبيقات الطبية. ونظراً للخصائص الذاتية للصور مثل الحجم الضخم والارتباط الوثيق والارتفاع العالي في تكرار البيانات بين البكسلات المتجاورة، فإن خوارزميات التشفير التقليدية المخصصة للنصوص تثبت عدم كفاءتها. تسلط هذه الورقة المسحية الضوء على المشهد الحالي لخوارزميات تشفير الصور الرقمية، حيث تقدم تصنيفاً شاملاً لأبرز التقنيات الحديثة بما في ذلك الأنظمة القائمة على نظرية الفوضى (Chaos) الحوسبة الحيوية للحمض النووي (DNA) ، والتحويلات الرياضية، بالإضافة إلى الأنظمة الهجينة. علاوة على ذلك، توفر الورقة تحليلاً نقدياً واستعراضاً مفصلاً لمقاييس تقييم الأمان والكفاءة الحسابية المستخدمة للحكم على قوة هذه الخوارزميات، مثل تحليل مخطط التكرار (Histogram)، معامل الارتباط، الإنتروبيا، ومعايير الحساسية للهجمات التفاضلية (UACI&NPCR). واختتمت الورقة باستعراض أبرز التحديات الراهنة والتوجهات المستقبلية في هذا المجال، مثل التشفير المتوافق مع أجهزة إنترنت الأشياء والتشفير المقاوم للحوسبة الكمومية، لتكون هذه الدراسة مرجعاً شاملاً للباحثين والمطورين في مجال أمن الوسائط المتعددة.

الكلمات المفتاحية: أمن الوسائط المتعددة، تشفير الحمض النووي (DNA)، تشفير الصور الرقمية، مقاييس الأمان، نظرية الفوضى، هجمات تفاضلية.

A survey paper on digital image encryption algorithms and their evaluation criteria

* K.M Elhadad[1] and LTFEI .A. Abdalsmd[2].
[1]Department of Electrical and Computer Engineering - Faculty of Engineering Qarahbulli - Elmergib University.
[2]Department of Computer - Faculty of Arts and Sciences Mislata - Elmergib University

Abstract

Image encryption technologies are a cornerstone of cybersecurity for protecting multimedia across unsecured networks. The exchange of digital images over open communication networks has grown exponentially in recent years, making their protection and confidentiality crucial in various

*المؤلف الرئيسي: عناوين البريد الإلكتروني kmelhadad@elmergib.edu.ly تاريخ استلام البحث 19 أبريل 2026 استلام رد المحكمين 25 يونيو 2026 تم قبوله 26يوليو 2026 تاريخ النشر 1أغسطس 2026

fields such as cybersecurity, military systems, and medical applications. Due to the inherent characteristics of images, such as their large size, close correlation, and high data redundancy between adjacent pixels, traditional encryption algorithms designed for text prove inadequate.
This overview sheds light on the current landscape of digital image encryption algorithms, providing a comprehensive classification of the most prominent modern techniques, including chaos-based systems, DNA bio computation, mathematical transformations, and hybrid systems. Furthermore, the paper provides a critical analysis and detailed review of the security and computational efficiency metrics used to assess the strength of these algorithms, such as histogram analysis, correlation coefficient, entropy, and differential attack sensitivity criteria (UACI and NPCR).
The paper concludes by reviewing the most prominent current challenges and future trends in this field, such as IoT-compatible encryption and quantum computing-resistant encryption, making this study a comprehensive reference for researchers and developers in the field of multimedia security.
Keywords: Security Metrics, DNA Cryptography, Digital Image Encryption, Multimedia Security, Chaos Theory, Differential Attacks.

المقدمة

في العصر الرقمي الحالي، أصبحت الصور الرقمية وسيلة أساسية لنقل وتبادل المعلومات عبر شبكات الاتصالات المفتوحة والإنترنت. تُستخدم هذه الصور بكثافة في تطبيقات بالغة الحساسية تشمل التشخيص الطبي (مثل صور الأشعة والرنين المغناطيسي)، والأنظمة العسكرية (مثل صور الأقمار الصناعية والاستطلاع)، بالإضافة إلى المعاملات التجارية والخصوصية الشخصية. نظراً لطبيعة الشبكات غير الآمنة، فإن هذه البيانات المرئية معرضة باستمرار لمخاطر أمنية جمة مثل التنصت، التعديل غير المصرح به، والسرقة. بناءً على ذلك، أصبحت حماية سرية الصور الرقمية وضمان سلامتها ضرورة ملحة وأولوية قصوى في مجال الأمن السيبراني، وأمن الوسائط المتعددة[1](Multimedia Security) .

تاريخياً، تم تطوير العديد من خوارزميات التشفير التقليدية لحماية البيانات النصية، ومن أبرزها معيار التشفير المتقدم(AES) [2]، ومعيار تشفير البيانات الثلاثي(3DES) ، وخوارزمية [3]ورغم الكفاءة العالية التي أثبتتها هذه الخوارزميات في حماية النصوص، إلا أنها تواجه تحديات وقصوراً كبيراً عند تطبيقها مباشرة على الصور الرقمية. يعود هذا الإخفاق إلى الخصائص الذاتية الفريدة التي تتميز بها الصور مقارنة بالنصوص؛ فالصور تحتوي على حجم بيانات ضخم جداً(Bulk Data Size) ، وتكرار عالٍ في البيانات (High Redundancy)، والأهم من ذلك هو وجود ارتباط وثيق وقوي جداً (Strong Linear Correlation)بين البكسلات المتجاورة في الاتجاهات الأفقية والعمودية والمائلة. هذه الخصائص تجعل التشفير التقليدي بطيئاً جداً وغير فعال، كما أنه قد يترك أنماطاً مرئية تسرب معلومات عن الصورة الأصلية، مما يسهل اختراقها إحصائياً.

لتجاوز هذه العقبات، اتجه العلماء نحو تطوير خوارزميات تشفير مخصصة للصور تعتمد على آليات معقدة وغير خطية لكسر الارتباط بين البكسلات وتوزيع القيم بشكل عشوائي. برزت في هذا السياق "نظرية الفوضى (Chaos Theory) كواحدة من أكثر التقنيات نجاحاً وشعبية[4]، نظراً لحساسيتها الفائقة للشروط الأولية وعشوائيتها العالية. كما ظهرت تقنيات واعدة أخرى مستوحاة من الطبيعة مثل تشفير الحمض النووي

(DNA Computing)، وتقنيات النطاق الترددي والتحويلات الرياضية، بالإضافة إلى الأنظمة الهجينة التي تدمج أكثر من تقنية لرفع مستوى الأمان.[5] ومع هذا التنوع الهائل في الخوارزميات المقترحة، برزت حاجة ماسة لوجود مقاييس تقييم معيارية وصارمة للحكم على قوة التشفير، مثل تحليل مخطط التكرار (Histogram)، اختبارات العشوائية(Entropy) ، ومعاملات الحساسية للهجمات التفاضلية UACI و NPCR.

سدّاً لهذه الفجوة، تأتي هذه الورقة المسحية لتقديم مراجعة شاملة ومنهجية لأحدث التطورات في مجال تشفير الصور الرقمية. لا تقتصر مساهمة هذه الدراسة على سرد الخوارزميات فحسب، بل تمتد لتقديم تصنيف هيكلي واضح للتقنيات الحديثة، مع التركيز على شرح آلية عمل كل عائلة ومناقشة نقاط قوتها وضعفها. كما توفر الورقة دليلاً تفصيلياً للمقاييس الرياضية والإحصائية المستخدمة في تقييم جودة التشفير. وأخيراً، تسلط الورقة الضوء على التحديات الراهنة وتفتح آفاقاً للتوجهات المستقبلية، مما يجعلها مرجعاً أساسياً للباحثين والمطورين الساعين لبناء أنظمة تشفير صور أكثر أماناً وكفاءة.

على الرغم من وفرة الدراسات التي تقترح أنظمة تشفير صور جديدة، إلا أن تقييم قوتها التشفيرية لا يزال يمثل تحديًا معقدًا. يجب أن يُظهر التشفير القوي مقاومة لمجموعة من الهجمات المتطورة، بما في ذلك هجمات القوة الغاشمة، والهجمات الإحصائية، والهجمات التفاضلية، وهجمات النص الصريح المُختار. ونتيجة لذلك، يعتمد الباحثون على مجموعة متنوعة من مؤشرات الأداء، مثل إنتروبيا المعلومات، ومعاملات الارتباط، وتحليل فضاء المفاتيح، والمقاييس التفاضلية مثل معدل تغير عدد البكسلات (NPCR) ومتوسط شدة التغير الموحد(UACI).[6] .

في حين نُشرت العديد من الدراسات الاستقصائية في هذا المجال، إلا أن العديد من المراجعات الحالية غالبًا ما تركز على فئة واحدة من الخوارزميات (على سبيل المثال، الأنظمة القائمة على الفوضى فقط أو الأنظمة القائمة على الحمض النووي فقط) مما يُعيق تقديم رؤية شاملة. وغالبًا ما يتجاهلون الاشتقاق الرياضي الشامل ومعايير الأساس الموحدة لمقاييس التقييم نفسها، مما قد يؤدي إلى تباين في المقارنة المعيارية. كما أنهم لا يتناولون التحديات المعاصرة بشكل كافٍ، مثل قيود أجهزة إنترنت الأشياء (IOT) التي تعمل في الوقت الفعلي، أو التهديد الوشيك لتحليل التشفير ما بعد الكمومي.[7]

تستند هذه الدراسة إلى الحاجة لسد هذه الفجوة من خلال تقديم مراجعة شاملة حديثة ودقيقة وموحدة، تُدقّق في كلٍ من التصاميم الخوارزمية ومقاييس التقييم الإحصائي الخاصة بها، ويمكن تلخيص المساهمات الرئيسية لهذه الدراسة الاستقصائية على النحو الآتـــي:

- التصنيف المنهجي: نقدم تصنيفًا منظمًا لأحدث خوارزميات تشفير الصور الرقمية، مع تفصيل آليات عملها الأساسية ومزاياها وقيودها المتأصلة.
- تحليل معياري دقيق: نقدم تحليلًا رياضيًا شاملًا لمقاييس الأمان والأداء المعيارية، مما يُرسي أساسًا دقيقًا لتقييم متانة التشفير.
- تقييم مقارن نقدي: نقدم تحليلًا مقارنًا لنماذج التشفير المختلفة، مع تقييم المفضالات بين مستوى الأمان والتعقيد الحسابي.
- خارطة طريق مستقبلية: نحدد تحديات البحث المفتوحة ونرسم مسارات مستقبلية واعدة، مع التركيز بشكل خاص على تشفير الصور المقاوم للحوسبة الكمومية والتشفير الخفيف للبيئات ذات الموارد المحدودة.

يُقسم باقي هذا البحث كما يلي: يستكشف القسم 2 البنية الأساسية لتشفير الصور، مع تفصيل نموذج التشويش والانتشار التقليدي. يُلخص القسم 3 التصنيف المنهجي لخوارزميات التشفير الحديثة. يقدم القسم 4 عرضًا شاملًا لمقاييس تقييم الأمان مع صياغاتها الرياضية. يناقش القسم 5 التوصيات والأعمال المستقبلية وأخيرًا يُختتم البحث في القسم 6.

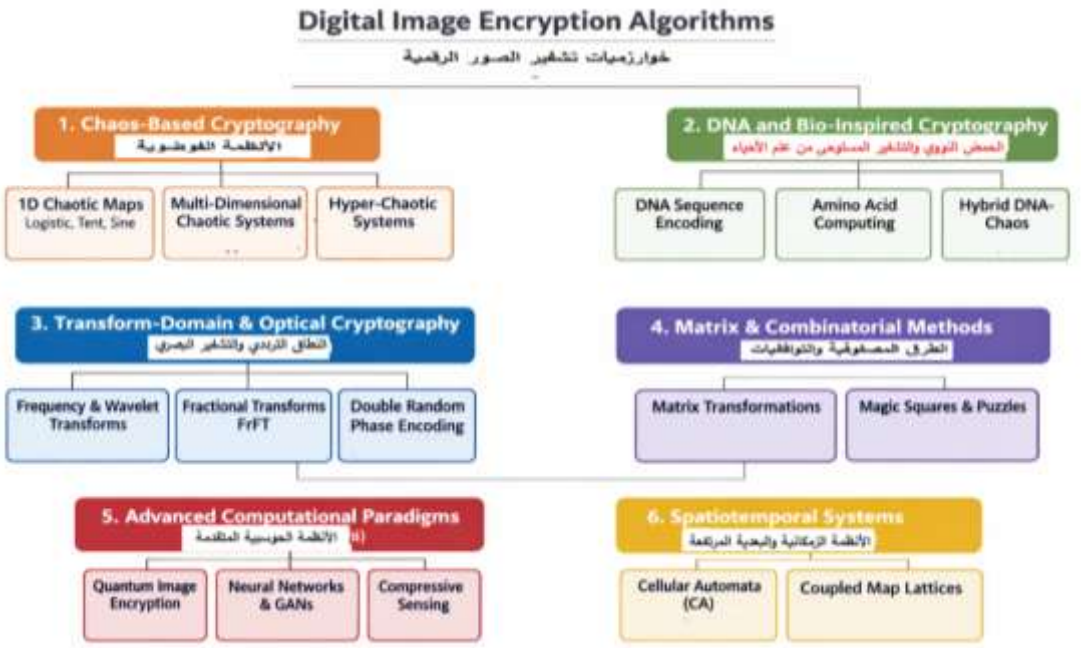
البنية الأساسية لتشفير الصور

يعتمد الأمن الهيكلي لأنظمة تشفير الصور الرقمية الحديثة بشكل أساسي على بنية التشويش (Confusion) والانتشار (Diffusion) الكلاسيكية، وهي نموذج تشفيري قدمه كلود شانون.[8] على عكس معايير التشفير النصية العامة، تتطلب البيانات المرئية إطار عمل تشغيلي متخصص من مرحلتين لكسر التوزيعات المكانية شديدة الارتباط والتكرار الهائل للبيانات المتأصل في شبكات البكسل الرقمية بكفاءة. مرحلة التشويش (تبديل البكسل) التي غالبًا ما تُنفذ رياضيًا على مستوى البكسل كتشويش أو تبديل هو إخفاء الارتباط الخطي المحلي بين صورة النص الأصلي المدخلة والنص المشفر الناتج. في هذه المرحلة يقوم تسلسل ديناميكي شبه عشوائي أو فوضوي برسم إحداثيات كل بكسل المكانية الأصلية (x, y) إلى مواقع جديدة غير منتظمة للغاية داخل المصفوفة دون تغيير قيم تدرج الرمادي أو شدة اللون الفعلية. يُقلل هذا الترتيب الهندسي بشكل كبير من معاملات ارتباط التجاور إلى الصفر، مما يُفكك الأنماط المرئية للصورة فعليًا[9].

أما مرحلة الانتشار(استبدال البكسل) فإنه يُبقي إحصائيات الصورة العامة، مثل توزيع الهيستوغرام (Histogram)، دون تغيير تمامًا وعرضة للتحليل الإحصائي. وللتخفيف من ذلك تُنفذ البنية الأساسية طبقة انتشار بشكل متسلسل؛ فيتم تُغير آلية الانتشار القيم العددية الفعلية للبكسلات عن طريق نشر تأثير بت واحد من النص الأصلي أو مُعامل مفتاح عبر شبكة الصورة بأكملها. عادةً ما يتم حساب الانتشار عبر الحساب النمطي أو عمليات XOR الثنائية مع تدفقات المفاتيح، مما يُسطح هيستوغرام النص المُشفر إلى توزيع مُنتظم، ويجعل التحليل الإحصائي للتشفير غير ضروري [10].

التصنيف المنهجي لخوارزميات تشفير الصور الحديثة

تم تطوير أنظمة تشفير الصور الحديثة للتغلب على البنية الهيكلية لشبكات البكسل. الشكل 1 يوضح التصنيف المنهجي لأهم عائلات خوارزميات تشفير الصور:



شكل 1: التصنيف المنهجي لخوارزميات تشفير الصور الحديثة

خوارزميات التشفير القائمة على الفوضى (Chaos–Based Encryption Algorithms)

تعتمد هذه المجموعة من الخوارزميات على المعادلات الديناميكية غير الخطية لتوليد حالات شبه عشوائية. وهي تنقسم إلى خرائط منخفضة الأبعاد (أحادية البعد) مثل خريطة لوجستيك (Logistic map) أو خريطة الخيمة (Tent map)، وأنظمة عالية الأبعاد/شديدة الفوضى (Lorenz or Chen systems) التي تمتلك أسس Lyapunov exponents [11].

حيث تعمل المعلمات الأولية (initial parameters) كمفتاح سري، تُكرر الخوارزمية الخريطة الفوضوية لإنتاج متواليات فوضوية. تُستخدم هذه المتواليات بعد ذلك لخلط إحداثيات البكسل (Confusion phase) وتغيير قيم البكسل عبر عملية XOR أو الحساب النمطي (Diffusion phase). مزايا هذه الخوارزميات الحساسية الفائقة للشروط الأولية (حساسية عالية للمفتاح)، تكوين مسار فوضي عالي وغير قابل للتنبؤ، مما يوفر مقاييس أمان ممتازة. وسرعة حسابية عالية نسبيًا للخرائط منخفضة الأبعاد. من عيوبها تدهور الدقة المحدودة في الحواسيب الرقمية حيث تكون أعداد الفاصلة العائمة (floating–point numbers) محدودة [12]. ومع تكرار العمليات الحسابية، قد تصبح المدارات الفوضوية دورية، مما يقلل من العشوائية.

وأيضا يمكن أحيانًا التنبؤ بالخرائط منخفضة الأبعاد باستخدام تحليل السلاسل الزمنية إذا كانت مساحة المفاتيح صغيرة.

الحوسبة باستخدام الحمض النووي والتشفير المستوحى من علم الأحياء
(DNA–Computing and Bio–Inspired Cryptography)

يربط هذا النموذج علمين هما علم الأحياء وعلم التشفير وذلك من خلال التعامل مع تدفقات البيانات كسلاسل بيولوجية؛ حيث تُحوّل وحدات البكسل في الصورة الرقمية (من 0 إلى 255) إلى نظام ثنائي، ثم تُشفّر في نيوكليوتيدات الحمض النووي، وذلك باستخدام قواعد ثابتة ($00 \rightarrow A$, $01 \rightarrow C$,$10 \rightarrow G$,$11 \rightarrow T$). تُجرى عمليات التشفير باستخدام قواعد جبرية بيولوجية (جمع الحمض النووي،

وطرحه، وXOR). أخيرًا، تُفكّ شفرة المصفوفات مرة أخرى إلى قيم البكسل. المزايا هي قدرة معالجة متوازية هائلة متأصلة في نظريات الحوسبة الجزيئية الحيوية [13]، مساحات مفاتيح واسعة للغاية عند دمجها مع قواعد التشفير البيولوجي الديناميكية، مقاومة عالية ضد تحليل التشفير الخطي القياسي. العيوب هي عبء حسابي كبير يتطلب محاكاة عمليات الحمض النووي البيولوجي على أجهزة الكمبيوتر السيليكونية القياسية قوة معالجة عالية وتسبب زمن استجابة كبير، نادرًا ما تُستخدم كحل مستقل؛ فهي تتطلب دائمًا تقريبًا مولدًا فوضويًا للتعامل مع تشفير المفتاح البيولوجي ديناميكيًا.

النطاق الترددي والتشفير البصري (Transform–Domain and Optical Cryptography)

بدلاً من معالجة البكسلات في التخطيط المكاني، تحوّل هذه الخوارزميات بيانات الصورة إلى مكونات ترددية. وآلية التشغيل تكون بمعالجة الصورة باستخدام تحويلات رياضية مثل تحويل فوريه المنفصل (DFT) أو تحويل المويجات المنفصل (DWT). في الأطر البصرية، مثل التشفير الطوري العشوائي المزدوج (DRPE)، تُحوّل الصورة الأصلية إلى توزيعات طور وسعة بصرية باستخدام العدسات البصرية وأشعة الليزر. ومن مزايا هذا النوع المقاومة العالية للتشويش والقص، إذا فُقد جزء من الصورة المشفرة أثناء الإرسال، فإن طيف التردد يحافظ على البنية العامة، مما يسمح بفك التشفير بنجاح مع فقدان طفيف في الجودة، وسرعات تنفيذ فائقة عند التنفيذ مباشرةً في الأجهزة باستخدام معدات الحوسبة البصرية. ولكن من عيوب هذه الطريقة الاعتماد على الأجهزة التي توفر للأنظمة البصرية محاذاة دقيقة للعدسات ومصادر الليزر، وهي حساسة للغاية للاهتزازات البيئية، وأيضا تتضمن عمليات المحاكاة الرقمية لمجالات التردد عمليات ضرب معقدة للأعداد المركبة، مما يؤدي إلى اختناقات حسابية[14] .

الطرق المصفوفية والتوافقيات(Matrix & Combinatorial Techniques)

تعتمد هذه الطرق على استخدام التحويلات المصفوفية والعلاقات التوافقية لإعادة ترتيب أو تبديل عناصر الصورة بطريقة يصعب عكسها دون المفتاح الصحيح. يتم استخدم مصفوفات رياضية (مثل مصفوفة هادامارد أو مصفوفة هيل) لتغيير مواقع البكسلات أو قيمها (Matrix Transformations) [15].

أو باستخدام المربعات السحرية والألغاز (Magic Squares & Puzzles) التي يتم عن طريقها ترتيب عناصر الصورة وفق أنماط رياضية محددة بحيث يكون مجموع الصفوف والأعمدة متساويًا، مما يخلق توزيعًا معقدًا للبكسلات. هذه الطريقة تُستخدم غالبًا في التشفير الخفيف أو كمرحلة أولى قبل تطبيق خوارزميات أكثر تعقيدًا. وتتميز بسهولة التنفيذ رياضيًا وسرعة في المعالجة مقارنة بالخوارزميات الفوضوية أو الكمومية. ويتم أحيانا الدمج مع طرق أخرى (مثل الفوضى أو التحويلات الترددية) لزيادة الأمان، ويعاب عليها ضعف الأمان إذا استخدمت مصفوفات صغيرة أو أنماط متكررة. وأنها قابلة للهجوم بالإحصاء أو التحليل الرياضي إذا لم تُدمج مع تقنيات أخرى.

الأنظمة الحوسبية المتقدمة (A Compressive Sensing & Quantum Encryption)

ويمثل هذا الحدود الحديثة لأمن الوسائط المتعددة، ويستهدف بيئات هندسية محددة وتشمل[1]:

الاستشعار المضغوط (CS)

الآلية: يقوم الاستشعار المضغوط بأخذ عينات من الصور المتفرقة بمعدل أقل بكثير من معيار Nyquist criterion باستخدام مصفوفة قياس عشوائية كمفتاح أمان، يتم ضغط الصورة وتشفيرها في نفس الوقت تمامًا، وتتميز بتوفير عرض نطاق ترددي للإرسال ومساحة التخزين مثاليه للبنى ذات الموارد المحدودة مثل

شبكات الاستشعار اللاسلكية (WSN)، ويعاب عليها أنها تتطلب عملية إعادة البناء في جانب المُستقبِل وحل مسائل تحسين غير خطية معقدة، مما يستغرق وقتًا طويلاً.

تشفير الصور الكمومي:

يتم تُمثل الصور باستخدام حالات كمومية (مثل نموذج NEQR) ويعالج البكسلات باستخدام البوابات الكمومية والمسارات الكمومية. ومزايا هذا التشفير انه محصن ضد الهجمات المستقبلية التي تشنها الحواسيب الكمومية (أمان ما بعد الكم). وعيوبه انه لا يمكن تشغيله بشكل أصلي حتى يصبح جهاز كمومي كامل النطاق متاحًا تجاريًا.

الأنظمة الزمكانية والبعدية المرتفعة(Spatiotemporal & High-Dimensional Systems)

تعتمد هذه الأنظمة على دمج البعدين الزماني والمكاني في عملية التشفير، بحيث تتغير قيم البكسلات عبر الزمن والموقع في الصورة، مما يولّد ديناميكية معقدة يصعب تحليلها أو كسرها رياضيًا. والنموذج الرياضي (Cellular Automata) يتكون من شبكة خلايا تتفاعل وفق قواعد محددة. كل خلية تمثل بكسلًا، وتتغير حالتها بناءً على حالات الجيران. وتستخدم هذه التقنية لتوليد أنماط تشفير تعتمد على التطور الزمني للنظام، مما يزيد من العشوائية، ويتم أيضا عن طريق الشبكات المترابطة (Coupled Map Lattices) وهي تجمع بين الخرائط الفوضوية والأنظمة المكانية، حيث يتم ربط عدة خرائط فوضوية لتعمل بشكل متزامن عبر الشبكة .هذه الطريقة تنتج توزيعًا معقدًا للبكسلات وتزيد من مقاومة الهجمات الإحصائية.

وتتميز هذه الخوارزميات بتوليد مفاتيح تشفير عالية التعقيد ومقاومة قوية لهجمات التحليل الزمني والمكاني وإمكانية الدمج مع خوارزميات فوضوية أو كمومية لزيادة الأمان. لكن تتطلب قدرة حسابية عالية وصعوبة ضبط المعاملات لتحقيق التوازن.

ويوضح جدول 1 اهم التطبيقات النموذجية التي يتم استخدام إحدى خوارزميات التشفير فيها واهم مقياس التقييم المستخدمة للقياس مدي قوة وامان خوارزمية التشفير.

جدول 1: أهم مزايا وعيوب أنظمة التشفير

عائلة الخوارزميات	الفكرة الأساسية	المزايا الرئيسية	العيوب والقيود المتأصلة
الأنظمة الفوضوية (Chaos-Based)	استخدام معادلات ديناميكية غير خطية لتوليد سلاسل عشوائية تدفع مراحل الإرباك (Confusion) والانتشار (Diffusion).	• سرعة تنفيذ عالية جداً. • حساسية فائقة للمفاتيح والشروط الأولية. • إنتروبيا مرتفعة.	• تدهور عشوائية السلسلة بسبب الدقة الرقمية المحدودة للحواسيب (Finite Precision).
حوسبة الحمض النووي (DNA-Computing)	تحويل البكسلات إلى نيوكليوتيدات بيولوجية (A, C, G, T) وتطبيق عمليات جبرية جزيئية عليها.	• مساحة مفتاح فائقة الضخامة تمنع الهجمات الغاشمة. • قدرة معالجة متوازية هائلة.	• عبئ حسابي ثقيل جداً. • (Time Latency) عند محاكاتها على معالجات السيليكون التقليدية.
نطاق التحويل والبصريات (Transform-Domain)	تشفير مكونات الصورة الترددية (مثـل DWT/DFT) أو الطور البصري باستخدام عدسات وأشعة الليزر(مثل DRPE).	• مقاومة ممتازة للضوضاء وفقدان البيانات (Cropping). • سرعة معالجة فائقة إذا	• قيود صارمة في المحاذاة الفيزيائية للعدسات. • عبء معالجة الأعداد المركبة الحسابي رقمياً.

		نُفذت عبر عتاد بصري.	
الاستشعار المضغوط (Compressive Sensing)	أخذ عينات متناثرة من الصورة وضغطها وتشفيرها في خطوة واحدة عبر مصفوفة قياس عشوائية.	• توفير هائل في حجم البيانات المتداولة والنطاق الترددي لشبكة الاتصال.	• بطء حاد وتأخير زمني كبير عند فك التشفير وإعادة بناء الصورة لدى المستقبل.
التشفير الكمومي (Quantum Encryption)	تمثيل الصورة باستخدام حالات الكيوبتات (Qubits) وتعديلها عبر بوابات ومسارات عشوائية كمومية.	• مناعة مطلقة ضد الاختراق الحسابي. • توفير أمان مستقبلي ضد الحواسب الكمومية (Post-Quantum).	• تطبيق فيزيائي معقد جداً؛ حيث يظل معظمها نظرياً ومخبرياً في الوقت الحالي.

مقاييس تقييم الأمان

1. مقاييس التحليل الإحصائي (Statistical Analysis Metrics)

معيار إنتروبيا (Entropy)

هو اختبار إحصائي يُستخدم لقياس العشوائية في الأنظمة، وقد قدمه Claude Shannon عام 1948. ويستخدم في تشفير الصور لقيس مدى عشوائية توزيع البكسلات في الصورة المشفرة، وتدل قيمته العالية على إخفاء قوي للنص الأصلي وعدم وجود أنماط يمكن استغلالها. ويتم حسباها بالمعادلة

$$H = -\sum_{i=0}^{n} p(i) log_2 p(i) 4 \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots (1)$$

حيث يمثل n عدد البتات المستخدمة لتمثيل الرمز p(i) ، و p(i) يمثل احتمال ظهور الرمز i ، يمكن حساب إنتروبيا الصورة باستخدام المعادلة (4)، حيث يمثل p(i) عدد مرات ظهور كل قيمة شدة إضاءة في الصورة، وفقًا للتوزيع التكراري المعياري بافتراض أن أقصى قيمة شدة إضاءة ممكنة للبيكسل في تمثيل 8 بت هي 256، وأن احتمال ظهور قيمة البيكسل هو 1، فإن القيمة المثالية للإنتروبيا للصورة يمكن حسابها باستخدام المعادلة (4)، كما يلي:

$$H = -\sum_{i=0}^{255} \frac{1}{256} log_2 \frac{1}{256} = 8 \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots (2)$$

ويوضح معيار إنتروبيا (Entropy) مدى العشوائية وعدم القدرة على التنبؤ في الصورة المشفرة. حيث انه كلما اقتربت قيمة الإنتروبيا من الحد المثالي (≈ 8 للصور الرمادية)، زادت قوة الخوارزمية[16].

معامل **الارتباط (Correlation Coefficient)**

هو مقياس إحصائي يُستخدم في تشفير الصور لتحديد مدى العلاقة بين قيم البكسلات في الصورة الأصلية والمشفرة. كلما كان معامل الارتباط قريبًا من الصفر، دلّ ذلك على أن الصورة المشفرة عشوائية، ولا تحتوي على أنماط يمكن استغلالها، مما يعني أن الخوارزمية أكثر أمانًا، ويتم يتم حساب معامل الارتباط في ثلاث اتجاهات أفقي (Horizontal) وعمودي (Vertical) وقطري (Diagonal)، والمعادلة الرياضية له:

$$\boldsymbol{r} = \frac{\sum_{i=1}^{n}(\boldsymbol{x_i} - \tilde{\boldsymbol{x}})((\boldsymbol{y_i} - \tilde{\boldsymbol{y}})}{\sqrt{\sum_{i=1}^{n}(\boldsymbol{x_i} - \tilde{\boldsymbol{x}})^2 \sqrt{\sum_{i=1}^{n}(\boldsymbol{y_i} - \tilde{\boldsymbol{y}})^2}} \quad \dots\dots\dots\dots\dots\dots (3)$$

عندما $\boldsymbol{x_i}, \boldsymbol{y_i}$ قيم البكسلات المتجاورة و $\tilde{\boldsymbol{x}}, \tilde{\boldsymbol{y}}$ المتوسط الحسابي للقيم

مقاييس تحليل الهجوم التفاضلي (تحليل الهجوم التفاضلي)

يقيّم التحليل التفاضلي مدى حساسية التشفير للتغييرات الطفيفة في صورة النص الأصلي. إذا أدى تغيير بكسل واحد في الصورة الأصلية إلى صورة مشفرة مختلفة تمامًا، فإن الخوارزمية آمنة. يُقاس ذلك باستخدام مؤشرين رئيسيينNPCR و UACI.

معدل تغيير البكسل الواحد(NPCR)

اختصار لـ (Number of Pixels Change Rate) يقيس هذا المؤشر نسبة عدد البكسلات التي تغيرت قيمتها بين الصورتين المشفرتين نتيجة لتغيير بكسل واحد في الصورة الأصلية. ويحسب بالمعادلة الرياضية:

$$NPCR = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j)}{M * N} * 100\% \quad \ldots\ldots\ldots\ldots\ldots \quad (4)$$

حيث أن:

M و N هما أبعاد الصورة (الارتفاع والعرض).

$D(i,j)$ هي مصفوفة ثنائية (Binary Matrix) يتم تحديد قيمها بناءً على المقارنة بين الصورتين المشفرتين C_1 و C_2 عند الإحداثيات (i,j) كالتالي:

$$D(i,j) = \begin{cases} 0, & if\ C_1(i,j) = C_2(i,j) \\ 1, & if\ C_1(i,j) \neq C_2(i,j) \end{cases}$$

بالصيغة النظرية للصورة الرمادية ذات العمق الموجي(8–bit) ، فإن القيمة المثالية لـ $NPCR$ هي 99.6094% .كلما اقتربت النتيجة من هذه القيمة، كانت الخوارزمية أكثر مقاومة للهجوم.

متوسط شدة التغيير الموحد(UACI)

اختصار لـ (Unified Average Changing Intensity) لا يكتفي هذا المقياس بمعرفة هل تغير البكسل أم لا مثلNPCR بل يحسب معدل شدة وفارق الاختلاف في القيمة بين البكسلات المتغيرة في الصورتين المشفرتين ويحسب بالمعادلة الرياضية:

$$.UACI = \frac{1}{M*N}\left[\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|C_1(i,j)-C_2(i,j)|}{255}\right] * 100\% \quad \ldots\ldots\ldots\ldots \quad (5)$$

حيث إن:

$|C_1(i,j) - C_2(i,j)|$ هو القيمة المطلقة للفرق بين قيمة البكسل في الصورة الأولى والصورة الثانية.

الرقم 255 يمثل الحد الأقصى لقيمة البكسل في الصور من نوع(8 bit) .

والقيمة النظريّة المثالية لـ $UACI$ للصور الرمادية هي 33.4635% الاقتراب العالي من هذه النسبة يعني أن الخوارزمية توزع الفروقات بشكل عشوائي وممتاز جداً.

مساحة المفاتيح وتحليل الحساسية (Key space and Sensitivity Analysis)

يعتبر حجم مساحة المفاتيح أسلوب للتغلب على التكهنات الحسابية لفك التشفير، يجب أن يفي إجمالي مساحة مفاتيح نظام التشفير K_S ويحسب بحيث $K_S = 2^{128}$ ، اما حساسية المفتاح (Key Sensitivity) فهي حساسية المفتاح بت واحد التبديل في ناقل المفتاح السري K يجب أن ينشئ مصفوفة غير مترابطة تمامًا. من الناحية الكمية إذا تم تشفير C_K باستخدام K وتم فك تشفيره باستخدام $K + \Delta$ فإن الصورة الناتجة P_{fail} يجب أن تحقق ما يلي:

$$H(P_{fail}) \approx 8, \qquad and \quad \gamma(P_{fail}, Plain) \approx 0$$

تحليل المدرج التكراري (Histogram Analysis)

يوضح تحليل المدرج التكراري توزيع مستويات شدة البكسل داخل الصورة. يجب أن تضمن خوارزمية تشفير الصور الآمنة أن يكون المدرج التكراري للصورة المشفرة مسطحًا ديناميكيًا ومتجانسًا بشكل كبير، بحيث لا يكشف عن أي أنماط إحصائية للصورة الأصلية. وللتحقق كميًا من هذا التجانس ومنع التحليل الإحصائي للتشفير، يتم حساب اختبار Chi-Square(χ^2)بمعادلة التالية:

$$x^2 = \sum_{i=0}^{255} \frac{(O_i - E_i)^2}{E_i} \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots (6)$$

حيث O_i يمثل القيمة لمستوى اللون الرمادي i للصورة المشفرة

و E_i القيمة المثالية المتوقعة وتحسب رياضيا $E_i = \frac{M*N}{256}$ ، تعتبر الخوارزمية آمنة ضد الهجمات الإحصائية إذا كانت قيمة χ^2 المحسوبة أقل من قيمة العتبة $X^2_{0.05,255} = 293.2478$.

المقاييس الإحصائية لتقييم الخوارزميات

يعتمد الباحثون على مجموعة شاملة من المقاييس لتقييم خوارزميات تشفير الصور، ومنها معامل الارتباط (Correlation Coefficient) ويستخدم لقياس العلاقة بين الصورة الأصلية والمشفرة، ويكون هذا المقياس جيد كلما كان قريبًا من الصفر لإثبات العشوائية في التشفير. ثانيا معيار إنتروبيا Entropy وثالثا متوسط مربع الخطأ (Mean Square Error)[5].

معيار متوسط مربع الخطأ Mean Square Error (MSE)

يُستخدم متوسط مربع الخطأ (MSE) لحساب متوسط مربع الفرق بين قيم البكسل في صورة النص الأصلي وصورة النص المشفر. في تشفير الصور، يُستخدم لتقييم جودة خوارزمية تشفير الصور[17] تشير قيمة MSE المنخفضة إلى تشابه أكبر بين صورة النص الأصلي وصورة النص المشفر، بينما تشير قيمة MSE المرتفعة إلى تشابه أقل بينهما؛ وبالتالي، تدل قيمة MSE المرتفعة على جودة تشفير أعلى. يمكن حساب متوسط مربع الخطأ بين صورة النص الأصلي وصورة النص المشفر كما يلي:

$$MSE = \frac{1}{M-N} \sum_{i=1}^{M} \sum_{j=1}^{N} (p(i,j) - c(i-j))^2 \dots\dots\dots\dots\dots\dots (7)$$

حيث أن:

M, Nعدد الصفوف والأعمدة

$P(i,j)$:قيمة البيكسل في الصورة الأصلي

$C(i,j)$:قيمة البيكسل في الصورة المشفر

إذا افترضنا أن الصورتين متطابقتان، فإن P (i, j) − C (i, j) ستكون 0. وبالتالي، فإن الحد الأدنى لقيمة MSEهو 0. أما بالنسبة للحد الأقصى، فنفترض أن الصورتين مختلفتان تمامًا عن بعضهما البعض إحداهما بقيم 255 بيكسل، والأخرى بقيم 0 بيكسل؛ ويمكن حساب الحد الأقصى لقيمة MSE الممكنة كما يلي:

$$MSE = \frac{1}{M-N} \sum_{i=1}^{M} \sum_{j=1}^{N} (255-0)^2 \dots\dots\dots\dots\dots\dots\dots\dots (8)$$

$$MSE = \frac{1}{M-N} * M * \mathrm{N} * [255]^2 = 65{,}025$$

ومن هذا المعيار يتم حسب MSE (Peak Signal-to-Noise Ratio) PSNR ، والتي تُستخدم عادةً لتقييم جودة التشفير بالمعادلة التالية

$$PSNR = 10\ log_{10}\left(\frac{MAX_i^2}{MSE}\right) \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \quad (9)$$

حيث أن:

MAX_I :القيمة العظمى الممكنة للبيكسل في الصورة.

MSE :متوسط مربع الخطأ المحسوب بين الصورة الأصلية والمشفرة.

كلما ارتفع PSNR دلّ ذلك على أن الصورة المشفرة أو المضغوطة أقرب إلى الأصلية.

ويوضح هذا الجدول أهم التطبيقات النموذجية التي يتم استخدام إحدى خوارزميات التشفير فيها واهم مقياس التقييم المستخدمة للقياس مدي قوة وأمان خوارزمية التشفير.

جدول 2: أهم التطبيقات النموذجية ومقياس التقييم فيها

عائلة الخوارزميات	التطبيقات النموذجية	أهم مقاييس التقييم المستخدمة
الأنظمة الفوضوية (Chaos-Based)	• البث الفوري بالفيديو. • اتصالات الوسائط المتعددة الحية.	• الإنتروبيا (H). • معاملات الارتباط (γ). • اختبارات NIST الإحصائية.
حوسبة الحمض النووي (DNA-Computing)	• أرشفة السجلات الطبية والصور الشعاعية. • التخزين السحابي عالي الأمان.	• مساحة المفتاح (K_s). • مقاييس الهجمات التفاضلية $(NPCR/UACI)$.
نطاق التحويل والبصريات (Transform-Domain)	• صور الأقمار الصناعية. • الاتصالات العسكرية وتطبيقات الرادار.	• معامل الارتباط العكسي. • نسبة الإشارة إلى الضوضاء $(PSNR)$. • اختبارات القص والضوضاء.
الاستشعار المضغوط (Compressive Sensing)	• شبكات الاستشعار اللاسلكية (WSN). • أجهزة إنترنت الأشياء (IoT).	• جودة إعادة البناء $(Structural\ Similarity - SSIM)$. • الكفاءة الحسابية في الإرسال.
التشفير الكمومي (Quantum Encryption)	• شبكات الاتصال الحكومية فائقة السرية والسرية العسكرية المستقبلية.	• مقاييس الأمان الكمومي الإحصائية. • إنتروبيا شانون وعشوائية المفاتيح.

التوصيات والأعمال المستقبلية

أن اختيار خوارزمية معينة يعني بالضرورة التضحية بجانب آخر حيث لا توجد خوارزمية "مثالية في كل شيء"، ويمكن أن نحدد أكثر من جانب للمقارنة ونلخص كل ذلك في الآتـي:

1. معادلة السرعة مقابل الأمان الكلي:(Speed vs. Security)
   - الأنظمة الفوضوية (Chaos) تمتاز بسرعة فائقة جداً تجعلها خياراً ممتازاً للبث المباشر (مثل الكاميرات الأمنية)، لكن عيبها هو "تدهور الدقة الحسابية" داخل الكمبيوتر، مما قد يجعل السلسلة العشوائية تكرر نفسها بعد فترة طويلة.[18]

- أنظمة الحمض النووي (DNA) توفر مساحة مفتاح ضخمة جداً وأماناً فائقاً مستحيلاً الكسر بالقوة الغاشمة، ولكن عيبها هو البطء الشديد لأن محاكاة العمليات البيولوجية على معالجات السيلكون العادية تتطلب قوة معالجة عالي[19] .

2. تحمل أخطاء القنوات والاتصالات(Transmission Error Tolerance)

- الأنظمة الفوضوية وأنظمة الـ DNA تعاني من مشكلة حساسة: إذا حدث تشويش في الشبكة وضاع جزء صغير من الصورة المشفرة(Cropping Attack) ، فإن تأثير كرة الثلج (Avalanche Effect) سيتسبب في تدمير الصورة بالكامل عند فك التشفير.
- على العكس تماماً، أنظمة التشفير البصري والترددي (Transform–Domain) ممتازة هنا؛ لأن تشفير البكسلات يتم بتوزيع خصائصها على الترددات، فلو ضاع جزء من الصورة المشفرة أثناء النقل، ستُفك الصورة الأصلية بنجاح ولكن مع "غبش أو ضبابية" بسيطة بدلاً من الدمار الكامل.

3. معمارية الأجهزة محدودة الموارد(Resource Asymmetry)

في بيئات إنترنت الأشياء (IoT) والمستشعرات الطبية، تكون البطاريات والمعالجات صغيرة جداً. هنا تبرز ميزة الاستشعار المضغوط (Compressive Sensing) لأنه يقوم بالضغط والتشفير معاً في خطوة واحدة بسيطة داخل المستشعر (المرسل)، ويترك العبء الحسابي الثقيل لإعادة بناء الصورة ليدار بالكامل في السحابة الإلكترونية أو لدى المستلم(Server) .

وهنا نشير إلى الثغرات الحالية في العلم والتي تمثل "فرصاً بحثية مستقبليّة" للباحثين في هذا المجال:

- التشفير المقاوم للحوسبة الكمومية (Post–Quantum Image Cryptography) حيث أن ظهور الحواسيب الكمومية قريباً سيهدد أنظمة التشفير الحالية بالكامل (مثل التشفير البصري أو الخوارزميات غير المتناظرة) لأن خوارزميات كمومية مثل Shor's وGrover's تستطيع كسر مفاتيح التشفير التقليدية في ثوانٍ. التحدي المفتوح هو بناء خوارزميات تشفير صور تعتمد على مصفوفات الشبيكة (Lattice–based) أو المسارات الكمومية لمقاومة هذه الحواسيب.
- التشفير الخفيف والتحسين للأجهزة الطرفية (Lightweight Edge Optimization) بسبب انتشار الأجهزة الطبية الذكية المحمولة وكاميرات المراقبة الصغيرة، نحتاج إلى تشفير الصور بدقة عالية (HD) ولكن بخوارزميات "خفيفة الوزن" جداً(Lightweight Primitives) لا تستهلك بطارية الجهاز ولا تتطلب ذاكرة عشوائية كبيرة، مع الحفاظ على الحد الأدنى للأمان عالمياً وهو أن تكون مساحة المفتاح أكبر من 2^{128}.
- تحليل التشفير القائم على الذكاء الاصطناعي (Deep Learning–Driven Cryptanalysis) هذا هو التحدي الأحدث عالمياً، حيث بدأ المهاجمون في استخدام الشبكات العصبية العميقة والشبكات التوليدية التخاصمية(GANs) لمحاولة تخمين السلاسل الفوضوية والعشوائية أو كسر نظام الإرباك والانتشار عبر التعرف على الأنماط المخفية في الصورة المشفرة. التحدي هو تصميم خوارزميات تثبت رياضياً عجز الذكاء الاصطناعي عن كسرها.
- غياب معايير القياس الموحدة والمتحركة (Standardization of Benchmarks) حتى اليوم، يختبر كل باحث خوارزميته على صور كلاسيكية ثابتة عمرها عقود مثل صورة Lena أو Cameraman لكن التحدي هو غياب بيئة اختبار معيارية موحدة تختبر الصور الطبية الحديثة، الصور ثلاثية الأبعاد(3D) .

الخاتمة

قدمت هذه الورقة المسحية تصنيفاً منهجياً وشاملاً لأحدث خوارزميات تشفير الصور الرقمية، مع تحليل آليات عملها الهيكلية، ومزاياها، وقيودها المتأصلة؛ حيث تمت جدولت الفكرة الأساسية للورقة بحيث شملت المزايا والعيوب لهذه العائلات لكي يستطيع الباحث اختيار الخوارزمية المناسبة لاحتياجاته.

من خلال هذا الاستعراض نلاحظ أن أمن الصور الحديث لم يعد يقتصر على مجرد خلط المواقع في النطاق المكاني، بل اتجه بقوة نحو دمج نماذج متقدمة مثل الأنظمة الفوضوية الفائقة، وحوسبة الحمض النووي (DNA)، والاستشعار المضغوط لكسر التكرار الكثيف والارتباط العالي بين البكسلات. وبينما تظل الأنظمة الفوضوية الخيار الأمثل للتطبيقات الفورية نظراً لكفاءتها الحسابية العالية، فإن تشفير النطاق الترددي والبصري يقدم مقاومة فائقة ضد ضوضاء القنوات وهجمات القص. وفي الختام، فإن سد الفجوة بين قوة التشفير النظرية ومحدودية موارد العتاد الرقمي مع مجابهة ثغرات عصر الحوسبة الكمومية وكسر التشفير المعتمد على الذكاء الاصطناعي يمثل الخط الأمثل والركيزة الأساسية لتطوير أطر أمن الوسائط المتعددة القادمة.

قائمة المراجع

[1] A. Mehmood, A. Shafique, M. Alawida, and A. N. Khan, “Advances and vulnerabilities in modern cryptographic techniques: A comprehensive survey on cybersecurity in the domain of machine/deep learning and quantum techniques,” *IEEE access*, vol. 12, pp. 27530–27555, 2024.

[2] M. J. Dworkin *et al.*, “Advanced encryption standard (AES),” 2001.

[3] X. Zhou and X. Tang, “Research and implementation of RSA algorithm for encryption and decryption,” in Proceedings *of 2011 6th international forum on strategic technology*, 2011, pp. 1118–1121.

[4] P. Fang, H. Liu, C. Wu, and M. Liu, “A survey of image encryption algorithms based on chaotic system,” *Vis.* Comput., vol. 39, no. 5, pp. 1975–2003, 2023.

[5] K. Mahalakshmi and S. Nagarajan, “Comprehensive review and analysis of image encryption techniques,” *IEEE Access*, 2025.

[6] M. M. Hashim, M. M. Kareem, W. K. Al-Azzawi, A. A. Nahi, M. S. Taha, and A. H. Ali, “Based complex key cryptography: new secure image transmission method utilizing confusion and diffusion,” in *2022 8th International Conference on Contemporary Information Technology and Mathematics (ICCITM)*, 2022, pp. 59–65.

[7] Z. A. Ali, T. S. Atia, A. Y. Yousuf, and A. J. Khahdim, “A comprehensive review of quantum image encryption methods: design characteristics, cryptographic properties, and AI integration,” *Quantum Inf. Process.*, vol. 23, no. 10, p. 335, 2024.

[8] W. J. BUCHANAN, “Chaos-based Confusion and Diffusion of Image Pixels using Dynamic Substitution,” *Chaos*, vol. 16, p. 18.

[9] M. M. Hashim, M. M. Kareem, W. K. Al-Azzawi, A. A. Nahi, M. S. Taha, and A. H. Ali, “Based complex key cryptography: new secure image transmission method utilizing confusion and diffusion,” in *2022 8th International Conference on Contemporary Information Technology and Mathematics (ICCITM)*, 2022, pp. 59–65.

[10] A. Dhaw, K. El Hadad, and A. Elbori, “a.bib,” *AlQalam Journal of Medical and Applied Sciences*, vol. 9, pp. 73–83, 2026.

[11] M. Sandri, “Numerical calculation of Lyapunov exponents,” *Mathematica Journal*, vol. 6, no. 3, pp. 78–84, 1996.

[12] I. Yasser, M. A. Mohamed, A. S. Samra, and F. Khalifa, "A Chaotic-Based Encryption/Decryption Framework for Secure Multimedia Communications," *Entropy*, vol. 22, no. 11, 2020, doi: 10.3390/e22111253.
[13] Q. Liang and C. Zhu, "A new one-dimensional chaotic map for image encryption scheme based on random DNA coding," *Opt. Laser Technol.*, vol. 160, May 2023, doi: 10.1016/j.optlastec.2022.109033.
[14] Y. Alghamdi and A. Munir, "Image Encryption Algorithms: A Survey of Design and Evaluation Metrics," Mar. 01, 2024, *Multidisciplinary Digital Publishing Institute (MDPI)*. doi: 10.3390/jcp4010007.
[15] G. S. Nandeesh, P. A. Vijaya, and M. V Sathyanarayana, "An image encryption using bit level permutation and dependent diffusion," *Int J Comput Sci Mob Comput*, vol. 2, no. 5, pp. 145–154, 2013.
[16] Y. Wu, J. P. Noonan, S. Agaian, and others, "NPCR and UACI randomness tests for image encryption," *Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT)*, vol. 1, no. 2, pp. 31–38, 2011.
[17] A. Qayyum *et al.*, "Chaos-based confusion and diffusion of image pixels using dynamic substitution," *IEEE Access*, vol. 8, pp. 140876–140895, 2020.
[18] J. Niu and Z. Li, "Chaos-Based Fault Diagnosis: Methodologies and Practices," International Journal of Bifurcation and Chaos, vol. 35, no. 09, p. 2550112, 2025, doi: 10.1142/S0218127425501123.
[19] F. Masood et al., "A new color image encryption technique using DNA computing and Chaos-based substitution box," Soft comput., vol. 26, no. 16, pp. 7461–7477, 2022.

الشكر والتقدير

ال نعم لا

تضارب الم نعم لا

توافرالبيا نعم لا

مساهمات المؤلفين:

ت	اسم المؤلف وإيميلة رابط منصة ORCID iD	تصور أوفكرة الدراسة	جمع أو المساهمة في جمع البيانات	المساهمة في الدراسات السابقة	وضع منهجية الدراسة	إجراء التحاليل (الجانب العملى)	تحليل البيانات	تفسير ومناقشة النتائج	المواقة على النسخة النهائية
1	خالدالحداد kmelhadad@elmergib.edu.ly								
2	**سعد صوان** laabdalsmd@elmergib.edu.ly								
3									