International Science and Technology Journal
المجلة الدولية للعلوم والتقنية
Volume 37 العدد
Part 1 المجلد
المجلة الدولية للعلوم والتقنية
International Science and Technology Journal
ISTJ

http://www.doi.org/10.62341/abak1308

Received	2025/07/16	تم استلام الورقة العلمية في
Accepted	2025/08/11	تم قبول الورقة العلمية في
Published	2025/08/13	تم نشر الورقة العلمية في

تأمين الصور الرقمية باستخدام التشفير المعتمد على النظام الفوضوي وترميز الحمض النووي وإخفائها بالاعتماد على DWT–DCT–SVD

أ. أسماء عبد الله الكريك

كلية التقنية الصناعية – مصراته –ليبيا

Asma.alkraik2025@gmail.com

الملخص

يقدم البحث منهجية جديدة لتشفير الصور الرقمية الملونة وإخفائها داخل صورة غلاف بهدف تعزيز أمان نقل البيانات. تعتمد المرحلة الأولى على تشفير الصورة السرية باستخدام خوارزميات متكاملة تشمل نظامًا فوضويًا فائق الأبعاد سداسيًا لتوليد مفاتيح تشفير معقدة، بالإضافة إلى ترميز مستوحى من القاعدة التكميلية للحمض النووي (DNA) لتعزيز التعمية. وفي المرحلة الثانية، تُدمج الصورة المشفرة داخل صورة الغلاف باستخدام تقنيات دمج متعددة مثل تحويل الموجة المتقطع (DWT)، تحويل جيب التمام المتقطع (DCT)، وتحليل القيمة المفردة (SVD)، مما يضمن تضمينًا فعالًا ومستقرًا للبيانات مع مقاومة عالية لهجمات الكشف. تم تقييم جودة التشفير والإخفاء باستخدام مؤشرات معيارية منها نسبة الإشارة إلى الضوضاء (PSNR)، متوسط مربع الخطأ (MSE)،والإنتروبيا (Entropy)، مما يعكس كفاءة وأمان المنهجية المقترحة.

الكلمات المفتاحية: تحويل الموجة المتقطع(DWT) ، تحويل الجيب تمام المنفصل (DCT)، تحليل القيمة المفردة SVD) النظام الفوضوي الفائق سداسي الأبعاد، وترميز الحمض النووي.(DNA) .

International Science and Technology Journal
المجلة الدولية للعلوم والتقنية
Volume 37 العدد
Part 1 المجلد
المجلة الدولية للعلوم والتقنية
International Science and Technology Journal
ISTJ
http://www.doi.org/10.62341/abak1308

Securing Digital Images Using Chaos-Based Encryption and DNA Encoding with DWT-DCT-SVD Based Steganography

Asma Abdullah Alkraik
College of Industrial Technology – Misurata – Libya
Asma.alkraik2025@gmail.com

ABSTRACT
This study proposes a novel methodology for encrypting color digital images and embedding them within a cover image to enhance secure data transmission. The first stage focuses on encrypting the secret image using an integrated set of algorithms, including a six-dimensional hyper-chaotic system for generating complex encryption keys, alongside encoding inspired by the complementary DNA base pairs to strengthen data obfuscation. In the second stage, the encrypted image is embedded into the cover image employing multiple fusion techniques such as Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), and Singular Value Decomposition (SVD), ensuring effective and robust data hiding with high resistance to detection attacks. The encryption and embedding quality were evaluated using standard metrics including Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE), and Entropy, reflecting the efficiency and security of the proposed approach.

Keywords: Discrete Wavelet Transformation (DWT), Discrete Cosine Transformation (DCT), Singular Value Decomposition (SVD), 6-dimensional hyper chaotic system and DNA encoding.

1. المقدمة:

في عصرنا الرقمي، حيث يتم نقل وتخزين كميات هائلة من المعلومات إلكترونيًا، أصبحت قضايا سرية البيانات وسلامتها وأمنها من الأولويات الأساسية. وتُعد تقنيتا التشفير والإخفاء من أبرز الأدوات المستخدمة لتحقيق هذه الأهداف.

يُعرف التشفير (Encryption) بأنه عملية تحويل البيانات المقروءة (النص الصريح) إلى صيغة غير مفهومة (النص المشفر) باستخدام خوارزميات رياضية ومفاتيح تشفير. ويهدف إلى ضمان أنه حتى في حال اعتراض البيانات، لا يمكن فهمها دون امتلاك المفتاح

http://www.doi.org/10.62341/abak1308

الصحيح لفك التشفير. ويُستخدم التشفير على نطاق واسع في مجالات الاتصالات، والمعاملات المالية، والحوسبة السحابية [1].

أما الإخفاء (Steganography)، فهو علم وفن إخفاء المعلومات داخل وسائط رقمية أخرى مثل الصور أو الملفات الصوتية أو مقاطع الفيديو، بحيث لا تُظهر هذه الوسائط أي دليل على وجود معلومات مخفية بداخلها. وعلى عكس التشفير الذي يُخفي محتوى الرسالة، يسعى الإخفاء إلى إخفاء وجود الرسالة من الأساس. ولهذا، يُعد أداة فعّالة في البيئات التي تتطلب مستوى عالٍ من السرية وعدم الكشف [2].

وعلى الرغم من اختلاف المبادئ التي تقوم عليها كل من التقنيتين، إلا أن دمجهما معًا يمكن أن يُنتج أنظمة أكثر قوة وأمانًا. فالتشفير يُوفّر الحماية لمحتوى البيانات، بينما يُخفي الإخفاء هذه البيانات عن الأنظار. لذلك فإن هذه الدراسة تهدف إلى استكشاف منهجيات حديثة تدمج بين تقنيتي التشفير والإخفاء، بهدف تعزيز أمن البيانات وخصوصيتها في البيئات الرقمية المتقدمة.

2. التقنيات المستخدمة للتشفير في المنهجية المقترحة:

سيتم توضيح التقنيات المستخدمة في نظام التشفير المقترح والأساليب المستخدمة وأسباب اختيارها. وهذه التقنيات هي:

1.2 النظام الفوضوي (Chaos Theory) والدوال الفوضوية:

النظام الفوضوي هو نظام غير خطي يظهر سلوكًا غير منتظم حتى مع وجود معادلات حتمية تحكمه. تعتمد هذه الأنظمة على مفاهيم رياضية معقدة، ولكنها تُستخدم بشكل واسع في تطبيقات عملية مثل التشفير بسبب صعوبة التنبؤ بأنماطها.

يُستخدم النظام الفوضوي في إنشاء مفاتيح سرية في أنظمة التشفير لعدة مزايا رئيسية ترتبط بخصائص الأنظمة الفوضوية. هذه الخصائص تجعلها مفيدة لتوليد مفاتيح سرية آمنة وصعبة التنبؤ بها. ومن هذه المزايا الحساسية العالية للشروط الابتدائية والعشوائية الظاهرة وصعوبة الاستنتاج العكسي وقابلية التكرار مع الشروط الصحيحة وكفاءة الأداء وأمان أعلى ضد الهجمات التقليدية [3].

أ. معادلات لورينز (Lorenz Equations):

معادلات لورينز وهي من الأنظمة الفوضوية المستمرة وهي عبارة عن نظام غير خطي يعرض سلوكًا ديناميكيًا معقدًا، تتميز معادلات لورينز ببنيتها الرياضية البسيطة، مما

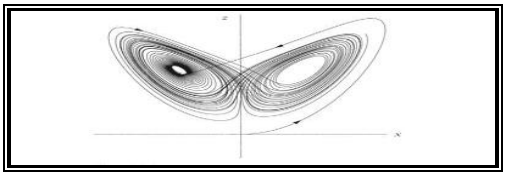
http://www.doi.org/10.62341/abak1308

يجعلها نموذجًا شائعًا لدراسة ظهور الفوضى في الأنظمة غير الخطية. وهذه المعادلات تُظهر سلوكًا فوضويًا وتستخدم في نمذجة تدفق السوائل والأرصاد الجوية. ومعادلاته:

$$\frac{dx}{dt} = \sigma(y - x) \quad (1)$$
$$\frac{dy}{dt} = rx - y - xz \quad (2)$$
$$\frac{dz}{dt} = xy - bz \quad (3)$$

حيث إن x, y, z هي متغيرات الحالة أو القيم الابتدائية (Initial Value)، و σ, r, b هي معاملات تحكم أو معاملات النظام (System Parameters).

تمتلك معادلات لورينز جاذبًا فوضويًا (Chaotic Attractor) يشبه شكل الفراشة كما في الشكل (1)، وتُعرف معادلات لورينز بأنها حساسة جدًا للظروف الأولية [3].



الشكل.1. نمط الفراشة الذي تنشئه معادلات لورينز

وقد تم تطوير هذه معادلات لورينز ذو الثلاث أبعاد لاحقا الى نماذج ذات ابعاد أعلى مثل (DLM5) و(DLM6) لتحليل تأثيرات أكثر تفصيلا في النماذج المناخية.

ب. النظام الفوضوي الفائق Six dimensional hyper Chaotic system:

النظام الفوضوي الفائق هو تطوير لأنظمة Lorenz التقليدية، حيث يتم توسيع عدد الأبعاد لزيادة تعقيد النظام، فهذا التعقيد يوفر مستويات أعلى من الأمان عند استخدامه في أنظمة التشفير. لتكون معادلاته كالتالي:

$$\frac{dx}{dt} = \sigma(y - x) \quad (4)$$
$$\frac{dy}{dt} = rx + x_1 z - y - xz - 2x_1 z_1 \quad (5)$$
$$\frac{dz}{dt} = xy - xy_1 - x_1 y - bz \quad (6)$$
$$\frac{dx_1}{dt} = \frac{\sigma}{d_o} y_1 - d_o \sigma x_1 \quad (7)$$
$$\frac{dy_1}{dt} = rx_1 + xz - d_o y_1 - 2xz_1 \quad (8)$$
$$\frac{dz_1}{dt} = 2xy_1 + 2x_1 y - 4bz_1 \quad (9)$$

http://www.doi.org/10.62341/abak1308

حيث x, y, z و x1, y1, z1 تمثل القيم الابتدائية للنظام، كما أن زيادة أبعاد نموذج لورينز يمكن أن يحسن التنبؤات، ويساعد في تحسين دقة التوقعات، لكن يكون أكثر تعقيدًا رياضيا ويتطلب حسابات مكثفة [4].

2.2 القاعدة التكميلية لشفرة الحمض النووي (DNA):

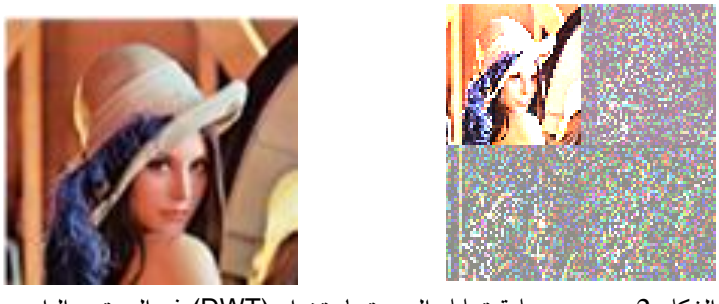
القاعدة التكميلية لشفرة (DNA) هي تقنية تستخدم خصائص الحمض النووي في عمليات التشفير لحماية البيانات، تستند هذه التقنية الى تمثيل البيانات الرقمية باستخدام قواعد الحمض النووي البيولوجية، حيث تقوم بتحويل البيانات الرقمية الى تسلسلات من الاحرف التي تمثل النوكليوتيدات الأربع في الحمض النووي وهي (A: أدينين، T: ثايمين، C: سيتوزين، G: غوانين) وتحويلها إلى سلسلة من القيم الثنائية مثل: A ; 01→T →00 G→11 ; C→10 ;، وأخيرا يتم تطبيق عمليات حسابية مثل الإضافة أو الطرح أو XOR وكذلك من الممكن التبديل بين C↔T ; A↔G مما يجعل التشفير أكثر تعقيدًا. يتم استخدام القاعدة التكميلية لشفرة DNA بسبب خصائصه وهي أمان عالي ومساحة تخزين ضخم ومقاومة للهجمات التقليدية ودمج مع الأنظمة الفوضوية [5].

3. التقنيات المستخدمة لإخفاء الصورة في المنهجية المقترحة:

سيتم توضيح التقنيات المستخدمة لإخفاء الصورة، وهذه التقنيات هي:

1.3 تحويل المويجة المتقطع Discrete Wavelet Transformation (DWT):

يُعد تحويل المويجات المتقطع (DWT) أحد الأساليب الرياضية المستخدمة لتحليل الصور الرقمية إلى نطاقات فرعية ذات مستويات مختلفة من التردد المكاني. وتكمن فكرته في تفكيك الصورة الأصلية إلى مجموعة من النطاقات تمثل مكونات التردد المنخفض والمتوسط والعالي، مما يتيح تمثيلًا متعدد الدقة للصورة كما موضح في الشكل (2)، حيث يتم تطبيق مرشحات التمرير المنخفض والمرتفع أفقياً وعمودياً على الصورة [6] [7].

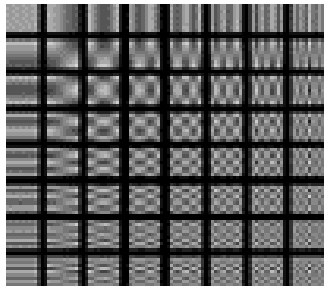


الشكل.2. يوضح عملية تحليل الصورة باستخدام (DWT) ذو المستوى الواحد

http://www.doi.org/10.62341/abak1308

2.3 تحويل الجيب تمام المتقطع Discrete Cosine Transformation (DCT):

يُعد تحويل الجيب تمام المتقطع (DCT) ثنائي الأبعاد من التحويلات الرياضية الشائعة في معالجة الصور، حيث يُستخدم لتحليل الصورة إلى مجموعة من المركبات الترددية. يقوم (DCT) بتمثيل الصورة كمجموع من الدوال الجيبية التمامية (Cosine Functions) ذات سعات وترددات مختلفة، مما يساعد في فصل مكونات الصورة حسب أهميتها الطيفية. يوضح الشكل أدناه مصفوفة (DCT Blocks) بحجم (8×8) [6] [8].



الشكل.3. تحويل الجيب تمام المتقطع (DCT Blocks) بحجم (8×8)

3.3 تحليل القيمة المفردة Singular Value Decomposition (SVD):

يُعد تحليل القيمة المفردة (SVD) من الأدوات المهمة في الجبر الخطي، وهو تقنية فعّالة في التحليل والتقريب، حيث يُستخدم لتحليل أي مصفوفة إلى مكونات أبسط قابلة للعكس. ويقوم هذا التحليل بتفكيك المصفوفة المستطيلة A إلى الشكل التالي:

$$A_{M*N} = U_{M*M} S_{M*N} V_{N*N} \quad (10)$$

حيث U و V مصفوفتان متعامدتان و S مصفوفة قطرية [9] [10].

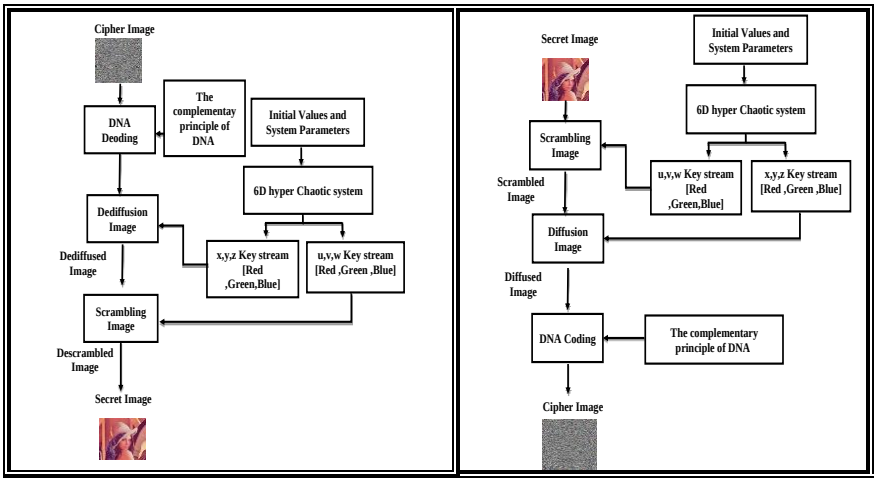
الخوارزميات المقترحة:

بما أن المنهجية المقترحة تعتمد على مرحلتين: مرحلة التشفير ومرحلة الاخفاء والاستخراج فسيتم توضيح الخوارزميات المستخدمة في كل مرحلة على حدة، وذلك كالتالي:

1.4 مرحلة التشفير وفك التشفير للمنهجية المقترحة:

يعتمد نظام التشفير المقترح في هذه الدراسة على دمج الأنظمة الفوضوية مع تشفير الحمض النووي لإنشاء نظام تشفير أكثر تعقيدًا وأمانًا، ومراحل التشفير في النظام المقترح يتم على عدة مراحل كما موضح في الشكل (4) الذي يوضح المراحل المتبعة للحصول على صورة مشفرة (Cipher Image). كما يوضح المراحل المتبعة لفك التشفير للصورة المشفرة وهي تعمل بصورة معاكسة لمرحلة التشفير.

http://www.doi.org/10.62341/abak1308



(أ) مرحلة التشفير (ب) مرحلة فك التشفير

الشكل.4. مرحلة التشفير وفك التشفير للنظام المقترح

وكما موضح في الشكل (4) فإن النظام المقترح مكون من أربع خوارزميات رئيسية للتشفير، وسيتم توضيح كل خوارزمية على حدة للحصول في النهاية على صورة مشفرة (علما بأن خوارزميات فك التشفير تعمل بصورة معاكسة لها)، وهذه الخوارزميات كالتالي:

أ. **خوارزمية توليد المفاتيح (Key Generation Algorithm):**

الإدخال:

- حجم الصورة السرية (M×N) ومعاملات النظام (a,b,c,d,h,k_1,k_2).
- القيم الأولية للنظام الفوضوي ($x_{10},x_{20},x_{30},x_{40},x_{50},x_{60}$).

الإخراج:

- سلسلة مفاتيح بحجم M×N×3 خاصة ببعثرة بكسلات الصورة (key stream scrambling).
- سلسلة مفاتيح بحجم M×N×3 خاصة بخوارزمية انتشار الصورة (key stream diffusion).

خطوات توليد المفاتيح keys stream:

1. حساب المعادلات الستة التالية الخاصة 6_D hyper chaotic system:

$$x_1 = a(x_{20} - x_{10}) + x_{40} \quad (11)$$

$$x_2 = c.x_{10} - x_{10}.x_{30} + x_{40} + x_{20} \quad (12)$$

$$x_3 = x_{10}.x_{20} - b.x_{30} \quad (13)$$

http://www.doi.org/10.62341/abak1308

$$x_4 = d.x_{40} - x_{10}.x_{30} \quad (14)$$
$$x_5 = -h.x_{20} + x_{60} \quad (15)$$
$$x_6 = -k_1.x_1 + k_2.x_2 \quad (16)$$

2. تخصيص القيم الناتجة إلى مصفوفات سلسلة المفاتيح الخاصة بالبعثرة والانتشار.
3. تغيير القيم الأولية لمعادلات نظام لورينز بالقيم الجديدة الناتجة من المعادلات السابقة:

$x_{10} = x_1,\ x_{20} = x_2, x_{30} = x_3,\ x_{40} = x_4, x_{50} = x_5,\ x_{60} = x_6$

4. تكرار الخطوات السابقة n=M*N من المرات للحصول على سلاسل المفاتيح الخاصة بالبعثرة والانتشار كاملة.

ب. خوارزمية بعثرة بكسلات الصورة (Scrambling Algorithm):

<u>الإدخال:</u>

- صورة ملونة (Secret Image) بحجم (M×N).
- سلسلة المفاتيح الخاصة بالبعثرة (key stream scrambling).

<u>الإخراج:</u> صورة مبعثرة (Scrambling image).

<u>خطوات بعثرة بكسلات الصورة:</u>

1. استبدال بكسلات الصورة وذلك بعد جعلها أحادية البعد لثلاث القنوات اللونية للصورة كالتالي:

Secret Image(1:n) ↔ Secret Image(Key stream scrambling(1:n))

2. تتم هذه العملية للثلاث القنوات اللونية للصورة (Red, Green and Blue).
3. إعادة تخزين بكسلات الصورة المبعثرة في مصفوفة ثلاثية الابعاد "القنوات اللونية":

Scrambled image(:,:,:)= Secret Image(1:n) (Red, Green and Blue)

4. لينتج لنا صورة مبعثرة البكسلات (Scrambled image).

لنفترض أن لدينا مصفوفة ثنائية الابعاد بحجم 2*2 كالتالي:

$$\begin{bmatrix} 1 & 212 \\ 111 & 133 \end{bmatrix}$$

يتم تحويلها الى مصفوفة أحادية البعد:

[1 212 111 133]

http://www.doi.org/10.62341/abak1308

وكانت لدينا سلسلة المفاتيح الخاصة بالبعثرة بحجم 4 مفاتيح:

$$[3 \quad 1 \quad 4 \quad 2]$$

وتم تطبيق خوارزمية البعثرة على المصفوفة الأحادية، سنتحصل على مصفوفة

مبعثرة كالتالي: $[111 \quad 1 \quad 133 \quad 212]$

ويتم تحويلها الى مصفوفة ثنائية لتصبح بالصورة التالية:

$$\begin{bmatrix} 212 & 133 \\ 1 & 111 \end{bmatrix}$$

ت. خوارزمية الانتشار (Diffused Algorithm):

الإدخال:

- صورة ملونة (Scrambled image) حجم M×N (مبعثرة).
- سلسلة المفاتيح الخاصة بالانتشار (key stream diffusion).

الإخراج: صورة مشفرة (diffusion image) باستخدام XOR.

خطوات التشفير بالانتشار:

1. جعل قيم سلسلة المفاتيح بحجم 8 بت وتأخذ القيم من 0 الى 255.
2. استخدام الدالة XOR (تتم هذه العملية للثلاث القنوات اللونية للصورة)، كالتالي:

Scrambled image(1:n) ↔ (Scrambled image(1:n) XOR key stream diffusion (1:n))

3. إعادة تخزين بكسلات الصورة المبعثرة في مصفوفة ثلاثية الابعاد "ثلاث القنوات اللونية للصورة":

diffusion image (:,:,:)= Secret Image(1:n)(Red, Green and Blue)

4. لينتج لنا صورة معاد انتشار بكسلاتها (diffusion image).

ث. خوارزمية التشفير باستخدام القاعدة التكميلية لشفرة الحمض النووي (DNA):

تعتمد هذه الخوارزمية على المبدأ التكميلي لقاعدة الحمض النووي (DNA)، والذي يستند على ربط القواعد النووية [A C G T] معًا بواسطة الرابطة الهيدروجينية A↔T , G↔C.

والخوارزمية تكون كالتالي:

1. إنشاء مصفوفة أحادية بحجم 1*4 لبناء القاعدة التكميلية لDNA كالتالي:

http://www.doi.org/10.62341/abak1308

$$[65 \quad 67 \quad 71 \quad 84]$$

حيث أنها تمثل القواعد النووية لشفرة DNA $[A \quad C \quad G \quad T]$

2. يتم انشاء مصفوفة خاصة بسلسلة تشفير DNA بحجم M,N*4.
3. يتم تحويل كل بكسل في الصورة المراد تشفيرها الى قيمة ثنائية 8 بت ويتم أخذ كل 2 بت مع بعض من أجل تطبيق مبدأ DNA التكميلي:
4.

00	01	10	11
65	67	71	84

واستبدالها كالتالي:

$$00 \leftrightarrow 11 \qquad 01 \leftrightarrow 10$$

5. سينتج عن كل بكسل 4 قيم مخزنة في 4 خلايا هذه القيم تكون أحد القيم 84، 71، 67، 65.
6. لكل قيمة من القيم الناتجة لها موقع في مصفوفة القاعدة التكميلية DNA اما أن يكون 1، 2، 3، 4.
7. يتم أخذ كل قيمة من القيم الأربعة بالترتيب وتحديد موقعها في مصفوفة القاعدة التكميلية DNA وتحويل هذا الموقع ليكون من 0 الى 3 الذي يعتمد على قاعدة DNA التكميلية 11 10 01 00.
8. يتكون لدينا بكسل بحجم 8 بت ليكون هذا هو البكسل المشفر.
9. يتم تشفير كل بعد لوني blue, green, red بشكل منفصل بنفس الخوارزمية ليتكون لدينا صورة مشفرة باستخدام تشفير DNA، وهذه هي الصورة المشفرة (Cypher Image) للصورة السرية (Secret Image).

2.4 مرحلة إخفاء واستخراج الصورة المشفرة:

أ. **خوارزمية إخفاء الصورة المشفرة:**

الإدخال:

- صورة الغطاء (Cover Image) ،ومعامل التضمين "a".
- الصورة السرية المشفرة (Cypher Image) الناتجة من المرحلة السابقة.

الإخراج: الصورة الحاملة (Stego Image).

http://www.doi.org/10.62341/abak1308

خطوات إخفاء الصورة المشفرة:

1. تطبيق تحويل المويجات (DWT) من المستوى الأول على صورة الغلاف، ويتم فصل الصورة إلى ثلاث قنوات لونية (R–G–B) لمعالجة كل قناة على حدة.
2. تطبيق تحويل (DCT Blocks) على نطاق LL (الجزء منخفض التردد). واستخراج معاملات DC لكل قناة لونية لتكون بحجم الصورة السرية المشفرة المراد إخفائها.
3. تطبيق التحليل بالقيم المفردة (SVD) للحصول على [U1 S1 V1] لكل قناة لونية.
4. فصل الصورة السرية المشفرة إلى ثلاث القنوات اللونية للحصول على W_{sc} لكل قناة.
5. تضمين الصورة السرية المشفرة في كل قناة لونية باستخدام المعادلات:
6.

$$X = S1 + \alpha Wsc \quad (17)$$

$$SVD(X) = [u\ s_{new} v] \quad (18)$$

7. تعديل معاملات S1 في كل قناة باستبدالها بـ S_{new} باستخدام المعادلة:

$$inverse\ SVD(U1\ s_{new} V1) \quad (19)$$

8. تغيير كل قيمة DC في DCT Blocks بقيمة DC المضمنة الجديدة.
9. تطبيق DCT العكسي على كل قناة (R–G–B) ودمج القنوات الثلاث معًا.
10. تطبيق DWT العكسي لإعادة بناء الصورة والحصول على الصورة الحاملة (Stego Image)، والتي تحتوي على الصورة السرية.

ب. خوارزمية استخراج الصورة المشفرة:

الإدخال:

- الصورة الحاملة (Stego Image).
- ومعامل التضمين "a" و (S1, u, v) المستخدمة في مرحلة الاخفاء.

الإخراج: الصورة السرية المشفرة المضمنة.

خطوات استخراج الصورة المشفرة:

1. تطبيق نفس خطوات (3,2,1) الخوارزمية السابقة على الصورة الحاملة، وبعد تطبيق SVD يتم الحصول على $[U_{EX}\ S_{EX}\ V_{Ex}]$ لكل قناة لونية.
2. لاستخراج الصورة السرية المشفرة المضمنة يتم تطبيق لكل قناة لونية المعادلات التالية:

$$X^{*} = \text{inverse SVD } [u\ S_{EX}\ v] \quad (20)$$

http://www.doi.org/10.62341/abak1308

$$Wex = \frac{X^* - S1}{\alpha} \quad (21)$$

3. دمج القنوات اللونية الثلاث للحصول على الصورة السرية المشفرة المضمنة.

5. مقاييس الأداء:

تم اختبار أداء النظام المقترح باستخدام مقاييس أداء مختلفة، ومن هذه المقاييس:

1.5 الرسم البياني (Histogram):

هو نوع من الرسوم البيانية يستخدم لتحليل توزيع قيم البكسل في الصورة مما يساعد في فهم الإضاءة والتباين ومدى انتشار الألوان داخل الصور. وتم استخدامه لتوضيح شكل توزيع البكسلات قبل التشفير وبعده.

2.5 الارتباط (Correlation):

هو مقياس احصائي يحدد العلاقة بين متغيرين، حيث يكون الارتباط في الصورة الاصلية قوي بين البكسلات المتجاورة وبعد التشفير يصبح الارتباط أقل في الصورة المشفرة.

3.5 مدى عشوائية الصور (Entropy):

وهي تقيس مدى عشوائية الصورة المشفرة، وتكون معادلتها كالتالي:

$$entropy = -\sum_{i=0}^{255} P(i).\log_2 P(i) \quad (22)$$

حيث أن P(i) هي احتمال تكرار البكسل بالقيمة i.

4.5 نسبة الإشارة إلى الضوضاء العظمى (PSNR):

تم استخدام (PSNR) كأداة قياس لنظام التشفير المقترح والتي تم استخدامها لقياس الفرق بين الصورة السرية والصورة المشفرة لها ، وتكون معادلتها كالتالي:

$$PSNR = 10.\log_{10}(\frac{255^2}{MSE}) \quad (23)$$

حيث أن MSE هو متوسط الخطأ التربيعي بين الصور.

وكذلك تم استخدامها كأداة قياس لنظام الاخفاء لقياس الفرق بين صورة الغلاف (Cover Image) والصورة المحتوية على الصورة المشفرة (Stego Image).

http://www.doi.org/10.62341/abak1308

5.5 متوسط الخطأ التربيعي (MSE):

تم استخدام (MSE) لقياس الفرق بين الصورة السرية والصورة المشفرة لها بناءً على متوسط الأخطاء التربيعية بين البكسلات، وتكون معادلتها كالتالي:

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}[I(i,j) - K(i,j)]^2 \quad (24)$$

وكذلك تم استخدامه لقياس مدى التشابه بين الصورة السرية (Secret Image) "قبل وبعد التشفير" والصورة السرية المسترجعة "مشفرة وبعد فك التشفير".

6.5 مؤشر التشابه البنيوي (SSIM):

لقياس مدى التشابه بين الصورة السرية والصورة المشفرة لها، وتكون معادلته كالتالي:

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \quad (25)$$

حيث:

μ_x, μ_y: المتوسط الحسابي لكل صورة.

σ_x^2, σ_y^2: التباين في كل صورة.

σ_{xy}: التباين المشترك.

C_1, C_2: ثوابت صغيرة لتجنب القسمة على صفر.

7.5 معدل تغيير البكسلات (NPCR):

الذي يقيس النسبة المئوية للبكسلات التي تغيرت بعد التشفير مقارنة بالصورة الاصلية لها "الصورة السرية (Secret Image)"، وتكون معادلته كالتالي:

$$NPCR = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j)}{M \times N} \times 100\% \quad (26)$$

حيث:

$$D(i,j) = \begin{cases} 1, & if\ I(i,j) \neq K(i,j) \\ 0, & otherwise \end{cases} \quad (27)$$

$I(i,j)$: قيمة البكسل في الصورة المشفرة.

$K(i,j)$: قيمة البكسل في الصورة الاصلية.

$M \times N$: عدد البكسلات الكلي.

http://www.doi.org/10.62341/abak1308

8.5 شدة التغيير الموحدة (UACI):

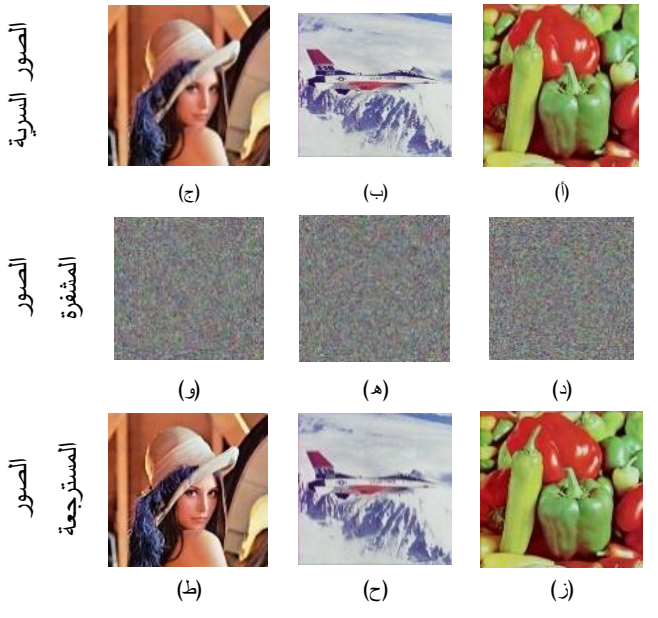
لقياس متوسط الفرق في شدة اللون بين الصورة السرية (Secret Image) والصورة المشفرة لها (Cipher Image)، وتكون معادلتها كالتالي:

$$UACI = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|I(i,j)-K(i,j)|}{255} \times 100\% \quad (28)$$

6. الجانب العملي ودراسة النتائج:

في هذا الجزء سيتم توضيح النتائج المتحصل عليها من خلال التطبيق العملي للخوارزميات المقترحة لنظام التشفير والاخفاء للصور الرقمية الملونة والذي تم برمجته من خلال برنامج MATLAB، ونظراً لأن منهجية البحث مكونة من مرحلتين مرحلة التشفير ومرحلة الاخفاء والاستخراج لذلك سيتم دراسة النتائج كلا على حدة.

دراسة المرحلة الأولى (مرحلة التشفير وفك التشفير): تم استخدام عدة صور كصورة سرية بحجم (256*256) بكسل وصورة الغلاف (Lena) بحجم (512*512) وكانت نتائج تشفيرها وفك التشفير عنها، كما هو موضح في الشكل (6).



الشكل.5. يوضح عدة صور مستخدمة كصورة سرية وناتج تشفيرها والصورة المسترجعة بعد فك التشفير على الترتيب

http://www.doi.org/10.62341/abak1308

والجدول (1) يوضح النتائج المتحصل لقيمة (Entropy) للصورة المشفرة لمجموعة من الصور بحجم (512*512) وصورة الغلاف (Lena) بحجم (1024*1024)، ومقارنتها بمراجع أخرى استخدمت صورة (Lena: 512*512).

الجدول.1. يوضح النتائج المتحصل لقيمة الانتروبيا (Entropy)

الصورة السرية (Secret Image)	الانتروبيا (Entropy) للصورة المشفرة لها		
	Blue	Green	Red
Lena	7.9993	7.9993	7.9992
Airplane	7.9993	7.9992	7.9993
Pepper	7.9992	7.9994	7.9992
[11] "lena image"	7.9993	7.9994	7.9993
[12] "lena image"	7.9987	7.9985	7.9987

كما هو موضح في الجدول (1)، فإن قيم الانتروبيا المحسوبة للنظام المقترح تقاربت بشكل كبير من القيمة المثالية وهي (8.0)، مما يشير إلى أن التوزيع الاحتمالي للبكسلات في الصورة المشفّرة قريب جداً من التوزيع العشوائي المثالي، وهو ما يعتبر مؤشراً على قوة النظام في مقاومة التحليل الإحصائي، وبمقارنته مع مراجع أخرى فالقيم المتحصل عليها أعلى من أحد المراجع وقريبة من المرجع الأخر.

الجدول.2. يوضح النتائج المتحصل لبعض مقاييس الأداء مابين الصورة الاصلية والصورة المشفرة

القيم المثالية والصورة السرية	PSNR(dB)	MSE	SSIM	NPCR	UACI
	أقل من 7db	كبيرة جدا	قريبة من 0	99.9-99.6	33.5-32.5
Lena	7.8900	e+041.0570	0.0089	99.61	32.9152
Airplane	7.9908	1.0328e+04	0.0093	99.6091	32.5395
Pepper	8.0949	e+041.0083	0.0073	99.6014	32.1858

كما هو موضح في الجدول (2)، فإن النظام المقترح أظهر أداءً ممتازًا في المعايير الأمنية والتقنية لتشفير الصور حيث يوضح حساسية عالية للتغييرات (NPCR) و(UACI)، وفقدان شبه كامل للبنية الأصلية (SSIM) منخفض جدًا. واختلاف كبير عن الأصل (MSE)عالي و (PSNR) منخفض.

http://www.doi.org/10.62341/abak1308

حيث تُظهر النتائج أن النظام قادر على مقاومة الهجمات التفاضلية، والهجمات المعتمدة على التشابه البنيوي، كما أن الصور المشفرة تُظهر تشويشًا كبيرًا يمنع فهم محتواها، مما يجعل النظام المقترح خيارًا قويًا لتطبيقات تشفير الصور عالية الأمان.

وفي الجدول (3) سيتم مقارنة النتائج المتحصل عليها من النظام المقترح مع مراجع أخرى لصور مختلفة لاستخدامها كصورة سرية بحجم 256.

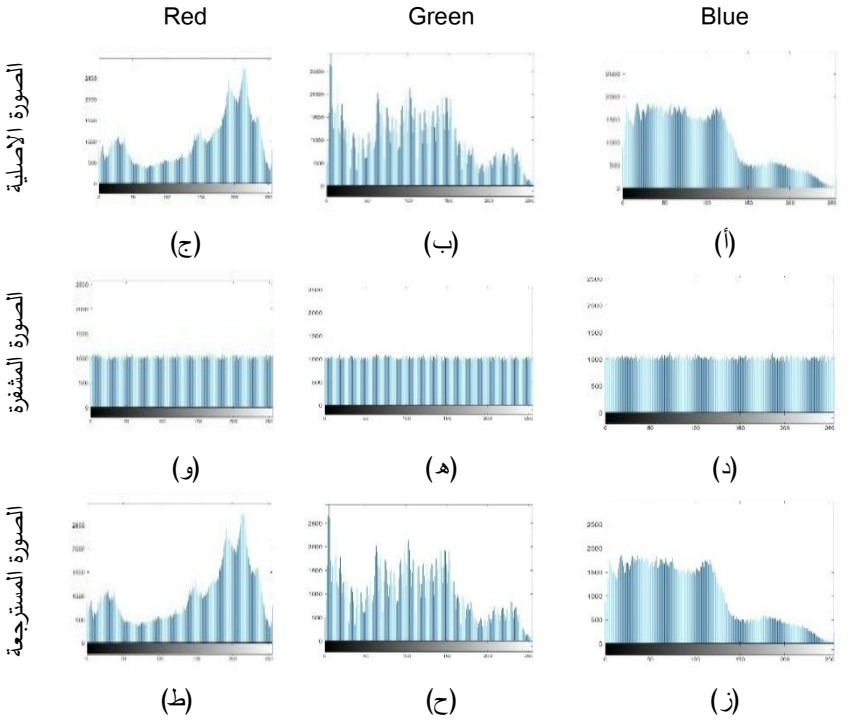
الجدول.3. يوضح مقارنة النتائج المتحصل عليها من النظام المقترح مع تقنيات أخرى

UACI(%)	NPCR(%)	Entropy	القيم المثلى	المراجع	الصورة السرية (Secret Image)
33.5–32.5	99.9–99.6	8			
32.4364	99.5906	7.9972	النظام المقترح		Airplane
32.67	99.61	7.9993	[13]		
33.4561	99.6082	7.9971	[14]		
32.93	99.66	7.9971	[15]		
32.1578	99.6104	7.9970	النظام المقترح		Pepper
32.35	99.61	7.9993	[13]		
33.4539	99.6048	7.99708	[14]		
33.17	99.61	7.9972	[15]		

أظهرت النتائج أن نظام التشفير المقترح يحقق أداءً تنافسيًا مقارنةً بالمراجع [13،8،6]. حيث بلغت قيمة (NPCR) للصورة Airplane حوالي (99.5906%)، وهي قريبة جدًا من أعلى القيم المسجلة، في حين بلغت قيمة (UACI) حوالي (32.4364%)، مما يشير إلى درجة تغير جيدة بين الصورة الأصلية والمشفرة. أما الانتروبيا فقد وصلت إلى (7.9972db)، وهي قيمة تقارب الحد الأقصى المثالي (8)، مما يدل على قوة العشوائية في الناتج المشفر. وبناءً على هذه النتائج، يمكن اعتبار النظام المقترح فعالًا وآمنًا بدرجة عالية. وفي نظامنا المقترح تم تعزيز درجة الأمان بإخفاء الصورة السرية وذلك بعد أن يتم تشفيرها باستخدام نظام التشفير المقترح مما يعطي ميزة أخرى عن المراجع السابقة.

والشكل (6) يوضح نتائج (Histogram) المتحصل عليها لصورة السرية(Lena) الملونة بحجم (512*512) قبل التشفير والصورة المشفرة وبعد فك التشفير عنها.

http://www.doi.org/10.62341/abak1308

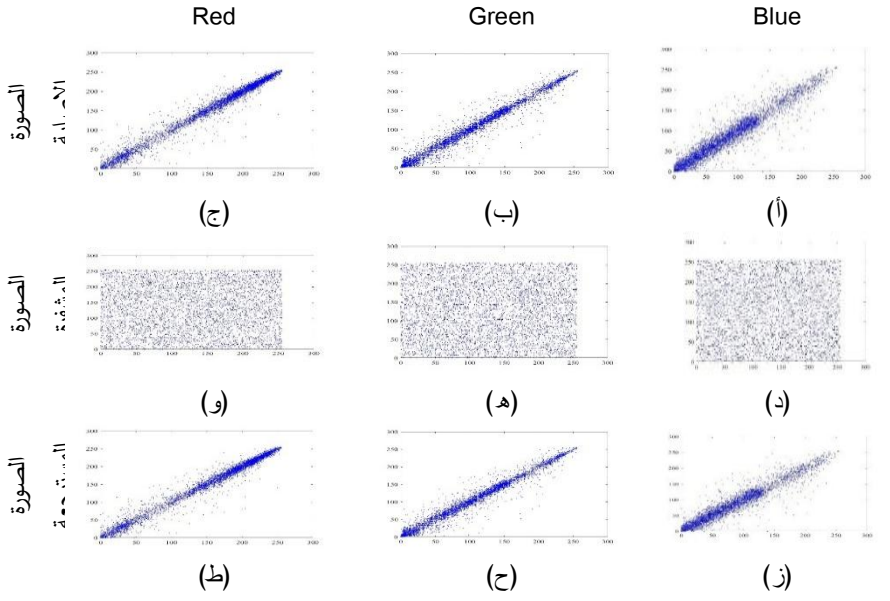


الشكل.6. يوضح نتائج (Histogram) للصور قبل التشفير والصورة المشفرة وبعد فك التشفير

نلاحظ من الشكل (6) أن (histogram) بالنسبة للصورة السرية الاصلية يُظهر مدى تكرار ظهور قيم الألوان المختلفة في الصورة بحيث تميل لأن تكون مركزة في مناطق معينة على حسب الصورة والألوان المستخدمة فيها مما يدل على وجود مناطق واضحة التدرج، أما نتائج (histogram) للصورة المشفرة أصبحت موزعة بشكل متساوٍ تقريبًا ولم تكن هناك قمم واضحة أو تركز لدرجات معينة وهذا يعني أن الاحتمالات متساوية لكل قيمة لونية، وهو ما يدل على أن الصورة فقدت معلوماتها الاصلية.

والشكل (7) يوضح نتائج الارتباط المتحصل عليها للصورة السرية(Lena) الملونة بحجم (512*512) قبل التشفير والصورة المشفرة وبعد فك التشفير عنها.

http://www.doi.org/10.62341/abak1308



الشكل.7. يوضح نتائج الارتباط (Correlation)

من الشكل (7) نلاحظ أن الارتباط بالنسبة للصورة السرية الاصلية فإنه هناك ارتباط خطي واضح بين قيم البكسلات مما يشير الى وجود ترابط كبير بين البكسلات المتجاورة وهو مؤشر على التجانس في الصورة. أما نتائج الارتباط للصورة المشفرة أصبحت عشوائية بالكامل في الصورة المشفرة، وهذا يدل على أنه تم تقليل الارتباط بين البكسلات المتجاورة وهو أحد الأهداف الأساسية لتشفير الصور.

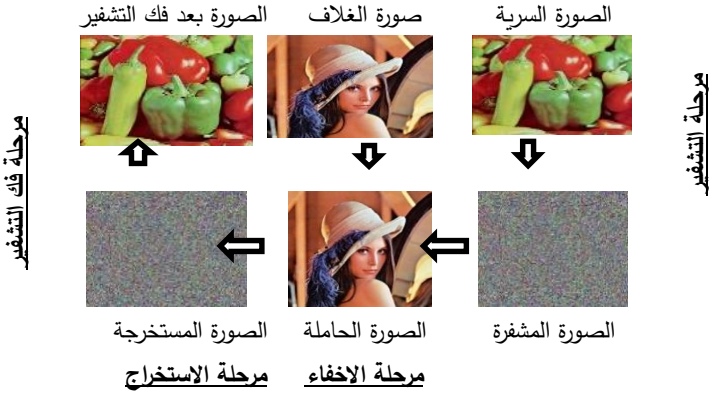
نأتي الآن لاختبار حساسية النظام وهو من الاختبارات الأساسية لتقييم قوة وأمان نظام التشفير، ويتم ذلك بالقيام بتغيير أحد القيم الأولية أو معاملات النظام الفوضوي عند القيام باسترجاع الصورة المشفرة، فمثلًا اذا قمنا بتشفير صورة (Lena) باستخدام النظام القائم بالمعامل الاولي a=10 وعند استرجاع الصورة تم تغيير نسبة بسيطة في هذه القيمة لتصبح a=10.0001، فإن ناتج فك التشفير للصورة المشفرة يكون كما فالشكل (8).

الشكل.8. يوضح ناتج فك التشفير للصورة المشفرة

http://www.doi.org/10.62341/abak1308

في الشكل (8) يتضح أنه لم يتم استرداد الصورة الاصلية بسبب تغيير طفيف في أحد معاملات النظام الفوضوي وهذا يدل على ان النظام ذو درجة حساسية عالية للتغيرات البسيطة لبعض القيم الأولية ومعاملات النظام الفوضوي.

دراسة نتائج المرحلة الثانية (مرحلة الإخفاء والاستخراج): هنا سيتم إخفاء صورة مشفرة (Pepper) بحجم (256*256) ضمن صورة الغلاف (Lena) بحجم (512*512)، وسيتم إخفاء الصورة المشفرة بمعامل تضمين (a=0.0001)، كما موضحة في الشكل:



الشكل.9. يوضح المراحل التي يمر بها النظام المقترح

ونتائج خوارزمية الإخفاء لمقاييس أداء مختلفة بين صورة الغلاف والصورة المحملة مع تغيير قيمة معامل التضمين (a) هي كما موضحة في الجدول التالي لصور مختلفة للغلاف بحجم (512*512):

الجدول.4. يوضح نتائج خوارزمية الإخفاء لأدوات قياس مختلفة مع تغيير قيمة معامل الاخفاء

صورة الغلاف (Cover Image)	PSNR (db) (المثالي ≤ 50 dB)			MSE (المثالي ≥1)		
معامل التضمين (a)	0.1	0.01	0.001	0.1	0.01	0.001
Lena	45.262852	98.056516	Inf	1.935509	0.000010	0
Airplane	43.439077	92.035916	Inf	2.945592	0.000041	0
Pepper	44.366188	87.742431	Inf	2.379368	0.000109	0

هنا من الممكن أن نستنتج أن فعالية النظام تعتمد بشكل كبير على عامل الإخفاء (a)، فعند اختيار قيم صغيرة لـ (a)، يكون النظام قادرًا على إخفاء الصور بكفاءة مع الحفاظ على جودة الصورة المستخرجة. وعند زيادة (a) يزداد التشوه إلى درجة تؤدي إلى تدهور الجودة. وقيم (MSE) الصغيرة و (PSNR) العالية تعكس كفاءة النظام.

http://www.doi.org/10.62341/abak1308

والجدول (5) يوضح النتائج المتحصل لمقاييس الأداء (MSE, SSIM) ما بين الصورة السرية الاصلية والصورة السرية المسترجعة من فك التشفير بعد المرور بمرحلة الاخفاء وكذلك مقارنة الصورة المشفرة لها (Cypher Image) "قبل مرحلة الاخفاء" مع الصورة المسترجعة "صورة مشفرة" من مرحلة الاخفاء للنظام المقترح.

الجدول.5. يوضح النتائج المتحصل لمقاييس الأداء (MSE, SSIM)

صورة الغلاف (Cover Image)	الصور غير مشفرة		الصور مشفرة	
	MSE (≈0)	SSIM (≈1)	MSE (≈ 0)	SSIM (≈ 1)
Lena	0	1	0	1
Airplane	0	1	0	1
Pepper	0	1	0	1

النظام المقترح يحقق جودة مثالية حيث أن الصورة المستخرجة مطابقة تمامًا للصورة الأصلية (بغض النظر عن كونها مشفرة أو غير مشفرة). هذا يعكس كفاءة عالية في تصميم النظام. والقيم (MSE = 0) و(SSIM = 1) تؤكد عدم وجود أي تشوه في الصور المستخرجة. وهو أمر مختبر وموثق في عدة أبحاث كما في [16] ذكرت تطابقًا كامل بين الصورة السرية والمستخرجة.

الخلاصة:

في الختام، يُظهر النظام المقترح كفاءة عالية في تشفير الصور وإخفائها، حيث أثبتت النتائج قدرته على تحقيق عشوائية قوية حيث أن قيم الانتروبيا المحسوبة للنظام المقترح تقاربت بشكل كبير من القيمة المثالية وهي (8)، وكسر الارتباط بين البكسلات، والحفاظ على جودة الصورة المستخرجة دون تشوه. كما أظهرت نتائج التجارب أن النظام المقترح يحتفظ بكفاءة عالية في استرجاع الصورة السرية، حتى عند استخدام معاملات تضمين صغيرة (α)، والتي عادة ما تؤثر سلبًا على دقة الاستخراج بسبب انخفاض طاقة الإشارة المخفية. ويُعزى هذا الأداء المرتفع إلى اعتماد النظام على دمج ثلاثي للتحويلات (DWT–DCT–SVD)، حيث يتم أولًا فصل الصورة إلى مكوناتها الترددية باستخدام تحويل المويجة (DWT)، ثم تطبيق تحويل الجيب تمام المنفصل (DCT) على النطاق منخفض التردد (LL)، ومن ثم تحليل القيمة الفردية (SVD) لاستخلاص مكونات الصورة الأكثر ثباتًا. ويتم تضمين الصورة السرية المشفرة داخل معاملات DC الناتجة منDCT ، والتي تُعد الأكثر مقاومة للتشويش وفقدان البيانات، مما يُمكّن من الحفاظ على تفاصيل الصورة

http://www.doi.org/10.62341/abak1308

السرية حتى في ظل قيم α منخفضة. كما أن استخدام نفس القيم (S1، v، u) في مرحلتي الإخفاء والاستخراج يعزز من دقة الاسترجاع ويضمن استعادة الصورة السرية بشكل مطابق للأصل.

وقد أكدت النتائج الرقمية ذلك، حيث تم تحقيق مؤشرات مثالية في الجودة، تمثلت في حصول الصورة المستخرجة على قيمة SSIM =1 و MSE =0 في أغلب التجارب، مما يبرهن على قدرة النظام على تحقيق استرجاع دقيق للصورة السرية دون التأثير على جودة الصورة الحاملة. كما أظهرت التجارب أن النظام حساس جدًا للتغيرات الطفيفة في القيم الأولية، مما يعزز من أمانه ضد محاولات الاختراق. وبفضل تكامل مرحلتي التشفير والإخفاء، ويقدم النظام حلاً فعالًا وآمنًا لحماية البيانات البصرية، وفي المستقبل نقترح دراسة مقاومة هذه المنهجية ضد أي هجمات هندسية أو هجمات غاشمة.

المراجع

[1] J. Liu, H. Chang, W. Ran, and E. Wang, “Research on Improved DNA Coding and Multidirectional Diffusion Image Encryption Algorithm,” *Entropy*, vol. 25, no. 5, Art. no. 746, May 2023, doi: 10.3390/e25050746.

[2] N. Provos and P. Honeyman, "Hide and Seek: An Introduction to Steganography," IEEE Security & Privacy, vol. 1, no. 3, pp. 32–44, May-June 2003, doi: 10.1109/MSECP.2003.1203220.

[3] B. Zhang and L. Liu, "Chaos-Based Image Encryption: Review, Application, and Challenges," *Mathematics*, vol. 11, no. 11, p. 2585, 2023, doi: 10.3390/math11112585.

[4] B.-W. Shen, "Nonlinear feedback in a six-dimensional Lorenz model: Impact of an additional heating term," Nonlinear Processes in Geophysics, vol. 22, pp. 749–764, 2015, doi: 10.5194/npg-22-749-2015.

[5] T. Wang and M. Wang, "Hyperchaotic image encryption algorithm based on bit-level permutation and DNA encoding," *Optics and Laser Technology*, vol. 132, p. 106355, 2020, doi: 10.1016/j.optlastec.2020.106355.

[6] B. L. Gunjal and S. N. Mali, “Secured color image watermarking technique in DWT-DCT domain,” *Int. J. Comput. Sci. Eng. Inf. Technol.*, vol. 1, no. 3, pp. 36–44, Aug. 2011, doi: 10.48550/arXiv.1109.2325.

[7] E. R. Pramudya, L. B. Handoko, B. Harjo, R. R. Sani, C. A. Sari, G. F. Shidik, P. N. Andono, and M. K. Sarker, “Securing Medical Images Using Discrete Wavelet Transform (DWT) and

http://www.doi.org/10.62341/abak1308

Singular Value Decomposition (SVD) for Image Steganography," *J. Teknol. Informatika (Jutif)*, vol. 6, no. 2, Art. no. 4426, 2025, doi: 10.52436/1.jutif.2025.6.2.4426.

[8] A. K. Jain, *Fundamentals of Digital Image Processing*. Englewood Cliffs, NJ, USA: Prentice-Hall, 1989.

[9] R. A. Jadav and S. S. Patel, "Application of singular value decomposition in image processing," *Indian J. Sci. Technol.*, vol. 3, no. 2, pp. 148–150, Jan. 2010, doi: 10.17485/ijst/2010/v3i2.2.

[10] R. S. Choraś, Ed., *Image Processing & Communications Challenges 2*. Advances in Intelligent and Soft Computing, vol. 84, Berlin, Germany: Springer, 2010, doi: 10.1007/978-3-642-16295-4.

[11] J. Liu, H. Chang, W. Ran, and E. Wang, "Research on Improved DNA Coding and Multidirectional Diffusion Image Encryption Algorithm," *Entropy*, vol. 25, no. 5, Art. no. 746, May 2023, doi: 10.3390/e25050746.

[12] Y. Li, W. Liu, H. Liu, H. Zhao, and C. Guo, "Multi-Image Compression–Encryption Algorithm Based on Compressed Sensing and Optical Encryption," *Entropy*, vol. 24, no. 6, Art. no. 784, Jun. 2022, doi: 10.3390/e24060784.

[13] H. Tong, T. Li, Y. Xu, X. Su, and G. Qiao, "Chaotic coyote optimization algorithm for image encryption and steganography," *Multimedia Tools and Applications*, vol. 83, no. 7, pp. 20861–20887, 2024, doi: 10.1007/s11042-023-16240-w.

[14] M. Wang, X. Wang, T. Zhao, C. Zhang, Z. Xia, and N. Yao, "Spatiotemporal chaos in improved cross coupled map lattice and its application in a bit-level image encryption scheme," *Information Sciences*, vol. 544, pp. 1–24, 2021, doi: 10.1016/j.ins.2020.07.051.

[15] Y. Li, W. Liu, H. Liu, H. Zhao, and C. Guo, "Multi-Image Compression–Encryption Algorithm Based on Compressed Sensing and Optical Encryption," *Entropy*, vol. 24, no. 6, Art. no. 784, Jun. 2022, doi: 10.3390/e24060784.

[16] S. L. Gomez-Coronel, E. Moya-Albor, and J. Brieva, "A Robust and Secure Watermarking Approach Based on Hermite Transform and SVD-DCT," *Applied Sciences*, vol. 13, no. 14, Art. 8430, 2023, doi: 10.3390/app13148430.