طريقة مُقترحة للنقل الآمن للصور الطبية في معيار DICOM

عبادة عثمان آغا*، يحيى فريد **، لؤي شاشاتي***

* طالب دراسات عليا (دكتوراه)، قسم هندسة الاتصالات، كلية الهندسة الكهربائية والإلكترونية، جامعة حلب

**أستاذ، قسم هندسة الاتصالات، كلية الهندسة الكهربائية والإلكترونية، جامعة حلب

***أستاذ، قسم الهندسة الالكترونية، كلية الهندسة الكهربائية والإلكترونية، جامعة حلب

الملخص

مع التطور المُتسارع لتقنيات الطب عن بعد، شكّلت مهمة تبادل الصور الطبية بشكلٍ آمن موضع اهتمامٍ بالغٍ لمراكز الرعاية الصحية، لا سيّما تلك التي تعتمد على معيار DICOM، أحد أكثر المعايير تطوراً وانتشاراً في هذا المجال.

اقترحنا في هذا البحث مُخطط تشفير يستخدم خوارزميات مختلفة وفقاً لأهمية البيانات المُعالجة، حيث يتم تطبيق نموذج هجين في منطقة الاهتمام وفق مرحلتين، تعتمد المرحلة الأولى على تنفيذ خلط مزدوج على مستويي البت والبكسل، عبر الدمج بين نموذج المسح Y-Index، لكسر ارتباط البكسلات المتجاورة، وخريطة Hènon ثنائية البعد، بينما تعتمد المرحلة الثانية على التشفير التدفقي عبر نسخة مطورة من خوارزمية RC4 لتحسين مستوى الحماية وتجاوز الثغرات التي تتعلق بالمفاتيح.

إن الاعتماد على طريقة فعالة وغير معقدة لتجزئة مصفوفة بكسلات صور DICOM باستخدام خوارزمية OTSU التلقائية، ومن ثم تطبيق خوارزمية مُنخفضة التعقيد الحسابي في منطقة خلفية الصورة يُساهم في تخفيض زمن التشفير الكلي، مع تأمين حماية سريعة وعالية المستوى لبيانات المريض النصية المُستخرجة من صورة DICOM باستخدام نسخة مُعدلة لخوارزمية AES، بزمن معالجة قدره 0.2382 ثانية.

تم اختبار فعالية المُخطط عبر معايير الحماية NPCR وUACI وPSNR التي بلغت 99.95 و33.26 و5.572 على التتالي، وكذلك تحليل الهيستوغرام، ثم مُعاملات الارتباط التي قاربت قيمها الصفر، وقيمة الانتروبي التي بلغت 7.9993.

الكلمات المفتاحية: الصور الطبية، خوارزميات التشفير التدفقي، معيار DICOM، الخرائط العشوائية.

ورد البحث للمجلة بتاريخ 2023/12/3

قُبل للنشر بتاريخ 2024/2/15

1- المقدمة:

مع النمو الكبير والمتسارع لتقنيات الاتصالات والطب عن بعد، تزداد أهمية تأمين تبادل الصور الرقمية بين المراكز الطبية، لما تتضمنه من معلومات هامة وحساسة تتعلق بالتشخيص الطبي للمرضى. يُمثّل معيار DICOM (Digital Imaging and Communications in Medicine) مساراً طويلاً من الجهود المتراكمة لتحقيق المعيار الأمثل والأكثر انتشاراً في مراكز الرعاية الصحية وشركات التجهيزات الطبية، حيث لا يُمكن اختزال دوره على أنه نمط أو صيغة للصور، بل هو بروتوكول مُتكامل يدعم تبادل وتخزين واستعراض الصور الطبية الرقمية بجودة عالية وميزات متقدمة، مما يجعله محط أنظار الباحثين حول العالم، مع الإشارة إلى أن صورة DICOM الطبية تشمل بيانات توصيفية، تتضمن بيانات المرضى والمشفى والتجهيزات الطبية (Patient Data)، إضافةً إلى مصفوفة بكسلات الصورة (Pixel Data Array) [1]. إن تبادل هذا الحجم الهائل من الصور الرقمية، يجعلها عُرضةً للعديد من الهجمات، لذا فإننا نهدف لاقتراح مخطط تشفير فعال يوازن بين تحقيق السرعة العالية، والقدرة على تجاوز اختبارات الحماية عبر معايير التقييم المطلوبة، وذلك باستخدام خوارزميات تشفير مختلفة وفقاً لأهمية البيانات المُعالجة.

2- الدراسة المرجعية:

اعتمد البحث [2] في عام 2020 على توليد المفاتيح السرية من خلال معلومات صورة DICOM المُدخلة، مثل أبعاد الصورة وقيم التدرجات الرمادية، فيما يتم تبديل مواقع البكسلات عبر سلاسل دورية شبه عشوائية، ثم التشفير باستخدام خريطة عشوائية لوجستية (Logistic Map)، بينما قدّم البحث [3] طريقة لتشفير هذه الصور باستخدام خريطة Tinkerbell ثنائية البعد، يلي ذلك استخدام سلاسل DNA (Deoxyribonucleic Acid) مع تنفيذ عملية XOR على مستوى البت. في العام ذاته، اختبر البحث [4] خوارزمية لتشفير صور DICOM عبر تقسيم الصورة إلى كتل، ثم تشفيرها كتلة تلو الأخرى باستخدام خوارزمية Vigenèr، مع تعديل المفتاح لكل منها عبر تحويل Arnold، والإشارة إلى أفضلية تطوير الخوارزمية المقترحة مُستقبلاً لتشمل حماية بيانات المريض النصية في هذه الصور.

اقترح البحث [5] في 2022 استخدام مفتاح يتم توليده عبر خريطة Bülban، حيث تُطبّق آلية التشفير وفق مرحلتين، تتم الأولى في مجال التحويل (Transform Domain) عبر التحويل 5/3، بينما تُنفذ الثانية في المجال المكاني (Spatial Domain) عبر تغيير قيم البكسل باستخدام المفتاح، فيما اختبر البحث [6] في 2023 مخطط فوضوي هجين يعتمد على كل من النموذج اللوجستي (Logistic chaotic) ونموذج Lorentz، بعد تطبيق المرشح الوسيط في مرحلة المعالجة الأولية.

قدم البحث [7] في 2023 طريقة تعتمد على استخراج مناطق الاهتمام باستخدام طريقة لكشف مناطق الذروة في الهيستوغرام ثم تشفيرها عبر مصفوفة Sudoku، إلا أن البحث لم يُظهر أي نتائج تتعلق بمعايير تقييم مخطط التشفير المُقترح أو اختبارات الحماية من الهجمات.

اقترح البحث [8] في 2023 آلية لاختيار طريقة التشفير، يتم فيها استخراج مناطق الاهتمام من خلال آلية تجزئة عتبة البكسل، مع استخدام خوارزمية AES بطول مفتاح يختلف وفقاً لأهمية البيانات المُعالجة، وذلك بالمقارنة مع بيانات المريض النصية وخلفية الصورة، حيث تركزت غاية البحث الأساسية على تقليل زمن المعالجة، مُشيراً إلى ضرورة تطوير الآلية المُقترحة مُستقبلاً لتحقيق متطلبات الحماية.

إلا أن النتائج الاختبارية تُظهر عدم فعالية خوارزمية AES في حماية الصور، إذ يتلاءم هذا النمط من الخوارزميات مع البيانات النصية، بينما تتمتع صور DICOM بحجم بيانات كبير وكثافة شديدة وترابط عالي بين البكسلات [4][9].

تُظهر الدراسة البحثية استخدام تقنيات هجينة بالاستفادة من الخرائط العشوائية لتأمين الحماية واختبارها وفق معايير NPCR وUACI وPSNR ومُعاملات الارتباط، مع التركيز مؤخراً على التشفير وفق مناطق الاهتمام بهدف تخفيض الزمن [7-8]، لكن دون تحقيقها لمعايير الحماية المطلوبة.

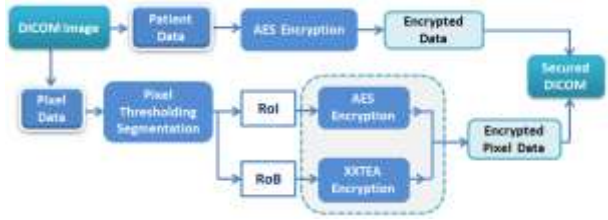
3- أهمية البحث وأهدافه:

نسعى في هذا البحث إلى تحقيق التوصيات التي قدمتها الدراسة المرجعية بضرورة حماية بيانات المريض التي تتضمنها صور DICOM، وتقليل زمن المعالجة

عبر تشفير مناطق الاهتمام في الصورة عبر خوارزمية هجينة أكثر تعقيداً من تلك المُستخدمة مع خلفية الصورة أو بيانات المريض، بهدف تحقيق متطلبات الحماية التي تضمن النقل الآمن، والجمع بين غايتَي تعزيز مستوى الحماية وتخفيض زمن التنفيذ.

4- الآلية المقترحة:

يُظهر الشكل (1) بنية مخطط التشفير المُقترح في البحث [8]، الذي يعتمد على استخدام خوارزمية AES لتشفير كل من بيانات المريض ومناطق الاهتمام RoI التي تم استخراجها بتطبيق آلية تجزئة عتبة البكسل على صور DICOM، في حين يتم استخدام خوارزمية XXTEA مع خلفية الصورة RoB لتخفيض زمن التشفير.

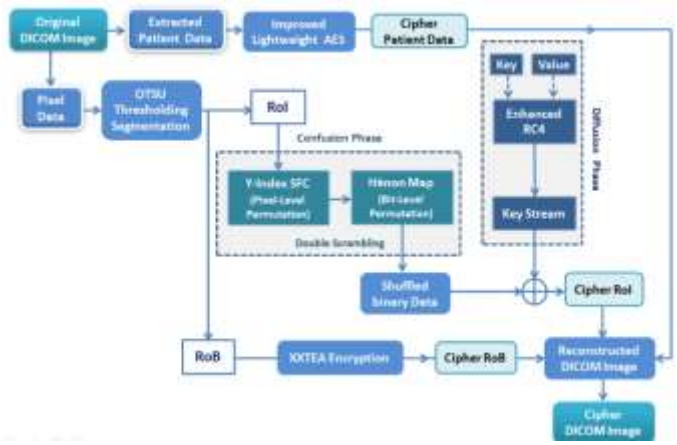


الشكل (1): بنية مخطط التشفير الأصلي [8].

ونتيجةً لعدم فعالية استخدام خوارزمية AES مع الصور، لا سيّما صور DICOM التي تتمتع بكثافة شديدة وارتباط عالي بين البكسلات، إذ يتلاءم نمط هذه الخوارزميات مع البيانات النصية [9][4]، فقد قمنا باستبدال هذه الخوارزمية بمرحلة مزدوجة من الخلط على مستويي البت والبكسل معاً لزيادة مستوى الحماية.

تعتمد هذه المرحلة على نموذج المسح Y-Index وخريطة Henon ثنائية البعد، قبل تنفيذ نسخة مطورة من خوارزمية RC4 على مناطق الاهتمام في الصورة، حيث يتم استخراج هذه المناطق عبر خوارزمية OTSU التلقائية، التي تتميز بفعاليتها في تحقيق تجزئة الصور (Segmentation)، مما يُساهم في تخفيض زمن التشفير.

إذ تهدُف مرحلة الخلط (Confusion) بشكل أساسي للتخلص من العلاقة التي تربط بين مواقع بكسلات الصورة، أما مهمة مرحلة النشر (Diffusion) فهي التحقق من أن أي تغيير بسيط في الصورة الأصلية سيتسبب بتغييرات كبيرة في الصورة المشفرة، في حين قمنا بتوظيف نسخة مطورة وسريعة لخوارزمية AES لحماية بيانات المريض النصية لدورها في زيادة العشوائية وتخفيض الزمن وفق الشكل (2).



الشكل (2): المخطط العام لنظام التشفير المُقترح.

1-4 الاختيار التلقائي لمناطق الاهتمام RoI وتحديد عتبة التجزئة:

بهدف تقليل زمن المعالجة عند التشفير، سنعمل على استخراج مناطق الاهتمام باستخدام خوارزمية OTSU التلقائية لتحديد العتبة (Thresholding)، والتي أثبتت كفاءتها العالية في التوصل إلى مناطق الاهتمام وتجزئة الصور الطبية، لما تتمتع به من سهولة التنفيذ وعدم تأثرها بسطوع الصورة أو تباينها، إذ يُمكن النظر إليها باعتبارها إحدى أمثل الطرق لتحقيق ذلك وفقاً للبحث [10] عام 2022، حيث يتم استخدام التجزئة للحصول على العتبة المُستهدفة التي تُستخدم لاستخراج مناطق الاهتمام مُعتمدةً في مبدأ عملها على التجميع (Clustering).

تعتمد هذه الآلية على تقسيم المستويات الرمادية تلقائياً إلى جزءين، من خلال مستوى رمادي مناسب يتم التوصل إليه عبر حساب التباين (Variance) بين فئتي منطقة الاهتمام وخلفية الصورة، ليتم استخدام طريقة العبور (Traversing) للحصول على العتبة الأمثلية k التي تحقق أعظم قيمة للتباين بين الفئتين، وأصغر قيمة تباين ضمن كل فئة، فبفرض أن الصورة مُمثلة وفق L مستوى رمادي، فإن المجالين [0, k] و[k+1, L-1] يُمثلان مستويات بكسلات الفئتين الأولى والثانية، ويتم حساب احتمال ارتباط البكسل P(k) بإحدى الفئتين وفق المعادلات التالية [11-12].

$$P_1(k) = \sum_{i=0}^{k} P_i \quad (1)$$

$$P_2(k) = \sum_{i=k+1}^{L-1} P_i \quad (2)$$

ويتم تقسيم الصورة ذات الأبعاد M*N إلى كتل بحجم n*n، بفرض n عدد صحيح وأحد قواسم M و N لتشكيل كتل مربعة بأحجام ثابتة، حيث قمنا بتحديد n وفق القيمة 4، بما يتناسب مع أبعاد الصور في مجموعات البيانات Datasets المُستخدمة، كما في الأبعاد 512*512 و320*320، فيكون حجم الكتلة هو 4*4=16، ويتم تجزئة الصورة إلى S كتلة يُحسب عددها عبر العلاقة التالية [10]:

$$S = (M*N) / n\text{^}2 \quad (3)$$

وحساب المتوسط الحسابي للتدرجات الرمادية لكلا الفئتين عبر العلاقات التالية [12]:

$$m_1(k) = \sum_{i=0}^{k} \frac{i\,P_i}{P_1(k)} \quad (4)$$

$$m_2(k) = \sum_{i=k+1}^{L-1} \frac{i\,P_i}{P_2(k)} \quad (5)$$

وتحديد العتبة بما يُحقق أقل قيمة للتباين ضمن الفئة عبر العلاقة التالية [12]:

$$\sigma_\omega^2(k) = m_1(k)\sigma_1^2(k) + m_2(k)\sigma_2^2(k) \quad (6)$$

في حين يُحسب التباين للفئتين الأولى والثانية باستخدام العلاقات التالية [12]:

$$\sigma_1^2(k) = \sum_{i=0}^{k}[i - m_1(k)\,]^2 \frac{iP_i}{P_1(k)} \quad (7)$$

$$\sigma_2^2(k) = \sum_{i=k+1}^{L-1}[i - m_2(k)\,]^2 \frac{iP_i}{P_2(k)} \quad (8)$$

يتم تصنيف الكتل B ضمن إحدى الفئتين، وذلك عبر تفعيل خانة Flag للكتل التي تقع في مناطق الاهتمام RoIBr، حيث r هو رقم المنطقة، وإلا فإنها تعتبر جزء من الخلفية، ثم يتم دمج سلسلة مناطق الاهتمام لتشكيل مصفوفة بطول n*n وبترتيب من أعلى لأسفل بما يتوافق مع عدد المناطق عبر المعادلة التالية [10].

$$ROI_M = \left[ROIB_1, ROIB_2, \cdots, ROIB_{(n\times n)}\right] \quad (9)$$

4-2 مرحلة الخلط المزدوج (Double Scrambling):

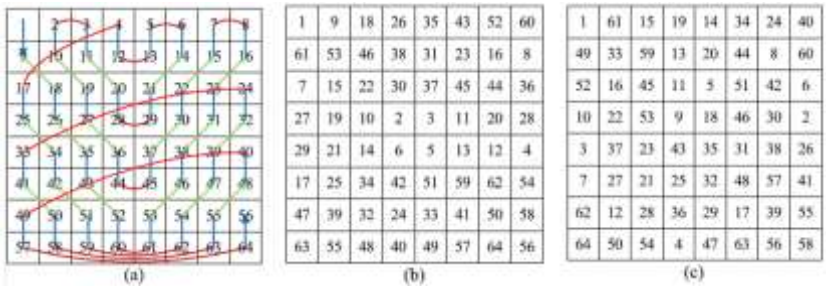
تُستخدم الخرائط العشوائية بشكل واسع في مرحلة الخلط بسبب ميزاتها العديدة، مثل التعقيد البنيوي، وقدرتها على تحقيق العشوائية بالتساوي على كامل المساحة المطلوبة، حيث تُنتج متتاليات عشوائية غير خطية وحساسة للشروط الأولية [13]، إلا أن الاختبارات تشير إلى أن بعض طرق التشفير التي تعتمد على الخرائط العشوائية فقط تكون عرضة للهجمات [14]، كما أن اعتماد مخطط التشفير على

مرحلة خلط تقليدية يُعرّضه لهجمات القوة القاسية (Brute Force Attack)، لذا فإن تنفيذ عملية خلط على كل من مستويي البت والبكسل، مثل إضافة نماذج المسح أو منحنيات ملئ الفراغ SFC (Space Filling Curve)، يزيد من مستوى الحماية بشكل فعال، حيث تتوفر نماذج مسح متعددة [15]. لتحقيق ذلك، استخدم البحث [16] في 2022 مُنحنى Hilbert لتبديل مواقع بكسلات الصورة دون تغيير محتواها، قبل تطبيق الخريطة العشوائية على مستوى البت، ثم التشفير التدفقي باستخدام خوارزمية grain-128، إلا أن تطبيق المسح باستخدام هذا المنحني يُظهر درجة ارتباط عالية بين البكسلات، لذا فقد اقترح البحث [17] في 2022 دمج المنحنى مع خوارزمية Knuth-Durstenfeld لتخفيض الارتباط دون اختبارها على الصور الطبية.

نستخدم مرحلة خلط مزدوجة تعتمد على نموذج SFC Y-index وخريطة Henon العشوائية لتنفيذ التبديل على مستويي البت والبكسل معاً، بالاستفادة من نتائج اختبار تحليل الارتباط في البحث [18] التي أظهرت تفوقاً واضحاً لهذا النموذج مقارنةً بنموذجي Hilbert و Square-wave، قبل تطبيق مرحلة التشفير التدفقي باستخدام خوارزمية RC4 مُعدّلة، ذلك أن الهدف من استخدام مرحلة الخلط المزدوج هو عدم الاكتفاء بكسر الارتباط بين البكسلات المتجاورة فقط، وإنما تغيير قيمة البكسل كذلك.

4-2-1 نموذج Y-Index SFC (Space Filling Curve):

بهدف توضيح عمل هذا النموذج، يبيّن المثال التالي عملية المسح لمصفوفة البيانات ذات الأبعاد 8*8 كما في الشكل (3-a)، يبدأ مسار المسح من الخلية اليسرى العليا للمخطط ليتم تغيير مواقع البكسلات وفق شكل المحرف Y على التتالي، ويُظهر الشكل (3-b) مصفوفة البيانات المُبعثرة، حيث انتقلت البكسلات ذات القيم (9–18–26-35-43-52-60) نتيجة موقعها إلى الصف الأول، مع تكرار ذلك حتى تشكيل المصفوفة، فيما يوضح الشكل (3-c) نتيجة إعادة تنفيذ المسح مرة أخرى[18].



1	9	18	26	35	43	52	60
61	53	46	38	31	23	16	8
7	15	22	30	37	45	44	36
27	19	10	2	3	11	20	28
29	21	14	6	5	13	12	4
17	25	34	42	51	59	62	54
47	39	32	24	33	41	50	58
63	55	48	40	49	57	64	56

1	61	15	19	14	34	24	40
49	33	59	13	20	44	8	60
52	16	45	11	5	51	42	6
10	22	53	9	18	46	30	2
3	37	23	43	35	31	38	26
7	27	21	25	32	48	57	41
62	12	28	36	29	17	39	55
64	50	54	4	47	63	56	58

(a) (b) (c)

الشكل (3): مثال توضيحي لآلية عمل نموذج Y-Index SFC.

4-2-2 خريطة Hènon:

هي خريطة عشوائية ثنائية البعد، حيث أي تغيير في القيمة البدائية يُنتج قيم عشوائية مختلفة، مما يؤمن عشوائية أفضل من الخريطة أحادية البعد [3]، كما أنها تتميز بسرعتها العالية وفعاليتها في تحقيق جودة عالية في التشفير [13]، ويُمكن التعبير عن التمثيل الرياضي لخريطة Hènon وفق المعادلتين التاليتين [16]:

$$x_{n+1} = y_n + 1 - a_1 x_n^2 \quad (10)$$

$$\bar{y}_{n+1} = b_1 \bar{x}_n \quad (11)$$

تمثّل $\bar{x}$ و$\bar{y}$ متغيرات الحالة، التي يتم التعبير عن محتواها عند التكرار n^{th} وفق $\bar{x}_n$ و$\bar{y}_n$ على التتالي، ثم بناء الخريطة اعتماداً على بارمتري التحكم a1 وb1، مع اختيار القيم 1.4 و0.3 لها على التتالي، التي تم التوصل إليها تجريبياً بما يحقق أفضل تأثير عشوائي وفق الشروط الأولية [16]، ثم تكرارها وفقاً لحجم الصورة.

4-3 استخدام خوارزمية RC4 في تشفير الصور:

يُحقق التشفير التدفقي سرعة وفعالية عالية ويعمل على تنفيذ التشفير على مستوى البت [19-20]، لذا سنستخدمه لتشفير مناطق الاهتمام في صور DICOM.

وقد اعتمدت عدة أبحاث حديثة على خوارزميات التشفير التدفقي، لا سيما RC4، في تشفير الصور الطبيعية (غير الطبية) لما تحققه من سرعة عالية وزيادة قيمة الانتروبي (Entropy Value) ومعدل خطأ البت مما يزيد صعوبة كسر التشفير.

في 2019، طور البحث [21] طريقة تجمع بين التشفير باستخدام خوارزمية RC4 وإخفاء المعلومات بتقنية LSB (Least Significant Bit) مُحسّنة، مع تطبيق معالجة أولية تتضمن تقسيم الصورة إلى كتل وإعادة ترتيبها وفقاً لحالتها الفردية أو

الزوجية، في حين اختبر البحث [22] اقتراحاً لحماية الصور عبر تقنية إخفاء البيانات القابلة للعكس RDH (Reversible Data Hiding) عبر إزاحة الهيستوغرام (Histogram shifting) ثم استخدام RC4 في التشفير. اقترح البحث [23] في 2020 الدمج بين ثلاث طبقات، وهي طبقة إزاحة البت، وخريطة Arnold العشوائية، وتشفير RC4 التدفقي، فيما اقترح البحث [24] عام 2022 تقنية تشفير تستخدم RC4 لتشكيل المفتاح مع الاعتماد على خريطة Arnold بهدف تغيير بكسلات الصورة.

4-3-1 استخدام نسخة RC4 مُطورة لتشفير مناطق الاهتمام:

على الرغم من الكفاءة العالية، إلا أن هذه الخوارزمية تتضمن ثغرات تجاه الهجمات التي تتعلق بالمفاتيح، فهي تُعاني من مشكلة التعارض بين المفاتيح، الأمر الذي يُعطّل تحقيق العشوائية المطلوبة ويُمكّن من حساب الحالة الأولية، مما يُنتج تدفق البايتات ذاتها، حيث ترتكز غالبية الهجمات على نقاط ضعف تعتمد على عشوائية الحالة الداخلية والانتشار المنخفض للبتات في جدولة المفاتيح [25]، كما تُظهر الدراسة العميقة للارتباط بين بايتات تدفق المفاتيح والمفتاح السري أن السلوك غير العشوائي لهذه الخوارزمية يتسبب بتشكيل انحياز يوضّح العلاقات التي تربط بينها، مما يجعلها عُرضةً لهجمات تحليل التشفير (Cryptanalysis Attacks) [26].

اقترح البحث [26] عام 2019 دمج مولد تابع عشوائي لتأمين العشوائية في جدولة المفتاح، مع تخزين بايتات المفتاح لتنفيذ فك التشفير لاحقاً، بدلاً من استخدام مفتاح واحد لمرحلتي التشفير وفك التشفير، فيما اعتمد البحث [27] في 2020 على معادلة خطية بأربع جداول حالة لتوليد أرقام عشوائية، باستخدام مفتاح تحكم لاختيار أحد الجداول، ومُعتمداً على استبدال الحالتين بأربع حالات لزيادة حجم المفتاح.

في 2021، حلل البحث [28] خوارزمية RC4A الناتجة عن تطوير RC4، والتي تتطلب عمليات أقل وتتمتع بأفضلية في توفير الحماية، مؤكداً أنها لا تزال عُرضة لثغرات عديدة، ومُقترحاً استخدام مُعامل تدوير لاخطي ضمن مرحلة استبدال البكسلات لتحسين الحماية، فيما اختبر البحث [29] ميزات دمج مولد أرقام شبه عشوائية PRNG (Pseudo-Random Number Generator) ضمن بنية RC4.

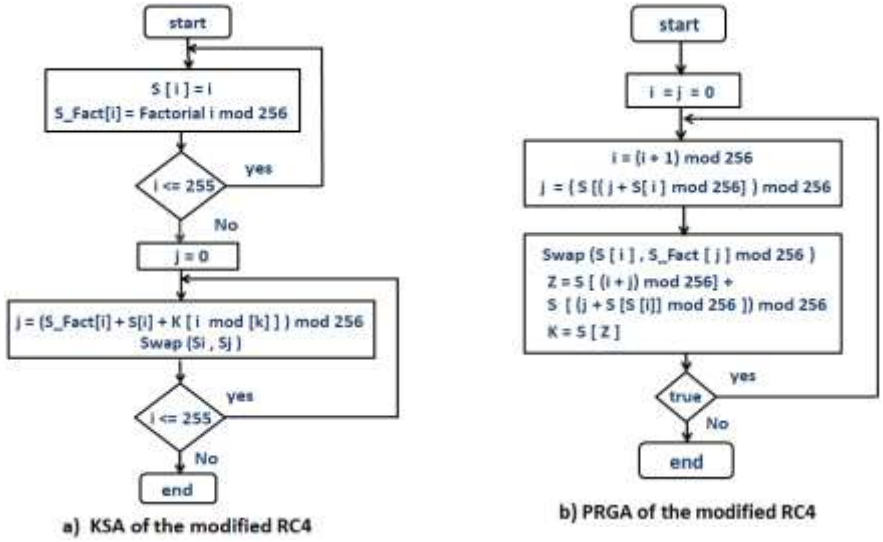
ضمن المخطط المُقترح في هذا البحث، نستخدم تطويراً لخوارزمية RC4 لتحقيق التشفير التدفقي بعد تنفيذ مرحلة الخلط المزدوجة على مناطق الاهتمام في صورة DICOM، وذلك عبر تعديلات تعتمد استخدام جدول الحالتين الأوليتين (two initial states table) وتوظيف عاملي الحالة الأولية (Initial State Factorial) لتحسين العشوائية في خوارزميتي KSA (Key Scheduling Algorithm) و PRGA (Pseudo-Random Generation Algorithm) لما لها من تأثير في الحماية من الهجمات، حيث أظهرت نتائج البحث [30] في 2022، والتي تم اختبارها على البيانات النصية، قدرة هذه التعديلات على تحقيق الحماية الكاملة من هجمة القوة القاسية وتحسينها ضد هجمة تغيير البت (Bit Flipping). تعمل خوارزمية KSA على تهيئة مصفوفة الحالة باستخدام مفتاح التشفير، حيث يتم بناؤها وفق الشكل S[0], S[1],….., S[255] ضمن المجال [0-255] [24]، وتحقيق التعديل الأساسي اعتماداً على توظيف حالة أولية إضافية باستخدام العاملي وفق المعادلة التالية [30]:

$$S\_Fact[i] = Factorial\ i \bmod 256 \quad (12)$$

وذلك حتى اكتمال بناء مصفوفة S_Fact[i]، بينما تبدأ عشوائية مصفوفة الحالة وفق j=0 اعتماداً على المتغير state_fact[i] بدلاً من j، ثم تبديل المحتوى بين s[i] و s[j] وتشكيل الخرج وفق الشكل (4-a). فيما تهدف مرحلة PRGA لتشكيل المفتاح التدفقي للتشفير، حيث تبدأ التهيئة بقيم صفرية للعدّادين i و j حتى استيفاء كامل البيانات [23]، ويتم حساب j بعد التعديل وفق المعادلة التالية [30].

$$j = (State [(j + State [i] \bmod 256]) \bmod 256 \quad (13)$$

ثم تتم عملية التبديل للحصول على تسلسل المفتاح كما في الشكل (4-b) [30].



الشكل (4): مرحلتي KSA (a) وPRGA (b) في خوارزمية RC4 المُعدّلة

4-4 استخدام خوارزمية AES مُطورة لتشفير بيانات المريض:

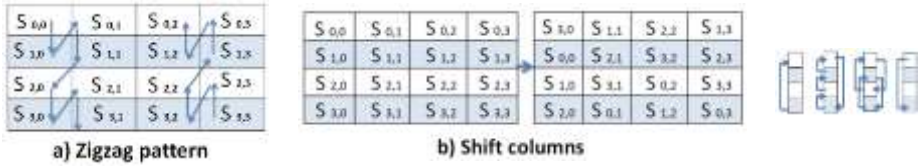
فيما يتعلق بتشفير بيانات المريض، سنلجأ لاستخدام خوارزمية AES لكفاءتها العالية في مجال البيانات النصية [4] [9]، إلا أن اختبارات حديثة أظهرت الحاجة لتطوير هذه الخوارزمية لتحقيق مستوى حماية أعلى أو تخفيض زمن التنفيذ.

في 2020، اقترح البحث [31] تعديل مرحلة توسيع المفاتيح وتنفيذ التشفير على مستوى البت من خلال دفعات تعتمد على مفاتيح متغيرة، يُطبّق على كلٍ منها عمليتي XOR وتحويل استبدال البايتات، مع استخدام قيم S-box لزيادة اللاخطية.

بينما قدم البحث [32] في 2020 تطويراً لخوارزمية AES في بيئة التخزين السحابي، يتم فيها تعديل خطوة مزج الأعمدة وتوليد المفتاح عبر خريطة Skew Tent لحساسيتها العالية للشروط الأولية، فيما اختبر البحث [33] في 2021 تعديلات تضمنت إهمال خطوة مزج الأعمدة لتسببها في بطء عملية التشفير، مع إضافة خطوة تبديل المواقع (permutation) باستخدام 14 حلقة لتعزيز الحماية في الخوارزمية.

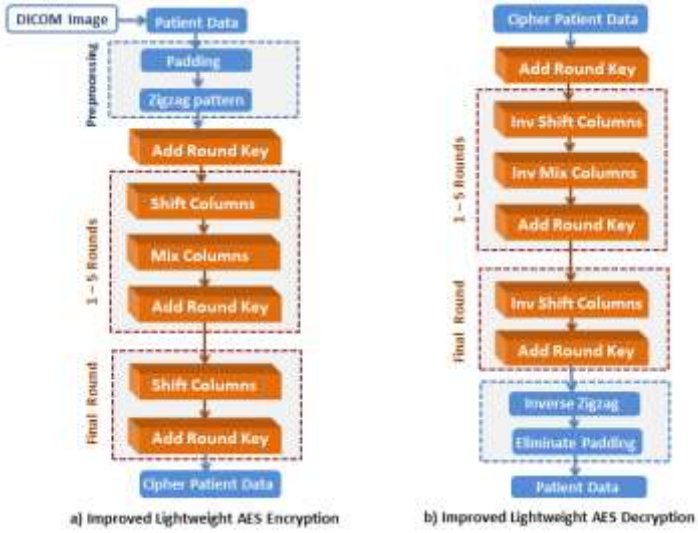
سنستخدم ضمن المخطط المُقترح، نسخة مطورة من خوارزمية AES، بالاستفادة من التعديلات التي اقترحها البحث [34] عام 2021، والتي تم اختبارها في بيئة التجارة الالكترونية لما تتطلبه من مستوى حماية متقدم وسرعة تنفيذ، بحيث يتم استخدامها بما يتلاءم مع صيغة بيانات المرضى المُستخرجة من صور DICOM، إذ

تشير اختبارات البحث [34] إلى أن هذه التعديلات تزيد درجة العشوائية بمقدار 29.5% وتخفّض زمن التشفير بمقدار 10% مقارنةً مع خوارزمية AES التقليدية. تتضمن التعديلات إضافة خطوات معالجة أولية تتمثل بعملية حشو الخانات (Padding) لإعادة تشكيل الرسائل إلى مصفوفات بحجم 4*4 بايت، ثم نموذج التعرج (Zigzag) الذي يمثل إعادة ترتيب محارف النصوص لكسر أي علاقات إحصائية وفق الشكل (5-a)، حيث يُنفذ مرة واحدة لتعويض حذف خطوة استبدال البايتات وتخفيض زمن الخوارزمية دون التأثير على أدائها، فيما يتم استخدام الإزاحة العمودية بدلاً من السطرية لزيادة صعوبة التنبؤ بآلية التنفيذ وفق الشكل (5-b).



الشكل (5): آلية تنفيذ الإزاحة العمودية (b) ونموذج Zigzag (a) في خوارزمية AES المعدّلة

يتم استخدام ست حلقات، تتضمن عمليات الازاحة العمودية ومزج الأعمدة وجمع المفتاح، عدا الجولة الأخيرة التي لا تتضمن الازاحة العمودية وفق الشكل (6).



الشكل (6): خطوات عمليتي التشفير (a) وفك التشفير (b) في خوارزمية AES المعدلة

تُعتبر عملية مزج الأعمدة الخطوة الأهم والأطول لتنفيذ العمليات الحسابية اللازمة لتأمين التعقيد والحماية، فيما يُساهم تخفيض عدد الحلقات في تقليل الزمن

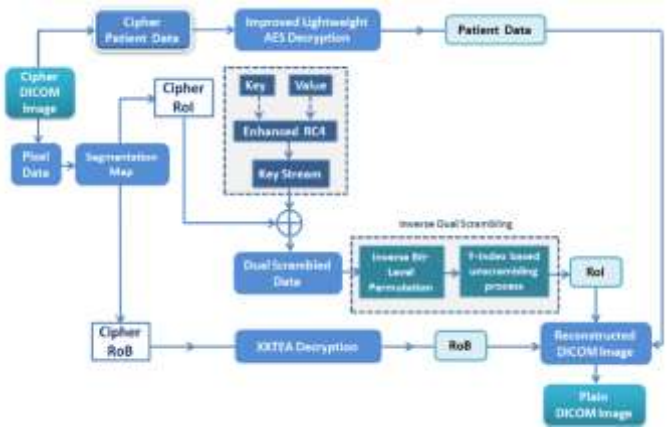
اللازم دون تخفيض مستوى الحماية، نتيجةً لدور نموذج التعرج (Zigzag) في تحسين مرحلتي الخلط والانتشار [34]، فيما تُنفذ بقية المراحل وفق آلية AES الاعتيادية.

4-5 استخدام خوارزمية XXTEA في تشفير منطقة خلفية الصورة RoB:

هي خوارزمية تشفير كُتلي ناتجة عن تطوير خوارزميتي TEA و XTEA، تعمل وفق كتل متغيرة الحجم من مضاعفات 32 بت [35]، تتميز باستهلاكها البسيط للموارد وانخفاض تعقيدها الحسابي، مما يجعلها إحدى أفضل الخيارات لتحقيق سرعة التنفيذ عند عدم وجود معلومات هامة، كما في منطقة خلفية الصورة، لذا فقد تم استخدامها ضمنها وفق 128 بت [36]، مع الإشارة إلى إمكانية عدم تشفير منطقة الخلفية بشكل مُشابه للبحث [7]، إلا أن ذلك سيمنع آلية المقارنة الصحيحة وسينعكس سلباً على بعض معايير الاختبار مثل تحليل الهيستوغرام ومعاملات الارتباط.

4-6 مرحلة فك التشفير:

يتم تطبيق خطوات فك التشفير وفق آلية مُعاكسة لمرحلة التشفير وفق الشكل (7)، إذ تُنفذ خوارزمية RC4 المُطوّرة عبر المفتاح السري والقيمة الابتدائية لتوليد المفتاح التدفقي، ثم تنفيذ XOR بينه وبين منطقة الاهتمام المُشفرة، بالاستفادة من خريطة التجزئة للحصول على البيانات التي تم تطبيق مرحلة الخلط المزدوج عليها، يلي ذلك تطبيق آليات معاكسة لمرحلتي التبديل على مستوى البت وخريطة Hènon لاستعادة الصورة، بعد جمعها مع خلفية الصورة الناتجة عن فك تشفير خوارزمية XXTEA ثم استخراج بيانات المريض عبر خوارزمية AES المُعدلة لفك التشفير.



الشكل (7): المخطط العام لمرحلة فك التشفير

5- الاختبارات العملية ومناقشة النتائج:

تم التنفيذ باستخدام Python 3.9 في بيئة Google-Colab وفق المواصفات (RAM: 12G, GPU: Nvidia-K80)، واستخراج بيانات المريض ومصفوفة بكسلات DICOM بالاعتماد على مكتبة Pydicom 2.4.3.0 وبناء الخوارزميات باستخدام مكتبة Pillow 10.1.0، بالاستفادة من skimage 0.22.0 في تنفيذ خوارزمية OTSU، وتنفيذ الاختبارات على مجموعة البيانات (Siim-DICOM-Images) [37]، ومجموعة البيانات (LIDC-IDRI) [38].

5-1 تحليل الهجمات التفاضلية (Differential attacks):

تتحقق الحماية من هذه الهجمات عندما يتسبب أي تغيير طفيف في الصورة الأصلية بحدوث اختلاف كبير في بكسلات الصورة المُشفرة [6]، وتُختبر باستخدام المعيار NPCR (Number of Pixels Change Rate) لقياس مقدار الاختلاف النسبي بين صورتين، وUACI (Unified Average Changing Intensity) لتحديد متوسط التباين في الكثافة بينهما وفق المعادلات التالية، إذ تُمثل M1 وN1 أبعاد الصورتين المُشفرتين C1 وC2 الناتجة عن صورتين تختلفان بقيمة بكسل واحد [3].

$$NPCR = \frac{\sum_{i,j} D(i,k)}{M1 \times N1} \times 100\% \quad (14)$$

$$UACI = \frac{1}{M1 \times N1}\left[\sum_{i,j} \frac{|C_1(i,k) - C_2(i,k)|}{255}\right] \times 100 \quad (15)$$

فيما تشير D(i,k) إلى مصفوفة ثنائية بالأبعاد ذاتها وفق المعادلة التالية [3].

$$D(l,k) = \begin{cases} 0 \; if \; C_1(l,k) = C_2(l,k) \\ 1 \; if \; C_1(l,k) \neq C_2(l,k) \end{cases} \quad (16)$$

يبيّن الجدول (1) نتائج اختبار بعض صور DICOM، حيث تراوحت قيم المعيار NPCR ضمن المجال [99.98 – 99.92]، وقيم المعيار UACI ضمن المجال [33.41 - 33.22] مما يُظهر تقارباً كبيراً مع القيم الأمثلية (NPCR>99% وUACI≈33%) [3]، ويؤكد قدرة المخطط المُقترح على الحماية من هذه الهجمات.

5-2 تحليل انتروبي المعلومات (Information Entropy):

وهي المعيار الأهم في تحديد العشوائية عبر قياس توزّع القيم الرمادية للصورة باعتبار أنها تؤمن 256 رمزاً (Q) بعمق 8 بت، وتُحسب وفق المعادلة التالية[2].

$$H(q) - \sum_{j=1}^{Q} P(q_j) log_2 \left(\frac{1}{P(q_j)} \right) \quad (17)$$

تُشير q_j إلى معلومات المصدر و$p(q_j)$ لاحتمال حدوثها، وتُظهر قيم الجدول (1) القدرة على مقاومة الهجمات الانتروبية نتيجة اقترابها من القيمة الأمثلية 8 [4].

5-3 تحليل حساسية المفتاح (Key Sensitivity):

لابدّ أن تتمتع خوارزمية التشفير بحساسية عالية لأي تغير طفيف في المفتاح وأن تؤمن الحماية من هجمة القوة القاسية، وهو ما يتحقق عندما يكون المجال أكبر من 2^{128} [4]، وفي حين أن مجال المفتاح في خوارزمية RC4 هو [8–2048 bits] [25]، فقد قمنا بتوظيف نسخة مُطورة أثبتت اختبارات البحث [30] فعالية تعديلاتها في منع هذه الهجمات بشكل كامل. كما أن أحد أهم أسباب توظيف آلية الدمج المُقترحة بين RC4 المُعدلة وخريطة Hènon هو تأمين الحماية من هذه الهجمة نتيجة تسببها في زيادة مجال المفتاح حيث يعتمد أيضاً على الشرو$(\bar{x}_0, \bar{y}_0)$ لخريطة Hènon، إضافةً إلى القيمة الأولية IV ومفتاح خوارزمية التشفير التدفقي.

5-4 الاختبارات الإحصائية (Statistical Tests):

يُستخدم PSNR (Peak Signal-to-Noise Ratio) لتحليل جودة التشفير من خلال الخطأ التربيعي المتوسط MSE (Mean Squared Error) بين الصورتين O و D، إذ تُمثل M و N أبعادهما، و B عمق الترميز، وفق المعادلتين التاليتين [3].

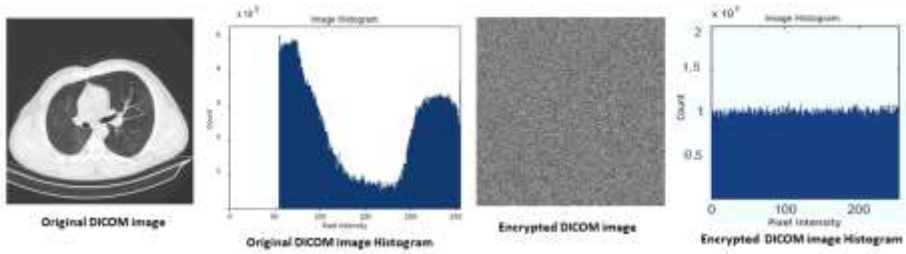
$$PSNR = 10 \times \log_{10} \left\{ \frac{(2^B - 1)^2}{MSE} \right\} \quad (18)$$

$$MSE = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} (O_{i,k} - D_{i,k})^2 \quad (19)$$

تُشير قيمة PSNR للخطأ بين الصورتين الأصلية والمُشفرة، وتتوافق قيمتها الأقل مع قيمة أعلى للتباين بينهما مما يُحقق جودة التشفير، وهو ما أظهرته نتائج الاختبار على الصور المُختبرة وفق الجدول (1)، مع الإشارة إلى أن بعض الأبحاث تستخدم هذا المعيار بين الصورتين الأصلية والناتجة عن فك التشفير، كما في [3] [6]، إذ تُشير القيم المُرتفعة لجودة التشفير نتيجة انعدام الأخطاء أو التباين بينهما.

5-5 تحليل الهيستوغرام ومعامل الارتباط (Correlation coefficient):

يوضح الهيستوغرام عدد مرات ظهور بكسلات الصورة، حيث يتوافق الهيستوغرام المثالي للتشفير مع ظهور قيمة كل بكسل عدد متساوي من المرات، أي أنه سيكون موحّد أو مُسطّح تقريباً [5]، يوضح الشكل (8) الهيستوغرام الناتج عن تطبيق مخطط التشفير المُقترح، مما يُظهر مستوى عالي من العشوائية.



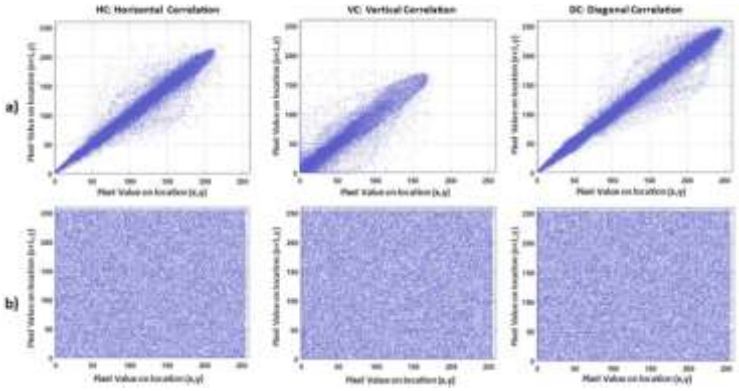
الشكل (8): تحليل الهيستوغرام لصورة DICOM الأصلية والمُشفرة

ولتأمين الحماية من الهجمات الإحصائية لا بد من تحليل العلاقة الإحصائية بين البكسلات المتجاورة للصورة المشفرة، والوصول إلى معامل ارتباط أقرب ما يُمكن إلى الصفر لكسر أي ارتباط، لا سيّما أن صور DICOM تتمتع بمعامل ارتباط عالي [3]، لذا تم الاستفادة من دمج نموذج المسح Y-Index الذي يُظهر أفضل النتائج في تحليلات مُعاملات الارتباط [18]، ويُظهر الشكل (9) مخطط الارتباط لإحدى عينات الاختبار وفق الاتجاهات الأفقية والعامودية والقطرية، إذ يُمكن حساب هذا المُعامل r وفق المعادلات التالية [2]، باستخدام الانحراف المعياري D، والتباين cov.

$$r_{ab}=\frac{cov(a.b)}{\sqrt{D(a)}\sqrt{D(b)}} \qquad D(a)=\frac{1}{M}\sum_{i=1}^{M}(a-E(a_i))^2 \qquad (20)$$

$$E(a)=\frac{1}{M}\sum_{i=1}^{M}a_i \qquad cov(a.b)=\frac{1}{M}\sum_{i=1}^{M}(a_i-E(a))(b_i-E(b))$$

تُشير a و b إلى قيم اثنتين من البكسلات المتجاورة، فيما تُعبر E(a) و E(b) عن متوسط جوار البكسلين على التتالي، و M عن عدد البكسلات المتجاورة في الصورة، حيث تُحسب M تلقائياً عند التنفيذ العملي باستخدام مكتبة Numpy.



الشكل (9): مخططات الارتباط بمختلف الاتجاهات لصورة DICOM_1 قبل التشفير (a) وبعد التشفير (b)

يُظهر الجدول (1) قيم معايير الحماية لمجموعة من صور DICOM في مجموعة البيانات، حيث تُشير المعايير HC (Horizontal Correlation) و VC (Vertical Correlation) و(Diagonal Correlation) DC إلى مُعاملات الارتباط الأفقية والعمودية والقطرية على التتالي، والتي تُحسب وفق المعادلات (20) السابقة.

الجدول (1): نتائج اختبار معايير الحماية لعينات من صور DICOM المُشفرة

DICOM Images	NPCR	UACI	Entropy	Correlation Coefficients HC	VC	DC	PSNR
DICOM-1	99.95	33.22	7.9997	0.0007	− 0.0034	0.0246	5.364
DICOM-2	99.92	33.39	7.9999	- 0.0163	0.0026	0.0024	4.527
DICOM-3	99.99	33.29	7.9992	0.0271	−0.0031	0.0017	5.461
DICOM-4	99.93	33.33	7.9990	0.0029	−0.0121	0.0031	6.162
DICOM-5	99.98	33.41	7.9997	0.0252	0.0233	0.0059	7.008

ويُظهر الجدول (2) مقارنةً بين القيم المتوسطة لأهم معايير الاختبار بين التقنيات الحالية والمخطط المُقترح عبر تطبيقها على مجموعة الصور ذاتها [38-37].

الجدول (2): مقارنة القيم المتوسطة لمعايير الحماية بين المخطط المُقترح والتقنيات الحالية

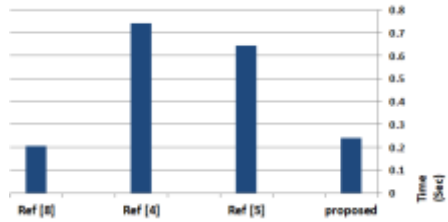
	NPCR	UACI	Entropy	Correlation Coefficients HC	VC	DC	PSNR (dB)
Ref [2]	99.6	33.5	7.9994	0.00931	0.01036	0.00498	−
Ref [3]	99.606	33.47	7.9976	0.00163	0.00065	0.00225	Infinity
Ref [4]	99.62	33.20	7.9996	0.0037			-
Ref [5]	−	−	(16 bits) 15.9815	0.0275	- 0.0027	0.018	7.084
Ref [6]	99.99	26.03	7.9993	0.0374	0.0007	−0.0377	73.475
Ref [7]	−	−	−	−	−	−	−

Ref [8]	~100	93.3	15.08 (16 bits)	0.000088			16.13
Proposed	**99.95**	**33.26**	**7.9993**	**0.0082**	**−0.0031**	**0.0019**	**5.572**

تُشير القيم السالبة لمُعاملات الارتباط في اتجاه مُعين إلى أن علاقة الارتباط بين البكسلات المتجاورة عكسية في هذا الاتجاه، حيث تُأخذ قيم هذا المعيار وفق القيمة المُطلقة لتكون أمثلية كلما اقتربت من الصفر، فيما تُحقق مخططات التشفير المثالية قيم PSNR أقل من 10 dB [5]، مما يُظهر تفوقاً واضحاً للمخطط المُقترح، حيث تتوافق قيمتها الأقل مع قيمة أعلى للتباين بين الصورة الأصلية والمشفرة مما يُحقق جودة التشفير.

5-6 زمن التشفير:

يُظهر الشكل (10) مقارنةً بين زمن التشفير للتقنيات الحالية عبر منصة المعالجة ذاتها (Google Colab) وباستخدام نفس المواصفات، ويُشير لتفوق كبير للمخطط المُقترح والبحث [8] مقارنةً مع الأبحاث الأخرى، مع أفضلية للبحث [8] بمقدار 12.5%، فيما لم توفر الأبحاث الأخرى معلومات عن زمن التشفير.



الشكل (10): مقارنة زمن التشفير الكلي مع التقنيات الحالية

5-7 مناقشة النتائج:

تُظهر اختبارات المعيار NPCR تقارباً لقيم مخطط التشفير المُقترح مع البحثين [6] و[8]، إذ تتراوح القيم ضمن المجال [100 - 99.9]، متفوقةً على الأبحاث الأخرى نسبياً، بينما تُظهر اختبارات المعيار UACI تقارباً عاماً في القيم، باستثناء البحث [8]، وبمقارنة قيم تحليل الانتروبي، حققت جميع الأبحاث قيماً قريبة جداً من القيم المثالية (وفقاً لعمق البت)، في حين حقق البحث [8] قيمة أقل نسبياً. أما فيما يتعلق باختبارات المعيار PSNR، فقد حقق المخطط المُقترح أفضل نتيجة مقارنةً مع الأبحاث [5] [8]، حيث تجاوزت قيمة هذا المعيار dB 10 في البحث [8]، وهي القيمة التي تُعتبر بمثابة عتبة لاينبغي تجاوزها، فيما لم تُظهر بعض الأبحاث نتائج

هذا المعيار، واستخدمته الأبحاث [3] [6] كمعيار بين الصورة الأصلية والصورة الناتجة عن فك التشفير، في حين حققت جميع التقنيات الحالية قيم أمثلية لمُعاملات الارتباط في الاتجاهات الثلاث. ويُمكن تفسير القيم السلبية لبعض معايير التقييم في البحث [8] بتركيزه بشكل أساسي على تخفيض الزمن دون تحقيق متطلبات الحماية الكافية نتيجةً لاستخدام خوارزمية AES التي أثبتت الأبحاث عدم ملاءمتها للصور.

6- التوصيات:

اختبرنا في هذا البحث مخطط تشفير مُقترح لصور DICOM عبر خوارزميات متفاوتة التعقيد وفقاً لأهمية البيانات المُعالجة. في مناطق الاهتمام المُستخرجة، تم استخدام نموذج هجين يستخدم مرحلة خلط مزدوجة لتحقيق عمليات التبديل على مستويي البت والبكسل معاً، يعمل على الجمع بين خريطة Henon ونموذج المسح Y-Index، ومن ثم دمجها مع نسخة مطورة من خوارمية RC4، بينما تُستخدم خوارزمية تشفير سريعة ومنخفضة التعقيد في خلفية الصورة، مع تأمين حماية لبيانات المريض المُتضمنة في الصور باستخدام نسخة مُحسنة من خوارزمية AES، بزمن معالجة قدره 0.2382 ثانية ومُعاملات ارتباط للصورة المشفرة تبلغ 0.0082 و0.0031− و0.0019، وفق الاتجاهات الأفقية والعمودية والقطرية على التتالي.

استطاع المخطط المُقترح تخفيض زمن التشفير دون التفريط بمتطلبات الحماية الضرورية، حيث تجاوز اختبارات الحماية بنسب قريبة من القيم المثالية للمعايير PSNR وNPCR وUACI، وكذلك تحليل الهيستوغرام ومعاملات الارتباط وقيمة الانتروبي، حيث نهدف مُستقبلاً لمقارنة فعالية استخدام طرق تجزئة أخرى لاستخراج مناطق الاهتمام، واختبار توظيف خوارزميات أسرع في خلفية الصورة.

References

1-CLUNIE, D.A., 2021. **DICOM Format and protocol standardization—a core requirement for digital pathology success**. *Toxicologic Pathology*, *49*(4), pp.738-749.

2-MORTAJEZ, S., TAHMASBI, M., and JAMSHIDNEZHAD, A., 2020**. A novel chaotic encryption scheme based on efficient secret keys and confusion technique for confidential of DICOM images.** Informatics in Medicine Unlocked, 20, p.100396.

3- AASHIQ BANU, S. and AMIRTHARAJAN, R., 2020**. Tri-level scrambling and enhanced diffusion for DICOM image cipher-DNA and chaotic fused approach.** *Multimedia Tools and Applications*, pp.28807-28824.

4-BOUSSIF, M., AND CHERIF, A., 2020**. Securing DICOM images by a new encryption algorithm using Arnold transform and Vigenère cipher**. *IET Image Processing*, *14*(6), pp.1209-1216.

5- MANIKANDAN, V. and AMIRTHARAJAN, R., 2022. **A simple embed over encryption scheme for DICOM images using Bülban Map**. *Medical & Bio Engineering & Computing*, pp.701-717.

6- JOHN, S. and KUMAR, S.N., 2023. **2d lorentz chaotic model coupled with logistic chaotic model for medical image encryption: Towards ensuring security for teleradiology.** *Procedia Computer Science*, *218*, pp.918-926.

7- Al-RAWI, M.F., ABBOUD, I.K. and AL-AWAD, N.A., 2023. **Digital Medical Images Encryption Approach in Real Time Applications.** International Journal of Open Information Technologies, 11(9), pp.24-27.

8- NATSHEH, Q., SĂLĂGEAN, A., ZHOU, D. and EDIRISINGHE, E., 2023**. Automatic Selective Encryption of DICOM Images.** *Applied Sciences*, *13*(8), p.4779.

9- BANU S, A. and AMIRTHARAJAN, R., 2020**. A robust medical image encryption in dual domain: chaos-DNA-IWT approach.** *Medical & biological engineering & computing*, *58*, pp.1445-1458.

10- MENG, X., Li, J., Di, Y. and JIANG, D., 2022**. An Encryption Algorithm for Region of Interest in Medical DICOM Based on One-Dimensional eλ-cos-cot Map**. *Entropy*, *24*(7), p.901.

11- RULANINGTYAS, R. and AIN, K., 2021. **CT scan image segmentation based on hounsfield unit values using Otsu thresholding method**. In *Journal of Physics:* Vol. 1816, p. 012080.

12- SALECK, M.M., M.O.M., MAHMOUD, E.B.M. and RMILI, M., 2022**. Otsu's Thresholding for Semi-Automatic Segmentation of Breast Lesions in Digital Mammograms.** *International Journal of Advanced Computer Science and Applications*, *13*(10).

13- PRIYANKA and SIN, K., 2023. **A survey of image encryption for healthcare applications.** *Evolutionary Intelligence*,pp.801-818.

14- LI, Y. and GE, G., 2019. **Cryptographic and parallel hash function based on cross coupled map lattices**. *Multimedia Tools and Applications*, *78*, pp.17973-17994.

15- SHAHNA,and MOHAMED, A., 2020**. A novel image encryption scheme using both pixel level and bit level permutation with chaotic map.** Applied Soft Computing, 90, p.106162.

16- DEB, S ., BHUYAN, B., KAR, N., and REDDY, K.S., 2022. **Colour image encryption using an improved version of stream cipher and chaos**. Int. J. Ad Hoc Ubiquitous Comput., 2 ,118–133.

17- RAN, W., WANG, E. and TONG, Z., 2022**. A double scrambling-DNA row and column closed loop image encryption algorithm based on chaotic system**. *Plos one*, *17*(7), p.e0267094.

18- NIU, Y. and ZHANG, X., 2020**. An Effective Image Encryption Method Based on Space Filling Curve and Plaintext-Related Josephus Traversal**. IEEE Access, 8, pp.196326-196340.

19- MAZHER, A.N., WALEED, J. and MAOLOOD, A.T., 2021**. Developed Lightweight Cryptographic Algorithms for The Application of Image Encryption:** A Review. *Journal of Al-Qadisiyah for computer science and mathematics*, *13*, pp.Page-11.

20- JIAO, L., HAO, Y. and FENG, D., 2020**. Stream cipher designs: a review.** Science China Information Sciences, 63, pp.1-25.

21- TAHA, Z.K., ALTURFI, M.N., ALBAKER, and Ali, A.S., 2019**. Robust and Secured Image Steganography using Improved LSB and RC4 Cryptography with Preprocessing Operation.** *Internation Journal of Recent Technology and Engineering,8*.

22- FADHIL, M., RACHMANTO, E.H., RIZQA, I. and SETYONO, A., 2019**,** September**. Secure reversible data hiding in the medical image using histogram shifting and RC4 encryption.** In *2019 International Seminar on Application for Technology of Information and Communication (iSemantic)* (pp. 1-6). IEEE.

23- SUSANTO, SARI, C.A., and SAZAL, M.R., **2020. Triple layer image security using bit-shift, chaos, and stream encryption**. *Bulletin of Electrical Engineering and Informatics*, *9*(3 pp.980-987.

24- KUMAR, A and SINGH S., 2022**. A robust encryption scheme using RC4 and Arnold's Chaotic Map. YMER,** PP.448-454.

25- JASSIM, S.A. and FARHAN, A.K., 2021**,** April**. A survey on stream ciphers for constrained environments.** In 2021 1st Babylon International Conference on Information Technology and Science (BICITS) (pp. 228-233). IEEE.

26- SAHA, R., GEETHA, G., KUMAR, G., KIM, T.H. and BUCHANAN, W.J., 2019**. MRC4: a modified rc4 algorithm using symmetric random function generator for improved cryptographic features.** *IEEE Access*, *7*, pp.172045-172054.

27- KAREEM, S.M. and RAHMA, A.M.S., 2020**. A modification on key stream generator for RC4 algorithm.** *Engineering and Technology Journal*, *38*(2), pp.54-60.

28- GAFFAR, A., JOSHI, A.B., KUMAR, D. and MISHRA, V.N., 2021**. Image Encryption Using Nonlinear Feedback Shift Register And Modified Rc4a Algorithm.** *Journal of applied mathematics & informatics*, *39*(5_6), pp.859-882.

29- DENG, L.Y., BOWMAN, D., YANG, C.C. and LU, H.H.S., 2021**. Extending RC4 to construct secure random number generators.** *Annual Modeling and Simulation Conference* (pp. 1-12). IEEE.

30- AMINUDIN, A. and NURYASIN, I., 2022**,** July**. Modification of RC4 algorithm utilizing the two-state table and initial state factorial.** In *AIP Conference Proceedings* (Vol. 2453, No. 1).

31- SHARMA, P. and SABHARWAL, H., 2020**. A new image encryption using modified aes algorithm and its comparision with AES.** *International Journal Of Engineering Research & Technology*, *9*(8), pp.194-197.

32- TENG, L., LI, H., and SUN, Y., 2020**. A Modified Advanced Encryption Standard for Data Security.** *Secur.22*(1), pp.112-117.

33- MOHD, N.A.A. and ASHAWESH, A.Y.A., 2021**,** February**. Enhanced AES algorithm based on 14 rounds in securing data and minimizing processing time.** In *Journal of Physics: Conference Series* (Vol. 1793, No. 1, p. 012066). IOP Publishing.

34- ABDUL HUSSIEN, F.T., RAHMA, A.M.S. and ABDUL WAHAB, H.B., 2021**. A secure environment using a new lightweight AES encryption algorithm for e-commerce websites.** *Security and Communication Networks*, *2021*, pp.1-15.

35-MISHRA, Z. and ACHARYA, B., 2023. **High throughput compact area architecture of XXTEA for IoT application**. Sādhanā, 48, pp.1-7.

36-NATSHEH, A., 2019. **Securing DICOM images through automatic selective encryption** *(Doctoral dissertation, Loughborough University)*.

37-https://www.kaggle.com/abhishek/siim-dicom-images

38- https://www.kaggle.com/datasets/washingtongold/lidcidri30