مجلة جامعة طرطوس للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (6) العدد(8) 2022
Tartous University Journal for Research and Scientific Studies - engineering Sciences Series Vol. (6) No. (8) 2022

تحسين أداء معيار التشفير المتقدم المصمم باستخدام الشبكات العصبونية بالاعتماد على شبكات الخصومة التوالدية

د. راغب طعمه*

علي فواز محمود**

(تاريخ الإيداع 7/8 /2022 . قُبِل للنشر في 2022/9/11)

□ ملخّص□

مع تقدم التكنلوجيا في مختلف جوانب الحياة و تسارع تبادل البيانات بين المستخدمين عبر شبكة الانترنت ، حيث يتم ارسال و استقبال حجم هائل من البيانات المختلفة بشكل يومي و ظهور العديد من المخاطر الأمنية التي تهدد أمن هذه البيانات و خصوصية المستخدمين ، كل ذلك أدى الى تزايد الاهتمام في مجال أمن المعلومات و تشفير البيانات المتبادلة عبر وسائل التواصل الاجتماعي باستخدام عدة تقنيات و خوارزميات تشفير و مؤخرا دخل الذكاء الصناعي و بالأخص الشبكات العصبونية في مجال الأمن و تشفير البيانات و المحافظة على سرية الاتصال بين المستخدمين . في هذا البحث تم الاعتماد على الشبكات العصبونية (الشبكات الخصومة التوالدية) لتصميم نظام يقوم بتشفير و فك تشفير الصور مع تحسين في الزمن المستغرق لكل من عمليتي التشفير و فك التشفير و دقة الصورة الناتجة بعد عملية فك التشفير .

الكلمات المفتاحية :التشفير ، أمن المعلومات ،شبكات عصبونية، شبكات الخصومة التوالدية ، معيار التشفير المتقدم .

* مدرس في قسم هندسة تكنولوجيا المعلومات – كلية هندسة تكنولوجيا المعلومات و الاتصالات – جامعة طرطوس –سوريا

** طالب ماجستير في قسم هندسة تكنولوجيا المعلومات – كلية هندسة تكنولوجيا المعلومات و الاتصالات – جامعة طرطوس –سوريا

مجلة جامعة طرطوس للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (6) العدد(8) 2022
Tartous University Journal for Research and Scientific Studies - engineering Sciences Series Vol. (6) No. (8) 2022

Improving performance of an advanced encryption standard designed using neural networks using generative adversarial networks

Dr.Ragheb Toemeh*
Ali Fawaz Mahmoud**

(Received 7/8/ 2022 . Accepted 11/9/ 2022)

□ ABSTRACT

With the advancement of technology in various fields of life and the acceleration of data exchange between users over the Internet, where a huge volume of different data is sent and received on a daily basis and the emergence of many security risks that threaten the security of this data and the privacy of users, all of this has led to increased interest In the field of information security and encryption of data exchanged through social media using several techniques and encryption algorithms. Recently, Artificial Intelligence, especially neural networks, entered the field of data security and encryption and maintaining the confidentiality of communication between users. In this research, neural networks (generative adversarial networks) have been relied on to design a system that encrypts and decrypts images with an improvement in the time taken for both the encoding and decoding processes and the accuracy of the resulting image after the decoding process.

Key Words : Encryption , Information security , Neural Networks , generative adversarial networks , Advance Encryption Standard

* Teacher, Information Technology Engineering Department, Information and communication Technology Engineering, Tartous University, Syria
** Master student, Information Technology Engineering Department, Information and communication Technology Engineering, Tartous University, Syria

1. المقدمة :

تطورت الخوارزميات و التقنيات المستخدمة في عملية تشفير البيانات و ذلك نظرا لتزايد المخاطر الأمنية التي تهدد البيانات على شبكة الانترنت عامة و وسائل التواصل الاجتماعي خاصة ، و تزايد دور الذكاء الصناعي في تأمين البيانات المختلفة (صورة ، صوت ، نص ، .....) محليا أو عبر الانترنت لجميع البرامج و التطبيقات و ذلك لكسب ثقة مستخدمي تلك البرامج في المحافظة على سرية بياناتهم .

يعتبر معيار التشفير المتقدم / AES/ من أقوى خوارزميات التشفير المستخدمة في تشفير و حماية مختلف أنواع البيانات ، حيث يتم استخدام خوارزمية AES بتشفير الصور المتبادلة بين المستخدمين عبر مختلف تطبيقات التواصل الاجتماعي ، كما أنها تستخدم في تشفير كلمة المرور و جميع تدفقات البيانات في بعض الشبكات العسكرية و المدنية [1]، و تعد الشبكات العصبونية من أحدث التقنيات المستخدمة في مجال أمن المعلومات و التشفير ، حيث أنها استخدمت في عدة أبحاث لتحل مكان خوارزمية التشفير بشكل كامل أو لتوليد مفتاح التشفير ، و بجميع الحالات قدمت تحسين في أداء عملية التشفير سواء من حيث زمن التشفير / فك التشفير أو قوة التشفير [2] .

قامت العديد من الأبحاث و الدراسات باستخدام الشبكات العصبونية بمختلف أنواعها لتحسين عمل خوارزمية ال AES و استبدال العمليات الرياضية ضمن الخوارزمية بطبقات الشبكة العصبونية .

قام الباحثZhenlong Man [3] ببناء شبكة عصبونية التفافية /CNN/ مكونة من أربع طبقات و كل طبقة مكونة من 256 عصبون ، و من ثم تدريب الشبكة على مجموعة تدريب و هي عبارة عن الصور المعيارية المستخدمة في مجال معالجة الصورة حيث قدمت سرعة متوسطة في عمليتي التشفير و فك التشفير (1 ثانية).

وقام الباحث Yasin Kh. Yasin [4] باقتراح نموذج شبكة عصبونية ذات انتشار امامي مكون من 5 طبقات مخفية بالإضافة لطبقتي الدخل و الخرج ، و من ثم تدريب النموذج بحيث يصل لأقل خطأ ممكن (Bit error) و مع ذلك حدث اختلاف في قيم البيكسلات بين الصور قبل التشفير و الصورة بعد فك التشفير .

اقترح الباحث AMEEN S [5] بناء أربع شبكات عصبونية ، بحيث كل شبكة من الشبكات المقترحة تحل مكان مرحلة من مراحل خوارزمية ال AES الأربعة . قدم هذا المقترح قوة عالية لعملية التشفير و زاد من تغيير قيم بيكسلات الصورة بعد عملية التشفير و لكن كان ذلك على حساب الزمن المستغرق

استخدمت جميع الدراسات السباقة الشبكات العصبونية المتعارف عليها أنها تستخدم لعمليات التصنيف و هذا يؤدي إلى عدم الحصول كفاءة جيدة في عملية التشفير كون الشبكات العصبونية غير مخصصة لتعطي على خرجها صور و إنما تعطي تصنيف للصور ، بينما تقدم الدراسة المقترحة آلية تشفير معتمدة على شبكات الخصومة التوالدية و شبكات الخصومة التوالدية مخصصة لإنشاء الصور .

2. أهمية البحث و أهدافه :

تكمن أهمية البحث كونه يقدم مساهمة قيمة في مجال تشفير و فك تشفير الصور عن طريق بناء نظام معتمد على شبكات الخصومة التوالدية و هي نوع من أنواع الشبكات العصبونية الحديثة و التي تتكون من شبكتين عصبونيتين الشبكة الأولى مسؤولة عن تشفير / فك تشفير الصور و الشبكة الثانية عبارة عن شبكة عصبونية التفافية للتصنيف مهمتها تدريب و تحسين دقة الشبكة الأولى [6] ، و تأتي أهمية البحث في تحديد البنية الأساسية لكل من شبكة المولد و شبكة المميز في كل من مرحلتي التشفير و فك التشفير بحيث تعطي أفضل أداء من حيث الزمن

المستغرق في التشفير / فك التشفير و دقة الصورة الناتجة بعد فك التشفير ، و تظهر الأهمية الرئيسية للبحث في إمكانية تعميم هذا النظام بحيث يؤدي عمل مختلف أنواع خوارزميات التشفير مثل معيار تشفير البيانات DES و معيار التشفير المتقدم AES أو أي نوع من أنواع خوارزميات التشفير المتعارف عليها .

3. طرائق البحث و مواده :

يعتمد البحث على شبكات الخصومة التوالدية لبناء كل من نظامي التشفير و فك التشفير ، حيث أن شبكات الخصومة التوالدية تعتبر نوع من أنواع الشبكات العصبونية التي تم اقتراحها حديثا و التي تستخدم في تطبيقات توليد الصور و تحسين جودة الصورة أو إعادة بناءها . تتكون شبكة الخصومة التوالدية من جزأين و كل جزء عبارة عن شبكة عصبونية ، الشبكة الأولى هي شبكة المولد و هي المسؤولة عن توليد الصور المشفرة / الصور بعد فك التشفير و الشبكة الثانية هي شبكة المميز و هي المسؤولة عن تحسين خرج شبكة المولد [6]. تم استخدام بلوكات صور ملونة بأبعاد 256x256 لعملية تدريب الشبكة العصبونية بحيث تكون دخل لشبكة المولد و تم تشفير هذه البلوكات باستخدام خوارزمية التشفير AES-256 لاستخدامها في تدريب شبكة المميز . تم استخدام لغة البرمجة بايثون لكتابة التعليمات الخاصة ببناء الشبكة العصبونية المكونة للنظام و تم تطبيق التعليمات و الحصول على النتائج باستخدام منصة العمل CoLab و هي منصة عمل مجانية مقدمة من غوغل تتيح للباحثين تنفيذ أكواد البايثون مع تقديم قدرة معالجة عالية لمجالات تعلم الآلة التي تطلب ذوكر عالية و معالج رسومي / كرت شاشة عالي .

3-1- مجموعة بيانات التدريب Training Data Set :

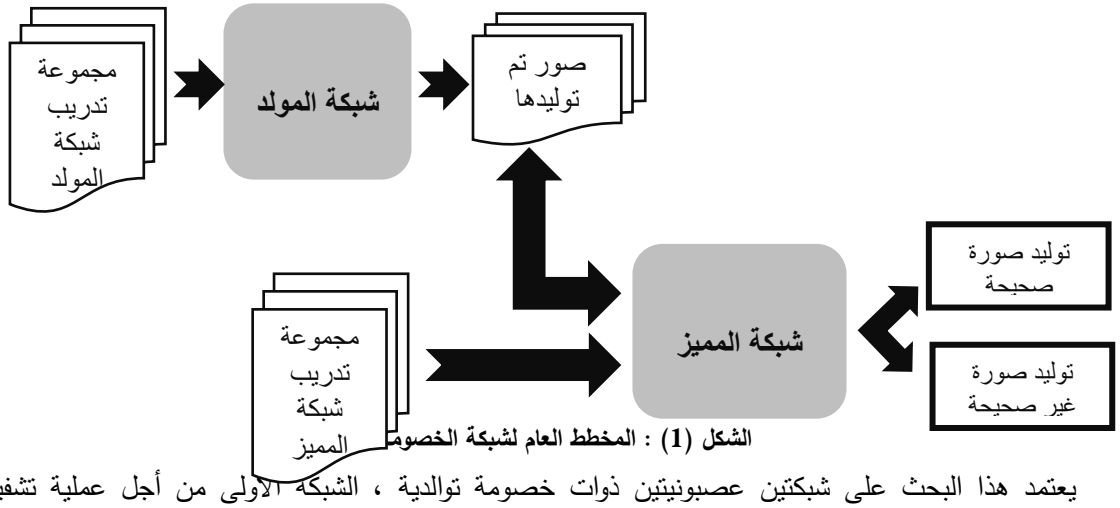
مجموعة البيانات عبارة عن صور ملونة عددها 20 صور أبعادها 3×256×256 وهي صور مختلفة و شائعة في مجال معالجة الصورة ، تم ترميزها باستخدام معيار ترميز و ضغط الصور Jpeg و تقسم هذه المجموعة بنسبة 50% منها لتدريب شبكة المولد أي 10 صور و هي عبارة عن الصور قبل التشفير و 50% لتدريب شبكة المميز و هي نفس الصور المستخدمة لتدريب شبكة المولد و لكن بعد تشفيرها باستخدام خوارزمية التشفير AES-256 ، و تم اختيار النسب السباقة كونها النسب المتعارف عليها لتدريب شبكة الخصومة اتوالدية.

صيغة الصورة	أبعاد الصورة	نوع الصورة
Jpeg	256x256	ملونة (RGB)

3-2- شبكات الخصومة التوالدية Generative Adversarial Networks:

شبكات الخصومة التوالدية نوع من أنواع الشبكات العصبونية الصناعية و هي نموذج تم اقتراحه من قبل الباحث Ian J.Goodflelw في جامعة مونتريال عام 2014 [6] و قدمت نقلة نوعية في مجالات معالجة الصور ، توليدها ، تحسين جودتها و إعادة بنائها . فشبكات الخصومة التوالدية حالها حال الشبكات العصبونية الصناعية كلاهما يحاكي عمل الشبكة العصبية للإنسان من ناحية القدرة على المعالجة و التعلم و اتخاذ القرارات و توليد البيانات بناء على نموذج رياضي و برمجي ، ولكن شبكة الخصومة التوالدية تتكون في الواقع

من شبكتين عصبونيتين لكل منهما عمل محدد هما شبكة المولد Generator و شبكة المميز Discriminator يبين الشكل (1) المخطط العام لشبكة الخصومة التوالدية.



الشكل (1) : المخطط العام لشبكة الخصومة

يعتمد هذا البحث على شبكتين عصبونيتين ذوات خصومة توالدية ، الشبكة الأولى من أجل عملية تشفير الصور و تتكون بدورها في بنيتها الداخلية من شبكتين التفافيتين CNN لكل من المولد و المميز حيث أن شبكة المولد لها طبقة دخل و خرج بحجم 256x256x3 و 7 طبقات مخفية بينما شبكة المميز عبارة عن شبكة التفافية بطبقة دخل حجمها 256x256x3 و طبقة خرج بمخرج وحيد هو إما 0 أو 1 و بنية متعاقبة من الطبقات الالتفافية بهدف تصنيف / كشف الصور الصحيحة من الصور الغير صحيحة . بينما شبكة الخصومة الثانية من أجل عملية فك التشفير تتكون أيضا من نفس البنى السابقة و لكن يختلف الدخل المقدم لكل من شبكة المولد و شبكة المميز.

3-2- معيار التشفير المتقدم Advanced Encryption Standard:

معيار التشفير المتقدم (AES) ، والمعروف أيضًا باسم طريقة تشفير Rijndael في التشفير ، هو معيار تشفير كتلي اعتمدته الحكومة الفيدرالية الأمريكية. يستخدم هذا المعيار ليحل محل DES الأصلي ، الذي تم تحليله من قبل العديد من الأطراف واستخدامه على نطاق واسع في جميع أنحاء العالم. بعد عملية اختيار مدتها خمس سنوات تم نشر معيار التشفير المتقدم بواسطة المعهد الوطني للمعايير والتكنولوجيا (NIST) في 26 نوفمبر 2001 وأصبح معيارًا فعالًا في 26 مايو 2002. و هنالك ثلاثة أنواع من خوارزميات التشفير AES و تصنف حسب طول مفتاح التشفير وفق الجدول الآتي :

الجدول -1- يوضح أنواع خوارزمية ال AES

الاسم	طول المفتاح
AES-128	128 بت
AES-192	196 بت
AES-256	256 بت

ير

أيضا وفق الجدول الآتي :

الجدول -2- يوضح عدد الدورات في خوارزمية ال AES

عدد الدورات	طول المفتاح
10 round	128 بت
12 round	196 بت
14 round	256 بت

256 بت و

لكنها تحتاج لزمن تنفيذ أكبر كونها تحتاج لعدد دورات تنفيذ هو 14، بينما خوارزمية AES−128 تعد الأسرع في عملية التشفير و فك التشفير من الخوارزميتين السابقتين كون المفتاح المستخدم طوله 128 بت و عدد دورات تنفيذ الخوارزمية أقل و هو 10 [1] .

3−3− الخوارزمية المقترحة:

تم في هذا البحث تطوير نظام تشفير / فك تشفير باستخدام تقنيات تعلم الآلة (الشبكات العصبونية العميقة) و ذلك عن طريق تدريب شبكتين عصبونيتين من نوع الخصومة التوالدية واحدة للتشفير في طرف المرسل و الثانية لفك التشفير في طرف المستقبل و تحديد نوع البيانات التي سيتم تشفيرها على أنها صور ملونة وفق المراحل الأتية :

- ✓ بناء و تدريب شبكة الخصومة التوالدية الخاصة بعملية التشفير .
- ✓ بناء و تدريب شبكة الخصومة التوالدية الخاصة بعملية فك التشفير .

3−3−1− بناء و تدريب شبكة التشفير :

في هذه الخطوة يوجد عدة مراحل للوصول لبنية النظام المستخدم في عملية التشفير بدء من مرحلة تجهيز بيانات التدريب انتهاء بمرحلة الاختبار و الحصول على النتائج و نلخص المراحل كما يلي :

- تجهيز بيانات التدريب .
- بناء الشبكة العصبونية .
- تدريب الشبكة العصبونية و اختباراها .

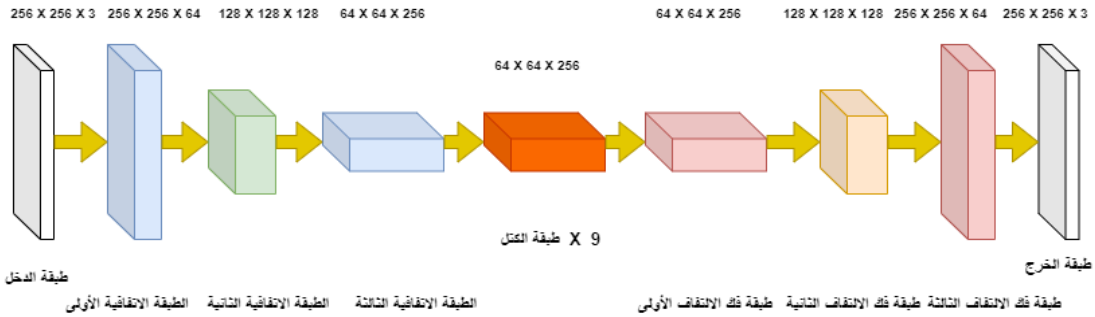
تجهيز بيانات التدريب : في هذه المرحلة يتم تجهيز مجموعتي بيانات / Dataset و ذلك كون شبكة الخصومة التوالدية المستخدمة في عملية التشفير تتكون من شبكتين عصبونيتين ، حيث من أجل شبكة المولد تكون بيانات التدريب عبارة عن الصور الحقيقية قبل تشفيرها ، و يتم ضبط أبعاد جميع الصور الى (256 x 256) لتصبح مناسبة لأن تكون دخل لشبكة المولد ، أما بالنسبة لشبكة المميز فإن مجموعة التدريب هي الصور الحقيقة نفسها المستخدمة في تدريب المولد و لكن بعد أن يتم تشفيرها باستخدام خوارزمية ال AES− 256 .

بناء و تدريب الشبكة العصبونية : في هذه المرحلة سيتم إنشاء شبكة خصومة ، في بنتيها الداخلية تتكون من شبكتين عصبونيتين الشبكة الأولى لعملية توليد الصور و هي عبارة عن شبكة عصبونية التفافية CNN مكونة من طبقتي دخل وخرج و سبع طبقات مخفية ، حيث تم استخدام الطبقات الالتفافية و طبقات فك الالتفاف و تم الاستغناء عن طبقات الاقتراع كون طبقة الاقتراع تقوم بتقليل دقة قيم بيكسلات الصورة و أيضا تم الاستغناء عن طبقة الاتصال الكامل كما هو موضح في الشكل (1) ، أما بالنسبة لتوابع التنشيط المستخدمة في طبقات شبكة المولد تم استخدام تابع التنشيط ReLU بالنسبة لكل طبقات الشبكة ما عدا طبقة الخرج تم استخدام تابع التنشيط Tanh و الفكرة من استخدام تابع التنشيط / النقل ReLU كونه تابع تنشيط يعطي أداء عالي من حيث دقة قيم خرج الطبقة في الشبكة العصبونية بالإضافة الى أنه يخفض زمن التدريب و المعالجة ضمن الشبكة و يعطى تابع ال ReLU بالعلاقة (1) بينما تابع Tanh يستخدم في تطبيقات شبكات توليد الصور كونه يعطي قيم خرج ضمن المجال [1،−1] .

$$F(x) = \max(0,x) \qquad \textbf{(1)}\ [5]$$

$$\tanh(x)=2\cdot\sigma(2x)-1 \quad : \sigma(x)=ex / (1 + ex) \qquad \textbf{(2)}\ [5]$$

أما فيما يخص شبكة المميز فهي مكونة من طبقة دخل و طبقة خرج و أربع طبقات مخفية ذات انتشار أمامي و لا تحتوي أي تغذية عكسية و بتابع تنشيط لكل الطبقات LeakyReLU و هو تابع يعمل نفس عمل تابع ReLU ولكن يسمح بتمرير بعض القيم السالبة صغيرة القيمة [4].



الشكل (2) : بنية شبكة توليد الصورة المشفرة

بعد بناء شبكة التشفير و تجهيز بيانات / صور الدخل لكل من شبكة المولد و شبكة المميز تتم عملية تدريب الشبكة وفق المراحل الآتية :

- تدريب شبكة المميز على صور مشفرة حقيقة باستخدام خوارزمية ال AES للصور المراد تشفيرها .
- توليد صور مشفرة غير حقيقية باستخدام شبكة المولد بناء على الدخل المقدم لها و هو الصور قبل تشفيرها.
- تدريب شبكة المميز مرة أخرى على الصور التي تم توليدها من قبل المولد بحيث تصبح قادرة على التمييز بينها و بين الصور المشفرة الحقيقة.
- تدريب شبكة المولد بناء على خرج شبكة المميز مع تثبيت أوزان الطبقة الأولى كون قيم الأوزان هي مفتاح التشفير .
- حساب تابع الخطأ لكل من شبكة المميز و المولد وفق المعادلات الرياضية الآتية :

❖ تابع الخطأ Loss Function لشبكة المولد يعطى بالعلاقة 3 :

$$E_g = \frac{1}{m}\sum_{i=1}^{m}\log\left(1 - D\left(G\left(z^{(i)}\right)\right)\right) \quad (3) \quad [8]$$

θ هي نسبة التعلم **g** حيث أن Generatorتعبر العلاقة السابقة عن قيمة الخطأ في خرج شبكة المولد هي احتمالية أن المولد وصل للدقة المطلوبة في الصور المولدة . **G(z)**لشبكة المولد و

❖ تابع الخطأ Loss Function لشبكة المميز :

$$E_d = \nabla_{\theta_d}\frac{1}{m}\sum_{i=1}^{m}\left[\log D\left(x^{(i)}\right) + \log\left(1 - D\left(G\left(z^{(i} \quad (4) \quad [8]$$

تعبر العلاقة السابقة عن قيمة الخطأ في خرج شبكة المميز حيث أن θ_d هي نسبة التعلم لشبكة المولد و **log(D(x))** هي احتمالية أن المميز نجح في تمييز الصور المولد من الصور الحقيقية و **log(1− D(G(z)))** و هو خطأ شبكة المولد [4].

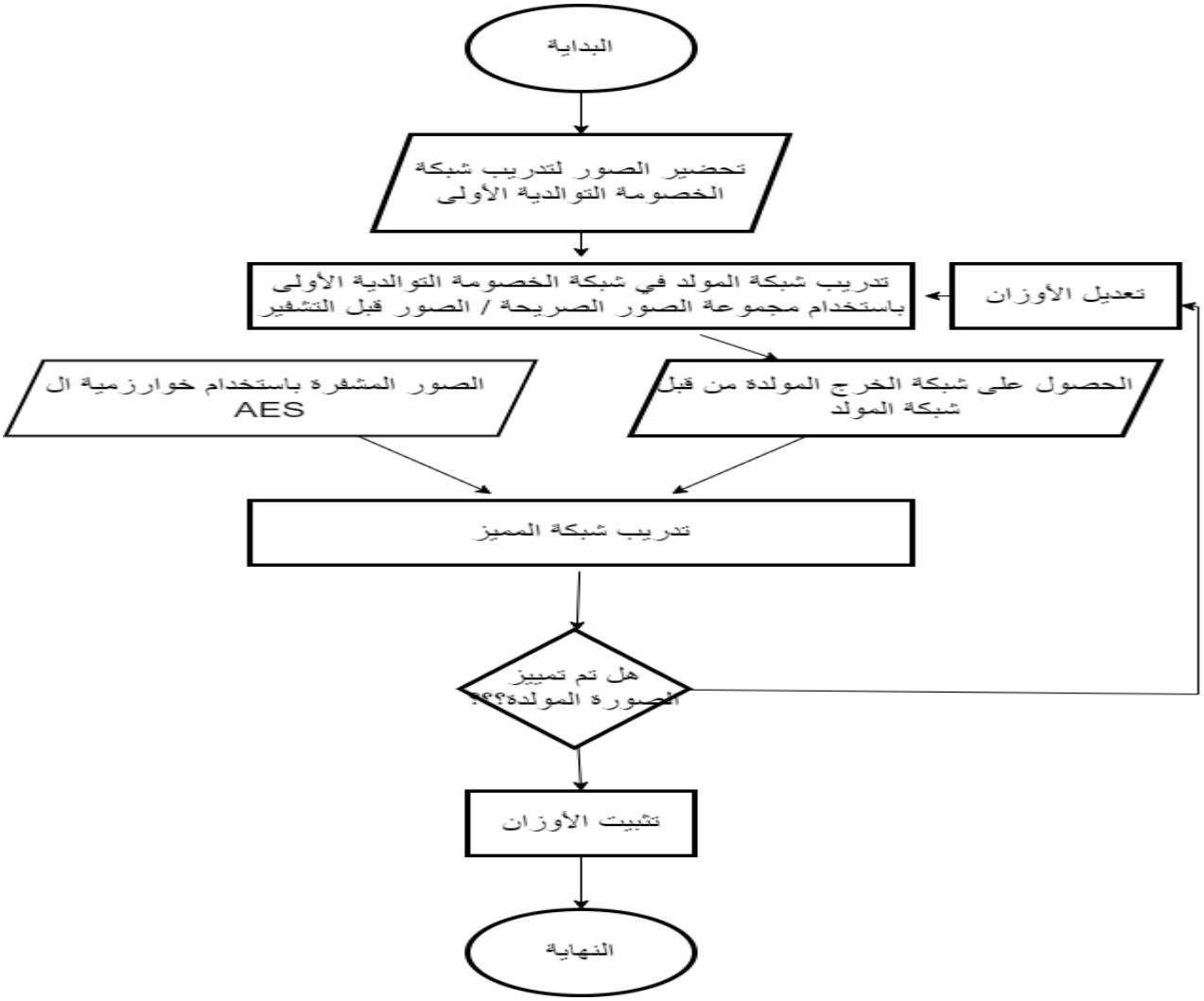
❖ تابع الخطأ بالنسبة لشبكة الخصومة التوالدية GAN المسؤولة عن التشفير يعطى بالعلاقة :

$$\min_G \max_D V(D,G)$$

$$V(D,G) = \mathbb{E}_{x\sim p_{data}(x)}[\log D(x)] + \mathbb{E}_{z\sim p_z(z)}[\log(1 - D(G(z) \quad (5) \quad [8]$$

حيث أننا نسعى جعل قيمة خطأ شبكة المولد أصغر ما يمكن و قيمة خطأ شبكة المميز أكبر ما يمكن و قيمة خطأ الشبكتين تتناسبان طردا [8].

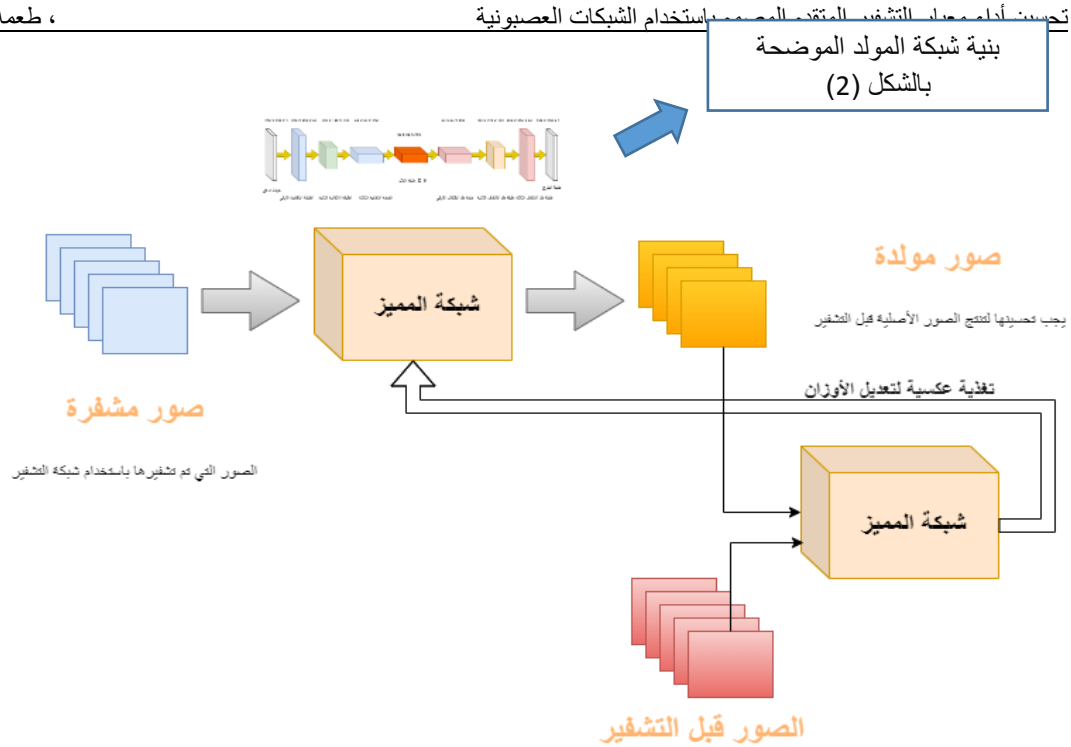
و بناء على ما سبق نلخص مراحل تدريب شبكة التشفير وفق المخطط الآتي :



الشكل (3) : المخطط العام لمراحل تدريب شبكة التشفير

3-3-2- بناء و تدريب شبكة فك التشفير :

بالنسبة لشبكة فك التشفير تمتلك بنية مطابقة لبنية شبكة الخصومة المستخدمة في عملية التشفير ، فهي تتكون من شبكتين واحدة لتوليد الصور بعد فك تشفيرها و بنيتها موضحة في الشكل (2) ، و الشبكة الثانية لتدريب الشبكة الأولى و لكن الاختلاف هنا هو المدخلات و المخرجات لكلا الشبكتين أثناء مرحلة التدريب و مرحلة استخدام الشبكة (فك التشفير) ، حيث سيكون دخل شبكة المولد هو الصورة المشفرة و سيتم تدريبها للحصول على الصورة الأصلية التي تم تشفيرها بينما دخل شبكة المميز سيكون الصور الأصلية قبل التشفير و الصور المولدة من قبل شبكة المولد و يوضح الشكل (2) مراحل تدريب شبكة فك التشفير :



الشكل (4) : المخطط العام لمراحل تدريب شبكة التشفير

الاختبار و الحصول على النتائج : بعد تدريب الشبكة العصبونية و الوصول لنسبة خطأ مناسبة و تثبيت الأوزان ضمن الشبكة بشكل نهائي تصبح جاهزة للاستخدام و الاختبار ، فبعد عملية التدريب يمكن الاستغناء عن شبكة المميز كون عملها ينحصر فقط في تدريب شبكة المولد . و لاختبار الشبكة سيتم اختيار عامل قوة التشفير و عامل الزمن المستغرق للتشفير و دقة الصورة بعد عملية فك التشفير . يتم إدخال صورة جديدة الى شبكة المولد لتشفيرها و بناء على الصورة الناتجة نقوم بحساب قوة عملية التشفير و ذلك بناء تابع ال NPCR (Number of pixel change rate) حيث يعبر عن نسبة الاختلاف في قيم بيكسلات الصورة قبل التشفير و قيم بيكسلات الصورة بعد التشفير [8] و يعطى بالعلاقة (6):

$$NPCR = 100\% \times \frac{\sum_{i=0}^{W}\sum_{j=0}^{H} D(i,j)}{W \times H} \quad \textbf{(6)}$$

حيث أن W , H تمثل أبعاد الصورة و MSE (Mean Square Error) متوسط الخطأ التربيعي و الفرق بين بيكسلات الصورة الأصلية و الصورة بعد عملية التشفير [8] و يعطى بالعلاقة (7) :

$$MSE = \frac{\sum_{M,N}[I1(m,n) - I2(m,n)]^2}{M \times N} \times 100\% \quad \textbf{(7)}$$

و في مرحلة فك التشفير تعبر القيمة MSE عن دقة عملية فك التشفير كونها تمثل الفرق في قيم البيكسلات بين الصورة قبل التشفير و الصورة بعد فك التشفير ، و التابع NPCR (Number of Pixels changing Rate) لاختبار نسبة التغير بين الصورة الأصلية و الصورة المشفرة [9] و يعطى بالعلاقة (8) :

$$NPCR = \frac{\sum_{i=0}^{W}\sum_{j=0}^{W} D(i,j)}{W \times H} \times 100\% \quad \textbf{(8)}$$

حيث أن T1 قيمة البيكسل عند السطر i و العمود j في مصفوفة الصورة قبل التشفير ، T2 قيمة البيكسل عند السطر i و العمود j في مصفوفة الصورة بعد التشفير و (W,H) أبعاد الصورتين.

3-4- تقييم الأداء و مناقشة النتائج :

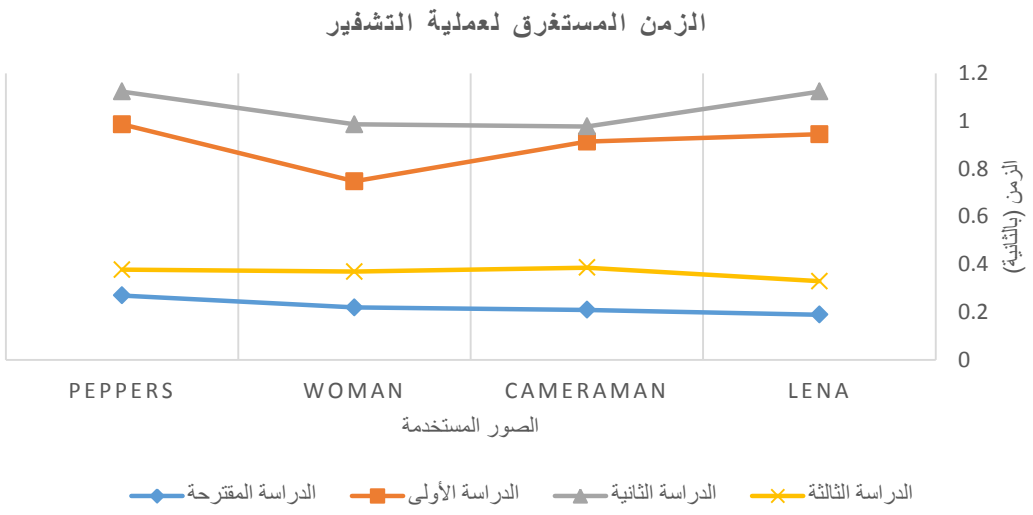
تم استخدام مجموعة بيانات (صور) معتمدة من قبل الدراسات السابقة و ذلك لضمان حدوث مقارنة عادلة حيث تم استخدام Dataset مكونة من 20 صورة و هي الصور المشهورة في مجال معالجة الصورة الرقمية (Cameraman, Woman , Lena , Peppers , ...) و سنرمز لها بالمجموعة الأولى D1 و تم تشفير هذه الصور وفق خوارزمية ال AES-256 باستخدام برنامج الماتلاب و بذلك نحصل على مجموعة البيانات الثانية D2 .

بعد بناء شبكة التشفير و تدريبها باستخدام D1 لشبكة المولد و D2 لشبكة المميز حيث سنرمز لها Cn ، و بناء شبكة فك التشفير و تدريبها باستخدام D2 لشبكة المولد و D1 لشبكة المميز و نرمز لها Dn ، قمنا باختبار الطريقة المقترحة عن طريق ادخال صور لتشفيرها من خلال Cn و من ثم فك تشفيرها من خلال Dn و من ثم تم تطبيق تابع متوسط الخطأ التربيعي المعطى بالعلاقة (7) و كانت النتائج وفق الجدول الآتي الذي يوضح الفرق بين الخوارزمية المقترحة و الخوارزميات المقترحة في الدراسات السابقة من حيث دقة الخطأ الناتج بعد فك التشفير لكل خوارزمية و بتطبيق نفس التابع المعطى بالعلاقة (7) :

الجدول -3- الخطأ الحاصل بعد فك التشفير

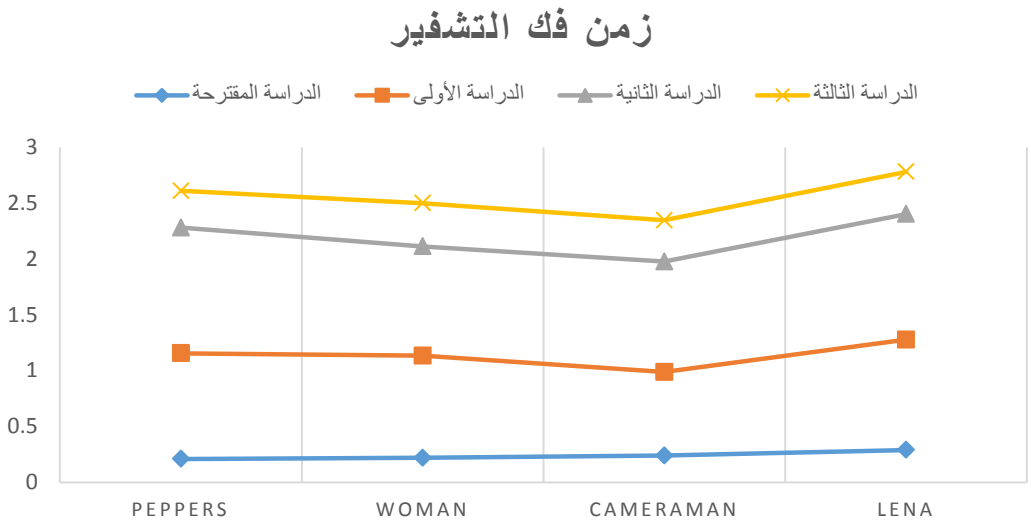
الخوارزمية	الخوارزمية المقترحة	الدراسة الأولى [6]	الدراسة الثانية [10]	الدراسة الثالثة [11]
الصورة	(MSE %)	(MSE %)	(MSE %)	(MSE %)
Lean	0.01235	0.0965	0.2	0.9
CameraMan	0.02367	0.12	0.135	0.6
Woman	0.03658	0.0999	0.1956	0.7
Peppers	0.05689	0.2356	0.152	0.5

بالنسبة لتقييم نتائج الخوارزمية المقترحة من حيث سرعة الأداء (زمن التنفيذ) ، تم من خلال طرح زمن الحصول على صورة الخرج (سواء في حال التشفير أو فك التشفير) من زمن بدأ التنفيذ ، بحيث نحصل على الزمن المستغرق في تنفيذ جميع العمليات الحسابية و كانت النتائج وفق المخطط الآتي بالنسبة لعملية التشفير :



الشكل (5) : المخطط البياني لزمن التشفير لكل خوارزمية

أما بالنسبة لزمن فك التشفير لكل خوارزمية ، فهو موضح بالمخطط الآتي :



الشكل (6) : المخطط البياني لزمن فك التشفير لكل خوارزمية

من خلال دراسة المخططين السابقين نلاحظ أن الخوارزمية المقترحة تحقق أعلى سرعة في كل من عمليتي التشفير و فك التشفير مقارنة مع الخوارزميات السابقة .

فيما يخص قوة التشفير لكل من الدراسة المقترحة و الدراسات السابقة تم حسابها من خلال التابع المعطى بالعلاقة (8) و الذي يعبر عن نسبة عدد البيكسلات التي تتغير قيمها بين الصورة الأصلية قبل عملية التشفير و الصورة نفسها بعد أن يتم تشفيرها [12] و كانت النتائج وفق الجدول الآتي :

الجدول –4– الخطأ الحاصل بعد فك التشفير

الخوارزمية	الخوارزمية المقترحة	الدراسة الأولى [6]	الدراسة الثانية [10]	الدراسة الثالثة [11]
الصورة	(NPCR %)	(NPCR %)	(NPCR %)	(NPCR %)
Lean	99.75	99.14	99.566	99.895
CameraMan	99.124	99.23	99.648	99.814
Woman	99.254	99.35	99.548	99.911
Peppers	99.368	99.18	99.712	99.896

من الجدول السابق نلاحظ أن الخوارزمية تعطي قوة تشفير أعلى من الخوارزميات في كل من الدراستين الأولى و الثانية ولكن أقل من الدراسة الثالثة و ذلك بسبب تعقيد طريقة التشفير في الخوارزمية المقترحة في الدراسة الثالثة بسبب استخدام أربع شبكات عصبونية و لكن على حساب الزمن المستغرق .

ملخص النتائج :

من الجداول و المخطط السابقة نلاحظ أن الخوارزمية المقترحة قد قدمت أفضل أداء من حيث سرعة التنفيذ في كل من عمليتي التشفير و فك التشفير مقارنة مع الدراسات السابقة و أيضا بالنسبة دقة الصورة الناتجة بعد عملية فك التشفير حصلنا على أقل خطأ (bit error) من الدراسات السابقة ، كما قدمت تحسين في قوة عملية التشفير أعلى من الدراسة الأولى و الثانية .

4– الأفكار المستقبلية و التوصيات:

النظام المقترح يقوم بتشفير الصور باستخدام خوارزمية التشفير /AES–256/ ، سيتم العمل على إضافة إمكانية تشفير الفيديوهات و ذلك عن طريق تعديل مراحل الخوارزمية بحيث يتم إضافة مرحلة المعالجة الأولية للفيديو و التي تتضمن تقسيم الفيديو لمجموعة من الأطر ، حيث أن كل إطار يمثل صورة ليتم تشفير كل إطار و من ثم إعادة دمج الأطر للحصول على الفيديو المشفر .

المراجع :

[1] Ako Muhammad Abdullah.; . Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data, Research Gate, Vol. 108, No. 10 , 2017 , 3176-15794.

[2] Sooyong Jeong., Cheolhee Park., Dowon Hong., Changho Seo., Namsu Jho.; . Neural Cryptography Based on Generalized Tree Parity Machine for Real-Life Systems, Hindawi, Vol. 101, No. 4 , 2021 , 668-0782.

[3] Zhenlong Man., Jinqing LI., Xiaoqiang DI., Yaohui Sheng., Zefei Liu.; . Double image encryption algorithm based on neural network and chaos, Elsevier Journal, Vol. 152, No. 11 , 2021 ,111-318.

[4] Yasin Kh. Yasin.; . Advanced Encryption Standard (AES) Enhancement Using Artificial Neural Networks, International Journal of Scientific & Engineering Research, Vol. 3, No. 2 , 27-39.

[5] AMEEN S., MAHDI A.; . AES Cryptosystem Development Using Neural Networks, International Journal of Computer and Electrical Engineering, Vol. 3, No. 2, 2017 , 27-39.

[6] Ian J. Goodfellow., Jean Pouget-Abadie., Mehdi Mirza., Bing Xu., David Warde-Farley., Sherjil Ozair., Aaron Courville., Yoshua Bengio.; . Generative Adversarial Networks, NIPS , 2014.

[7] Phillip Isola., Jun-Yan Zhu., Tinghui Zhou., Alexei A. Efros.; . Image-to-Image Translation with Conditional Adversarial Networks, CVPR , 2017.

[8] Jan Low., Jame S.; . Cycle Generative Adversarial Network (Cycle GAN) Research Gate, Vol. 77, No. 10 , 2022.

[9] Shima Ramesh Maniyath., Thanikaiselvan V.; . An efficient image encryption using deep neural network and chaotic map, Elsevier Journal, Vol. 77, No. 8 , 2020 , 103134.

[10] Archana Swaminathan.; . Image Encryption and Decryption using Artificial Neural Networks, IEEE , Vol. 222 , No. 5 , 2020 , 203-154.

[11] Minal Chauhan., Rashmin Prajapati.; . Image Encryption and Decryption using Artificial Neural Networks, International Journal of Scientific & Engineering Research , Vol. 5 , No. 10 , 2014 , 2229-5518.

[12] Ragheb Toemeh.; . Various Approaches towards Cryptanalysis, International Journal of Computer Applications, Vol. 127, No. 14,2015 , 0975 – 8887.