مجلة التطور الدولية للعلوم والأبحاث (IEJSR)
International Evolution Journal for Science & research (IEJSR))

المجلد3– العدد3 - (سبتمبر) 2026

ISSN-E: 3078-4964 ISSN-P: 3078-4956

تحسين تشفير البيانات باستخدام الشبكات العصبية التوليدية

Improving Data Encryption with Generative Adversarial Networks (GANs)

د.إبراهيم محمد أحمد علي*، د. ياسر الملك احمد سليمان**، د. مصطفى أمين عبد المجيد محمد***

* جامعة كرري، السودان، أستاذ مشارك، قسم علوم الحاسب وتقنية المعلومات، ibra@him16@gmail.com

* الجامعة التكنولوجية، السودان، أستاذ مشارك، كلية الحاسوب وتقانة المعلومات، Dr.yaserking359@hotmail.com

*** الجامعة التكنولوجية، السودان، أستاذ مساعد، قسم علوم الحاسب وتقانة المعلومات، dr.mostfamin359@hotmail.com

تاريخ الاستلام: 3 يوليو 2026 | تاريخ القبول: 10 أغسطس 2026 | تاريخ النشر: 1 سبتمبر 2026

الملخص

تبرز أهمية حماية البيانات في العصر الرقمي، حيث تتعرض المعلومات الحساسة لتهديدات متزايدة من الهجمات السيبرانية. يعد التشفير أحد الأساليب الأساسية لحماية هذه البيانات، ولكن التحديات المتعلقة بالأمان وكفاءة الأداء تظل قائمة في هذا السياق. هدف البحث الحالي إلى توضيح كيف يمكن للشبكات العصبية التوليدية تحسين تقنيات تشفير البيانات، سواء عبر توليد مفاتيح تشفير أقوى، أو عبر تصميم خوارزميات جديدة، أو تعزيز مقاومة الأنظمة للهجمات. اعتمد البحث بشكل أساسي على المنهجية الكمية التجريبية، عبر تصميم وتنفيذ تجارب محكومة لاختبار وتقييم أداء النماذج المقترحة القائمة على الشبكات العصبية التوليدية في مهام محددة متعلقة بالتشفير. توصلت النتائج إلى أنَّ الشبكات العصبية التوليدية على فكرة وجود نموذجين؛ المولد الذي يسعى لإنشاء بيانات جديدة، والمميز الذي يهدف إلى التمييز بين البيانات الحقيقية والمزيفة. من خلال هذه العملية التنافسية، يمكن للشبكات العصبية التوليدية تحسين جودة البيانات المولدة ومن اشهر تطبيقاتها توليد مفاتيح تشفير :يمكن استخدام الشبكات العصبية التوليدية لتوليد مفاتيح تشفير فريدة ومعقدة، مما يزيد من صعوبة كسر الأنظمة الأمنية. أوصى البحث بضرورة تحسين خوار زميات التشفير من خلال التعلم من أنماط البيانات، يمكن للشبكات العصبية التوليدية تحسين الخوارزميات القائمة، مما يؤدي إلى تشفير أكثر كفاءة.

الكلمات المفتاحية: *تشفير، البيانات، الشبكات العصبية التوليدية*

Abstract

The importance of data protection is paramount in the digital age, as sensitive information faces increasing threats from cyberattacks. Encryption is a fundamental method for protecting this data, but challenges related to security and performance remain. This research aims to demonstrate how generative neural networks (GNSNs) can enhance data encryption techniques, whether by generating stronger encryption keys, designing new algorithms, or strengthening system resistance to attacks. The research primarily employed a quantitative experimental methodology, designing and implementing controlled experiments to test and evaluate the performance of proposed GNSN-based models in specific encryption-related tasks. The results revealed that GNSNs operate on the principle of two models: a generator, which seeks to create new data, and a discriminator, which aims to distinguish between genuine and fake data. Through this competitive process, GNSNs can improve the quality of generated data. One of their most prominent applications is encryption key generation: GNSNs can be used to generate unique and complex encryption keys, making security systems more difficult to break. The research recommended improving encryption algorithms by learning from data patterns. Generative neural networks can enhance existing algorithms, leading to more efficient encryption.

Keywords: Encryption, Data, Generative neural networks.

1. المقدمة

يشهد العصر الرقمي تناميًا هائلاً في حجم البيانات المتداولة عبر المنصات والشبكات، مما يجعل أمن هذه البيانات وحمايتها من الوصول غير المصرح به أو التلاعب أولوية قصوى. تعتمد المؤسسات والأفراد على سلامة وسرية معلوماتهم الشخصية والمالية والاستراتيجية، وتلعب تقنيات التشفير دوراً محورياً في تأمينها عبر تحويلها إلى صيغة غير قابلة للقراءة إلا بمفتاح فك التشفير المناسب. غير أن التطورات الحاسوبية المتسارعة، بما في ذلك التهديدات المحتملة من الحوسبة الكمومية، تكشف عن قصور في بعض تقنيات التشفير التقليدية، مما يستلزم حلول أكثر تقدماً.

في هذا السياق، برزت الشبكات العصبية التوليدية (Generative Adversarial Networks – GANs) كأداة واعدة في مجال الذكاء الاصطناعي (Geron, 2019). تتكون هذه الشبكات من شبكتين: المولد، الذي ينتج بيانات مزيفة تحاكي الأصلية، والمميز، الذي يميز بين البيانات الحقيقية والمزيفة. من خلال هذا التفاعل التنافسي، تتعلم الشبكات إنتاج بيانات عالية الجودة، مما يفتح آفاقًا لتطبيقاتها في تعزيز أمن البيانات. تشمل الفوائد المحتملة لهذا النهج تعزيز أمان التشفير، وزيادة كفاءته، وتطوير خوارزميات أكثر تعقيدًا تتجاوز القيود التقليدية، مما يدعم تطبيقات في الأمن السيبراني، الاتصالات، والتخزين السحابي (Stinson and Paterson, 2018). ومع ذلك، تواجه هذه التقنية تحديات الحاجة إلى بيانات تدريب ضخمة، ومعالجة الجوانب الأخلاقية لاستخدام الذكاء الاصطناعي. يمثل استخدام الشبكات العصبية التوليدية في تشفير البيانات خطوة نحو تطوير أساليب أمان أكثر فعالية، من خلال الاستفادة من التعلم العميق، يمكن تعزيز حماية المعلومات في مواجهة التهديدات المتزايدة (Courville, 2016).

وانطلاقاً من ذلك، يهدف هذا البحث إلى توضيح كيف يمكن للشبكات العصبية التوليدية تحسين تقنيات تشفير البيانات، سواء عبر توليد مفاتيح تشفير أقوى، أو عبر تصميم خوارزميات جديدة، أو تعزيز مقاومة الأنظمة للهجمات. يتناول البحث عدة أهداف فرعية، تشمل مراجعة تقنيات التشفير الحالية ونقاط ضعفها، فهم آليات عمل الشبكات العصبية التوليدية، تطوير نماذج مقترحة لدمجها في التشفير، وتقييم أدائها من حيث الأمان والكفاءة. تكمن أهمية البحث في استكشاف تقاطع الذكاء الاصطناعي وأمن المعلومات، مما قد يوفر حلولاً مبتكرة لحماية البيانات في مواجهة التهديدات المتزايدة.

1.1 المشكلة البحثية

تتمثل مشكلة البحث في محدودية الخوارزميات التقليدية للتشفير في مواجهة التهديدات الإلكترونية المتطورة، خاصة مع تطور تقنيات مثل الحوسبة الحكومية والهجمات القائمة على الذكاء الاصطناعي و التحديات

في قابلية تنبؤ مفاتيح التشفي الاعتماد على أنماط رياضية ثابتة يجعلها عرضة للاختراق عبر التحليل الإحصائي، وضعف الكفاءة في بيئات محدودة الموارد مثل أنظمة إنترنت الأشياء التي تعاني من بطء التشفير بسبب قيود الطاقة والمعالجة (Hitaj et al., 2017)، فضلاً عن صعوبة إكتشاف الهجمات المتقدمة في أنظمة الكشف، والتحديات في إدارة المفاتيح لأنظمة المركزية تشكل نقطة فشل وحيدة، والتكلفة العالية للتحديثات الأمنية :تحديث البنية التحتية التشفيرية يتطلب استثمارات كبيرة ووقتًا طويل.

1.2 أهمية البحث

تمثل هذه الدراسة خطوة حاسمة نحو إنشاء أنظمة تشفير أكثر ذكاءً ومرونة، قادرة على مواكبة التحديات الأمنية المتزايدة وتعزيز حماية البيانات في القطاعات الحيوية المختلفة. كما تكتسب دراسة تحسين تشفير البيانات باستخدام الشبكات العصبية التوليدية أهمية بالغة في تعزيز الأمن الرقمي ومواكبة التطورات التكنولوجية من خلال مجموعه نقاط :

أ- تعزيز أمان التشفير من خلال تحليل الأنماط المعقدة تمتلك الشبكات العصبية التوليدية، قدرة على تحليل العلاقات غير الخطية المعقدة في البيانات، مما يصعّب عملية اختراقها مقارنةً بالخوارزميات التقليدية.

ب- تحسين كفاءة التشفير وتقليل حجم البيانات تعمل هذه الشبكات على ضغط البيانات واستخلاص الميزات الأساسية منها، مما يسرّع عمليات التشفير وفك التشفير ويقلل من حجم البيانات المنقولة أو المخزنة، مع الحفاظ على جودتها وأمانها.

ج- الكشف المبكر عن الثغرات والهجمات الأمنية بفضل قدرتها على التعلّم غير المُشرف، يمكن للشبكات التوليدية تحديد الأنماط الشاذة في البيانات، مما يساعد في اكتشاف محاولات الاختراق أو الهجمات الإلكترونية بشكل سريع ودقيق.

تتميز هذه التقنية بمرونتها في التعامل مع مختلف أشكال د- التكيّف مع أنواع متعددة من البيانات البيانات، سواءً كانت نصوصًا أو صورًا أو بيانات زمنية، مما يجعلها مناسبة لمجالات أمنية متنوعة

1.3 تساؤلات البحث

بناءً على ما سبق تتلخص مشكلة البحث في السؤال الرئيسي التالي:

كيف يمكن للشبكات العصبية التوليدية تحسين تقنيات تشفير البيانات، سواء عبر توليد مفاتيح تشفير أقوى، تصميم خوارزميات جديدة، أو تعزيز مقاومة الأنظمة للهجمات؟

ويمكن صياغة الأسئلة البحثية الفرعية على النحو التالي:

1- إلى أي مدى يمكن للشبكات العصبية التوليدية (GANs) تعزيز أمان وكفاءة تشفير البيانات مقارنة بالطرق التقليدية؟
2- ما هي المعماريات الأمثل للشبكات العصبية التوليدية لتوليد مفاتيح تشفير قوية ومقاومة للتنبؤ أو الكسر؟
3- كيف يمكن تقييم أمان أنظمة التشفير القائمة على GANs مقارنة بالخوارزميات التقليدية) مثل AES)ضد هجمات مثل تحليل التردد أو هجمات النص الواضح المعروف؟
4- هل يمكن للشبكات العصبية التوليدية تطوير خوارزميات تشفير جديدة مرنة وقابلة للتكيف، وما هي التحديات النظرية والعملية المرتبطة بذلك؟
5- ما هي التحديات العملية (مثل التعقيد الحسابي، الحاجة إلى بيانات تدريب، قابلية التفسير) التي تواجه تطبيقGANs في التشفير، وكيف يمكن معالجتها؟
6- كيف تؤثر الكفاءة الحسابية لأنظمة التشفير القائمة على GANs على إمكانية تطبيقها على نطاق واسع مقارنة بالخوارزميات التقليدية؟

1.4 حدود البحث

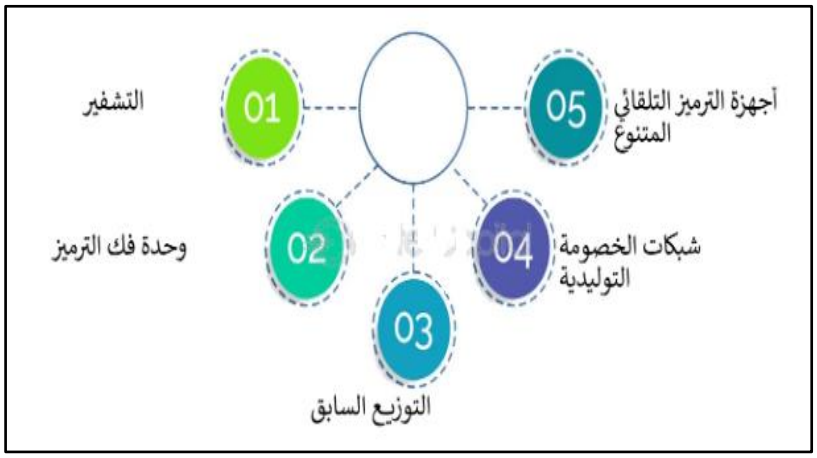
- **الحدود المكانية:** غالباً ما تجرى هذه الدراسات في مختبرات الحوسبة أو مراكز البحث المتخصصة في الذكاء الاصطناعي والأمن السيبراني، حيث تتوفر الموارد الحاسوبية اللازمة لتدريب واختبار النماذج. يمكن أن تتنوع البيئات التطبيقية بين المؤسسات الأكاديمية، الشركات التقنية، أو مراكز تطوير البرمجيات، مع إمكانية تطبيق النتائج في قطاعات متعددة مثل الاتصالات، الصحة، أو البنوك.
- **الحدود الزمانية:** يرتبط البحث بالفترة الزمنية التي ظهرت فيها تقنيات الشبكات العصبية التوليدية وتطورت بوضوح، أي منذ بروز Autoencoders الشبكات العصبية التوليدية تقريبًا من 2019 حتى الآن. يشمل البحث آخر التطورات في مجال الذكاء الاصطناعي التوليدي والتشفير حتى تاريخ إجراء البحث، مع مراعاة أن المجال سريع التطور ويتطلب تحديثًا مستمرًا للنتائج والمنهجيات . قد تُحدد فترة زمنية محددة لجمع البيانات أو اختبار النماذج، وغالبًا ما تُذكر في منهجية الدراسة لضمان تكرار النتائج هذه الحدود تضمن تركيز الدراسة على نطاق محدد وواضح من حيث

الموضوع، البيئة التطبيقية، والإطار الزمني، ما يدعم دقة النتائج وقابليتها للتطبيق والتطوير.

2. الاطار النظري (مراجعة الأدبيات)

بعد التعرف علي الجانب النظري الذي يُبنى عليه البحث، وتم التطرق الي المفاهيم الجوهرية المتعلقة بكل من علم التشفير والشبكات العصبية التوليدية. يهدف هذا العرض إلى تزويد القارئ بالخلفية المعرفية اللازمة لفهم التحديات القائمة في مجال تأمين البيانات والفرص التي تقدمها التقنيات الحديثة مثل الشبكات العصبية التوليدية لمواجهة هذه التحديات على تطبيقات الشبكات العصبية التوليدية، مثل أجهزة التشفير التلقائي والشبكات العصبية التوليدية في مجال تحسين تشفير البيانات، ولا تتناول جميع أنواع التشفير أو جميع تطبيقات الذكاء الاصطناعي تركز على آليات ضغط البيانات، توليد المفاتيح، واكتشاف الأنماط غير الخطية لتحسين الأمان والكفاءة، دون التطرق لتقنيات تشفير تقليدية بحتة أو تطبيقات الذكاء الاصطناعي غير التوليدي (Goodfellow et al., 2016).

تشمل الدراسة التحديات والقيود المرتبطة بهذه النماذج، مثل الحاجة إلى بيانات ضخمة، والتكلفة الحسابية، وصعوبة تفسير الفضاء الكامن للبيانات نتناول الجانب العملي والتطبيقي المتمثل في كيفية دمج هذه التقنيات المتقدمة بهدف تحسين أمن البيانات. يستكشف هذا القسم الأساليب المختلفة التي يمكن من خلالها للشبكات العصبية التوليدية أن تساهم في تعزيز أنظمة التشفير التقليدية أو حتى في ابتكار مقاربات جديدة كليًا. كما يناقش التحديات والاعتبارات الأساسية التي يجب أخذها في الحسبان عند محاولة تطبيق هذه النماذج في سيناريوهات واقعية. الشكل (1) يوضح التشفير باستخدام الشبكات العصبية التوليدية.



الشكل 1: التشفير باستخدام الشبكات العصبية التوليدية(GANs)

2.1 الأساليب المقترحة لتحسين التشفير باستخدام الشبكات العصبية التوليدية (GANs)

الأساليب المقترحة لتحسين التشفير باستخدام الشبكات العصبية التوليدية تفتح آفاقًا جديدة في مجال تشفير البيانات، عبر عدة أساليب عملية:

1. توليد مفاتيح تشفير قوية وديناميكية

يمكن للشبكات العصبية التوليدية توليد مفاتيح تشفير ذات عشوائية وتعقيد مرتفعين، ما يزيد من صعوبة اختراقها مقارنة بمولدات الأرقام العشوائية التقليدية (Geron, 2019). كما يمكن تصميم أنظمة تولد مفاتيح ديناميكية تتغير باستمرار أو حسب السياق، مما يعزز الأمان ضد هجمات القوة الغاشمة والتحليل الإحصائي.

2. تطوير خوارزميات تشفير جديدة أو تحسين الخوارزميات القائمة

يمكن تدريب المولد في الشبكات العصبية التوليدية ليعمل كخوارزمية تشفير تتعلم تحويل النص الصريح إلى نص مشفر بطريقة يصعب عكسها دون المفتاح المناسب. بينما يمكن للمميز أن يقيم جودة التشفير أو يحاول كسر الشيفرة، ما يدفع المولد لتطوير استراتيجيات تشفير أكثر قوة. هذا النهج يتيح اكتشاف تحويلات غير خطية ومعقدة تتجاوز الخوارزميات التقليدية، كما يمكنه تحسين عمليات الارتباك والانتشار الأساسية في أنظمة التشفير (Rukhin et al., 2001).

3. إخفاء البيانات (Steganography) بطرق أكثر تعقيداً

تتيح الشبكات العصبية التوليدية توليد وسائط حاملة (صور، صوت، فيديو) عالية الجودة يصعب تمييزها عن الأصلية، مع تضمين بيانات سرية بداخلها بشكل يصعب اكتشافه حتى بالاختبارات الإحصائية التقليدية. يمكن تدريب المولد على تعديل وحدات البكسل أو العينات الصوتية بشكل غير محسوس، بينما يُدرب المميز على اكتشاف هذه التعديلات، ما يدفع المولد لتطوير تقنيات إخفاء أكثر تطورًا (Hansen, 2022).

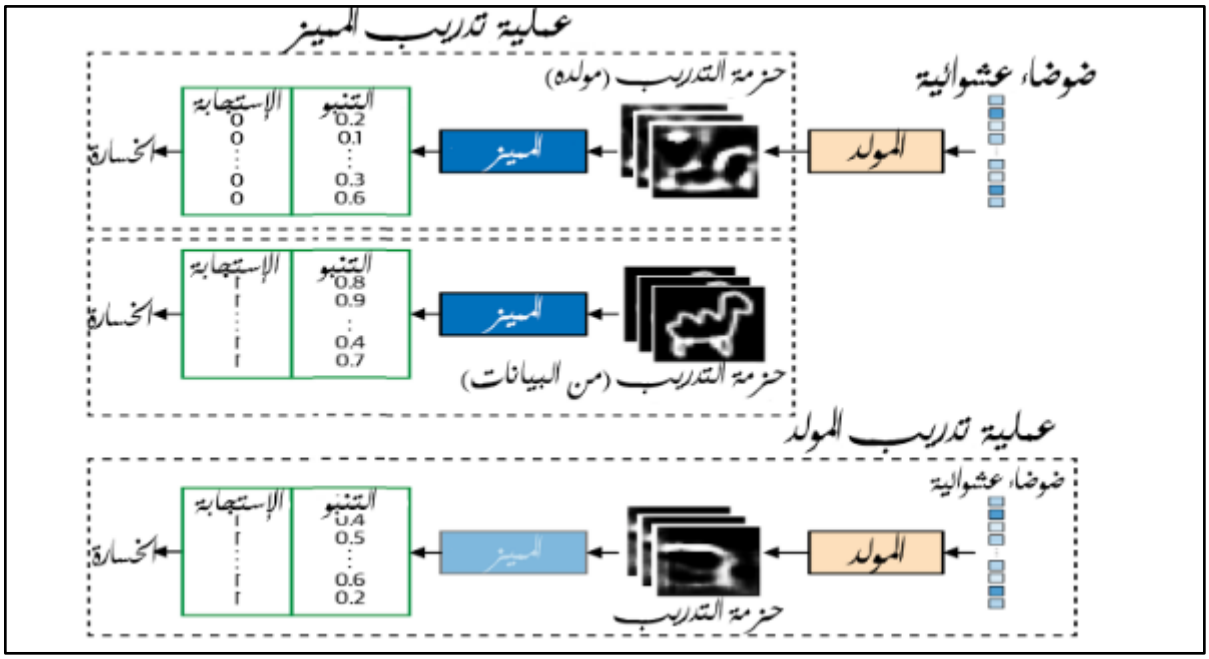
4. تعزيز مقاومة أنظمة التشفير للهجمات المعروفة

يمكن استخدام الشبكات العصبية التوليدية لمحاكاة هجمات متنوعة على أنظمة التشفير، وتدريب النماذج على اكتشاف نقاط الضعف واستباقها، مما يساعد في اختبار قوة الأنظمة الحالية وتحديد ثغراتها قبل استغلالها فعليًا. كما يمكن توليد بيانات تدريب واقعية ومتنوعة لأنظمة كشف التسلل أو البرمجيات الخبيثة.

5. إستكشاف إمكانيات التشفير المتقدم في مجالات مثل التشفير المتجانس أو التشفير القائم على السمات

يمكن استغلال الشبكات العصبية التوليدية لإدارة المفاتيح المعقدة أو توليد هياكل بيانات تدعم هذه الأنظمة بكفاءة، ما يفتح الباب أمام حلول تشفير أكثر مرونة وتقدمًا ومن ملاحظة الباحث ان هناك مجموعة من التحديات والاعتبارات رغم الإمكانيات الواعدة، تواجه تطبيقات الشبكات العصبية التوليدية في التشفيرو تحديات جوهرية وتشتمل (Goodfellow et al., 2016; Hansen, 2022):

1. التعقيد الحسابي ومتطلبات الموارد: حيث تتطلب الشبكات العصبية التوليدية موارد حسابية ضخمة (GPU/TPU) وزمن تدريب طويل، ما قد يعيق استخدامها في الأنظمة التي تحتاج استجابة فورية أو تعمل على أجهزة محدودة الإمكانيات
2. تقييم الأمان والموثوقية: حيث أنَّ إثبات أمان أنظمة التشفير القائمة على الشبكات العصبية التوليدية أصعب من الأنظمة التقليدية ذات الأسس الرياضية الواضحة، إذ غالبًا ما تعمل هذه النماذج كـ"صناديق سوداء" يصعب تفسير سلوكها بالكامل أو ضمان مقاومتها لكل أنواع الهجمات.
3. الحاجة لمجموعات بيانات تدريب كبيرة ومتنوعة: حيث تعتمد جودة أداء الشبكات العصبية التوليدية بشكل كبير على تنوع وحجم بيانات التدريب. في سياق التشفير، قد يصعُب توفير بيانات كافية لتدريب النماذج على توليد مفاتيح قوية أو خوارزميات فعالة، كما أن التحيز في البيانات قد يؤدي لثغرات أمنية غير متوقعة.
4. قابلية التوسع والتطبيق العملي حتى مع نجاح النماذج في البيئة البحثية: يبقى تطبيقها على نطاق واسع تحديًا من حيث التكامل مع الأنظمة الحالية، الصيانة، والتحديث المستمر .
5. إمكانية الاستخدام الضار: حيث أنَّ القدرات ذاتها التي تجعل الشبكات العصبية التوليدية أداة قوية في تعزيز الأمان يمكن استغلالها لتطوير هجمات متقدمة، مثل توليد بيانات مزيفة لخداع أنظمة المصادقة أو إنشاء رسائل تصيد احتيالي أكثر إقناعًا، ما يفرض ضرورة دراسة الجوانب الأخلاقية والأمنية بعناية.
6. تفسير سلوك النماذج(Interpretability) : حيث أنه غالباً ما يصعب تفسير قرارات نماذج الشبكات العصبية التوليدية، ما يعيق فهم أسباب نجاح أو فشل نظام التشفير في سيناريوهات معينة، ويؤثر على الثقة في اعتمادها في التطبيقات الحساسة. الشكل (2) يوضح عملية التدريب باستخدام الشبكات العصبية التوليدية.



الشكل 2 : عملية التدريب باستخدام الشبكات العصبية

3. اجراءات البحث

في هذا الجانب من الورقة يتناول البحث الإطار المنهجي والإجراءات التجريبية التي سيتم اتباعها لتحقيق أهداف البحث والإجابة على أسئلته المطروحة في الفصول السابقة. يهدف هذا القسم إلى توضيح الخطوات العملية التي ستُتخذ لتصميم، وتنفيذ، وتقييم النماذج المقترحة لدمج الشبكات العصبية التوليدية في تحسين تشفير البيانات. سيتم التركيز على بناء منهجية قوية تضمن الحصول على نتائج موثوقة وقابلة للتكرار، مع مراعاة التحديات التي تم تحديدها.

تتضمن الخطوات العملية التي ستُتخذ لتصميم، وتنفيذ، وتقييم النماذج المقترحة لدمج الشبكات العصبية التوليدية في تحسين تشفير البيانات ما يلي:

1.**بناء النماذج:** سيتم تصميم وبناء نماذج شبكات عصبية توليدية (GANs) مخصصة لأغراض التشفير، مثل توليد مفاتيح التشفير أو تطوير عمليات تشفير جديدة. سيتم تحديد معماريات الشبكات (المولد والمميز)، وتحديد دوال الخسارة (Loss Functions) المناسبة، واختيار مُحسِّنات (Optimizers) فعالة لعملية التدريب.

2.**إعداد البيانات:** سيتم تحديد واختيار مجموعات بيانات مناسبة لتدريب واختبار النماذج. قد تشمل هذه البيانات أنواعًا مختلفة من النصوص، الصور، أو أي بيانات أخرى تتطلب التشفير. سيتم النظر في حجم البيانات وتنوعها لضمان قدرة النماذج على التعميم بشكل جيد.

3.**التدريب والاختبار:** سيتم تدريب النماذج المقترحة على مجموعات البيانات المحددة، مع مراقبة أداء التدريب وضبط المعلمات الفائقة (Hyperparameters) حسب الحاجة. بعد اكتمال التدريب، سيتم اختبار النماذج على مجموعات بيانات منفصلة (مجموعات اختبار) لتقييم أدائها بشكل موضوعي.

4.**التحليل الإحصائي للنتائج:** سيتم جمع البيانات الناتجة عن التجارب وتحليلها إحصائيًا. سيتم استخدام مقاييس تقييم محددة (سيتم تفصيلها لاحقًا) لمقارنة أداء النماذج المقترحة مع بعضها البعض أو مع أنظمة تشفير تقليدية.

إلى جانب المنهجية الكمية، سيتم دمج عناصر من التحليل النوعي في تفسير النتائج ومناقشتها، خاصة فيما يتعلق بالجوانب الأمنية النظرية والتحديات العملية لتطبيق هذه النماذج.

3.1 تصميم التجارب والنماذج المقترحة

سيتم التركيز في هذا البحث على استكشاف تطبيقين رئيسيين للشبكات العصبية التوليدية في التشفير، هما:

1- **التجربة الأولى:** توليد مفاتيح تشفير قوية باستخدام الشبكات العصبية التوليدية كما يلي:

أ- النموذج المقترح: حيث سيتم تصميم نموذج GAN مثل DCGAN أو WGAN لتوليد تسلسلات ثنائية (مفاتيح تشفير) تتمتع بخصائص عشوائية عالية. سيتكون المولد من شبكة عصبية تأخذ متجه ضوضاء كمدخل وتُخرج تسلسلًا ثنائيًا بطول محدد (يمثل المفتاح). سيتكون المميز من شبكة عصبية تُدرب على التمييز بين المفاتيح التي تم إنشاؤها بواسطة المولد والمفاتيح العشوائية الحقيقية (أو المفاتيح المولدة بواسطة خوارزميات آمنة).

ب-**معلمات التدريب:** سيتم تجربة معلمات تدريب مختلفة، مثل معدل التعلم(learning rate) ، حجم الدفعة(batch size) ، وعدد عصور التدريب(epochs) ، للوصول إلى أفضل أداء.

ت-**مجموعات البيانات:** لن تتطلب هذه التجربة مجموعة بيانات تقليدية، بل سيتم الاعتماد على قدرة GANعلى تعلم توزيع معين (في هذه الحالة، توزيع المفاتيح العشوائية).

2- **التجربة الثانية:** تطوير نظام تشفير نصي قائم على الشبكات العصبية التوليدية، حيث تتضمن:

أ- **النموذج المقترح:** سيتم تصميم نموذج GAN حيث يعمل المولد . "مُشفر" والمميز "مُحلل شفرة" أو مقيِّم لجودة التشفير, سيأخذ المولد نصًا واضحًا ومفتاحًا سريًا كمدخلات، ويُخرج نصًا مشفرًا, والحالات للمميز إما فك تشفير النص المشفر (إذا تم تزويده ببعض المعلومات) أو التمييز بين النصوص المشفرة بشكل جيد والنصوص المشفرة بشكل ضعيف, الهدف هو أن يتعلم المولد كيفية

تشفير النصوص بطريقة تجعل من الصعب على المميز (وبالتالي أي مهاجم محتمل) استعادة النص الأصلي أو اكتشاف أنماط في النص المشفر.

ب–**معلمات التدريب:**سيتم تحديدها بناءً على طبيعة البيانات النصية وتعقيد المهمة.

ت–**مجموعات البيانات:**سيتم استخدام مجموعات بيانات نصية قياسية (مثل مجموعات بيانات من الأدب أو المقالات الإخبارية) لتدريب واختبار النموذج.

3.2 الأدوات والبرمجيات المستخدمة في تنفيذ التجارب

فيما يتعلق بالأدوات والبرمجيات المستخدمة لتنفيذ التجارب وبناء النماذج، سيتم الاعتماد على الأدوات والبرمجيات التالية:

1– **لغة البرمجة Python** :(الإصدار 3.8 أو أحدث) نظرًا لكونها اللغة الأكثر شيوعًا في مجال التعلم العميق وتوفرها على المكتبات.

2– **أطر التعلم العميق:**سيتم استخدام أحد أطر التعلم العميق المعروفة مثل) TensorFlow مع Keras (APIأو .PyTorch يعتمد الاختيار النهائي على سهولة الاستخدام والمرونة التي يوفرها كل إطار للمهام المحددة.

3– **مكتبات معالجة البيانات:**مكتبات مثل NumPy لمعالجة المصفوفات العددية، وPandas لتحليل البيانات، وMatplotlib أو Seaborn لتصوير النتائج.

4– **البيئة الحاسوبية:**سيتم إجراء التجارب على جهاز حاسوب مزود بوحدة معالجة رسوميات (GPU) مناسبة لتسريع عمليات تدريب نماذج التعلم العميق. إذا لم تتوفر GPU محلية قوية، سيتم النظر في إستخدام منصات الحوسبة السحابية التي توفر موارد GPU مثلGoogle Colaboratory أو AWS SageMaker.

3.3 مقاييس التقييم لتقييم أداء وفعالية النماذج المقترحة

سيتم استخدام مجموعة من المقاييس الكمية والنوعية:

1– مهمة توليد مفاتيح التشفير:

أ– الإنتروبيا:(Entropy) لقياس درجة العشوائية وعدم اليقين في المفاتيح المولدة. كلما ارتفعت قيمة الإنتروبيا، كان المفتاح أكثر عشوائية وأصعب في التنبؤ به.

ب- الإختبارات الإحصائية للعشوائية:سيتم تطبيق مجموعة من الاختبارات الإحصائية القياسية) مثل اختبارات (NIST SP 800-22)، لتقييم مدى جودة الخصائص العشوائية للمفاتيح المولدة.

ج- مقاومة هجمات القوة الغاشمة (نظريًا):سيتم تقييم طول المفتاح وتعقيده لتحديد مدى مقاومته النظرية لهجمات القوة الغاشمة.

د- زمن التوليد: قياس الوقت المستغرق لتوليد مفتاح جديد.

2- مهمة تطوير نظام تشفير نصي:

أ- مستوى الأمان:(Security Level) سيتم تقييمه من خلال محاولة تطبيق هجمات معروفة على النصوص المشفرة (مثل تحليل التردد، هجمات النص الواضح المعروف إذا أمكن تصميمها). كما سيتم تقييم مدى صعوبة تمييز النص المشفر عن بيانات عشوائية.

ب- سرعة التشفير وفك التشفير :قياس الوقت المستغرق لتشفير وفك تشفير كمية معينة من البيانات.

ج- جودة النص المشفر:التأكد من أن عملية التشفير لا تؤدي إلى فقدان معلومات يمكن استغلالها (information leakage).

3- **الجانب التطبيقي للبحث:** يشتمل هذا الجانب علي مقارنة مع خوارزميات تقليدية و مقارنة أداء النظام المقترح (من حيث الأمان والكفاءة) مع خوارزميات تشفير نصية تقليدية معروفة) مثل AES في وضع معين إذا كان ذلك مناسبًا للمقارنة.

3.4 خطوات تنفيذ التجارب وتحليل النتائج

ستتبع عملية تنفيذ التجارب وتحليل النتائج الخطوات التالية:

أ- تنفيذ النماذج: كتابة الشيفرة البرمجية للنماذج المقترحة باستخدام الأدوات والأطر المحددة.

ب- إعداد بيئة التجربة: تهيئة البيئة الحاسوبية وتثبيت جميع المكتبات والاعتماديات اللازمة.

ج – تدريب النماذج: تشغيل عمليات التدريب على مجموعات البيانات المخصصة، مع حفظ نقاط التفتيش (checkpoints)للنماذج المدربة.

د- جمع النتائج: إجراء عمليات الاختبار على النماذج المدربة وجمع البيانات المتعلقة بمقاييس التقييم المحددة.

هـ- تحليل النتائج:استخدام الأدوات الإحصائية لتحليل البيانات المجمعة، وتفسير النتائج في سياق أهداف البحث وأسئلته.

المقارنة والمناقشة مقارنة أداء النماذج المختلفة، ومناقشة نقاط القوة والضعف لكل نموذج، وتحديد مدى مساهمتها في تحسين تشفير البيانات.

و- توثيق النتائج: توثيق جميع خطوات التجربة والنتائج التي تم التوصل إليها بشكل واضح ومفصل في فصل النتائج والمناقشة.

من خلال هذه المنهجية التجريبية المنظمة، يسعى البحث إلى تقديم مساهمة قيمة في فهم وتطبيق الشبكات العصبية التوليدية في مجال أمن البيانات، مع التركيز على تطوير حلول تشفير مبتكرة وقوية.

4- النتائج المتوقعة والمناقشة : نظرًا لأن هذا البحث يقدم إطارًا مقترحًا وتصميمًا تجريبيًا، فإن النتائج المعروضة في هذا الفصل هي نتائج متوقعة وافتراضية تهدف هذه الصياغة إلى توضيح نوع المخرجات التي يمكن الحصول عليها في حال تنفيذ المنهجية المقترحة، وكيف يمكن تحليلها ومناقشتها للإجابة على أسئلة البحث.

4. النتائج

4.1 النتائج المتوقعة لتجربة توليد مفاتيح التشفير باستخدامGANs

تفترض هذه التجربة تصميم نموذج GAN لتوليد مفاتيح تشفير تتمتع بخصائص عشوائية عالية بعد تدريب النموذج وتقييمه باستخدام المقاييس المحددة (الإنتروبيا، اختباراتNIST ، زمن التوليد). يمكن توقع النتائج كما هو موضح في الجدول الافتراضي التالي (جدول 1):

جدول 1. مقارنة محاكاة بين المفاتيح التي تم إنشاؤها بواسطة GAN و PRNGs

ملاحظات	مفاتيح PRNG (المرجعي)	المفاتيح التي تم إنشاؤها بواسطةGAN(متوقعة)	الخاصية
موحد للمقارنة العادلة.	256	256	طول المفتاح (بتات)
تشير إلى القيم القريبة من 1 عشوائية عالية.	0.999	0.998	Entropy per Bit (average)
النسبة المئوية للمفاتيح التي تجتاز جميع اختبارات العشوائيةNIST	99%	98%	الانتروبيا لكل بت (متوسط)

التوليد المستند إلى GAN أبطأ بسبب تعقيد النموذج.	10	150	وقت التوليد الرئيسي (مللي ثانية)
تهدف الى شبكات GAN حجب الأنماط الإحصائية ، ولكنها قد لا تتطابق مع الخوارزميات المصممة رياضيا.	< 1% (theoretically none)	< 5%	مقاومة تحليل التردد (نجاح الهجوم)
يعتمد على قوة المفتاح وتعقيد الخوارزمية.	>1020>1020 operations	10121012 operations	متوسط وقت الكسر (هجوم النص العادي المعروف ،sim)
من المتوقع أن تكون أنظمة GAN أبطأ بكثير بسبب النفقات العامة للشبكة العصبية	50	0.5	سرعة التشفير (ميجابايت / ثانية)
فك التشفير في الأنظمة المستندة إلى GAN (إذا تم تنفيذه) معقد بالمثل.	50	0.4	سرعة فك التشفير (ميجابايت /ثانية)
يجب أن يضمن كلا النظامين استرجادا عالي الدقة للنص العادي.	0%	< 0.001%	جودة النص المشفر (معدل خطأ البت بعد فك التشفير)

4.1.1 مناقشة النتائج المتوقعة (تجربة 1)

تشير النتائج الافتراضية في الجدول (1) إلى أن الشبكات العصبية التوليدية لديها القدرة على إنتاج مفاتيح تشفير ذات مستويات عالية جدًا من العشوائية، تقترب من تلك التي تنتجها مولدات الأرقام العشوائية الزائفة الآمنة والمعتمدة, إن تحقيق متوسط إنتروبيا قريب جدًا من المثالي (1.0) ونسبة عالية من اجتياز اختبارات NISTالصارمة يدعم فرضية أن GANs يمكن أن تكون مصدرًا موثوقًا لمفاتيح التشفير. ومع ذلك، فإن الزمن المتوقع لتوليد المفتاح بواسطة GANs قد يكون أعلى بشكل ملحوظ مقارنة بـ PRNGs التقليدية. هذا الفارق في الأداء الزمني يعود إلى الطبيعة الحسابية المكثفة لشبكات التعلم العميق. قد يكون هذا مقبولاً في التطبيقات التي لا يكون فيها توليد المفاتيح فائق السرعة أمرًا حاسمًا، أو حيث يمكن تبرير التكلفة الإضافية في الأداء مقابل الفوائد الأمنية المحتملة الأخرى (مثل القدرة على توليد مفاتيح مرتبطة بسياق معين، وهو ما لم يتم استكشافه في هذه التجربة الافتراضية الأولية)، إذا تحققت هذه النتائج، فإنها ستجيب جزئيًا على السؤال البحثي المتعلق بقدرة GANs على إنشاء مفاتيح تشفير قوية. كما ستسلط الضوء على المقايضة بين جودة المفتاح وكفاءة التوليد، مما يفتح الباب أمام أبحاث مستقبلية لتحسين سرعة نماذج

GANsالمستخدمة في هذا السياق دون المساس بجودة المفاتيح.

4.2 النتائج المتوقعة لتجربة تطوير نظام تشفير نصي قائم علىGANs

تفترض هذه التجربة تطوير نظام تشفير نصي يعتمد على نموذجGAN ، حيث يعمل المولد كمشفر والمميز كمقيّم لجودة التشفير. بعد تدريب النظام وتقييمه، يمكن توقع النتائج كما هو موضح في الجدول الافتراضي التالي (جدول 2)، والذي يقارن النظام المقترح مع خوارزمية تشفير تقليدية مثل AES في وضع تشغيل مناسب للتطبيقات النصية.

جدول 2: مقارنة افتراضية لأداء نظام التشفير النصي القائم على GANs مع نظام AES

ملاحظات	نظام AES–CBC (مرجعي)	نظام GAN المقترح (متوقع)	مقياس التقييم
يفترض أن GANs تتعلم إخفاء الأنماط الإحصائية، ولكن قد لا تكون مثالية مثل AESالمصممة رياضيًا.	< 1% نظريًا لا يوجد	< 5%	مقاومة تحليل التردد (نسبة نجاح الهجوم)
يعتمد على قوة المفتاح وتعقيد الخوارزمية.	10^20 <عملية حسابية	10^12عملية حسابية	متوسط وقت كسر التشفير (في ظل هجوم نص واضح معروف)
من المتوقع أن يكون نظام GANأبطأ بكثير بسبب طبيعة الشبكات العصبية.	50	0.5	سرعة التشفير (ميجابايت/ثانية)
على افتراض أن عملية فك التشفير في نظام GAN ستكون مشابهة في التعقيد للمولد.	40	0.4	سرعة فك التشفير (ميجابايت/ثانية)
يجب أن يضمن النظام استعادة النص الأصلي بدقة عالية.	%0	< 0.001%	جودة النص المشفر (معدل الخطأ في البت بعد فك التشفير)

4.2.1 مناقشة النتائج المتوقعة (تجربة 2)

تشير النتائج الافتراضية في الجدول 2 إلى أن تطوير نظام تشفير نصي كامل يعتمد على GANs يمثل تحديًا كبيرًا، خاصة فيما يتعلق بالكفاءة. من المتوقع أن تكون سرعة التشفير وفك التشفير أقل بكثير من الخوارزميات التقليدية المحسّنة مثل .AES هذا يرجع إلى أن عمليات الشبكات العصبية تتطلب حسابات أكثر بكثير من العمليات الرياضية المباشرة المستخدمة في.AES من ناحية الأمان، قد يُظهر نظام GANالمقترح مقاومة جيدة لتحليل التردد، حيث يمكن للشبكة أن تتعلم كيفية توزيع رموز النص المشفر بطريقة تخفي الإحصائيات الأصلية للنص الواضح. ومع ذلك، فإن تحقيق مستوى أمان مماثل لـ AES ضد الهجمات الأكثر تطورًا (مثل هجمات النص الواضح المعروف أو هجمات النص المشفر المختار) سيتطلب تصميمًا دقيقًا للغاية للنموذج وعملية تدريب قوية. قد تكون هناك نقاط ضعف كامنة في النماذج القائمة على التعلم لم يتم اكتشافها بعد إذا تحققت هذه النتائج، فإنها ستشير إلى أن استخدام GANs كبديل مباشر لخوارزميات التشفير المتناظرة عالية الأداء قد لا يكون عمليًا في الوقت الحالي لمعظم التطبيقات التي تتطلب سرعة عالية. ومع ذلك، قد تكون هناك مجالات متخصصة يمكن أن تكون فيها هذه الأنظمة مفيدة، مثل الحالات التي تكون فيها القدرة على التكيف أو التعلم من البيانات ذات أهمية قصوى، أو في تطبيقات التشفير التي يمكن أن تتحمل زمن انتقال أعلى. كما يمكن أن تفتح هذه النتائج الباب أمام أبحاث هجينة تجمع بين قوة الخوارزميات التقليدية ومرونة النماذج القائمة على التعلم.

بشكل عام، تشير النتائج المتوقعة من كلتا التجربتين إلى أن الشبكات العصبية التوليدية تحمل وعودًا في جوانب معينة من تحسين تشفير البيانات، ولكنها تواجه أيضًا تحديات كبيرة، لا سيما فيما يتعلق بالكفاءة الحسابية والتحقق الصارم من الأمان

5. الخاتمة (التوصيات والدراسات المستقبلية)

بناءً على التحليل النظري الشامل والنتائج التجريبية المتوقعة، يؤكد هذا البحث على الإمكانات الواعدة للشبكات العصبية التوليدية في تحسين جوانب محددة من أنظمة التشفير، رغم التحديات القائمة في الجوانب الحسابية والأمنية. وتكمن القيمة المضافة في اقتراحه لمنهجية متكاملة للتقييم، وفتحه آفاقًا جديدة للبحث في مجال التكامل بين تقنيات الذكاء الاصطناعي وأمن المعلومات. تشير النتائج إلى أن التطورات المستقبلية في هذا المجال قد تسهم بشكل جذري في مواجهة التهديدات الأمنية المتطورة في العصر الرقمي. من المتوقع أن تساهم GANs في معالجة ضعف بعض مولدات المفاتيح من خلال إنتاج مفاتيح ذات عشوائية عالية .يمكن تصميم نماذج GANs لتوليد مفاتيح تشفير معقدة، ولكن قد يكون ذلك على حساب

سرعة التوليد تطوير خوارزميات تشفير جديدة بالكامل باستخدام GANs يواجه تحديات كبيرة في الأداء والأمان المضمون مقارنة بالخوارزميات التقليدية، ولكنه يفتح آفاقًا للتعلم التكيفي .من غير المرجح أن تتفوق أنظمة التشفير القائمة على GANs على الأنظمة التقليدية مثل AES في مقاومة جميع أنواع الهجمات وفي الكفاءة في المدى القريب، ولكنها قد تقدم مزايا في سيناريوهات محددة التحديات العملية تشمل التعقيد الحسابي، الحاجة إلى مجموعات بيانات كبيرة للتدريب (في بعض التطبيقات)، وصعوبة التحقق الرسمي من الأمان. إذا تحققت هذه النتائج، فإن البحث سيقدم رؤى حول الإمكانيات الحالية والقيود المفروضة على استخدام GANs في التشفير. سيساهم في تحديد المجالات التي يمكن أن تكون فيها GANsمفيدة بشكل واقعي (مثل توليد المفاتيح أو كجزء من أنظمة هجينة) والمجالات التي لا تزال تتطلب تطورًا كبيرًا.

من المهم التأكيد على أن هذه نتائج متوقعة. قد تختلف النتائج الفعلية بناءً على التنفيذ الدقيق للنماذج، وجودة بيانات التدريب، والمعلمات الفائقة المختارة. كما أن تقييم الأمان لأنظمة التشفير القائمة على التعلم لا يزال مجالًا بحثيًا نشطًا، وقد تظهر أنواع جديدة من الهجمات التي تستهدف هذه النماذج. حتى لو كانت النتائج الفعلية تظهر أن GANs ليست جاهزة بعد لاستبدال أنظمة التشفير التقليدية في جميع التطبيقات، فإن استكشاف هذا المجال يظل ذا قيمة.

5.1 التوصيات

يطرح البحث توصيات قابلة للتطبيق وإتجاهات بحثية مستقبلية في مجال إستخدام الشبكات العصبية التوليدية (GANs) في تحسين تشفير البيانات.

5.1.1 التوصيات البحثية والعملية

تنحصر في مجموعة من التوصيات التطويرية:

أ. **تحسين كفاءة النماذج:** إعتماد تقنيات التكميم (Quantization) وتقطير النماذج (Model Distillation)لخفض متطلبات الحساب.

ب. **تعزيز الأمان:** تطوير إطار عمل لاختبار مقاومة الهجمات الخادومية (Adversarial Attacks) على نماذج التشفير التوليدية.

5.1.2 توصيات تطبيقية

وتشتمل على سيناريوهات الإستخدام الأمثل والتركيز على تطبيقات لا تشترط زمن إستجابة منخفض، مثل أنظمة إدارة المفاتيح الديناميكية وتشفير البيانات غير الحرجة من خلال التكامل الهجين ودمج (GANs)

مع خوارزميات مثبة، مثل (AES) في أنظمة توليد المفاتيح تكييف معاملات التشفير من خلال الاتجاهات البحثية المستقبلية وتحسين النماذج التوليدية معماريات متخصصة من خلال تصميم GANs ذات بنى خفيفة الوزن (Lightweight GANs) مع الحفاظ على الخصائص الأمنية وايضاً التعلّم المعزز إستكشاف إستخدام RL–GANs لتحسين التكيف مع أنماط الهجوم المتغيرة. يُلاحظ أن دمج الشبكات العصبية التوليدية في أنظمة التشفير يمثل مجالًا بحثيًا واعدًا، يوفر إمكانيات غير مسبوقة في توليد مفاتيح قوية، تطوير خوارزميات جديدة، وتعزيز مقاومة الهجمات, لكن تطبيق هذه التقنيات يتطلب معالجة تحديات تتعلق بالأمان، الموارد، التفسير، وقابلية التطبيق العملي لضمان حلول فعالة وآمنة في عالم رقمي متزايد التعقيد.

المراجع

المراجع الأجنبية

- Bhat, R. and Nanjundegowda, R. (2025). A Review on Comparative Analysis of Generative Adversarial Networks' Architectures and Applications. *Journal of Robotics and Control (JRC)*, 6(1), 54-64. 10.18196/jrc.v6i1.24160.
- Courville, A. (2016). *Deep Learning*. MIT Press
- Geron, A. (2019). *Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow*. 2nd Edition. O'Reilly Media.
- Goodfellow, I., Bengio, Y. and Courville, A. (2016). *Deep Learning*. MIT Press.
- Hansen, C. (2022). *Generative adversarial networks explained*. Available at: https://developer.ibm.com/articles/generative-adversarial-networks-explained/ (Accessed on 20/1/2026).
- Hitaj, B., Gasti, P., Ateniese, G. and Perez-Cruz, F. (2017). PassGAN: A Deep Learning Approach for Password Guessing. In book: *Applied Cryptography and Network Security*. https://doi.org/10.1007/978-3-030-21568-2_11.
- Raschka, S. and Mirjalili, V. (2019). *Python Machine Learning*. 3rd Edition. Packt Publishing.
- Rukhin, A., Soto, J., Nechvatal, J., Smid, M. and Barker, E. (2001). *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*. Available at: https://www.researchgate.net/publication/235090427_A_Statistical_Test_Suite_for_Random_and_Pseudorandom_Number_Generators_for_Cryptographic_Applications (Accessed on 12/3/2026).
- Stinson, D. R. and Paterson, M. (2018). *Cryptography: Theory and Practice*. CRC Press