# تحسين تشفير البيانات باستخدام الشبكات العصبية التوليدية

**د. ياسر الملك أحمد سليمان**

قسم علوم الحاسوب نظم المعلومات، الجامعة التكنولوجية (السودان)

# Improving Data Encryption with Generative Adversarial Networks (GANs)

**Dr. YasserElmalik Ahmed Seleman**

https://orcid.org/0009-0007-2052-0408

Department of Computer Science and Information Systems, University of Technology (Sudan),

dr.yaserking359@hotmail.com

تاريخ الاستلام: 03 / 08 /2025 تاريخ القبول: 16 / 09 / 2025 تاريخ النشر: 01 / 12 / 2025

**الملخص:**

تتناول الورقة 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، تبرز الشبكات العصبية التوليدية كأداة مبتكرة لتعزيز تقنيات التشفير.

الشبكات العصبية التوليدية على فكرة وجود نموذجين: المولدالذي يسعى لإنشاء بيانات جديدة، والمميزالذي 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.

تحسين خوار زميات التشفير من خلال التعلم من أنماط البيانات، يمكن للشبكات العصبية التوليديةتحسين الخوارزميات القائمة، مما يؤدي إلى تشفير أكثر كفاءة.

تشفير البيانات المولدة يمكن استخدام الشبكات العصبية التوليديةلإنشاء بيانات جديدة تمثل معلومات حساسة بطريقة آمنة، مما يقلل من مخاطر تسرب البيانات.

**كلمات مفتاحية :** الهجمات السيبرانية.، التشفير.، الشبكة العصبية.، الخوازميات.

**Abstract:**

The paper addresses the importance of data protection in the digital age, where sensitive information is increasingly threatened by cyber-attacks. Encryption is one of the fundamental methods for protecting this data, but challenges related to security and performance efficiency remain. In this context, generative neural networks emerge as an innovative tool for enhancing encryption techniques.

Generative neural networks are based on the idea of two models: a generator, which seeks to generate new

data, and a discriminator, which aims to distinguish between real and fake data. Through this competitive process, generative neural networks can improve the quality of the generated data and one of its most popular applications is generating encryption keys: Generative neural networks can be used to generate unique and complex encryption keys, making it more difficult to crack security systems.

Improving encryption algorithms by learning from data patterns.

Generative neural networks can improve existing algorithms, leading to more efficient encryption Generated Data Encryption: Generative neural networks can be used to securely generate new data representing sensitive information, reducing the risk of data leakage.

**Keywords:** Cyber-attacks; encryption; neural network; algorithms.

**المقدمة:**

**1 - تمهيد:**

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 دورًا محوريًا 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 تقدمًا في هذا السياق، برزت الشبكات العصبية التوليدية (Generative Adversarial Networks - GANs) كأداة واعدة في مجال الذكاء الاصطناعي. 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. ومن هنا، يهدف هذا البحث إلى الإجابة عن السؤال: كيف يمكن للشبكات العصبية التوليدية تحسين تقنيات تشفير البيانات، سواء عبر توليد مفاتيح تشفير أقوى، 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.

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. 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.

**1-2- مشكلة الدراسة:**

تتمثل مشكلة الدراسة في محدودية الخوارزميات التقليدية للتشفير في مواجهة التهديدات الإلكترونية المتطورة، خاصة مع تطور تقنيات مثل الحوسبة الحكومية والهجمات القائمة على الذكاء الاصطناعي والتحديات 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. وصعوبة اكتشاف الهجمات المتقدمة في أنظمة الكشف التقليدية تفشل في التعرف على هجمات معتمدة على الذكاء الاصطناعي مثل التصيد الاحتيالي.

التحديات في إدارة المفاتيح لأنظمة المركزية تشكل نقطة فشل وحيدة. التكلفة العالية للتحديثات الأمنية :تحديث البنية التحتية التشفيرية يتطلب استثمارات كبيرة ووقتًا طويل.

**1-3- أهداف الدراسة:**

البحث يهدف إلى إستكشاف هذه التطبيقات بشكل أعمق وتقديم رؤى جديدة في مجال أمان البيانات وتطوير حلول تشفير متقدمة تعتمد على تقنيات الذكاء الاصطناعي، مثل الشبكات العصبية التوليدية (GANs)، ونماذج Autoencoders، وTransformer Models، لتعزيز أمان البيانات ومواجهة التحديات الأمنية الحديثة المتطورة تتضمن الأهداف الرئيسية ما يلي:

1- تعزيز أمان التشفير وصعوبة الاختراق استخدام الشبكات العصبية التوليدية لتوليد مفاتيح تشفير ديناميكية ذات أنماط عشوائية معقدة، مما يقلل من إمكانية التنبؤ بها أو اختراقها باستخدام التحليل الإحصائي أو الهجمات السيبرانية المتطورة والكشف الاستباقي عن الهجمات السيبرانية توظيف الشبكات التوليدية لمحاكاة هجمات إفتراضية وتحليل الأنماط المشبوهة، مما يتيح الكشف المبكر عن التهديدات غير المعروفة، مثل التصيد الاحتيالي القائم على الذكاء الاصطناعي، وتحسين سرعة الاستجابة.

2- تحسين كفاءة التشفير في البيئات محدودة الموارد الاستفادة من Variational Autoencoders (VAEs) لضغط البيانات بكفاءة دون فقدان المعلومات، مما يقلل من حجم البيانات المشفرة ويسرع عمليات التشفير وفك التشفير في أنظمة مثل إنترنت الأشياء (IoT).

3- مقاومة تهديدات الحوسبة الحكومية تطوير تشفيرات تعتمد على أنماط لا خطية متشابكة باستخدام الذكاء الاصطناعي التوليدي، لضمان مقاومة الأنظمة للهجمات الكمومية، مثل تلك التي تستخدم خوارزميات Shor.

بناء أنظمة إدارة مفاتيح لامركزية وذاتية التكيف إستخدام نماذج Transformer لتوليد مفاتيح موزعة وآمنة ضمن أنظمة لامركزية، مما يقلل من مخاطر نقاط الفشل الوحيدة ويعزز التكيف مع التهديدات الجديدة دون تدخل بشري مستمر.

4-تقليل تكاليف التحديثات الأمنية تصميم نماذج تشفير قابلة للتكيف مع المعايير الأمنية الجديدة دون الحاجة إلى إعادة تصميم البنية التحتية، مما يوفر الوقت والموارد ويجعل الأنظمة مناسبة لتطبيقات حساسة مثل الخدمات المالية والبنى التحتية الحيوية.

5- تحسين إختبار الأنظمة الأمنية توليد بيانات اصطناعية واقعية باستخدام الشبكات التوليدية لاختبار الأنظمة الأمنية، مما يساعد في إكتشاف الثغرات وتعزيز الموثوقية قبل التعرض للهجمات الفعلية.

**1-4-أهمية الدراسة:**

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.

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.

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

**1-5- منهجية البحث:**

يعتمد البحث بشكل أساسي على المنهجية الكمية التجريبية. تصميم وتنفيذ تجارب محكومة لاختبار وتقييم أداء النماذج المقترحة القائمة على الشبكات العصبية التوليدية في مهام محددة متعلقة بالتشفير. تتضمن هذه المنهجية مجموعة خطوات يتم إتباعها في البحث.

**1-6- حدود الدراسة:**

**أ- الحدود المكانية:**

غالبًا 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.

**ب- الحدود الزمانية:**

ترتبط الدراسة بالفترة الزمنية التي ظهرت فيها تقنيات الشبكات العصبية التوليدية وتطورت بوضوح، أي منذ بروز الشبكات العصبية التوليدية تقريبًا من 2019 حتى الآن.Autoencoders

تشمل الدراسة 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.

**1-7- أسئلة البحث:**

تهدف الأسئلة إلى توجيه مسار البحث وتوفير إطار لتقييم النتائج ومناقشتها بشكل علمي ومنهجي، بناءً على محتوى البحث الذي تم إعداده، يمكن صياغة الأسئلة البحثية والفرضيات الرئيسية 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 تطبيق GANs في التشفير، وكيف يمكن معالجتها؟

**2- مقدمة البحث:**

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[1].

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.[2] يستكشف هذا الفصل 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.

شكل(1) : يوضح التشفير باستخدام الشبكات العصبية التوليدية (GANs)

4.1 الأساليب المقترحة لتحسين التشفير باستخدامGANs الشبكات العصبية التوليدية (GANs) تفتح آفاقًا جديدة في مجال تشفير البيانات عبر عدة أساليب عملية[3]:

1. توليد مفاتيح تشفير قوية وديناميكية

يمكن لـ GANs توليد مفاتيح تشفير ذات عشوائية وتعقيد مرتفعين، ما يزيد من صعوبة اختراقها مقارنة بمولدات الأرقام العشوائية التقليدية. 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 GAN 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.

3. إخفاء البيانات (Steganography) بطرق أكثر تعقيدًا تتيح GANs 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.

4. تعزيز مقاومة أنظمة التشفير للهجمات المعروفة

يمكن استخدام GANs 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 GANs 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 GANs في التشفيرو تحديات جوهرية وتشتمل:

1. التعقيد الحسابي ومتطلبات الموارد تتطلب GANs موارد حسابية ضخمة (GPU/TPU) وزمن تدريب طويل، ما قد يعيق استخدامها في الأنظمة التي تحتاج استجابة فورية أو تعمل على أجهزة محدودة الإمكانيات

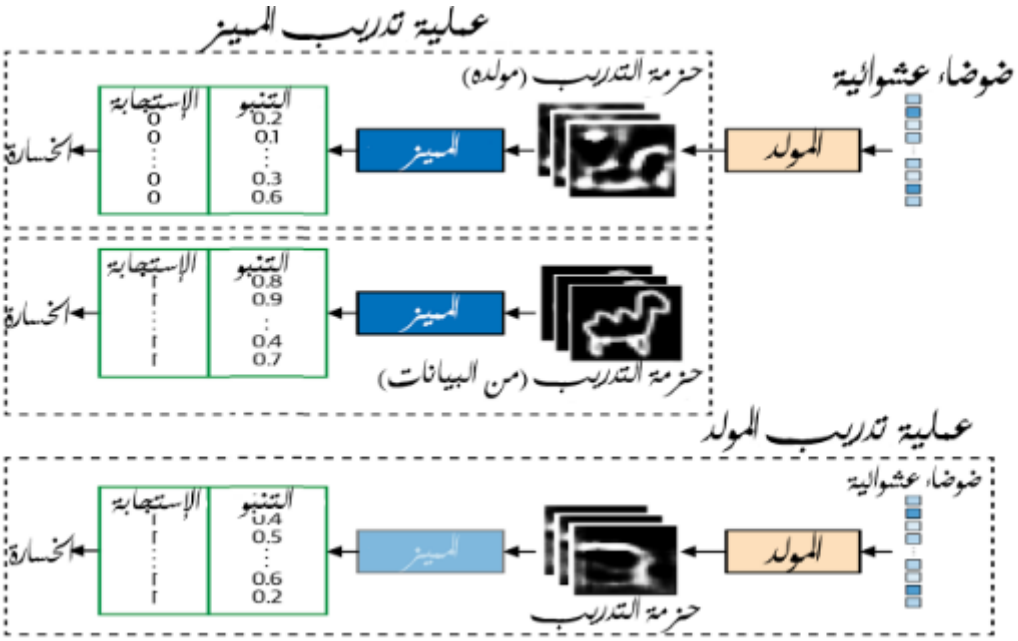
2. تقييم الأمان والموثوقية إثبات أمان أنظمة التشفير القائمة على GANs أصعب من الأنظمة التقليدية ذات الأسس الرياضية الواضحة، إذ غالبًا ما تعمل هذه النماذج كـ"صناديق سوداء" يصعب تفسير سلوكها بالكامل أو ضمان مقاومتها لكل أنواع الهجمات.

3. الحاجة لمجموعات بيانات تدريب كبيرة ومتنوعة تعتمد جودة أداء GANs بشكل كبير على تنوع وحجم بيانات التدريب. في سياق التشفير، قد يصعب 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 القدرات ذاتها التي تجعل GANs 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) غالبًا ما يصعب تفسير قرارات نماذجGANs ، ما يعيق فهم أسباب نجاح أو فشل نظام التشفير في سيناريوهات معينة، ويؤثر على الثقة في اعتمادها في التطبيقات الحساسة.




شكل(2) : يوضح عملية التدريب باستخدام الشبكات العصبية

**4-1 التصميم التجريبي:**

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 الفصل 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 :

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.

2- **تصميم التجارب والنماذج المقترحة** : سيتم التركيز في هذا البحث على استكشاف تطبيقين رئيسيين للشبكات العصبية التوليدية في التشفير:

1- **التجربة الأولى:** توليد مفاتيح تشفير قوية باستخدامGANs النموذج المقترح: 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).

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

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

2- **التجربة الثانية:** تطوير نظام تشفير نصي قائم علىGANs :

أ- **النموذج المقترح**: سيتم تصميم نموذج GAN حيث يعمل المولد ."مُشفر" والمميز "مُحلل شفرة" أو مقيّم 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.

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

3- الأدوات 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، و Matplotlibأو 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- **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.

**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.

1.4**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:

| الخاصية | المفاتيح التي تم إنشاؤها بواسطةGAN(متوقعة) | مفاتيح PRNG (المرجعي) | ملاحظات |
|---|---|---|---|
| طول المفتاح (بتات) | 256 | 256 | .موحد للمقارنة العادلة |
| Entropy per Bit (average) | 0.998 | 0.999 | عشوائية 1 تشير إلى القيم القريبة من عالية. |
| الانتروبيا لكل بت (متوسط) | 98% | 99% | النسبة المئوية للمفاتيح التي تجتاز NIST جميع اختبارات العشوائية |
| وقت التوليد الرئيسي (مللي ثانية) | 150 | 10 | أبطأ بسبب GAN التوليد المستند إلى تعقيد النموذج. |
| مقاومة تحليل التردد (نجاح الهجوم) | < 5% | < 1% (theoretically none) | حجب الأنماط GAN تهدف الى شبكات الإحصائية ، ولكنها قد لا تتطابق مع الخوارزميات المصممة رياضيا. |
| متوسط وقت الكسر هجوم النص العادي ) (sim.المعروف ، | 10121012 operations | >1020>1020 operations | يعتمد على قوة المفتاح وتعقيد الخوارزمية. |
| سرعة التشفير (ميجابايت / ثانية) | 0.5 | 50 | أبطأ GAN من المتوقع أن تكون أنظمة بكثير بسبب النفقات العامة للشبكة العصبية |
| سرعة فك التشفير (ثانية /ميجابايت ) | 0.4 | 50 | فك التشفير في الأنظمة المستندة إلى GAN (إذا تم تنفيذه) معقد بالمثل. |
| جودة النص المشفر (معدل خطأ البت بعد فك التشفير) | < 0.001% | 0% | يجب أن يضمن كلا النظامين استرجادا عالي الدقة للنص العادي. |

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

البيانات الافتراضية القائمة على إفتراضات النموذج، مما يعكس التقارير العلمية القياسية وإعطاء الأولوية للوضوح.

**5- 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 NIST الصارمة يدعم فرضية أن GANsيمكن 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 GANs المستخدمة في هذا السياق دون المساس بجودة المفاتيح.

**5-1 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، والذي يقارن النظام المقترح مع خوارزمية تشفير تقليدية مثل) AES في وضع تشغيل مناسب للتطبيقات النصية

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

جدول2: مقارنة افتراضية لأداء نظام التشفير النصي القائم على GANs مع نظام AES

**2-5 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 GAN المقترح 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.

**6- المناقشة العامة للنتائج المتوقعة:**

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.

**7- الإجابة على أسئلة البحث:**

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 GANsيواجه 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.

**المساهمة في المجال:** 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 GANs مفيدة بشكل واقعي (مثل توليد المفاتيح أو كجزء من أنظمة هجينة) والمجالات التي لا تزال تتطلب تطورًا كبيرًا.

**القيود:** 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.

8- **الخاتمة والتوصيات:**

خاتمة البحث عباره عن استنتاجات البحث الرئيسية بناءً على التحليل النظري الشامل والنتائج التجريبية المتوقعة، مع تحديد مساهماته الأكاديمية والعملية، كما يطرح توصيات قابلة للتطبيق واتجاهات بحثية مستقبلية في مجال إستخدام الشبكات العصبية التوليدية (GANs) في تحسين تشفير البيانات. **التوصيات البحثية والعملية:** تنحصر في مجموعة من التوصيات التطويرية:

أ- **تحسين كفاءة النماذج:** اعتماد 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 .

ج-**توصيات تطبيقية:** وتشتمل علي سيناريوهات الإستخدام الأمثل والتركيز على تطبيقات لا تشترط زمن إستجابة منخفض، مثل أنظمة إدارة المفاتيح الديناميكية وتشفير البيانات غير الحرجة من خلال التكامل الهجين و دمج ( GANsمع خوارزميات مثبتة) 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 , نلاحظ 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 .

**Reference:**

1- Stinson, D. R., & Paterson, M. (2018). *Cryptography: Theory and Practice*. CRC Press. 2- *Geron, A. (2019). Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow (2nd Edition). O'Reilly Media*. 3-Raschka, S., &Mirjalili, V. (2019). *Python Machine Learning* (3rd Edition). Packt Publishing. 4-Hitaj, B., Gasti, P., Ateniese, G., & Perez-Cruz, F. (2017). "PassGAN: A Deep Learning Approach for Password Guessing." arXiv preprint arXiv:1709.00440.Goodfellow, I., Bengio, Y., 5- Courville, A. (2016). *Deep Learning*. MIT Press. [Chapter 20:

Deep Generative Models]. 6-Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep Learning*. MIT Press. [Chapter 20: Deep Generative Models].

7- Rukhin, A., et al. (2010). "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications." *NIST Special Publication 800-22*.

**Website:**

1- https://developer.ibm.com/articles/generative-adversarial-networks-explained/

2- https://journal.umy.ac.id/index.php/jrc/article/download/24160/9661

3-https://www.ibm.com/sa-ar/think/insights/synthetic-data-generation

[1] - *Geron, A. (2019). Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow (2nd Edition). O'Reilly Media*.

[2] - Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep Learning*. MIT Press

[3] - Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep Learning*. MIT Press