الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

المدرسة العليا لأساتذة التعليم التكنولوجي

-سكيكدة-

قسم التكنولوجيا

التخصص: هندسة كهربائية

مذكرة التخرج لنيل شهادة أستاذ التعليم الثانوي

تطبيق الأنظمة الفوضوية في تشفير الصور الرقمية الثابتة

من اعداد:

- بلفراق المختار
- مزواط إبراهيم
- رحماني محمد أمين

تحت اشراف الأستاذة:

بلاسكة نوال

لجنة المناقشة:

دتوش نجمة	أستاذ مساعد أ	رئيسا
بلاسكة نوال	أستاذ محاضر ب	مؤطرا
عثمان إيمان	أستاذ مساعد أ	ممتحنا

السنة الجامعية 2024/2023

شكر وتقدير

الحمد لله رب العلمين وأصلّي وأسلّم على المبعوث رحمة للعالمين وعلى آله وصحبه ومن تبعهم بإحسان إلى يوم الدين وبعد

فإننا من هذا المقام نشكر الله عز وجل أن منّ علينا من فضله وأعاننا على إتمام هذا العمل بنجاح فله الفضل والمنة وله الحمد كله وله الشكر كله بيده الخير كلّه فأهل أن نحمد إنه على كل شيء قدير فنسأله سبحانه عملا صالحا يرضى به عنا .

كما نتقدّم شكرنا لمشرفتنا الفاضلة الأستاذة بلاسكة نوال على توجيهاتها وتعليماتها المستمرة إلى حين إنهاء عملنا المتواضع ولإتاحتها لنا فرصة العمل على هذا الموضوع. لقد كانت نصائحها وملاحظاتها حافزاً كبيراً لنا خلال مسيرتنا الأكاديمية وإنا نشكرها على ذلك شكراً كثيرا فنسأل الله أن يجزل لها المثوبة.

كما نتوجه بالشكر لأعضاء لجنة التحكيم الأفاضل، الذين تفضلوا بقبول مهمة تقييم هذا العمل. فنقدّر لهم وقتهم الثمين وسعيهم المبذول في دراسة وتقييم بحثنا . وغدونا شاكرين همكم العلية.

ولا يفوتنا أن نعبر عن شكرنا لجميع الأساتذة الذين ساهموا في تعليمنا وتكويننا الأكاديمي، وخاصة أساتذة قسم الإلكترونيات. لقد كان لجهودهم وسعيهم أثر كبير في توجيه مسيرتنا التعليمية.

وختاما، بكل الحب والوفاء وبأرق كلمات الشكر والثناء، ومن قلوب ملؤها الإخاء نتقدم بالشكر إلى كل من ساعدنا، من قريب أو بعيد، في إنجاز هذا العمل. كما نتقدم بالشكر إلى كلّ من علمنا معنى النجاح، وغرس فينا حب التميز فإنّه لا بقاء للنعمة إذا كفرت، ولا زوال لها إذا شكرت. وكما قال رسولنا الأمين عليه صلوات الله وأزكى التسليم: "لا يشكر الله من لا يشكر الناس" فنسأل الله أن يجعل هذا العمل خالصاً لوجهه الكريم وأن ينفع به النفع العميم لكل من تلقاه بقلب سليم. إنه ولي التوفيق والهادي إلى أصوب الطريق.

والمرجو ممن اطّلع على هذا العمل وصرف وجهه إليه أن يُصلح خلله بعد التأمل والإمعان بقلم الإنصاف والإحسان لأن الإنسان مركز الجهل والنسيان.

إهداء

إلى من علمني أولى حروف الحياة، وأهداني الأمل والدعم والحنان، إلى "**أمي الغالية**"، التي كانت ولا تزال سندي وملاذي في كل حين، أهديك ثمرة تعبي وجهدي.

إلى "**أبي العزيز**"، الذي لم يتوانَ يوماً عن تقديم كل ما بوسعه لتأمين مستقبلي وتحقيق طموحاتي، أقدم لك هذا العمل تعبيراً عن شكري وامتناني العميقين.

إلى "**أخواتي العزيزات**"، اللواتي كنَّ دوماً معي في كل خطوة أخطوها، يزهر عن البسمة في وجهي ويدعمني بكل حب، أهديكن هذا الإنجاز.

إلى أصدقاء الدراسة "**أشرف**" "**آدم**" "**سعد**" "**لمين**" "**فيصل**" "**عماد**" "**ياسين**" "**أيمن**" "**عبد المعز**" "**براهيم**" "**سيدأحمد**" "**دادي**" "**نبيل**" "**فارس**" "**عاشور**" "**سامي**"، الذين شاركوني السهر والتعب، وكانوا رفاق الدرب في مسيرتي الأكاديمية، شكراً لكم على كل لحظة تقاسمنا فيها الفرح والحزن.

إلى أصدقائي الأعزاء "**حامادا**" "**أنور**" "**سعيد**"، الذين كانوا دائماً مصدر قوة وإلهام لي، ووقفوا بجانبي في أصعب الأوقات، أهديكم هذا الإنجاز بفخر واعتزاز.

إلى أساتذتي الأفاضل، الذين كانوا نبراساً للعلم والمعرفة، وأضاءوا دربي بنور علمهم وإرشاداتهم، أهديكم هذا العمل عرفاناً وتقديراً.

إلى أساتذتي في الثانوية "**عطاف مليكة**" "**عيدي**" "**صحراوي عبد القادر**"، الذين كانوا نبراساً للعلم والمعرفة، وأضاءوا دربي بنور علمهم وإرشاداتهم، أهديكم هذا العمل عرفاناً وتقديراً.

إلى كل من ساندني ودعمني خلال مسيرتي الدراسية، ولو بكلمة طيبة أو دعوة صادقة، أقدم لكم هذا الإهداء تعبيراً عن امتناني الكبير.

دمتم جميعاً ذخراً لي وأدامكم الله سنداً وعوناً، وشكراً لكم من القلب.

مختار

إهداء

عبر نفحات النسيم وأريج الأزاهير وخيوط الأصيل أرسل شكراً من الأعماق لوالديّ

بشوق الأزاهير وروائح المسك وبصوت الفرح ينبثق صوتي لأغلى ما نملك قائلا شكراً لكما على عطائكما يا أبواي

كلمات الثناء لا توفيك حقك، شكراً لك على عطائك يا أمي .

مهما بحثت في قاموس الكلمات ونثرت من عبارات الشكر فلن ولم أجد كلمات توفيك حقك وقدرك يا أبي .

وفي أعماق نفسي يتصاعد الشكر لكما بخوراً لأنكما أوحيتما إليّ ما عجز دونه الآخرون .

إلى كل من يذكرهم القلب قبل أن يكتب القلم إلى من قاسموني حلو الحياة ومرها تحت السقف الواحد "إخوتي"

إلى كل أقاربي إلى كل إخواني الذين طالما أحببتهم وأحبوني إلى الذين طالما لم يتوقفوا يوما عن تشجيعي .

إلى أصدقائي الذين طالما ألفتهم وألفوني أنا اسطر عباراتي والأسى يرافقني

إبراهيم

إهداء

الحمد لله أولا وآخرا والشكر له ظاهرا وباطنا .

أما بعد فيقول رسول الله صلى الله عليه وعلى آله وصحبه ومن اهتدى بهديه واستن بسنته إلى يوم الدين: "لا يشكر الله من لا يشكر الناس"

أتقدم بجزيل الشكر لله أولا ثم لوالدي الذين ربياني ووصلت بسببهما إلى ما أنا عليه أبي العزيز شفاه الله وأمي الفاضلة أحسن الله إليهما ثم أخي عبد الحق وفقه الله ثم أختي جزاها الله خيرا ثم لمن علمني ولو حرفا من الابتدائي إلى يومنا هذا وإلى كل أساتذة المدرسة العليا وأستاذتنا المؤطرة أهدي تحياتي وشكري وثنائي وتقديري فقد كانت معلمة لنا ومرافقة طيلة فترة كتابة المذكرة وأحيي كل من يقرأ هذه المذكرة ثم إلى أخي وصديقي زميل الدراسة إسلام وسعد قسمي والمختار وإبراهيم وغيرهم ممن كان له فضل بعد فضل الله .

تعلم فليس المرء يولد عالما

وليس أخو جهالة كمن هو عالم

أسأل الله أن يبارك في الجميع ويجزيهم خير الجزاء "إن ربي لسميع الدعاء" وصلى الله وسلم على نبينا محمد وعلى آله وصحبه وسلم .

محمد الأمين

الملخص

تشفير الصور الرقمية باستخدام الأنظمة الفوضوية، وبالأخص الخريطة اللوجستية ثنائية الأبعاد، هو تقنية حديثة تهدف إلى حماية الصور من الوصول غير المصرح به. تعتمد هذه التقنية على خصائص الفوضى التي تتميز بالعشوائية العالية والحساسية الكبيرة للشروط الابتدائية.

الأنظمة الفوضوية تُظهر سلوكًا عشوائيًا ناتجًا عن معادلات رياضية. الخريطة اللوجستية ثنائية الأبعاد تعد مثالًا بارزًا على هذه الأنظمة، حيث تتميز بقدرتها على توليد تسلسلات عددية معقدة وحساسة لأي تغييرات بسيطة في الشروط الابتدائية.

عملية التشفير تبدأ بتحويل الصورة إلى مصفوفة من القيم الرقمية التي تمثل البكسلات. بعد ذلك، يتم استخدام الخريطة اللوجستية ثنائية الأبعاد لتوليد تسلسلات فوضوية بناءً على قيم ابتدائية محددة تعتبر مفتاحا للتشفير. هذه التسلسلات تُستخدم لإعادة ترتيب مواقع البكسلات عن طريق الخلط، مما يجعل من الصعب التعرف على الصورة الأصلية. بعد ذلك، تُعدل قيم البكسلات عن طريق الانتشار بحيث يؤدي أي تغيير طفيف في الصورة الأصلية إلى تغييرات كبيرة في الصورة المشفرة. المرحلة النهائية هي دمج نتائج الخلط والانتشار للحصول على الصورة المشفرة النهائية.

استخدام الخريطة اللوجستية ثنائية الأبعاد في تشفير الصور يوفر مستوى عاليًا من الأمان بفضل تعقيدها الفائق وقدرتها على إنتاج نتائج غير قابلة للتنبؤ. بالإضافة إلى ذلك، تتطلب هذه العملية حسابات رياضية بسيطة نسبيًا، مما يجعلها مناسبة للتطبيقات التي تتطلب معالجة سريعة وفي الوقت الحقيقي. بشكل عام، يعتبر تشفير الصور باستخدام الخريطة اللوجستية ثنائية الأبعاد من الأساليب الفعالة والآمنة لحماية الصور الرقمية.

كلمات مفتاحية: الأنظمة الفوضوية، تشفير الصور، الخلط، الإنتشار.

Summary

Digital image encryption using chaotic systems, particularly the two-dimensional logistic map, is a modern technique aimed to protect images from unauthorized access. This technique relies on the high randomness and significant sensitivity to initial conditions.

Chaotic systems exhibit random behavior resulting from mathematical equations. The two-dimensional logistic map is a prominent example of these systems, known for their ability to generate complex numerical sequences that are highly sensitive to any slight changes in initial conditions.

The encryption process begins by converting the image into a matrix of digital values representing the pixels. Then, the two-dimensional logistic map is used to generate chaotic sequences based on a specific initial value that serve as the encryption key. These sequences are used to rearrange the pixel positions through scrambling, making it difficult to recognize the original image. Subsequently, pixel values are modified through diffusion so that any minor change in the original image results in significant changes in the encrypted image. The final stage is to combine the results of scrambling and diffusion to obtain the final encrypted image.

Using the two-dimensional logistic map in image encryption provides a high security level due to its extreme complexity and its ability to produce unpredictable results. Moreover, this process requires relatively simple mathematical computations, making it suitable for applications that demand fast, real-time processing. Overall, image encryption using the two-dimensional logistic map is considered an effective and secure method for protecting digital images.

Key words: chaotic systems, image encryption, confusion, diffusion.

Résumé

Le chiffrement des images numériques utilisant des systèmes chaotiques, en particulier la carte logistique bidimensionnelle, est une technique moderne visant à protéger les images contre tout accès non autorisé. Cette technique repose sur les caractéristiques du chaos, qui sont : le caractère pseudo aléatoire et la sensibilité significative aux conditions initiales.

Les systèmes chaotiques montrent un comportement aléatoire résultant d'équations mathématiques. La carte logistique bidimensionnelle est un exemple emblématique de ces systèmes, connue pour sa capacité à générer des séquences numériques complexes qui sont très sensibles à tout changement minime des conditions initiales.

Le processus de chiffrement commence par convertir l'image en une matrice de valeurs numériques représentant les pixels. Ensuite, la carte logistique bidimensionnelle est utilisée pour générer des séquences chaotiques basées sur des valeurs initiales spécifiques qui servent de clé de chiffrement. Ces séquences sont utilisées pour réorganiser les positions des pixels par un mélange, rendant difficile la reconnaissance de l'image originale. Par la suite, les valeurs des pixels sont modifiées par diffusion de sorte que tout changement mineur dans l'image originale entraîne des changements significatifs dans l'image chiffrée. La dernière étape consiste à combiner les résultats du mélange et de la diffusion pour obtenir l'image chiffrée finale.

L'utilisation de la carte logistique bidimensionnelle dans le chiffrement des images offre un haut niveau de sécurité grâce à sa complexité extrême et à sa capacité à produire des résultats imprévisibles. De plus, ce processus nécessite des calculs mathématiques relativement simples, ce qui le rend adapté aux applications nécessitant un traitement rapide et en temps réel. Dans l'ensemble, le chiffrement des images en utilisant la carte logistique bidimensionnelle est considéré comme une méthode efficace et sécurisée pour protéger les images numériques.

Mots clé : Systèmes chaotique, cryptage d’image, confusion, diffusion.

الفهرس

الفصل الثاني: عموميات حول الصور الرقمية

قائمة الأشكال

قائمة الجداول

قائمة الاختصارات

الاختصار	أصل الاختصار بالإنجليزي	ترجمة الاختصار بالعربي
IBM Watson	International Business Machines	شركة الآلات والتجارة العالمية
DES	Data Encryption Standard	معيار تشفير البيانات
AES	Advanced Encryption Standard	معيار التشفير المتقدم
RSA	Rivest, Shamir, Adleman	رونالد ريفست، آدي شامير، وليونارد أدلمان
ACM	Arnold's Cat Map	خريطة أرنولد للقطط
IDES	International Data Encryption Standard	المعيار الدولي لتشفير البيانات
CAIN	Confidentiality; Authentication; Integrity ; Non-repudiation	السريّة، المصادقة، سلامة البيانات، عدم الإنكار
XOR	eXclusive OR	أو إستبعادي
PNG	Portable Network Graphic	رسم الشبكة المحمولة
JPEG	Joint Photographic Experts Group	مجموعة الخبراء المشتركة في التصوير الفوتوغرافي
GIF	Graphic Interchange Format	تنسيق تبادل الرسومات
TIFF	Tagged Image File Format	تنسيق ملف الصورة الموسومة
SVG	Scalable Vector Graphic	رسومات المتجهات قابلة للتطوير

EPS	Encapsulated PostScript	البرنامج النصي المغلف
PDF	portable document format	تنسيق المستندات المحمولة
AI	Adobe Illustrator	أدوبي المصور
BMP	bitmap	صورة نقطية
RGB	red, green, and blue	الأحمر، الأخضر والازرق
2D	A two-dimensional	ثنائي البعد
3D	three-dimensional	ثلاثي البعد
LUT	Lookup Table	جدول البحث
PRNG	Pseudo random number generator	مولد أرقام شبه عشوائية
NPCR	Number of Pixels Change Rate	معدل تغيير عدد النقاط الصورية
UACI	Unified Averaged Changed Intensity	معدل التغيير الموحد للكثافة اللونية
IEEE	Institute of Electrical and Electronics Engineers	معهد مهندسي الكهرباء والإلكترونيات

المقدمة العامة

المقدمة العامة

لقد جعل ظهور أجهزة الحاسوب الشخصية والإنترنت من الممكن لأي شخص توزيع المعلومات الرقمية على مستوى عالمي بسهولة واقتصاد. العديد من التطبيقات مثل قواعد بيانات الصور العسكرية، ومؤتمرات الفيديو السرية، ونظام الصور الطبية، وتلفزيون الكابل، والألبومات الشخصية على الإنترنت للصور تتطلب نظام أمان قوي وسريع لتخزين ونقل الصور الرقمية. في هذه البيئة، هناك العديد من مشاكل الأمان المرتبطة بمعالجة ونقل الصور الرقمية عبر شبكة مفتوحة حيث من الضروري ضمان سرية ونزاهة وأصالة الصورة الرقمية المرسلة. أيضا، تشفير الصور يختلف عن تشفير النصوص بسبب بعض الخصائص الجوهرية للصور مثل تكرار البيانات، والترابط القوي بين البكسلات المجاورة، وكونها أقل حساسية مقارنة بالبيانات النصية أي أن تغييرًا طفيفًا في سمة أي بكسل من الصورة لا يؤثر بشكل كبير على جودة الصورة وسعة البيانات الضخمة.

لتلبية هذه الحاجيات، ظهرت مجموعة واسعة من بروتوكولات التشفير في الأدب العلمي. تظهر بعض الأنظمة التقليدية لتشفير البيانات مثل DES وAES وRSA بعض العيوب والضعف في تشفير الصور الرقمية (على سبيل المثال، يحتاج إلى وقت حوسبة كبير وقدرة حاسوبية عالية، لذلك تعاني هذه التقنيات من فاعلية منخفضة عندما يكون حجم الصورة كبيرًا). وبناءً على ذلك، فإنها ليست مناسبة لتشفير الصور. في هذا الصدد، تُعتبر تقنيات التشفير القائمة على الفوضى جيدة للاستخدام العملي، حيث توفر خوارزميات الفوضى مزيجًا جيدًا من السرعة والأمان العالي والتعقيد والعبء الحسابي المعقول والقدرة الحاسوبية. علاوة على ذلك، تتمتع خوارزميات الفوضى وغيرها من خوارزميات الأنظمة الديناميكية بخصائص هامة مثل الاعتماد الحساس على الظروف الابتدائية ومعلمات النظام، وخصائص العشوائية الزائفة، والتردد، وعدم الدورة. تلبي هذه الخصائص بعض المتطلبات مثل الحساسية تجاه المفاتيح، والانتشار والخلط من حيث تشفير المعلومات. لذلك، يتوقع أن تقدم الديناميكيات الفوضوية وسيلة سريعة وسهلة لبناء أنظمة تشفير ذات أداء متفوق.

يحتوي هذا العمل على أربع فصول كل فصل يغطي جانب

فالفصل الأول يتناول لمحة تاريخية عن التشفير والمفاهيم الأساسية للتشفير من تعريف التشفير وتعريف مفتاحه وكيفية عمله وذكر أهدافه وآلياته وشرح مبسط للتشفير الكلاسيكي مع ذكر أنواعه. كما ركزنا في هذا

الفصل على التشفير الحديث وذكر أنواعه من التشفير المتماثل وغير المتماثل وفي الأخير ختمنا الفصل بالتطرق الى تحليل الشفرات.

أما الفصل الثاني فيركز على عموميات حول الصور الرقمية وطرق تشفيرها حيث ألممنا بمعلومات عامة عن الصور الرقمية من تعريف الصورة الرقمية وذكر أنواعها مع التطرق الى صيغ الصور الرقمية وذكر الخصائص الرئيسية للصور الرقمية وأخيرا قمنا بختام الفصل بطرق تشفير الصور والتطرق الى استخدام الفوضى في توليد الأرقام شبه العشوائية مع ذكر أداء قياسات الخوارزميات.

والفصل الثالث يتمحور حول الانظمة الفوضوية حيث ابتدأنا الفصل بنبذة تاريخية عن الأنظمة الفوضوية ثم تطرقنا الى تعريف الانظمة الفوضوية وذكر خصائصها بما في ذلك مخطط التفرع ثم تطرقنا الى الفرق بين الفوضى والعشوائية مع شرح موجز لأقسام الأنظمة الفوضوية كما قمنا بتسليط الضوء بشكل خاص على الخرائط الفوضوية والتشفير الفوضوي وذكر تقنياته مع التطرق الى الخريطة اللوجستية ثنائية الأبعاد وأخيرا ختمنا الفصل بشرح الخوارزمية المطبقة.

وأخيرا الفصل الرابع وهو فصل المحاكاة والنتائج والذي سنقوم فيه بتطبيق الخوارزمية في برنامج الماتلاب بعد ذلك قمنا بتحليل النتائج من جهة تحليل الهيستوغرام ومعامل الارتباط والانتروبيا وتحليل مساحة وحساسية المفتاح.

الفصل الأول

مقدمة حول التشفير

1.1 مقدمة

علم التشفير هو علم موجودٌ منذ قرون. ويعتبر فناّ قديمًا وعلمًا حديثًا، حيث يمثّل علم السّرية. ومنذ اختراع الكتابة أصبحت الحاجة إلى الأمان مبرَّرة نظرًا لقضايا السّرية والنّزاهة، حيث يجب أن تكون المعلومات المكتوبة متاحة فقط للوصول إليها من طرف الأشخاص المناسبين، ويجب ألا يتم تعديلها عمدا لغرض التّزوير، ويجمع علم التشفير بين التشفير وتحليل الشفرات.

كلمة التّشفير تأتي من كلمات يونانية قديمة (Cryptography) حيث كلمة "Crypto" تعني مخفي و"graphy" تعني الكتابة. التّشفير هو فنّ تشفير محتوى رسالة من المحتمل أن يتم اعتراضها أثناء إرسالها. ويتمثل تحليل الشّفرات في كسر مفتاح حماية الرّسالة المُشفرة. لقد تطور علم التّشفير بشكل كبير خاصّة مع ظهور الكمبيوتر، حيث كان مخصَّصًا بشكل أساسي في المجال العسكري والدّيبلوماسي، وتمتد اليوم إلى المجال المدني لأمن البيانات المتداولة على شبكات الكمبيوتر.

في هذا الفصل، سنقدّم نبذة تاريخية مختصرة عن التّشفير، ثمّ سنكشف عن الأسس الرّئيسية للتّشفير وخصائصه وأنواعه المختلفة، ثمّ سنقوم بوصف تحليل الشفرات والأنواع المختلفة للهجمات.

2.1 لمحة تاريخية عن التشفير

- في عام 487 قبل الميلاد، استخدم اليونانيون جهازًا يسمى."Scytale" . ويتكون من عصا يلتف حولها حزام جلدي. حيث يكتب المرسِل رسالته ويفتحها ويرسلُها، ويجب على المستقبِل إعادة لف الحزام على عصا من نفس القطر ليتمكن من العثور على الرسالة الأصلية[1] .
- في عام 50 قبل الميلاد، اخترع يوليوس قيصر أول نظام تشفير يعتمد على الرياضيات. وهو عبارة عن تشفير تبديل أحادي الأبجدية يعتمد على إزاحة الحروف [2].
- في عام 1970: قاد هورست فيستل مشروعًا بحثيًا في مختبر أبحاث IBM Watson الذي طوّر تشفير لوسيفر، والذي أدى فيما بعد إلى ظهور تشفير DES وتشفيرات أخرى. ومن مميزات هذا النوع من الخوارزميات أن التشفير وفك التشفير متطابقان من الناحية الهيكلية [3].
- في عام 1976: نشر ويتفيلد ديفي ومارتن هيلمان كتاب "اتجاهات جديدة في التشفير"، حيث طرحا فكرة تشفير المفتاح العام.

- في عام 1978: تم نشر خوارزمية RSA في اتصالات جمعية آلات الحوسبة ACM [2].
- في عام 1990: نشر شيويجيا لاي وجيمس ماسي في سويسرا خوارزمية تشفير البيانات الدولية (IDES) . التي تستخدم مفتاح 128 بت وتستخدم عمليات عملية لأجهزة الكمبيوتر ذات الأغراض العامة.
- 1985: استخدم فيكتور ميلر ونيل كوبليتز المنحنيات الإهليجية للتشفير [3].

3.1 مفاهيم التشفير الأساسية

سنقدّم في هذا القسم بعض المفاهيم الأساسية المتعلقة بالتشفير:

1.3.1 معلومات عامّة عن التشفير

التشفير هو دراسة التقنيات الرياضية المتعلقة بأمن المعلومات من أجل ضمان سريّتها وسلامتها وأصالتها وعدم التنصّل منها. يتكون التشفير بشكل خاص من تطوير أنظمة التشفير / فك التشفير أو أنظمة التشفير التي يمارسها علماء التشفير.

في علم التشفير، تسمّى المعلومات المراد إخفاؤها أيضًا بالرّسالة أو النّص العادي. وتسمّى نتيجة تشفير النص العادي بالنص المشفر؛ النص المشفر هو نتيجة تحويل يعتمد على الرسالة والمفتاح. بفضل التشفير، يمكن تشفير أي نوع من المعلومات الرقمية (نص أو بيانات أو كلام أو صور) بحيث لا يتمكن من فك تشفيرها إلا الأشخاص الذين لديهم المفتاح الصحي [1].

2.3.1 مصطلحات

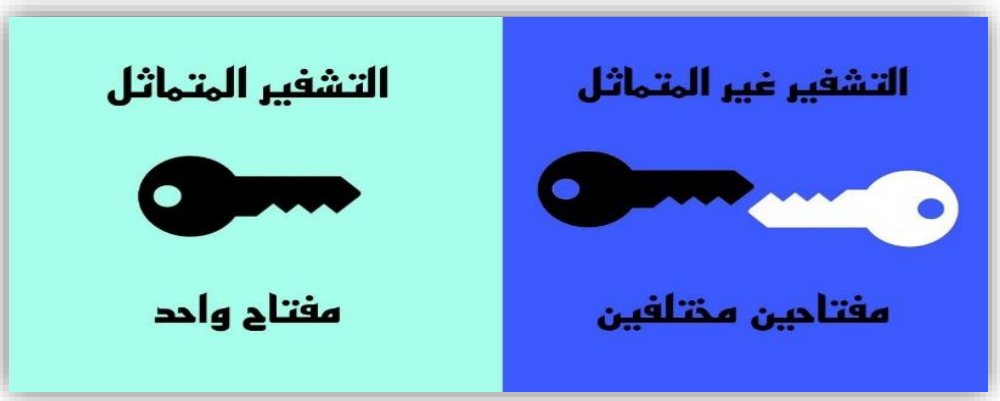
- علم التشفير (Cryptology): هو علم رياضي يضمّ فرعين: التشفير وتحليل التشفير[2].
- التشفير (Cryptography): التشفير هو دراسة الطرق التي تجعل من الممكن إرسال البيانات بشكل سري على وسيط معين [2].
- التشفير (Encryption): التحويل باستخدام مفتاح تشفير لرسالة واضحة تسمى نص واضح أو نص مكتوب إلى رسالة غير مفهومة تسمى نص مُشفر [2].
- المفتاح (Key): السّر المشترك المستخدم لتشفير النّص العادي إلى نص مشفر ولفك تشفير النص المشفر إلى نص عادي [2].

- كريبتوغرام (Cryptogram): رسالة مشفرة؛ يجب أن يكون المستلم الشرعي قادرًا على فك تشفير التشفير والحصول على النص العادي.
- النص المشفر (Encrypted text): هو نتيجة تطبيق التشفير على النص العادي.
- فك التشفير (Decryption): هو البحث عن الرسالة الواضحة المقابلة للرسالة المشفرة، وهو العملية العكسية للتشفير.
- خوارزمية التشفير (Encryption algorithm): هي دالة رياضية تستخدم في عملية التشفير وفك التشفير.
- نظام التشفير (Encryption system): يتم تعريفه على أنه مجموعة المفاتيح المحتملة (مساحة المفتاح) والنصوص العادية والمشفرة المحتملة المرتبطة بخوارزمية معينة.
- تحليل التشفير (Cryptanalysis): هو الأسلوب الذي يقوم على استنتاج نص عادي من نص مُشفر دون الحاجة إلى مفتاح التشفير. تسمّى عملية محاولة فهم رسالة معينة بالهجوم [2].

3.3.1 تعريف التشفير

التّشفير هو مجموعة من التقنيات التي تسمح بتشفير الرسائل (النصوص أو الصور)، أي جعلها غير مفهومة وسريّة. الطريقة العكسية للعثور على الرسالة الأصلية تسمّى فك التشفير. يتم التشفير بشكل عام باستخدام مفتاح التشفير، ويتطلب فك التشفير مفتاح فك التشفير. يوجد بشكل عام نوعان من المفاتيح:

- **المفاتيح المتماثلة:** هي المفاتيح المستخدمة للتشفير وفك التشفير. وهذا ما يسمّى بالتشفير المتماثل أو تشفير المفتاح السري.
- **المفاتيح غير المتماثلة:** هي المفاتيح المستخدمة في حالة التشفير غير المتماثل (وتسمّى أيضًا تشفير المفتاح العام). في هذه الحالة يتم استخدام مفتاح مختلف للتشفير وفك التشفير.



الشكل1.1: المفتاح المتماثل وغير المتماثل

4.3.1 تعريف مفتاح التشفير

هو قيمة تُستخدم في خوارزمية التشفير. هذه القيمة هي عبارة عن رقم معقد يُقاس حجمه بوحدة البت. يتألف مفتاح التشفير من مجموعة من الأحرف العشوائية التي يمكن تقسيمها إلى عدة أجزاء أو أقسام. كلما زاد حجم مفتاح التشفير زادت صعوبة فك رمز الرسالة، وزاد إسهامُه في رفع مستوى الأمان.

يجب تخزين المفاتيح بطريقة آمنة بحيث يكون الوصول إليها واستخدامها ممكنًا فقط لصاحبها. وبشكل عام يجب أن يتم حماية مفتاح التشفير بشكل صارم، وهذا هو الهدف الأكثر أهمية في جميع بروتوكولات التشفير.

5.3.1 كيفية عمل التشفير

للتمكّن من فك تشفير البيانات المشفرة، يجب أن يكون لدى المستخدم مفتاحا صحيحا يمكنه من فتح القفل، ويتم فك التشفير على العكس من ذلك، إذا حاول شخص ما فك تشفير البيانات باستخدام المفتاح الخاطئ، فلن يتمكن من قراءة البيانات.

الشكل 2.1: التشفير وفك التشفير

6.3.1 آليات التشفير

يحدّد نظام التشفير وصفًا لعملية التشفير / فك التشفير. وهو يتألف من إرسال رسالة لا يفهمها إلا المتلقي. وللقيام بذلك، فإنه يشارك سرًا مع مرسل الرسالة. يتم تحويل الرسالة "الواضحة" باستخدام " دالّة التشفير" المحدّدة بواسطة "مفتاح" إلى رسالة مشفرة "نص مشفر" ويتم تحويل الرسالة المشفرة باستخدام " دالة التشفير" لرسالة واضحة [3].

- التشفير

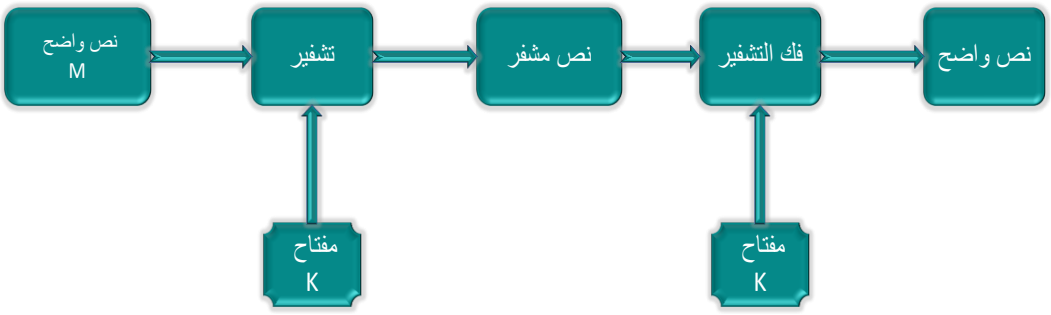
هو عملية تحويل الرسالة M بطريقة تجعلها غير مفهومة. يعتمد على دالة التشفير E ومفتاح التشفيرK [3].

$$C = Enc(K, M) \qquad (1.1)$$

- فك التشفير

هو العملية العكسية التي تسمح لنا باسترجاع الرسالة الواضحة انطلاقا من الرّسالة المشفرة [3].

$$M = Dec(K, C) \qquad (1.2)$$



الشكل3.1: مبادئ نظام التشفير

7.3.1 أهداف التشفير

يُعرَّف "الأمن السيبراني" على أنه مجموع الوسائل التي يتم استخدامها لتقليل ضعف نظام معين ضد التهديدات العرضية أو العمدية. حيث يشير إلى خاصية معينة لنظام ما، أو خدمة، أو كيان. يُعبر عنه من خلال

أهداف الأمان الملخصة في كلمة CAIN، وهي السريّة (Confidentiality)، المصادقة (Authentication)، النزاهة (Integrity) وعدم الرفض (Non-repudiation) [4].

- السريّة (Confidentiality)

يتعين على المستخدمين المسموح لهم فقط للوصول إلى المعلومات، ولضمان سريّة البيانات يجب تنفيذ إجراءين هما:

- ✓ تقييد ومراقبة وصول البيانات.
- ✓ تحويل البيانات باستخدام تقنيات التّشفير لجعلها غير قابلة للقراءة. في حالة التشفير بالمفتاح الخاص يتم استخدام نفس المفتاح للتشفير وفك التشفير، أما في حالة التشفير بالمفتاح العام يمتلك كل كيان زوجًا من المفاتيح الخاصة بها، وفي التشفير الهجين يتم استخدام التشفير بالمفتاح الخاص لتشفير الرسالة، ثم يتم تأمين تبادل المفتاح من خلال نظام المفتاح العام.

- سلامة البيانات (Integrity)

آلية للتحقق من أن البيانات المستلمة لم يتم تغييرها أو تحريفها، وأنها تظل غير معدّلة أو متلازمة.

- المصادقة (Authentification)

هي الخاصية التي تتضمن التحقق من هوية كيان ما قبل منحه الوصول إلى مورد معين. يجب على هذا الكيان أن يثبت هويته. جميع آليات التحكم في الوصول المنطقي إلى الموارد المعلوماتية تتطلب إدارة عمليات تحديد الهوية والمصادقة.

- عدم الإنكار (Non- Repudiation)

آلية لتسجيل فعل أو التزام شخص أو كيان بحيث لا يمكن للشخص أو الكيان أن ينكر أداء هذا الفعل أو الالتزام ويتضمن ما يلي:

- عدم رفض المنشأ (Non-repudiation of Origin (NRO))

لا يستطيع الشخص الذي أرسل الرسالة أن ينكر كتابتها، ويمكنه إثبات عدم مسؤوليته إذا كان هذا هو الواقع.

- عدم رفض الاستلام (Non-repudiation of Receipt (NRR))

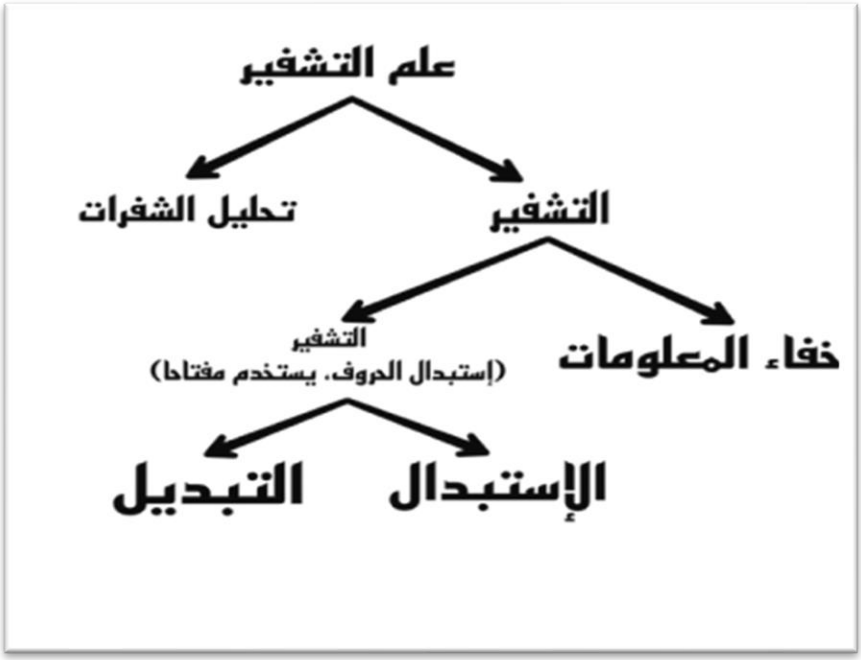
لا يمكن للمتلقي أن ينكر استلام الرّسالة، ويمكنه إثبات عدم استخدامها إذا كان هذا هو الواقع.

- عدم رفض الإرسال (Non- Repudiation of transmission)

لا يمكن للشخص الذي أرسل الرسالة أن ينكر إرسالها، ويمكنه إثبات عدم إرسالها إذا كان هذا هو الواقع.

4.1 التشفير الكلاسيكي

في التشفير الكلاسيكي (Classical Encryption)، تكون طريقة التشفير ومفتاحه بالإضافة إلى طريقة فك التشفير معروفة من قبل المرسل والمتلقي. تعتمد معظم طرق التشفير التقليدية على مبدأين أساسيين: التشفير بالاستبدال والتشفير بالنّقل.



الشكل4.1: المجالات المضمنة في علم التشفير

1.4.1 التشفير بالاستبدال

التشفير بالاستبدال (Substitution encryption) هو طريقة لتشفير الرسائل عن طريق استبدال واحدة أو أكثر من المكونات (عادةً الحروف) بمكونات أخرى [5].

1.1.4.1 التشفير بالاستبدال الأبجدي الأحادي

التشفير بالاستبدال الأبجدي الأحادي (Monoalphabetic substitution cryptography) يتم استبدال كل حرف في الرّسالة بحرف آخر، حيث كل حرف يتم استبداله بحرف آخر بشكل ثابت. على سبيل المثال، يُستبدل الحرف "أ" في الرسالة الأصلية دائمًا بنفس الحرف في الرسالة المشفرة. مثال شهير على هذا النوع من التشفير هو تشفير سيزار. تشفير سيزار هو مثال بسيط على التشفير بالاستبدال الأبجدي الأحادي حيث يتم نقل كل حرف في الرسالة بعدد ثابت من المواقع في الأبجدية. على الرغم من أن هذه الطريقة سهلة الفهم، إلا أن أمانها يُعتبر ضعيفًا. يمكن بسهولة فك تشفيره باستخدام تقنيات تحليل التواتر أو التجريب والخطأ. مثال آخر على التشفير بالاستبدال الأبجدي الأحادي هو التشفير الخطي، الذي يشمل مزيجًا من التحريك والضرب. وعلى الرّغم من هذه التغييرات، يظل هذا النوع من التشفير عرضة للهجمات.

عمومًا، يُعتبر التشفير بالاستبدال الأبجدي الأحادي قليلاً من حيث الأمان في السياقات الحديثة، حيث يكون عرضة للهجمات التحليلية المتقدمة. يُفضل عادةً استخدام أساليب أكثر تعقيدًا، مثل الاستبدال متعدد الأبجدي أو استخدام خوارزميات أكثر تطورًا، لضمان أمان كافٍ [5].

الجدول 1.1: التشفير بالاستبدال الأبجدي الأحادي

نص واضح	a	b	c	d	e	F	j	h	i	g	K	L	m	N	o	P	Q	r	S	T	U	V	w	x	y	Z
نص مشفر	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

2.1.4.1 التشفير بالاستبدال الأبجدي المتعدد

التشفير بالاستبدال الأبجدي المتعدد (polyalphabetic substitution cryptography) وهو يتألف من استخدام عدة أبجديات متغيرة لتشفير الرّسالة. في هذا النوع من التشفير، يتم تطبيق قواعد الاستبدال بطرق متعددة، ممّا يجعل من الصّعب فهم النّمط الأساسي للاستبدال ويزيد من صعوبة فك التشفير.

أشهر خوارزمية استبدال متعددة الأبجدية هي تشفير فيجنير. حيث في تشفير فيجنير، يتم استخدام مفتاح (كلمة أو عبارة) لتحديد كيفية التشفير. يتم تكرار المفتاح على طول الرسالة لإنشاء نمط متعدد الأبجديات. كل حرف في الرسالة يتم تشفيره باستخدام حروف المفتاح المتوافقة.

على سبيل المثال، إذا كان المفتاح هو"KEY" ، سيتم تكراره لتطابق طول الرسالة. ثم يتم استخدام هذا المفتاح لتحديد كيفية تشفير كل حرف في الرسالة. تشفير الاستبدال الأبجدي المتعدد يزيد من صعوبة فك التشفير مقارنةً بتشفير الاستبدال الأبجدي أحادي المفتاح. ومع ذلك، يجب الحرص على استخدام مفاتيح قوية للتأكد من أمان النظام [2].

الجدول 2.1: التشفير بالاستبدال الأبجدي المتعدد

النصل الواضح	C	R	Y	P	T	O	G	R	A	P	H	I	E
مفتاح	C	H	I	F	F	R	E	C	H	I	F	F	R
الإزاحة	2	7	8	5	5	17	4	2	7	8	5	5	17
النص المشفر	E	Y	W	U	Y	F	K	T	H	X	M	N	V

2.4.1 التشفير بالتبديل

التشفير بالتبديل (Transposition encryption) يكون عن طريق تغيير أماكن حروف النص الأصلي، أي مجرد تبديل في المواقع. وأحيانا يطلق عليها (تقليب permutation).

الشكل 5.1: التشفير بالتبديل

5.1 التشفير الحديث

التشفير الحديث (Modern encryption) يركز بشكل عام على مشاكل أمان الاتصالات. في هذا السياق، يشمل التشفير الحديث مجموعة واسعة من التقنيات والبروتوكولات المصمّمة لتأمين المعلومات المرسلة بين أطراف مختلفة، سواء على شبكات الحواسيب أو أنظمة الاتصالات اللاسلكية أو غيرها من القنوات.

تشمل أهداف التشفير الحديث السريّة، وسلامة البيانات، وتوثيق الأطراف المعنية، وعدم الإلغاء. فيما يلي بعض التقنيات والمفاهيم الرئيسية في التشفير الحديث.

1.5.1 التشفير غير المتماثل

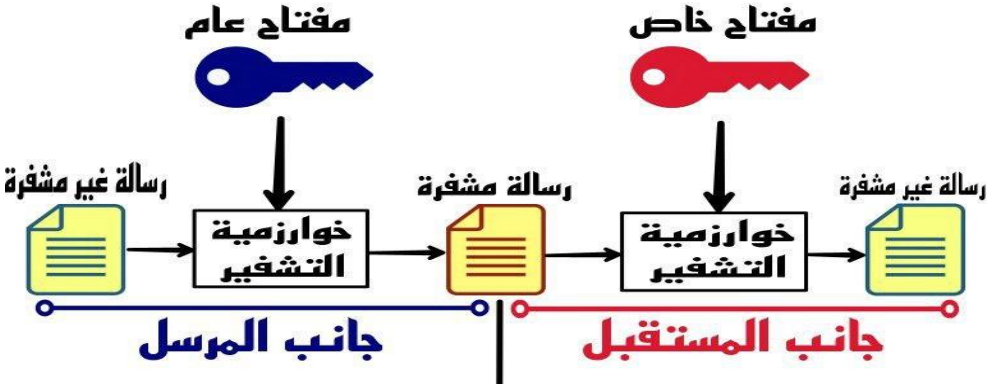
1.1.5.1 تعريف التشفير غير المتماثل

في التشفير غير المتماثل (Asymmetric cryptography) يتم استخدام مفتاح عام معروف للجميع ومفتاح خاص معروف فقط لمستلم الرسالة المشفرة كما هو موضح في الشكل (6.1).

هذا التشفير له هدفين رئيسيين؛ الأوّل هو تشفير الرسالة المراد إرسالها، أي أن المرسل يستخدم المفتاح العام للمستلم لتشفير رسالته، ويستخدم المستلم مفتاحه الخاص لفك تشفير رسالة المرسل مع ضمان سرية المحتوى، والثاني هو التأكد من صحة المرسل، أي أن المرسل يستخدم مفتاحه الخاص لتشفير رسالة، يمكن للمستلم فك تشفيرها باستخدام المفتاح العام للمرسل؛ هذه هي العملية التي يستخدمها التوقيع الرقمي للتحقق من مؤلف الرسالة.

أول خوارزمية تنفذ التشفير غير المتماثل هي خوارزمية RSA التي سميت بالأحرف الأولى من أسماء منشئيها: رونالد ريفست (Ronald Rivest)، آدي شامير (Adi Shamir) وليونارد أدلمان (Leonard Adleman)، يعتمد تشفير RSA على المشكلة الصعبة المتمثلة في تحليل عدد صحيح إلى جدائي عددين أوليين كبيرين، وتستخدم على نطاق واسع في التجارة الإلكترونية، وبشكل عام لتبادل البيانات السرية على الإنترنت [6].

هناك العديد من طرق التشفير غير المتماثلة الأخرى، منها تشفير الجمل (TAHER ELGAMAL) وهو أسلوب تشفير احتمالي [7] ، والتشفير الذي اقترحه ميلر (Miller) يعتمد على مشكلة صعبة أكثر تعقيدًا بكثير والتي تستخدم المنحنيات الإهليجية [8].



الشكل 6.1: التشفير غير المتماثل

2.1.5.1 مزايا التشفير غير المتماثل

- القضاء على مشكلة نقل المفتاح :على عكس التشفير المتماثل، حيث يجب على الطرفين مشاركة نفس المفتاح السري، يستخدم التشفير غير المتماثل زوجًا من المفاتيح (عامة / خاصة). يمكن مشاركة المفتاح العام بحرية، مما يقضي على الحاجة لنقل مفتاح سري.
- إمكانية استخدام التوقيع الإلكتروني: يتيح التشفير غير المتماثل تنفيذ التوقيع الإلكتروني، مما يسمح للمرسل بإرفاق توقيع رقمي بالرسالة، مؤكدًا مصدرها وضمان سلامتها. يمكن للمستلم التحقق من التوقيع باستخدام المفتاح العام للمرسل.
- عدم إمكانية فك تشفير الرسالة في حال اعتراضها من قبل شخص غير مخوّل :حتى وإن كان بإمكان الجميع الوصول إلى المفتاح العام، فإنه لا يمكن فك تشفير الرسالة إلا باستخدام المفتاح الخاص المقابل، الذي يعرفه فقط الشخص المخوّل. وهذا يوفر أمانًا إضافيًا في حالة اعتراض الرسالة.

- توسعة عمر الأزواج المفتاحية :يمكن استخدام أزواج المفاتيح (العامة / الخاصة) في التشفير غير المتماثل لفترات أطول مقارنة بالمفاتيح المتماثلة. وهذا يقلل من تكرار تحديث المفاتيح، مما يكون مفيدًا من حيث إدارة المفاتيح.

3.1.5.1 عيوب التشفير غير المتماثل

- زمن التنفيذ

أبطأ من التشفير المتماثل. يتطلب تنفيذ عمليات التشفير وفك التشفير باستخدام مفاتيح مختلفة، مما يجعله أبطأ في بعض الحالات مقارنةً بالتشفير المتماثل الذي يستخدم نفس المفتاح للعمليتين.

- خطر هجمات الاستبدال للمفاتيح

قد يتعرض لخطر هجمات الاستبدال للمفاتيح، ولذلك يتعين التحقق من صحة المرسلين للمفاتيح. في حالة تزويد مفتاح عام غير صالح، يمكن للمهاجم استخدامه لتشفير معلومات كاذبة.

- حجم المفاتيح

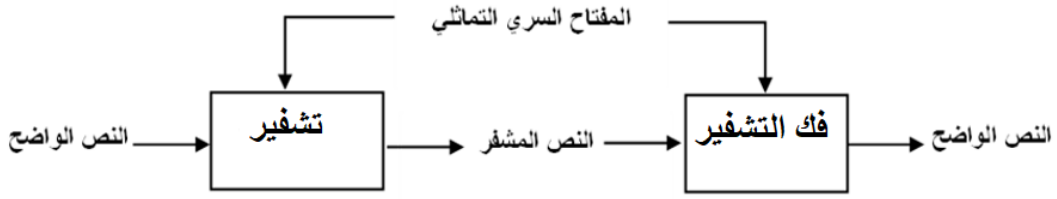
حجم المفاتيح في التشفير غير المتماثل عادةً يكون أكبر من تلك المستخدمة في أنظمة التشفير المتماثل. هذا يعني أنه يمكن أن يتطلب تبادل وتخزين المفاتيح كميات أكبر من البيانات.

فهم هذه العيوب يساعد في تحديد السياقات التي يكون فيها التشفير غير المتماثل هو الخيار المناسب، حيث يُفضل عادة استخدامه في حالات الأمان المتقدم على حساب بعض من الأداء.

2.5.1 التشفير المتماثل

1.2.5.1 تعريف التشفير المتماثل

التشفير المتماثل (Symmetric cryptography) المعروف أيضًا باسم المفتاح السري أو الخاص، يسمح بتشفير وفك تشفير الرسالة باستخدام نفس المفتاح وهذا يعني أن المرسل والمتلقي يجب أن يكونا لديهما نفس المفتاح. الذي يجب أن يبقى سريًا، لأن أمان هذه الرسالة يعتمد على هذا المفتاح. كما هو موضح في الشكل:



الشكل 7.1: التشفير المتماثل

غالبًا ما تعتمد خوارزميات التشفير المتماثل على تقنيات الاستبدال حيث يتم استبدال كل حرف بحرف آخر مع الاحتفاظ بمكانه الأصلي، وعلى عمليات النقل حيث يتم وضع الحرف في مكان آخر دون تغييره. وهذا يوفر طريقة سريعة وفعالة لتشفير الرسالة. التشفير باستخدام مفاتيح متماثلة يمكن تصميمه لتوفير معدلات نقل بيانات عالية. بعض التنفيذات الاعتقادية تحقق معدلات تشفير تصل إلى مئات الميجابايت في الثانية، بينما يمكن لتنفيذا البرمجيات أن تصل إلى معدلات نقل بيانات تتراوح في حدود الميجابايت في الثانية.

الثاني مفاتيح تشفير المفاتيح المتماثلة قصيرة نسبيًا، ومع ذلك يوجد مفتاح مختلف لكل اتصال مع كل مشارك ضروري. ولذلك فمن الضروري إدارة توزيع عدد كبير من المفاتيح، مع العلم أن الكشف عن المفتاح السري سيكون كارثيا على أمن الاتصالات [9].

يمكن تصنيف أنظمة التشفير المتناظرة إلى فئتين، التشفير الكتلي والتشفير التدفقي.

2.2.5.1 التشفير بالكتلة

عبارة عن نظام تشفير يقوم بتقسيم الرسالة الأصلية إلى كتل من البتات ذات حجم ثابت (64 بت أو 128 بت). يتم تشفير الكتل واحدة تلو الأخرى. يتم التشفير إما عن طريق الاستبدالات، أي يتم استبدال بتات الكتلة ببتات أخرى، أو عن طريق عمليات النقل، حيث يتم تبديل بتات الكتلة فيما بينها. في طريقة الاستبدال يمكن جعل العلاقة بين رسالة النص العادي والرسالة المشفرة معقدة قدر الإمكان. أما في طريقة عملية النقل فيتيح إمكانية الحصول على بت، وبالتالي يتم تبديل أجزاء الرسالة لمنع العثور على أي تكرار في الرسالة العادية في الرسالة المشفرة.

الأمثلة الكلاسيكية لشفرات الكتل هي DES (معيار تشفير البيانات) وAES (معيار التشفير المتقدم). كانت خوارزمية DES هي المعيار العالمي للتشفير حتى نهاية التسعينيات، وهي تجمع بين تقنيتي الاستبدال والتحويل حيث تعمل على تشفير كتلة بيانات ذات حجم 64 بت. يتم تقسيم البيانات إلى كتل بحجم 64 بت،

وبمجرد تقسيم البيانات إلى كتل، يتم استخدام المفتاح بحجم 56 بت لتشفير كل كتلة بيانات على حدة [10]. تتيح خوارزمية AES تشفير كتل مكونة من 128 أو 192 أو 256 بت باستخدام مفاتيح 128 أو 192 أو 256 بت. يعد اختيار حجم المفتاح وحجم الكتلة مستقلاً، لذا يوجد إجمالي 9 مجموعات محتملة، مما يترك مرونة أكبر للمستخدم اعتمادًا على المستوى المطلوب من الأمان وسرعة الحساب [11]، [12].

3.2.5.1 التشفير التدفقي

في التشفير التدفقي (Stream encryption)، يتم تشفير الرسائل حرفًا بحرف أو بتًا ببت، يشير "التشفير التدفقي" إلى عملية تشفير البيانات بشكل متسلسل أثناء انتقالها، حيث يتم معالجة البيانات بتسلسل أحادي البت (بت ببت) بدلاً من تقسيمها إلى كتل ثابتة. ويتم تشفير كل بت أو مجموعة صغيرة من البتات بشكل فوري أثناء نقل البيانات، وهذا يعتبر مختلفًا عن تشفير الكتل حيث يتم تشفير البيانات في وحدات كبيرة مثل كتل ثابتة. وتستخدم تقنيات التشفير التدفقي في عدة سياقات، مثل تشفير الاتصالات عبر الإنترنت وتأمين المعلومات أثناء النقل. واحدة من أمثلة أنظمة التشفير التدفقي هي RC4. يُستخدم التشفير التدفقي أيضًا في بعض تقنيات الاتصالات السلكية واللاسلكية. من أنواع التشفير التدفقي تشفير فيرنام الذي اخترعه جي فيرنام عام 1917، حيث تتكون هذه الطريقة من سلسلة من البتات العشوائية بنفس طول الرسالة المراد تشفيرها. هذه السلسلة هي سر يعرفه فقط المشاركان ولا يمكن استخدامها إلا مرة واحدة. حيث الرسالة الأصلية مشفرة على شكل بتات، وفي عملية التشفير، يتم مقارنة كل بت من القناع والرسالة. إذا كانا متطابقين، فسيكون بت الرسالة المشفرة 1 وإلا فسيكون 0، وهذا يعود إلى إجراء جمع بتات "موديول 2" أو "أو استبعادي "(XOR) بين بتات الرسالة الواضحة وبتات القناع القابل للتصرف. بمعرفة القناع، من السهل بعد ذلك إعادة إنشاء الرسالة الأصلية. وهو معرف بالأبجدية A= {0,1}، يتم تشفير الرسالة الثنائية $m1\ m2 \dots ml$ بواسطة مفتاح ثنائي $k1\ k2 \dots kl$ بنفس الطول لإنتاج الرسالة المشفرة $c1\ c2 \dots cl$ باستخدام المعادلة التالية:

$$c_i = m_i \oplus k_i \quad , \quad 1 \le i \le l \qquad (3.1)$$
$$M \times N$$

عملية فك التشفير مطابقة لعملية التشفير إذن:

$$m_i = c_i \oplus k_i \quad , \quad 1 \le i \le l \qquad (4.1)$$

هذا التشفير هو ما يُسمّى بالمخطط السري الكامل الوحيد، أي أنه من الناحية النظرية غير قابل للكسر طالما تم استخدام المفتاح مرة واحدة فقط، وعلى الرغم من ذلك يواجه هذا النظام صعوبات كبيرة في التنفيذ العملي، يعتمد أمانه على التوليد العشوائي تمامًا للمفتاح ولا يمكن استخدامه لتشفير تدفقات كبيرة من البيانات بسبب حجم المفتاح الذي يتطلب مولدات عشوائية لإنتاجه.

لذا باختصار، المفتاح يجب أن يكون:

- ✓ بطول يعادل طول الرسالة المراد تشفيرها.
- ✓ يتم اختياره بشكل كامل عشوائي.
- ✓ يستخدم مرة واحدة فقط.

أثبت شانون أن هذا النظام يوفر أمانًا نظريًا مطلقًا إذا تم احترام القواعد الثلاثة المذكورة أعلاه بشكل صارم [13].

يعتمد التشفير التدفقي على فكرة تشفير فيرنام، ولكنه يستخدم تسلسلًا شبه عشوائي من البتات، يتم إنشاؤه من عدد قليل من بتات المفاتيح القصيرة نسبيًا، ولتنفيذه يتم استخدام خوارزمية تسمى مولّد الأرقام شبه العشوائية، ويتم إدخال مفتاح ذو حجم ثابت إلى مولّد الأرقام شبه العشوائية، ويتم الحصول على سلسلة من البتات التي سيتم تطبيقها على الرسالة البسيطة عند إخراج المولد.

ومن بين خوارزميات التشفير التدفقي المستخدمة على نطاق واسع نجد خوارزمية RC4 التي صمّمها رونالد ريفست (Ronald Rivest) عام 1987 [14]، وخوارزمية Grain التي تم تقديم النسخة الأولية منها في عام 2005 بواسطة هال (Hell) [15] ، وتلاه متغيران المعينان Grain وGrain-128 على التوالي [16].

4.2.5.1 مزايا التشفير المتماثل

- ➢ **سرعة التنفيذ** :حيث يستخدم مفتاح واحد فقط لكل من عمليات التشفير وفك التشفير، مما يؤدي إلى تنفيذ أسرع بشكل عام مقارنة بالتشفير غير المتماثل لاستخدامه مفاتيح مختلفة.
- ➢ **سهولة التنفيذ** :إدارة مفتاح واحد تُبسط عملية التنفيذ وإدارة المفاتيح. توزيع وإدارة المفاتيح غالباً ما تكون أكثر سهولة مقارنة بالتشفير اللاتماثلي لاستخدامه مفاتيح مختلفة لعمليتي التشفير وفك التشفير.

- **القدرة على تصميم آليات تشفير متنوعة :**يمكن استخدام التشفير التماثلي كمكون أساسي في مختلف الآليات الأمنية، بما في ذلك وظائف التجزئة (hachage). يوفر هذا المرونة في تصميم أنظمة أمان معقدة.

مع ذلك، يجب أن نلاحظ أن التشفير التماثلي يأتي مع بعض العيوب، مثل ضرورة توزيع المفتاح بشكل آمن بين الأطراف المتواصلة. ولذلك في بعض الحالات، يُستخدم مزيج من التشفير التماثلي والتشفير غير التماثلي اللازم للاستفادة من مزايا التهجين (ويُسمى هذا بالتشفير المختلط).

5.2.5.1 عيوب التشفير المتماثل

- **مفاتيح ذات طول نسبياً قصير:** في التشفير المتماثل، يتم استخدام مفتاح واحد لكليهما (التشفير والفك). وغالبًا ما تكون المفاتيح ذات طول محدود نسبيًا، مما قد يجعلها عرضة للهجمات مثل هجمات التجسس والكسر.
- **تعقيد العملية:** من الضروري أن يكون عدد المفاتيح الخاصة متساويًا مع عدد المستلمين المحتملين. يمكن أن يؤدي ذلك إلى إدارة معقدة للمفاتيح، خاصة في البيئات التي تتطلب الكثير من التواصلات المأمونة.
- **تأمين سلسلة نقل المفتاح:** يعد تأمين نقل المفاتيح العامة وأحيانًا الخاصة إلى المستلمين أمرًا حاسمًا. إذا لم يتم نقل هذه المفاتيح بشكل آمن، فإن ذلك يمكن أن يعرض أمان النظام بأكمله للخطر.
- **عدم إمكانية ضمان خاصية عدم الرفض في أنماط التوقيع الإلكتروني:** في بعض أنماط التوقيع الإلكتروني التي تعتمد على التشفير المتماثل، قد يكون من الصعب ضمان خاصية عدم الرفض، أي القدرة على تعزيز إجراء بشكل لا يمكن إنكاره لفعل معين لكيان معين. وهذا يمكن أن يكون تحديًا في الحالات التي تتطلب فيها عدم الرفض، كما هو الحال في المعاملات المالية.

من المهم أن نلاحظ أن التشفير المتماثل يظل جزءًا أساسيًا من العديد من أنظمة أمان الحواسيب بسبب مزاياه في مجال الأمان، مثل سهولة توزيع المفاتيح العامة وإمكانية تنفيذ آليات مثل التوقيع الرقمي.

الجدول 1.1: مقارنة بين التشفير التماثلي والتشفير غير التماثلي

الميزة	التشفير التماثلي	التشفير غير التماثلي
عدد المفاتيح	مفتاح واحد للتشفير ولفك التشفير	مفتاحين: مفتاح عام للتشفير، ومفتاح خاص لفك التشفير
توزيع المفاتيح	توزيع وإدارة المفاتيح بشكل آمن يشكل تحديًا	يمكن توزيع المفاتيح العامة بحرية؛ يجب الاحتفاظ بالمفاتيح الخاصة بسرية
السرعة	عادةً أسرع من التشفير اللاتماثلي	أبطأ مقارنة بالتشفير التماثلي
الأمان	عرضة لقضايا توزيع المفاتيح واختراقها	أكثر أمانًا بسبب فصل المفاتيح؛ مقاوم لبعض الهجمات
إدارة المفاتيح	يتطلب تبادل وإدارة المفاتيح بشكل آمن	إدارة المفاتيح أسهل، خاصة للشبكات الكبيرة
استخدامات	يستخدم عادة لتشفير البيانات بالجملة، على سبيل المثال، تشفير القرص الصلب	يستخدم لنقل البيانات بشكل آمن، التوقيعات الرقمية.
أمثلة	AES (معيار التشفير المتقدم) ، DES (معيار تشفير البيانات)	RSA

3.5.1 التشفير الهجين

التشفير غير المتماثل يعتبر بطيئًا بطبيعته بسبب الحسابات المعقدة المرتبطة به، في حين يتميز التشفير المتماثل بسرعته. ومع ذلك، يعاني التشفير المتماثل من نقص خطير، وهو نقل المفاتيح بطريقة آمنة. وللتغلب على هذا العيب، يتم اللجوء إلى التشفير غير المتماثل الذي يعمل مع زوج من المفاتيح: خاصة وعامة. يجمع التشفير الهجين بين النظامين للاستفادة من سرعة التشفير المتماثل لمحتوى الرسالة واستخدام التشفير غير المتماثل فقط للمفتاح.

6.1 تحليل الشفرات

تحليل الشفرات (cryptanalysis) هو عملية استنتاج النص العادي من النص المشفر دون الحاجة إلى مفتاح التشفير، تسمى عملية محاولة فك تشفير الرسالة هجومًا. وهناك عدة أنواع من الهجمات [17] :

1.6.1 هجوم على النص المشفر فقط

هجوم على النص المشفر فقط (Cipher text only attack) وهذه الوضعية هي الأصعب لمحلل الشفرات، الذي لا يملك سوى رسالة مشفرة واحدة أو أكثر، دون أن يكون لديه معلومات إضافية عن معناها في نص عادي. تعتبر قدرة الشخص الذي يمارس هذا الهجوم على الحصول على أي معلومات حول النص العادي الأساسي نجاحًا له.

2.6.1 الهجوم بنص واضح معروف

الهجوم بنص واضح معروف (known plain text attack) حيث باستخدام هذه التقنية يحصل محلل الشفرات على النص المشفر والنص العادي، وباستخدام هذه البيانات يحاول العثور على معلومات حول المفتاح السري المستخدم. سيتطلب هذا عدة آلاف من النصوص العادية والنصوص المشفرة للحصول على أي فرصة للنجاح.

3.6.1 الهجوم بنص واضح مختار

في الهجوم بنص واضح مختار(Chosen-plain text attack)، يحصل محلل الشفرات على النصوص المشفرة المقابلة لمجموعة من النصوص الواضحة التي يختارها، وهذا يمكن أن يسمح له بمحاولة استنتاج المفتاح السري المستخدم. وبالتالي يقوم بفك تشفير الرسائل الأخرى المشفرة بهذا المفتاح. قد يكون هذا النوع من الهجوم صعبًا ولكنه ليس مستحيلًا.

4.6.1 هجوم النص المشفر المختار

هجوم النص المشفر المختار (adaptive chosen-plaintext attack) يحصل محلل الشفرات على النصوص الواضحة المقابلة لمجموعة من النصوص المشفرة التي يختارها، ومن هذه المعلومات يمكنه محاولة استعادة المفتاح السري المخفي المستخدم في فك التشفير.

5.6.1 الهجوم باستخدام المفاتيح المرتبطة

الهجوم باستخدام المفاتيح المرتبطة (chosen-ciphertext attack) هو شكل من أشكال تحليل الشفرات حيث يمكننا ملاحظة تشغيل التشفير تحت عدة مفاتيح مختلفة تكون قيمها غير معروفة في البداية، ولكن تكون العلاقة الرياضية التي تربط المفاتيح معروفة لمحلل الشفرات.

7.1 الخاتمة

في هذا الفصل، قمنا بعرض مقدمة حول علم التشفير وتاريخ نشأته، حيث قمنا في بادئ الأمر بشرح بعض المفاهيم الأساسية للتشفير مع تعريف مفتاح التشفير وذكر أنواعه، كما استعرضنا كيفية عمل التشفير وذكر آلياته وأهدافه، وأيضا تطرقنا الى ذكر أنواع التشفير الكلاسيكي والتشفير الحديث، كما قمنا بتعريف طريقتي التشفير المتماثلة وغير المتماثلة مع ذكر مزايا وعيوب كلا منهما وفي نهاية الفصل تطرقنا الى مفهوم تحليل الشفرات وأنواع الهجومات. ونظرا لتعدد مجالات التشفير سنركز في الفصل الثاني حول تشفير الصور الرقمية مع ذكر أنواع وصيغ الصور وطرق تشفيرها.

الفصل الثاني

عموميات حول الصور الرقمية وطرق تشفيرها

1.2 مقدمة

تاريخ تشفير الصور الرقمية يعكس تطور الاستخدام الرقمي للصور وتقنيات الأمان على مرّ السنين. في بداية استخدام الصور الرقمية في التسعينات كانت الحاجة إلى حماية هذه البيانات الرقمية تزداد أهمية مع تقدم التكنولوجيا وزيادة استخدام الإنترنت. تمثل تقنيات تشفير الصور جزءًا أساسيًا من التدابير الأمنية المتخذة للحفاظ على خصوصية وسلامة البيانات. في بداياتها تمّ استخدام تقنيات بسيطة للتشفير لحماية الصور الرقمية من الوصول غير المصرّح به، مع تزايد تبادل الصور عبر الشبكة وارتفاع حجم البيانات الرقمية تطورت تقنيات التشفير لتشمل خوارزميات معقدة وبروتوكولات متقدمة.

في الوقت الحالي يُستخدم تشفير الصور بشكل واسع في مختلف المجالات، بدءًا من تأمين الصور الشخصية على وسائل التواصل الاجتماعي إلى حماية البيانات الطبية والتقنيات الصناعية. يواجه مستقبل تشفير الصور التحديات التكنولوجية المتزايدة، ولكن التطور المستمر في هذا المجال يسهم في تعزيز الأمان الرقمي وحماية الخصوصية للمستخدمين.

في هذا الفصل، سنقدم معلومات حول الصور الرقمية، بالإضافة إلى ذكر طرق تشفير الصور. قياسات أداء خوارزميات تشفير الصور.

2.2 معلومات عامة عن الصور الرقمية

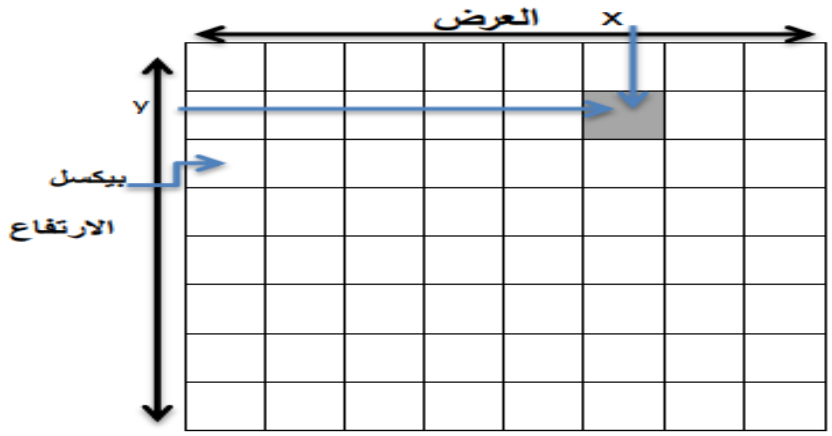
سنقدّم في هذا القسم بعض المفاهيم المتعلقة بالصور الرقمية.

1.2.2 تعريف الصورة الرقمية

الصورة الرقمية أو ما يُعرف بـ "Digital image" هي ملف يأتي بأحجام وتنسيقات متنوعة، يمكن فتحه على شاشات الأجهزة الرقمية مثل الكمبيوترات والهواتف الذكية وشاشات أخرى. يمكن أن تكون هذه الصور أحادية اللون أو ملونة، وتُمَثَّل بشكل ثنائي البُعد عند عرضها على أجهزة العرض. ورغم عدم وجود ملموس للصورة الرقمية يمكن طباعة معظم تنسيقاتها باستخدام مجموعة متنوعة من الطابعات. كما يُمكن تبادل ونقل الصور الرقمية بين معظم الأجهزة الإلكترونية بسهولة [18].

رياضياً يُمكن تمثيل الصورة الرقمية بشكل مصفوفة ثنائية البعد f(x,y)، حيث يعبر x و y عن إحداثيات نقطة معينة في الصورة، وتُمثل قيمة f(x,y) الشدّة الضوئية أو اللون في تلك النقطة [19].

تمثيل الصورة الرقمية بشكل رياضي يسهل تطبيق العديد من العمليات الرياضية والتحليلات عليها ممّا يجعلها قابلة للمعالجة بشكل فعّال باستخدام الحوسبة الرقمية [20].



الشكل 1.2: صورة رقمية

2.2.2 أنواع الصور الرقمية

توجد عدّة أنواع من الصور الرقمية، وتختلف حسب الاستخدام والمتطلبات. هنا بعض أنواع الصور الرقمية الشائعة:

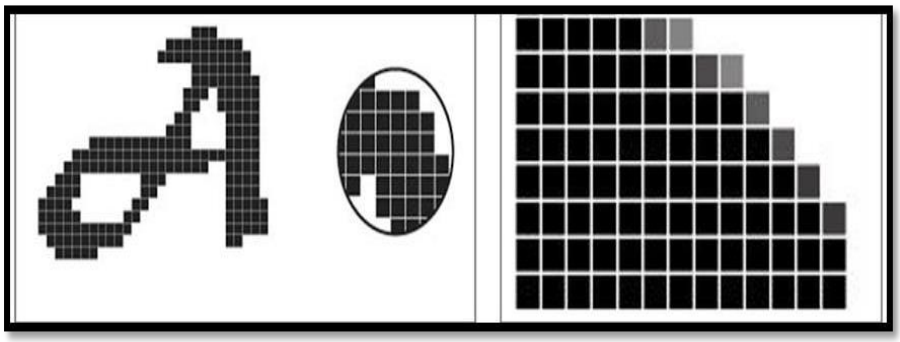
1.2.2.2 من حيث الرسومات

بناءً على سمات أي صورة، يتم تصنيفها إلى صور مصفوفية وصور متجهة.

- ✓ **الصور المصفوفية**

الصور المصفوفية (Matrix images) هي نوع من الصور تتألف من مجموعة من النقاط الصغيرة المعروفة بإسم البكسلات حيث كل بكسل له موقع محدد ولون معين. تُسمى أحيانًا الصور المصفوفية أيضًا بصور البتماب. هذا النوع من الصور هو الأكثر شيوعًا ويستخدم على نطاق واسع في الصور الفوتوغرافية الرقمية والوثائق الممسوحة ضوئيًا.

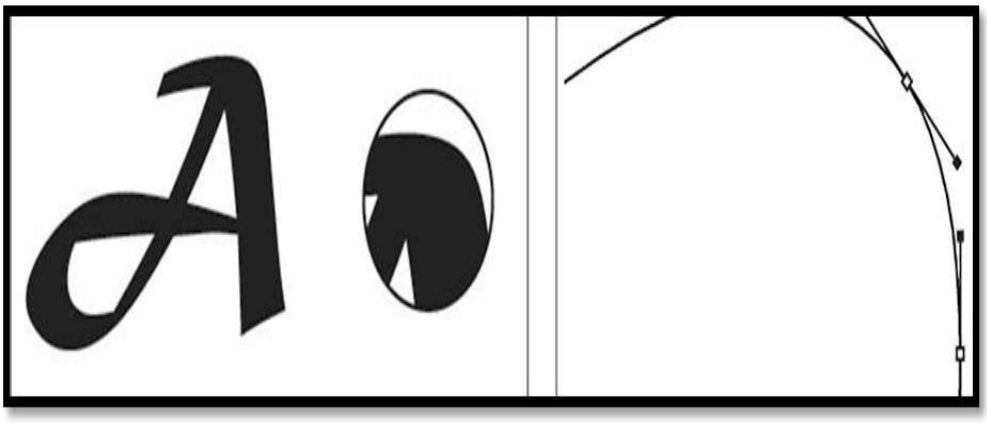
تُستخدم الصور المصفوفية على نطاق واسع في مجال معالجة وتحليل الصور. غالبًا ما تكون مخزنة بتنسيقات ملفات متعددة مثل PNG,JEPG,GIF,TIFF,SVG التي تُعد أمثلة على ملفات صور البتماب. تصف هذه التنسيقات كيفية تخزين بيانات البكسل في الملف، ولكل تنسيق ميزاته وعيوبه الخاصة فيما يتعلق بجودة الصورة وحجم الملف ودعم الشفافية، وبين خصائص أخرى [21].



الشكل 2.2: صورة مصفوفية

- ✓ **الصورة المتجهة**

الصورة المتجهة (vector images) تتألف من أشكال هندسية يمكن وصفها رياضيًا (خطوط مستقيمة، دوائر، نقاط، ...). تكون هذه الصور ذات فائدة كبيرة لإعادة الإنتاج على نطاق واسع حيث يمكن إجراء الحسابات في كل مرة للحصول على الصورة الدقيقة بغض النظر عن الحجم المختار. صيغ ملفات المتجهة مثل EPS وPDF تُستخدم في العديد من تطبيقات الويب التي تتطلب بشكل متكرر تغيير الحجم وإنشاء الرسومات. على سبيل المثال استخدام تطبيق الكتابة بواسطة لاتكس مع صور "eps" لتحسين الرؤية والقراءة [21].



الشكل 3.2: صورة متجهة

الجدول 1.2: الفرق بين الصور المصفوفية والمتجهة

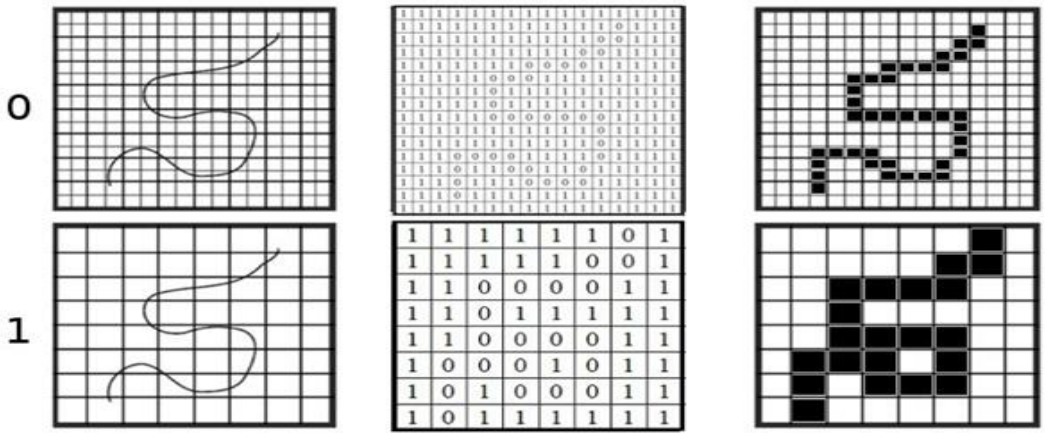
الصور المتجهة	الصور المصفوفية
تمثل بياناتها بواسطة معادلات هندسية ورياضية	تمثل بياناتها بواسطة قيم لون البكسل
تشمل أشكالًا هندسية مثل الدوائر والخطوط	تشمل نقاطًا فردية (بكسل)
يمكن تكبيرها أو تصغيرها دون فقدان الجودة	قد يحدث فقدان في الجودة عند التكبير أو التصغير
تحتفظ بوضوح التفاصيل حتى عند التغيير في الحجم	قد يظهر تشوه في التفاصيل عند تغيير حجم الصورة
تستهلك مساحة تخزين أقل	تستهلك مساحة تخزين أكبر
مثال على تنسيقاتها: SVG، AI، EPS	مثال على تنسيقاتها: BMP، JPG، PNG
مفيدة للرسوم التوضيحية والشعارات والطباعة	مفيدة للصور الفوتوغرافية والصور الفنية

2.2.2.2 من حيث الألوان

يتم تصنيف الصور من حيث الألوان إلى ثلاثة أنواع رئيسة:

- ✓ **الصورة الثنائية**

الصورة ثنائية اللون (Binary images) المعروفة علمياً باسم الصورة السوداء والبيضاء هي نوع من الصور الرقمية حيث يمكن لكل بكسل أن يتخذ إحدى قيمتين فقط: الأسود أو الأبيض. تُظهر هذه التمثيلات الثنائية الصورة بأبسط شكل لها ممّا يجعلها مناسبة لمختلف الأغراض الحسابية والتحليلية. في الصورة السوداء والبيضاء يُمثل كل بكسل وحدة صغيرة من الصورة، ويمكن لكل بكسل أن يتخذ إحدى القيمتين: 0 (الأسود) أو 1 (الأبيض) [21].



الشكل 4.2: صورة ثنائية

توجد الصور السوداء والبيضاء تطبيقات في مجموعة من المجالات العلمية والهندسية:

- تحليل الصور: تبسط مهام معالجة الصور، مما يجعل الكشف عن الأشكال والحواف والأنماط أمرًا سهلاً.
- رؤية الحاسوب: تستخدم في خوارزميات الكشف والتعرف على الكائنات.
- التصوير الطبي: يتم تطبيقها في مهام مثل التشغيل واستخراج السمات.

✓ **الصور الرمادية**

الصور الرمادية (Gray images) أو الصور ذات المستوى الرمادي هي صور تحتوي على درجات مختلفة من اللون الرمادي فقط. وتُعرف أيضًا باسم الصور أحادية اللون أو الصور الرمادية. تتميز بدقة البت والتي تشير إلى عدد مستويات الرمادي التي يمكن أن تحتوي عليها الصورة. على سبيل المثال يمكن أن تحتوي صورة ذات 8 بت على 256 مستوى رمادي، بينما يمكن أن تحتوي صورة ذات 16 بت على 65536.

الشكل 5.2: صورة رمادية

تُستخدم الصور ذات المستوى الرمادي في مجموعة متنوعة من التطبيقات:

- التصوير الفوتوغرافي: لإنشاء صور بالأبيض والأسود.
- التصوير الطبي: لإنشاء صور بالأشعة السينية والتصوير بالرنين المغناطيسي.
- في الهندسة: لإنشاء رسومات تخطيطية وصور ثنائية الأبعاد.

✓ **الصورة الملونة**

الصورة الملونة (Colors images) هي في الواقع تتألف من ثلاث صور مستقلة لتمثيل الأحمر والأخضر والأزرق. تسمى كل من هذه الصور الثلاثة بـ "الخانة" حيث يحتوي كل بكسل من الصورة الملونة على ثلاثة أرقام (R، G، B) كل منها عدد صحيح بين 0 و255. إذا (255;0;0) = (R,G,B) فإنه لا يحتوي إلا على معلومات حمراء ويتم عرضه باللون الأحمر. وبالمثل يتم عرض البكسلات التي تساوي (0;255;0) و (0;0;255) باللون الأخضر والأزرق على التوالي [21].

على سبيل المثال إذا كانت قيمة البكسل في الخانة الحمراء تساوي 255 فإنّ هذا البكسل يمثل اللون الأحمر الخالص. وإذا كانت قيمة البكسل في الخانة الخضراء تساوي 255 فإنّ هذا البكسل يمثل اللون الأخضر الخالص. وإذا كانت قيمة البكسل في الخانة الزرقاء تساوي 255 فإنّ هذا البكسل يمثل اللون الأزرق الخالص.

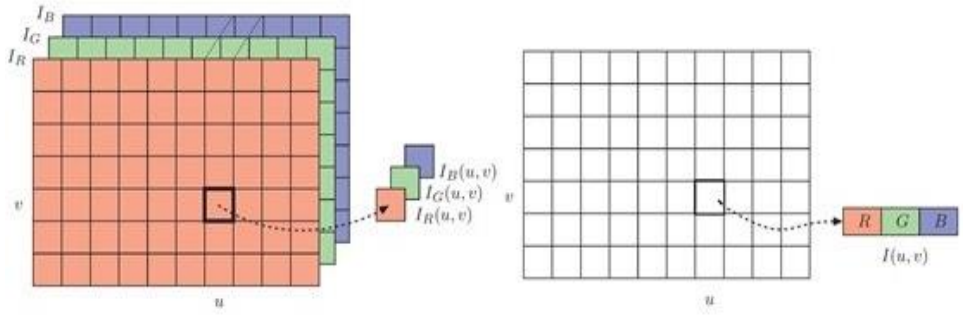
الشكل 6.2: صورة ملونة

هناك طريقتان لترتيب مكونات الألوان في الصور اللونية الحقيقية [1].

الطريقة الأولى هي ترتيب المكونات، وفي هذه الطريقة يتم تنظيم مكونات الألوان في مصفوفات منفصلة.

الطريقة الثانية هي الترتيب المعبأ، حيث يحتوي عنصر واحد من مصفوفة الصورة (بكسل واحد) على مكونات تُعبأ حيث تُمثل المكونات الألوان الثلاثة.

تعتبر الصور الملونة أداة قوية للتواصل والتحليل في عدة مجالات. في التصوير الفوتوغرافي، تلتقط الصور جمال المشاهد وتنقل القصص بلغة الألوان. في التصميم الجرافيكي، يلعب اللون دورًا حيويًا في تعزيز العلامات التجارية والإعلانات. بالإضافة إلى ذلك، تُستخدم الصور الملونة في ميدان العلوم والطب لتشخيص الأمراض وتوفير رؤى حول التغيرات البيئية من خلال الأقمار الصناعية.



الشكل 7.2: ترتيب مكونات الألوان في الصور الملونة

3.2.2.2 من حيث الأبعاد

نميز نوعين من الصور، الصور ثنائية الأبعاد والصور ثلاثية الأبعاد.

- ✓ **الصور ثنائية الأبعاد**

الصور ثنائية الأبعاد (2D) هي صور تحتوي على بعدين فقط هما الطول والعرض. يمكن تمثيلها بمصفوفة تحتوي على مجموعة من المتجهات المحددة بـ (u; v) كفهرس لعناصر المصفوفة. تُستخدم الصور ثنائية الأبعاد في مجموعة متنوعة من التطبيقات بما في ذلك التصوير الفوتوغرافي والرسومات الحاسوبية والطباعة والإعلانات [22].

✓ **الصور ثلاثية الأبعاد**

الصور ثلاثية الأبعاد (3D) هي صور تحتوي على ثلاثة أبعاد وهي الطول والعرض والعمق. يمكن تمثيلها بمصفوفة تحتوي على مجموعة من المتجهات المحددة بـ (u; v; w) كفهرس لعناصر المصفوفة. يتم تطبيق الصور ثلاثية الأبعاد في مجموعة واسعة من التطبيقات مثل التصميم الهندسي، وألعاب الفيديو، والتحليل الطبي، حيث توفر إمكانية رؤية الأشياء بشكل واقعي وتفاعلي [22].

الشكل 8.2: صورة ثلاثية البعد

3.2.2 صيغ الصور الرقمية

صيغة الصورة هي تمثيل حاسوبي للصورة مرتبط بمعلومات حول كيفية تشفيرها وتقديم إرشادات حول فك تشفيرها والتلاعب بها. يتألف معظم الصيغ من رأس يحتوي على سمات مثل أبعاد الصورة ونوع التشفير وجدول تحويل الألوان (LUT)، تليها البيانات الفعلية للصورة. تتنوع هيكلة السمات والبيانات بين صيغ الصور [21].

1.3.2.2 تنسيق JPEG

هو اختصار لـ "Joint Photographic Experts Group" وهو تنسيق ملف الصور الرقمية المستخدم بشكل شائع لتخزين الصور الملتقطة بواسطة الكاميرات الرقمية والصور الفوتوغرافية. وهو تنسيق يستخدم تقنية ضغط البيانات لتقليل حجم الملف وتسهيل تخزين الصور بكفاءة. يتميز هذا التنسيق بقدرته على الحفاظ على جودة مقبولة للصور مع تقليل الحجم مما يجعله مناسبًا للاستخدام في مجموعة واسعة من التطبيقات والأغراض[21].

الشكل 9.2: تنسيق JEPG

2.3.2.2 تنسيقGIF

وهو اختصار لعبارة "Graphic Interchange Format" أي تدعم الصور المتحركة على شكل فيديو لكن هي على شكل صورة متحركة تدعم حوالي 256 تدرج من الألوان كما أنها تمتاز بحفظ الصور بصيغة شفافة إلاّ إن السبب الذي يجعلها ضعيفة في الجودة أنها لا تحتوي على أكثر من 256 لون مما تتعرض غالبا للتشوه في الجودة.

الشكل 10.2: تنسيق GIF

3.3.2.2 تنسيق PNG

وهو اختصار لعبارة "Portable Network Graphic"، يُعتبر أعلى صيغة في جودة الصور، وغالبًا لا يُستخدم بشكل واسع من قِبَل أصحاب اتصال الإنترنت الضعيف لرفع صورهم على مواقعهم المفضلة. يتميز PNG بجودة خارقة وممتازة، ويجمع بين ميزتي الشفافية وتعدد الألوان، مما يجعله يتفوق على الصيغ السابقة.

تتوفر صيغتا 8 بت و24 بت (حتى 32 بت في بعض الحالات) لجودة الصورة في تنسيق PNG حيث تُعتبر هذه الصيغة الأفضل للصور، حيث تقدم نتائج ممتازة في استخراج الصور للتصميمات وغيرها. وتتميز بعدم تأثرها بمشكلة البيكسل خاصةً أن غالبية الخلفيات ذات الجودة العالية يمكن العثور عليها بصيغة PNG.

الشكل 11.2: تنسيق PNG

4.3.2.2 تنسيق TIFF

هو اختصار لـ "Tagged Image File Format"، وهو تنسيق ملف صور يُستخدم لتخزين الصور والرسوم البيانية بجودة عالية. يمتاز بقدرته على دعم صور غنية بالتفاصيل وجميع التأثيرات البصرية مما يجعله مثاليًا للمشاريع التي تتطلب دقة وتفصيلًا عاليين مثل الطباعة الفوتوغرافية والتصميم الاحترافي. ورغم فوائده العديدة، إلا أنّ ملفات TIFF تكون أكبر حجماً بالمقارنة مع بعض تنسيقات الضغط الأخرى مما يقلل من فعاليتها في استهلاك مساحة التخزين عند نقل الصور عبر الإنترنت [19].

الشكل 12.2: تنسيق TIFF

5.3.2.2 تنسيق SVG

هو اختصار لـ "Scalable Vector Graphics"، وهو تنسيق ملف صور يُستخدم لتخزين الرسوميات القابلة للتحكم والتي يمكن تغيير حجمها بدون فقدان جودتها. يتميز SVG بكونه يعتمد على الرسوميات المتجهة، حيث يتم توصيل الصور باستخدام معلومات رياضية تصف الشكل والألوان.

رغم بساطة هيكله، يُعتبر SVG قويًا ومفيدًا للصور التي يتم تكبيرها أو تصغيرها بشكل متكرّر، ويُستخدم بشكل شائع في تصميم الويب. يمكن تحرير ملفات SVG بسهولة باستخدام نصوص التحرير أو البرمجيات المخصصة مما يجعله مثاليًا للرسوميات التفاعلية والرسوم البيانية في الويب.

الشكل 13.2: تنسيق SVG

الجدول 2.2: مقارنة بين التنسيقات

نوع	الضغط	العرض التدريجي	التنشيط	الشفافية
JPEG	نعم (قابل للتعديل، بفقدان)	16مليون	نعم	لا
GIF	256 كحد أقصى (لوحة)	نعم	نعم	نعم
PNG	نعم (بدون فقدان)	نعم	لا	نعم
TIFF	ضغط بفقد أو بدون فقد	لا	لا	نعم
SVG	ضغط ممكن (بشكل طبيعي)	لا	نعم	نعم

4.2.2 الخصائص الرئيسية للصور الرقمية

نذكر في هذا العنصر أهم الخصائص الرئيسة للصور الرقمية من البكسل، وعمق البت، الضوضاء، الأبعاد، الدقة، التباين، السطوع، الحواف والأنسجة، وحجم الملف.

1.4.2.2 البكسل

البكسل (Pixel) هو اختصار لكلمتي عنصر الصورة"Picture éléments"، وتشير إلى أصغر وحدة رئيسية في الصور الرقمية. يمثل البكسل نقطة صغيرة على الشاشة تحمل لونًا محددًا. يتم ترتيب البكسلات بشكل متسلسل لتشكيل الصورة ككل [20].

عادةً ما يتم تعريف الصورة بوحدات البكسل في الارتفاع والعرض. على سبيل المثال إذا كانت صورة ما تحتوي على أبعاد 50x100، فهذا يعني أنها تتألف من 100 بكسل في العرض و50 بكسل في الارتفاع [23].

في السياق الأكثر تقدّمًا يمكن للبكسل أن يحمل معلومات إضافية مثل اللون. في الفضاء اللوني RGB يُمثل كل بكسل مزيجًا من اللون الأحمر والأخضر والأزرق. هذا التكوين اللوني يسمح بتكوين مجموعة واسعة من الألوان عند تجميع البكسلات في الصورة.

2.4.2.2 عمق البت

يتم تحديد عمق البت (Bit depth) بواسطة عدد البتات المستخدمة لتعريف كل بكسل. يحمل كل بكسل قيمة عددية بعمق البت الذي قد يشير إلى قيمة لون أو درجة رمادية. وبالتالي يمكن إنتاج الصور الرقمية بالأبيض والأسود (ثنائي)، أو بدرجات الرمادي، أو بالألوان. على سبيل المثال عندما يكون عمق بت البكسل ثمانية بت يمكن للبكسل الإشارة إلى صورة رمادية تحتوي على 256 قيمة مختلفة، حيث تمثل كل قيمة درجة من درجات الرمادي. الصورة الثنائية تكون لديها عمق 2 بت، في حين أنه في صورة الرمادية ستكون لدينا 8 بت (بايت واحد) لقيمة كل بكسل. يمكن أن تكون بكسلات صورة RGB بإجمالي 24 بتًا.

3.4.2.2 الضوضاء

الضوضاء(noise) غالبًا ما تكون موجودة على صور الوثائق لأنها قد تظهر في مراحل مختلفة من سلسلة التحويل إلى رقم: أثناء الطباعة، على مدى فترة حياة الوثيقة، وأثناء عملية الفحص الرقمي.

تُستخدم أساليب المعالجة التقليدية، مثل استخدام مرشحات الوسيط لتصفية البكسل المعزولة على الصورة. بالإضافة إلى ذلك، تُستخدم الرياضيات بشكل شائع لتصحيح العيوب الطفيفة على الصور مثل "إعادة تجميع" قطع الأحرف [11].

الشكل 14.2: تأثير الضوضاء على الصورة

4.4.2.2 الأبعاد

البُعد (Dimension) هو حجم الصورة ويظهر في شكل مصفوفة تكون عناصرها قيم رقمية تُمثل الشدّة الضوئية (بيكسل). حيث يكون عدد الأسطر في هذه المصفوفة مضروبًا في عدد الأعمدة يُعطي عدد البكسل الإجمالي في الصورة [19].

الشكل 15.2: أبعاد الصورة

5.4.2.2 الدقة

يشير مصطلح "الدقة" (Resolution) إلى القدرة على تفصيل التفاصيل في الصورة أو الرسم بشكل واضح. تعتمد الدقة على عدد البكسلات في الصورة، حيث كلما زاد عدد البكسلات زادت دقة الصورة. الصور ذات الدقة العالية تحتوي على مزيد من التفاصيل وتعرض الصور بشكل أوضح، بينما الصور ذات الدقة المنخفضة قد تظهر باهتة وتفتقر إلى التفاصيل الدقيقة.

الشكل16.2 : دقة الصورة

6.4.2.2 التباين

التباين (contraste) هو الاختلاف الملحوظ بين منطقتين في صورة، وتحديداً بين المناطق المظلمة والمناطق الفاتحة في هذه الصورة. يتم تعريف التباين بناءً على سطوع منطقتين من الصور. فإن التباين (C) يتم تعريفه بالعلاقة التالية:

$$C = \frac{L1 - L2}{L1 + L2} \qquad (1.2)$$

حيث:

- $L1$: درجة السطوع المنطقة الأولى.
- $L2$: درجة السطوع المنطقة الثانية.

7.4.2.2 السطوع

السطوع (Brightness) هو الإحساس البصري الذي نتلقاه من الضوء. من بين جميع الكميات التي تميز الضوء يعتبر السطوع هو الأكثر أهمية بالنسبة لنا. عندما تتعطل الرؤية في ظروف الإضاءة المنخفضة أو عندما يبهرنا ضوء أمامي فإن السطوع هو العامل المؤثر.

هناك العديد من العوامل التي تؤثر على مستوى السطوع. أولاً هناك شدة ضوء المصدر. ثم يتأثر السطوع أيضًا بكيفية انعكاسه بواسطة سطح مضاء. أخيرًا، يؤثر لون مصدر الضوء أيضًا على مستوى السطوع [10].

الشكل 17.2: سطوع صورة

8.4.2.2 الحواف والأنسجة

الحواف والأنسجة (Edges and textures) هما مفهومان مهمان في معالجة الصور والرؤية الحاسوبية. الحواف هي الحدود بين الأشياء في الصورة، بينما تصف الأنسجة أنماط السطح لتلك الأشياء. يهدف استخراج الحواف إلى تحديد حواشي الأشياء، بينما يهدف تحليل الأنسجة إلى تصنيف أو تقسيم الأنسجة بناءً على خصائصها.

الشكل 18.2: حواف صورة

9.4.2.2 حجم الملف

حجم الملف (Size file) يحدده إجمالي عدد البكسلات في الصورة. يمكن استخدام معادلة بسيطة لإيجاد حجم ملف الصورة إذا تم إعطاء أبعاد البكسل، حيث نضربها ببعضها البعض وبعمق البت لتحديد عدد البتات في ملف الصورة كما هو موضح في المعادلة حجم الملف (بايت) = (أبعاد البكسل × عمق البت) / 8

مثال: إذا أخذنا صورة 24 بت بأبعاد بكسل 1024 × 640، فإن حجم الملف يساوي 1966080 بايت

حجم الملف (بايت) = 1024 × 640 × 24 / 8

3.2 طرق تشفير الصور

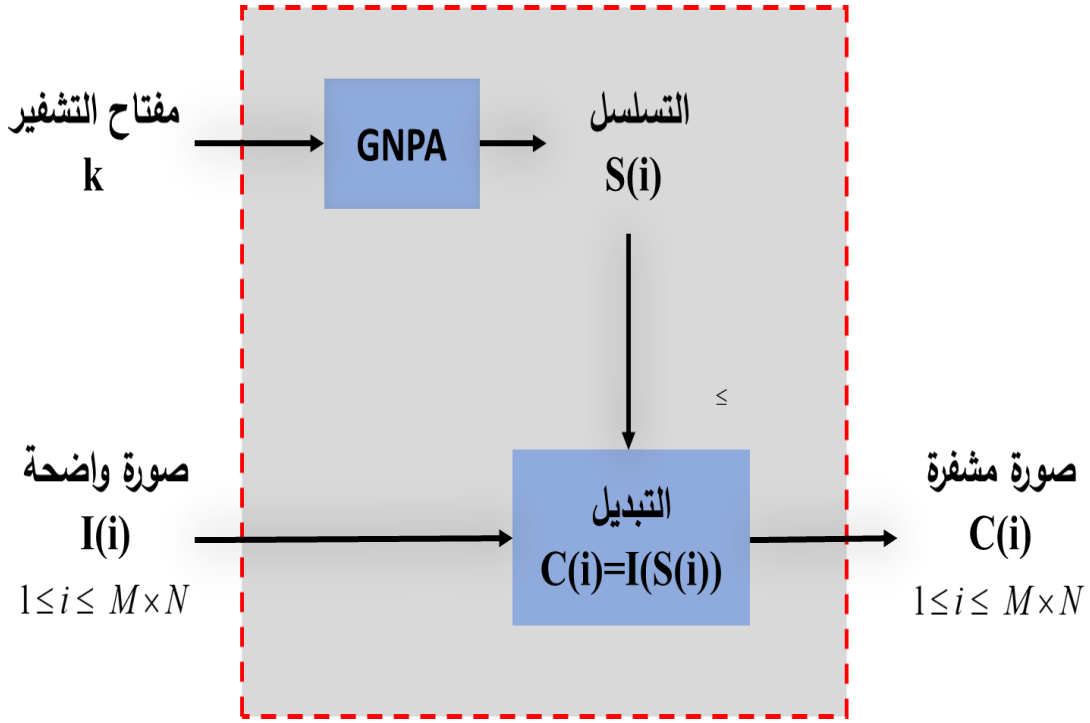
وفقًا لـ شانون يجب أن تتضمن طريقة التشفير خاصستين رئيسيتين هما: الخلط والانتشار. في تشفير الصور يتعلق الخلط بجعل العلاقة بين مفتاح التشفير والصورة المشفرة أكثر تعقيدًا. أما الانتشار فيشير إلى أن الزائدة الإحصائية بين بكسلات الصورة الواضحة يجب أن تتبدد في إحصائيات الصورة المشفرة، وهذا يعني أن الترابط بين بكسلات الصورة الواضحة لا يجب أن يظهر في الصورة المشفرة. ببساطة يتم تحقيق الخلط والانتشار عن طريق عمليات الترتيب والاستبدال للبكسلات [13].

نظرًا لحجم البيانات الكبير الذي يجب التعامل معه تستخدم خوارزميات تشفير الصور عادةً طريقة تشفير تقليدية. سنتحدث أولاً عن الطرق الشائعة لتشفير الصور التي تعتمد على مولد أرقام عشوائية زائفة (GNPA) ومبدأ الترتيب والاستبدال. بعد ذلك سنناقش تطبيق نظرية الفوضى في إنتاج الأرقام العشوائية لتشفير الصور.

1.3.2 تشفير الصور عن طريق التبديل والاستبدال

تتضمن خوارزميات تشفير الصور التي تعتمد على عمليات التبديل والاستبدال (Image encryption by permutation and substitution) استخدام مولد للأرقام الشبه عشوائية (GNPA) [25]. يتعين توفير بيانات المفتاح السري K وطول التسلسل الشبه عشوائي الذي سيتم إنشاؤه إلى مُدخلات هذه المُولِّدات. تهدف طرق التشفير عبر التبديل إلى تحويل صورة واضحة إلى صورة غير قابلة للفهم، من خلال تبديل مواقع البكسل [26]،[27].

فلنفترض أن هناك صورة واضحة I بحجم $M\times N$ بكسل، باستخدام مفتاح سري K، يتم تشفير I بواسطة التبديل باستخدام GNPA لإنشاء تسلسل S بحجم $M\times N$ عناصر شبه عشوائية تحدد المواقع الجديدة للبكسلات في الصورة I، وذلك وفقًا للشرط التالي:

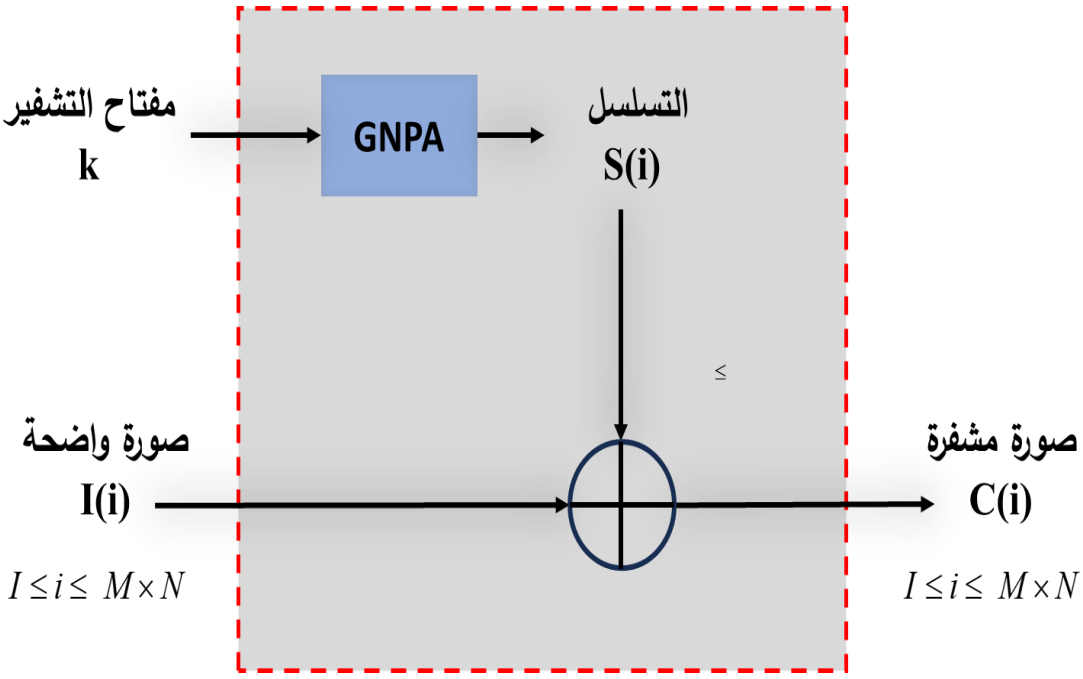


الشكل 19.2: مبدأ التشفير الصور بالتبديل

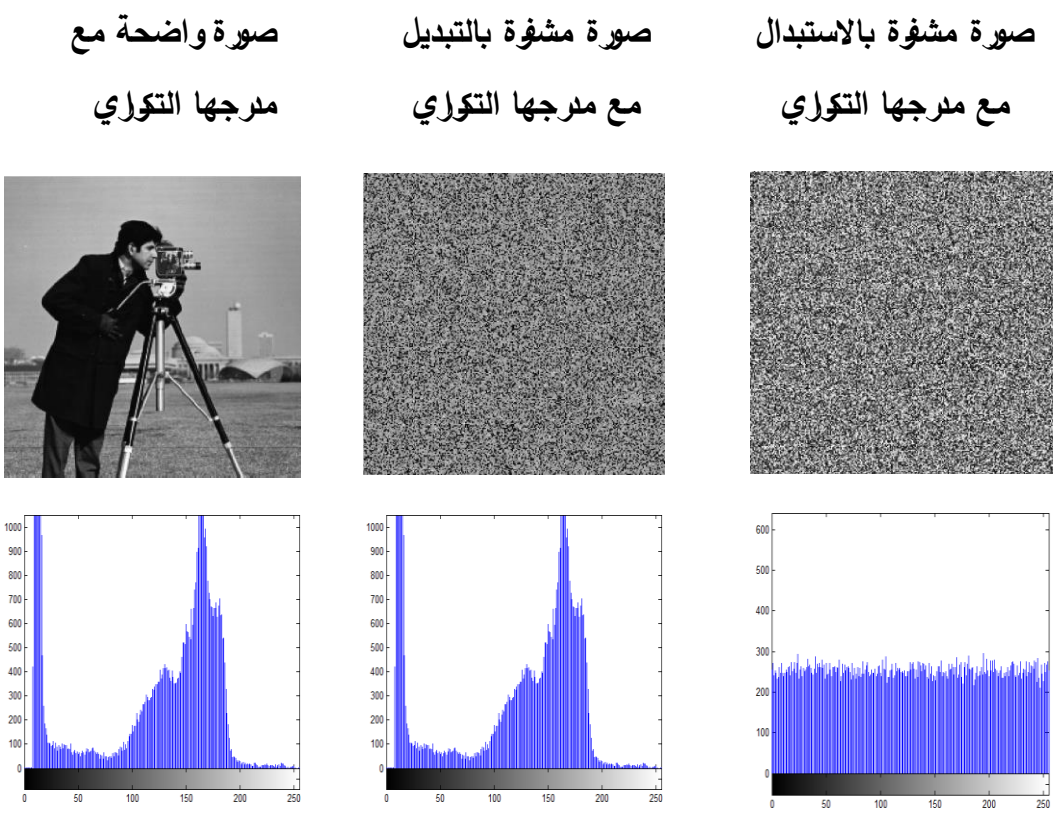
$$\forall\ I\le i,j\le M\times N\,,\ i\neq j\ \Rightarrow S(i)\neq S(j) \qquad (2.2)$$

فيما يتعلق بتشفير الصور بواسطة الاستبدال، يعتمد على عملية "أو استبعادي" بين محتوى الصورة الواضحة والتسلسل الشبه العشوائي المُنشأ [28]،[29]. كما هو موضح في المعادلة (3.2) والشكل (20.2) حيث يتم الحصول على الصورة المشفرة C عن طريق إجراء عملية الأو استبعادي على مستوى البت بين كل بكسل في الصورة I (i) والبايت S(i) المرتبط في التسلسل الشبه عشوائي S.

$$C(i)=I(i)\oplus S(i) \qquad I\le i\le m\times n \qquad (3.2)$$



الشكل20.2: مبدأ تشفير الصور بالاستبدال



الشكل 21.2: صورة مشفرة بالتبديل وبعدها بالاستبدال

الشكل (21.2) يقدم صورة واضحة، بالإضافة إلى نسختها المشفرة باستخدام التشفير بالتبديل والتشفير بالاستبدال، مع الهيستوغرامات المرتبطة. يظهر أن هيستوغرام البكسلات في الصورة المشفرة بالتبديل متطابق تمامًا مع هيستوغرام الصورة الواضحة. هذه الطريقة في التشفير تعاني من عيب الاحتفاظ ببعض الخصائص الإحصائية للصورة الواضحة. بالمقابل توزيع البكسلات في الصورة المشفرة بالتبديل يقترب من التوزيع القياسي. لذلك باستخدام طريقة التشفير بالتبديل إذا كانت البكسلات المجاورة مرتبطة بشكل قوي في الصورة الواضحة فإن هذا ليس الحال في الصورة المشفرة. بالتالي وعلى عكس النتائج التي تم الحصول عليها باستخدام التشفير بالتبديل، يظهر تحليل الصورة المشفرة بالتبديل أن محتوى الصورة الواضحة هو سري بصريًا.

2.3.2 استخدام الفوضى في توليد الأرقام شبه العشوائية

اكتسبت مولدات الأرقام شبه العشوائية أهمية كبيرة في مجال تأمين البيانات وأثبتت فعاليتها الكبيرة، حيث يتم استخدامها بشكل شائع في التطبيقات التشفيرية وأنظمة التشفير. لا يمكن لأي خوارزمية شبه عشوائية أن تولد حقًا سلسلة آمنة من التحليل الإحصائي، ويجب على المولدات الحالية أن تشمل جزءًا من الصدفة الذي لا يتم إنتاجه بواسطة وسيلة محددة، لذلك نتجه نحو مولدات الفوضى التي تمتلك خوارزمية توليد لأرقام شبه عشوائية قوية، وتبدأ بالتهيئة باستخدام وسيلة فيزيائية لإنتاج الفوضى [30].

وبالتالي تكمن ميزة استخدام الفوضى في أنظمة تشفير الصور في سلوكها العشوائي والقدرة على التنبأ بها. وهكذا تمتلك التسلسلات المُشيدة من أنظمة الفوضى خصائص إحصائية تقترب من الخصائص العشوائية [31]،[32]،[33]،[34].

يمكن تقسيم الأنظمة الفوضوية المستخدمة في تشفير الصور إلى أنظمة فوضوية أحادية الأبعاد وأنظمة فوضوية متعددة الأبعاد. تتمتع الأنظمة الفوضوية أحادية الأبعاد بهياكل بسيطة وسهلة التنفيذ، ولكنها قد تكون لديها مجموعة محدودة من السلوك الفوضوي ومساحة مفتاح محدودة. وبالتالي قد تكون طرق تشفير الصور التي تستخدمها ذات مستوى أمان نسبيًا منخفضًا، وبالتالي فهي عرضة للتهديدات [35].

تم تصميم معظم أنظمة تشفير الصور التي تستخدم GNPA بناءً على الفوضى باستخدام هيكل الخلط والانتشار. الخلط يعني إلى أي مدى يمكن أن يؤثر تغيير بت واحد من المفتاح السري على الصورة المشفرة، والانتشار يعني إلى أي مدى يمكن أن يؤثر تغيير بت واحد من الصورة الواضحة على الصورة المشفرة [35].

3.3.2 تطور تشفير الصور بناءً على الفوضى

يتم استخدام الأنظمة الفوضوية على نطاق واسع في علم التشفير بسبب خصائصها مثل الحساسية للظروف الابتدائية والقدرة على عدم التنبؤ بها. تم نشر العديد من الأعمال حول تشفير الصور باستخدام الخرائط الفوضوية. على سبيل المثال استخدم الباحثون خريطة قطة آرنولد الفوضوية لتبديل مواقع البكسلات في الصورة، ثم تم معالجة إشارة مخرج النظام الفوضوي لـ تكييفها لتشفير الصور بالألوان الرمادية، وتم تشفير الصورة المبادلة بواسطة إشارة معالجة بيكسل بيكسل [36].

قدم الباحثون هيكل الشبكة الكلاسيكي للاستبدال والتبديل في علم التشفير لضمان خصائص الخلط والانتشار لتحقيق تشفير آمن باستخدام الخريطة اللوجستية ثنائية الأبعاد [37]. ولتجاوز القيود الموجودة في الخرائط الفوضوية أحادية الأبعاد كأنظمة بسيطة وسهلة التنبؤ اعتمد الباحثون على خريطة لوجستية جيبية جديدة ثنائية الأبعاد لتشفير الصور كما اقترحوا بأن تكون الخريطة اللوجستية الجيبية جديدة ومعدلة، حيث استخدموا الخريطة اللوجستية لضبط إدخال الخريطة الجيبية، ثم قاموا بتوسيع مستوى المرحلة الثنائية الأبعاد [38]،[39]،[40].

تم اقتراح خوارزميات جديدة لتشفير الصور الحساسة بناءً على الخريطة الفوضوية لزاسلافسكي، حيث استخدم الباحثون الخريطة الفوضوية لزاسلافسكي كمولد شبه عشوائي لتوليد مفتاح التشفير. في هذا النموذج الأخير تمّ استخدام شبكة الاستبدال والتبديل لضمان خصائص الخلط والانتشار في الصورة المشفرة ليتم تطبيق هيكل جديد لتشفير الصور بناءً على خريطة فوضوية بسيطة أحادية الأبعاد [41]،[42].

فيتم تقديم خوارزمية جديدة مع ثلاث تسلسلات فوضوية غير خطية وهي خرائط لوجستية ثلاثية الأبعاد لتشفير الصور. تقدم أعمال خوارزمية تشفير للصور اللونية RGB والنصوص بناءً على أنظمة فوضوية كسورية [43]. تم استخدام خريطة اقتصادية فوضوية أحادية الأبعاد لتشفير وفك تشفير الصور. تركز العديد من الأعمال الحديثة على تشفير الصور بناءً على الفوضى [44]،[45].

4.2 قياسات أداء خوارزميات تشفير الصور

بمجرد أن يتم تشفير الصورة، يصبح من الضروري تقييم مستوى أمانها. في هذا القسم، سنقدّم تعريفًا لأهم قياسات الأمان المعروفة لتشفير الصور.

1.4.2 المدرج التكراري

يوفر المدرج التكراري (Histogram) نظرة رسومية على توزيع قيم البكسل من خلال تمثيل عدد البكسل المرتبطة بكلّ مستوى رمادي. غالبًا ما يتم استخدام هذا التمثيل الرسومي كمقياس لتقييم توزيع البيانات بشكل نوعي بهدف تحليل مقاومة نظام التشفير للهجمات الإحصائية. لضمان فعالية نظام التشفير يجب أن يخفي هذا المقياس أيَّ معلومات ملحوظة تتعلق بالصورة الأصلية أو العلاقة بين الصورة الأصلية والصورة المشفرة.

1.1.4.2 المدرج التكراري أحادي النمط

يُعرف المدرج التكراري الأحادي النمط (Unimodal Histogram) بأنه المدرّج الذي يحتوي على قمة واحدة فقط. يشير هذا إلى أن جميع البكسل في الصورة تقريبًا لها نفس مستوى الرمادي.

2.1.4.2 المدرج التكراري ثنائي النمط

يُعرف المدرج التكراري ثنائي النمط (Bimodal Histogram) بأنه المدرج الذي يحتوي على قمتين منفصلتين جيدًا. يشير هذا إلى أن هناك مجموعتين من البكسل في الصورة حيث كل مجموعة لها مستوى رمادي مختلف.

3.1.4.2 المدرج التكراري متعدد الأنماط

يُعرّف المدرج التكراري متعدد الأنماط (Multimodal Histogram) بأنه المدرج الذي يحتوي على عدة قمم منفصلة. يشير هذا إلى أن هناك عدة مجموعات من البكسل في الصورة حيث كل مجموعة لها مستوى رمادي مختلف.

2.4.2 معامل الارتباط

الارتباط (Correlation) يكون البكسل مرتبطًا ارتباطًا وثيقًا بالبكسلات المجاورة له. يعد الارتباط قياسًا يتمثل في مراقبة الارتباط بين البكسلات في الاتجاهات الأفقية والعمودية والمائلة للصورة المشفرة. يجب أن تلغي خوارزمية التشفير الآمنة هذا الارتباط بين البكسلات المجاورة، أي جعله قريبًا جدًا من الصفر، حتى يكون نظام التشفير مقاومًا للهجمات الإحصائية.

يتم اختيار m أزواج من البكسلات المجاورة (xi، yi) في الاتجاهات الثلاثة لحساب معامل الارتباط وفقًا للمعادلة التالية:

$$Corr(x,y)=\frac{\sum_{i=0}^{m-1}(x_i-\mu_X)\times(y_i-\mu_y)}{\sqrt{\sum_{i=0}^{m-1}(x_i-\mu_x)^2}\times\sqrt{\sum_{i=0}^{m-1}(y_i-\mu_y)^2}} \quad (4.2)$$

حيث:

μx و μy هي المتوسطات الحسابية للمجموعات x و y، مع xi ∈ x و yi ∈ y. تتراوح قيمة معامل الارتباط هذا بين 1− و 1.

لتقييم جودة التشفير، يتم حساب الارتباط بين صورة واضحة I بحجم (M × N) ونسختها المشفرة J بحجم (M × N) وفقًا للمعادلة التالية:

$$C(I,J)=\frac{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\left((I(i,j)-\bar{I}(i,j)\right)\times\left(J(i,j)-\bar{j}(i,j)\right)}{\sqrt{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\left((I(i,j)-\bar{I}(i,j)\right)^2}\times\sqrt{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\left(J(i,j)-\bar{j}(i,j)\right)^2}} \quad (5.2)$$

حيث I و J هي المتوسطات الحسابية للصورة الأصلية I والصورة المشفرة J.

3.4.2 الإنتروبيا

إنّ الإنتروبيا Shannon هي مقياس لكمية المعلومات المستخدمة لتقييم الطبيعة العشوائية لتوزيع البكسلات في صورة مشفرة. نظريًا يجب أن تكون إنتروبيا المعلومات 8 بتات للصور ذات المستوى الرمادي و1 بت للصور الثنائية. إذا أنشأ مخطط التشفير صورة مشفرة يكون إنتروبيا المعلومات لها أقل من 8 بتات للصور ذات المستوى الرمادي أو أقل من 1 بت للصور الثنائية فهناك إمكانية للتنبؤ. يتم حساب الإنتروبيا (Shannon) وفقًا للمعادلة التالية:

$$H(m)=\sum_{i=0}^{2^n-1}p(m_i)\times\log_2\frac{1}{p(m_i)} \quad (6.2)$$

- n = 1 للصور الثنائية و n = 8 للصور ذات المستوى الرمادي.
- p(mi) هي احتمال حدوث المستوى الرمادي mi.

4.4.2 معدل تغيير البكسل

يُعرف معدّل تغيير البكسل (NPCR - Number of Changing Pixel Rate) بأنه مقياس يتم التعبير عنه بالنسب المئوية ويستخدم لتحديد مدى اختلاف الصورة المشفرة عن الصورة الواضحة. وبالتالي كلما كانت قيمة NPCR أقرب إلى 100٪، كانت الصورتان مختلفتان، وبالتالي كان مستوى الأمان البصري أعلى [46].

يتم حساب NPCR بين صورتين بحجم m × n بكسل $p(i,j)$ و $p'(i,j)$ من أجل $0 \prec i \prec m-1$ و $0 \prec i \prec n-1$ وفقًا للمعادلة التالية:

$$NPCR = \frac{\sum_{i=0}^{m-1}\sum_{j=0}^{n-1} d(i,j)}{m \times n} \times 100\% \qquad (7.2)$$

حيث $d(i,j)$ معرفة كما يلي:

$$d(i,j) = \begin{cases} 1 & p(i,j) \neq p'(i,j) \\ 0 & p(i,j) = p'(i,j) \end{cases} \qquad (8.2)$$

5.4.2 متوسط كثافة الشدة المتغيرة الموحدة

يعرف متوسط كثافة الشدة المتغيرة الموحدة (UACI - Unified Averaged Changed Intensity) بأنه مقياس يتم التعبير عنه بالنسب المئوية ويستخدم لقياس الفرق بين صورتين بحجم m × n بكسل، وحيث يتم ترميز البكسلات $p(i,j)$ و $p'(i,j)$ ، من أجل $1 \prec i \prec m$ و $1 \prec j \prec n$ على 2^l قيم من مستويات الرمادي، كلما كانت قيمة UACI أكبر، كان مستوى الأمان البصري أعلى، يتم حسابها وفقًا للمعادلة التالية [46]:

$$UACI = \frac{1}{m \times n} \sum_{i=0}^{m-1}\sum_{j=0}^{n-1} \frac{|p(i,j) - p'(i,j)|}{2^l - 1} \times 100\% \qquad (9.2)$$

6.4.2 تحليل الهجوم التفاضلي

تحليل الهجوم التفاضلي (Differential attack analysis) يستخدم NPCR وUACI لتحليل مقاومة الهجمات التفاضلية. تُستخدم هذه الهجمات لاختبار حساسية نظام تشفير الصور لتغييرات طفيفة في الصورة الواضحة، بشكل عام يتم تغيير بت واحد فقط، ثم يتم تشفير الصورة الواضحة الأصلية والصورة الواضحة المعدلة باستخدام نفس المفتاح، ويتم بعد ذلك مقارنة الصور المشفرة الناتجة. على الرغم من أن الصور الواضحة متشابهة تقريبًا يجب أن تكون الصور المشفرة مختلفة جدًا.

وفقًا للنظريات فإن القيمة المتوقعة لـ NPCR بين صورة ذات مستوى رمادي تعسفي وصورة عشوائية مثالية تساوي 99.6094٪، وتلك الخاصة بـ UACI لصورتين عشوائيتين تساوي 33.4635٪[47].

7.4.2 تحليل مساحة مفتاح التشفير

يجب أن تكون مساحة المفتاح لنظام التشفير كبيرًا بما يكفي لمقاومة هجمات القوة الغاشمة. هجوم القوة الغاشمة هو هجوم يحاول فيه شخص ما كسر خوارزمية التشفير عن طريق إجراء بحث شامل لجميع المفاتيح الممكنة. لتوفير أمان كافٍ ضد هجمات القوة الغاشمة يجب أن تكون حجم مساحة المفتاح أكبر من 2^{100} [48].

8.4.2 تحليل حساسية مفتاح التشفير

يجب أن يكون التشفير الآمن حساسًا لمفتاح التشفير. يتم اختبار حساسية المفتاح في حالة التشفير وفك التشفير بحيث يتم إجراء الاختبار باستخدام ثلاث مفاتيح، المفتاح الصحيح ومفتاحين آخرين، يختلف كل منهما عن المفتاح الصحيح ببت واحد فقط. في هذه الحالة يجب أن تنتج خوارزميات التشفير وفك التشفير صورًا مختلفة تمامًا. يتم استخدام NPCR وUACI لإجراء اختبارات حساسية المفتاح.

5.2 الخاتمة

في هذا الفصل، قمنا بعرض مقدمة حول تشفير الصور الرقمية، حيث قمنا في بادئ الأمر بتقديم معلومات عامة عن الصور الرقمية مع تعريف الصور الرقمية وذكر أنواعها، كما تطرقنا إلى ذكر صيغ الصور الرقمية وذكر خصائصها الرئيسية، وأيضا تطرقنا إلى طرق تشفير الصور الرقمية، كما تحدثنا عن استخدام الفوضى في

توليد الأرقام شبه العشوائية وتطور تشفير الصور بناء على الفوضى وفي نهاية الفصل تطرقنا إلى قياسات أداء تشفير الصور.

الفصل الثالث

تطبيق الأنظمة الفوضوية في عملية التشفير

1.3 مقدمة

مع تطور علم الحوسبة ونظرية أمان المعلومات، تزايد الاهتمام بدراسة تشفير البيانات وأصبح هذا المجال موضوعًا واسع النطاق للبحث. بشكل خاص أصبح تشفير الصور تكنولوجيا رائجة للدراسة، حيث يسعى الباحثون لتحقيق فعالية أكبر في تأمين الصور. رغم استخدام الخوارزميات التقليدية مثل RSA وDES في تشفير الصور، إلا أنها غالبًا ما تواجه صعوبات في التعامل مع التحديات الحديثة لمعالجة الصور، مما يستدعي الحاجة الملحة إلى تطوير خوارزميات جديدة وفعّالة لهذا الغرض.

يمكن القول إن ظهور علم الفوضى حفز الباحثين على استكشاف مجال تشفير الفوضى، حيث أصبحت تقنيات التشفير التي تعتمد على الفوضى جزءًا هامًا من تقنيات تشفير الصور. حيث تتميز هذه التقنيات بالتفاعل مع خصائص الفوضى التي تكون حساسة للشروط الابتدائية والقيم الحالية. تستطيع أنظمة الفوضى إنتاج إشارات متنوعة باستخدام مفاتيح مختلفة، ويمكن إعادة إنتاج هذه الإشارات للفك فقط باستخدام النظام الفوضوي والقيم الابتدائية. وبالتالي ينتج عن ذلك الحاجة إلى تخزين أقل للمعلومات خلال عمليات التشفير وفك التشفير، مما يقلل من مخاطر تسرب المعلومات. بالإضافة إلى ذلك، فإن إشارات الفوضى تعتبر شبه عشوائية، مما يجعلها سهلة الاستخدام في عمليات التشويش والتشتيت للمعلومات بشكل فعّال.

2.3 الأنظمة الفوضوية

في هذا الجزء سنتعرف على الأنظمة الفوضوية بشكل عام.

1.2.3 نبذة تاريخية عن الأنظمة الفوضوية

لم تُعطَ أهمية علمية لنظرية الفوضى إلا في نهاية القرن التاسع عشر على يد هنري بوانكاريه (1854–1912)، وذلك لعدة أسباب منها أعمال إسحاق نيوتن (1642–1727) التي جعلت الحتمية تسيطر على العلم. ومن خلال معرفة الحالة الأولية لنظام معين، اعتقد العلماء أنهم يستطيعون التنبؤ بشكل كامل ودقيق بمستقبل هذا النظام.

بعد حوالي قرن من أعمال نيوتن، قام بيير سيمون لابلاس (1749–1827) بتحديد المعنى المطلق للحتمية وأكد أن الحالة الحاضرة للكون تمكّن من التنبؤ بمستقبله. ومع ذلك قام بوانكاريه بإثبات أن لابلاس كان

على خطأ، واعتمد في آرائه على مشكلة الأجرام الثلاثة في الميكانيكا السماوية، التي تجعل التنبؤ غير ممكن تمامًا وأن حركة الأجسام الثلاثة لا تتكرر إلا في الحالات الخاصة.

لاحظ بوانكاريه هذه الظاهرة وقال: "أسباب صغيرة جدًا لا نلاحظها يكون تأثيرها كبيرًا." وقام جيمس ماكسويل في عام 1860 بتقديم مثال حول حركة الجزيئات التي لا يمكن رؤيتها وكيف أن حركتها تزيد من الحركة العشوائية للغازات تدريجيًا.

في عام 1898 لاحظ جاك هادامارد الاختلاف العام في المسارات في الفضاء، وفي عام 1908 ناقش بيير دوهيم الأهمية العامة المحتملة لهذا الاختلاف، وتوصل إلى نتيجة أنه لا يمكن للإنسان أبدًا الوصول إلى توقع كامل للنظام الفوضوي بسبب عشوائية الحالة الأولية.

في عام 1961 لاحظ إدوارد لورنز عالم الأرصاد الجوية وأستاذ الرياضيات في معهد ماساتشوستس للتكنولوجيا الظاهرة التي سُميت لاحقًا نظرية الفوضى الحتمية أثناء محاولته لحساب توقعات الظواهر الجوية. كانت هذه التنبؤات تتطلب عددًا كبيرًا من الحسابات للمعادلات التفاضلية المعقدة، واستخدم لورنز جهاز الكمبيوتر "Royal Mcbee LGP-300"، مما جعله الأب الرسمي لنظرية الفوضى [49].

بعد عدة ساعات من الحسابات، اكتشف لورنز أن تغييرًا طفيفًا في المتغيرات الأولية يؤدي إلى نتائج مختلفة تمامًا، مما أدّى إلى إكتشافه للحساسية الشديدة للظروف الأولية. أطلق لورنز على هذه الخاصية اسم "تأثير الفراشة"، حيث أن أدنى اختلاف في المعاملات يؤدي إلى تغيير جذري في حلا المعادلة، مما يؤدي إلى سلوك فوضوي.

في عام 1971 نشر الفيزيائي البلجيكي ديفيد رويل وعالم الرياضيات فلوريس تاكنز مقالًا حللا فيه الحالات النهائية للنماذج الرياضية للأنظمة التي تبدد جزءًا من طاقتها كحرارة، وأظهرت النتائج أن مجموعة الحالات النهائية لكل نظام ذات بعد كسري تكون جاذبًا فوضويًا.

2.2.3 تعريفها

ظاهرة الفوضى هي عملية معقدة وغير خطية، تعتمد على عدة متغيرات وتتميز بحساسية شديدة للظروف الابتدائية.

الأنظمة الفوضوية تُعرف بأنها أنظمة يتطور مسارها في منطقة محددة، حيث تظهر ثباتًا دون أن تتقارب نحو نقطة ثابتة أو دورة حدودية. تلك المسارات التي تظل كثيفة في هذه المنطقة تظهر حساسية قوية للظروف الابتدائية. لا يمكن الحصول بدقة على حلول المعادلات التفاضلية غير الخطية باستخدام الطرق التحليلية، نظرًا لعدم وجود طرق عامة للحل التحليلي لهذا النوع من المعادلات، إلا إذا كان ذلك ينطبق على فئات معينة. ونتيجة لذلك يتم تحديد هذه الحلول عدديًا، ويتم تحليل سلوك النظام من خلال المحاكاة.

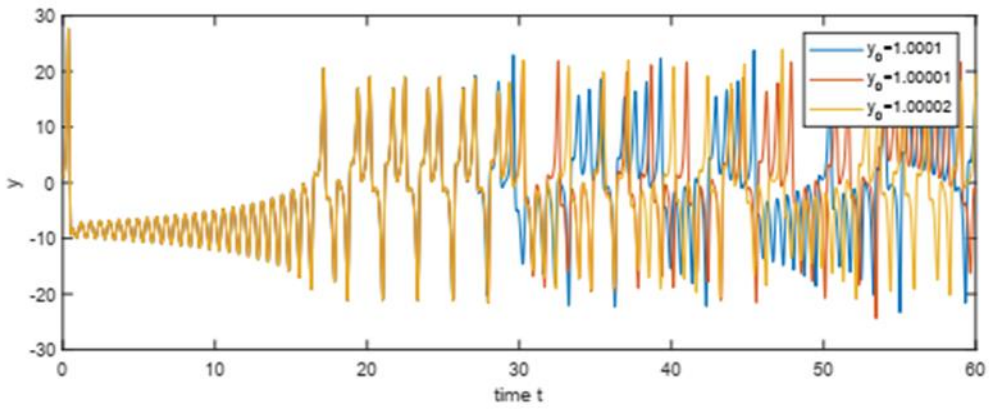
3.2.3 خصائصها

تظهر الأنظمة الفوضوية عدة خصائص مميزة تفرقها عن الأنظمة المنتظمة والقابلة للتنبؤ. فيما يلي بعض الخصائص الرئيسية للأنظمة الفوضوية:

1.3.2.3 حساسية للظروف الابتدائية

حساسية للظروف الابتدائية هي إحدى السمات الأساسية للأنظمة الفوضوية، كما شرحها لورنز في عبارته الشهيرة حول "تأثير الفراشة". فإذا حدث تغيير طفيف في الظروف الابتدائية لنظام فوضوي يؤدي ذلك إلى وجود مسارين يكونان في البداية متقاربين ثم يتباعدان بشكل تسارعي. فيما بعد تصبح المسارات غير قابلة للمقارنة، مما يجعل الأنظمة الفوضوية غير قابلة للتنبؤ على المدى الطويل [50]. نأخذ مثالًا على نظام لورنز الذي يُوصف بواسطة مجموعة المعادلات التالية:

$$\begin{cases} \dot{x} = \sigma(y - x) \\ \dot{y} = rx - y - xz \\ \dot{z} = -bz + xy \end{cases} \tag{1.3}$$



الشكل 1.3: تطور نظام لورنز

يمثل الشكل (1.3) تطور نظام لورنز بدلالة الزمن عند ثلاث قيم ابتدائية حيث نلاحظ أن أي تغيير بسيط في القيم الابتدائية المكونة من 4 أرقام أو 5 أرقام بعد الفاصلة يؤدي إلى مسارات مختلفة مع تطور النظام.

2.3.2.3 غير خطي

النظام الفوضوي هو نظام ديناميكي غير خطي، ولا يمكن أن يكون النظام الخطي فوضويًا. يتعلق مفهوم النظام الديناميكي بجميع الأنظمة التي تعتمد تطوراتها على الزمن. بشكل عام، للتنبؤ بالظواهر الحقيقية التي تولدها هذه الأنظمة، تتمثل الخطوة الأولى في بناء نموذج رياضي ينشئ علاقة بين مجموعة من الأسباب ومجموعة من النتائج (أسباب / نتائج). إذا كانت هذه العلاقة عبارة عن عملية تناسبية، فإن الظاهرة تكون خطية. أما في حالة الظاهرة غير الخطية، فإن النتيجة لا تكون متناسبة مع السبب [51].

3.3.2.3 التحديد وعدم القدرة على التنبؤ:

في السياق العلمي مفهوم التحديد يشير إلى القدرة على التنبؤ بالمستقبل استنادًا إلى حدوث حدث معين في الماضي أو الحاضر. ومع ذلك تشير الظواهر الفوضوية إلى التغيرات غير المنتظمة في سلوك النظام، وتعود هذه التغيرات غالبًا إلى الخصائص غير الخطية. في حالة الظواهر العشوائية من الصعب تمامًا توقع مسار النظام الذي يظهر تأثيرًا عشوائيًا، سواء كان هذا التأثير مشددًا أو غير ذلك دون الاعتماد على قوانين رياضية تم تطويرها بدقة وبطريقة غير قابلة للتنبؤ. وهذا يعكس فكرة أن الظواهر العشوائية لا تتبع نمطًا محددًا أو قوانين ثابتة، مما يجعل من الصعب جدًا إنشاء نموذج دقيق لها. لذلك في عالم الفوضى والظواهر العشوائية قد يكون التنبؤ بالمستقبل أمرًا صعبًا جدًا أو حتى مستحيلًا بشكل كامل، وذلك بسبب طبيعة العشوائية وعدم قدرة القوانين الرياضية على تمثيلها بدقة [51].

4.3.2.3 الانتظامية

الانتظامية (Ergodicity) هي خاصية في الأنظمة الاحتمالية والمتغيرات العشوائية، التي تعني أن النظام يسير في فضاء حالاته بشكل اعتباطي ولكنه يقترب من المراحل السابقة له. بمعنى آخر، إن النظام يكون مستقلًا

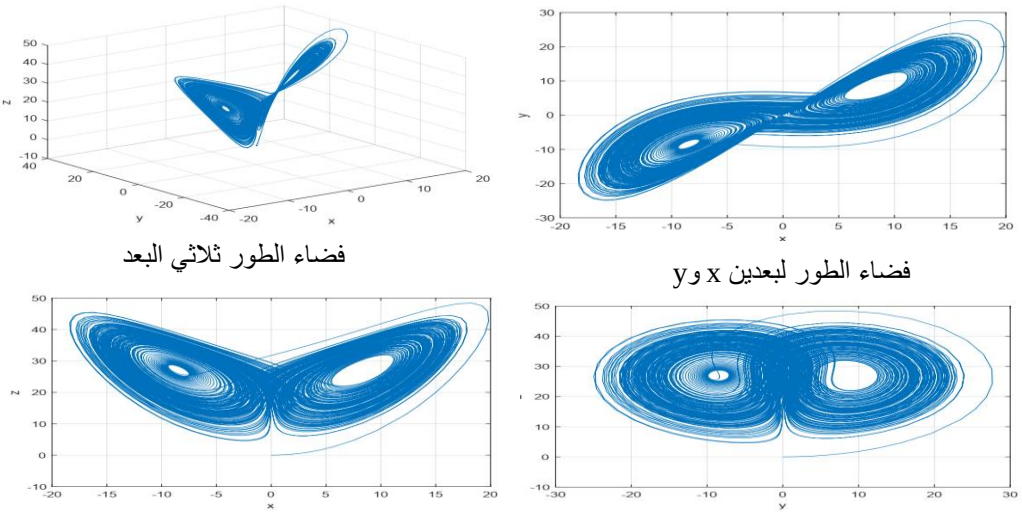
عن الظروف الابتدائية وغير قابل للتكهن به، إلا أن كثافة القيم تكون ثابتة في وقت محدد. هذه الخاصية تلعب دورًا مهمًا في مجال التشفير [52].

5.3.2.3 الجانب العشوائي

على الرغم من أن الأنظمة الفوضوية هي نظم محددة، فإن جميع حالات النظام الفوضوي تظهر جوانب عشوائية. على سبيل المثال من الصعب التنبؤ بدقة بالطقس في المستقبل، لأن النظام المناخي هو نظام فوضوي. كما أنه من الصعب التنبؤ بسلوك الأسواق المالية، لأن النظام الاقتصادي هو أيضًا نظام فوضوي.

6.3.2.3 الجاذب الغريب

الجاذب الغريب (Strange attractors)، عندما بدأ إدوارد لورنز في رسم حلاً لنظامه باستخدام حاسوبه، حيث قام برسم منحنيين باستخدام مجموعتين من الظروف الابتدائية قريبة جدًا، كان يتوقع أن تتباعد المنحنيات، ولكن كانت المنحنيات الاثنتين تشبه إلى حد كبير جناحي فراشة [49].



الشكل 2.3: جاذب غريب لنظام لورنز

يمثل الشكل (2.3) جاذب غريب لنظام لورنز حيث يظهر شكل الفراشة في فضاء الطور x و z، ونلاحظ ان الجاذب الغريب له بنية معقدة.

7.3.2.3 معاملات ليابونوف

ثوابت ليابونوف (Lyapunov Exponent) هي أداة تمكن من قياس التباعد بين المدارات التي تنشأ من شروط ابتدائية متجاورة. حيث تسمح بتأكيد الحساسية للشروط الابتدائية لنظام فوضوي وكذلك التعقيد ونميز حالتين.

✓ **حالة الأنظمة المستمرة**

في حالة الأنظمة المستمرة، تُعرَّف معاملات ليابونوف على النحو التالي:

$$\lambda_i = \lim_{t\to\infty} \frac{1}{t} \ln\left(\frac{|\partial x(t)|}{|\partial x(0)|}\right) \qquad (2.3)$$

حيث:

- λ_i هو ثابت ليابونوف للأبعاد i.
- $\partial x(t)$ تمثل التغيير في حالة النظام في الزمن t .
- $\partial x(0)$ تمثل التغيير في حالة النظام في الزمن الابتدائي $t = 0$.

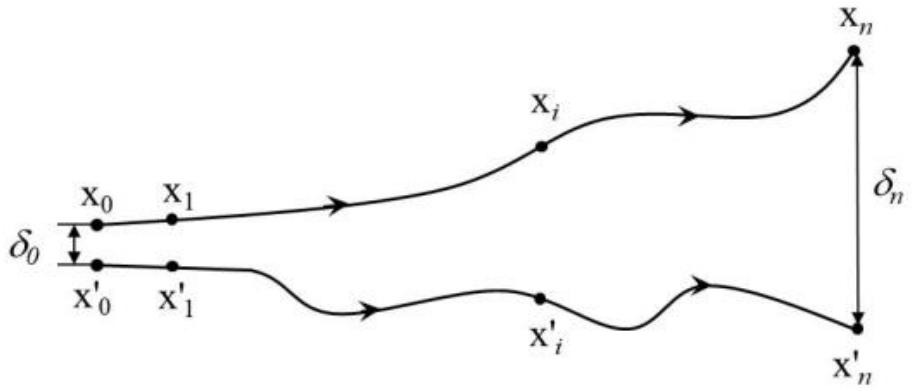
✓ **حالة الأنظمة المتقطعة**

في حالة الأنظمة المتقطعة، يمكن تعريف معاملات ليابونوف على النحو التالي:

$$\lambda = \lim_{k\to\infty} \lim_{\varepsilon\to 0} \frac{1}{k} \ln\left(\frac{|\partial x_k|}{|\partial x_0|}\right) \qquad (3.3)$$

حيث:

- λ هو ثابت ليابونوف.
- ∂x_k هو التغيير في حالة النظام بعد التكرار k .
- ∂x_0 هو التغيير في حالة النظام في البداية $k = 0$.



الشكل 3.3: معاملات ليابونوف

يمثل الشكل (3.3) معاملات ليابونوف عن طريق تبع مداران $\{x_0, x_1, \ldots, x_i, \ldots, x_n\}$ و $\{x'_0, x'_1, \ldots, x'_i, \ldots, x'_n\}$ يتطوران، مع ظروف ابتدائية x_0 و x'_0 متباعدين δ_0.

الجدول 1.3: حالة الأنظمة بدلالة معامل ليابونوف

الوضع	معامل ليابونوف (Lyapunov)
ثابت	$\lambda_n \leq \cdots \leq \lambda_1 \leq 0$
دوري	$\lambda_1 = 0$ $\lambda_n \leq \cdots \leq \lambda_2 \leq 0$
دوري من الدرجة الثانية	$\lambda_1 = \lambda_2 = 0$ $\lambda_n \leq \cdots \leq \lambda_3 \leq 0$
دوري من الدرجة K	$\lambda_1 = \cdots = \lambda_k = 0$ $\lambda_n \leq \cdots \leq \lambda_{k+1} \leq 0$
فوضوي	$\lambda_1 \succ 0$ $\sum_{i=1}^{n} \lambda_i \prec 0$

يوضح الجدول (1.3) حالة الأنظمة بدلالة معامل ليابونوف حيث نلاحظ انه عندما يكون λ_1 أكبر من الصفر يكون النظام فوضويا.

✓ **مخطط التفرع**

مخطط التفرع (The bifurcation diagram) هو تمثيل بياني يساعد على تقييم بسرعة مجموع الحلول الممكنة لنظام واستقرارها بناءً على تغيرات في أحد معلميه. يساعد أيضًا في تحديد القيم الخاصة للمعلم التي تؤدي إلى حدوث تفرعات. يعرض هذا المخطط فترات حيث تتطور الحلول اللاحقة بشكل مستمر مع المعلم، ويُصنف قيم المعلم على طول محور الفواصل وقيم إحدى متغيرات الحالة على محور التراتيب [53].

8.3.2.3 الفرق بين الفوضى والعشوائية

يعتبر الفرق بين الفوضى والعشوائية نقطة مهمة جدًا في فهم الفوضى. في الواقع يميل الناس دائمًا إلى الاعتقاد بأن الظاهرة تصبح غير قابلة للتنبؤ بسبب العدد الكبير جدًا من المتغيرات المشاركة في وصفها. وهذا ما يدفعنا إلى تبني نهج احتمالي، لكنه يحتفظ بدرجة معينة من العشوائية بالتعريف.

ومع ذلك فيما يتعلق بالفوضى، فإن الأمر ليس كذلك حيث تتصرف الأنظمة الفوضوية، في الواقع بطريقة قد تبدو عشوائية. ولكن هذا السلوك يُوصف في الحقيقة بشكل قاطع من خلال معادلات غير خطية محدد تمامًا، أي بشكل خاص باستخدام أدوات رياضية تسمح بنهج دقيق ومحدد.

4.2.3 أمثلة على الأنظمة الفوضوية

تنقسم الأنظمة الفوضوية الى نوعين حسب قاعدة الزمن هما:

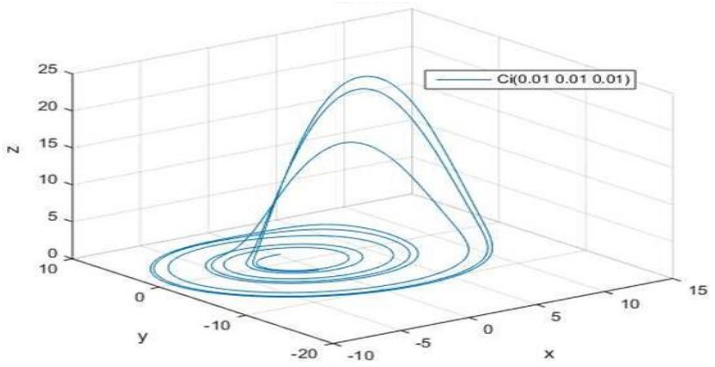
1.4.2.3 الأنظمة الفوضوية في الزمن المستمر

هي الأنظمة التي تكون مستمرة مع الأنظمة الفوضوية في الزمن المستمر هي الأنظمة التي تتغير باستمرار بمرور الوقت وتظهر سلوكًا غير قابل للتنبؤ، مما يجعلها حساسة جداً للظروف الابتدائية. من الأمثلة على ذلك نظام لورينز، ونظام روسلر، والتي تُظهر ديناميكيات معقدة وفوضوية.

✓ **نظام روسلر**

نظام روسلر (Rossler system) اقترحه العالم الألماني أوتو روسلر، مرتبط بدراسة تدفق السوائل وينبثق من معادلات نافير–ستوكس. تم اكتشاف معادلات هذا النظام على إثر الأبحاث في الحركية الكيميائية. تتمثل معادلات هذا النظام في:

$$\begin{cases} \dfrac{dx}{dt} = \dot{x} = -1(y+z) \\ \dfrac{dy}{dt} = \dot{y} = x - ay \\ \dfrac{dz}{dt} = \dot{z} = b + z(x-c) \end{cases} \qquad (4.3)$$



الشكل 04.3: جاذب غريب لنظام روسلر

يوضح الشكل (4.3) رسم الجاذب الغريب لنظام Rössler، حيث تم تثبيت قيم المعاملات على القيم $(a = 0.2 \text{ ,b=0.2 ,c=5.7})$، وبشروط ابتدائية $x_0 = (0.2 \text{ ; } 2 \text{ ;1})$.

2.4.2.3 أمثلة على الأنظمة الفوضوية في الزمن المتقطع

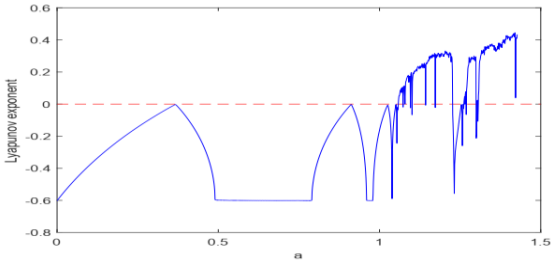
هي الأنظمة غير المستمرة وعلى سبيل المثال نظام هينو والخرائط الفوضوية:

✓ **نظام هينون**

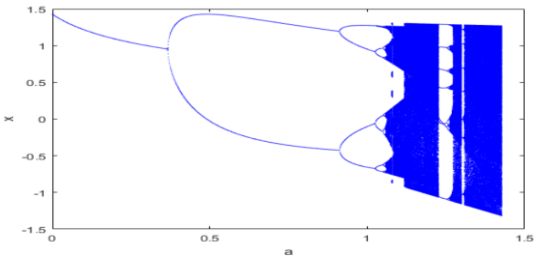
نظام هينون (Henon System) هو نظام ديناميكي ذو تكرار زمني مقترح من قبل عالم الفلك ميشيل هينون في عام 1976. ويُمثل هذا التكرار بواسطة المعادلات التالية:

$$\begin{cases} x_{n+1} = y_n + 1 - ax_n^2 \\ y_{n+1} = b_n x_n \end{cases} \quad (5.3)$$

حيث x_{n+1} و y_{n+1} هما المتغيران في الخطوة $n+1$ و x_n و y_n هما المتغيران في الخطوة n. القيم a و b هي معاملات قابلة للتغيير مما يعني أنها يمكن أن تختلف بتغيير مع كل خطوة.



الشكل6.3: معاملات ليابونوف



الشكل 0.53: مخطط التفرع

يمثل الشكل (5.3) مخطط التفرع لنظام هينون عند تثبيت القيمة b=0.3 و تغيير قيمة a في المجال [0,1.5] كما يمثل الشكل (6.3) معاملات ليابونوف مع نفس القيم ل a و b.

5.2.3 الخرائط الفوضوية

من بين العديد من الخرائط الفوضوية نعرض بإيجاز أدناه معادلات ثلاث خرائط فوضوية تُستخدم على نطاق واسع في الممارسة العملية، وهي: الخريطة اللوجستية، خريطة أرنولد، والخريطة الجيبية. تتمتع هذه الخرائط بعدة خصائص، منها سهولة التنفيذ، وغالبًا ما تتميز بخصائص تشفير جيدة [54].

1.5.2.3 الخريطة اللوجستية

الخريطة اللوجستية (Logistic map) هي خريطة بسيطة، حيث أنها غير خطية وهي معرفة بالعلاقة التالية:

$$x_{i+1} = rx_i(1 - x_i) \quad (6.3)$$

حيث:

- ✓ x هي المتغيرة الديناميكية التي تأخذ قيمًا بين 0 و1 (باستثناء 1)
- ✓ r هو معامل النظام.

ووفقًا لقيمة r، يمكن أن تكون السلسلة نقطة ثابتة أو سلسلة دورية بفترات 2، 4، 8، وهكذا حتى 64 عند r=3.569682، أو سلسلة فوضوية عندما يكون r في النطاق 3.56996 و4.

2.5.2.3 خريطة أرنولد

خريطة أرنولد (Arnold map) خريطة فوضوية تأخذ اسمها تكريمًا للرياضي الروسي فلاديمير أرنولد، الذي اكتشفها باستخدام صورة لقطة (ACM) . حيث هي عرض بسيط وأنيق لبعض مبادئ الفوضى، وهي تصف تطورًا يبدو عشوائيًا لنظام.

تُعد خريطة قطة أرنولد مثالًا نموذجيًا لخريطة فوضوية، وتُعبر عنها المعادلة التالية:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \times \begin{bmatrix} x_n \\ y_n \end{bmatrix} \quad \text{mod } n \qquad (9.3)$$

حيث:

- ✓ x_{n+1} و y_{n+1} هما مواقع البيكسل الجديدة.
- ✓ x, y هما المواقع الأصلية لهذا البيكسل.
- ✓ a, b قيم ومعاملات صحيحة إيجابية.

3.5.2.3 الخريطة الجيبية

الخريطة الجيبية (sine map) يتم تمثيلها بالمعادلة التالية:

$$x_{n+1} = F_s(r, x_n) = r \times \sin(\pi \times x_n) \qquad (10.3)$$

الخريطة الجيبية حقاً تكون فوضوية إذا كان $r \in [0,1]$.

3.3 التشفير الفوضوي

يعتبر التشفير الفوضوي أحد البدائل التي تم تطويرها خلال العقد الأخير. حيث لا يلبي فقط متطلبات الأمان بل أثبت مقاومة كبيرة للتحليل التشفيري، حيث يتماشى بشكل مثالي مع الصفات اللازمة لخوارزميات التشفير. ومن المعروف أن هناك نوعين من الوظائف الفوضوية، أولهما تلك التي لديها سلوك فوضوي بحت والتي لا يمكن تصنيفها، والثانية هي الوظائف الفوضوية التي يمكن تصنيفها بواسطة أنظمة المعادلات المعروفة باسم "الأنظمة الديناميكية غير الخطية"، وهذه الأخيرة هي تلك التي تستخدم في التشفير الفوضوي حيث يكون جاذبها على شكل تكتلات، وتجعل تطور المسارات معتمدًا بالكامل على الظروف الابتدائية، وبالتالي لا يمكن التنبؤ بتلك المسارات دون معرفة حالتها الابتدائية، مما يجعل السلوك الفوضوي غير قابل للتنبؤ وأمانها يقترب من الكمال. ولإدخالها في التشفير يجب أولاً اختيار دالة فوضوية، ثم يتعين تراكب الإشارة الفوضوية على تدفق البيانات المراد نقلها بناءً على إحدى التقنيات المختارة للتشفير بالفوضى.

1.3.3 تقنيات تشفير الفوضى

تنقسم تقنيات التشفير الفوضوي الى قسمين هما:

1.1.3.3 تشفير الفوضى التماثلي

في إطار نقل المعلومات بشكل مشفر باستخدام الفوضى التماثلية، يتم تشفير إشارة سرية باستخدام إشارة فوضوية وفقًا لوظيفة معينة. الإشارة التي تم إنتاجها والتي تحتوي على الرسالة السرية، يتم نقلها مباشرة إلى المستقبل عبر قناة عامة.

تكمن صعوبة هذه الطريقة بالكامل في فك التشفير. في الواقع أثناء انتشار الإشارة عبر بيئة مضطربة، هناك احتمالية لتشويشها وتدميرها، في هذه الظروف يشكل استعادة الإشارة المعلوماتية تحديًا حقيقيًا بسبب الحساسية الكبيرة لأنظمة الفوضى تجاه التغيرات، ويصبح تطبيق آلية المزامنة ضروريًا لاستخراج المعلومات الواردة.

2.1.3.3 تشفير الفوضى الرقمية

تحفّز الثغرات الناتجة عن تقنيات التشفير بالفوضى التماثلية توسيع نطاق التشفير الفوضوي إلى مجال الإشارات الرقمية بالكامل، بهدف خلق جيل جديد من التشفير بالفوضى يعتمد على آليات التزامن الرقمية المستقلة.

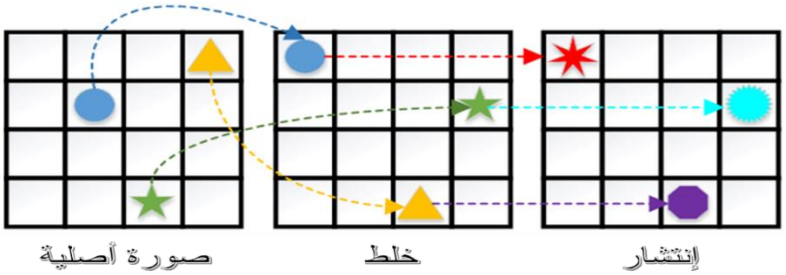
الفائدة الرئيسية لترقية الإشارات الفوضوية إلى النطاق الرقمي:

- ✓ إمكانية إنشاء تسلسلات رقمية بشكل أسهل وقابل للتكرار، وكذلك التحكم الفعّال في خصائصها الطبيعية.
- ✓ البدء الفعّال لأنظمة الفوضى دون الاهتمام بمشاكل المزامنة بين المرسل والمستقبل.
- ✓ تحويل الإشارات الفوضوية إلى نظام ثنائي ينطوي على استخدام دقة محددة (32 بت أو 64 بت)، مما يبسط التنفيذ ويزيد من أداء التشفير وفك التشفير.
- ✓ آليات فعّالة لتنفيذ ومراقبة الأنظمة الفوضوية على مستوى الحواسيب الرقمية، مما يقضي على تأثيرات التشويش الناجمة عن التغييرات القياسية.
- ✓ إمكانية استخدام الظروف الابتدائية والمعاملات كمفاتيح سرية بأحجام مناسبة.

نظرًا لأن هذه الفئة من تقنيات التشفير بالفوضى مستوحاة بشكل كبير من التشفير التماثلي، فإن مبدأها الأساسي يتمثل في بناء تحولات ثنائية الاتجاه بالنسبة للظروف الابتدائية والمعلومات التحكمية للأنظمة الفوضوية المستخدمة، وفقًا للمفهومين الإثنين التي صاغها شانون في إطار نظرية المعلومات:

الخلط: يستخدم لإخفاء العلاقة بين النص الواضح والنص المشفر من خلال مفتاح سري. الطريقة الأكثر شيوعًا لتطبيق الخلط هي الاستبدال، غالبًا ما تكون غير خطية مثلما هو الحال في خوارزمية AES (معيار التشفير المتقدم).

الانتشار: يستخدم للقضاء على التكرارات في الرسالة السرية ونشر تأثير تغيير بت واحد في المفتاح أو النص الواضح على كل النص المشفر المتعلق به. يتم تحقيق الانتشار عادةً من خلال عملية الاستبدال أو عملية التبديل.



الشكل 7.3: الخلط والانتشار في الصورة

2.3.3 الخريطة اللوجستية ثنائية الأبعاد

الخريطة اللوجستية ثنائية الأبعاد (The Two-dimensional Logistic Map) لديها سلوكات فوضوية أكثر تعقيدًا من الخريطة اللوجستية أحادية البعد.

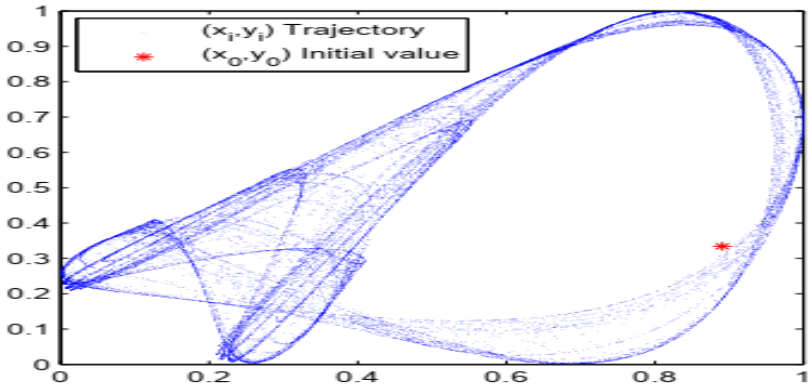
1.2.3.3 التعريف الرياضي

يمكن تعريف الخريطة اللوجستية ثنائية الأبعاد رياضيًا بشكل منفصل كما هو موضح في المعادلة (11.3)، حيث يمثل r معامل النظام و (x_i, y_i) هما قيم النظام عند النقطة i .

خريطة لوجستية ثنائية الأبعاد

$$\begin{cases} x_{i+1} = r(3y_i + 1)x_i(1 - x_i) \\ y_{i+1} = r(3x_{i+1} + 1)y_i(1 - y_i) \end{cases} \quad (11.3)$$

$$\begin{cases} x_i = L_x^{2D}(x_0, y_0, r, i) \\ y_i = L_y^{2D}(x_0, y_0, r, i) \end{cases} \quad (12.3)$$



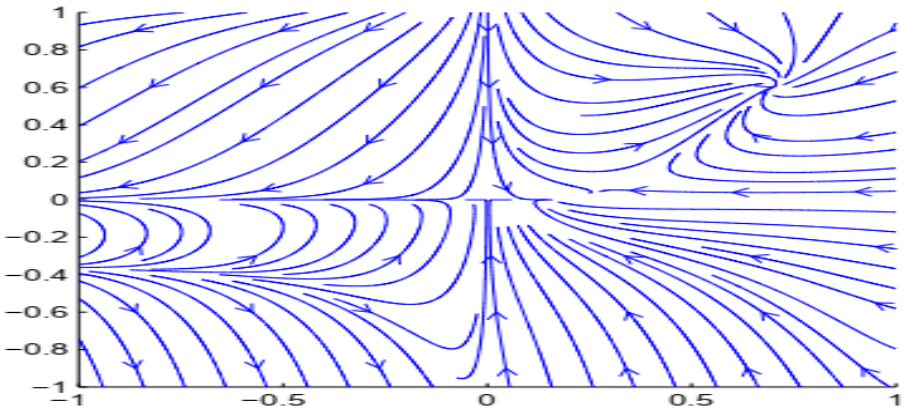
الشكل 08.3: مسار الخريطة اللوجستية ثنائية الأبعاد

حيث يظهر في الشكل (8.3) الرسم البياني 30,000 نقطة من المسار الناتج للخريطة اللوجستية ثنائية الأبعاد باستخدام معامل النظام r = 1 .19 والقيم الابتدائية (x_0, y_0) عند $(0.8909, 0.3342)$.

2.2.3.3 الرسم البياني للطور والسلوكات الفوضوية

الرسم البياني للطور والسلوكات الفوضوية (Phase Portrait and Chaotic Behaviors)، الخريطة اللوجستية ثنائية الأبعاد المعرفة في المعادلة (11.3) هي نظام ديناميكي معقد وفقًا لقيمة معامل النظام r، حيث تتطور الخريطة من نوع واحد من الديناميكيات إلى آخر. وبشكل أكثر تحديدًا يمكن تلخيص سلوكات الخريطة على النحو التالي [55]:

- ✓ عندما تكون قيمة r في المجال $(-1, 1)$، يحتوي النظام على نقطة جاذبة واحدة ونقطتي سرج (النقطة الجاذبة هي النقطة التي يتجمع حولها النظام، نقطة السرج تشير إلى نقطة في النظام الديناميكي حيث يحدث تغير منتظم بين حالتين مختلفتين أو بين مجموعتين من السلوك الديناميكي)، ويجعل كل من المحاور x وy منحنيات غير مستقرة.
- ✓ عندما تساوي قيمة $r = 1$، تتعرض النقطة المركزية الجاذبة لانقسام نيمارك–هوبف [56].
- ✓ عندما تكون قيمة r في المجال $(1.11, 1.19)$، يحدث تناوب بين وجود منحنى مغلق ثابت مع التذبذبات، والسلوكات الفوضوية الدورية.
- ✓ عندما تكون قيمة r أكبر من 1.19 يصبح النظام غير مستقر.

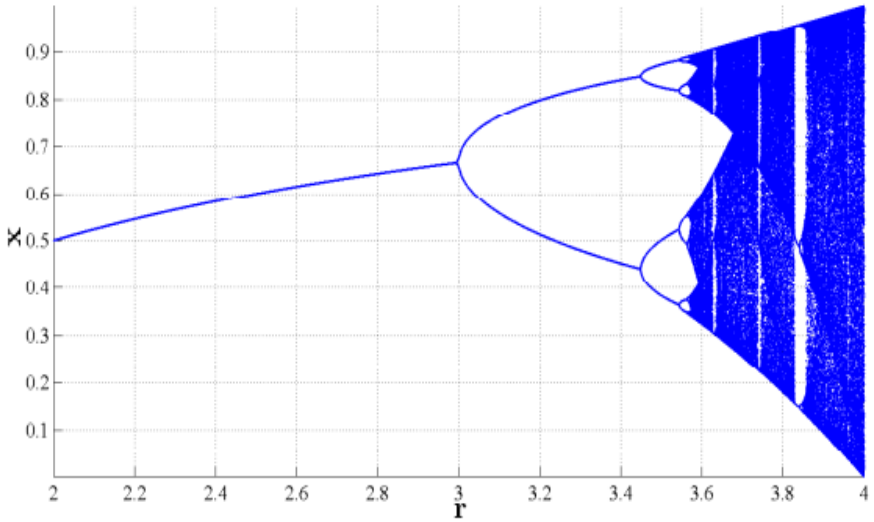


الشكل9.3: الرسم البياني لطور لخريطة لوجستية ثنائية الأبعاد

يظهر الشكل (9.3) الرسم البياني للطور الخاص بالخريطة اللوجستية ثنائية الأبعاد عندما تساوي قيمة r=1.19، ومن الملاحظ أن هذا الرسم البياني يتطابق مع الوصف الرياضي للخريطة اللوجستية ثنائية الأبعاد عندما تساوي قيمة r=1.19. نظرًا لأن مسار (x,y) يشبه العشوائية ولكنه قابل للتنبؤ تمامًا عندما يتم معرفة كل من r و (x_0,y_0)، ومنه يمكن استخدامه كمولد لأرقام شبه عشوائية للتشفير. حيث x و y يمثلان القيمتين المتتاليتين للسلسلة الزمنية للنظام. والأسهم تشير الى الاتجاه الذي يتطور فيه النظام بمرور الزمن، والنقاط التي تتجمع حولها الأسهم تمثل نقاط السرج (الحرجة).

3.2.3.3 التعقيد

التعقيد (Complexity)، تتمتع الخريطة اللوجستية ثنائية الأبعاد المُعرّفة في المعادلة (11.3) بتعقيد أعلى مقارنة بالخريطة اللوجستية التقليدية أحادية البعد المُعرّفة في المعادلة (6.3)، حيث يعتبر المعامل r المتحكم في السلوك الفوضوي. يظهر الشكل (10.3) مخطط التفرع لخريطة لوجستية أحادية البُعد، حيث يُعبر المحور الأفقي عن معامل النظام "r" والمحور العمودي عن "x"، ويتم رسم كل مسار لخريطة لوجستية أحادية البُعد حول "x" مع قيمة ثابتة لـ "x" كنقاط على الشكل.



الشكل 10.3: مخطط التفرع للخريطة اللوجستية أحادية البعد

يمكن قياس تعقيدات الخرائط اللوجستية أحادية وثنائية البعد وخريطة هينون باستخدام وسائل مختلفة ملخصة في الجدول:

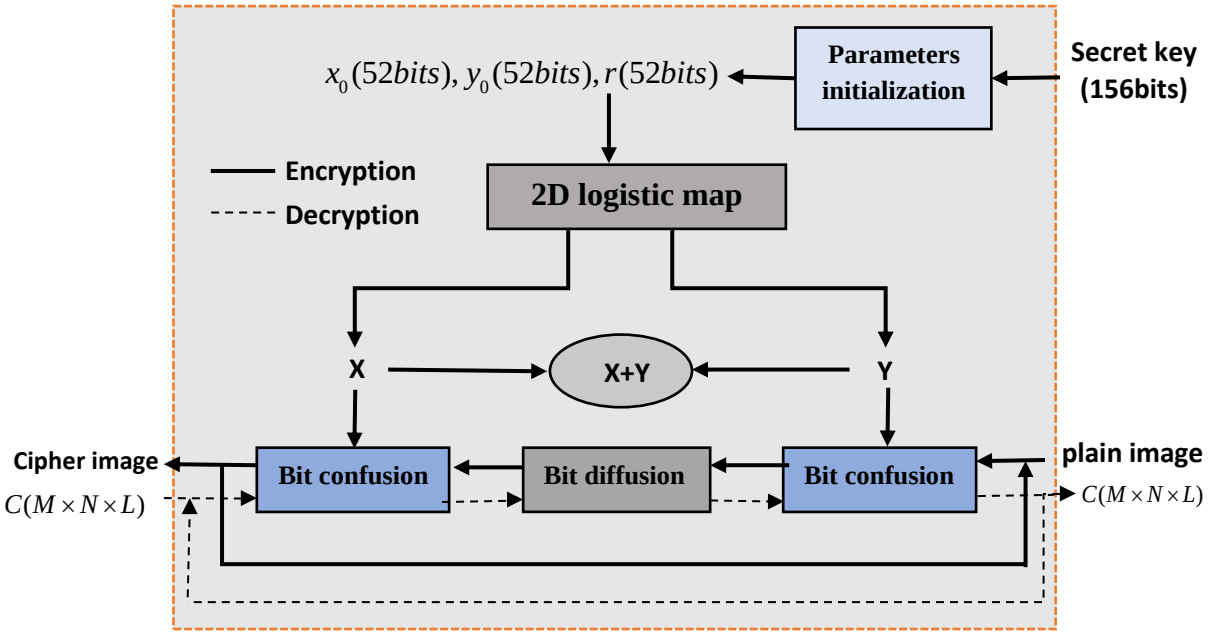
الجدول 2.3: تحليل تعقيد الأنظمة الفوضوية [57]

		خريطة لوجيستية أحادية البعد		خريطة هينو		خريطة لوجيستية ثنائية البعد			
		4 نهاية الفوضى	3.57 بداية الفوضى	(1.40 , 0.3) الفوضى		1.19 نهاية الفوضى		1.11 بداية الفوضى	
إنتروبيا المعلومات	Bins	H(x)	H(x)	H(x)	H(y)	H(x)	H(y)	H(x)	H(y)
	256	7.689	4.811	7.815	7.8155	7.894	7.893	6.260	6.554
	512	8.677	5.273	8.804	8.804	8.890	8.890	7.185	7.455
معامل ليابونوف		0.069	0.001	0.424	-1.628	0.565	-0.21	0.364	-0.116

يظهر الجدول (2.3) مقارنة التعقيدات بين هذه الخرائط الفوضوية باستخدام إنتروبيا المعلومات ومعامل ليابونوف بالنسبة لأزواج مختلفة من القيم الابتدائية. كما هو موضح في الجدول فالخريطة اللوجستية ثنائية البعد تحتوي على إنتروبيا المعلومات أعلى من الخريطة اللوجستية أحادية البُعد، مما يعني أن مسارها يشبه العشوائية أكثر. في الوقت نفسه لدى الخريطة اللوجستية ثنائية البعد أيضًا معامل ليابونوف أكبر من الخريطة اللوجستية التقليدية، مما يعني أن الأولى أكثر ديناميكية.

4.3 تشفير الصور باستخدام الخريطة اللوجستية ثنائية الأبعاد

الخريطة اللوجستية ثنائية الأبعاد تُستخدم لتشفير الصور من خلال الاستفادة من خصائصها الفوضوية في مجال معين. نركز على المجال $r \in [1.1, 1.19]$، حيث يكون النظام فوضويًا كما تم الذكر سابقًا. في هذا المجال، تكون القيم الناتجة حساسة جداً للظروف الابتدائية، مما يعزز تعقيد وصعوبة فك التشفير دون معرفة المفتاح الصحيح. يتم تشفير كل بكسل في الصورة بشكل مختلف، مما يضمن توزيع البيانات بشكل عشوائي ويصعب التنبؤ بها. هذه الفوضى تجعل من الصعب على المهاجمين إعادة بناء الصورة الأصلية أو استنتاج أي نمط يمكن استخدامه لفك التشفير، مما يوفر أمانًا عاليًا للصور المشفرة.



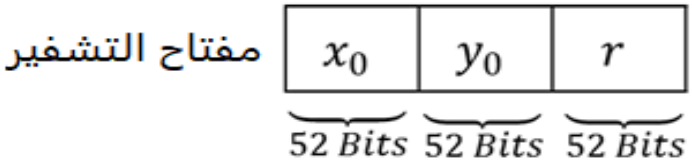
الشكل11.3: الرسم التخطيطي لطريقة تشفير الصور المقترحة

يُظهر الشكل (11.3) الرسم التخطيطي لطريقة تشفير الصور المقترحة باستخدام الخريطة اللوجستية ثنائية الأبعاد. والحلقة الداخلية مكونة من الخلط وبعده الانتشار، ثم الخلط حيث كل مرحلة منها هي بمثابة شفرة لصورة وتشكل معًا الشبكة الخلط – الانتشار. يتم مناقشة تفاصيل هذه المراحل في القسم التالي. على غرار إجراءات التشفير، فإن إجراءات فك التشفير ليست سوى عكس ترتيب المعالجة باستخدام مفتاح فك التشفير كما يظهر في الشكل (14.3). باختصار يمكن كتابة عملية التشفير على النحو التالي $C = Enc(P,K)$، وعملية فك التشفير هي $P = Dec(C,K)$.

1.4.3 جدول المفتاح ومولد تسلسل الخريطة اللوجستية ثنائية الأبعاد

جدول المفتاح ومولد تسلسل الخريطة اللوجستية ثنائية الأبعاد (Key Schedule and 2D Logistic Sequence Generator) نحدد مفتاح التشفير K الخاص بنا كسلسلة بت بطول 156 بت تتألف من ثلاثة أجزاء x_0 ، y_0 و r، كما هو موضح في الخوارزمية التالية حيث (x_0, y_0) هما القيمة الابتدائية للنظام و r معامل النظام.

$$\begin{aligned} &Key(1) = k(1) \oplus k(156) \\ &For\ i = 2:156 \\ &Key(i) = key(i-1) \oplus k(i) \\ &end \end{aligned} \qquad (13.3)$$



الشكل12.3: مفتاح التشفير(Key)

حيث نقوم بتحديد قيم (x_0, y_0, r) باستعمال دقة IEEE 754 كما هو موضح في المعادلة التالية:

$$\upsilon = \sum_{i=1}^{52} b_{-i} 2^{-i} \tag{14.3}$$

$$\begin{aligned} x_0 &= 0.8909 + 0.1 \times \upsilon(1) ; \\ y_0 &= 0.3342 + 0.1 \times \upsilon(2) ; \\ r &= 1.19 - 0.1 \times \upsilon(3) ; \end{aligned} \tag{15.3}$$

2.4.3 الخلط والانتشار

الخلط والانتشار (Diffusion and confusion) الهدف من خطوة الخلط هو تقليل الارتباط العالي بين وحدات البكسل المتجاورة في الصورة الأصلية. حيث يعد الانتشار خاصية مهمة قدمها شانون في التشفير. يجب أن يضمن نظام التشفير انتشارًا أفضل، حيث إذا تم تغيير بت واحد في صورة النص العادي، فيجب أن تتغير صورة النص المشفر بالكامل [24].

تتم الإشارة إلى الصورة الأصلية المراد تشفيرها بواسطة(P (M × N × L، حيث:

- M وN : تمثلان الارتفاع.
- P : تمثل العرض.
- L : تمثل مكونات اللون الأحمر والأخضر والأزرق للصورة الملونة.

يتم تحويل P إلى متجه(شعاع) ثنائي P_{Bin} من K بت، حيث:

$$K = \begin{cases} M.N.L & \text{if P is logical} \\ M.N.L.8 & \text{otherwise} \end{cases} \tag{16.3}$$

بعد ذلك يتم توليد التسلسلين الفوضويين $X=\{x_1,x_2,\ldots,x_k\}$ و $Y=\{y_1,y_2,\ldots,y_k\}$ من المعاملات (x_0,y_0,r) باستخدام المعادلة (11.3).

يتم استخدام التسلسل الفوضوي Y للخلط الأول وفقا للمعادلات التالية:

$$[V(1,\ldots,K),W(1,\ldots,K)]=sort(Y(1,\ldots,K)) \quad (17.3)$$

$$P_{Conf}(1,\ldots,K)=P_{Bin}(W(1,\ldots,K)) \quad (18.3)$$

حيث V يمثل قيم السلسلة Y بعد ترتيبها ترتيبا تصاعديا او تنازليا، وW تمثل مواقع هذه القيم الابتدائية.
يكون الخلط حسب المعادلة (18.3) باستخدام الشعاع لنتحصل على الصورة المخلوطة P_{Conf} .

بعد الانتهاء من الخلط الأول، تأتي مرحلة الانتشار وهذا باستخدام مجموع السلسلتين X وY معا حسب المعادلة (19.3) للحصول على P_{Diff} .

$$Z(1,\ldots,K)=\left[\begin{pmatrix}X(K-D+1,\ldots,K)\\+\\Y(K-D+1,\ldots,K)\end{pmatrix}\times 10^{15}\right]\bmod m \quad (19.3)$$

$$\begin{cases}m=2 & \text{if P is logical}\\ m=256 & \text{otherwise}\end{cases}$$

$$\begin{aligned}&P_{Diff}(1)=P_{Conf}(1)\oplus P_{Conf}(K)\oplus Z_{Bin}(1)\\&for\ \text{i=2,…,K}\\&P_{Diff}(i)=P_{Conf}(i)\oplus P_{Conf}(i-1)\oplus Z_{Bin}(i)\\&end\end{aligned} \quad (20.3)$$

بعد عملية الانتشار نقوم بتطبيق الخلط الثاني على P_{Diff} للحصول C_{Bin} حسب المعادلات (21.3) و (22.3).

$$[H(1,\ldots,K),F(1,\ldots,K)]=sort(X(1,\ldots,K)) \quad (21.3)$$

$$C_{Bin}(1,\ldots,K)=P_{Diff}(F(1,\ldots,K)) \quad (22.3)$$

عند الانتهاء من عملية الخلط والانتشار نقوم بتحويل الشعاع الثنائي الى الصورة المشفرة C.

بالنسبة لطريقة فك التشفير الصورة المشفرة، فالعمليات المطبقة تبقى نفسها و لكن في الاتجاه المعاكس لعملية التشفير.

5.3 الخاتمة

في هذا الفصل، قمنا بعرض مقدمة تتناول علم الفوضى ونبذة تاريخية عن الأنظمة الفوضوية، ثم قمنا في بادئ الأمر بتعريف الأنظمة الفوضوية وذكر خصائصها، كما استعرضنا الفرق بين الفوضى والعشوائية والتطرق إلى أمثلة عن الأنظمة الفوضوية، وأيضا تطرقنا الى الخرائط الفوضوية والتشفير الفوضوي وتقنيات تشفير الفوضى، وفي نهاية الفصل تطرقنا إلى الخريطة اللوجستية ثنائية الأبعاد وتشفير الصور باستخدام الخريطة اللوجستية ثنائية الأبعاد. وسنركز في الفصل الرابع عن المحاكاة وتحليل النتائج والذي سنقوم فيه بتطبيق الخوارزمية في برنامج الماتلاب بعد ذلك قمنا بتحليل النتائج من جهة تحليل الهيستوغرام ومعامل الارتباط والانتروبيا وتحليل مساحة وحساسية المفتاح.

الفصل الرابع

المحاكاة والنتائج

1.4 مقدمة

يجب على طريقة تشفير الصور الجيدة أن تقاوم جميع أنواع الهجمات المعروفة وأن تكون جودة التشفير لا تعتمد على النص الأصلي أو المفتاح. في نهاية المطاف يجب أن تكون طريقة تشفير الصور الجيدة قادرة على تشفير أي صورة نصية إلى نص مشفر يشبه العشوائية إذا افتُرض استخدام المفتاح بشكل موحد.

في هذا الفصل، سنتطرق إلى محاكاة طريقة تشفير الصور باستخدام خريطة اللوجستية ثنائية الأبعاد المذكورة في الفصل السابق، سنقدم أيضًا نتائج قياسات أداء الخوارزمية، وسيتم عرض اختبارات التقييم لإظهار جودة طريقة التشفير.

2.4 لغة البرمجة المستعملة

نستعمل في تطبيق الخوارزمية برنامج الماطلاب MATLAB.

1.2.4 تعريف الماطلاب

MATLAB (« مختبر المصفوفات ») هو لغة برمجة من الجيل الرابع وبيئة تطوير، يستخدم لأغراض الحوسبة الرقمية. تم تطوير MATLAB من قبل شركة "The Math Works"، يسمح بالتلاعب حسابياً بالمصفوفات وعرض المنحنيات والبيانات وتنفيذ الخوارزميات وإنشاء واجهات المستخدم، ويمكن أن يتفاعل مع لغات أخرى مثل C، C++، Java وFortran. يأتي مستخدمو MATLAB من خلفيات مختلفة مثل الهندسة والعلوم والاقتصاد في سياق صناعي وبحثي، حيث بلغ عدد المستخدمين حوالي 4.1 مليون مستخدم في عام 2022. يمكن استخدام MATLAB بمفرده أو مع حزم الأدوات.

يتم بناء البرنامج حول لغة MATLAB. توفر واجهة سطر الأوامر والتي تعتبر واحدة من عناصر سطح المكتب في MATLAB، تساهم في إمكانية تنفيذ أوامر بسيطة. يمكن حفظ تسلسلات الأوامر في ملف نصي شكل "سكربت" أو يمكن تضمينها في دالة.

تمت محاكاة طريقة تشفير الصور باستخدام برنامج MATLAB R2020a، تحت بيئة Windows11، وذلك باستخدام معالج Core i5 من الجيل الحادي عشر بسرعة 2.9 جيجا هرتز وذاكرة بسعة 16 جيجابايت.

3.4 تحليل نتائج المحاكاة

لتقييم أداء الخوارزمية المطبقة ندرس القياسات التالية:

1.3.4 وقت التنفيذ

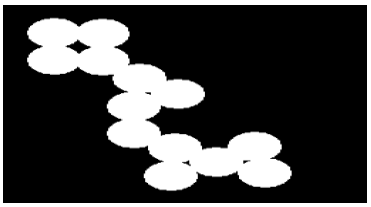
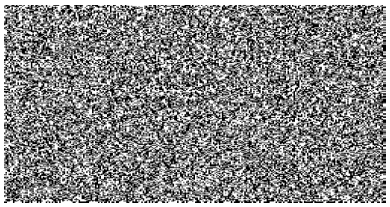
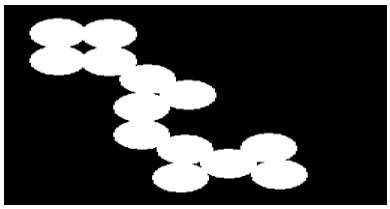
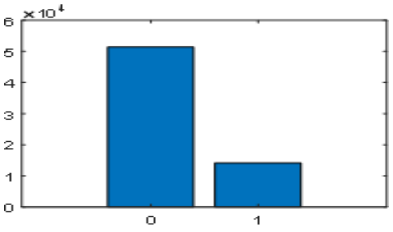
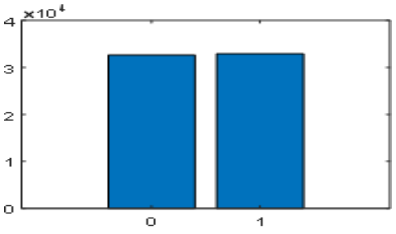
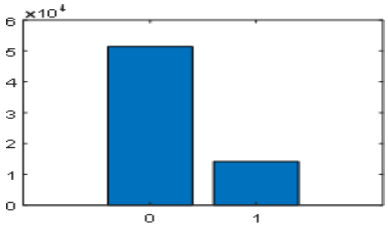
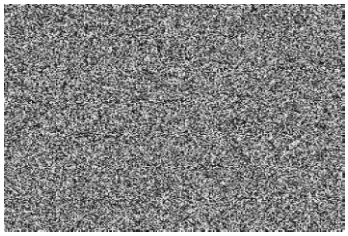
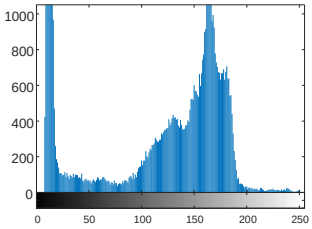
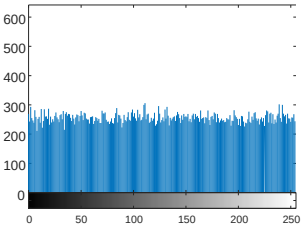
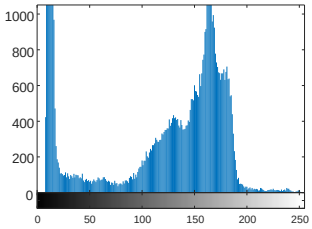
يمثل الجدول (1.4) حجم كل صورة تم استخدامها في محاكاتنا بالإضافة إلى وقت تشفير الصورة وفك تشفيرها. يمكن ملاحظة أن الوقت اللازم لتشفير الصورة وفك تشفيرها يتعلق بحجم الصورة وأنّ قيمته صغيرة جدّا وبالتالي طريقة التشفير ليست مكلفة من حيث وقت التنفيذ.

الجدول 1.4: حجم الصور ووقت محاكاتها

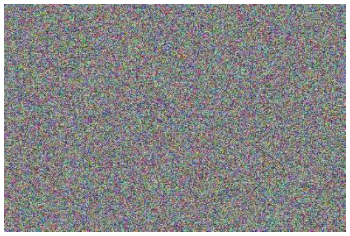
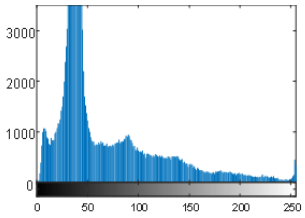
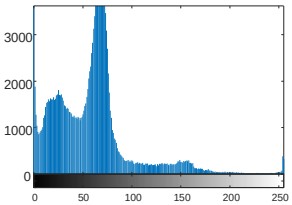
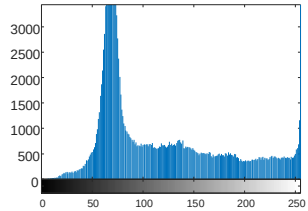
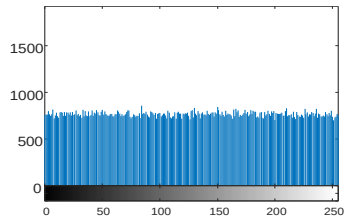
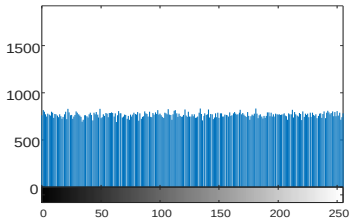
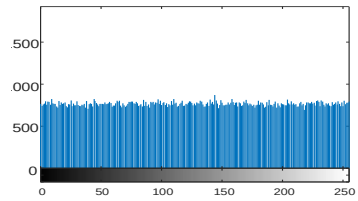
نوع الصورة	بعد الصورة $(M \times N)$	زمن التشفير (الثانية)	زمن فك التشفير (الثانية)
ثنائية	256×256	0.048831	0.046610
رمادية	256×256	0.375834	0.350711
ملونة	384×512	3.450903	3.404213

2.3.4 تحليل هيستوغرام

تحليل هيستوغرام الصورة المشفرة هو واحد من أكثر الطرق لتوضيح جودة تشفير الصورة. نظرًا لأن طريقة التشفير الجيدة تميل إلى تشفير صورة معينة إلى شكل عشوائي، فمن المرغوب رؤية هيستوغرام منتشر بشكل متساوٍ للصورة المشفرة. يوضح الشكل (1.4) و (2.4) هيستوغرامات الصور الأصلية والصور المشفرة.

الصورة بعد فك التشفير	الصورة المشفرة	الصورة الاصلية
		
هيستوغرام الصورة المشفرة	هيستوغرام الصورة بعد فك التشفير	هيستوغرام الصورة الاصلية
		
الصورة بعد فك التشفير	الصورة المشفرة	الصورة الأصلية
		
هيستوغرام الصورة بعد فك التشفير	هيستوغرام الصورة المشفرة	هيستوغرام الصورة الأصلية
		

الشكل 1.4: تحليل الهيستوغرام للصور الثنائية و الرمادية

الصورة بعد فك التشفير	الصورة المشفرة	الصورة الأصلية
		
هيستوغرام الصورة الأصلية للون الأزرق	هيستوغرام الصورة الأصلية للون الأخضر	هيستوغرام الصورة الأصلية للون الأحمر
		
هيستوغرام الصورة المشفرة للون الأزرق	هيستوغرام الصورة المشفرة للون الأخضر	هيستوغرام الصورة المشفرة للون الأحمر
		

الشكل 2.4: تحليل الهيستوغرام للصورة الملونة

واضح من هذه النتائج أنه على الرغم من أن بعض الصور النصية لها هيستوغرامات ليست منتشرة بشكل متساوٍ، فإن هيستوغرامات الصور المشفرة تصبح مسطحة جدًا بعد التشفير. بعبارة أخرى فإن الصور المشفرة تشبه الصورة العشوائية.

3.3.4 تحليل معامل الارتباط

الارتباط هو مقياس يحدد درجة التشابه بين متغيرين. إذن هو مقياس عملي لتقييم جودة التشفير لأي طريقة تشفير. ويمكن حسابه وفق العلاقة (4.2).

الجدول2.4: معامل الارتباط بين الصورة الأصلية والمشفرة

نوع الصورة	معامل الارتباط بين الصورة الأصلية والمشفرة		
ثنائية	−0.0012		
رمادية	6.3293×10^{-5}		
ملونة	الأخضر	الأحمر	الأزرق
	−0.0026	-7.2912×10^{-4}	−0.0032

يلخص الجدول (2.4) معاملات الارتباط المحسوبة بين الصور الأصلية والمشفرة. حيث تشير هذه النتائج بوضوح إلى الارتباط الضعيف جدًا بين الصورة الأصلية والصورة المشفرة المقابلة لها. ووفقًا لهذه النتائج، نؤكد أن طريقة التشفير مقاومة للهجمات الإحصائية.

4.3.4 تحليل إنتروبيا المعلومات

كما تم الذكر سابقا يُفترض أن يكون أنتروبي المعلومات 8 بت للصور الرمادية و1 بت للصور الثنائية المشفرة. وفي حالة إنتاج صورة مشفرة تحتوي على أنتروبي أقل من 8 بت للصور الرمادية أو أقل من 1 بت للصور الثنائية، فإن هذا يشير إلى وجود إمكانية للتنبؤ بالمحتوى الأصلي. ويتم حسابها وفق العلاقة (6.2)

الجدول 3.4: نتائج الإنتروبيا

نوع الصورة	أنتروبيا الصورة الأصلية	أنتروبيا الصورة المشفرة
ثنائية	0.7522	1.0000
رمادية	7.0097	7.9972
ملونة	7.3785	7.9997

نتائج تحليل الإنتروبيا تظهر أن قيمتها قريبة جدًا من القيمة المثالية المتوقعة ب 8 بت و1 بت بالنسبة. وأن الخوارزمية المستخدمة للتشفير مؤمنة ضد الهجمات.

وفيما يتعلق بالصورة الأصلية يبدو أن هناك ترابطًا بين قيم البكسلات، مما ينتج عنه قيمة أنتروبيا أقل من القيمة المثالية المتوقعة 8. هذا يشير إلى أن الصورة الأصلية تحتوي على بعض الترتيب أو الهيكلية في القيم.

5.3.4 التحليلات الخاصة بخصائص الانتشار

التحليلات المتعلقة بخصائص الانتشار تشير إلى أن أدنى تغيير في الصورة الأصلية ينبغي أن يؤدي إلى تغييرات كبيرة في الصورة المشفرة. ولدراستها نستخدم مقياسين:

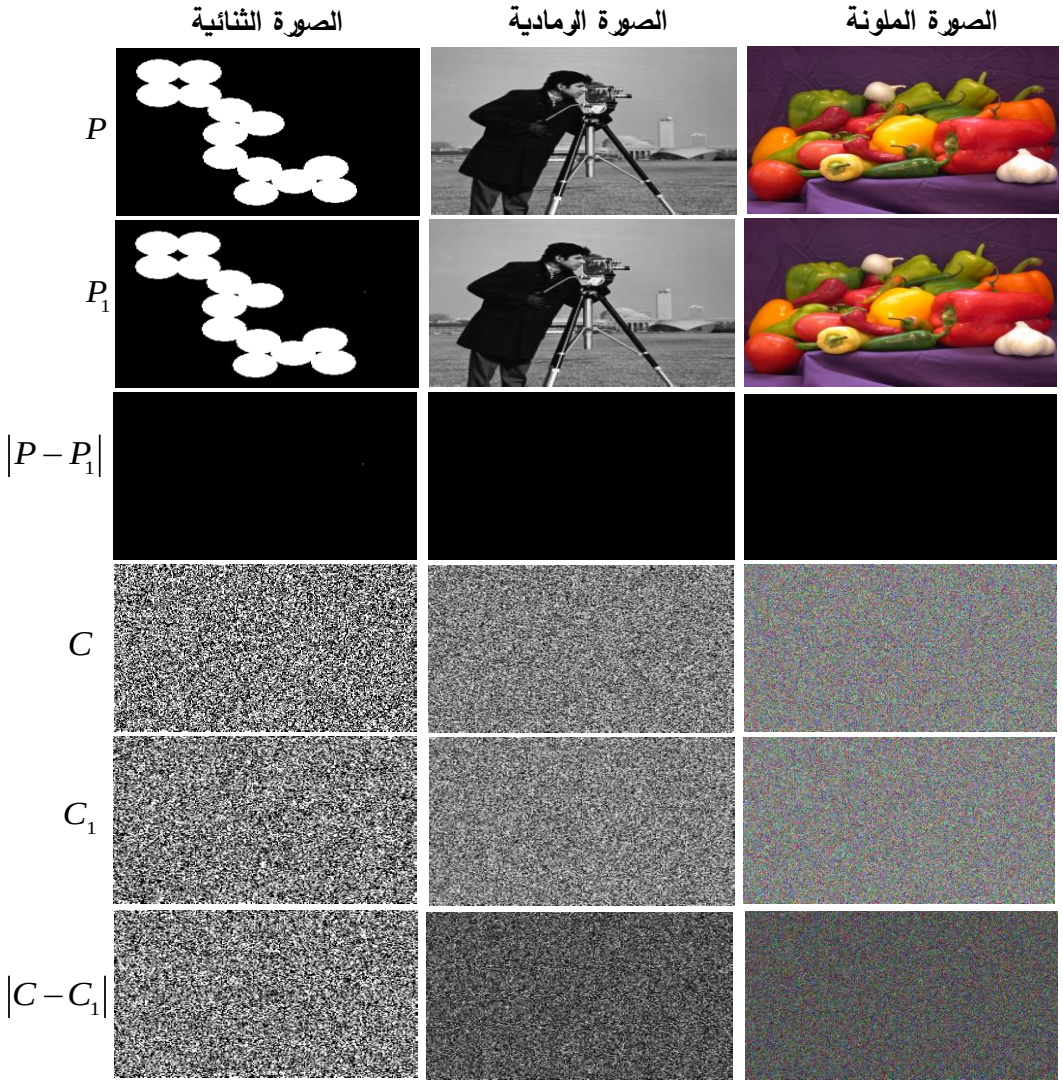
معدل تغيير عدد البكسلات (NPCR): يقيس هذا المعدل باستخدام المعادلة (7.2).

متوسط تغيير الكثافة الموحد (UACI): يحسب هذا المعامل وفق العلاقة (8.2).

كما سبق الذكر **أن** القيم المثالية لمعدل تغيير عدد البكسلات (NPCR) ومتوسط تغيير الكثافة الموحد (UACI) تعتمد على نوع الصورة المشفرة. ففي الصور الملونة والرمادية تكون القيم المثالية لـ NPCR حوالي 99.6094٪ ولـ UACI حوالي 33.4635٪. أما في الصور الثنائية فتكون القيم المثالية لكل من NPCR وUACI قريبة من 50٪.

الجدول 4.4: تحليل UACI وNPCR

نوع الصورة	حساسية المفتاح للتشفير		حساسية المفتاح لفك التشفير		حساسية المفتاح للإنتشار	
	NPCR (%)	UACI (%)	NPCR (%)	UACI (%)	NPCR (%)	UACI (%)
ثنائية	49.9710	49.9710	49.6063	49.6063	49.7620	49.7620
رمادية	99.5728	33.4677	99.6201	33.6445	99.5895	33.4279
ملونة	99648	33.3806	99.6214	33.4842	99.6104	33.4560



الشكل 3.4: تحليل خصائص الإنتشار

- ✓ P : الصورة الأصلية
- ✓ P_1 : الصورة المعدلة (تغيير بت واحد فقط)
- ✓ $|P-P_1|$: الفرق بين الصورتين P و P_1
- ✓ C : الصورة المشفرة للصورة الأصلية
- ✓ C_1 : الصورة المشفرة للصورة المعدلة
- ✓ $|C_1-C_2|$: الفرق بين الصورتين المشفرتين C و C_1

توضح النتائج المعروضة في الجدول (4.4) أن قيم معدل تغيير عدد البكسلات (NPCR) ومتوسط تغيير الكثافة الموحد (UACI) قريبة من القيم المثالية عندما يتغير بت واحد في بكسل المستوى الرمادي الأصلي. بينما يظهر الشكل (3.4) وجود فرق كبير جدًا بين الصورة الأصلية المشفرة والصورة المعدلة المشفرة. هذه النتائج تؤكد

على فعالية الانتشار لطريقة التشفير، حيث يصعب التنبؤ بالصورة الأصلية بناءً على الصورة المعدلة المشفرة والصورة الأصلية المشفرة، مما يعزز الأمان والحماية للبيانات.

6.3.4 تحليل مساحة المفتاح

يُعتبر تحليل مساحة المفتاح ضروريًا لأنه يجب أن تكون مساحة مفتاح نظام التشفير كافية كي تتحمل هجمات القوة الغاشمة. في هذا النوع من الهجمات يقوم المهاجم بتجربة جميع القيم الممكنة للمفتاح بهدف كسر نظام التشفير.

تتضمن الخوارزمية مفتاحًا سريًا يتألف من 156 بت، وبالتالي فإن مساحة المفتاح تبلغ 2^{156} . وبالتالي فإن هذه الطريقة تحتوي على مساحة مفتاح كافية لمقاومة هجمات القوة الغاشمة.

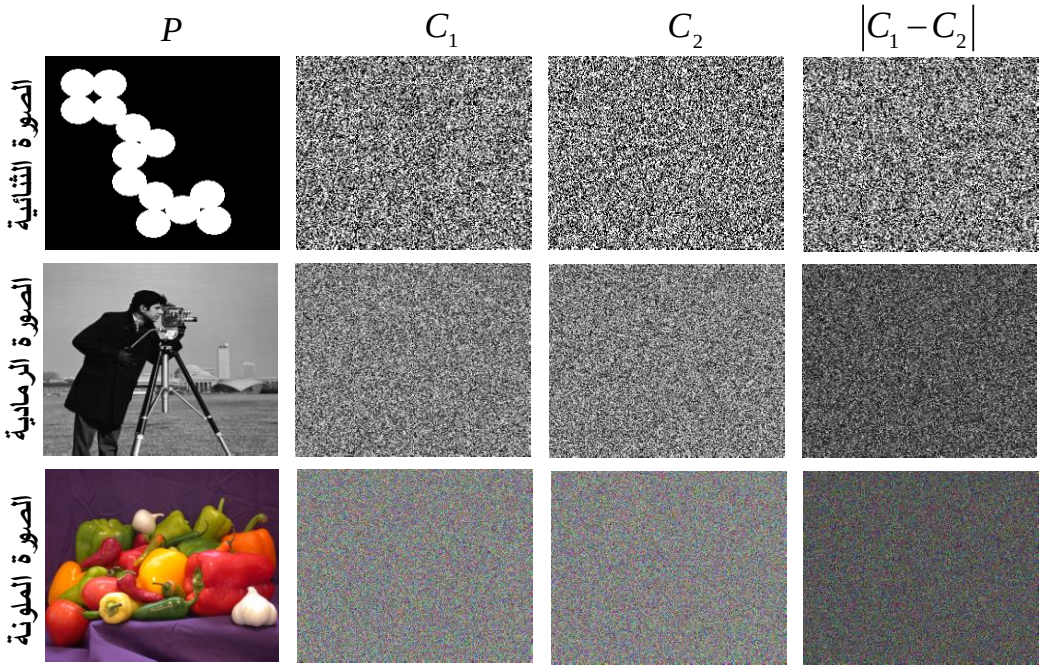
7.3.4 تحليل حساسية المفتاح

تعتبر حساسية المفتاح في عمليات التشفير وفك التشفير أمرًا مهما لضمان الأمان الفعّال. يتم اختبار حساسية المفتاح عادةً من خلال استخدام مفاتيح متعددة، حيث يُعتبر المفتاح الصحيح كـ "key"، بينما "key1" و "key2" هما مفاتيح أخرى يختلف كل منهما عن "المفتاح" الصحيح ببت واحد.

يتم تقييم حساسية المفتاح عن طريق الاختلافات التي تظهر في عمليات التشفير وفك التشفير كما يلي:

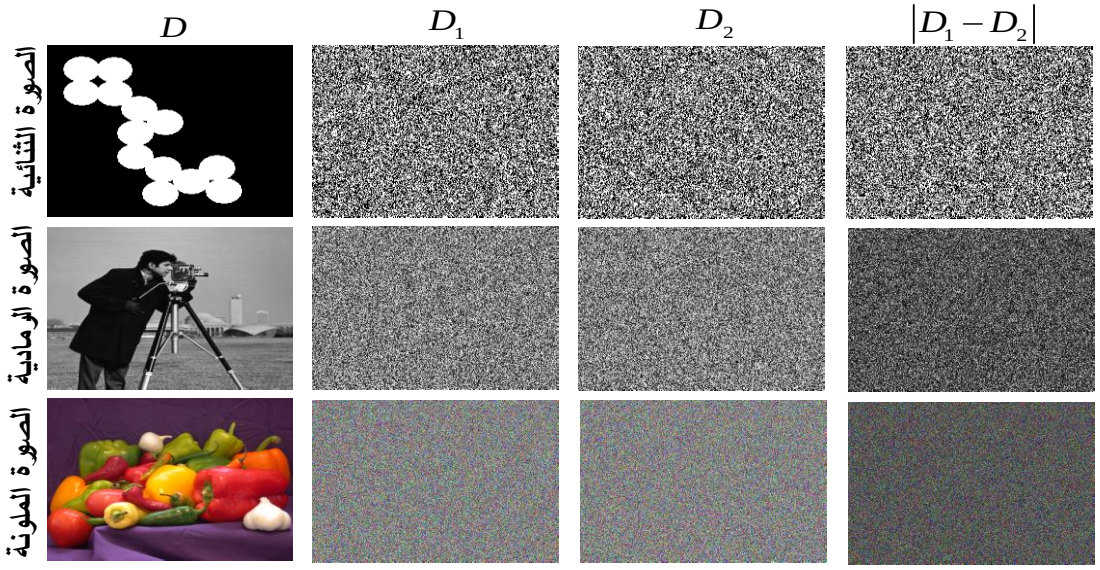
- في عمليات التشفير: يقارن الفرق بين الصورتين المشفرتين C_1 و C_2 باستخدام مفاتيح التشفير key1 وkey2 في التعامل مع نفس الصورة الأصلية، حيث يختلفان فقط في بت واحد.
- في عمليات فك التشفير: يتم مقارنة الاختلافات بين الصورتين المفككتين D_1 و D_2 باستخدام مفاتيح التشفير key1 وkey2 في التعامل مع نفس الصورة المشفرة، حيث يختلفان فقط في بت واحد.

هذا الاختبار يسمح بتقييم حساسية المفتاح وقدرته على التعرف على التغييرات الدقيقة في البيانات المشفرة، ويعتبر جزءًا أساسيًا من عمليات التحليل الأمني لنظام التشفير.



الشكل 4.4: تحليل حساسية المفتاح في التشفير

- ✓ P : الصورة الأصلية
- ✓ C_1 : الصورة المشفرة بالمفتاح 1
- ✓ C_2 : الصورة المشفرة بالمفتاح 2
- ✓ $|C_1 - C_2|$: الفرق بين الصورتين المشفرتين C_1 و C_2



الشكل 5.4: تحليل حساسية المفتاح في فك التشفير

- ✓ D : الصورة بعد فك التشفير بالمفتاح الصحيح
- ✓ D_1 : الصورة بعد فك التشفير بالمفتاح1 (key1)
- ✓ D_2 : الصورة بعد فك التشفير بالمفتاح2 (key2)
- ✓ $|D_1 - D_2|$: الفرق بين الصورتين المشفرتين D_1 و D_2

الشكلان (4.4) و (5.4) يوضحان أن تغيير بت واحد في مفتاح التشفير يؤدي إلى تغيير كامل في الصورة المشفرة، مما يدل على حساسية عالية لمفتاح التشفير. يلاحظ أنه لا يمكن فك تشفير الصورة باستخدام مفتاح يختلف عن المفتاح الصحيح ببت واحد. تظهر هذه النتائج بوضوح أن خوارزمية التشفير القائمة على خريطة لوجستية ثنائية الأبعاد حساسة جدًا لمفتاح التشفير في كل من عمليات التشفير وفك التشفير.

4.4 الخاتمة

الخريطة اللوجستية ثنائية الأبعاد تعتبر تطويرًا مهمًا على الخرائط اللوجستية أحادية البعد التقليدية. حيث تظهر هذه النماذج سلوكًا فوضويًا في بُعدين إضافيين، مما يؤدي إلى إنتاج سلاسل من الأرقام العشوائية تتمتع بمزيد من التعقيد والشبه العشوائية. ونتيجة لذلك، يتمتع استخدام الخريطة اللوجستية ثنائية الأبعاد في تشفير الصور بفعالية أكبر وأمان محسّن. وبالتالي يتيح هذا النهج إنشاء صور مشفرة تصعب عمليات التحليل والكسر، مما يعزز الأمان في مجال حماية البيانات.

طريقة تشفير الصور تظهر قدرة عالية على مقاومة العديد من هجمات التشفير الحالية وتقنيات التحليل التشفيري المعروفة، مثل الهجمات الإحصائية والهجمات التفاضلية. تُظهر النتائج المستخلصة من المحاكاة أن الطريقة المقترحة قادرة على تحويل الصور النصية المفهومة إلى صور نصية تبدو شبه عشوائية للمراقب، مما يجعلها غير قابلة للتعرف عليها أو فهمها. بمعنى آخر تكون الصور المشفرة التي تم إنشاؤها باستخدام الخريطة اللوجستية ثنائية البعد غير قابلة للكشف أو الفك، وخصائصها الإحصائية تتماشى بشكل كبير مع تلك الصور العشوائي.

الخاتمة العامة

الخاتمة العامة

أدى التطور السريع لشبكات الاتصال إلى ظهور مشاكل جديدة تتعلق بأمان الصور الرقمية. يتم عادةً تأمين الصور المخزنة أو المنقولة باستخدام تقنيات التشفير، حيث أصبح تطوير هذه التقنيات تحديًا كبيرًا في السنوات الأخيرة. بعد دراسة بيبليوغرافية لتقنيات تشفير الصور الرقمية لاحظنا أنها ليست قوية بما يكفي ضد الهجمات الحديثة وأن سرعتها التنفيذية غير كافية للتطبيقات في الوقت الحقيقي. المشروع الذي تم اقتراحه يهدف إلى تعزيز قوة تقنيات التشفير المعتمدة على التحويلات وتحسين سرعة التنفيذ.

خلال هذا العمل البحثي، حققنا الهدف أعلاه من خلال الخريطة اللوجستية ثنائية الأبعاد وهي من الأساليب الجديدة لتشفير الصور، يتمتع استخدام الخريطة اللوجستية ثنائية الأبعاد في تشفير الصور بفعالية أكبر وأمان محسّن. وبالتالي يتيح هذا النهج إنشاء صور مشفرة تصعب عمليات التحليل والكسر، مما يعزز الأمان في مجال حماية البيانات.

النتائج التجريبية لتحليل الأمان، وتحديدًا تحليل المدرج التكراري ومعامل الارتباط والانتروبيا وتحليل مساحة وحساسية المفتاح والقياسات الموضوعية التي أجريت على الصور المشفرة والمفككة، هذه النتائج التي تم الحصول عليها في هذا البحث، تؤكد فعالية وقوة الخريطة اللوجستية ثنائية الأبعاد.

في هذا العمل، تناولنا حالة الصور الرقمية وطرق تشفيرها. لذا، نقترح في المستقبل استغلال الأفكار المطورة في هذا البحث لتصميم أساليب جديدة مناسبة لتشفير الفيديو.

قائمة المراجع

[1] J. Pipher, J. H. Silverman, J. Hoffstein, J. Pipher, and J. H. Silverman, *An Introduction to Cryptography*. Springer, 2014.

[2] R. Dumont, "Cryptographie et Sécurité informatique," *Université de Liège*, 2010.

[3] G. Florin and S. Natkin, "Les techniques de cryptographie," *Mars*, 2002.

[4] Amokrane, B. M., & Lyes, D. 2018. Etude et implémentation d'algorithmes de chiffrement à clé secrète et à clé publique: Application au cryptage de la parole (Doctoral dissertation, Université Mouloud Mammeri).

[5] J.-F. Pillou and J.-P. Bay, *Tout sur la sécurité informatique-5e éd.* Dunod, 2020.

[6] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[7] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Trans Inf Theory*, vol. 31, no. 4, pp. 469–472, 1985.

[8] Miller, J. I. 1985. A private-key encryption system based on plane geometry (Doctoral dissertation, University of Wisconsin-Milwaukee).

[9] S. Blake-Wilson, D. Johnson, and A. Menezes, "Key agreement protocols and their security analysis," in *IMA international conference on cryptography and coding*, Springer, 1997, pp. 30–45.

[10] P. U. B. FIPS, "46, 1977," *Data Encryption Standard*, 1977.

[11] X. X. X. FIPS, "Advanced encryption standard (AES)," *National Institute for Standards and Technology (NIST)*, vol. 197, no. 1, 2001.

[12] J. Daemen and V. Rijmen, *The design of Rijndael*, vol. 2. Springer, 2002.

[13] C. E. Shannon, "Communication theory of secrecy systems," *The Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.

[14] G. Paul and S. Maitra, *RC4 stream cipher and its variants*. CRC press, 2011.

[15] M. Hell, T. Johansson, and W. Meier, "Grain: a stream cipher for constrained environments," *International journal of wireless and mobile computing*, vol. 2, no. 1, pp. 86–93, 2007.

[16] M. Hell, T. Johansson, A. Maximov, and W. Meier, "The grain family of stream ciphers," *New stream cipher designs: The eSTREAM finalists*, pp. 179–190, 2008.

[17] W. Easttom and W. Easttom, “Cryptanalysis,” *Modern Cryptography: Applied Mathematics for Encryption and Information Security*, pp. 357–372, 2021.

[18] H. Naciri and N. Chaoui, “Conception et Réalisation d’un système automatique d’identification des empreintes digitales,” *Mémoire de PFE, Université de Tlemcen*, 2003.

[19] W. Burger and M. J. Burge, *Principles of digital image processing: fundamental techniques*. Springer Science & Business Media, 2010.

[20] ع. ح. جروب “ البحث عن الصور على أساس تحليل محتواها ,” *Journal of Science and Technology*, vol. 15, no. 1, 2010.

[21] W. Burger and M. J. Burge, *Digital Image Processing: An Algorithmic Introduction*. Springer Nature, 2022.

[22] B. Jähne, *Digital image processing*. Springer Science & Business Media, 2005.

[23] R. Isdant, “Traitement numérique de l’image,” 2009.

[24] K. Bhamidipati and S. Annadurai, “Permutation–substitution-based image encryption algorithms using pseudorandom number generators,” *Handbook of Computer Networks and Cyber Security: Principles and Paradigms*, pp. 825–848, 2020.

[25] P. Premaratne and M. Premaratne, “Key-based scrambling for secure image communication,” in *Emerging Intelligent Computing Technology and Applications: 8th International Conference, ICIC 2012, Huangshan, China, July 25-29, 2012. Proceedings 8*, Springer, 2012, pp. 259–263.

[26] K. Usman *et al.*, “Medical image encryption based on pixel arrangement and random permutation for transmission security,” in *2007 9th international conference on e-health networking, application and services*, IEEE, 2007, pp. 244–247.

[27] A. Ramesh and A. Jain, “Hybrid image encryption using pseudo random number generators, and transposition and substitution techniques,” in *2015 International Conference on Trends in Automation, Communications and Computing Technology (I-TACT-15)*, IEEE, 2015, pp. 1–6.

[28] A. Belmeguenai, O. Berrak, and K. Mansouri, “Image encryption using improved keystream generator of achterbahn-128,” in *International Conference on Computer Vision Theory and Applications*, SCITEPRESS, 2016, pp. 333–339.

[29] V. Lynnyk, N. Sakamoto, and S. Čelikovský, “Pseudo random number generator based on the generalized Lorenz chaotic system,” *IFAC-PapersOnLine*, vol. 48, no. 18, pp. 257–261, 2015.

[30] H. Khanzadi, M. Eshghi, and S. E. Borujeni, “Image encryption using random bit sequence based on chaotic maps,” *Arab J Sci Eng*, vol. 39, pp. 1039–1047, 2014.

[31] M. L. Sahari and I. Boukemara, “A pseudo-random numbers generator based on a novel 3D chaotic map with an application to color image encryption,” *Nonlinear Dyn*, vol. 94, pp. 723–744, 2018.

[32] D. Herbadji, A. Belmeguenai, N. Derouiche, and H. Liu, “Colour image encryption scheme based on enhanced quadratic chaotic map,” *IET Image Process*, vol. 14, no. 1, pp. 40–52, 2020.

[33] L. Zhou, H. Zhou, Y. Ma, and N.-R. Zhou, “Double-image encryption scheme based on the phase-truncated multiple-parameter Fresnel transform,” *Optica Applicata*, vol. 52, no. 2, 2022.

[34] D. Kumar, A. B. Joshi, and V. N. Mishra, “Optical and digital double color-image encryption algorithm using 3D chaotic map and 2D-multiple parameter fractional discrete cosine transform,” *Results in Optics*, vol. 1, p. 100031, 2020.

[35] Z.-H. Guan, F. Huang, and W. Guan, “Chaos-based image encryption algorithm,” *Phys Lett A*, vol. 346, no. 1–3, pp. 153–157, 2005.

[36] Y. Wu, G. Yang, H. Jin, and J. P. Noonan, “Image encryption using the two-dimensional logistic chaotic map,” *J Electron Imaging*, vol. 21, no. 1, p. 13014, 2012.

[37] Z. Hua, Y. Zhou, C.-M. Pun, and C. L. P. Chen, “Image encryption using 2D Logistic-Sine chaotic map,” in *2014 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, 2014, pp. 3229–3234. doi: 10.1109/SMC.2014.6974425.

[38] Z. Hua and Y. Zhou, “Image encryption using 2D Logistic-adjusted-Sine map,” *Inf Sci (N Y)*, vol. 339, pp. 237–253, 2016.

[39] Z. Hua, F. Jin, B. Xu, and H. Huang, “2D Logistic-Sine-coupling map for image encryption,” *Signal Processing*, vol. 149, pp. 148–161, 2018.

[40] R. Hamza and F. Titouna, “A novel sensitive image encryption algorithm based on the Zaslavsky chaotic map,” *Information Security Journal: A Global Perspective*, vol. 25, no. 4–6, pp. 162–179, 2016.

[41] X.-D. Chen, Q. Liu, J. Wang, and Q.-H. Wang, “Asymmetric encryption of multi-image based on compressed sensing and feature fusion with high quality image reconstruction,” *Opt Laser Technol*, vol. 107, pp. 302–312, 2018.

[42] J. J. Montesinos-García and R. Martinez-Guerra, “Colour image encryption via fractional chaotic state estimation,” *IET Image Process*, vol. 12, no. 10, pp. 1913–1920, 2018.

[43] P. Praveenkumar, R. Amirtharajan, K. Thenmozhi, and J. B. B. Rayappan, "Fusion of confusion and diffusion: a novel image encryption approach," *Telecommun Syst*, vol. 65, pp. 65–78, 2017.

[44] M. Zarebnia, H. Pakmanesh, and R. Parvaz, "A fast multiple-image encryption algorithm based on hybrid chaotic systems for gray scale images," *Optik (Stuttg)*, vol. 179, pp. 761–773, 2019.

[45] Y. Wu and J. Noonan, "Shannon Entropy based Randomness Measurement and Test for Image Encryption," *Computing Research Repository - CORR*, Mar. 2011.

[46] Y. Zhang, "Statistical test criteria for sensitivity indexes of image cryptosystems," *Inf Sci (N Y)*, vol. 550, pp. 313–328, 2021.

[47] G. Alvarez and S. Li, "Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems.," *I. J. Bifurcation and Chaos*, vol. 16, pp. 2129–2151, Aug. 2006, doi: 10.1142/S0218127406015970.

[48] E. N. Lorenz, "Deterministic nonperiodic flow," *Journal of atmospheric sciences*, vol. 20, no. 2, pp. 130–141, 1963.

[49] N. Hamri and T. Hamaizia, "Systemes dynamiques et Chaos," 2013.

[50] G. Elert, "Measuring chaos," *The Chaos Hypertext book*, 2007.

[51] أسامة, م. جادر ،إ. س. جاسم "التشفير الفوضوي باستخدام مفتاح المقياس الحيوي" *AL-Rafidain Journal of Computer Sciences and Mathematics*, vol. 7, no. 3, 2010.

[52] P. F. Curran and L. O. Chua, "Absolute stability theory and the synchronization problem," *International Journal of Bifurcation and Chaos*, vol. 7, no. 06, pp. 1375–1382, 1997.

[53] Z. Qiao, "Nonlinear dynamics, applications to chaos-based encryption." [Online]. Available: https://hal.science/tel-03200707.

[54] D. Fournier-Prunaret and R. Lopez-Ruiz, "Basin bifurcations in a two-dimensional logistic map," *arXiv preprint nlin/0304059*, 2003.

[55] S. H. Strogatz, *Nonlinear dynamics and chaos: with applications to physics, biology, chemistry, and engineering*. CRC press, 2018.

[56] Y. Wu, G. Yang, H. Jin, and J. P. Noonan, "Image encryption using the two-dimensional logistic chaotic map," *J Electron Imaging*, vol. 21, no. 1, p. 13014, 2012.