تصميم ومحاكاة نظام لمعالجة الصور
(التشفير والترميز)

رسالة مقدمة من الطالبة

إسراء عدنان مهدي الوائلي

إلى

مجلس كلية العلوم جامعة بابل

وهي جزء من متطلبات نيل درجة الماجستير علوم

في علوم الحاسبات

١٤٢٢هـ ٢٠٠١م

بسم الله الرحمن الرحيم

وعلمك ما لم تكن تعلم وكان فضل الله

عليك عظيما

صدق الله العلي العظيم

النساء: ١١٣

توصية الأستاذ المشرف

أشهد أن إعداد هذه الرسالة جرى تحت إشرافي في قسم علوم الحاسبات/ كلية العلوم / جامعة بابل وهي جزء من متطلبات نيل درجة الماجستير في علوم الحاسبات الإلكترونية.

أسم المشرف: د. ستار بدر سدخان
المرتبة العلمية: رئيس باحثين
العنوان: شركة الميلاد العامة
التوقيع:
التأريخ: / / ٢٠٠١

أسم المشرف: السيد توفيق عبد الخالق الأسدي
المرتبة العلمية: أستاذ مساعد
العنوان: كلية العلوم / جامعة بابل
التوقيع:
التأريخ: / / ٢٠٠١

توصية رئيس القسم

إشارة إلى التوصية أعلاه المقدمة من قبل الأساتذة المشرفين، أحيل هذه الرسالة إلى لجنة المناقشة لدراستها وبيان الرأي فيها.

الاسم: د. نبيل هاشم كاغد
المرتبة العلمية: أستاذ
العنوان: كلية العلوم / جامعة بابل
التوقيع:
التأريخ:

قرار لجنة المناقشة

نشهد بأننا أعضاء لجنة التقويم والمناقشة اطلعنا على هذه الرسالة وقد ناقشنا الطالبة في محتوياتها وفيما له علاقة بها وذلك بتاريخ / / ٢٠٠١ ووجدنا أنها جديرة بالقبول بدرجة ( ) لنيل درجة الماجستير في علوم الحاسبات.

رئيس اللجنة
التوقيع:
الاسم:
المرتبة العلمية:
التأريخ: / / ٢٠٠١

عضو اللجنة
التوقيع:
الاسم:
المرتبة العلمية:
التأريخ: / / ٢٠٠١

عضو اللجنة
التوقيع:
الاسم:
المرتبة العلمية:
التأريخ: / / ٢٠٠١

عضو اللجنة (المشرف)
التوقيع:
الاسم:
المرتبة العلمية:
التأريخ: / / ٢٠٠١

عضو اللجنة (المشرف)
التوقيع:
الاسم:
المرتبة العلمية:
التأريخ: / / ٢٠٠١

مصادقة عميد كلية العلوم
أصادق على ما جاء في قرار اللجنة أعلاه.
التوقيع:
الاسم: د. فلاح حسن حسين
المرتبة العلمية: أستاذ
العنوان: كلية العلوم / جامعة بابل
التأريخ: / / ٢٠٠١

الشكر والتقدير

الحمد لله رب العالمين والصلاة والسلام على خير الخلق سيدنا محمد (ص)

أتقدم بالشكر الجزيل إلى كل من:

- رئاسة جامعة بابل وعلى رأسها الأستاذ الدكتور يحيى توفيق الراوي، لتعاونه في تطوير الدراسات العليا في أقسام الجامعة.
- عمادة كلية العلوم / جامعة بابل وعلى رأسها الأستاذ الدكتور فلاح حسن حسين، لملاحظاته السديدة في دعم طلبة الدراسات العليا في كلية العلوم.
- قسم علوم الحاسبات وعلى رأسه الأستاذ الدكتور نبيل هاشم كاغد، على كافة التسهيلات والإرشادات في أثناء فترة الدراسة.
- أستاذي الدكتور ستار بدر سد خان، وأستاذي السيد توفيق عبد الخالق، لتعاونهما في الإشراف على رسالتي.
- الأخت زينب جواد لمعاونتها في طبع هذه الرسالة.

الباحثة

الخلاصة

إن العمل المنجز في هذه الرسالة قد تم في جامعة بابل للفترة من تشرين أول ١٩٩٩ إلى حزيران ٢٠٠١ وبإشراف الدكتور ستار بدر سد خان والسيد توفيق عبد الخالق عباس. وباستثناء ما مشار إليه بمصدر معين فان المعلومات الموجودة هي من نتاج الباحثة وإنها لم تقدم لنيل درجة علمية أخرى سابقا .

يقدم هذا البحث طريقة لنقل ومعالجة وحماية بيانات الصور من خلال تصميم نظام يتضمن عدة مراحل وهي، المعالجة الأولية للصور، ومن ثم تشفير بيانات هذه الصور باستخدام كل من نظام التشفير الجمعي(Additive Cipher System)، نظام التشفير الضربي(Multiplicative Cipher System)، نظام التشفير الهجين(Affine Cipher System)، نظام التشفير الخلطي(Scrambling Cipher System)، نظام التشفير الانسيابي الخطي(Linear Stream Cipher System)، ونظام التشفير الانسيابي الخطي باستخدام الحقل العشوائي(Linear Stream Cipher System Using Random Field). ومن ثم محاكاة نقل الصور المشفرة عبر قناة اتصال غير أمينة، حيث تتم هنا عملية الترميز وفك الترميز للحفاظ على معلومات الصور المرسلة، وبعد ذلك العمل على فك تشفير الصور التي أدخلت للقناة والحصول على الصور الواضحة أي بعد إجراء المعالجة المعكوسة والتخلص من الضوضاء والتشويه الذي قد يحصل ويقوم النظام بعرض الصور الناتجة من كل مرحلة.

تم اعتماد البرمجة بلغة باسكال الإصدار ٧ في كتابة الايعازات الخاصة بتصميم النظام.

Abstract

This work described in this thesis was undertaken at the University of Babylon between October ١٩٩٩ and June ٢٠٠١ under the supervision of Dr. Sattar B. Sadkan and Mr. Tawfiq A. Abbas. Except where indicated by reference, it is the original work of the author and has not submitted for any degree.

This work presents a method for transferring, processing and protecting image data through the construction of a design of a multifold system. The design includes: image preprocessing, the ciphering of image data by the use of additive cipher system, multiplication cipher system, affine cipher system, scrambling cipher system, linear stream cipher system, and linear stream cipher system using the random field.

Afterwards, the assimulation of ciphered image transferring is carried out via an insecure communication channel, where coding and decoding are carried out to maintain security of image data. Deciphering image data is also employed in respect of images received through channel to obtain clear images, i.e., after the application of reverse treatment to get rid of the noise that may result in. The system, however, displays the resulting images after each stage.

The proposed system was written in Pascal Language Ver.٧.

الخلاصة

إن العمل المنجز في هذه الرسالة قد تم في جامعة بابل للفترة من تشرين أول ١٩٩٩ إلى حزيران ٢٠٠١ وبإشراف الدكتور ستار بدر سد خان والسيد توفيق عبد الخالق عباس. وباستثناء ما مشار إليه بمصدر معين فان المعلومات الموجودة هي من نتاج الباحثة وإنها لم تقدم لنيل درجة علمية أخرى سابقا .

يقدم هذا البحث طريقة لنقل ومعالجة وحماية بيانات الصور من خلال تصميم نظام يتضمن عدة مراحل وهي، المعالجة الأولية للصور، ومن ثم تشفير بيانات هذه الصور باستخدام كل من نظام التشفير الجمعي(Additive Cipher System)، نظام التشفير الضربي(Multiplicative Cipher System)، نظام التشفير الهجين(Affine Cipher System)، نظام التشفير الخلطي(Scrambling Cipher System)، نظام التشفير الانسيابي الخطي(Linear Stream Cipher System)، ونظام التشفير الانسيابي الخطي باستخدام الحقل العشوائي(Linear Stream Cipher System Using Random Field). ومن ثم محاكاة نقل الصور المشفرة عبر قناة اتصال غير أمينة، حيث تتم هنا عملية الترميز وفك الترميز للحفاظ على معلومات الصور المرسلة، وبعد ذلك العمل على فك تشفير الصور التي أدخلت للقناة والحصول على الصور الواضحة أي بعد إجراء المعالجة المعكوسة والتخلص من الضوضاء والتشويه الذي قد يحصل ويقوم النظام بعرض الصور الناتجة من كل مرحلة.

تم اعتماد البرمجة بلغة باسكال الإصدار ٧ في كتابة الايعازات الخاصة بتصميم النظام.

المحتويات

قائمة الرموز

رموز التشفير	
P	النص الواضح (الصورة الواضحة)
C	النص المشفر (الصورة المشفرة)
K	مفتاح التشفير
f_E	خوارزمية التشفير
f_D	خوارزمية فك التشفير
n	المعيار الحسابي والذي يمثل عدد هجائية التشفير
L	طول المتتابعة العشوائية
$\oplus$	الدالة البوليانية XOR
$\wedge$	الدالة البوليانية AND
$\vee$	الدالة البوليانية OR
M	الرسالة (الصورة)
رموز معالجة الصورة	
H	عملية التدني
η (x, y)	الضوضاء الجمعي
f (x, y)	الصورة المدخلة
g(x, y)	الصورة المتدنية
σ_n^2	التباين لـ n
رموز الترميز	

n	طول الرمز أو طول الكتلة
k	عدد بتات الفحص
٢^k	عدد كلمات الرمز
m	بتات المعلومات
C	كلمة الرمز
G	المصفوفة المولدة
P	مصفوفة فحص التماثل المستخدمة في عملية الترميز
H	مصفوفة فحص التماثل المستخدمة في عملية فك الترميز
R	كلمة الرمز المستلمة
S	السيندروم الذي يكتشف الأخطاء
E	متجه الخطأ

قائمة الجداول

قائمة الأشكال

الفصل الأول

المقدمة

١.١ مقدمة عامة (General Introduction)

مع التطور الكبير الذي حصل في تطبيقات علم الحاسبات وظهور أنظمة حديثة للتعامل مع البيانات مثل قواعد البيانات وقواعد المعلومات وأنظمة معالجة الصور باختلاف أنواعها أصبح نقل المعلومات المرئية في صيغة صور رقمية هو طريقة الاتصالات الأساسية في العصر الحديث .

وللمحافظة على أمنية هذه المعلومات ظهرت وسائل وطرائق حماية وأمنية متعددة، لذلك تم التركيز في السنوات الأخيرة على أنظمة تشفير البيانات ومن بينها أنظمة تشفير الصور وترميزها ونقلها عبر قنوات الاتصالات خصوصاً بعد اتساع استخدام شبكة الانترنيت وما يتم خلالها من نقل للصور بمختلف أنواعها .

يعرف علم التشفير (Cryptology) بأنه العلم الذي يعنى بإخفاء المعلومات المهمة بطريقة ما، بحيث يصبح معنى هذه المعلومات غير واضح للشخص غير المخول . يعد علم التشفير من الحقول الرياضية المهمة التي يتم تطبيقها لضمان إرسال المعلومات بصورة أمينة عبر قنوات اتصال غير أمينة [١] .

يقسم علم التشفير إلى قسمين : علم تصميم أنظمة التشفير (Cryptography) الذي يختص بتصميم وبناء الأنظمة الشفرية (أي الطرائق التي يتم فيها تحويل النص الواضح إلى نص مشفر وبالعكس وذلك بتوفر مفتاح التشفير) .وعلم تحليل التشفير (Cryptanalysis) الذي يختص بتصميم وبناء طرائق تحويل النص المشفر إلى نص واضح بدون توفر المفتاح[٢].

تقسم أنظمة التشفير إلى أنواع مختلفة من الشفرات التقليدية والحديثة ، وتضم الشفرات التقليدية الشفرات الأبدالية والشفرات التعويضية ، أما الشفرات الحديثة فتضم أنظمة التشفير القياسي للبيانات والتشفير الانسيابي والمفتاح المعلن [٢].

يشير مصطلح معالجة الصورة الرقمية (Digital Image Processing) إلى معالجة صور ثنائية الأبعاد (Two – Dimensional) بوساطة الحاسبة ، والصورة الرقمية هي عبارة عن مصفوفة أعداد تمثل بعدد محدد من البتات [٣] .

ترقـمن (Digitized) الصـورة المعطـاة أولاً ، وتخـزن كمصفوفـة أرقـام ثنائيـة (Binary Digits) في ذاكرة الحاسوب [٥,٤]، وفيما بعد يمكن معالجتها وعرضـها على شاشة حاسوبية أو تلفزيونية.

يوجد مدى واسع من التطبيقات المعتمدة على معالجة الصورة الرقمية مثل التحسس النائي عبر الأقمار الصناعية ، نقل وخزن الصور عبر شبكات ألحوا سيب لتطبيقات الأعمال ، الاتصالات العسكرية، المعالجات الطبية ، السونار، الرادار والسيطرة النوعية الصناعية [٦,٣].

ينبع الاهتمام بطرائق معالجة الصور الرقمية من مجالي تطبيق أساسيين هما :-

الأول: تحسين المعلومات التي تمثل الصورة من اجل تفسيرها من قبل الإنسان [٧]، والثاني: معالجة بيانات الصورة الناتجة لإدراكها من قبل الحاسوب بشكل مستقل. يمكن تقسيم العمليات المستعملة في معالجة الصورة إلى الأقسام الآتية : رقمنة الصورة (Image Digitization)، تحسين الصورة (Image Enhancement)، واسترجاع الصورة (Image Restoration) وترميز الصورة (Image Coding) [٩,٨].

وفيما يخص الترميز وفك الترميز للبيانات المرسلة عبر قنوات الاتصالات فهو من المواضيع المهمة ، وذلك لحماية قنوات الاتصال والسيطرة على الأخطاء التي تحصل وتصحيح تلك الأخطاء[١١,١٠].

إن هدف دوائر الترميز – فك الترميز هو لتقليل الضوضاء الناتجة عن المرور بالقناة، ويحصل ذلك بإضافة صيغة معينة من الفائضية (Redundancy) إلى بيانات المصدر[١٣,١٢] . ومع إن البيانات الخارجة من مرمز المصدر قد تحتوي على بعض الفائضية إلاّ إنها تكون حساسة إلى الضوضاء الناتجة أثناء الإرسال إذا لم يتم إضافة الفائضية المسيطر عليها ، وان فكرة استخدام الفائضية لزيادة معوليه (Reliability) المعلومات تعود إلى العالم Claude Shannon مؤسس نظرية المعلومات [٦]، وقد تم تصميم رموز تصحيح الأخطاء (Error Correction Codes) لتقليل احتمالية أخطاء البتات ولتعطي حماية متساوية لكل البيانات وهنالك تقنيات تكتشف الأخطاء وتصححها [١٥,١٤] .

في عام ١٩٩٦ قدمت طريقة لتشفير الصورة باستخدام المحولات (Transforms) حيث يعمل أسلوب التشفير المعتمد على تجزئة الصورة ، تحويل الأجزاء ، وبعثرة وحدات الصورة ، وفقا لذلك فان الصورة المراد تشفيرها تجزأ إلى عدد عشوائي من الأجزاء ويتم تحويل كل جزء باستخدام إحدى المحولات مثل محول فورير السريع ومحول وولش السريع ، ثم تبعثر وحدات (نقاط) الصورة بمرحلتين ، البعثرة المحلية وهي بعثرة وحدات الصورة داخل جزء من الصورة والبعثرة الشاملة وهي بعثرة وحدات الصورة داخل الصورة ككل [١٦].

ظهرت في عام ١٩٩٦ تقنية تشفير الصورة بالاعتماد على مقابلات Chaos (Chaotic maps)، والتشفير هو من نوع التشفير الكتلي(Block Cipher) مع مفتاح سري حيث يعمم مقابل Chaos ثنائي الأبعاد بإدخال المعالم (Parameters) ثم تقطيعها بحيث إنها ترسم خارطة لمجموعة من النقاط قائمة الزاوية، وأخيراً يتم توسيع الخارطة إلى ثلاثة أبعاد لتعديل السويات الرمادية. ومعالم الخارطة هي بمثابة مفاتيح تشفير، حيث ينتج التشفير من التطبيق المكرر لمقابل Chaos على صورة رقمية ، أما في عملية فك التشفير فيتم تطبيق معكوس الخارطة وبنفس عدد المرات. وبغض النظر عن الصورة الابتدائية ، فان الصورة المشفرة تمثل التوازن غير المترابط على شاشة خالية من الإشارة ، ويصبح المدرج الإحصائي للصورة المشفرة منتظماً. تناسب هذه التقنية تشفير الصورة بسبب سهولتها ومعدل تشفيرها العالي [١٧] .

في عام ١٩٩٨ ظهرت طريقة مبتكرة لامنية إرسال البيانات عبر قنوات عمومية غير أمينة وذلك باستخدام تقنية تشفير قوية وسريعة وذلك بالتطبيق المكرر لمقابل Chaotic المتقطعة والقابلة للانعكاس على مجموعة من النقاط (يعني صورة ما) وانتاج تبديل معقد لتلك النقاط ، ويمكن فك الشفرة بتطبيق خاصية الانعكاس وبدون فقدان للمعلومات وتكون معالم مقابل Chaotic هي مفاتيح تشفير ، يعتمد عدد مفاتيح التشفير الكلية على عدد النقاط في الصورة الرقمية حيث تمتلك الصورة ذات الحجم ٥١٢ × ٥١٢ اكثر من $١٠^{٢٧}$ مفتاح تشفير، والتي تم تقديرها رياضيا بأنها تحتاج $١٠^{١١٢}$ سنة للبحث في المفاتيح الممكنة ازدادت الأمنية باستخدام تقنيات الإخفاء (Steganography)التي تعني إن الصورة المشفرة تكون مخبأة في صورة حاملة وذلك باستخدام طريقة البت الأقل أهمية (Least Significant Bit) (LSB) وبذلك يكون حجم الصورة الحاملة أربع مرات بقدر حجم الصورة المشفرة بتشويه بسيط لنوعية الصورة الحاملة [١٨].

في عام ١٩٩٩ تم تطوير خوارزميات جديدة وتطبيق خوارزميات موجودة لإنجاز التشفير الأمين ، السريع ، الكفء والقوي وإخفاء الرسائل السرية داخل صور رقمية ، فيديو ، ووثائق وكذلك تطوير تقنيات الإخفاء التي تعطي أمنية أعلى من ترميز البت الأقل أهمية ، وذلك لتقوية الاتصالات المخبأة والإشارات الرقمية. وتم تطبيق طريقة تشفير الصورة الأمينة (التشفير / الإخفاء) للوثائق داخل صور رقمية حاملة، وكذلك توضيح كيفية إرسال واسترجاع فك شفرة معينة لصور مشفرة / مخبأة على الانترنيت [١٩].

في عام ٢٠٠٠ نشر تقرير عن صنف جديد لتحويل الخلط (Scrambling Transformation) وتطبيقاته في تمويه معلومات الصورة (Image Information Covering)، حيث يناقش هذا التقرير نوعين من المحولات اللاخطية والتي تدعى محول آرنولد عالي الأبعاد ومحول فيبوناجي عالي الأبعاد ويشرح عملية الخلط (Scrambling) للمحولين مركزاً على فضاء الشكل (Phase Space) للصور الرقمية، إن الشرط الضروري والكافي

لمصفوفة تحويل الصورة الرقمية هو إنها تمتلك الدورية. تبين النتائج بأنه يمكن تطبيق المحولين في خزن ونقل معلومات الصورة وذلك لغرض أمنية المعلومات [٢٠] .

في العام ٢٠٠١ صدر تقرير عن خلط الصورة (Image Scrambling) والذي ذكر بان نظام تشفير الصورة (Image Cryptographic) هو توحيد لتكنولوجيا التشفير وتكنولوجيا معالجة بيانات الصورة حيث يتم تطبيق التشفير لعمل ترتيب غير منتظم للون وموقع النقطة وذلك لغرض منع بيانات الصورة من التزوير بينما يتم تطبيق معالجة بيانات الصورة وذلك لإرجاع الصورة الأصلية من بيانات الصورة المرمزة، إن نظام تشفير الصورة هو عملية نقل الصورة الأصلية إلى صورة مختلفة وذلك لمنع خطر التزوير أو تغيير بيانات الصورة ، بكلام آخر، انه ينقل بيانات الصورة الشخصية أو الختم المسجل والتوقيع والتي تكون هدف للتزوير إلى موقع ولون غير منتظم ونقطة بعد أخرى وباستخدام خوارزمية تشفير مناسبة وبعدها يتم طبع الصورة المنقولة على كارت، ويقوم النظام بقراءة الصورة المنقولة أو المحولة، ثم العمل على استرجاع الصورة الأصلية بوساطة خوارزمية فك التشفير وفحص تلك الصورة فيما إذا كانت قد زوّرت أم لا . [٢١]

تهدف الأطروحة إلى بناء بعض أنظمة (التشفير ـ فك التشفير) لبيانات الصور حيث تتم عملية (التشفير ـ فك التشفير) باستخدام نظام التشفير الجمعي والضربي والهجين والمزج والتشفير الانسيابي الخطي والتشفير الانسيابي باستخدام الحقل العشوائي، وتهدف الأطروحة كذلك إلى محاكاة إمكانية استخدام معالج بيانات مصدرية (مرمز- فاك الترميز) من نوع المرمز الكتلي الخطي (LBC) بهدف تطويع إمكانية استخدام مثل هذا المعالج سوية مع نظام التشفير لتوفير قابلية كشف أو تصحيح بعض أخطاء البيانات الناتجة عن مرور الإشارة عبر القنوات الضوضائية ومن ثم استرجاع الصورة غير المشفرة (الواضحة) بعد إنجاز المعالجة المطلوبة لتخليصها من الضوضاء والأخطاء والتشويه .

لقد تم تنظيم محتويات هذه الرسالة في ثلاثة فصول، تضمن الفصل الأول مقدمة عامة حول معالجات الصورة في أنظمة الاتصالات (التشفير والترميز)، مع تغطية للأفكار الأساسية للموضوع. وتمت في هذا الفصل مناقشة الأسس النظرية لكل من التشفير، معالجة الصورة، والترميز. وتضمن الفصل الثاني عرضا"مفصلا" للطرائق والخوارزميات المقترحة لبناء نظام جديد لمعالجة الصور ومحاكاة تأثير ضوضاء قناة الاتصال. أما الفصل الثالث فقد قدم أهم النتائج التي تم الحصول عليها عند تنفيذ النظام، وعرض الاستنتاجات العامة وتوجهات العمل المستقبلي.

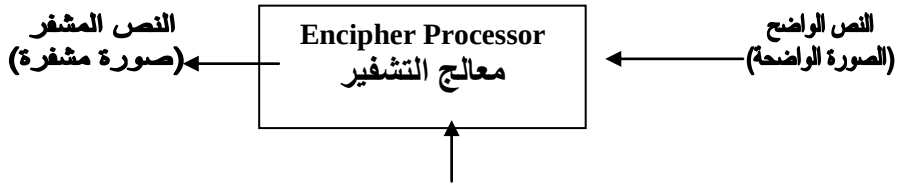
٢.١ معالجات الصورة في أنظمة الاتصالات (التشفير والترميز)

يعرف نظام الاتصالات بأنه مجموعة من معالجات الإشارة التي تتعامل مع إشارة المصدر ضمن (أو من خلال) خوارزميات أو تقنيات متعددة [٢٢]. ويتضح ذلك بصورة جلية في الشكل رقم (١-١) . حيث يمثل هذا الشكل المخطط الكتلي لمكونات نظام الاتصالات، أي مجموعة معالجات الإشارة المختلفة التي يمكن أن تستخدم لأهداف مختلفة.

وفي البنود اللاحقة من هذا الفصل سوف نعرض الأسس النظرية للأساليب والتقنيات التي يتكون منها النظام المقترح وهي تشمل حقول معالجات التشفير/ فك التشفير، معالجات الترميز/ فك الترميز ومعالجات الصور الرقمية.

٣.١ معالجات التشفير(Encipher Processors)

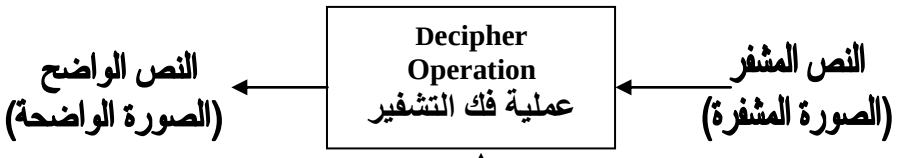
يهدف معالج التشفير (Encipher Processor) إلى إخفاء المعلومات المهمة بطريقة ما، بحيث يصبح معنى هذه المعلومات غير واضح للشخص غير المخول(المتنصت)، تعرف المعلومات التي نريد إخفاءها بالنص الواضح (Plaintext) أو الرسالة (Message) أو الصورة، وتعرف عملية الإخفاء بعملية التشفير(Enciphering) وتسمى الرسالة الناتجة: النص المشفر (Ciphertext) أو (Cryptogram) [٢٣,٢]. وكما موضح بالشكل (١–٢).



الشكل رقم (١-٢) مبدأ عمل معالج التشفير

وتعرف مجموعة الخطوات التي يستخدمها معالج التشفير لتشفير النص الواضح بخوارزمية التشفير(Encryption Algorithm) ، ويعتمد عمل هذه الخوارزمية على مفتاح التشفير (key) الذي يدخل مع النص الواضح إلى الخوارزمية، وهذا المفتاح يكون معروفاً للمستلم وبهذا فانه يستطيع استعادة النص الواضح من النص المشفر.

تدعى عملية استعادة النص الواضح من النص المشفر باستخدام مفتاح فك الشفرة: عملية فك التشفير (Deciphering) [٢٣] , وكما موضح في الشكل (١ – ٢) .



شكل (١ – ٢) مبدأ عملية فك التشفير
مفتاح فك الشفرة

يعبر رياضياً عن عملية التشفير بالعلاقة الآتية :

$$C = f_E (P, K) \quad \ldots(١-١)$$

حيث C النص المشفر ، f_E خوارزمية التشفير، P النص الواضح ، K مفتاح التشفير

ويعبر عن عملية فك التشفير بالعلاقة الآتية :

$$P = f_D (C, K) \quad \ldots(٢-١)$$

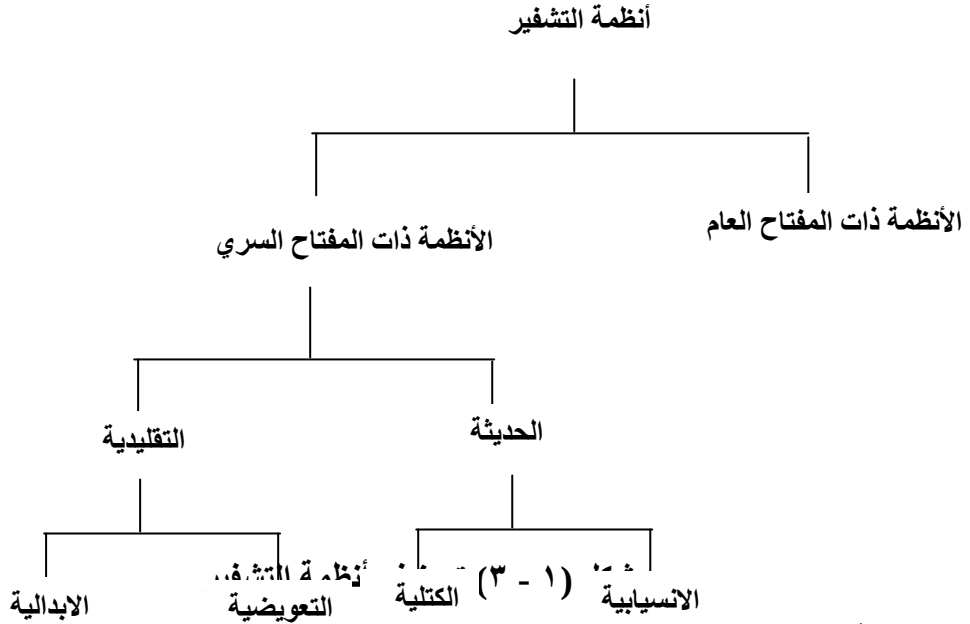
حيث P النص الواضح ، f_D خوارزمية فك التشفير، C النص المشفر، K مفتاح فك التشفير[٢].

من أجل أن يكون النظام الناتج عن استخدام معالج التشفير ومعالج فك التشفير أمينا" يجب أن يحقق النظام ما يلي :

١. أن لا يكون للمحلل القدرة على إيجاد النص الواضح عند معرفته النص المشفر.
٢. أن لا يكون للمحلل القابلية على تحديد خوارزمية فك الشفرة (وإيجاد مفتاح التشفير) عند معرفته بالنص المشفر حتى لو تمكن من معرفة النص الواضح [٢٤].

يكون نظام التشفير مثالياً عندما تكون له القدرة على تشفير نص واضح بحيث تنتج أكثر من رسالة مفهومة عند فك شفرة الرسالة المشفرة من قبل المعترض، ولا تتوفر للمعترض المعلومات الكافية ليقرر أي الرسائل المفهومة تم إرسالها، عندها يقال على مثل هذا النظام الشفري إنه غير قابل للكسر[١].

هناك عدة أنواع من أنظمة التشفير ، يوضح الشكل (١ – ٣) هذه الأنواع [١].



شكل (١ - ٣) أنظمة التشفير

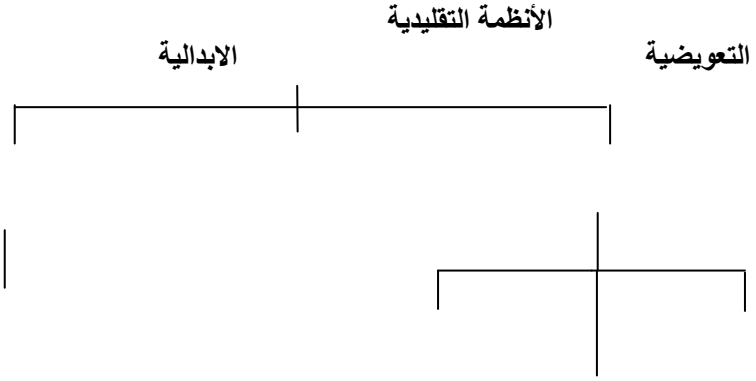
من الشكل أعلاه نلاحظ ان انظمه التشفير تقسم إلى [٢] هما :

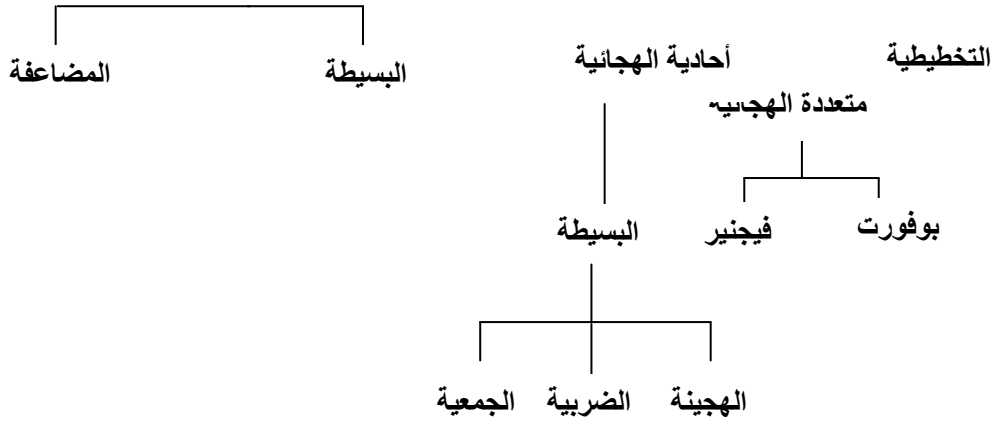
١. أنظمة التشفير ذات المفتاح السري والتي يستخدم فيها مفتاح سري واحد لعمليتي التشفير وفك الشفرة.
٢. أنظمة التشفير ذات المفتاح العام والتي يكون فيها مفتاح التشفير معروف (غير سري) ولكن مفتاح فك الشفرة يكون سريا" حيث يستخدم مفتاحين مختلفين بدلاً من مفتاح واحد.

من أعلاه نجد إن أنظمة التشفير ذات المفتاح السري تقسم إلى:-

أولا": أنظمة التشفير التقليدية

تقسم أنظمة التشفير التقليدية إلى عدة أنواع كما في الشكل (١ - ٤) [٢]:





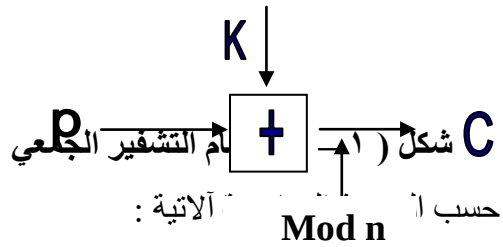
شكل (١ - ٤) أنواع أنظمة التشفير التقليدية

استخدم نظام المعالجة المقترح للصورة ثلاثة أنظمة تشفير تقليدية وهي :

أ . نظـام التشـفير الجمعـي (Additive Cipher System) : يعتبـر مـن أنظمـة التشـفير التعويضية من النوع وحيد الهجائية والذي يستخدم هجائية تشفير وحيدة لتشفير النص الواضح بأكمله . ويعتمد التعبير عنه رياضياً وفق الصيغة الآتية:

$$C = (P+K) \text{ Mod } n \qquad \ldots(١-٣)$$

حيث C هو النص المشفر ,P هو النص الواضح , K هو مفتاح التشفير السري أما n فتمثل المعيار الحسابي , ويعتبر معالج التشفير الجمعي من ابسط أنواع معالجات التشفير التقليدية، ويكون عدد مفاتيح التشفير المستخدمة في هذا النظام هو (n–١) [٢]، وكما موضح في الشكل (٥ – ١)



شكل (١ – ٥) نظام التشفير الجمعي

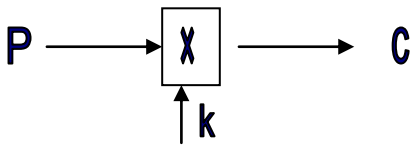
وتتم معالجة فك الشفرة حسب الآلية الآتية :

$$P = (C - K) \text{ Mod } n \qquad \ldots(١ - ٤)$$

ب ـ نظـام التشـفير الضـربي (Multiplicative Cipher System) : هـو نظـام الشـفرة التعويضية وحيدة الهجائية يعبر عنه رياضياً بالعلاقة الآتية :

$$C = (P * K) \text{ Mod } n \qquad \ldots (١ - ٥)$$

حيث C النص المشفر ، P النص الواضح ، K المفتاح ، و n المعيار الحسابي والذي يمثل عدد هجائية التشفير ، وكما موضح في الشكل (١ – ٦) :



(١ - ٦) نظام التشفير الضربي

وتتم معالجة فك الشفرة بالتعبير الرياضي الآتي :

$$P = (C * K^{-1}) \text{ Mod } n \qquad \ldots(١ - ٦)$$

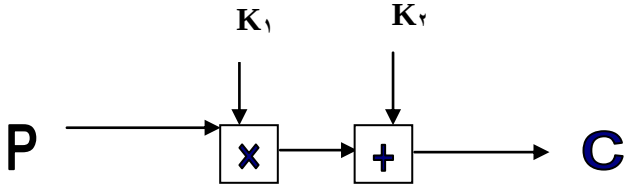
حيث إن K^{-1} يتم استخراجها من المعادلة التالية :

$$K^{-1} = ١ \text{ Mod } n / K \qquad \ldots(١ - ٧)$$

ج – نظام التشفير الهجين (Affine Cipher System) : وهو نظام شفرة تعويضية وحيدة الهجائية ، ويجمع نظامي التشفير الجمعي والتشفير الضربي معاً. ويمكن التعبير عنه رياضياً بما يأتي :

$$C = (P * K_١ + K_٢) \text{ Mod } n \qquad \ldots(١ – ٨)$$

حيث إن C النص المشفر ، P النص الواضح ، n الهجائية ، وكما موضح في الشكل (١ – ٧)



شكل (١ – ٧) نظام التشفير الهجين

وتتم معالجة فك الشفرة حسب الصيغة الرياضية الآتية :

$$P = [(C - K_٢) * K_١^{-1}] \text{ Mod } n \qquad \ldots (١ - ٩)$$

حيث $K_١^{-1}$ هو المفتاح الضربي المعكوس والذي يستخرج كما في المعادلة (١-٧) [٢].

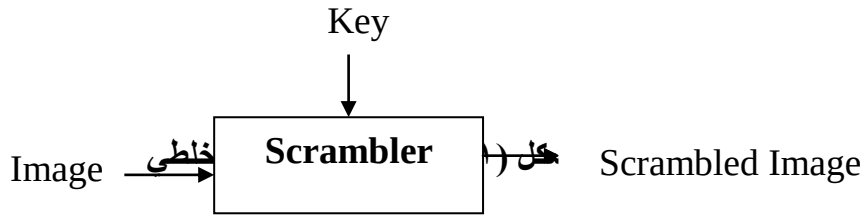
ثانياً : أنظمة التشفير الحديثة

وتتضمن كل من نظام التشفير القياسي (D E S) ونظام تشفير المفتاح العام (RSA ,Knapsack) ، نظام التشفير الانسيابي[٢٤] ، ونظام التشفير الخلطي [٥٢]. يعتبر كل من نظام التشفير القياسي (مفتاح سري) ونظام تشفير المفتاح العام (مفتاح عمومي) من أنظمة التشفير الكتلي التي تتعامل مع النص الواضح والمفتاح والنص المشفر وكل منها على هيئة

كتله (Block) مكونة من مجموعة بتات أو رموز أو كلمات , أما نظام التشفير الانسيابي ونظام التشفير الخلطي فانهما يتعاملان مع البتات: بت بعد أخر من النص الواضح ليشفره وينتج سلسلة متتابعة من البتات المشفرة وذلك باستخدام متتابعة شبه عشوائية من المفتاح [٢٦] .

أ. نظام التشفير الخلطي (Scrambling Cipher System) : وهو نظام معروف من أنظمة إخفاء الصورة ، ويعتمد على بعثرة نقاط الصورة بعد أن ترتب (توزع) هذه النقاط بصورة عشوائية [٢٥] . ويعد هذا النظام من بين الأنظمة الكفوءه في إنجاز عملية التشفير ، أي إن شفرة الخلط هي شفرة فاعلة في إخفاء معالم الصورة بشكل شبه تام أو تام .

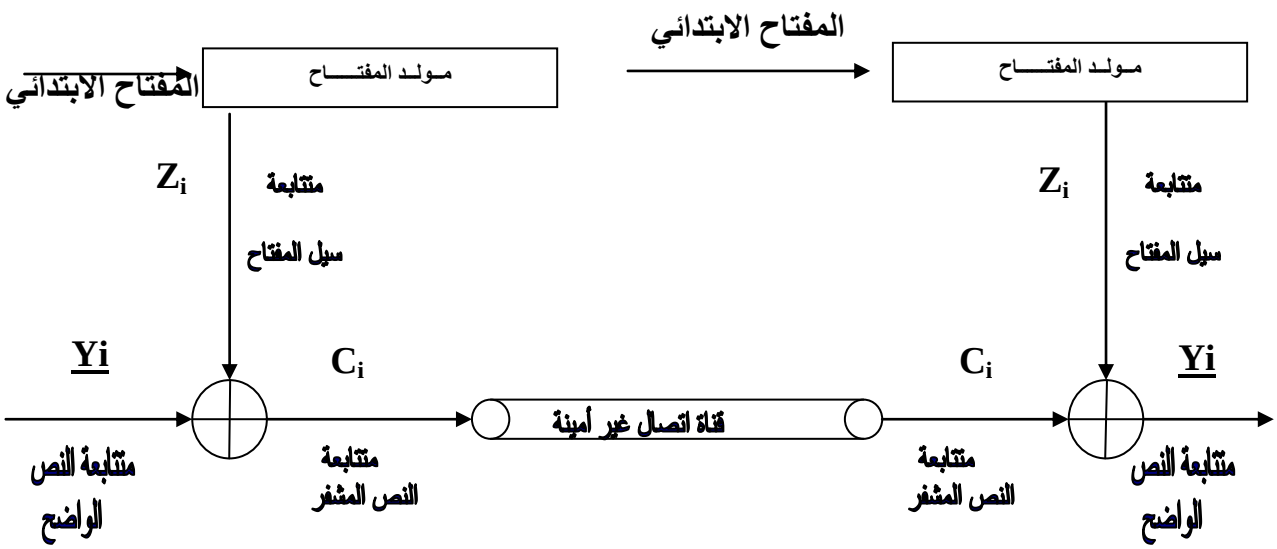
تتم معالجة التشفير بهذه الطريقة باستخدام دالة عشوائية (RANDOM) تقوم بتوليد الأعداد بصورة عشوائية وتستخدم فيما بعد كمفتاح للتشفير . وهذا يعني في الواقع إضافة الأعداد المولدة عشوائياً إلى بيانات الصورة وكما موضح في الشكل (١– ٨):



تتم معالجة فك التشفير بإزالة العشوائية واعادة نقاط الصورة إلى وضعها المرتب الأصلي وبذلك تسترجع الصورة .

ب- نظام التشفير الانسيابي الخطي (Linear Stream Cipher Processor) : يعد نظام التشفير الانسيابي من الأنظمة المهمة جداً لضمان أمنية البيانات ، حيث يتم جمع متتابعة شبه عشوائية (والتي تمثل سلسلة متتابعة المفتاح) جمعاً ثنائياً (للمعيار٢) مع متتابعة النص الواضح الثنائية لانتاج متتابعة النص المشفر [٢٧].

يتم التشفير بهذا النظام بتاً بعد بت مع استخدام دالة تشفير متغيرة زمنياً [٢٦]، وكما موضح في شكل (١ - ٩):



شكل (١ - ٩) نظام التشفير الانسيابي الخطي

تشترك معظم خوارزميات التشفير الانسيابي في استخدامها لمسجلات الإزاحة ذوات التغذية المرتدة الخطية (Linear Feedback Shift Register) التي تولد متتابعات

بدورات طويلة وتستخدم بتوليد مفتاح التشفير الانسيابي [٢٤].ويتكون كل مسجل إزاحة من [٢٩,٢٨] :

١. عدد (n) من المراحل (n stages) والتي تحتوي عند الإنشاء على مفتاح التشفير الابتدائي.

٢. دالة ربط خطية وهي الدالة البوليانية (XOR).

٣. يمكن الحصول على المخرجات (Outputs) من أي مرحلة من مراحل المسجل .

٤. يتم التعامل مع القيم على أساس ثنائي (Binary).

ويكون هدف مسجل الإزاحة تحقيق أعظم طول للمتتابعة ويمكن الحصول على طول المتتابعة من المعادلة الآتية:

$$L = ٢^{n} - ١ \quad \ldots (١١-١)$$

حيث L طول المتتابعة ، n عدد مراحل المسجل .

هناك نوعان من معالجات التشفير الانسيابي ، هما المعالج الخطي والمعالج اللاخطي . حيث تتكون المعالجات الخطية من مسجل إزاحة ذي تغذية مرتدة خطية (LFBSR) بطول معين ودالة مزج (تشفير) بوليانية خطية (XOR) ، ترتبط مراحل معينة من مسجل الإزاحة باستخدام دالة التغذية المرتدة الخطية، أما بالنسبة إلى المعالجات اللاخطية فيوجد اتجاهان لبنائهما: هما تقنية التوحيد و تقنية الترشيح[٣٠] .

هنالك ضرورة لامتلاك مفاتيح التشفير الانسيابي خواص عشوائية (يعني عدم التمكن من توقع المتتابعة بمعرفة جزء منها)، أي أنها تحقق خاصية عدم التنبؤ بسبب عدم وجود أي علاقة رياضية بين عناصر المتتابعة . وبذلك فان محلل الشفرة (عند معرفته جزء من متتابعة التشفير) لا يستطيع التوصل لأجزاء المتتابعة الأخرى [٢٦] .

ومن محاسن هذا النظام عدم تضاعف الأخطاء عند حدوثها ، وسهولة الاستخدام وسرعة التنفيذ ويتم التشفير وفق الصيغة الآتية:

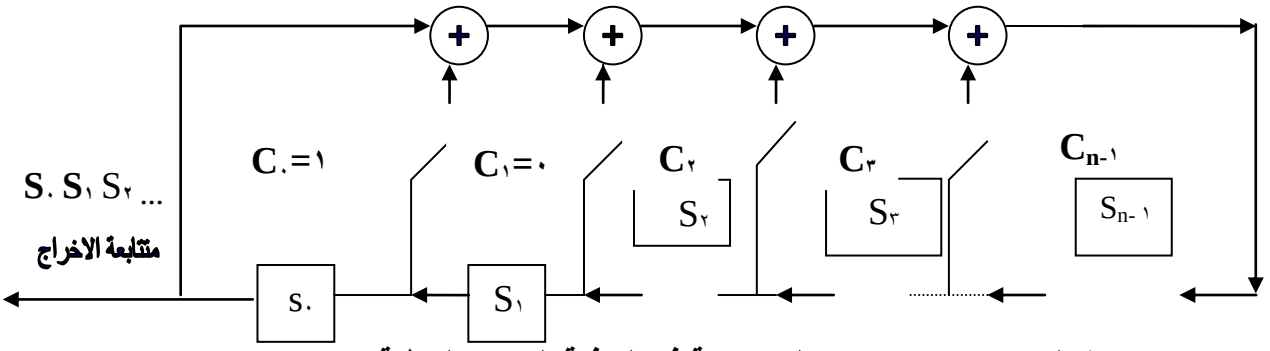
$$Ci = Xi \oplus Ki \quad \ldots(١٢-١)$$

حيث Ci بت من بتات الصورة المشفرة ، Xi بت من بتات الصورة الأصلية ، Ki تمثل بت من بتات المفتاح والرمز $\oplus$ يعني الدالة البوليانية XOR .

يدعى مسجل الإزاحة بمسجل الإزاحة ذي تغذية مرتدة خطية إذا مثلت دالة التغذية المرتدة الخطية بالمعادلة الآتية :

$$S_n=f(S_o, S_1,\ldots,S_{n-1}) = C_o S_o \oplus C_1 S_1 \oplus \ldots \oplus C_{n-1} S_{n-1} \quad \ldots (١٣-١)$$

حيث إن المعاملات Ci هو معاملات التغذية المرتدة الخطية ، وعندما تأخذ القيمة صفراً فأن هذا يعني عدم وجود اتصال وعندما تكون هذه القيمة واحداً يعني وجود اتصال[٢٨] ، وكما موضح في الشكل (١ - ١٠)



شكل (١ - ١٠) مسجل الإزاحة ذو التغذية المرتدة الخطية

ويوصف أي مسجل إزاحة ذي تغذية مرتدة خطية بالمعادلة الآتية :

$$f(X) = C_o \oplus C_1 X \oplus C_2 X^2 \oplus \cdots \oplus C_{n-1} X^{n-1} \oplus X^n \quad \cdots (١٤-١)$$

ج- نظام التشفير الانسيابي باستخدام الحقل العشوائي : جميع الأنظمة التي تم الحديث عنها هي تطبيق أحادي الأبعاد بما فيها نظام التشفير الانسيابي الخطي , في حين إن نظام التشفير باستخدام الحقل العشوائي هو تطبيق ثنائي الأبعاد للتشفير الانسيابي الخطي[٢٥]. ويقدم طريقة لتشفير الصورة الثنائية أي تلك التي تكون نقاطها أما سوداء أو بيضاء ويرمز لها بالقيم (٠ , ١) على التوالي .

نفترض إن الصورة هي $m \times n$ من النقاط ، ولدينا حقل عشوائي يتكون من $m \times n$ من النقاط وان هذا الحقل قد تولد بمساعدة مسجلات الإخراج الخطية، ويستخدم هذا الحقل كمفتاح يتم بوساطته تشفير الصورة الواضحة، وحسب الآتي:

- إذا كانت قيمة النقطة في الصورة الواضحة (M) هي١ ، فان النقطة التي تقابلها في الصورة المشفرة (C) ستكون النقطة المقابلة في الحقل العشوائي (K).

ويمكن التعبير عنها بالصيغة المنطقية آلاتية :

$$C = (M \wedge K) \quad \dots (١٥ - ١)$$

حيث $\wedge$ تعني الدالة البوليانية (AND).

ـ إذا كانت قيمة النقطة في الصورة الواضحة (M) هي ٠، فان النقطة في الصورة المشفرة تكون مساوية إلى مكملة النقطة المقابلة من K .

ويعبر عنها بالصيغة المنطقية الآتية :

$$C = \bar{}(M \vee K) \quad \dots (١٦ - ١)$$

حيث $\vee$ تعني الدالة البوليانية (O R).

مثال : لنأخذ جزء من صورة ما، M وجزء مقابل من الحقل العشوائي K

M: ١ ٠ ١ / ٠ ١ ٠ / ١ ٠ ١

K : ٠ ٠ ١ / ١ ٠ ٠ / ١ ١ ٠

فان المواقع في M التي تحتوي l ستكون قيمتها في الصورة المشفرة تساوي قيمة K المقابلة

C: ٠ ١ ١ / ٠ ٠ ١ / ١ ٠ ٠

والمواقع في M التي تحتوي القيمة ٠ ستكون قيمتها في الصورة المشفرة تساوي مكملة قيمة K المقابلة , وان الصورة المشفرة **C :**

ونلاحظ عدم وجود تطابق بين نقاط الصورة المشفرة ونقاط الصورة الأصلية. ويمكن فك شفرة الصورة وذلك بعكس العملية :

ـ في مواقع K التي تحتوي ١ فان القيمة المقابلة لـ C تبقى بدون تغيير في الصورة بعد فك التشفير . ويمكن التعبير عنها بالعلاقة الآتية.

$$M = (K \wedge C) \quad \dots (١٧ - ١)$$

حيث $\wedge$ تعني الدالة البوليانية (AND).

ـ في مواقع K التي تحتوي ٠ فان القيمة بعد فك الشفرة تساوي المكملة للنقطة المقابلة من C .

$$M = -(K \vee C) \quad \dots (١٨ - ١)$$

حيث $\vee$ تعني الدالة البوليانية (O R).

وبذلك ستكون M بعد فك التشفير كما يأتي :

M: | ١ ٠ ١ |
| ٠ ١ ٠ |
| ١ ٠ ١ |

٤.١ معالجة الصورة (Image Processing)

معالجة الصورة هي عملية معاملة (manipulating) الصورة أي فحصها والتأثير عليها من قبل الأشخاص باستخدام الحاسوب , تطورت أغلب تقنيات ووسائل معالجة الصورة استجابة لثلاث مشاكل أساسية [٨,٣] :-

- رقمنة وترميز الصورة (Image Digitizing and Coding)
- تحسين وإصلاح الصورة (Image Enhancement and Restoration)
- تجزئة ووصف الصورة (Image Segmentation and Description)

١.٤.١ تقنيات معالجة الصورة (Image Processing Techniques)

أولا"- النمذجة والتكمئة (Sampling and Quantization)

لأجل معالجة الصور حاسوبياً يجب رقمنتها (Digitizing)، والتعامل معها كمصفوفات من الأرقام محدودة الأطوال[٣٢,٣١] ,وتحصل هذه الرقمنة بوساطة نمذجة (Sampling) الصورة على شبكة متقطعة (Discrete) ومن ثم تكمئة (Quantization) هذه العينات باستخدام عدد محدد من البتات [٣٣] . حيث إن الطريقة المألوفة للنمذجة هي استخدام مصفوفات مربعة من النقاط ، وبتطبيق عملية التكمئة على تلك العينات نحصل على مجموعة متقطعة من قيم المستويات الرمادية(Gray-Levels) متساوية المسافة وقيمها صحيحة [٣] .

ثانياً – تحسين الصورة (Image Enhancement)

إن الهدف الرئيس من تقنيات التحسين هو معالجة صورة ما ، بحيث تكون النتيجة أكثر ملائمة من الصورة الأصلية لتطبيق محدد. على سبيل المثال الطريقة التي تصلح لتحسين صورة قمر صناعي قد لا تكون مناسبة لتحسين صورة طبية ,أي صممت تقنيات التحسين حسب خصائص نظام الرؤية البشري في معالجة الصور [٣٤].

يمكن تقسيم طرائق تحسين الصورة إلى قسمين : طرائق المجال الترددي (Frequency Domain) أي الأساليب المعتمدة على محول فوريير (Fourier Transform) للصورة المراد معالجتها. وطرائق المجال الحيزي (Spatial Domain) أي

الأساليب المعتمدة على معالجة عناصر الصورة (النقاط) مباشرة ، أي تعمل في مستوى الصورة نفسه [٣٦,٣٥]. ومن هذه الطرائق:

- تنعيم الصورة (Image Smoothing)

هو أحد أساليب المجال الحيزي في تحسين الصورة وتستخدم عمليات التنعيم لتقليل الضوضاء (Noise) [٣٧]، التي يمكن أن تكون موجودة في الصورة الرقمية وهي نتيجة لنظام نمذجة رديء أو قناة اتصال رديئة [٣٨].

أ ـ ترشيح الامرار الواطئ (Lowpass Filtering)

يستخدم هذا الترشيح للتشذيب وإزالة الضوضاء لصورة ما [٣٩]. يعمل التشذيب على إزالة التفاصيل التي تعتبر صغيرة بالنسبة إلى الصورة ككل ، وبذلك فإن ترشيح الامرار الواطئ لا يظهر حواف الصورة وكذلك التفاصيل الحادة الأخرى[٤٠] . يسمى هذا الترشيح معدل المجاورات (Neighborhoods Averaging) لأنه يأخذ قيمة معدل المجاورات للسوية الرمادية في كل نقطة [٤٢,٤١] .

ب ـ الترشيح الأوسطي (Median Filtering)

إن أحد الصعوبات الأساسية لطريقة التنعيم السابقة إنها لا تظهر التفاصيل الحادة (Sharp) ، ولتقليل الضوضاء تستخدم طريقة الترشيح الأوسطي التي تقوم بتبديل السوية الرمادية في كل نقطة بوسيط (Median) المستويات المجاورة بدلاً من المعدل[٤٣] . أن الوسيط لمجموعة قيم يقسمها بحيث أن نصف القيم تكون اقل منه والنصف الآخر تكون أكبر منه . ولإنجاز هذا الترشيح يجب أولا ترتيب قيم النقطة ومجاوراتها ومن ثم تحديد الوسيط . أن الوظيفة الأساسية للترشيح الأوسطي هي إجبار النقاط ذات الإضاءة المختلفة لتكون اكثر شبهاً لمجاوراتها [٣٩] .

- إزالة الضوضاء (Noise Removal)

تؤدي عملية رقمنة الصورة إلى إدخال بعض الاختلافات العشوائية على قيم النقاط(Pixels) ، وهذه تسمى الضوضاء (Noise) [٣٩]، فإذا كانت ضوضاء الصورة قليلة فإنها عادة ليست مشكلة وإذا كانت كثيرة ستكون الصورة خشنه (Rough) ، أما إذا كانت الضوضاء اكبر من الصورة نفسها فلا يمكن تمييز الصورة . لتقليل الضوضاء تستخدم عملية تحسين الرقمنة، وعادة تكون باستخدام المعدل الموضعي (Local Averaging) والذي يكون تأثيره الجانبي تنعيم الصورة الناتجة .

تكمن الصعوبة في تحديد أي الصفات لصورة ما، هل هي أصلية أو ناتجة من الضوضاء وبصورة عامة فإن الاختلافات في شدة الإضاءة (اللمعان) واللون ستكون تدريجية في الصورة الأصلية ، لذا فان تباين أي من النقاط عن مجاوراتها يمكن أن يعزى إلى الضوضاء.

إن الفكرة الأساسية لخوارزميات إزالة الضوضاء هي إبدال النقاط الشاذة أو المغايرة بقيم مشتقة من النقاط المجاورة [٤٤,٧].

- نماذج الضوضاء (Noise Models)

إن ابسط نموذج ضوضاء هو الضوضاء الجمعي (Additive Noise) . حيث أن كل نقطة في الصورة المنظورة g (x, y) هي نموذج لجمع الصورة الأصلية f (x, y) مع الصورة ذات الضوضاء η (x,y)، [٤٥] ، وفي اغلب الحالات تكون الضوضاء متغيرا" عشوائيا" ذا وسط حسابي يساوي صفرا" وتوزيع كاوس (Gaussian Distribution) .

يمكن توضيح مستوى الضوضاء وذلك بوساطة التباين، على سبيل المثال إذا تم رقمنة الصورة بقيم في المدى ٢٥٥ -- ٠ ، فان ضوضاء كاوس الجمعي ذا σ_n^2= ١ غالباً ما يصعب الكشف عنه بشكل منظور ، بينما في مستويات الضوضاء المعتدلة ذات σ_n^2 = ١٠٠ سوف تكون الصورة خشنة ، أما المستويات العالية ذات σ_n^2 = ١٠٠٠٠ فستحجب الصورة الواضحة [٣٥].

٢.٤.١ هيئات ملفات الصور (Image Files Formats)

هنالك عدة أساليب لخزن بيانات الصور في ملفات [٤٧,٤٦] ، وتمثل بالصيغ الآتية :

- صيغة الملف PCX (PC Paint Brush File Format) والتي تعتبر اقرب صيغة لتطبيق الحاسوب الشخصيPC.
- صيغة الملف GIF (Graphics Interchange File Format) والتي تستخدم غالبا" مع الصور المضغوطة .
- صيغة الملف BMP (Bit Map Paint Brush File Format) والتي تعتبر قياسية في تطبيقات أل Windows [٤٨,٣٤] .

وهي صيغة عامة الأغراض وصممت لتلائم كافة الصور ، حيث يتم خزن صور هذه الصيغة بسطور مرتبة من الأسفل إلى الأعلى (Bottom – Up)[٣٢,٣١]، ويتضمن هيكل هذه الصيغة [٥٠,٤٩]:

- مقطع رأس ملف أل B M P (BMP File Header Block)
- مقطع رأس المقابلة (Bitmap Header Block)
- مقطع جدول اللون (Color Table Block)
- مقطع بيانات المقابلة (Bitmap Data Block)

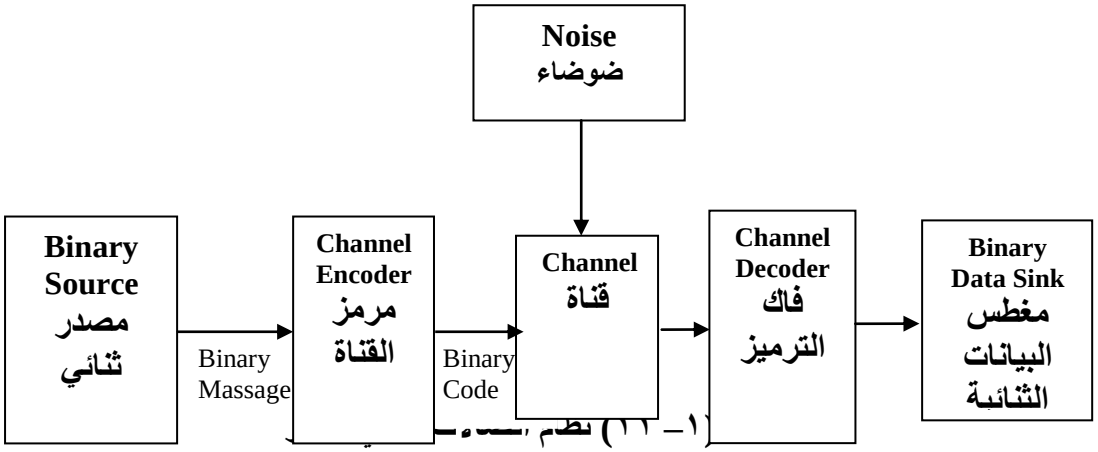
يشار إلى عدد الألوان في صورة ما بعدد البتات المطلوبة لخزن معلومات اللون[٥١,٣٤] . فالصورة الأحادية (Monochrome) تسمى صورة أحادية البت (Bit Image – ١) لأن كل نقطة من هذه الصورة تتطلب بت واحد من المعلومات، والصور ذات ١٦ لونا" تسمى صوراً رباعية البت (Bit Image – ٤) لأن كل نقطة تتطلب ٤ بت من المعلومات . وهكذا فالصور ذات

٢٥٦ لون تسمى صوراً ثمانية البت (Bit Image – ٨) حيث كل نقطة تتطلب ٨بت من المعلومات[٥٣,٥٢] . يرافق الصورة الملونة جدول الألوان (RGB) الأحمر والأخضر والأزرق ، فمثلاً الصور ذات ٢٥٦ لون يرافقها جدول يحتوي ٢٥٦ مدخل ويعني ٢٥٦ لون منفصل ، أي إن كل نقطة في الصورة هي إحدى قيم أل ٢٥٦ لون[٥٥,٥٤].

١.٥ الترميز (Coding)

من أجل الحصول على أنظمة اتصالات ذات درجة معوليه عالية تستخدم رموز كشف/ تصحيح الأخطاء (Error Detection / Correction) , حيث تتعرض البيانات المنقولة عبر قنوات الاتصال إلى تأثيرات الضوضاء وتسبب حدوث الأخطاء في هذه البيانات أي تكون البيانات المرسلة مختلفة عن البيانات المسترجعة منها . لذلك ظهرت عدة تقنيات للسيطرة على هذه الأخطاء ، ومنها رموز كشف / تصحيح الأخطاء [٥٦,١٠] .

يوضح الشكل (١ -١١) نظام اتصالات رقمي يستخدم رموز كشف / تصحيح الأخطاء للسيطرة على الأخطاء .



(١– ١١) نظام

يقوم المرمز(Encoder) باستلام الرسالة وحسب قواعد معينه يقوم بإضافة عدد من البتات الفائضة (Redundant Bits) التي بوساطتها يتم الكشف عن وجود الأخطاء وتصحيحها[٥٧,١٤] ، أما فاك الترميز (Decoder) فيقوم بالعملية المعاكسة ، إذن الترميز هو عملية إضافة عدد من البتات للرسالة بشكل ملائم وبوساطتها يمكن تصحيح الأخطاء (إن حصلت) في الرسالة [٥٨,١٢] .

١.٥.١ الرموز الكتلية الخطية الثنائية (Binary Linear Block Codes)

تعتبر رموز الكتلية الخطية (LBC) أحد الأصناف المهمة لرموز كشف / تصحيح الأخطاء التي تقسم المعلومات إلى كتل بأحجام متساوية (Message blocks) بحجم K مرتبة ثنائية ، لذلك سيكون عدد كتل الرسالة المحتملة ذات الحجمm هو ٢^m . يقوم المرمز باستلام كل كتلة على حدة وتحويلها إلى كلمة رمز Code word بحجم n حيثn > m و n يسمى طول الرمز Code)

(Length أو طول الكتلة(Block Length) [٥٩,٥٨] ، لذلك سوف يكون لكل كلمة من كلمات الرسالة رمزا" خاصا" بها وبالتالي سيكون عدد كلمات الرمز هو ٢^m أن هذه المجموعة المتكونة من ٢^m كلمة رمز كل واحدة بطول n تسمى الرمز الكتلي (n, m) . وتتميز الرموز الكتلية الخطية بأنه عند جمع أي كلمتين من كلمات الرمز تعطي كلمة رمز أخرى[٦٠,٥٦].

- بتات الفحص (Check Bits)

إن اكتشاف الخطأ وتصحيحه عادة يحصل بوساطة بتات الفحص ، والتي تضاف إلى بتات المعلومات الأصلية لكل كلمة من الرسالة , وبصورة عامة تلحق بتات الفحص k ببتات المعلومات m لتنتج كلمة رمز n أي $n = m + k$ من البتات ويتم إرسال كلمة الرمز هذه إلى المستلم , فإذا كانت الكلمة المستلمة غير متفق عليها فسيعدها المستلم كلمة خاطئة وبإضافة بتات فحص أكثر يستطيع المستلم تصحيح الأخطاء إضافة إلى اكتشافها ويحصل هذا التصحيح بان يختار المستلم كلمة الرمز الصحيحة التي تكون أقرب(Closest) واحدة للكلمة المستلمة [١٢,٦]. ويتم تغيير الأخطاء فإذا كانت ٠ تحول إلى ١ وبالعكس إذا كانت ١ تحول ٠.

٢.٥.١ عملية الترميز (Coding Operation)

تتلخص عملية الترميز بضرب بتات الرسالة (Message Bits) بالمصفوفة المولدة (Generator Matrix) ، أي

$$C = M * G \qquad \ldots(١٩-١)$$

حيث C هي كلمة الرمز وM هي بتات المعلومات وG هي المصفوفة المولدة .

تتكون المصفوفة المولدة (G) من جزء ين وهما مصفوفة الوحدة (Identity Matrix) التي تحتوي على k صف وk عمود ، وهذه المصفوفة تولد بتات المعلومات نفسها. أما الجزء الثاني فهو عبارة عن مصفوفة (P) ذات k صف و(n–k) عمود وهي مصفوفة فحص التماثل (Parity Check Matrix) [٥٨,١٣] .

$$G = (I_k \quad P) \qquad \ldots (٢٠-١)$$

حيث G المصفوفة المولدة ، I_k مصفوفة الوحدة و P مصفوفة فحص التماثل.

٣.٥.١ عملية فك الترميز (Decoding Operation)

بعد الانتهاء من عملية الترميز وإرسال الكلمات المرمزة عبر قناة الاتصال ذات الضوضاء المحتملة، تأتي مرحلة فك الترميز للكلمات المرسلة. تتم عملية فك الترميز باستخدام مصفوفة فحص التماثل (P) ولكن بترتيب مختلف[٥٦]، وكالآتي:

$$H = [P^T \quad I_{n-k}] \qquad \ldots (٢١-١)$$

حيث H مصفوفة فحص التماثل المستخدمة في عملية فك الترميز، P^T المبدلة لمصفوفة فحص التماثل، و I_{n-k} مصفوفة الوحدة التي تحتوي على n-k صف و n-k عمود.

ولفحص الكلمة المرمزة المستلمة يتم استخدام المعادلة الآتية:

$$S = R * H^T \qquad \ldots(٢٢-١)$$

حيث S يسمى السيندروم (Syndrome) لكلمة الرمز المستلمة، R كلمة الرمز المستلمة، H^T المبدلة لمصفوفة فحص التماثل المستخدمة لفك الترميز(H)[٥٨].

فإذا كان $S = ٠$ تكون كلمة الرمز المستلمة صحيحة ولا يوجد خطأ، أما إذا كان $S \neq ٠$ فستكون المعادلة بالشكل الآتي:

$$R = E \oplus C \qquad \ldots(٢٣-١)$$

حيث R كلمة الرمز المستلمة، E متجه الخطأ (Error Vector)، و C كلمة الرمز.

من ملاحظة المعادلة (١-٢٣)، يتضح أن هناك خطأ في كلمة الرمز المستلمة وذلك لوجود متجه الخطأ. وبإيجاد متجه الخطأ المقابل للسيندروم المحسوب يمكننا اكتشاف كلمة الرمز المرسلة أي بيانات الرسالة الصحيحة (الصورة المرسلة)، وذلك بعد تصحيح هذا الخطأ وابدال ١بـ ٠ و٠ بـ ١[٦٠]. حيث يمكن التعبير عن المعادلة (١-٢٢) بالمعادلة الآتية:

$$S = E_i * H^T \qquad \ldots(٢٤-١)$$

فيكون العنصر i من E مساويا" لـ ٠ إذا كان العنصر المقابل من R هو نفسه في C، ويكون مساويا" لـ ١ إذا كان العنصر المقابل من R يختلف عن العنصر في C، لكل i حيث ١ $i = ١,٢,\ldots,n$ [٥٨].

الفصل الثاني

التطبيق العملي للنظام المقترح

١.٢ تصميم نظام معالجة الصور المقترح

يقوم نظام معالجة الصور المقترح بمعالجة الصور المخزونة في ملفات نوع BMP من خلال محاكاة نظام اتصالات يتضمن عمليات التشفير والترميز ومن ثم فك التشفير وفك الترميز وإجراء التحسين (إذا كانت هنالك ضرورة للتحسين) للصور المدخلة والصور الناتجة من المعالجة ويوضح الشكل (٢-١) مخطط كتلي للنظام المقترح.

وفيما يأتي استعراض لوحدات النظام

أ ـ مصدر الإشارة الصورية:

وهو جهاز توليد الإشارة الصورية وقد يكون أحد مصادر الإشارة الصورية هو الماسح (Scanner) أو الكاميرا الرقمية (Digital Camera) أو القمر الاصطناعي (Satellite) [٥]، وسيتم التعامل في النظام المقترح مع الصور المخزونة في الملفات بغض النظر عن مصدر الإشارة الصورية.

ب ـ تحسين الصورة:

تأتي الحاجة إلى هذه المعالجة نتيجة للتشويه الذي تتعرض له الصورة والذي يكون ناتجا" عن استلام الصورة من المصدر أو ناتجا"عن التشفير والترميز، أو التشويه الذي يحصل عند نقل الصورة عبر قناة الاتصال ، لذلك تم استخدام هذه الوحدة في اكثر من مكان عند تنفيذ

النظام وقد تم اقتراح استخدام أنواع من التقنيات لتحسين هذه الصورة وحسب متطلبات النظام والظروف المسببة للتشويه ، وهذه التقنيات هي:-

أولا". خوارزمية تحسين الصورة باستخدام مرشح المتوسط

Image Enhancement Algorithm Using Mean Filter

```
Input: B Matrix
Output: C Matrix
  Begin
   {Put BMp File Data in B Matrix}
   For I=bmph.hgt – ١ downto  ١ Do
      For J=  ١ to bmph. Wid – ١ Do
          Sum= Sum+B [I- ١, j- ١]+B [I- ١, j]+B [I- ١, j+ ١]+
                B [I, J- ١]+B [I, j]+B [I, j+ ١]+
                B [i+ ١,j- ١]+B [i+ ١,j]+B [i+ ١,j+ ١]
         C [I, j]=sum div ٩
     Sum= ٠
End of algorithm
```

ثانيا". خوارزمية تحسين الصورة باستخدام مرشح الامرار الواطئ

Image Enhancement Algorithm Using Lowpass Filter

```
 Input: B Matrix
Output: C Matrix
   Begin
     Mask is ٣*٣ one's matrix
    {Put BMp File Data in B Matrix}
   For I= bmph.ght- ١ downto  ١ Do
    For J= ١ to bmph. Wid – ١ Do
      Begin
     For k=  ١ to ٣ Do
       For d=  ١ to ٣ Do
          Sum= Sum+b[I,j]*Mask [I+k,j+k]
     C [I, j]=sum div ٩
  Sum= ٠
End of algorithm
```

ثالثا". خوارزمية تحسين الصورة باستخدام المرشح الأوسطي

Image Enhancement Algorithm Using Median Filter

```
Input: B Matrix
Output: C Matrix
```

Begin
{Put BMp File Data in B Matrix}
For I=bmph.hgt – ١ downto ١ Do
For j= ١ to bmph. Wid – ١ D٠
For k= ١ to ٣Do
For d= ١ to ٣Do
{Sort the Pixel values in the Filter in increasing or decreasing Order and Picking the middle value, which replaced by input Pixel}
End of algorithm

ج ـ المشفر:

إن أحد أهداف البحث هو محاكاة تشفير بيانات الصورة باستخدام أنظمة مختلفة وتحليل نتائج كل نظام وكما يأتي:

أولا". نظام التشفير الجمعي

تمت الإشارة في الفصل الأول إلى انه يمكن التعبير عن عملية التشفير الجمعي باستخدام المعادلة (١-٣) ، وفي النظام المقترح فان النص الواضح يمثل الصورة المراد تشفيرها وان عدد مفاتيح التشفير المستخدمة هي (١...٢٥٥) أي ٢٥٥ مفتاح تشفير، وفيما يأتي خوارزمية التشفير الجمعي للصورة

Image Additive Enciphering Algorithm
Input: Image File
Output: Encipher Image File
Let k= key {١ ≤ key ≤ 255}
Begin
While not eof (Input File) Do
Begin
Read (Input File, byte)
Encipher byte = (byte+k) Mod ٢٥٦
Write (encipher Input File, Encipher byte)
End
End of algorithm

ثانيا". نظام التشفير الضربي

كما تم توضيحه في الفصل الأول فان عملية التشفير الضربي تتم باستخدام المعادلة (٥-١) حيث إن عدد الهجائية للخوارزمية n المشار إليه في المعادلة قد استخدم في النظام المقترح ليمثل عدد ألوان الصورة أي ٢٥٦ =n، أما مفتاح التشفير الضربي(k) فيمكن إيجاده باستخدام المعادلة الآتية:-

$$GCD\ (k, n) = ١ \qquad \ldots(١-٢)$$

فإذا تم التعويض عن n بـ ٢٥٦ سينتج ١٢٧ مفتاح للتشفير، (كما سيوضح في الفصل الثالث).
وفيما يأتي خوارزمية التشفير الضربي للصورة:

Image Multiplicative Enciphering Algorithm
Input: Image File
Output: Encipher Image File
Let K=Key { ٣≤ key ≤ ٢٥٥, key odd number}
Begin
While not eof (Input File) Do
Begin
Read (Input File, byte)
*Encipher byte = (byte*k) Mod ٢٥٦*
Write (Encipher Input File, Encipher byte)
End
End of algorithm

ثالثا". نظام التشفير الهجين

يجمع هذا النظام كلا" من التشفير الجمعي والتشفير الضربي ، كما موضح في المعادلة رقم (١ – ٨) ، حيث تم استخدام ألوان الصورة لتمثل هجائية التشفير n في النظام المقترح .

يستخدم التشفير الهجين مفتاحي التشفير الجمعي والضربي ، وبذلك فأن التشفير الهجين للصورة يمتلك ٣٢٣٨٥ (١٢٧ × ٢٥٥) مفتاح تشفير.

وفيما يأتي خوارزمية التشفير الهجين للصورة :

Image Affine Enciphering Algorithm

Input: Image File

Output: Encipher Image File
Begin
While not eof (Input File) Do
Begin
Read (Input File, byte)
Let $K_٢$= key { ١ ≤key ≤ ٢٥٥, Additive key}
Call GCD Algorithm {to generate multiplicative Key $K_١$}
*Encipher byte = (byte * $K_١$ + $K_٢$) Mod ٢٥٦*
Write (Encipher Input File, Encipher byte)
End

End of algorithm

رابعا". نظام التشفير الخلطي

يعمل هذا النظام على تشفير الصورة عن طريق بعثرة نقاطها باستخدام دالة عشوائية (RANDOME) وكما موضح في الخوارزمية الآتية :

Image Scrambling Enciphering Algorithm

Input: Image File

Output: Encipher Image File

Begin

Let R is Array of Randomize number

While not eof (Input File) Do

Begin

Read (Input File, byte)

Encipher byte = (byte + R) Mod ٢٥٦

Write (Encipher Input File, Encipher byte)

End

End of algorithm

خامسا". نظام التشفير الانسيابي الخطي

يتم العمل في هذا النظام بجمع متتابعة شبه عشوائية (التي تمثل مفتاح التشفير المتولد باستخدام مسجل الإزاحة ذي التغذية المرتدة الخطية) جمعاً ثنائياً (للمعيار٢) مع متتابعة النص الواضح الثنائية لانتاج متتابعة النص المشفر كما موضح في المعادلة (١ – ١٢) ، وحيث إن العمل في هذا البحث يعتبر النص الواضح صورة لذلك فأن الناتج سيكون صورة مشفرة . وكما مبين في الخوارزمية الآتية :

Image Linear Stream Enciphering Algorithm

Input: Image File

Output: Encipher Image File

Begin

While not eof (Input File) Do

Begin

Read (Input File, byte)

Convert byte to ٨ bits

Call linear key Generator Algorithm {to generate the key}

Encipher bit = bit XOR key

Write (Encipher Input File, Encipher bit)

End

End of algorithm

أما خوارزمية مولد المفتاح الخطي فهي كالأتي:

Linear key Generator Algorithm

Input: Initial key, No. Of stages (n)

Output: Linear stream key

Begin

Get connected stages by the linear function XOR

L = ٠

Repeat

Calculate feedback bits by linear function XOR

Shift the linear key one bit to right

Put the output in Array

L = L + l

Until (initial key = (current key) or (L = ٢^{n} – ١)

End of algorithm

أما خوارزمية القاسم المشترك الأعظم فهي كالأتي:

Greatest common Divisor Algorithm

Input: g ٠, g ١

Output: GCD

Begin

R = g ٠. Mod g ١

While (R< >o) Do

Begin

$g_0 = g_1$

$g_1 = R$

$R = g_0 \; Mod \; g_1$

End

$G C D = g_1$

End of algorithm

سادسا". نظام التشفير الانسيابي الخطي باستخدام الحقل العشوائي

وهو تطبيق ثنائي الأبعاد للتشفير الانسيابي الخطي حيث تشفر الصورة بالاعتماد على الحقل العشوائي المتولد من مسجلات الإزاحة الخطية الذي سيكون بمثابة مفتاح تشفير ، وذلك حسب الخوارزمية الآتية :

Image Linear Stream Enciphering Algorithm Using Random Field

Input: Image File

Output: Encipher Image File

Begin

While not eof (Input File) Do

Begin

Read (Input File, byte)

Convert byte to ٨ bits

Call linear key Generator Algorithm {to generate Random Field's Bits}

If (Input File, bit) = ١

Then (Encipher Input File, Encipher Bit) = key

Else (Encipher Input File, Encipher bit)= ١-key {key Complement}

Write (Encipher Input File, Encipher bit)

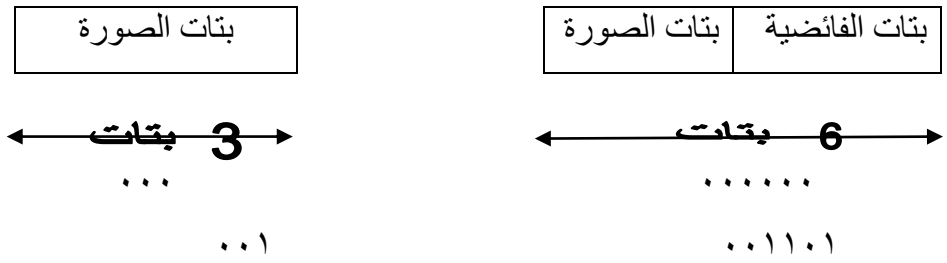
End

End of algorithm

د- المرمز:

بعد أن يستلم المرمز الصورة المشفرة يبدأ بإضافة عدد من البتات إلى بتات الصورة المشفرة وذلك لحمايتها من تأثيرات الضوضاء عند إرسالها عبر قناة الاتصال .

في البحث تم استخدام الرموز الكتلية الخطية (LBC) لكشف وتصحيح الأخطاء وكمثال على ذلك المرمز الذي يقسم سلسلة معلومات المصدر إلى كتل ذات ثلاثة أرقام يحول كل كتلة إلى رمز ذي ستة أرقام ، كما في الشكل رقم (٢-٢) .



الشكل رقم (٢-٢) تحويل المعلومات إلى رموز

تبين أول ثلاثة بتات في أي كلمة رمز بتات الرسالة أو الصورة (M) ، بينما آخر ثلاث بتات (والتي حددت بوساطة البتات الثلاثة الأولى) هي بتات الفائضية (U) ، والشيء المهم في عملية الترميز هو أيجاد مصفوفة فحص التماثل (parity Check Matrix) (p) لإيجاد المصفوفة G كما موضح في المعادلة رقم (١ - ٢٠) . حيث إن

المصفوفة G تستخدم لإيجاد كلمة الرمز (C) حسب المعادلة رقم (١ – ١٩) .

تتلخص عملية أيجاد مصفوفة فحص التماثل (p) بالخوارزمية الآتية :

Parity Check Matrix Algorithm

Input: ٢^{U} *of bits* *{U are Redundancy Bits}*

Output: P *{Parity Check Matrix}*

Begin

Label: Select U from ٢^{U}

Compute linear Sum (S ١) of columns

If S ١< > ٠ then Label

Else If ith column = jth column then Label

Else If ith column = ٠ then Label

Else if (I+(I+ ١)) < > I+ ٢ then Label {I's are matrix's rows}

Else Write P

End of algorithm

ولإيجاد كلمات الرموز (C) لملف الصورة المشفرة الذي تم إدخاله ، تطبق خوارزمية الترميز الآتية :

Coding Algorithm

Input: Encipher Image File

Output: Code Words File

Begin

Let n= ٦, k = ٣

While not eof (Encipher Input File) Do

Begin

Read (Encipher Input File Encipher byte)

Convert Encipher Input File on to ٣ bits Blocks

Let Block = M {M = array of [١ × ٣] }

Read M

Read G {The generator matrix [٣ × ٦] bits }

*Code = M * G*

Write (Code Words File, Code)

End

End of algorithm

هـ ـ فاك الترميز:

يعمل فاك الترميز على فك الرموز المرسلة عبر قناة الاتصال وذلك بعد تعرضها إلى الضوضاء المحتملة . ويتم العمل في هذا المعالج بمساعدة المصفوفة المشار إليها في المعادلة ٢١) (١ – . وباستخدام المعادلة (١ – ٢٢) يمكن فحص الكلمة المستلمة R ومن ثم العمل على كشف وتصحيح الخطأ (إن وجد) . حسب الخوارزمية الآتية:

Error Detection_ Correction Algorithm

Input: R, H {R is received word, H=[P^T I_{n-k}] }

Output: Correct Code Word

Begin

While not eof Encipher File Do

S=R×H^T {The Syndrome for Received Word (R)}

If S= ٠ then R= Code {Error Detection}

Else Find E Corresponding to S

Code R E {Error Correction}

End of algorithm

بعد ذلك تتم عملية فك الترميز واعادة ملف الصورة المشفرة وحسب الخوارزمية الآتية :

Decoding Algorithm

Input: Code Words File

Output: Encipher Image File

Begin

While not eof (Code Words File) Do

Begin

Read (Code Words File, Code)

Let M = ٣ bits blocks of Encipher Image File

*M = Code * G^T {G = Array [I_k ٠] of k × n bits}*

Convert M to bytes

Write (Encipher Image File, byte)

End

End of algorithm

و- فاك التشفير:

يبدأ عمل فاك التشفير بعد أن تم إرسال النص المشفر(الصورة المشفرة) عبر قناة الاتصال ، وذلك لمعرفة النص الواضح (الإشارة الصورية الواضحة) ومن ثم إرسالها إلى مستلم الإشارة الصورية للتعامل معها ، وقد تم استخدام خوارزميات عمليات فك التشفير لأنظمة التشفير المذكورة في هذا البحث وكالآتي:

أولا". عملية فك التشفير الجمعي

يمكن التعبير عن عملية فك التشفير الجمعي في النظام المقترح باستخدام المعادلة – ٤) (١ المشار إليها في الفصل الأول حيث إن n تمثل عدد ألوان الصورة ، k مفتاح تشفير الصورة ، C الصورة المشفرة و P هي الصورة بعد فك التشفير (الصورة الواضحة) . وكما مبين في خوارزمية فك التشفير الجمعي للصورة:

Image Additive Deciphering Algorithm
Input: Encipher Image File
Output: Decipher Image File
Begin
Let k = key { ١≤ key ≤ ٢٥٥}
While not eof (Encipher Image File) Do
Begin
Read (Encipher Input File, Encipher byte)
Decipher byte = (Encipher byte – k) mod ٢٥٦
Write (Decipher Input File, Decipher byte)
End
End of algorithm

ثانيا". عملية فك التشفير الضربي

تكون المعالجة هنا بعكس عمل نظام التشفير الضربي ، وذلك بتطبيق المعادلة (١ – ٦) والمعادلة (١ – ٧) المشار إليهما في الفصل الأول ، وحسب خوارزمية فك التشفير الضربي للصورة:

Image Multiplicative Deciphering Algorithm
Input: Encipher Image File

Output: Decipher Image File

Begin

While not eof (Encipher Image File) Do

Begin

Read (Encipher Image File, Encipher byte)

Call GCD Algorithm {to generate the key}

Read k^{-1} *{k * k* $^{-1}$ *= ١ mod n,* k^{-1} *is k inverse}*

*Decipher byte = (Encipher byte * k^{-1} *) Mod ٢٥٦*

Write (Decipher Image File, Decipher byte)

End

End of algorithm

ثالثا". عملية فك التشفير الهجين

يمكن معالجة فك التشفير الهجين بتطبيق المعادلة (١ – ٩) المشار لها في الفصل الأول ، وكما موضح في خوارزمية فك التشفير الهجين للصورة :

Image Affine Deciphering Algorithm

Input: Encipher Image File

Output: Decipher Image File

Begin

While not eof (Encipher Image File) Do

Begin

Read (Encipher Image File, Encipher byte)

Call GCD Algorithm {to generate to key (k ١)}

Read k_1 *, {*k_1 *** k_1^{-1} *mod n= ١}*

Read K_2 *{ ١ ≤* K_2 *≤ ٢٥٥}*

Read (Encipher Image File, Encipher byte)

Decipher byte = [(Encipher byte – k_2*) * k_1^{-1} *] Mod ٢٥٦*

Write (Decipher Image File Decipher byte)

End

End of algorithm

رابعا". عملية فك التشفير الخلطي

تكون هذه العملية على عكس عمل نظام التشفير الخلطي وذلك بحذف القيم العشوائية التي تولدت بوساطة دالة *Randomize* . وكما موضح في خوارزمية فك التشفير الخلطي للصورة:

Image Scrambling Deciphering Algorithm

Input: Encipher Image File

Output: Decipher Image File

Begin

While not eof (Encipher Image File) Do

Begin

Let R= RANDOMIZE

Decipher byte = (Encipher byte – R) Mod ٢٥٦

Write (Decipher Image File, Decipher File)

End of algorithm

خامسا". عملية فك التشفير الانسيابي الخطي

يتم العمل في هذا النظام بجمع متتابعة شبه عشوائية (التي تمثل مفتاح التشفير المتولد باستخدام مسجل الإزاحة ذي التغذية المرتدة الخطية) جمعاً ثنائياً (باستخدام الدالة الخطية XOR) مع المتتابعة الثنائية لقيم الصورة المشفرة لانتاج الصورة الواضحة . وكما مبين في خوارزمية فك التشفير الانسيابي الخطي للصورة:

Image Linear Stream Deciphering Algorithm

Input: Encipher Image File

Output: Decipher Image File

Begin

While not eof (Encipher Image File) Do

Begin

Read (Encipher Image File, Encipher bit)

Call linear key Generator Algorithm {to generate the key}

Decipher bit = Encipher bit XOR key

Convert bits to bytes

Write (Decipher Image File, Decipher byte)

End

End of algorithm

سادسا". عملية فك التشفير الانسيابي الخطي باستخدام الحقل العشوائي

تتم عملية فك التشفير في هذا النظام باستخدام العملية العكسية لعملية التشفير باستخدام عملية التشفير الانسيابي الخطي باستخدام الحقل العشوائي وذلك حسب الخوارزمية الآتية :

Image Linear Stream Deciphering Algorithm Using Random Field

Input: Encipher Image File

Output: Decipher Image File

Begin

While not eof (Encipher Image File) Do

Begin

Read (Encipher Image File, Encipher bit)

Call linear key Generator Algorithm {to generate Random Field's Bits}

I f k = ١ then (Decipher Image File , Decipher bit) =Encipher bit

Else

(Decipher Image File, Decipher bit) = ١- Encipher Bit

Convert bits to bytes

Write (Decipher Image File, Decipher byte)

End

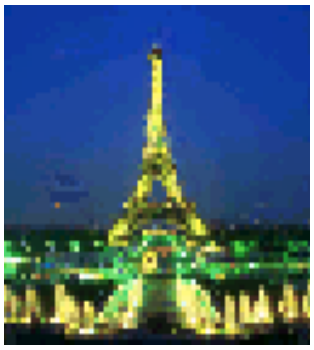
End of algorithm

الفصل الثالث

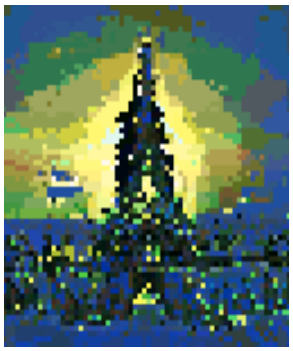
النتائج والمناقشة

١.٣ اختبار وتحليل عمل النظام المقترح

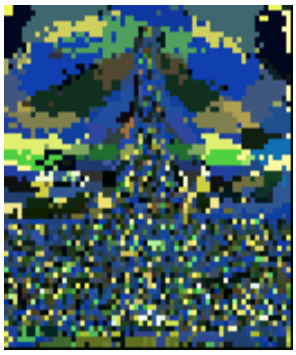
تم اختيار أثنى عشرة صورة مختلفة من ناحية درجة التعقيد واللون وكما موضحة في الشكل رقم (٣-١) لإجراء التجارب الاختبارية على تشفيرها من خلال استخدام خوارزميات التشفير / فك التشفير المختلفة والتي تم بناؤها ووصفها في الفصل السابق علما أن الصور قبل تشفيرها يمكن معالجتها بإحدى تقنيات تحسين الصورة المذكورة في الفصل الأول وهذه تتم عندما تحتوي الصورة المدخلة على ضوضاء وكالآتي.



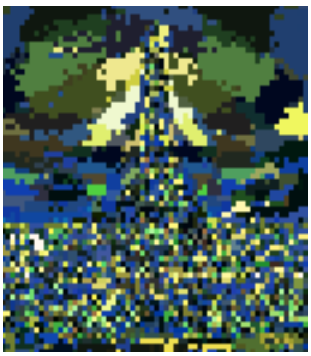
أ



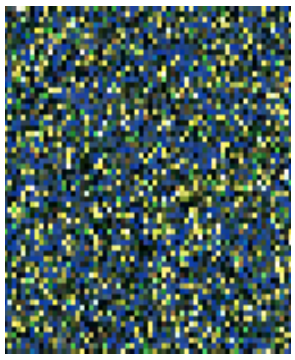
ب



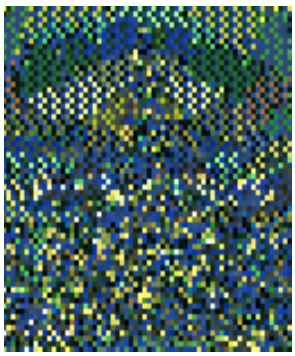
ج



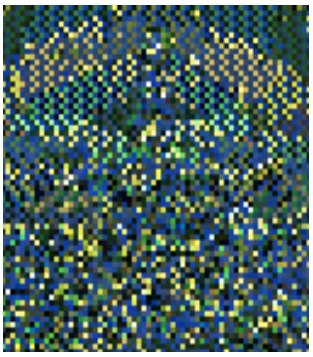
د



هـ



و



ز

ي

الشكل رقم (٣-١٣) تطبيق خوارزميات التشفير على الصورة رقم ٩

أ الصورة الملونة الواضحة

ب التشفير الجمعي باستخدام المفتاح ٨٩

ج التشفير الضربي باستخدام المفتاح ٨٩

د التشفير الهجين باستخدام المفتاحين ٨٩،٩٠

ه التشفير الخلطي باستخدام الدالة RANDOMIZE

و التشفير الانسيابي الخطي باستخدام الدالة البوليانية XOR

ز التشفير الانسيابي الخطي باستخدام الحقل العشوائي

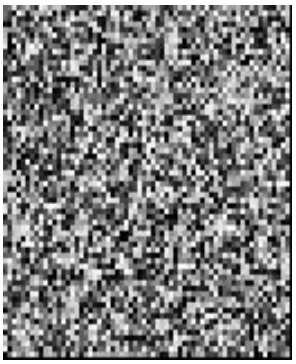
ي فك التشفير وإرجاع الصورة الواضحة بعد تطبيق معالجات فك التشفير لمعالجات التشفير المستخدمة

أ

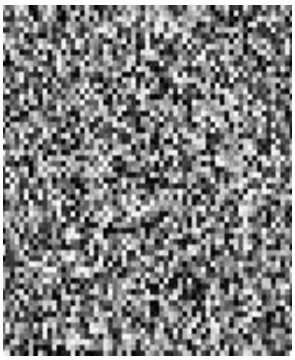
ب

ج

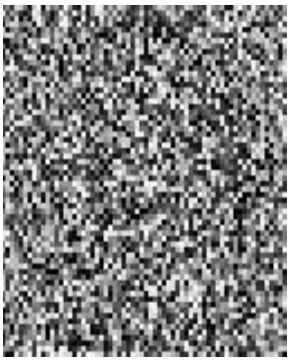
د



هـ



و



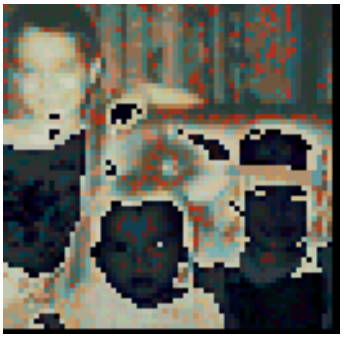
ز

ي

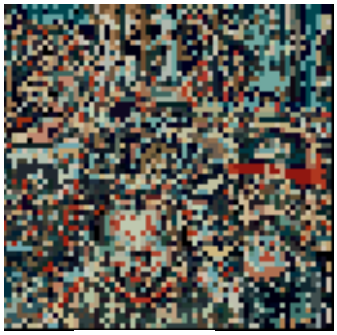
الشكل رقم (٣-٥) تطبيق خوارزميات التشفير على الصورة رقم ٣

أ الصورة ذات التدرجات الرمادية الواضحة
ب التشفير الجمعي باستخدام المفتاح ٨٩
ج التشفير الضربي باستخدام المفتاح ٨٩
د التشفير الهجين باستخدام المفتاحين ٨٩،٩٠
ه التشفير الخلطي باستخدام الدالة RANDOMIZE
و التشفير الانسيابي الخطي باستخدام الدالة البوليانية XOR
ز التشفير الانسيابي الخطي باستخدام الحقل العشوائي
ي فك التشفير وإرجاع الصورة الواضحة بعد تطبيق معالجات فك التشفير لمعالجات التشفير المستخدمة

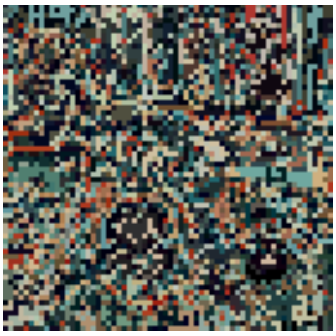
أ



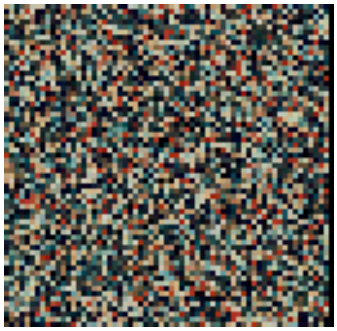
ب



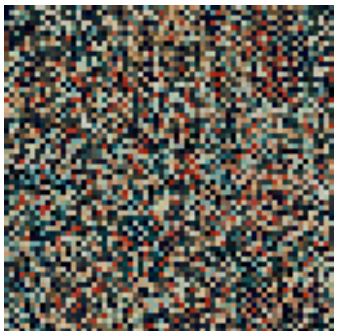
ج



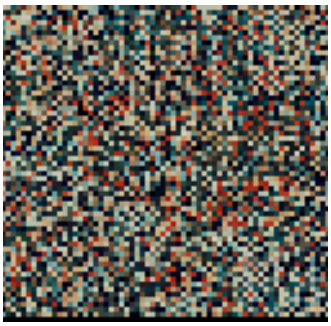
د



هـ



و



ز

ي

الشكل رقم (٣-١٥) تطبيق خوارزميات التشفير على الصورة رقم ١١

أ الصورة الملونة الواضحة

ب التشفير الجمعي باستخدام المفتاح ٨٩

ج التشفير الضربي باستخدام المفتاح ٨٩

د التشفير الهجين باستخدام المفتاحين ٨٩،٩٠

ه التشفير الخلطي باستخدام الدالة RANDOMIZE

و التشفير الانسيابي الخطي باستخدام الدالة البوليانية XOR

ز التشفير الانسيابي الخطي باستخدام الحقل العشوائي

ي فك التشفير وإرجاع الصورة الواضحة بعد تطبيق معالجات فك التشفير لمعالجات التشفير المستخدمة

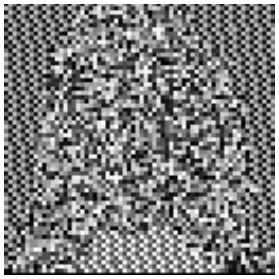
أ

ب

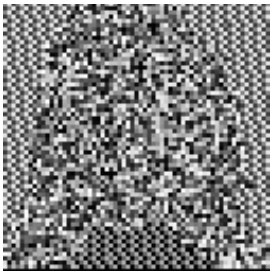
ج

د

هـ



و



ز

ي

الشكل رقم (٣-٤) تطبيق خوارزميات التشفير على الصورة رقم ٢

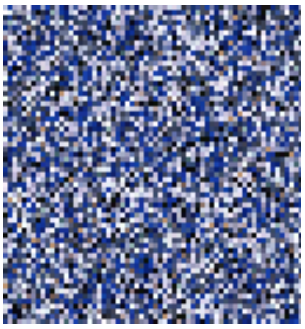
أ الصورة ذات التدرجات الرمادية الواضحة
ب التشفير الجمعي باستخدام المفتاح ٨٩
ج التشفير الضربي باستخدام المفتاح ٨٩
د التشفير الهجين باستخدام المفتاحين ٨٩،٩٠
ه التشفير الخلطي باستخدام الدالة RANDOMIZE
و التشفير الانسيابي الخطي باستخدام الدالة البوليانية XOR
ز التشفير الانسيابي الخطي باستخدام الحقل العشوائي
ي فك التشفير وإرجاع الصورة الواضحة بعد تطبيق معالجات فك التشفير لمعالجات التشفير المستخدمة

أ

ب

ج

د



هـ

و

ز

ي

الشكل رقم (٣-١٠) تطبيق خوارزميات التشفير على الصورة رقم ٧

أ الصورة الملونة الواضحة

ب التشفير الجمعي باستخدام المفتاح ٨٩

ج التشفير الضربي باستخدام المفتاح ٨٩

د التشفير الهجين باستخدام المفتاحين ٨٩،٩٠

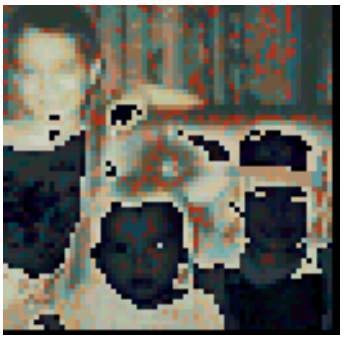
ه التشفير الخلطي باستخدام الدالة RANDOMIZE

و التشفير الانسيابي الخطي باستخدام الدالة البوليانية XOR

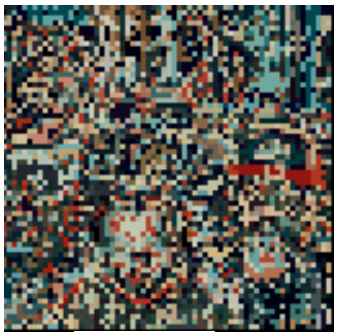
ز التشفير الانسيابي الخطي باستخدام الحقل العشوائي

ي فك التشفير وإرجاع الصورة الواضحة بعد تطبيق معالجات فك التشفير لمعالجات التشفير المستخدمة

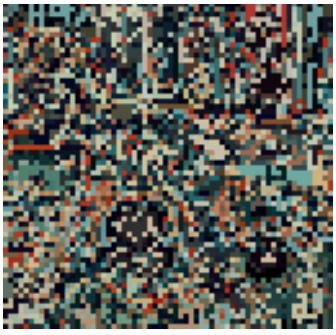
أ



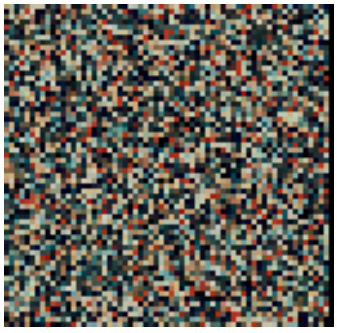
ب



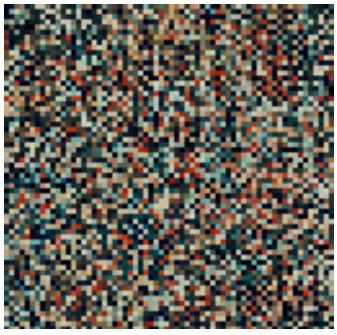
ج



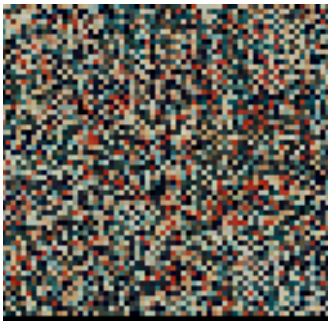
د



هـ



و

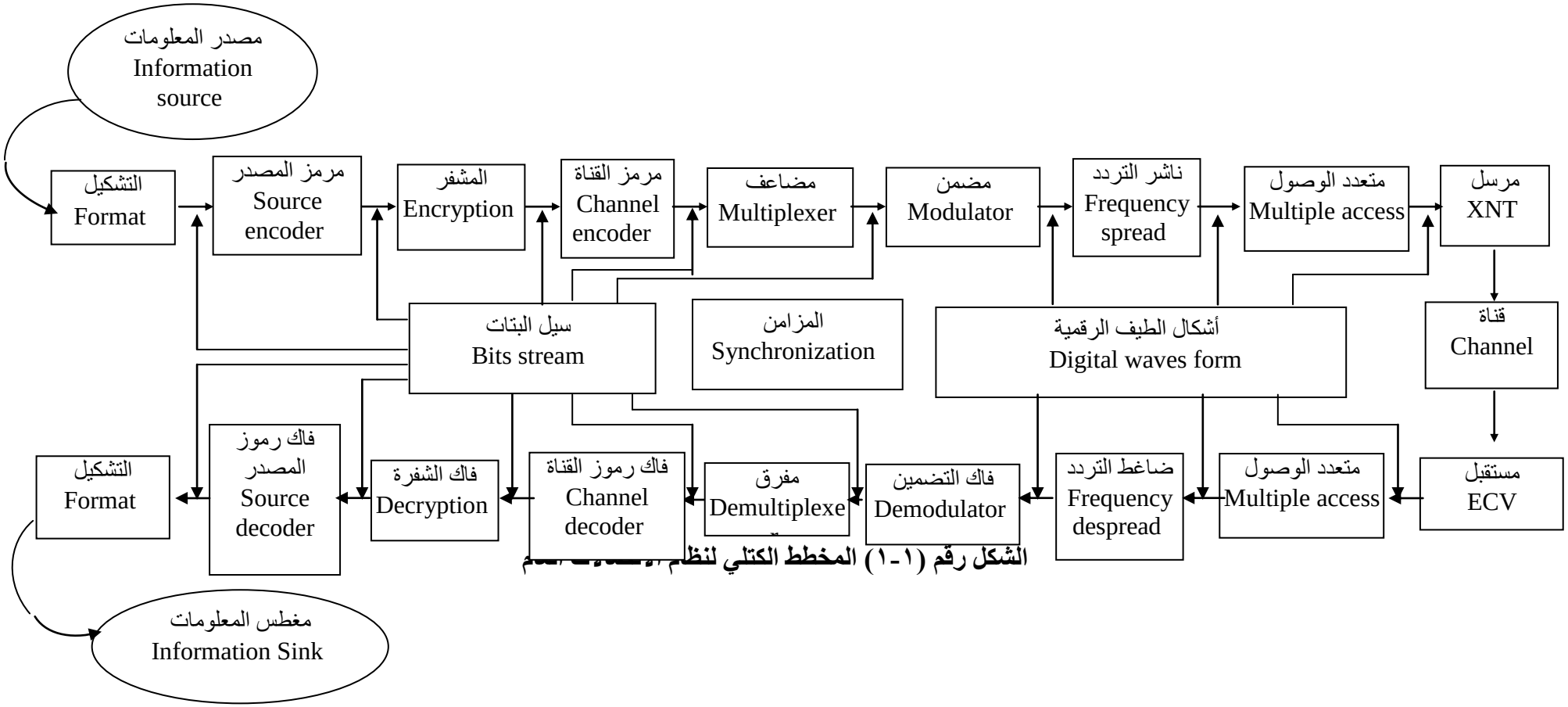


ز

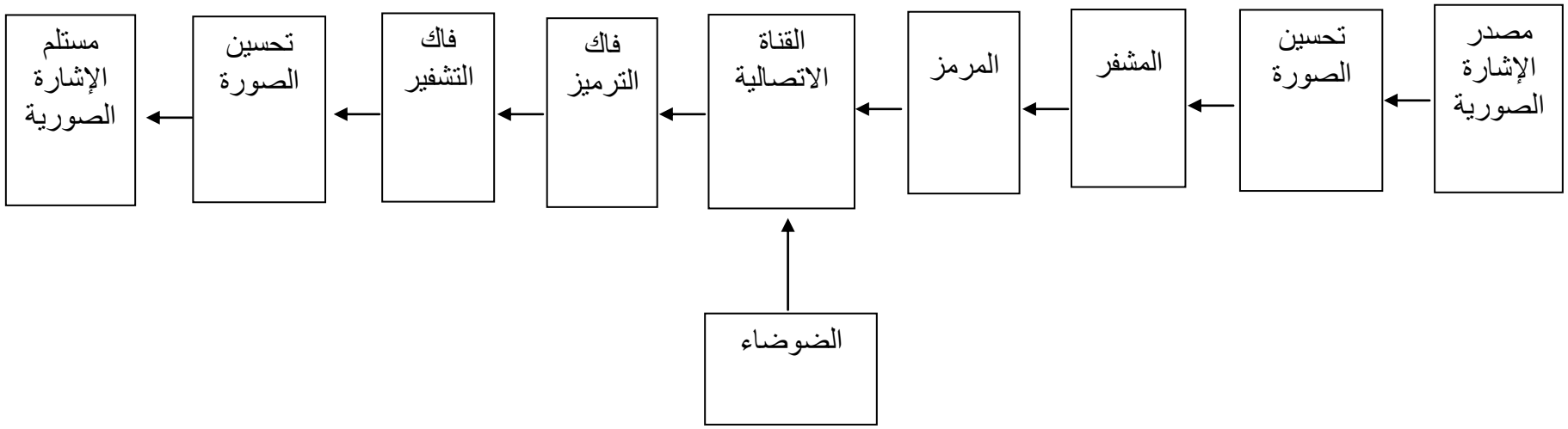
ي

الشكل رقم (٣-٦) تطبيق خوارزميات التشفير على الصورة رقم ٤

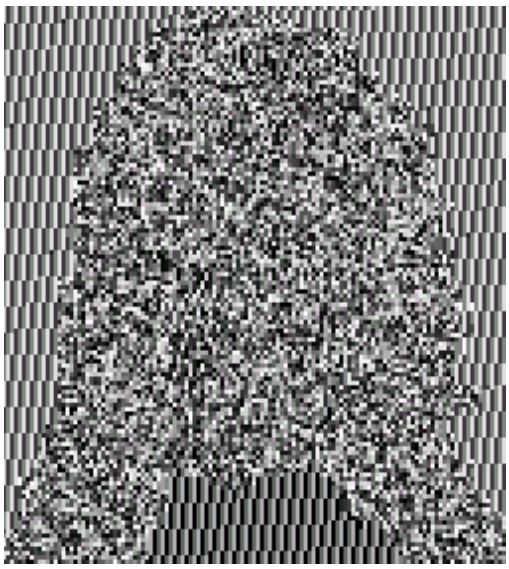
أ الصورة ذات التدرجات الرمادية الواضحة
ب التشفير الجمعي باستخدام المفتاح ٨٩
ج التشفير الضربي باستخدام المفتاح ٨٩
د التشفير الهجين باستخدام المفتاحين ٨٩،٩٠
ه التشفير الخلطي باستخدام الدالة RANDOMIZE
و التشفير الانسيابي الخطي باستخدام الدالة البوليانية XOR
ز التشفير الانسيابي الخطي باستخدام الحقل العشوائي
ي فك التشفير وإرجاع الصورة الواضحة بعد تطبيق معالجات فك التشفير لمعالجات التشفير المستخدمة



الشكل رقم (١-١) المخطط الكتلي لنظام [illegible]



الشكل رقم (٢-١) المخطط الكتلي لنظام معالجة الصور المقترح



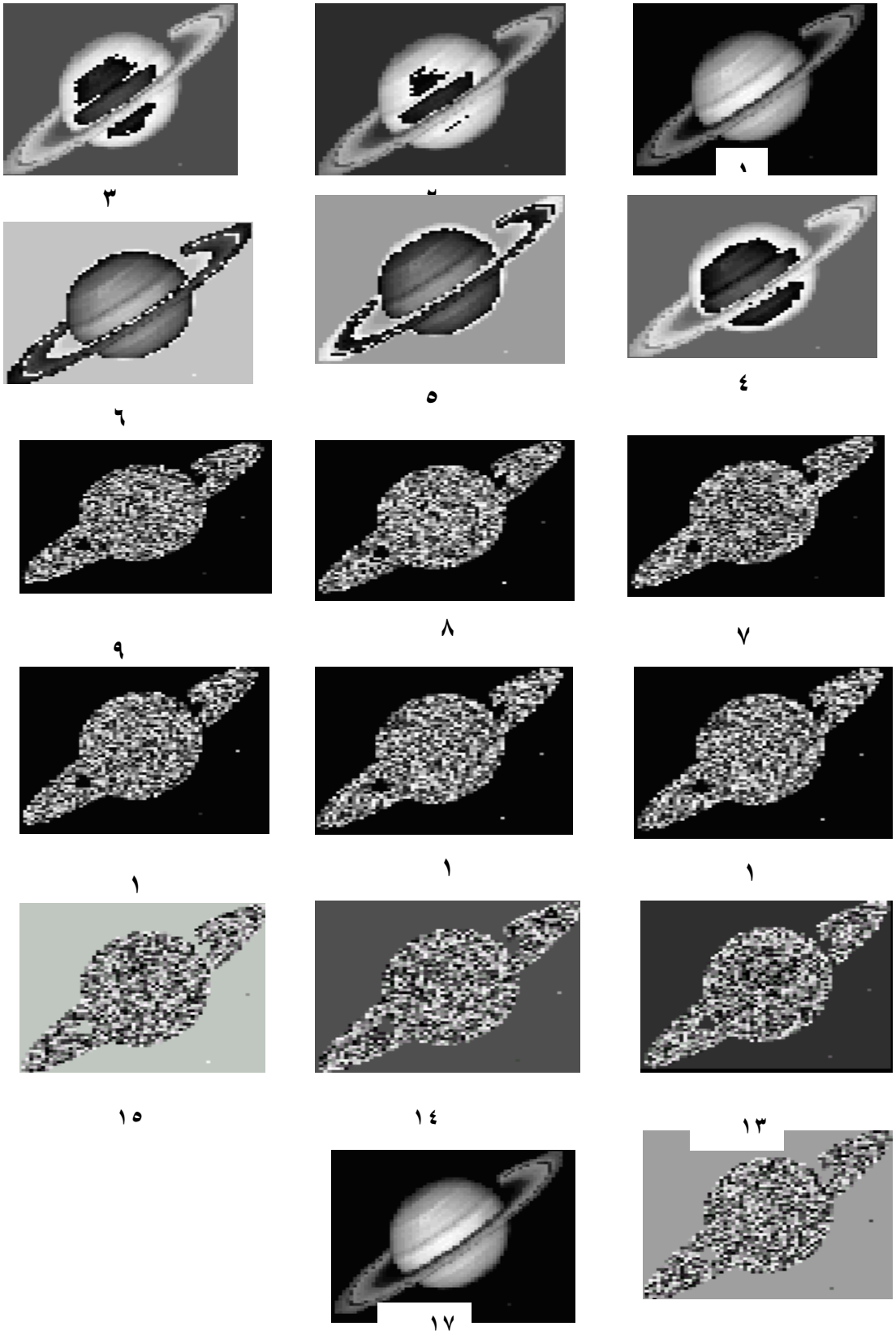
ب

الشكل رقم (٣-٧) تطبيق التشفير الانسيابي الخطي للصور باستخدام الحقل العشوائي

الشكل رقم (٣-٧ أ) الصورة الواضحة

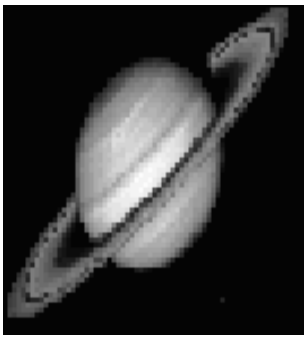
الشكل رقم (٣-٧ ب) الصورة المشفرة

الشكل رقم (٣-٧ ج) فك التشفير وإرجاع الصورة الواضحة

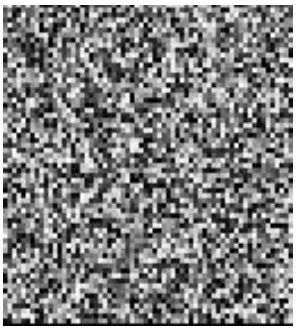


اســس رقم (٣-٢) تطبيق خوارزميات التشفير التقليدية على الصورة رقم ١

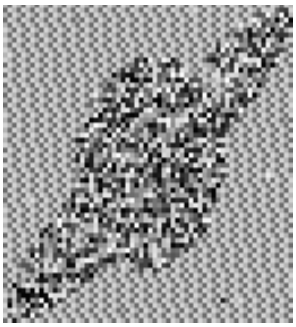
١ الصورة الواضحة
٢-٦ التشفير الجمعي باستخدام مفاتيح التشفير ٥٠، ٨٠، ١٠٠، ١٦٠، ٢٠٠ على التوالي
٧-١١ التشفير الضربي باستخدام مفاتيح التشفير ٥١، ٨١، ١٠١، ١٦١، ٢٠١ على التوالي
١٢-١٦ التشفير الهجين باستخدام مفاتيح التشفير ٥٠ و ٥١، ٨٠ و٨١ ، ١٠٠ و ١٠١، ١٦٠ و١٦١ ، ٢٠٠ و ٢٠١ على التوالي
١٧ الصورة الواضحة بعد فك التشفير



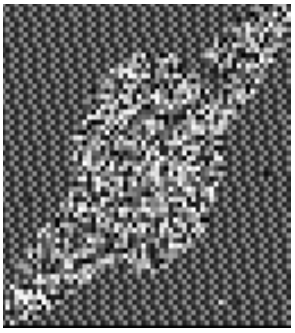
أ



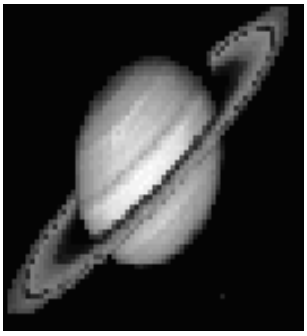
ب



ج



د



هـ

الشكل رقم (٣-٣) تطبيق خوارزميات التشفير الحديثة على الصورة رقم ١

أ الصورة ذات التدرجات الرمادية الواضحة

ب التشفير الخلطي باستخدام الدالة RANDOMIZE

ج التشفير الانسيابي الخطي باستخدام الدالة البوليانية XOR

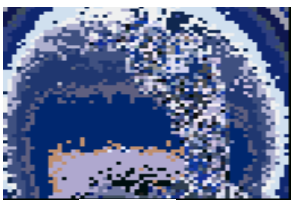
د التشفير الانسيابي الخطي باستخدام الحقل العشوائي

هـ الصورة الواضحة بعد فك التشفير

١

٢

٣



١٦

١٧

الشكل رقم (٣-١٠) تطبيق خوارزميات التشفير التقليدية على الصورة رقم ٧

١ الصورة الواضحة

٢-٦ التشفير الجمعي باستخدام مفاتيح التشفير ٥٠، ٨٠، ١٠٠، ١٦٠، ٢٠٠ على التوالي

٧-١١ التشفير الضربي باستخدام مفاتيح التشفير ٥١، ٨١، ١٠١، ١٦١، ٢٠١ على التوالي

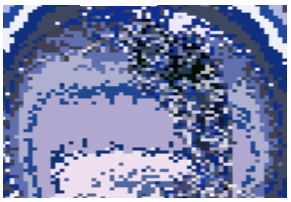
١٢-١٦ التشفير الهجين باستخدام مفاتيح التشفير ٥٠ و ٥١، ٨٠ و٨١ ، ١٠٠ و ١٠١، ١٦٠ و١٦١ ،
٢٠٠ و ٢٠١ على التوالي

١٧ الصورة الواضحة بعد فك التشفير

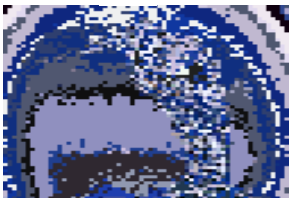
٤

٥

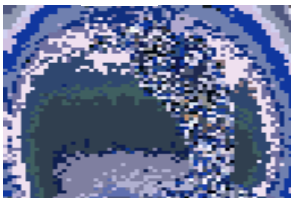
٦



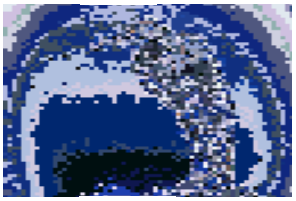
٧



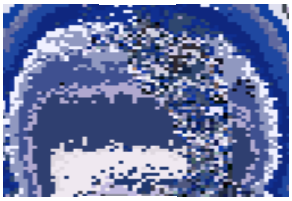
٨



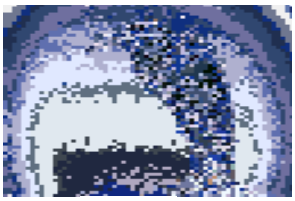
٩



١٠

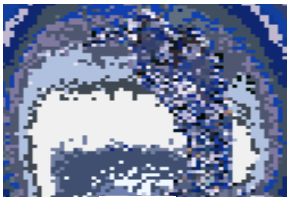


١١

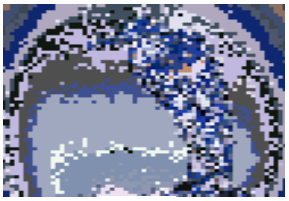


١٢

١٣



١٤

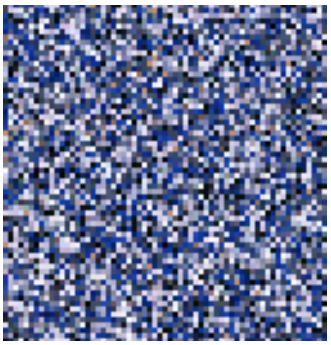


١٥

ت	الصور	الحجم	نوع الصورة	زمن تنفيذ خوارزميات التشفير بالثانية						زمن تنفيذ خوارزميات فك التشفير بالثانية					
				الأبعاد	الجمعي	الضربي	الهجين	الخلطي	الانسيابي الخطي	الانسيابي العشوائي	الجمعي	الضربي	الهجين	الخلطي	الانسيابي الخطي	الانسيابي العشوائي
١	الصورة رقم ١	١٠kb	تدرجات رمادية	١٢٨×١٢٨	١	١	٢	١	١٠	١٠	١	١	١	١	٦	٦
٢	الصورة رقم ٢	١٨kb	تدرجات رمادية	١٢٨×١٢٨	٢	٢	٣	١	١٢	١٢	١	١	١	١	٧	٧
٣	الصورة رقم ٣	١٨kb	تدرجات رمادية	١٢٨×١٢٨	٢	٢	٢	٢	١٥	١٤	١	١	١	١	٨	٧
٤	الصورة رقم ٤	١١kb	تدرجات رمادية	١٢٨×١٢٨	٢	٣	٤	٢	١٥	١٥	٢	٢	٢	٢	٨	٨
٥	الصورة رقم ٥	١١kb	تدرجات رمادية	١٢٨×١٢٨	٣	٣	٣	٢	١٤	١٥	٢	٢	٢	٢	٨	٩
٦	الصورة رقم ٦	١٨kb	تدرجات رمادية	١٢٨×١٢٨	٣	٣	٤	٣	١٥	١٤	٢	٢	٢	٢	٩	٩
٧	الصورة رقم ٧	١١kb	ملونة	١٢٨×١٢٨	٢	٢	٢	١	١١	١١	١	١	١	١	٦	٦
٨	الصورة رقم ٨	١٨kb	ملونة	١٢٨×١٢٨	٢	٢	٣	٢	١١	١١	١	١	٢	٢	٨	٧
٩	الصورة رقم ٩	١٨kb	ملونة	١٢٨×١٢٨	٣	٣	٤	٣	١٣	١٢	٢	٢	٣	٣	١٠	١٠
١٠	الصورة رقم١٠	١١kb	ملونة	١٢٨×١٢٨	٣	٣	٤	٤	١٤	١٤	٢	٢	٣	٤	١١	١٠
١١	الصورة رقم ١١	١١kb	ملونة	١٢٨×١٢٨	٤	٤	٥	٤	١٦	١٥	٣	٣	٣	٤	١٢	١٢
١٢	الصورة رقم ١٢	١٨kb	ملونة	١٢٨×١٢٨	٥	٥	٦	٦	١٩	١٨	٤	٤	٤	٦	١٥	١٥

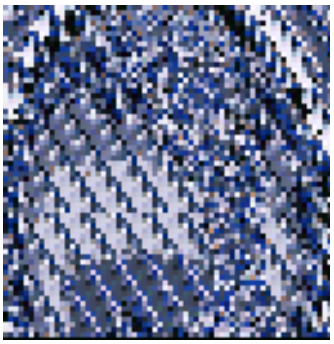
جدول رقم (٣-٢) زمن تنفيذ خوارزميات التشفير / فك التشفير

أ



ب

ج



د

هـ

الشكل رقم (٣-١١) تطبيق خوارزميات التشفير الحديثة على الصورة رقم ٧

أ الصورة الملونة الواضحة

ب التشفير الخلطي باستخدام الدالة RANDOMIZE

ج التشفير الانسيابي الخطي باستخدام الدالة البوليانية XOR

د التشفير الانسيابي الخطي باستخدام الحقل العشوائي

هـ الصورة الواضحة بعد فك التشفير

وذلك يعود إلى استخدام دالة RONDOMIZE في توليد مفاتيح التشفير الخلطي كما في الشكل رقم (٣-٣ب) .

خامسا". خوارزمية التشفير الانسيابي الخطي للصورة : بتطبيق خوارزمية التشفير الانسيابي الخطي باستخدام الدالة الخطية XOR على الصورة نفسها تم تشفير اغلب معلومات الصورة، وكما مبين في الشكل رقم (٣-٣ج).

سادسا". خوارزمية التشفير الانسيابي الخطي للصورة باستخدام الحقل العشوائي: بتطبيق هذه الخوارزمية على الصورة ظهرت النتيجة المبينة في الشكل رقم (٣-٣د).

ب ـ الاختبار الثاني

تم تطبيق خوارزميات التشفير المذكورة في الاختبار الأول على الصور ٢، ٣، ٤، ٥، و٦ في الشكل رقم (٣-١) والتي تمثل صورا" متدرجة في التعقيد، وكانت النتائج كما موضحة في الشكل رقم (٣-٤)، الشكل رقم (٣-٥)، الشكل رقم (٣-٦)، الشكل رقم (٣-٧)، الشكل رقم (٣-٨)، والشكل رقم (٣-٩) على التوالي. ومن ملاحظة الأشكال المذكورة يمكننا القول بان تشفير المعلومات واختفاءها يزداد بزيادة تعقيد الصورة.

ج ـ الاختبار الثالث

تم تطبيق النظام على الصورة رقم ٧ المبينة في الشكل رقم (٣-١) وهي صوره ملونة بسيطة، وكانت النتائج كما في الشكل رقم (٣-١٠) والشكل (٣-١١) على التوالي، ومن ملاحظتنا لهذين الشكلين وجد أن تطبيق خوارزميات التشفير التقليدية على الصورة الملونة لا يؤدي عمل التشفير المطلوب من ناحية اختفاء المعلومات كليا" ولكن هنالك اختفاء تدريجي للمعلومات. أما تطبيق خوارزميات التشفير الحديثة فانه عمل على تشفير معلومات الصورة بشكل تام تقريبا".

د ـ الاختبار الرابع

تم تطبيق النظام على الصور٨، ٩، ١٠، ١١، و ١٢ المبينة في الشكل (٣-١) وهي صورا" ملونة متدرجة التعقيد وكانت النتائج كما مبينة في الشكل (٣-١٢)، الشكل (٣-١٣)، الشكل (٣-١٤)، الشكل (٣-١٥)، الشكل (٣-١٦)، والشكل (٣-١٧) على التوالي. ومن ملاحظة النتائج يتبين بان تشفير المعلومات واختفاءها يزداد بزيادة تعقيد الصورة الملونة، حيث نلاحظ اختفاء معلومات الصورة بشكل تام تقريبا" عند تطبيق خوارزميات التشفير.

كما لاحظنا من تطبيق طرائق التشفير المستخدمة في النظام المقترح أن أمنية نظام التشفير تعتمد على عاملين وهما قوة الخوارزمية وطول المفتاح المستخدم، وان أمنية الخوارزمية يجب أن تعتمد على المفتاح وليس على تفاصيل الخوارزمية. ولهذا السبب فان مفتاح التشفير يتم توليده من قبل مستخدم النظام. تكمن قوة النظام المقترح في سرية مفتاح التشفير وطول مفتاح التشفير المستخدم.

إن إحدى تقنيات قياس قوة النظام المقترح هي حساب زمن تنفيذ خوارزميات التشفير وخوارزميات فك التشفير، حيث يمكننا حساب زمن التنفيذ وذلك بتنفيذ النظام وبيان الزمن اللازم لتنفيذ كل خوارزمية على حده، كما مبين في الجدول رقم (٣-٢).

ويمكن ملاحظة ما يأتي:

ـ يزداد زمن تنفيذ الخوارزمية بزيادة حجم الصورة المدخلة.

ـ هنالك اختلاف واضح في زمن تنفيذ الخوارزميات التقليدية وزمن تنفيذ الخوارزميات الحديثة، حيث إن تنفيذ الخوارزميات التقليدية أسرع من تنفيذ الخوارزميات الحديثة، وان عدد العمليات في الخوارزميات التقليدية يكون اقل من عدد العمليات في الخوارزميات الحديثة ولكن على حساب قوة التشفير وبالتالي سرية المعلومات المراد حمايتها.

ـ يزداد اختفاء معلومات الصورة بزيادة تعقيد الصورة المدخلة.

بعد إجراء عمليات التشفير السابقة على الصورة المدخلة يتم إرسالها عبر قناة اتصال تمت محاكاتها، وبذلك ستتم عملية ترميز معلومات الصورة المشفرة (الصورة المدخلة) لغرض حمايتها من الضوضاء المحتملة للقناة. ومن ثم تتم عملية فك الترميز بعد اكتشاف الخطأ وتصحيحه. وبعد مرور الصورة عبر القناة تتم عمليات فك التشفير واسترجاع الصورة الواضحة (الصورة المدخلة للنظام).

٢.٣ الاستنتاجات

ـ يستطيع النظام العمل على كل أنواع الصور وبأحجام مختلفة.

ـ إمكانية تقويم النظام اعتمادا" على نظام الرؤية البشري والوقت المطلوب لتنفيذ خوارزميات التشفير / فك التشفير .

ـ يجب أن يكون طول مفتاح التشفير المستخدم في خوارزميتي التشفير الانسيابي أكبر أو يساوي حجم بيانات الصورة لنضمن تشفير كل أجزاء الصورة.

ـ أثبت النظام إمكانية تطبيق تقنيات التحسين للصورة وحسب الحاجة.

ـ إمكانية محاكاة قناة اتصالات للصور وتطبيق خوارزميتي الترميز / فك الترميز على بيانات تلك الصور لحمايتها من الضوضاء المحتملة .

ـ أثبت النظام إمكانية التشفير التام للصور ومن ثم فك التشفير واسترجاع الصورة الواضحة كما أدخلت بدون أدنى تغيير.

٣.٣ توجهات العمل المستقبلي

ـ استخدام وسائل ضغط الصور ومن ثم تطبيق خطوات النظام عليها.

ـ استخلاص الخصائص المميزة للصورة ومن ثم تطبيق خطوات النظام عليها.

ـ استخدام تقنية تجزئة الصورة ومن ثم تطبيق خطوات النظام على كل جزء بشكل مستقل مما يؤدي إلى زيادة في أمنية المعلومات المرسلة.

ـ تطبيق تقنية الإخفاء (Steganography) في تشفير الصور .

د ـ الاختبار الرابع

تم تطبيق النظام على الصورة المبينة في الشكل رقم (٣-١ د) وهي صورة ملونة معقدة وكانت النتائج كما مبينة في الشكل رقم (٣-١٠)، ومن ملاحظة النتائج يتبين بان تشفير المعلومات واختفاءها يزداد بزيادة تعقيد الصورة الملونة، حيث نلاحظ اختفاء معلومات الصورة بشكل تام تقريبا" عند تطبيق خوارزميات التشفير عدا تطبيق خوارزمية التشفير الجمعي فلم تشفر الصورة بشكل جيد وبذلك فهي تعتبر ضعيفة في تشفير الصور المعقدة.

كما لاحظنا من تطبيق طرائق التشفير المستخدمة في النظام المقترح أن أمنية نظام التشفير تعتمد على عاملين وهما قوة الخوارزمية وطول المفتاح المستخدم ، وان أمنية الخوارزمية يجب أن تعتمد على المفتاح وليس على تفاصيل الخوارزمية. ولهذا السبب فان مفتاح التشفير يتم توليده من قبل مستخدم النظام.

تكمن قوة النظام المقترح في سرية مفتاح التشفير بالنسبة للطرائق التقليدية المستخدمة، وطول المفتاح المستخدم وتعقيده إضافة إلى سريته بالنسبة للطرائق الحديثة.

إن إحدى تقنيات قياس قوة النظام المقترح هي حساب زمن تنفيذ خوارزميات التشفير وخوارزميات فك التشفير، حيث يمكننا حساب زمن التنفيذ وذلك بتنفيذ النظام وبيان الزمن اللازم لتنفيذ كل خوارزمية على حده، كما مبين في الجدول رقم (٣-٢).

ويمكن ملاحظة ما يأتي:

- هنالك علاقة خطية بين حجم الصورة والزمن اللازم لتنفيذ الخوارزميات (يزداد زمن تنفيذ الخوارزمية بزيادة حجم الصورة المدخلة).
- هنالك اختلاف واضح في زمن تنفيذ الخوارزميات التقليدية وزمن تنفيذ الخوارزميات الحديثة، حيث إن تنفيذ الخوارزميات التقليدية أسرع من تنفيذ الخوارزميات الحديثة، ولكن على حساب قوة التشفير وبالتالي سرية المعلومات المراد حمايتها.

ـ هنالك علاقة خطية بين تعقيد الصورة وتشفيرها (يزداد اختفاء معلومات الصورة بزيادة تعقيد الصورة المدخلة).

بعد إجراء عمليات التشفير السابقة على الصورة المدخلة يتم إرسالها عبر قناة اتصال تمت محاكاتها، وبذلك ستتم عملية ترميز معلومات الصورة المشفرة (الصورة المدخلة) لغرض حمايتها من الضوضاء المحتملة للقناة. ومن ثم تتم عملية فك الترميز بعد اكتشاف الخطأ وتصحيحه. وبعد مرور الصورة عبر القناة تتم عمليات فك التشفير واسترجاع الصورة الواضحة (الصورة المدخلة للنظام).

٢.٣ الاستنتاجات

ـ يستطيع النظام العمل على كل أنواع الصور (الاحاديه، ذات ١٦ لون، ذات ٢٥٦ لون) وبأحجام مختلفة.

ـ إمكانية تقويم النظام اعتمادا" على نظام الرؤية البشري والوقت المطلوب لتنفيذ خوارزميات التشفير / فك التشفير .

ـ يجب أن يكون طول مفتاح التشفير المستخدم في خوارزميتي التشفير الانسيابي أكبر أو يساوي حجم بيانات الصورة لنضمن تشفير كل أجزاء الصورة.

ـ أثبت النظام إمكانية تطبيق تقنيات التحسين للصورة وحسب الحاجة.

ـ إمكانية محاكاة قناة اتصالات للصور وتطبيق خوارزميتي الترميز / فك الترميز على بيانات تلك الصور لحمايتها من الضوضاء المحتملة .

ـ أثبت النظام إمكانية التشفير التام للصور ومن ثم فك التشفير واسترجاع الصورة الواضحة كما أدخلت بدون أدنى تغيير.

٣.٣ توجهات العمل المستقبلي

ـ استخدام وسائل ضغط الصور ومن ثم تطبيق خطوات النظام عليها.

ـ استخلاص الخصائص المميزة للصورة ومن ثم تطبيق خطوات النظام عليها.

ـ استخدام تقنية تجزئة الصورة ومن ثم تطبيق خطوات النظام على كل جزء بشكل مستقل مما يؤدي إلى زيادة في أمنية المعلومات المرسلة.

ـ تطبيق تقنية الإخفاء (Steganography) في تشفير الصور .

المحتويات

قائمة الرموز	
رموز التشفير	
P	النص الواضح (الصورة الواضحة)
C	النص المشفر (الصورة المشفرة)
K	مفتاح التشفير
f_E	خوارزمية التشفير
f_D	خوارزمية فك التشفير
n	المعيار الحسابي والذي يمثل عدد هجائية التشفير
L	طول المتتابعة العشوائية
$\oplus$	الدالة البوليانية XOR
$\wedge$	الدالة البوليانية AND
$\vee$	الدالة البوليانية OR
M	الرسالة (الصورة)
رموز معالجة الصورة	
H	عملية التدني
η (x, y)	الضوضاء الجمعي
f (x, y)	الصورة المدخلة
g(x, y)	الصورة المتدنية
σ_n^2	التباين لـ n

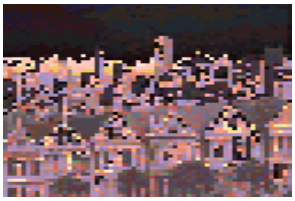
رموز الترميز	
n	طول الرمز أو طول الكتلة
k	عدد بتات الفحص
٢^k	عدد كلمات الرمز
m	بتات المعلومات
C	كلمة الرمز
G	المصفوفة المولدة
P	مصفوفة فحص التماثل المستخدمة في عملية الترميز
H	مصفوفة فحص التماثل المستخدمة في عملية فك الترميز
R	كلمة الرمز المستلمة
S	السيندروم الذي يكتشف الأخطاء
E	متجه الخطأ

قائمة الجداول

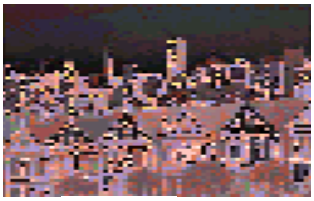
قائمة الأشكال

١

٢

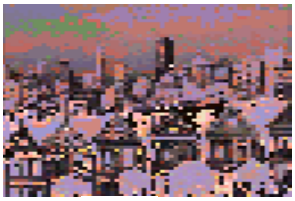


٣

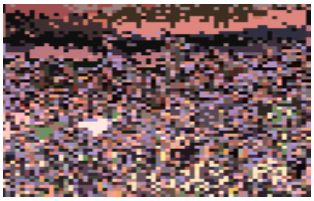


٤

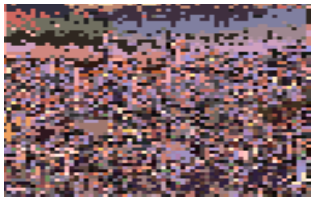
٥



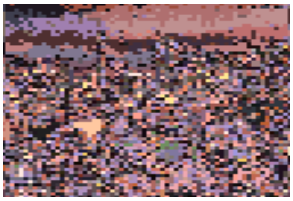
٦



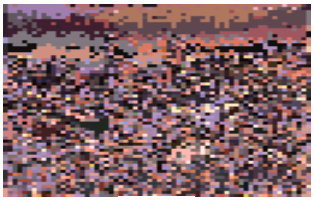
٧



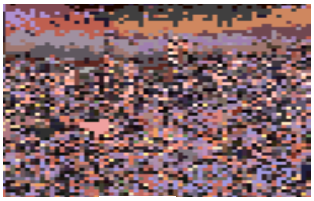
٨



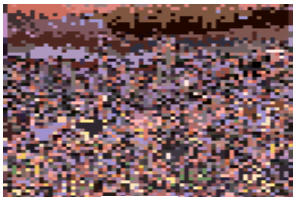
٩



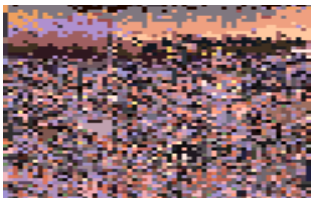
١٠



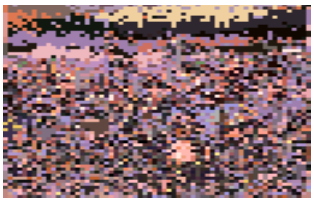
١١



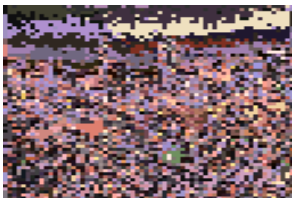
١٢



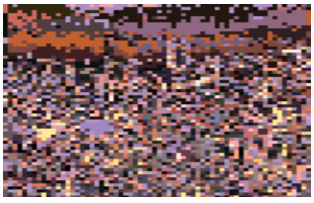
١٣



١٤



١٥



١٥

١

الشكل رقم (٣-١٦) تطبيق خوارزميات التشفير التقليدية على الصورة رقم ١٢

١ الصورة الواضحة

٢-٦ التشفير الجمعي باستخدام مفاتيح التشفير ٥٠، ٨٠، ١٠٠، ١٦٠، ٢٠٠ على التوالي

٧-١١ التشفير الضربي باستخدام مفاتيح التشفير ٥١، ٨١، ١٠١، ١٦١، ٢٠١ على التوالي

١٢-١٦ التشفير الهجين باستخدام مفاتيح التشفير ٥٠ و ٥١، ٨٠ و٨١، ١٠٠ و١٠١، ١٦٠ و١٦١،

٢٠٠ و ٢٠١ على التوالي

١٧ الصورة الواضحة بعد فك التشفير