جمهورية العراق
وزارة التعليم والبحث العلمي
جامعة بابل
كلية التربية للعلوم الصرفة

نظام التشفير الفوضوي

الباحث

عامر سلمان عبد الواحد جبار

إلى مجلس جامعة بابل كلية التربية للعلوم الصرفة وهو جزء من
متطلبات نيل شهادة البكالوريوس في قسم الرياضيات
بإشراف

أ. م. د. لميس حمود السعدي

١٤٤٥ هـ ٢٠٢٤ م

أَعُوذُ بِاللَّهِ مِنَ الشَّيْطَانِ الرَّجِيمِ بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

هُوَ الَّذِي جَعَلَ الشَّمْسَ ضِيَاءً
وَالْقَمَرَ نُورًا وَقَدَّرَهُ مَنَازِلَ
لِتَعْلَمُوا عَدَدَ السِّنِينَ وَالْحِسَابَ ۚ
مَا خَلَقَ اللَّهُ ذَٰلِكَ إِلَّا بِالْحَقِّ ۚ
يُفَصِّلُ الْآيَاتِ لِقَوْمٍ يَعْلَمُونَ ۝٥

سورة يونس

الإهداء:

أهدي ثمرة جهدي هذا...

إلى مثلي الأعلى وسندي الذي حملت اسمه بكل افتخار والدي العزيز.

إلى من ينبض قلبها بالحب والحنان والدتي الغالية حفظها الله.

إلى من اشدد بهم أزري... إخوتي وأخواتي الأعزاء.

إلى من تنبض قلوبهم مواقف عز وفخر.... أصدقائي وأحبائي أجمعين

إلى أساتذتي الأفاضل في جامعة بابل تثميناً لجهودهم وصبرهم طيلة سنوات الدراسة..

إلى الفاضلة د. لميس حمود السعدي دام توفيقها على جهودها الكبيرة في الإشراف وتقويم البحث.

الشكر والعرفان

الحمد لله مستحق الحمد حتى الانقطاع وموجب الشكر بأقصى ما يستطاع فقد منَّ عليَّ في إكمال هذا البحث والكمال له وحده وصلى الله على محمد خير من افتتحت بذكره الدعوات وعلى آله الطاهرين الطيبين سفينة النجاة.

ويسرني أيضاً أن أوجّه شكري وامتناني لكل من نصحني أو أرشدني أو ساهم معي في أي مرحلة أو مشاركة لإتمام هذا العمل وبالخصوص أستاذتي الفاضلة د. لميس حمود السعدي لإشرافه المباشر على جميع مراحل البحث والنصح والتوجيه.

كما إنّ شكري موجّه لإدارة جامعة بابل وكليّة التربية للعلوم الصرفة / قسم الرياضيات على جهودهم في تسهيل كافة العقبات لجميع طلبتها طيلة سنوات الدراسة وتوفير أفضل بيئة دراسيّة لأبنائها.

الباحث

عامر سلمان عبد الواحد

الواجهة	
الآية الكريمة	أ
الإهداء	ب
الشكر والعرفان	ت
فهرس المحتويات	ث
الفصل الأول	١-٧
المقدمة	١-٢
المقاييس الحيوية	٣-٤
استخلاص الخواص	٥-٦
هدف البحث	٦
الفصل الثاني	٧-١٩
نظام الفوضى	٧-٩
المخطط العام لطريقة التشفير المقترحة	١٠-١٢
خوارزمية التشفير المقترحة	١٢-١٣
تشفير الصورة باستخدام التشفير الفوضوي	١٤-١٩
الاستنتاجات	٢٠
المصادر	٢١

الفصل الأوّل

١- ١ المقدّمة:

كما هو معروف، فان التشفير بالطرائق التقليدية يعتمد على مفتاح التشفير الذي يعرف على انه سلسلة طويلة من ال(bits) ومن البديهي أن تذكر هذه السلسلة الطويلة من الأرقام، العشوائية امر صعب لهذا استخدم البحث بطريقةForce Brute للحصول على مفتاح التشفير (١).

إن أكثر الأعمال التي تعتمد على المفتاح المتماثل في التشفير ترتكز على كتلة من ال(bits) التي تعتمد عليها الخوارزمية في التشفير، إذ أن هذه الكتل تدخل بعدد من الجولات والحسابات وبمساعدة مفتاح التشفير ينتج النص المشفر، من هذه الخوارزميات خوارزمية(Data Encryption Standard: DES) ومع زيادة السرعة وعدد الحسابات فبمجرد محاولة الدخيل (الذي يمتلك خبرة بالتشفير) لعدد من المفاتيح الحصول على الرسالة الأصلية وبوقت لا يتجاوز ٤٨ ساعة (٢) .

ولهذا فالخوارزميات التي تستخدم مفتاح واحد لتشفير البيانات لا تمتلك سرية عالية والحل يكون باستخدام عدد من المفاتيح المختلفة(Multiple Keys) كل مفتاح يشفر كتلة من البيانات، ومع ذلك فان هذا الأسلوب ذو فائدة محددة. كما إن استخدام الدوال الرياضية لتوليد عدد من المفاتيح يعد من الطرائق الحديثة والغير مكتشفة إلى حد كبير، ولكن البسيطة منها تعتبر غير كافية وفي حالة كون

خوارزمية التشفير عامة (Public)أي إن عملية توليد المفتاح تكون معروفة للمتطفل، وهذا يعني من السهولة معرفة واكتشاف مفتاح واحد ومن ثم اكتشاف باقي المفاتيح ٠

وهنا تأتي أهمية المقاييس الحيوية لكي تلعب دور رئيسي في توليد المفتاح المستخدم في عملية التشفير، كما تتجلى فكرة استخدام الدالة الفوضوية في عملية التشفير لزيادة الأمنية في الطرق المستخدمة لتشفير البيانات (٣).

ومما ينبغي ذكره إن المقياس الحيوي قد استخدم في عديد من التطبيقات كعامل أساسي في عملية التمييز بين الأشخاص وبالذات استخدمت قزحية العين لهذا الغرض ، أما الدالة الفوضوية فقد تم التطرق اليها في عملية التشفير كما في تشفير الصور ،وفي عملية الاتصالات السرية ، بينما استخدمت من قبل عدد من الباحثين بعد دمجها مع خصائص المقاييس الحيوية في عملية تشفير الصور ،تتضمن فكرة هذا البحث التشفير بواسطة المقاييس الحيوية إذ تم توليد مفتاح المقياس الحيوي (قزحية العين) من خلال استخلاص الخواص المهمة والمفيدة بعملية التشفير باستخدام احد التقنيات الخاصة بذلك وهي تحويلات المويجة، إضافة إلى استخدام الدالة الفوضوية للاستفادة من خواصها العشوائية، وكنتيجة لذلك فقد تم هنا وصف كيفية توليد المفتاح الحيوي للتشفير وفك الشفرة ودمجها مع الدوال الفوضوية (٤).

١- ٢ المقاييس الحيوية:

تعرف المقاييس الحيوية على إنها مقاييس للصفات أو الميزات الفريدة للإنسان والمستخدمة عادة في عمليات التمييز الإلكترونية أو إثبات الشخصية. فالكائن البشري فريد وكذلك فان صفاته الفيزيائية والسلوكية فريدة أيضا، ولهذا يمكن اعتبار القيم الناتجة من عملية الاستخلاص الناجح لمعلومات هذه المقاييس المستحصلة من الميزات البشرية فريدة ولايمكن تكرارها عند أي شخص آخر.

أما عن مصطلح المقياس الحيوي(Biometrics) فهو مشتق من الكلمة الإغريقية (Bios) التي ترمز للحياة، وكلمة (motron) وتعني المقياس، والذي يشير أيضا إلى حقل الاختلاف وهو ما يسمى الآن بالإحصاء(Biostatistics) والذي يهتم بتطور النظريات الرياضية والإحصائية المطبّقة على مشاكل تحليل البيانات في علم البيولوجي.

فكل أنظمة المقاييس الحيوية تعمل بنفس الأسلوب، إذ يتم أولا التقاط عينة من مثال عن أحد صفات المقاييس الحيوية ثم يتم استخلاص الصفات الفريدة وتحويلها الى رموز رياضية وبالاعتماد على احتياجات التقنية المستخدمة فقد يتم اخذ عدد من العينات لبناء مستوى ثقة (confidence level) للبيانات الابتدائية.

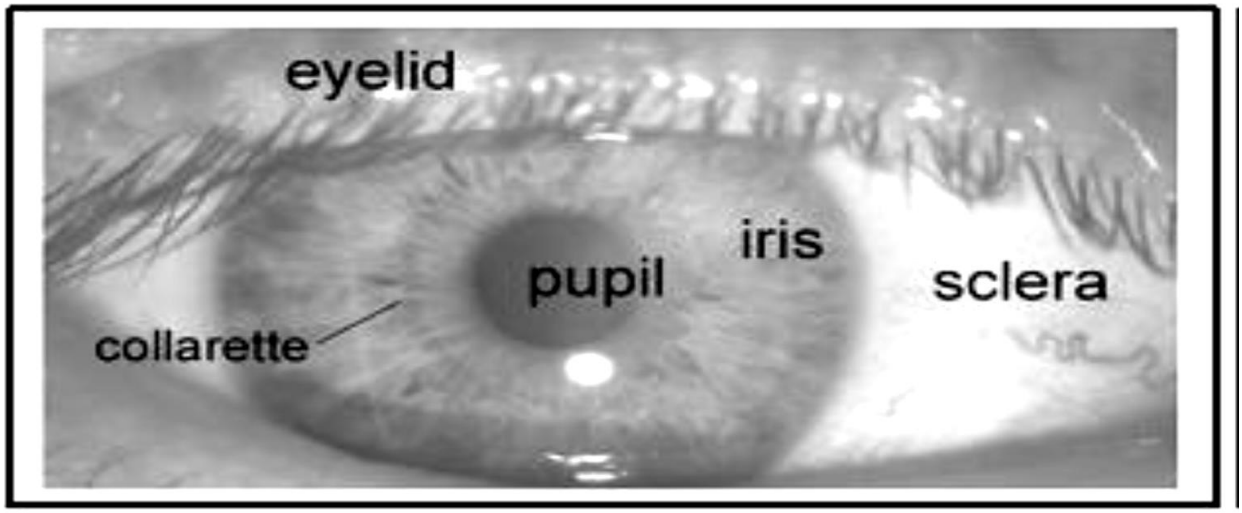
إن الفائدة الأساسية من استخدام المقياس الحيوي تكمن في كونها دائما حية وغير مستقرة الصفات من شخص لآخر ولهذا فلا يمكن الاشتباه بها ومع هذا فهي تعاني من تهديد خاص في سرية أنظمة المقاييس الحيوية. فالمهاجم قد يفسر بيانات المقياس الحيوي للفرد باستخدامها في عمليات أخرى غير قانونية .

في السنوات الأخيرة عرف عدد من التكنولوجيات المستخدمة لأخذ المقاييس الحيوية من الكائن البشري بصورة عامة والإنسان بصورة خاصة تختلف في محاسنها ومساوئها لكن القليل منها لاقى الترحيب والقبول منها (شكل الوجه، بصمة الإصبع، قزحية العين، شبكية العين، تمييز الصوت، التوقيع وهندسة اليد) .

١- ٢ - ١ خصائص قزحية العين:

في هذا البحث تم اعتماد قزحية العين كأحد المقاييس الحيوية حيث تعد الأنظمة المعتمدة عليها من اقل الأنظمة توليدا للأخطاء نسبة إلى باقي التقنيات المستخدمة للمقاييس الحيوية، فمن الواضح انه من الضروري إيجاد جزء في جسم الإنسان ذو صفات ثابته، فريدة جداً، سهلة القياس، وسريعة في حالة تمييز الأنماط.

تمثل قزحية العين خواص مقياس حيوي فسيولوجي فهي تحتوي على نسيج فريد ومعقد بما فيه الكفاية لاستخدامه كتوقيع حيوي للفرد كما في الشكل (١) الذي يوضح فسيولوجية قزحية العين. وبالمقارنة مع خواص المقاييس الحيوية الأخرى مثل الوجه وبصمة الإصبع فإن أنماط قزحية العين تكون ثابته وموثوق بها.



الشكل(1):فسيولوجية قزحية العين لدى الإنسان.

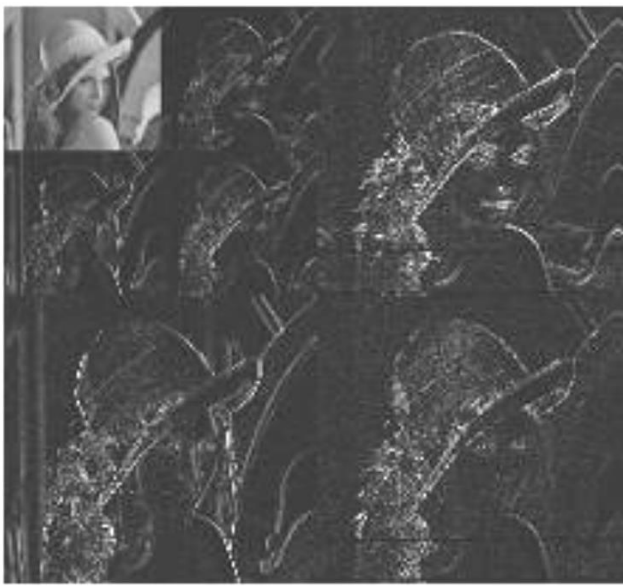
١- ٣ استخلاص الخواص:

لغرض تكوين مفتاح سرّي للتشفير يتميز بكونه وحيد بالاعتماد على الصفات المكتسبة من قزحية العين، فإن أغلب المعلومات المميزة لقزحية العين يجب أن تستخلص من صورة القزحية المعتمدة لدى المرسل والمستقبل، وإن الصفات المهمة والمميزة للقزحية فقط هي التي ترمز إلى رموز ثنائية لإتمام توليد المفتاح، وهناك طرائق عديدة يمكن بها استخلاص صفات صورة معينة من أشهرها ما يسمى بتحويل المويجة .

١-٣-١ تحويلات المويجة Wavelets Transformation

في السنوات العشر الأخيرة انتشرت الدراسات حول تحويلات المويجة بشكل واسع، إن استخدم هذا التحويل في العديد من التطبيقات منها الكبس والتمييز والاتصالات. تتلخص الفكرة الأساسية في عمل تحويل المويجة بتقسيم الإشارة الرقمية إلى جزئين (في حالة تحويل المويجة أحادي البعد) جزء الترددات العالية و جزء الترددات الواطئة باستخدام مرشحات خاصة (للترددات العالية والترددات الواطئة).

إن مكونات الحافات سوف تنحصر بشكل كبير في جزء الترددات العالية تتكرر عملية التقسيم هذه في جزء الترددات الواطئة إلى أن تتحلل الإشارة تماما أو تحدد من قبل المستخدم. أما إجراء عملية تحويل المويجة ذو البعد الثنائي للصورة بالأبعاد (m*n) فيمكن تعريفه بسهولة على انه تحويل مويجة أحادي البعد يطبق على البعدين m و n ، الشكل (٢) يوضح تطبيق تحويل المويجة ثنائي البعد على صورة ، ولهذا فان تحويل المويجة يمكن أن يستخدم في تحليل بيانات منطقة قزحية العين إلى مكونات تظهر بأبعاد محددة ومختلفة والتي ستمثل الصفات المستخلصة من صورة القزحية المعطاة.



LL_2	LH_2	LH_1
HL_2	HH_2	
HL_1		HH_1

(أ)الصورة بعد تطبيق تحويل الموجة (ب) هيكلية البيانات المحللة

الشكل (2): تحويل الموجة ثنائي البعد للصورة

١-٤ هدف البحث:

إن الهدف من البحث الاستفادة من خصائص الدالة الفوضوية بإدخالها كعامل أساسي بعملية التشفير.ومن خلال التداخل بين نتائج المرحلتين فقد تم الحصول على خوارزمية جديدة تمتاز بقوتها من حيث عدم إمكانية كشف المفتاح الا بعد الحصول على المقياس الحيوي المستخدم ومعرفة معلومات كاملة عن الدالة الفوضوية المستخدمة إضافة إلى خوارزمية العمل.

الفصل الثاني

٢-١ نظم الفوضى Chaotic Systems :

الفوضى هي واحدة من السلوكيات التي تربط الأنظمة الغير خطية والتي تحدث تطورا في القيم المحددة لنظام المعلومات، إذ اعتبر اكتشاف هذا النظام العشوائي ثورة أدت إلى العديد من القضايا المترابطة ونظرية الاستقرار وميزات هندسية جديدة وعروض لتمييز التواقيع، وقد استخدمت الدالة الفوضوية أساساً لتطوير النماذج الرياضية للأنظمة الغير خطية واجتذبت من قبل العديد من الرياضيين بسبب الحساسية العالية للقيمة الابتدائية وتطبيقاتها لمشاكل الحياة اليومية، ولما امتازت به الدوال الفوضوية من ميزات جيدة فقد استخدمت في هذا البحث لتشفير المفتاح المتماثل (Symmetric Key) في محاولة لزيادة سرية المعلومات المنقولة وتأمين عملية النقل .

٢-١-١ خصائص نظم الفوضى Properties Of Chaotic Systems :

يطلق مصطلح الفوضى على الأنظمة التي هي في الأساس غير خطية وتعرض سلوك عشوائي لمجموعة من القيم. ومع ذلك فان الحلول أو مسارات النظام تبقى محددة بمرحلة الفضاء. هذه المرحلة الغير مستقرة تعتمد بصورة كبيرة على قيم المتغيرات وعلى الطريقة التي يبدأ بها النظام. وفيما يلي الخصائص التي تميز النظام الفوضوي :

أ. الحساسية للقيمة الابتدائية Sensitivity to initial condition :

عند إعطاء قيمة ابتدائية لنظام معين فمن المعروف انه يمكن توقع الحالة المستقبلية للنظام الا انه في أنظمة الفوضى فان توقع المدى البعيد يستحيل التنبؤ به. وبصورة عامة فانه للقيم الابتدائية المعطاة مسارين والتي تكون في البداية حساسة ودقيقة للغاية وتختلف بشكل كبير وفي وقت قصير كما إن المعلومات الأولية للنظام تفقد نهائياً.

ب: Ergodicity

لا يوجد مصطلح علمي دقيق يعرف الـ (Ergodicity) لكنها خاصية المسير في الفضاء المحدد بشكل اعتباطي ويكون قريب من المراحل السابقة، وهذه ميزة الأنظمة الاحتمالية للمتغيرات العشوائية، أي انه النظام يعمل باستقلالية كما انه يكون بشكل محدد ومستقل عن الظروف الابتدائية ويفتقر إلى إمكانية التكهن به، كما أن كثافة القيم ثابتة في وقت محدد وهذه الخاصية ضرورية في مجال التشفير .

ج الدمج أو الخلط (Mixing):

وهي ميزة الأنظمة التي يكون الانتشار في الفضاء المحدد كله ضمن فترة قصيرة بفاصل زمني صغير من الشرط الابتدائي ، حيث انه في الأنظمة الفوضوية تكون هذه الفترة غير محدد بشرط ولكن عملها يكون بشكل اعتباطي من قيم الشرط الابتدائي حيث يكون المسير قريب من الشرط الابتدائي ولكن لا يتقاطع معه أبداً.

٢-١-٢ أنواع الدوال الفوضوية:

يوجد العديد من أنواع الدوال الفوضوية تمتاز كل منها بميزة عن غيرها ومن هذه الأنواع:

١- **Lorenz Equation**

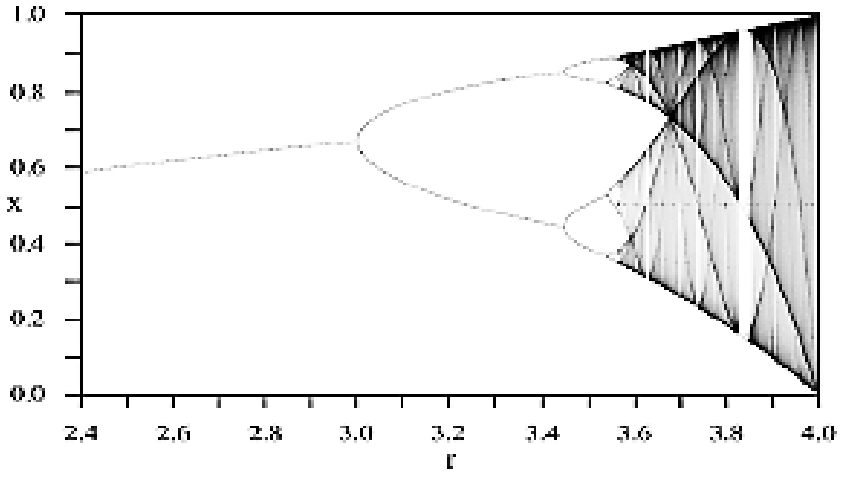
٢- **Rossler Equation**

٣- **Logistic Equation**

النوعين الأول والثاني(على التوالي) من الدوال الفوضوية تستخدم في النظام الفوضوي ثلاثي الأبعاد أما الدالة اللوجستية ، **Logistic Function**، فهي من ابسط أنواع الدوال الفوضوية المعروفة وقد تم دراستها لأول مرة عام ١٩٦٠ عندما لوحظ اهتمام الكثير

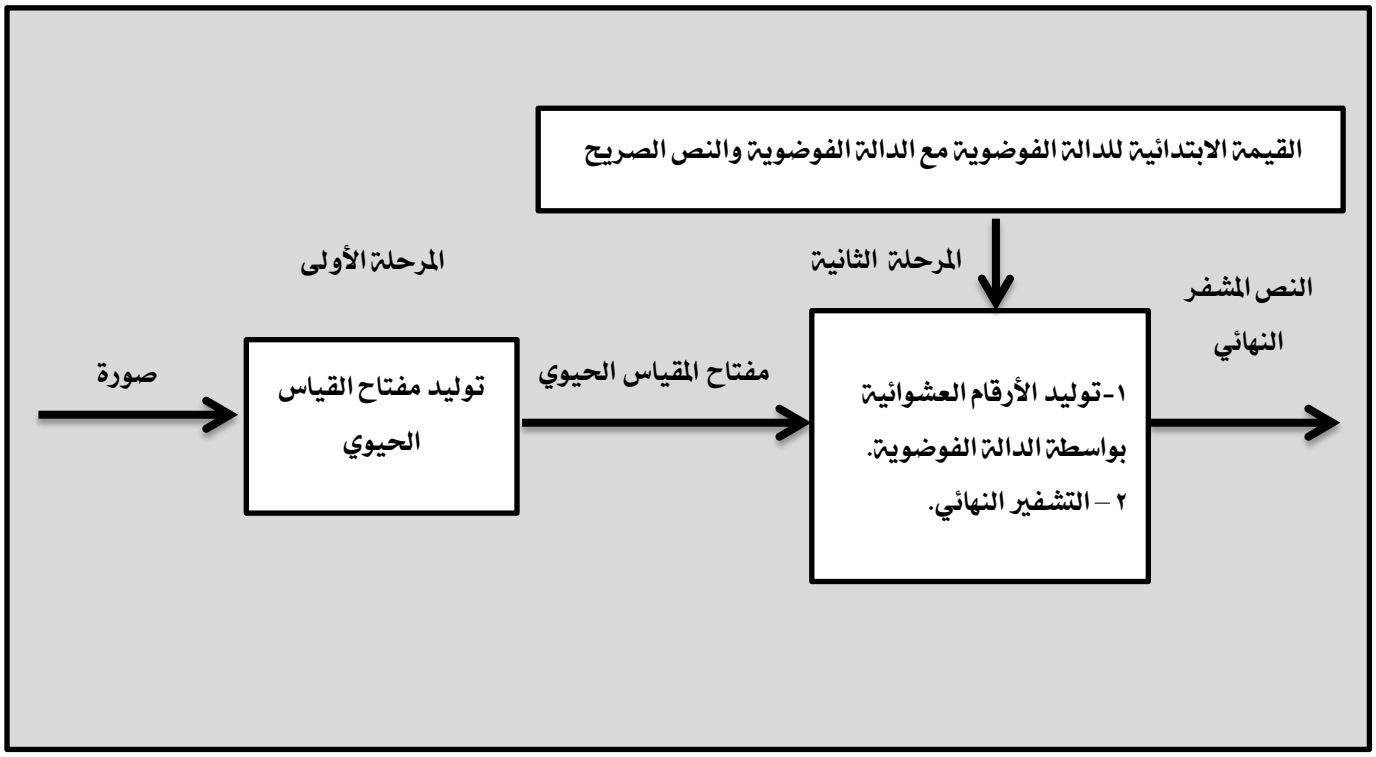
بخصائصها .إذ إن القيم المحددة التي تنشئها هذه الدالة هي قيم عشوائية تمامًا في صيغتها على الرغم من إنها تكون بين حدود، وهذه القيم لا تتكرر حتى بعد عدد من الدورات واهم صفة لهذه الدالة هي حساسيتها للقيمة الابتدائية وهذا يجعل الدالة ذات أهمية عالية في التشفير، أما التمثيل الرياضي للدالة فهو: $\chi_{n+1} = \lambda \chi_n (1 - \chi_n)$

حيث انه قيمة χ_n تتراوح بين (٠،١) وهو الجيل المتوقع وقيمة المتغير λ هي قيمة موجبة وهو الذي يحدد السلوك العشوائي للجيل التالي أما بالنسبة لقيمة χ_o تمثل القيمة الابتدائية، والشكل رقم (3) يوضح الرسم البياني التشعبي لسلوك الدالة اللوجستية (٦).



شكل (3) الرسم البياني التشعبي للدالة اللوجستية

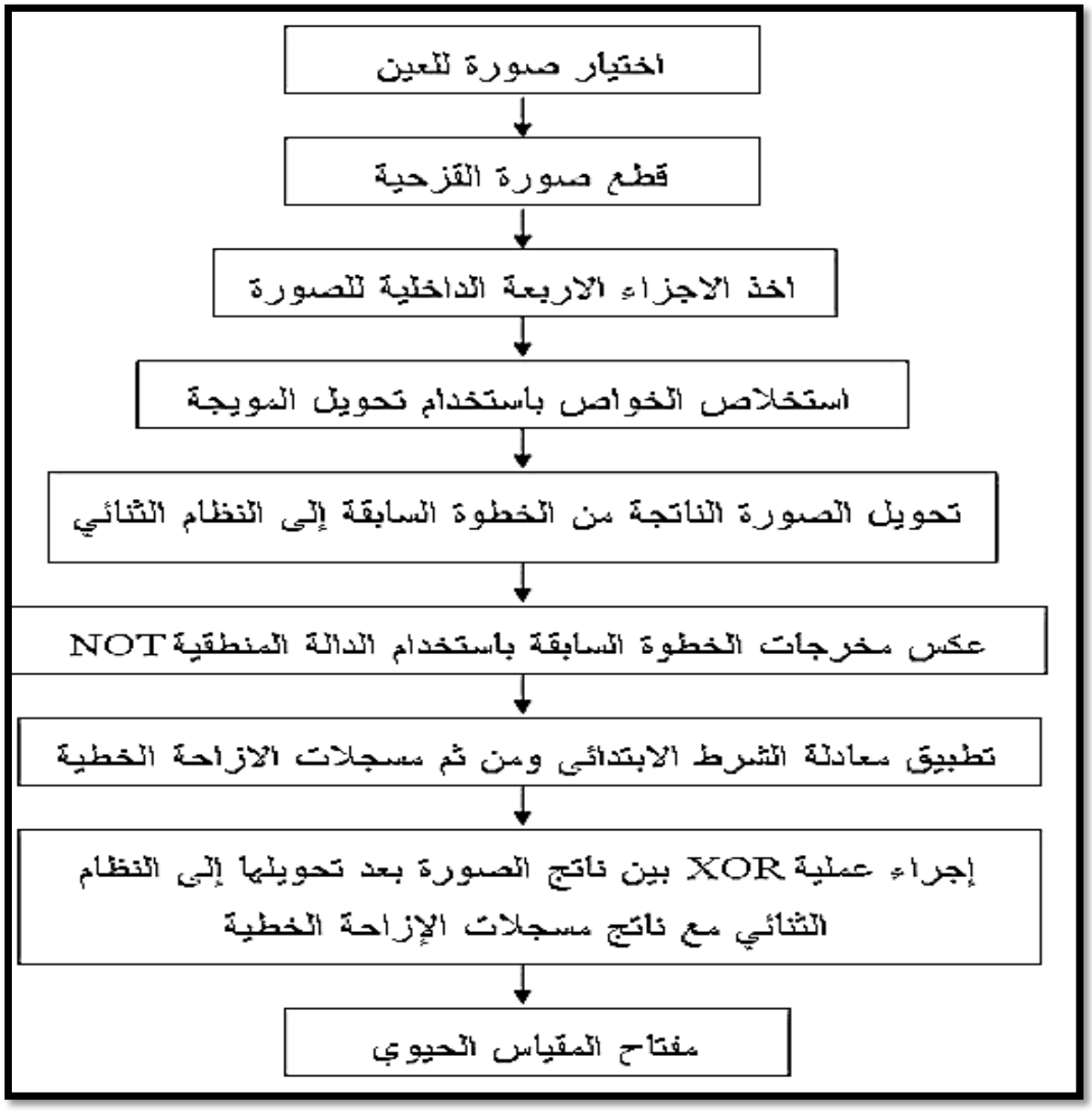
٢-٢ المخطط العام لطريقة التشفير المقترحة:



شكل (٤) طريقة التشفير المقترحة

٢-٢-١ المخطط الصندوقي لمرحلة توليد المفتاح الحيوي:

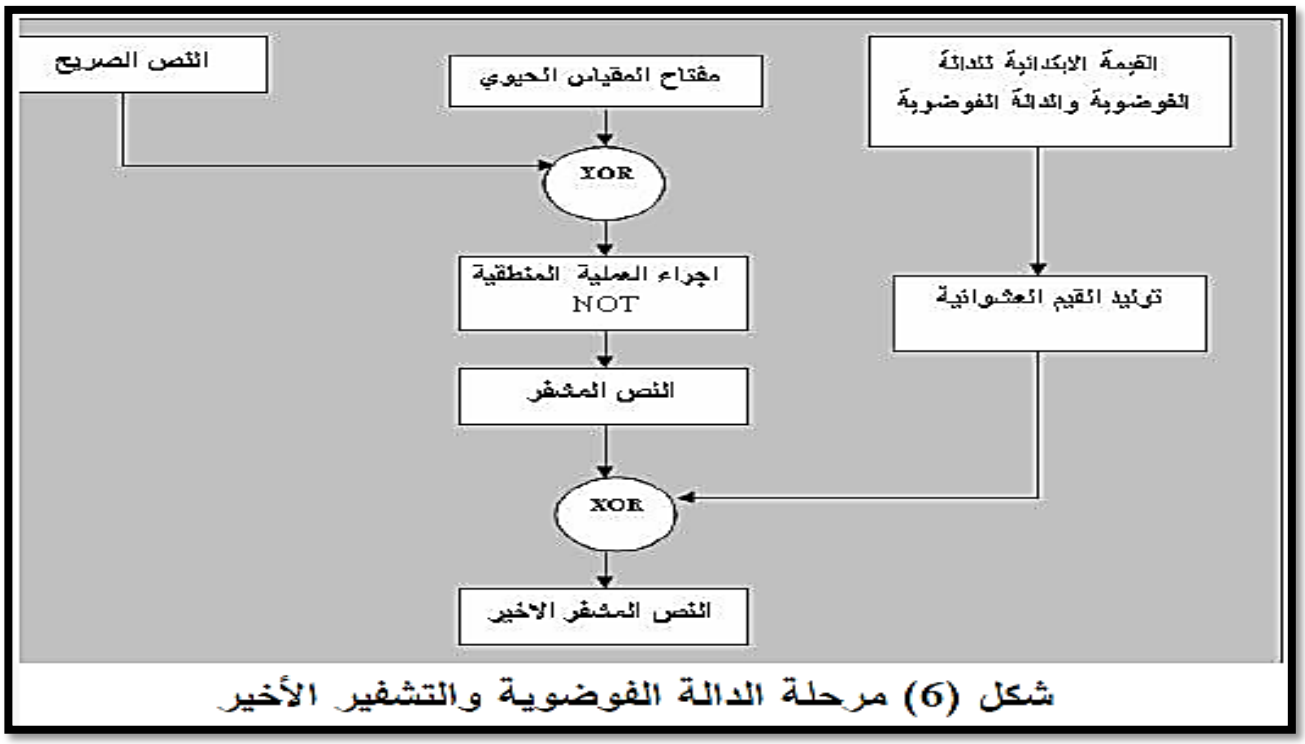
يوضح المخطط في الشكل التالي(٥) خطوات توليد المفتاح الحيوي بعد إدخال المقياس الحيوي (قزحية العين).



شكل (٥) مرحلة توليد المفتاح الحيوي

٢-٢-٢ المخطط الصندوقي لمرحلة الدالة الفوضوية والتشفير الأخير:

يوضح الشكل(٦) عملية توليد الأرقام العشوائية من الدالة الفوضوية واشتراكها بالتشفير الأخير.



شكل (6) مرحلة الدالة الفوضوية والتشفير الأخير

٢-٣ خوارزمية التشفير المقترحة:

المرحلة الأولى:

الإدخالات: قزحية العين

أ. البداية.

ب. اختيار صورة العين.

ج. قطع صورة القزحية باستخدام التقطيع المنتظمSystematic Classification

د. اخذ الأجزاء الأربعة الداخلية للصورة بأبعاد ١٦٠❖١٤٠.

هـ. استخدام طريقة تحويل المويجة لاستخلاص الخواص المهمة للصورة لإنتاج صورة مصغرة للقزحية بأبعاد ٢٤❖٢١.

و. تحويل الصورة الناتجة إلى الرمز الثنائي باستخدام طريقة العتبةThresholding

ز. استخدام الدالة المنطقية Not لعكس مخرجات الخطوة السابقة .

ح. استخدام معادلة الشرط الابتدائي على القيم الناتجة ومن ثم مسجلات الإزاحة الخطية LFSR.

ط. إجراء عملية XOR بين ناتج استخلاص الخواص والقيمة الناتجة من الخطوة السابقة لإنتاج مفتاح المقياس الحيوي.

ي. النهاية.

المخرجات مفتاح المقياس الحيوي.

المرحلة الثانية:

المدخلات: النص الصريح ،القيمة الابتدائية للدالة الفوضوية والدالة الفوضوية المستخدمة

أ. البداية

ب. إجراء عملية XOR بين النص الصريح ومفتاح المقياس الحيوي.

ج .استخدام الدالة المنطقية Not لعكس مخرجات الخطوة السابقة وإنتاج النص المشفر د. إجراء عملية XOR بين القيم العشوائية الناتجة من الدالة الفوضوية والنص المشفر

لإنتاج النص المشفر النهائي.

ه .النهاية

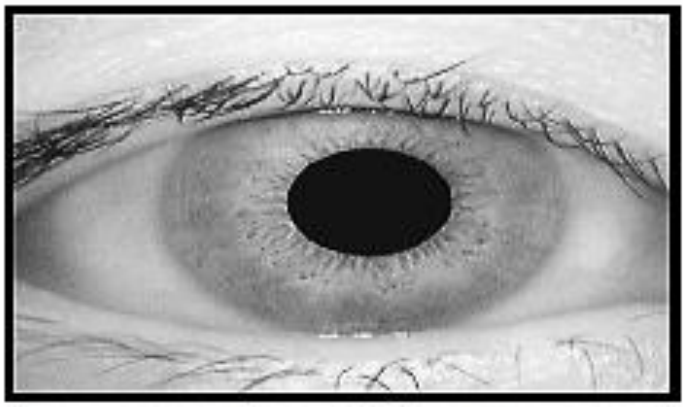
المخرجات: النص المشفر الأخير.

٢-٤ تشفير الصورة باستخدام التشفير الفوضوي :

كما ذكر سابقا فقد تم استغلال الصفات الفريدة الموجودة في قزحية العين لدى الإنسان في توليد مفتاح وحيد للتشفير بسلسلة من الخطوات لتتم عملية التشفير بعدها.

ففي المرحلة الأولى تتم عملية اشتقاق المفتاح كما يلي:

ك- يتم التقاط صورة العين للشخص المعتمد بجهاز تصوير خاص وهذه الصورة يجب أن تكون لدى الطرفين المرسل والمستقبل ، و نظرا لعدم إمكانية الحصول على كاميرا حرارية (Infrared Camera**) تم استخدام صور مأخوذة من الإنترنيت** CASIA DATABASE **وهي صور حرارية مستخدمة لأغراض الـ (** Biometric **) والشكل (٧) يوضح الصورة المعتمدة.**

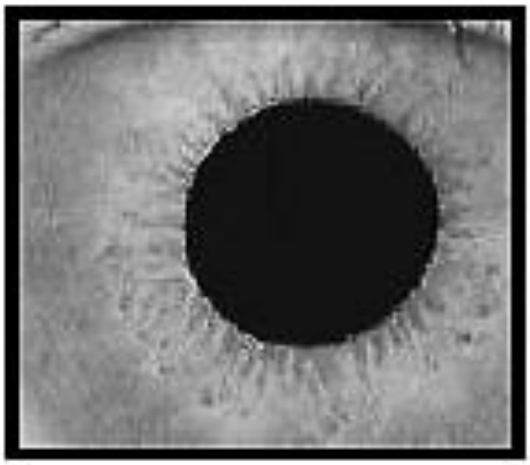


الشكل(7): صورة القزحية الناتجة

أ . بما أن الصورة الناتجة تضم صورة العين بأكملها بضمنها جفون ورموش العين وليست القزحية فقط، فيجب أولا قطع صورة القزحية ليتم التركيز عليها في عملية استخلاص الخواص، ولذا تقطع الصورة باستخدام التقطيع المنتظم(systematic classification**) إلى ١٦ جزء (٤×٤) كما في الشكل (٨).**

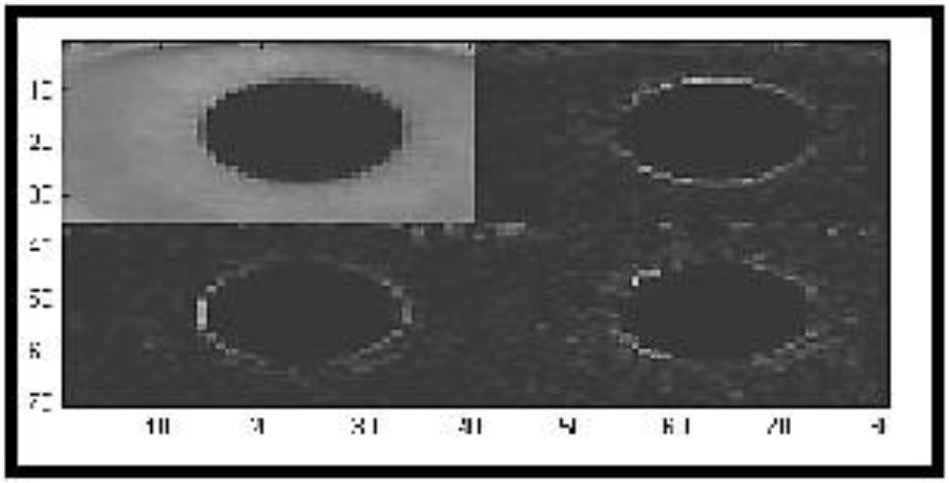
الشكل(8): صورة العين بعد تقطيعها الى 16 جزء

ب .من الشكل (5)نلاحظ استقرار القزحية في وسط الصورة أي الأجزاء الأربعة الداخلية للصورة بعد التقطيع لهذا يتم تجميع صورة القزحية من هذه الأجزاء لتكون الصورة الموضحة في الشكل (9)أبعادها ١٦٠*١٤٠.



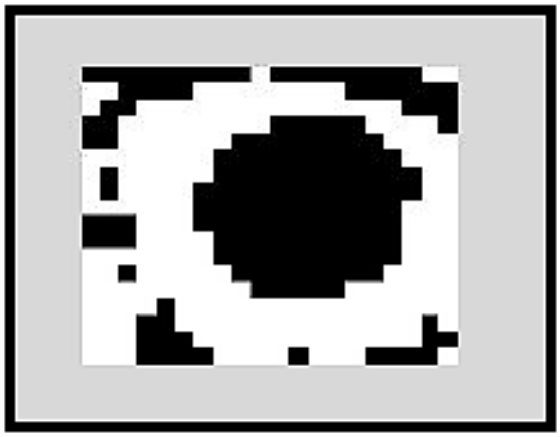
الشكل(9): القزحية بعد اقتصاصها من صورة العين

ج .بعد اقتصاص صورة القزحية من صورة العين تبدأ مرحلة استخلاص الخواص باستخدام دالة تحويل المويجة من نوع(Daubechies 1:DB 1) ولثلاث مستويات لتنتج صورة مصغرة للقزحية بأبعاد (٢١٠٢٤) تضم كافة الصفات الضرورية الموجودة فيها والتي ستوّلد المفتاح فيما بعد، الشكل (10) يوضح الصورة الناتجة بعد تحويل المويجة.



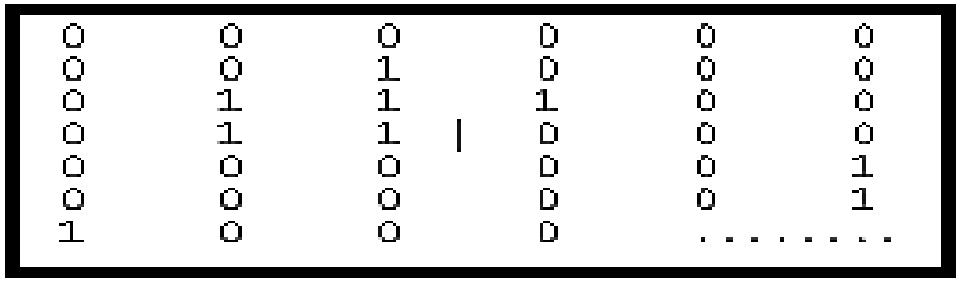
الشكل(10): صورة القزحية بعد استخلاص خواصها

د .تحول الصورة الناتجة من الخطوة (د) إلى رمز ثنائي باستخدام طريقة العتبة(thresholding) كما في الشكل التالي(١١) إذ يتم حساب قيمة العتبة من قيم الصورة نفسها بأخذ معدل القيم الناتجة مضافا اليها قيمة ثابتة لزيادة عشوائية القيم الناتجة، وبعد عدد من التجارب تم اختيار العدد ٥ كقيمة ثابتة مضافة إلى الناتج.



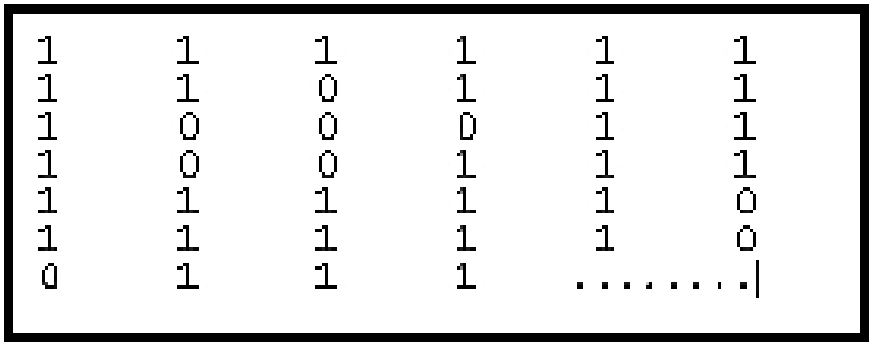
الشكل(11):الرمز الثنائي الناتج من قزحية العين

و. تحول الصورة الناتجة من الخطوة السابقة إلى مصفوفة ثنائية كما هو موضح بالشكل (١٢)



الشكل(12): التحويل الثنائي للصورة

ز .يتم استخدام الدالة المنطقية NOTلعكس الناتج السابق كما في الشكل(13) .



الشكل(13): المصفوفة بعد استخدام دالة NOT المنطقية

ح .يتم استخدام المعادلة رقم (2) الخاصة بتكوين الشرط الابتدائي:

Initial Condition =2n , n=1,2,3,….. ...(2)

ثم يحول الناتج إلى المفتاح السري باستخدام مسجلات الإزاحة الخطية ذات التغذية العكسية Linear feedback Shift Registers (LFSR) والذي يكون بطول n وآخر حقل هو Pq وهو متكون من مراحل بعدد n حسب ما هو موضح بالمعادلة رقم (٣)

[an-1,an-2,an-3,……..,a0], ai ϵ of Pq …(3)

وذلك بتطبيق المعادلة (٤):

$$B(x)= 1+ C_1 X+ C_2 X_2 .....,C_n X_n \text{ over} P_q \quad (٤)$$

وناتج هاتان العمليتان موضح في الشكل (١٤).

```
0   0   0   1   0   0   0
0   0   1   1   1   0   0
0   0   1   1   0   0   0
0   0   0   0   0   0   1
0   0   0   0   0   0   1
0   1   0   0   0   0   0
1   1   1   0   0   -------|
```

الشكل (14):الناتج من تطبيق المعادلتين السابقتين

ط. بعد ذلك يتم إجراء عملية XORبين ناتج استخلاص الخواص الأولى والمفتاح السري الناتج بالخطوة السابقة وكما في الشكل (١٥):

```
0   0   0   1   0   0   0
0   0   0   1   1   0   0
0   1   0   0   0   0   0
0   1   1   0   0   0   0
0   0   0   0   0   1   0
0   1   0   0   0   1   1
0   1   1   0   0   ......|
```

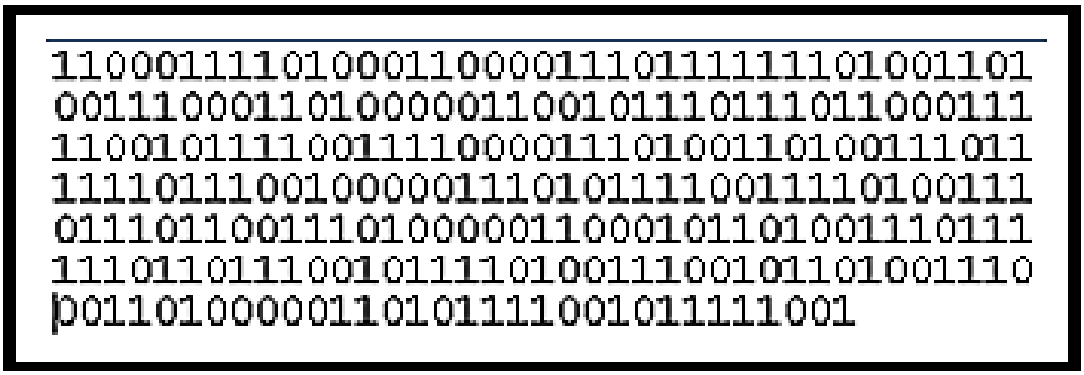
الشكل(15): ناتج عملية الـــXOR

ي. ثم يتم نقل ناتج الخطوة السابقة باستخدام الدالة المنطقية NOT وكان الناتج هو مفاتح المقياس الحيوي والذي يوضحه الشكل (١٦) :

```
1   1   1   0   1   1   1
1   1   1   0   0   1   1
1   0   1   1   1   1   1
1   0   0   1   1   1   1
1   1   1   1   1   0   1
1   0   1   1   1   0   0
1   0   0   1   1   |.......
```

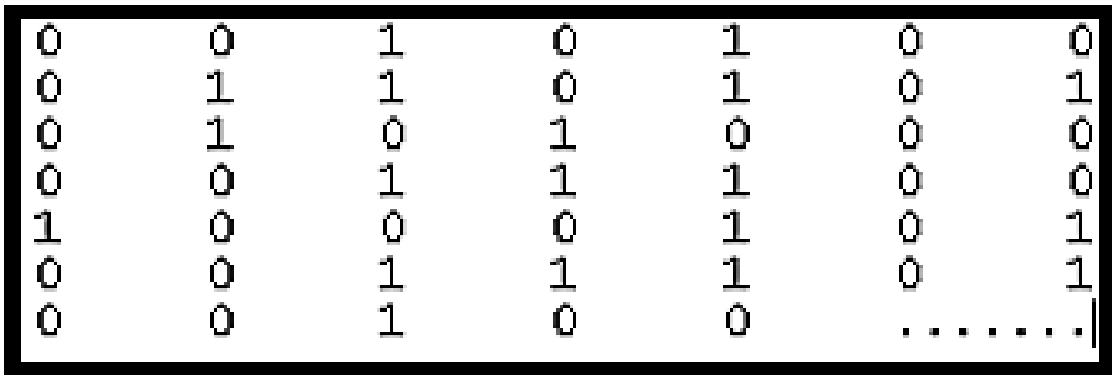
الشكل(16): مفتاح المقياس الحيوي الناتج

ك. لغرض تطبيق الخوارزمية المقترحة تم إدخال النص الصريح المراد تشفيره في بداية عملية التشفير وكان النص المعتمد هو: Chaotic Encryption using Biometric key حيث تم تحويله أولا إلى النظام الثنائي وكان الناتج كما في الشكل (17) :



الشكل(17) النص الصريح بعد تحويله الى النظام الثنائي

وبعد هذا يتم إجراء عملية XOR بين الصيغة الثنائية الناتجة للنص الصريح والمفتاح الحيوي الناتج بالخطوة السابقة لينتج النص المشفر الذي يوضحه الشكل (١٨) :



الشكل (18) النص المشفر الناتج ممثل بالصيغة الثنائية

٢-٥ الاستنتاجات

تم في البحث اقتراح فكرة وطريقة جديدة للتشفير وفك الشفرة باستخدام احد المقاييس الحيوية (قزحية العين) لتوليد مفتاح فريد ، وإخضاعه لعدد من العمليات بعد استخلاص خواصه المهمة باستخدام طريقة تحويل المويجة ومن ثم تطبيق معادلة الشرط الابتدائي وكذلك مسجلات الإزاحة الخطية، لينتج في النهاية مفتاح تشفير قوي السرية وامن كما تم إدخال احدى الدوال الفوضوية البسيطة لخوارزمية العمل للاستفادة من عشوائية الأرقام التي تنتجها والتي تدخل بعمليات مع النص المشفر لزيادة سرية النص المرسل وكناتج لهذه الخوارزمية فقد تم تشفير النصوص بطريقة حديثة تمتاز بالسرية العالية.

المصادر

(١) يو جي أون وكيم هيونجشيك، ٢٠١٠، "مخطط تشفير الصور مع التقليب العشوائي الزائف استنادًا إلى الخرائط الفوضوية"، محاكاة أرقام العلوم غير الخطية المشتركة.

(٢) خاريل روبوك وبوساونك. وغاسملويز.، ٢٠٠٨، "تقنية تشفير فوضوية جديدة للاتصالات الآمنة"، جامعة شمال أومبريا، Net 8ST، المملكة المتحدة.

(٣) ناكامورا ياسوهيسا، شارما تشيتان، (٢٠٠٣) "خدمات البيانات اللاسلكية: التقنيات ونماذج الأعمال والأسواق العالمية"، مطبعة جامعة كامبريدج.

(٤) - http://en.wikipedia.org/wiki/Biometrics.