Chaotic Encryption Based on Biometric Key

Saja j. Mohammed **Melad Jader** **Ielaf O. Abdul Majjed**
Sj_alkado@uomosul.edu.iq meladjader@uomosul.edu.iq io_osamah@uomosul.edu.iq
University of Mosul/ College of Computer Science and Mathematics

Received on: 20/8/2008 **Accepted on:4 /12/2008**

ABSTRACT

In this paper a new algorithm is suggested to encrypt data, as it was to benefit from human iris as one of Biometric properties in human body which distinguish the individual from the other to produce the encryption through extracting important features using Wavelet Transformation and then passing through a series of operations moderation as the first phase, at the second phase a chaotic function properties is used by leading it in encryption operation as a basic factor.

Through the overlap between the results of above phases a new encryption algorithm is produced which show strength, and could not discover the encryption key until getting the biometric property and finding complete information about the chaotic used function in addition to the working algorithm .

Keywords: biometrics, chaotic function, encryption, DWT.

التشفير الفوضوي باستخدام مفتاح المقياس الحيوي

سجى جاسم محمد **ميلاد جادر سعيد** **إيلاف أسامة عبدالمجيد**
كلية علوم الحاسبات والرياضيات
جامعة الموصل

تاريخ استلام البحث:٢٠/٨/٢٠٠٨ **تاريخ قبول البحث:٤/١٢/٢٠٠٨**

الملخص

تم في هذا البحث اقتراح خوارزمية جديدة لتشفير البيانات، اذ تم الاستفادة من احد المقاييس الحيوية للانسان التي تميز الفرد عن غيره لانتاج مفتاح التشفير، وذلك من خلال استخلاص الخواص المهمة باستخدام تحويلات المويجة Wavelet Transformation ومن ثم مروره بسلسلة من العمليات الوسطية كمرحلة اولى، في المرحلة الثانية فقد تم الاستفادة من خصائص الدالة الفوضوية بادخالها كعامل اساسي بعملية التشفير.

ومن خلال التداخل بين نتائج المرحلتين فقد تم الحصول على خوارزمية جديدة تمتاز بقوتها من حيث عدم امكانية كشف المفتاح الا بعد الحصول على المقياس الحيوي المستخدم ومعرفة معلومات كاملة عن الدالة الفوضوية المستخدمة اضافة الى خوارزمية العمل.

الكلمات المفتاحية: المقاييس الحيوية، الدالة الفوضوية، التشفير، التحويل المويجي المتقطع.

1. المقدمة:

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

إن أكثر الأعمال التي تعتمد على المفتاح المتماثل في التشفير تركز على كتلة من الـ(bits) التي تعتمد عليها الخوارزمية في التشفير، اذ ان 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 48 ساعة.[1][2].

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 الاسلوب ذو فائدة محددة. كما ان استخدام الدوال الرياضية لتوليد عدد من المفاتيح يعد من الطرائق الحديثة والغير مكتشفة الى حد كبير، ولكن البسيطة منها تعتبر غير كافية. وفي حالة كون خوارزمية التشفير عامة (Public) أي ان عملية توليد المفتاح تكون معروفة للمتطفل، وهذا يعني من السهولة معرفة واكتشاف مفتاح واحد ومن ثم اكتشاف باقي المفاتيح.[1]

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.

ومما ينبغي ذكره ان المقياس الحيوي قد استخدم في عديد من التطبيقات كعامل أساسي في عملية التمييز بين الأشخاص وبالذات استخدمت قزحية العين لهذا الغرض [3]، اما الدالة الفوضوية فقد تم التطرق اليها في عملية التشفير كما في تشفير الصور[4]، وفي عملية الاتصالات السرية[5]، بينما استخدمت من قبل عدد من الباحثين بعد دمجها مع خصائص المقاييس الحيوية في عملية تشفير الصور.[2]

تتضمن فكرة هذا البحث التشفير بواسطة المقاييس الحيوية اذ تم توليد مفتاح المقياس الحيوي (قزحية العين) من خلال استخلاص الخواص المهمة والمفيدة بعملية التشفير باستخدام احد التقنيات الخاصة بذلك وهي تحويلات المويجة ،إضافة الى استخدام الدالة الفوضوية للاستفادة من خواصها العشوائية، وكنتيجة لذلك فقد تم هنا وصف كيفية توليد المفتاح الحيوي للتشفير وفك الشفرة ودمجها مع الدوال الفوضوية.

2. المقاييس الحيوية:

تعرف المقاييس الحيوية على انها مقاييس للصفات او الميزات الفريدة للإنسان والمستخدمة عادة في عمليات التمييز الالكترونية او اثبات الشخصية. فالكائن البشري فريد وكذلك فان صفاته الفيزيائية والسلوكية فريدة ايضا، ولهذا يمكن اعتبار القيم الناتجة من عملية الاستخلاص الناجح لمعلومات هذه المقاييس المستحصلة من الميزات البشرية فريدة ولايمكن تكرارها عند اي شخص اخر[6]

أما عن مصطلح المقياس الحيوي (Biometrics) فهو مشتق من الكلمة الإغريقية (Bios) التي ترمز للحياة و كلمة (motron) وتعني المقياس، والذي يشير ايضاً الى حقل الاختلاف (وهو مايسمى الان بالاحصاء (Biostatistics)) والذي يهتم بتطور النظريات الرياضية والإحصائية المطبقة على مشاكل تحليل البيانات في علم البايولوجي. [7]

كل أنظمة المقاييس الحيوية تعمل بنفس الاسلوب، اذ يتم اولا التقاط عينة من مثال عن احد 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.[6]

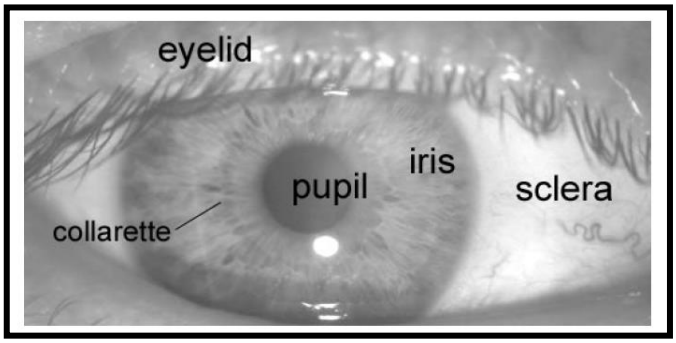
الفائدة الأساسية من استخدام المقياس الحيوي تكمن في كونها دائما حية وغير مستقرة الصفات من شخص لآخر ولهذا فلا يمكن الاشتباه بها ومع هذا فهي تعاني من تهديد خاص في سرية أنظمة المقاييس الحيوية. فالمهاجم قد يفسر بيانات المقياس الحيوي للفرد باستخدامها في عمليات أخرى غير قانونية.[2]

في السنوات الأخيرة عُرف عدد من التكنولوجيات المستخدمة لأخذ المقاييس الحيوية من الكائن البشري بصورة عامة والإنسان بصورة خاصة تختلف في محاسنها ومساؤها لكن القليل منها لاقى الترحيب والقبول منها (شكل الوجه، بصمة الإصبع، قزحية العين، شبكية العين، تمييز الصوت، التوقيع وهندسة اليد).[3]

2.1 خصائص قزحية العين:

في هذا البحث تم اعتماد قزحية العين كأحد المقاييس الحيوية حيث تعد الأنظمة المعتمدة عليها من اقل الأنظمة توليدا للأخطاء نسبة الى باقي التقنيات المستخدمة للمقاييس الحيوية. فمن الواضح انه من الضروري إيجاد جزء في جسم الإنسان ذو صفات ثابتة، فريدة جدا، سهلة القياس، وسريعة في حالة تمييز الأنماط.[8]

تمثل قزحية العين خواص مقياس حيوي فسيولوجي فهي تحتوي على نسيج فريد ومعقد بما فيه الكفاية لاستخدامه كتوقيع حيوي للفرد الشكل(1) يوضح فسيولوجية قزحية العين.



الشكل(1):فسيولوجية قزحية العين لدى الإنسان.

وبالمقارنة مع خواص المقاييس الحيوية الأخرى مثل الوجه وبصمة الإصبع فان أنماط قزحية العين تكون ثابتة وموثوق بها.[8]

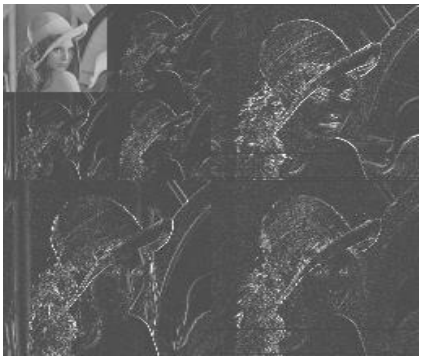
3. استخلاص الخواص:

لغرض تكوين مفتاح سري للتشفير يتميز بكونه وحيد بالاعتماد على الصفات المكتسبة من قزحية العين، فان اغلب المعلومات المميزة لقزحية العين يجب ان تستخلص من صورة القزحية المعتمدة لدى المرسل والمستقبل، ان الصفات المهمة والمميزة للقزحية فقط هي التي ترمز الى رموز ثنائية لإتمام توليد المفتاح، وهناك طرائق عديدة يمكن بها استخلاص صفات صورة معينة من أشهرها مايسمى بتحويل المويجة.

3.1 تحويلات المويجة Wavelets Transformation:

في السنوات العشر الاخيرة انتشرت الدراسات حول تحويلات المويجة بشكل واسع، اذ استخدم هذا التحويل في العديد من التطبيقات منها الكبس والتمييز والاتصالات. تتلخص الفكرة الأساسية في عمل تحويل المويجة بتقسيم الإشارة الرقمية الى جزئين (في حالة تحويل المويجة احادي البعد) جزء الترددات العالية و جزء الترددات الواطئة باستخدام مرشحات خاصة (للترددات العالية وللترددات الواطئة). [9]

مكونات الحافات سوف تنحصر بشكل كبير في جزء الترددات العالية. تتكرر عملية التقسيم هذه في جزء الترددات الواطئة الى ان تتحلل الإشارة تماما او تحدد من قبل المستخدم. أما إجراء عملية تحويل المويجة ذو البعد الثنائي للصورة بالابعاد (m*n) فيمكن تعريفه بسهولة على انه تحويل مويجة احادي البعد يطبق على البعدين m و n ، الشكل(2) يوضح تطبيق تحويل المويجة ثنائي البعد على صورة[9]، ولهذا فان تحويل المويجة يمكن ان يستخدم في تحليل بيانات منطقة قزحية العين الى مكونات تظهر بابعاد محددة ومختلفة والتي ستمثل الصفات المستخلصة من صورة القزحية المعطاة. [3]



LL_2	LH_2	LH_1
HL_2	HH_2	
HL_1		HH_1

(أ)الصورة بعد تطبيق تحويل المويجة **(ب) هيكلية البيانات المحللة**

الشكل (2): تحويل المويجة ثنائي البعد للصورة

4. نظم الفوضى Chaotic Systems:

الفوضى هي واحدة من السلوكيات التي تربط الأنظمة الغير خطية والتي تحدث تطوراً في القيم المحددة لنظام المعلومات. اذ اعتبر اكتشاف هذا النظام العشوائي ثورة أدت الى العديد من القضايا المترابطة ونظرية الاستقرار وميزات هندسية جديدة وعروض لتمييز التواقيع. وقد استخدمت الدالة الفوضوية اساساً 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.[10][11]

4.1 خصائص نظم الفوضى Properties Of Chaotic Systems:

يطلق مصطلح الفوضى على الأنظمة التي هي في الاساس غير خطية وتعرض سلوك عشوائي لمجموعة من القيم. ومع ذلك فان الحلول او 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: .[10][11]

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 ان المعلومات الاولية للنظام تفقد نهائياً.

ب. Ergodicity:

لا يوجد مصطلح علمي دقيق يعرف الـ(Ergodicity) لكنها خاصية المسير في الفضاء المحدد بشكل اع تباطي 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 الى إمكانية التكهن به، كما ان كثافة القيم ثابتة في وقت محدد وهذه الخاصية ضرورية في مجال التشفير.

ج. الدمج او 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 محددة بشرط ولكن عملها يكون بشكل اعتباطي من قيم الشرط الابتدائي حيث يكون المسير قريب من الشرط الابتدائي ولكن لا يتقاطع معه أبدا.

4.2 انواع الدوال الفوضوية:

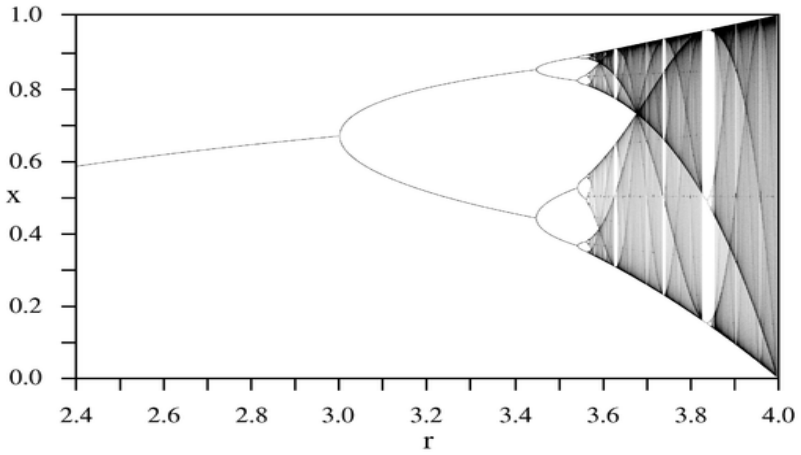
يوجد العديد من انواع الدوال الفوضوية تمتاز كل منها بميزة عن غيرها ومن هذه الأنواع:[11]

1. Lorenz Equation.
2. Rossler Equation.
3. Logistic Equation.

النوعين الاول والثاني (على التوالي) من الدوال الفوضوية تستخدم في النظام الفوضوي ثلاثي الابعاد، اما الدالة اللوجستية Logistic Function، فهي من ابسط انواع الدوال الفوضوية المعروفة وقد تم دراستها لاول مرة عام 1960 عندما لوحظ اهتمام الكثير بخصائصها. اذ ان القيم المحددة التي تنشئها هذه الدالة هي قيم عشوائية تماماً في صيغتها على الرغم من انها تكون بين حدود، وهذه القيم لاتتكرر حتى بعد عدد من الدورات واهم صفة لهذه الدالة هي حساسيتها للقيمة الابتدائية وهذا يجعل الدالة ذات اهمية عالية في التشفير.[1][11][12] اما التمثيل الرياضي للدالة فهو:

$$\chi_{n+1} = \lambda \chi_n (1 - \chi_n) \qquad \ldots(1)$$

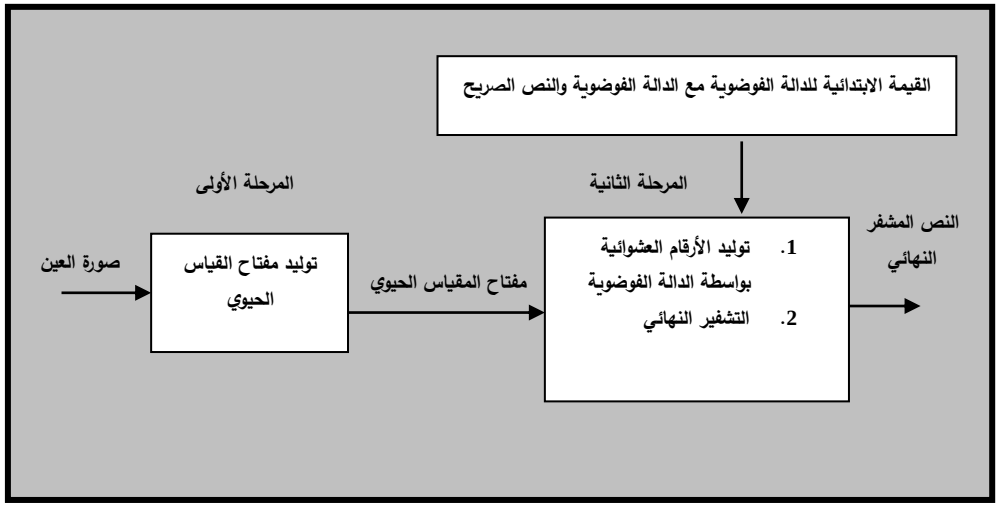
حيث انه قيمة χ_n تتراوح بين (0 ،1) وهو الجيل المتوقع وقيمة المتغير λ هي قيمة موجبة وهو الذي يحدد السلوك العشوائي للجيل التالي اما بالنسبة لقيمة χ_0 تمثل القيمة الابتدائية.، والشكل رقم (3) يوضح الرسم البياني التشعبي لسلوك الدالة اللوجستية.[7]



شكل (3) الرسم البياني التشعبي للدالة اللوجستية

5.المخطط العام لطريقة التشفير المقترحة:

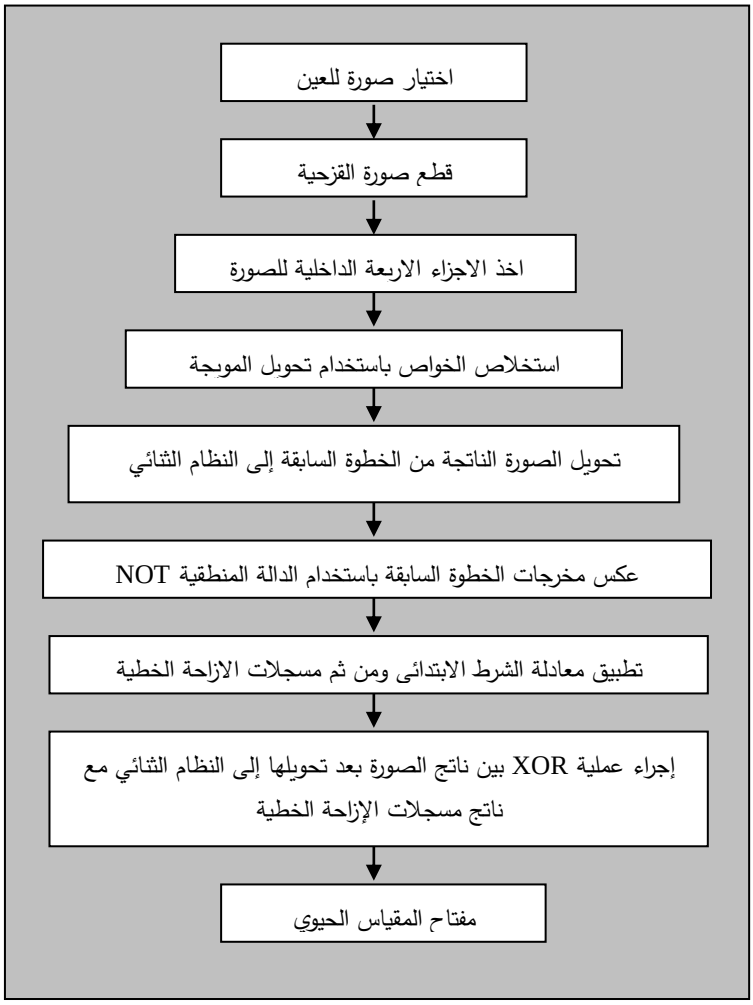
يوضح المخطط الموجود في الشكل رقم (4) الخطوات العامة لطريقة التشفير المقترحة



شكل (4) طريقة التشفير المقترحة

5.1 المخطط الصندوقي لمرحلة توليد المفتاح الحيوي:

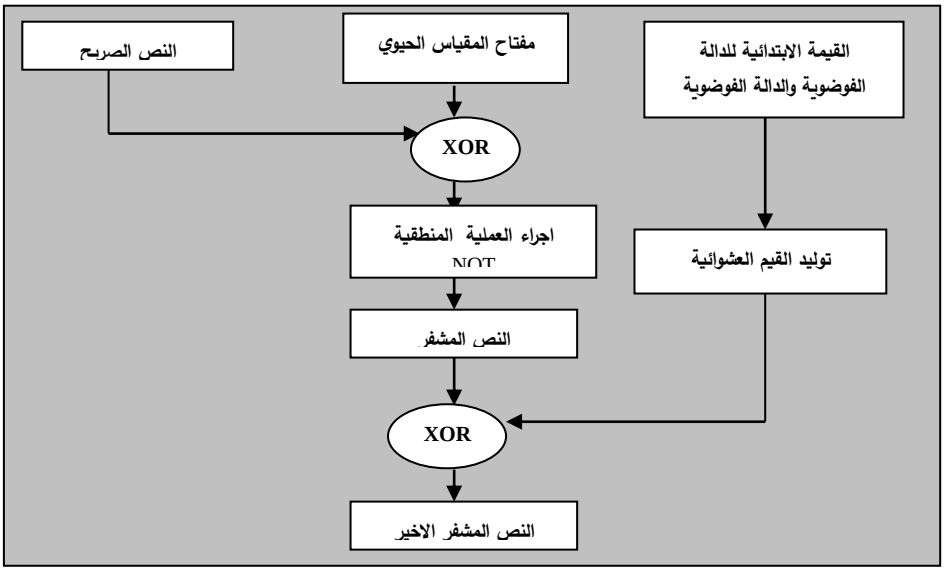
يوضح المخطط في الشكل رقم (5) خطوات توليد المفتاح الحيوي بعد إدخال المقياس الحيوي (قزحية العين).



شكل (5) مرحلة توليد المفتاح الحيوي

5.2 المخطط الصندوقي لمرحلة الدالة الفوضوية والتشفير الأخير:

يوضح الشكل (6) عملية توليد الارقام العشوائية من الدالة الفوضوية واشتراكها بالتشفير الاخير



شكل (6) مرحلة الدالة الفوضوية والتشفير الأخير

6. خوارزمية التشفير المقترحة:

المرحلة الاولى:

الادخالات: قزحية العين

أ. البداية.

ب. اختيار صورة العين.

ج. قطع صورة القزحية باستخدام التقطيع المنتظم Systematic Classification.

د. اخذ الأجزاء الأربعة الداخلية للصورة بأبعاد 160*140.

هـ. استخدام طريقة تحويل المويجة لاستخلاص الخواص المهمة للصورة لإنتاج صورة مصغرة للقزحية بأبعاد 24*21.

و. تحويل الصورة الناتجة الى الرمز الثنائي باستخدام طريقة العتبة Thresholding.

ز. استخدام الدالة المنطقية Not لعكس مخرجات الخطوة السابقة.

ح. استخدام معادلة الشرط الابتدائي على القيم الناتجة ومن ثم مسجلات الازاحة الخطيةLFSR.

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

ي. النهاية.

المخرجات:مفتاح المقياس الحيوي.

المرحلة الثانية:

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

أ. البداية.

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

ج. استخدام الدالة المنطقية Not لعكس مخرجات الخطوة السابقة وانتاج النص المشفر

د. اجراء عملية XOR بين القيم العشوائية الناتجة من الدالة الفوضوية والنص المشفر لانتاج النص المشفر النهائي.

هـ. النهاية.

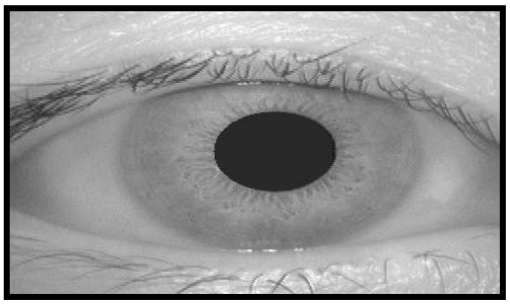
المخرجات:النص المشفر الاخير.

7. الجانب العملي:

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

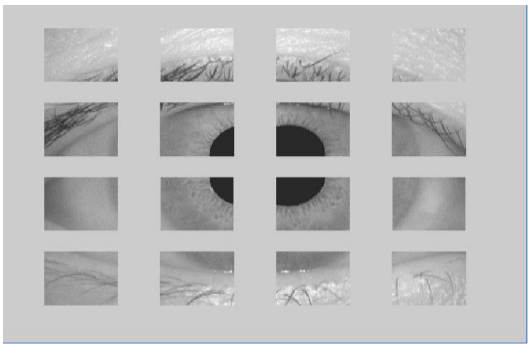
ففي المرحلة الأولى تتم عملية اشتقاق المفتاح كما يلي:

ك. يتم التقاط صورة العين للشخص المعتمد بجهاز تصوير خاص وهذه الصورة يجب ان تكون لدى الطرفين المرسل والمستقبل،و نظراً لعدم امكانية الحصول على كاميرا حرارية (Infrared Camera) تم استخدام صور مأخوذة من الانترنيت CASIA DATABASE وهي صور حرارية مستخدمة لأغراض الـ(Biometric) الشكل(7) يوضح الصورة المعتمدة.



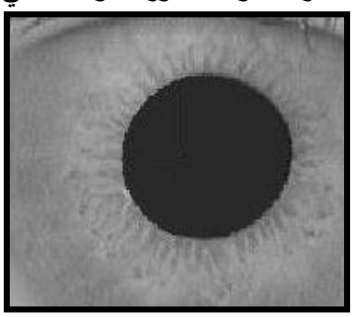
الشكل(7): صورة القزحية الناتجة

أ. بما ان الصورة الناتجة تضم صورة العين بأكملها بضمنها جفون ورموش العين وليست القزحية فقط فيجب اولا قطع صورة القزحية ليتم التركيز عليها في عملية استخلاص الخواص، ولذا تقطع الصورة باستخدام التقطيع المنتظم (systematic classification) الى 16 جزء (4*4) كما في الشكل (8).



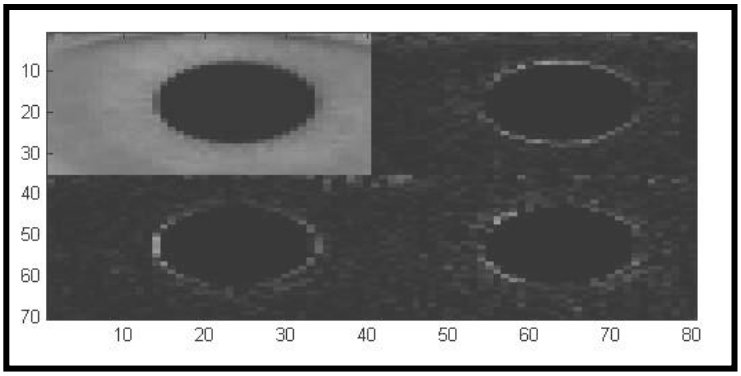
الشكل(8): صورة العين بعد تقطيعها الى 16 جزء

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 160*140.



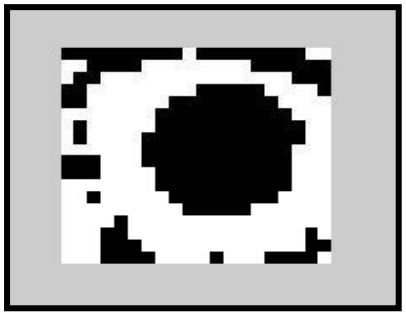
الشكل(9): القزحية بعد اقتصاصها من صورة العين

ج. بعد اقتصاص صورة القزحية من صورة العين تبدأ مرحلة استخلاص الخواص باستخدام دالة تحويل المويجة من نوع (Daubechies 1:DB1) ولثلاث مستويات لتنتج صورة مصغرة للقزحية (بأبعاد 24*21) تضم كافة الصفات الضرورية الموجودة فيها والتي ستولد المفتاح في ما بعد، الشكل (10) يوضح الصورة الناتجة بعد تحويل المويجة.



الشكل(10): صورة القزحية بعد استخلاص خواصها

د. تحول الصورة الناتجة من الخطوة (د) الى رمز ثنائي باستخدام طريقة العتبة(thresholding) الشكل (11)، اذ يتم حساب قيمة العتبة من قيم الصورة نفسها باخذ معدل القيم الناتجة مضافا اليها قيمة ثابتة لزيادة عشوائية القيم الناتجة، وبعد عدد من التجارب تم اختيار العدد 5 كقيمة ثابتة مضافة الى الناتج.



الشكل(11):الرمز الثنائي الناتج من قزحية العين

و. تحول الصورة الناتجة من الخطوة السابقة الى مصفوفة ثنائية كما هو موضح في الشكل (12).

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

الشكل(12): التحويل الثنائي للصورة

ز. يتم استخدام الدالة المنطقية NOT لعكس الناتج السابق كما في الشكل (13):

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

الشكل(13): المصفوفة بعد استخدام دالة NOT المنطقية

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

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

ثم يحول الناتج الى المفتاح السري باستخدام مسجلات الازاحة الخطية ذات التغذية العكسية Linear feedback Shift Registers (LFSR) والذي يكون بطول n واخر حقل هو Pq وهو متكون من مراحل بعدد n حسب ما هو موضح بالمعادلة رقم (3):

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

وذلك بتطبيق المعادلة (4):

$$B(x) = 1 + C_1X + C_2X_2 ....., C_nX_n overP_q \quad \ldots(4)$$

وناتج هاتان العمليتان موضح في الشكل (14):

```
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 XOR بين ناتج استخلاص الخواص الأولى والمفتاح السري الناتج بالخطوة السابقة وكما في الشكل (15):

```
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 الـXOR

ي. ثم يتم قلب ناتج الخطوة السابقة باستخدام الدالة المنطقية NOT وكان الناتج هو مفتاح المقياس الحيوي والذي يوضحه الشكل (16):

```
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 اولا الى النظام الثنائي وكان الناتج كما في الشكل (17):

```
11000111101000110000111011111111010011010
00111000110100000110010111011101100011110
11001011110011111000011101001101001110110
11110111001000001110101111100111101001110
01110111001110100000110001011010011101110
11101101110010111101001110010110100111010
00110100000110101111001011111001
```

الشكل(17) النص الصريح بعد تحويله الى النظام الثنائي

وبعد هذا يتم اجراء عملية XOR بين الصيغة الثنائية الناتجة للنص الصريح والمفتاح الحيوي الناتج بالخطوة السابقة لينتج النص المشفر الذي يوضحه الشكل (18) :

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

الشكل (18) النص المشفر الناتج ممثل بالصيغة الثنائية

ل. بعد تحديد قيمة ابتدائية للدالة الفوضوية (X_0=0.2) واستخدام الدالة اللوجستية المعرفة بالمعادلة(1) لإنتاج قيم عشوائية، تم ادخال النص المشفر الناتج مع ناتج الدالة اللوجستية الى دالة XOR المنطقية وكانت النتائج موضحة في الشكل (19):

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

الشكل (19) النص المشفر النهائي بعد تطبيق الدالة اللوجستية

م. اخيرا يتم تحويل النص المشفر النهائي الموضح في الشكل (19) الى حروف او رموز او أرقام ومن ثم إرساله كناتج للتشفير والموضح بما يلي:

áN«X1õ9æXdÏÙ ùó]-% Hæ) z :µYÉÁ>þ

أما بالنسبة لعملية فك الشفرة فإنها تسير بنفس مسار عملية التشفير لان المقياس الحيوي يكون معروف للمرسل والمستقبل، غير انه في حالة فك الشفرة نستخدم النص المشفر النهائي الذي يتم استلامه من قبل المخول المرسل له الرسالة في عملية XOR الثانية مع ناتج الدالة الفوضوية التي يكون هناك اتفاق مسبق قد تم بين الجهتين حول القيمة الابتدائية ونوعية الدالة الفوضوية المستخدمة والقيمة التي تنتج من هذه الخطوة يتم إدخالها الى XOR الأولى مع قيمة مفتاح المقياس الحيوي المتوفر في الجهتين والذي يستخدم للتشفير وفك الشفرة، وبهذا

فانه من السهولة للشخص المستلم للنص المشفر والذي يكون هو المعني بالمقياس الحيوي ان يفك شفرة النص ويرجعه الى النص الصريح.

8. تحليل ومناقشة الطريقة المقترحة:

اعتمادا على المقاييس المعتمدة في قياس أمنية أي خوارزمية تشفير، تمتاز الطريقة المقترحة بالميزات الآتية[13]:

- تنمح الطريقة المقترحة درجة عالية من السرية، ففي حالة تعرضها الى هجوم من هجمات فرضية أسوأ الاحتمالات لا يمكن الحصول على النص الأصلي وذلك بسبب انفرادية المفتاح المستخدم(قزحية العين).
- يمتاز مفتاح الطريقة بالبساطة (سلسلة ثنائية الأرقام) وسهولة الاشتقاق من المفتاح الحيوي بالإضافة الى عدم التكرار (non- periodic)، حيث انه يعتمد على مبدأ مفتاح المرة الواحدة (one time pad system).
- بساطة عملية التشفير (Encryption) او فك الشفرة (Decryption).
- عدم احتواءها على ميزة انتشار الخطأ (Error Propagation).
- لا يوجد توسيع (Expansion) للنص المشفر حيث ان حجمه بحجم النص الأصلي.

9. 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.

10. التوصيات:

1. استخدام دوال فوضوية أخرى.
2. دمج الدوال الفوضوية مع طرائق التشفير الأخرى مثل RSA او DES لتحسينها وجعلها أكثر أماناً.
3. استخدام أكثر من مقياس حيوي في خوارزمية واحدة.

المصادر

[1]. Bose Dr. Ranjan and Banerjee Amitabha,1999, "Implementing Symmetric Cryptography using Chaos Functions",Electrical Engineering Department,Indian Institute of Technology, Hauz Ichas, New Delhi-110016**.**

[2]. Alghamdi Abdullah Sharaf, Ullah Hanif, Mahmud Maqsood and Khan Muhammad khurram,2009;" Bio-Chaotic Stream Cipher-Based Iris Image Encryption",department of software engineering and information System King Saud University, Riyadh, Kindom of Saudi Arabia.

[3]. Al-Gurairi Maha Abdul-Rhman Hasso; 2006; "Biometric Identification Based on Improved Iris Recognition Techniques"; A Ph. D. Thesis Submitted To The Council of the College of Computer and Mathematical Sciences University of Mosul.

[4]. Yoou Ji on and Kim Hyoungshick,2010,"An image encryption scheme with a pseudorandom permutation based on chaotic maps", commun Nonlinear Sci Numer Simulat.

[5]. Kharel Rupuk and Busawon K. and ghassemlooy Z.,2008,

"A novel chaotic Encryption technique for secure communication", North Umbria university, Net 8ST,UK.

[6]. Nakamura Yasuhisa, Sharma Chetan, (2003) "*Wireless Data Services: Technologies, Business Models and Global Markets",* Cambridge University Press.

[7]. Wikipedia Contributors, "*Biometrics Information on Wikipedia.com", Wikipedia, The Free Encyclopedia",* Update: March 2010, Cited at:

http://en.wikipedia.org/wiki/Biometrics.

[8]. Daugman John G.**,** (1993), *"High Confidence Visual Recognition of Persons by a Test of Statistical Independence"***,** IEEE Transaction on Pattern Analysis and Machine Intelligence, Vol. 15, no. 11, pp. 1148-1161.

[9]. Taha Dujan Basheer; 2004;"Digital Image Watermarking Techniques For Copyright Protection",A Thesis Submitted to The Council of the College of Computer Sciences & Mathematics University of Mosul, In Partial Fulfillment for Ph.D. Degree In Computer Science.

[10]. Glenn Elert;2007 ;"Measuring Chaos".

[11]. Lawande Q.V. , Ivan B.R and Phodapkar S.D.,2005;"Chaos Based Cryptography" A new approach To Secure Communication.

[12]. Amri Abidin Ahmad Faisal ,2009;"A design For Chaotic Symmetric Cryptography Based on Baptista Method, European Journal of Scientific Research ,ISSN 1450-216x vol.36 NO.1 ,pp.10-21,EuroJournals Publishing .Inc.2009

[13]. Beker, Henry and Piper , Fred, 1982," cipher system the protection of communication ", Northworld publication, London, .pp., 162-166.