

تقنية رياضية لحماية الخصوصية و الموثوقية من خلال معلومات قزحية العين

باسم سهر ياسين

قسم علوم الحاسبات ، كلية شط العرب الجامعة

E-mail :basim_yaseen2000@yahoo.com

الخلاصة:

يقترح البحث طريقة رياضية لتعريف بهوية الشخص من خلال معلومات مستخلصة من قزحية العين، وتتكون من جزأين: الأول – بناء قاعدة بيانات للمعلومات الرقمية المستخلصة من قزحية العين للأشخاص المعنيين بالنظام ، والثاني – هو مجموعة خطوات رياضية لإنتاج معلومات سرية رقمية من المعلومات المستخلصة من الصورة ، و تبدأ مراحل النظام بأستحصال المعلومات الجينية للعين البشرية المتمثلة بصورة القزحية للشخص، تحول الى مجموع اوزان قيم مجموعة من الخلايا (اية خلية ومحيطها من الخلايا) محسوبة من مصفوفة القزحية ، تبدأ في المرحلة التالية اضافة السرية في انتاج الارقام من خلال انتخاب طريقة لإنتاج مواقع محددة من المصفوفة الرقمية الناتجة ، وتعتمد القيمة الرقمية المطلوبة على درجة سرية التطبيق المراد استخدام الرقم فيه، ثم تدخل الهيئة الرقمية الجديدة في خوارزمية اختزال وعزل لغرض التحويل للصيغة النهائية التي سوف تعتمد. والهدف من البحث الحالي هو اعتماد قاعدة ثابتة (قزحية العين) لإنتاج معلومات رقمية سرية وعشوائية لغرض استخدامها في التطبيقات المختلفة لعلم التشفير كمفاتيح لتشفير المعلومات السرية او في الموثوقية في أنظمة المفاتيح المعلن كالتوقيع والتحقق الرقمي وإنشاء اسلوب جديد في تحويل وعزل الارقام الصحيحة الى سلاسل بسيطة .

الكلمات المفتاحية: قزحية العين ، علم التشفير ، الخصوصية والموثوقية ، الارقام العشوائية.

Biology features أنواع السمات الحيوية types

هناك ثلاث انواع من السمات الحيوية (Fernald 2006,Hugo 2010)هي:

- أ (سمات حيوية تعتمد على الخواص الفسيولوجية : و هي سمات تعكس الشكل الجسدي للإنسان و تتضمن : بصمة الإصبع ، بصمة العين ، بصمة القزحية ، الشبكية ، الوجه ، البصمة الوراثية (DNA) ، بصمة راحة الكف ، بصمة أبعاد الكف.
- ب (سمات حيوية تعتمد على الخواص السلوكية : سمات تعكس سلوكيات و تصرفات الإنسان و تتضمن : التوقيع ، الخط ، الكتابة.
- ج (سمات مزدوجة : وهي التي تجمع بين السمات الفسيولوجية و السلوكية و تتضمن : البصمة الصوتية و أثار القدم.

3 . 1 خصائص السمات الحيوية Biology features characteristics (Hugo 2010)

تتميز كل سمة من السمات الحيوية بمجموعة خواص قياسية ، تعتبر بمجملها منظومة لقياس مدى اعتمادية هذه السمة عن غيرها ، وهذه الخصائص هي:

- (1) العالمية : مدى انتشارها بين البشر.
- (2) الوجدانية و الانفراد : مدى نجاح السمات الحيوية في التفريق بين الأفراد بعضهم البعض .
- (3) الدوام : مدى نجاح السمات الحيوية في البقاء و الثبات مدى الحياة.
- (4) التحصيل : سهولة الاكتساب للمقاييس.
- (5) الأداء : دقة و سرعة و قوة التقنية المستخدمة.
- (6) القبول : درجة القبول و الموافقة على التقنية.

المقدمة An introduction

أدى تطور حقول العلم المختلفة إلى إيجاد الكثير من الوسائل و التقنيات الحديثة التي ركزت و وجهت اهتماماتها على كيفية تعزيز الأمن بسبب ازدياد الحاجة للدرجات العالية من الأمانة و السرية لغرض حماية الأفراد و المجتمعات . ومن هنا تم تطوير علم المقاييس و السمات الحيوية الذي أثبت فيما بعد دقته و كفاءته في تحديد هوية الشخص و توثيقها. يستخدم المجال الأمني ثلاثة طرق لغرض التوثيق و المصادقية وتحديد الهوية و هي : ١-معلومات رقمية : ككلمة المرور أو المعلومات الشخصية.

٢-وثائق : كالبطاقات الذكية.

٣ -صفات حيوية : مثل السمات الحيوية (بصمة الإصبع أو القزحية ...الخ. و عند النظر في هذه الطرق الثلاث نجد أن الطريقة الأخيرة و هي ما يتسم به الإنسان من أكثر الطرق مصادقية و أوثقها نتائج، حيث أن كلمة المرور أو المعلومات الشخصية أو البطاقات الذكية تواجه الكثير من المشاكل، فمن الممكن أن تتعرض للسرق أو التخمين أو النسيان، كما أنها قد تتعرض للضياع أو الإغارة أو تكون مكلفة مادياً. ولكن ما يتسم به الإنسان خالفت جميع المشاكل التي تعرضت لها الطرق السابقة. كما يتم استخدام التقنيات المعتمدة على السمات الحيوية في القطاع الأمني سواء في المطارات أو الموانئ و يتم استخدامها أيضاً في أجهزة الصرف الآلي و في المجالات التي تتطلب أخذ الحيطة و الحذر من حيث الهوية و التحقق من مصداقيتها (Mark 2005, Serge 2006).

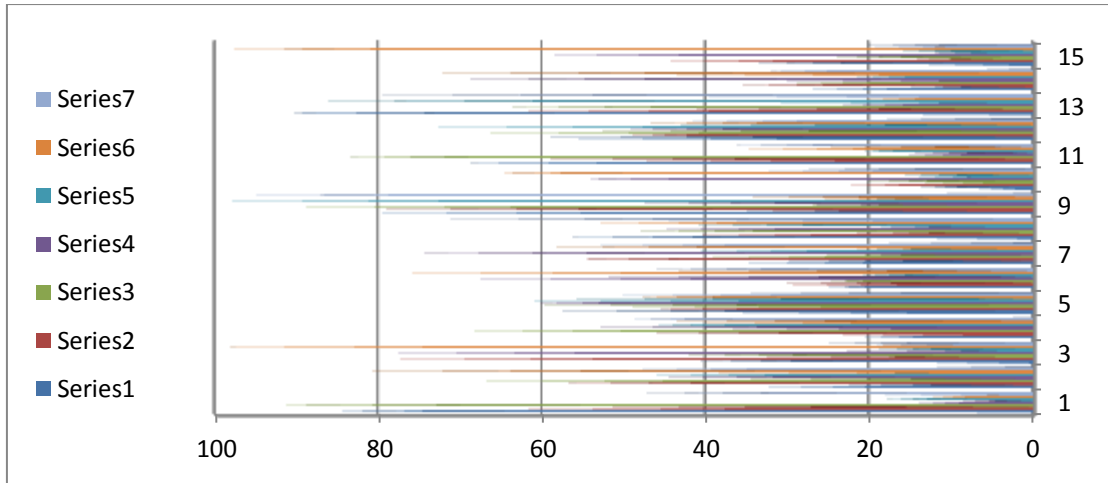
(7) المراوغة و التحايل: سهولة استخدام البدائل
جسم الانسان ممكن ان تستخدم في التعريف
والمصادقية الشخصية (Lee 2009):

ويوضح الجدول ادناه النسب المئوية لمدى
تحقق الخصائص المذكورة لكل سمة حيوية في

جدول 1- جدول بالنسب المئوية لخصائص السمات الحيوية.

السمة الحيوية	خاصية الوحدة	خاصية العالمية	خاصية الدوام	خاصية التحصيل	خاصية الاداء	خاصية القبول	خاصية التحايل	قيمة المعدل لنسب الخواص
DNA	87 %	95 %	94 %	19 %	19 %	15 %	55 %	54.85714
الاذن	46 %	58 %	85 %	50 %	53 %	100 %	50 %	63.14286
الوجه	44 %	92 %	50 %	84 %	25 %	99 %	37 %	61.57143
ابعاد الاصابع	23 %	58 %	70 %	75 %	47 %	70 %	50 %	56.14286
بصمة الاصبع	78 %	47 %	91 %	62 %	98 %	49 %	71 %	70.85714
المشي	25 %	50 %	25 %	100 %	21 %	100 %	50 %	53
بصمة ابعاد الكف	54 %	57 %	54 %	78 %	50 %	67 %	59 %	59.85714
بصمة اوردة الكف	57 %	52 %	53 %	52 %	50 %	56 %	97 %	59.57143
القزحية	96 %	93 %	97 %	62 %	98 %	50 %	95 %	84.42857
بصمة ايقاع الاصابع	17 %	23 %	28 %	56 %	25 %	67 %	50 %	38
رائحة الجسم	70 %	89 %	85 %	25 %	21 %	50 %	37 %	53.85714
بصمة راحة الكف	96 %	50 %	100 %	50 %	97 %	50 %	50 %	70.42857
الشبكية	94 %	86 %	66 %	29 %	98 %	23 %	100 %	70.85714
التوقيع	35 %	39 %	34 %	83 %	23 %	97 %	33 %	49.14286
الصوت	39 %	49 %	31 %	59 %	23 %	99 %	33 %	47.57143

من خلال جدول القيم اعلاه والمخطط التوضيحي ادناه ، يمكن ان نرى وبوضوح تفوق قيم خواص
سمة قزحية العين (الممثلة بالمخطط بالسلسلة رقم 9) على بقية خواص السمات الاخرى.



مخطط 1 : مخطط يوضح امتدادات قيم كل سلسلة رقمية تمثل خواص كل سمة حيوية في الجدول.

(Fernald 2006, Augustine 2011) وتلك العلامات موجودة منذ لحظة ولادة المرء وتظل حتى لحظة مماته ، بعضهم يشبه العلامات القرنية هذه ببصمات جينية ، وإذا ما نظرنا إلى القرنية كموقع طوبوغرافي ، وجدناها مقسمة أساساً إلى 12 قطاعاً شعاعياً (Radial) (تماماً كالساعة .تتوزع في العين اليسرى باتجاه عقارب الساعة أما في اليمين ، فبعكس اتجاه عقارب الساعة .



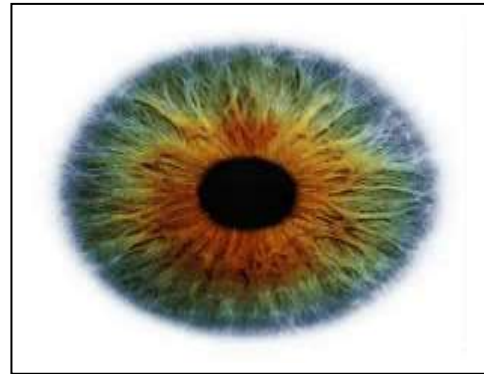
صورة-2: صورة توضيحية لقرنية العين

كما تعتبر قرنية العين العضو الداخلي الوحيد في الجسم البشري الذي يمكن مشاهدته من خارج الجسم . و تتكون القرنية من عدة طبقات و هي : عدد من الألياف الكولاجينية ،

قرنية العين Eye iris

الوصف التشريحي Eye iris description

يعود علم دراسة قرنية العين (Iridology) إلى ثلاثة آلاف عام ، وهو عبارة عن علم يقضي بأن نقرأ من القرنية (قسم الغشاء الوعائي من عدسة العين والذي يمنح هذه الأخيرة لونها الخاص) ، علامات أو مؤشرات



صورة-1: مقطع تشريحي لقرنية العين

تعتبر قرنية العين عضو من أعضاء العين الداخلية محمية بواسطة الجفون و القرنية بالإضافة إلى ماء العين (الخلط المائي) . و هي جزء من الطبقة المتوسطة للعين و تقع بين البؤبؤ و بياض العين (الصلبة) أمام العدسة

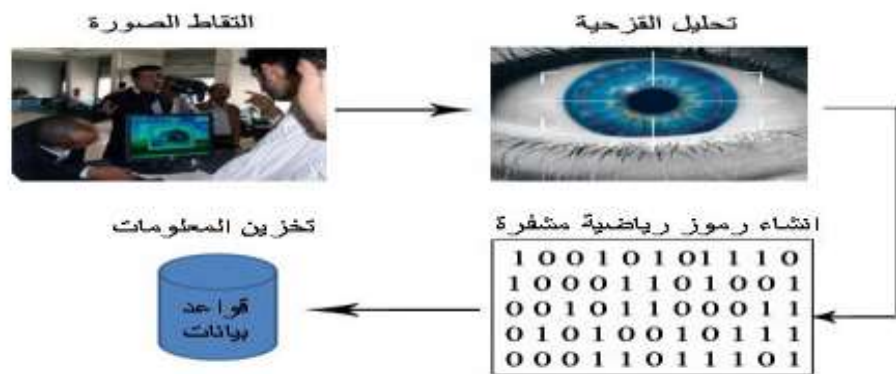
مراحل استحصال المعلومات الرقمية للقزحية و تخزينها : Stages for getting digital information

أ (مرحلة التقاط الصورة : تتم باستخدام الأجهزة التقليدية لدى أطباء العيون و لكن بعدسات ذات حجم مصغر حيث تتكون هذه الأجهزة من كاميرات تستخدم في تصوير بصمة قزحية العين التي تحتوي على أكثر من ٢٠٠ خاصية تدعى بدرجات الحرية تختلف من شخص إلى آخر كما أنها تختلف في الشخص نفسه ، و تقوم الكاميرات بالتقاط الصور لعين الشخص وذلك بتوجيه أشعة تحت الحمراء لالتقاط صور لها نسبة وضوح و دقة عالية (ب) مرحلة استخلاص و تحليل عناصر القزحية : و تتم بإزالة المناطق غير المهمة منها كما تقوم الماسحات بالقراءة من حدود القزحية اتجاهاً إلى أطراف البؤبؤ و تقوم أيضاً بتحديد الأشكال المميزة في القزحية. ج (تخزين الصور و جميع المعلومات في قواعد البيانات و إنشاء رموز رياضية مشفرة لها حتى يتم فيما بعد مقارنة المعلومات المخزنة بالصور المحصل عليها عن طريق عملية المسح.

مجموعة من الشقوق و الثقوب ، صبغات ملونة و التي تمد العين بجزئها الملون.

استخدام قزحية العين في تعريف الهوية Using eye iris in the identification

تعتبر قزحية العين من أكثر المقاييس الحيوية دقة لدى الإنسان . كما أنها تفوقت في دقتها على بصمة الإصبع التي تصل نسبة القبول الخاطئة فيها ١:١٠٠٠٠٠ مقارنة باستخدام قزحية العين التي لها ١:١٢٠٠٠٠٠ (Hugo ١٢٠٠٠٠٠, William 2010, 2010) بالإضافة إلى أنه يصعب التلاعب بقزحية العين سواء كان هذا التلاعب عن طريق النظارات أو العدسات اللاصقة أو إجراء عمليات جراحية للعين . و تبقى عملية تحديد الهوية عن طريق بصمة القزحية عملية ممكنة و سهلة سواء كان الشخص مبصراً أو فاقداً لحاسة البصر . و لذلك تم اعتماد هذه الوسيلة في كثير من الأنظمة التي تستدعي الكشف عن هوية الشخص كالأنظمة الأمنية في المطارات و البنوك في أجهزة الصرف الآلي وذلك لكفاءة القزحية العالية. كما تعتبر قزحية العين من أفضل السمات الحيوية نسبة إلى خواص السمات الحيوية التي تم ذكرها



مخطط - 2 : مراحل استحصال المعلومات الرقمية وتخزينها.

دوال الاتجاه الواحد الرياضية One Way mathematical functions

أن ابرز استخدام لدوال الاتجاه الواحد الرياضية، هو في أنظمة المفاتيح المعلن في علم التشفير [، ويتلخص مفهومها بأن من السهولة حسابها باتجاه معين ومن الصعوبة حسابها بالاتجاه المعاكس، فيمكن على ضوء ذلك حساب $f(x)$ عند توفر قيمة x وبسهولة، إلا أن حساب x عند توفر $f(x)$ صعب جداً وقد يتطلب وقت طويل قد يصل إلى سنين. وهناك أنواع من الدوال ذات الاتجاه الواحد منها: دالة باب المصيدة ذات الاتجاه الواحد trapdoor one way function وهي نوع خاص من دوال الاتجاه الواحد، يكون فيها حساب $f(x)$ عند توفر x سهلاً بينما يكون من الصعوبة حساب x بوجود $f(x)$ فقط، إلا بوجود y (كمعلومات سرية عن x) فعند ذاك يمكن بسهولة حساب x ، وهناك أيضاً دالة الاتجاه الواحد المشوشة One way hash function ولها تسميات عدة منها:

compression function, contraction function, message digest, fingerprint, cryptographic checksum, message integrity check (MIC), and manipulation detection code (MDC) [4]

وتكمن وظيفتها بتحويل المعلومات الرقمية إلى قيمة عددية أو سلسلة رقمية ضبابية، لا يمكن الرجوع منها إلى المعلومات الرقمية الأصلية. الآلية المسخرة لمحاكاة دالة الاتجاه الواحد، لم تعتمد في هكذا وظيفة سابقاً وقد نفذت بشكل تؤدي عمل دالة compression function الموصفة أعلاه.

إيجابيات وسلبيات استخدام القزحية لتعريف الهوية: Advantages and disadvantages for using eye iris in the identification

الإيجابيات Advantages :

- (1) بصمة قزحية العين ثابتة لا تتغير على مدى الحياة و لذلك لا تحتاج أنظمة المسح لقزحية العين إلى تجديد بياناتها المخزنة في قواعد البيانات الخاصة بها.
- (2) تمتاز عملية المسح للقزحية بالدقة والكفاءة و الفعالية العالية حيث أنها استطاعت التفوق بمراحل عديدة على دقة بصمة الإصبع أو شبكية العين أو راحة اليد كما أنها تمتاز أيضاً بسهولة الاستخدام.
- (3) لا يحتاج الشخص إلى تقريب عينه من العدسة حيث يكفي بالوقوف على بعد ٣٠ سم من العدسة.
- (4) لا تؤثر العدسات اللاصقة أو النظارات أو العمليات الجراحية للعين في بصمة القزحية مقارنة بالسّمات الأخرى التي يمكن تغييرها كتغيير ملامح الوجه أو ارتداء الأغشية البلاستيكية على بصمات الإصبع.

السلبيات Disadvantages :

- (1) عدم إمكانية إدخال أنظمة قراءة قزحية العين بسهولة في الأدوات الشخصية كالهواتف المحمول أو السيارة.
- (2) عدم القدرة على الاستفادة منها في الأدلة الجنائية مباشرة إذ أن قزحية العين لا تترك أثراً مثل بصمة الإصبع
- (3) التكلفة المادية المرتفعة لأنظمة قراءة معلومات قزحية العين.

نظام الموثوقية المقترح لإنتاج سلسلة الأرقام (المفاتيح) لتعريف الشخصية The suggested identification system

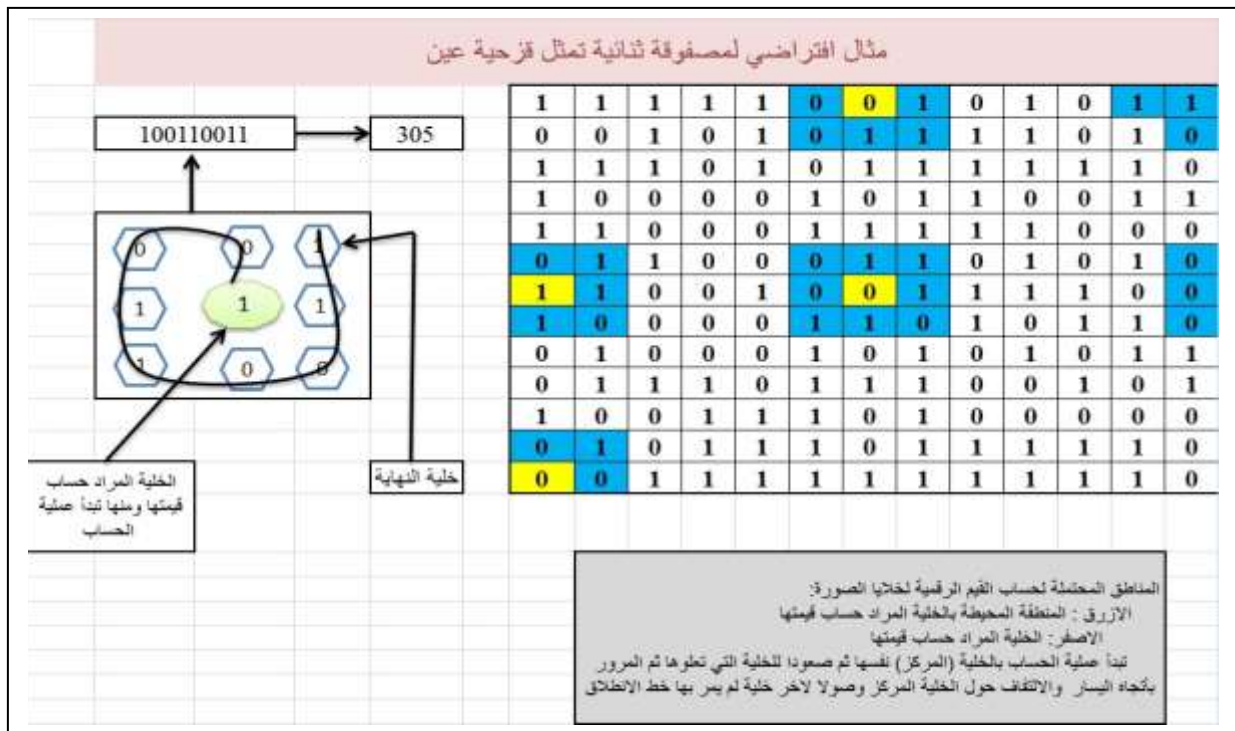
(أ) مرحلة استحصال المعلومات الرقمية
من قزحية العين Getting the digital
information:

بعد أخذ الصورة الرقمية لقزحية العين ، يعبر
عن مميزات القزحية من خلالها بواسطة قيم
ثنائية (0,1) مخزونة في مصفوفة مربعة
بابعاد محددة وموصفة ، وذلك باستخلاص
خواص تعرجات وشكل ونتوءات الخطوط

الموصفة للقزحية، فتكون كبصمة جينية
رقمية تعرف كل شخص.

(ب) مرحلة الترميز الرقمي لمعلومات
قزحية العين The coding Stage :
تحول المصفوفة الثنائية القيم ، الى مصفوفة
رقمية صحيحة ، حيث تحسب كل قيمة من قيم
المصفوفة الجديدة بواسطة جمع الاوزان للخلية
المناظرة له في المصفوفة الثنائية مع الخلايا
المجاورة لها في محيطها الدائري (كما يوضح
المخطط-4 ادناه) ، وبذلك سوف يكون مدى
القيم المخزونة في المصفوفة الرقمية يتراوح
بين (0 – 511) وذلك لان عدد الخلايا الداخلة
بجمع الاوزان هو 9 cells .

مخطط-3: عملية حساب قيم المصفوفة الرقمية من المصفوفة الثنائية



ستتولد المصفوفة الرقمية التالية كنتاج لمرحلة الترميز الرقمي لمعلومات قزحية العين:

جدول-2: مثال على قيم المصفوفة الرقمية .

382	58	13	66	155	259	48	451	399	453	25	216	365
49	510	168	400	52	348	6	384	330	183	269	322	87
239	424	85	86	111	300	276	76	201	227	136	368	287
317	204	108	154	237	474	214	360	72	448	466	249	277
350	327	296	395	170	446	386	122	433	30	216	215	164
92	188	114	258	125	491	508	436	206	494	502	380	0
417	446	419	468	495	213	167	96	176	363	376	483	94
411	393	106	157	88	428	82	497	471	196	83	236	380
196	385	388	217	35	361	54	79	101	308	510	409	508
378	463	315	178	236	62	93	303	504	165	494	469	475
87	103	496	69	489	221	203	471	486	336	313	428	360
195	336	148	475	81	252	338	280	91	455	26	264	246
467	338	449	267	83	128	136	257	416	299	17	496	315

(ج) مرحلة اختيار قيم رقمية عشوائية وجمعها The selection of random integer values :

تحدد في هذه المرحلة قيم ابتدائية للمعادلة من الدرجة الثانية (باعتبار ان المتغير يمثل قيمة ابتدائية لأحد الابعاد بالمصفوفة) الاتية:

$$F(i)=ai^2+bi+c \mod \text{direction size}$$

$$F(j)=aj^2+bj+c \mod \text{direction size}$$

وكذلك تحديد عدد مرات تنفيذ المعادلة n ، والذي يحدد المقدار الرقمي النهائي الذي سيمثل معلومات قزحية العين، وسيكون الناتج النهائي ممثل بالمعلمة N ، بحيث :

$$N \leftarrow 0$$

$$\text{For } i=0 \rightarrow n$$

$$F(i)=ai^2+bi+c \mod \text{direction size}$$

$$F(j)=aj^2+bj+c \mod \text{direction size}$$

$$N \leftarrow N + \text{loc}(F(i), F(j))$$

End for

مثال : $a=3, b=4, c=7, i=6, j=5, \text{direction siz}=13, n=3$

$N=0$

$$F(i=1)=3(6)^2+4(6)+7 \mod 13 = 9$$

$$F(j=1)=3(5)^2+4(5)+7 \mod 13 = 11$$

$$N=0+\text{loc}(9,11)=0+196=196$$

$$F(i=2)=3(9)^2+4(9)+7 \mod 13 = 0$$

$$F(j=2)=3(11)^2+4(11)+7 \mod 13 = 11$$

$$N=196+\text{loc}(0,11)=196+216=412$$

$$F(i=3)=3(0)^2+4(0)+7 \mod 13 = 1$$

$$F(j=3)=3(11)^2+4(11)+7 \mod 13 = 11$$

$$N=412+\text{loc}(1,11)=412+322= 734 \rightarrow \text{the final value of } N.$$

(2) Term2: يمثل مجموع مراتب

اول قيمة للعدد المدخل N .

(3) Term3 : يمثل تكرار آلية

المحاكاة وصولا الى شرط التوقف

(وصول قيمة Term1 الى عدد

معين ، كأن يكون 99).

لذلك فإن قيمة المعلمة Term3 يجب

ان تتساوى مع عدد قيم المعلمة

Term1.

وللمثال الموضح في الفقرة (ت) فإن :

(د) ادخال القيمة الرقمية الناتجة الى تقنية

محاكاة دالة الاتجاه الواحد الضبابية The

simulation of one way hash

function

تعتمد آلية المحاكاة على عملية

الانقاص المتكرر لمجموع مراتب

القيمة N من القيمة N نفسها ، مع

الاحتفاظ ببعض القيم الوسطية التي

بدون معرفتها لا يمكن اعادة احتساب

قيمة N الاصلية ، وهذه القيم هي :

(1) Term1 : يمثل عدد مرات

نقصان مجموع مراتب العدد من

قيمة العدد نفسه.

When $N=734 \rightarrow \text{Term1} = 65, \text{Term2} = 14, \text{Term3} = 1$

(هـ) تصنيف الناتج الى سلسلة رقمية علنية

وسلسلة رقمية سرية classification

into public and secret sequence

numbers

من سلسلة الارقام الناتجة ، يمكن ان نصنف

محتوياتها الى ارقام يجب ان تكون سرية (لان

معرفتها تؤدي الى معرفة الرقم الممثل

ان عملية اعادة تجميع الرقم الاصلية ،

تستند الى نتيجة رياضية مفادها : (أن

الرقم يعاد تجميعه من اضافة العدد 9

ومضاعفاته عدة مرات وبقدر قيمة

المعلمة Term1 ، مع قمة المعلمة

(Term2

لمعلومات القزحية وبسهولة (مثل :قيم Term1 و قيمة Term2 اما قيمة Term3 فمن غير الضروري الحفاظ على سريتها . ويمكن ان نرى النظام المقترح معبر عنه بالمخطط العام ادناه ، والذي يصور بشكل عام المهام الاساسية لمراحله المختلفة.



مخطط - 4 : مخطط يوضح مراحل النظام المقترح.

مناقشة

Jeffrey Hoffstein & Jill Pipher & Joseph H. Silverman, 2008, "An introduction to mathematical cryptography", springer, USA.

Kozmik, Zbynek; Ruzickova, Jana; Jonasova, Kristyna; Matsumoto, Yoshifumi; Vopalensky, Pavel; Kozmikova, Iryna; Strnad, Hynek; Kawamura, Shoji et al. (2008). ["Assembly of the cnidarian camera-type eye from vertebrate-like components"](#) (PDF). *Proceedings of the National Academy of Sciences* **105** (26): 8989–8993. [Bibcode 2008PNAS..105.8989K](#). [doi:10.1073/pnas.0800388105](#). [PMC 2449352](#). [PMID 18577593](#).

Lee Ann Remington, 2009, "Clinical Anatomy Of The Visual System", 2nd edition, chine .

Mark Ciampa ,2005,"Security + Guide to NETWORK SECURITY Fundamentals",
Second Edition, Thomson Course Technology, Netherlands.

Miltiades Leonidou ,2002,"Iris Recognition: Closer than we think?",UK, [online] "http://www.sans.org/reading_room/whitepapers/authentication/iris-recognition-closer-think_143" .

ان اسلوب عمل آلية التعريف بوجوب تطابق الارقام النهائية المنتجة من هذه التقنية مع الصفات البايولوجية المستخلصة من قزحية العين تحقق الاتي: (1) تعتبر وسيلة تعريفية فريدة للشخصية، ويمكن اعتمادها للحفاظ على الخصوصية، (2) وبواسطة جمع اسلوب اعتماد الارقام الممثلة لمعلومات القزحية مع القيم الابتدائية للمراحل تعطي آلية قوية لإنتاج معلومات سرية رقمية يمكن استخدامها كمفاتيح تشفيرية، او رموز دخول لنظام يعتمد عليها ويمكنه التحقق منها حتى لو تم نسيانها، (3) وبذلك فالتقنية تراعي جانب فقدان سلسلة المفاتيح، وكذلك يمكن لهذه التقنية ان تعالج مشكلة تخمين الارقام النهائية واكتشافها. (4) تعتبر مصدرا ثابتا لسلاسل ارقام عشوائية متغيرة.

المصادر

Augustine GJ, Fitzpatrick D, et al., 2011, "Neuroscience". 2nd edition. Purves D, editors Sunderland (MA)

Fernald, Russell D. (September 2006). "Casting a Genetic Light on the Evolution of Eyes". *Science* **313** (5795): 1914–1918. [Bibcode 2006Sci...313.1914F](#).

Hugo Proença ,2010,"Iris Recognition" , University of Beira Interior Department of Computer Science ,[online] <http://www.di.ubi.pt/~hugomcp>

Sean Callery,2008, “codes and ciphers”,HarrperCollins,ISBN:0061374075.

Serge Vaudenay,2006,"A classical introduction to cryptography:applications for communications security",USA.

William Stallings,2010,"cryptography and network security :principles and practice"UK.

Muhammad Khurram Khan ,2009,"Biometrics: Changing the Paradigm of Personal Identification", 18thNovember, USA.

Salil P.Vadhan,2009, “Theory of cryptography”,ISBN:3540709355,s pringer.

A mathematical technique to protect the privacy and authentication via iris information

Basim Sahar Yaseen ,M.Sc.in computer science

Department of computer science ,Shatt alaraab university collage

Abstract :

This research suggests a mathematical technique of identifying an individual's identity by using data extracted from the eye iris ,it consists of two parts: First ,building a database for the digital data extracted from eye iris of the concerned individuals .Second ,a set of mathematical steps for producing secret digital data from the data extracted from the photo ,the stages of the system begins with getting the genetic data of the human eye which is represented by the iris photo of the individual (it expresses its values by 0,1), and it has a stable volume that is already described. The founded matrix generates another digital matrix with the same volumes of the dimensions of the original matrix, but every value is the sum of the weights of values of a group of cells(any cell and surroundings) accounted from the first matrix ,then by using the sum of the elected locations content transformed into one integer. This represents the extracted data from the eye iris data, the new digital board enters an algorithm of isolation and reeducates, in order to transform into the last formula which will be deemed .

The goal of this research is to depend a stable base(eye iris) for producing random and secret digital data to be used in various applications of the cryptography science as keys for encryption the secret or the reliability in the public key systems as the signature ,digital investigation and establishing a new style in transforming and isolation the integers to simple chains.

Keywords :eye iris, cryptography, privacy and authentication , random numbers.