

تحسين الوثوقية باعتماد المقياس الحيوي والشبكات العصبية

نجلاء بديع ابراهيم ميلاد جادر سعيد نادية معن محمد
جامعة الموصل / كلية علوم الحاسوب والرياضيات

الخلاصة

نظرا للتطور الكبير في مجال تكنولوجيا المعلومات وتزايد وسائل الاتصال والشبكات وانتشار جرائم السرقات الالكترونية وانتحال الشخصية ، أصبح أمن المعلومات والتحقق من هوية المستخدم من اكبر اهتمامات المؤسسات والافراد. ومن هنا ظهرت عدة انواع للتحقق من وثوقية الأشخاص ، منها ما اعتمد على الوسائل التقليدية مثل كلمات السر والبطاقات الذكية أو الحديث الذي اعتمد على الصفات الحيوية وهو ما يخص علم الاحصاء الحيوي الذي يعتمد على خصائص طبيعية او سلوكية فريدة لدى الاشخاص. اما الشبكات العصبية الاصطناعية فقد استخدمت من قبل عدد كبير من الباحثين لتحقيق اهداف أمن المعلومات وذلك لما تمتاز به من القابلية على التعلم ونمذجة العلاقات المعقدة بين المدخلات والاخراجات. اقترح هذا البحث طريقة لتحسين اسلوب الوثوقية للمستخدم في التطبيقات عالية الامنية في الشبكات. استخدمت الشبكة العصبية الاصطناعية (شبكة الانتشار العكسي) لتوفر خصوصية للمستخدم والسمة الحيوية (بصمة قزحية العين) كونها من أفضل السمات الحيوية في التحقق من هوية المستخدم لما تمتاز به من الثبات والدقة العالية بالإضافة الى سهولة الاستخدام.

كلمات مفتاحية: الوثوقية ، المقياس الحيوي ، الشبكات العصبية

المقدمة

ويجب ان يحفظ هذا الجدول بصورة امينة لانه يكون عرضة للقراءة والتغيير من قبل المتطفل [1]. وفي طرق التحقق الاخرى فان النظام يستخدم جدول التحقق (Verification Table) حيث تحفظ كلمات السر بصورة مشفرة في هذا الجدول، ولايوجد ضرورة للاحتفاظ به بصورة سرية . وبالرغم من استخدام اسلوب التشفير الا ان المتطفل يستطيع ان يضيف نماذج زائفة ويعوض كلمات سر محل الاصلية . وفي نظم اخرى تم ادخال الذكاء الاصطناعي في حقل امن المعلومات ، حيث استخدمت الشبكات العصبية الاصطناعية لخصائصها في تخزين الاسم التعريفي المشفر وكلمة السر المشفرة باستخدام دالة الترميز (Hash Function) ليقوم النظام بخزن الازان (Weights) بدلا من جدول التحقق [2]. وبالرغم من الفوائد التي قدمتها هذه الطرق مثل عدم قدرة المتطفل من اضافة رقم تعريف وكلمة سر مزيفتين بالإضافة الى بساطة العمليات الحسابية لظهور النتائج المطلوبة الا انها بقيت تعاني من بعض نقاط الضعف مثل امكانية تعرضها لهجوم القاموس (Dictionary Attack) الذي يحاول فيه المتطفل بعد حصوله على الازان بتجربة كل كلمات السر الممكنة للتحقق.

بظهور شبكات الحاسوب زادت المخاطر الامنية التي تتعرض لها المعلومات ، كما ان هنالك خصوصية للامن في عالم الشبكات جعلت من الضروري ان ننظر الى امن الشبكات بشكل اكثر جدية وصرامة. فالشركات الان في حوارها مع فروعها لاتضمن عدم وجود (طرف ثالث) يتنصت على هذا الحوار، فالمعلومات المتبادلة تمر عبر عشرات الدول وملايين الحواسيب والكابلات، لذا فهناك دائما خشيّة من وجود الطرف الثالث. وقد يهون الامر اذا اقتصر تدخل الطرف الثالث على التنصت ، بل انه يقوم بتغيير الرسائل المتبادلة ، لذلك تظهر بشدة اهمية خدمة الوثوقية (Authentication) اوالتحقق من هوية المستخدم لامن التعامل عبر الشبكة. بالرغم من ان طرق التحقق التي تعتمد كلمة السر تعتبر من الطرق الشائعة الا انها لازالت تعاني من بعض نقاط الضعف، ففي الطرق البسيطة Simple_Password_based_Authentication فان النظام يحتفظ لكل مستخدم بالرمز التعريفي (ID) وكلمة السر (Password) الخاصة به في جدول خاص.

العين او بصمة الاصبع او سلسلة DNA او التوقيع. وفي كثير من التطبيقات قد يستخدم مزيج من الطرق السابقة يطلق عليها (الوثوقية باستخدام عاملين) كاستخدام رقم التعريف الشخصي مع البطاقة الذكية او بصمة الاصبع مع بصمة قزحية العين[6].

تعرف المقاييس الحيوية على انها مقاييس للصفات او الميزات الفريدة للانسان والمستخدم عادة في عمليات التمييز الالكترونية او اثبات الشخصية. فالكائن البشري فريد وكذلك فان صفاته الفيزيائية والسلوكية فريدة ايضاً، ولهذا يمكن اعتبار القيم الناتجة من عملية الاستخلاص الناجح لمعلومات هذه المقاييس المستحصلة فريدة ولا يمكن تكرارها عند اي شخص اخر[7].

تم اعتماد قزحية العين كاحد المقاييس الحيوية، حيث تعد الانظمة المعتمدة على قزحية العين 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 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.

وبالمقارنة مع خواص المقاييس الحيوية الاخرى مثل الوجه وبصمة الاصبع فان قزحية العين تكون ثابتة وموثوق بها [8].

يمكن تعريف الشبكات العصبية الاصطناعية (Artificial Neural Network) على أنه العلم الذي يهتم بدراسة أنظمة الضبط والاتصالات في الكائنات الحية بغية صنع نموذج شبيه بالعقل البشري ، كذلك يمكن تعريفها على أنها تراكيب حسابية تم صياغتها بالإعتماد على الخلايا الباثولوجية ، وتعرف أيضاً على أنها نظام معالجة للمعلومات له مميزات أداء معينة بإسلوب يحاكي الشبكات العصبية الحية.

بشكل عام تتميز خلايا الشبكة العصبية بسرعتها في معالجة المعلومات وقدرتها على التعلم والتعامل مع نماذج بيانية مختلفة ، مما جعلها مناسبة لكثير من التطبيقات [9].

في هذا البحث تم استخدام خوارزمية الانتشار العكسي (Back propagation Algorithm) لتعلم الشبكة العصبية، حيث تم اعطاء قيم ابتدائية عشوائية للاوزان ومن ثم تعديلها خلال مرحلة التدريب باستخدام Hebbian Rule.

اما دالة الترميز فهي دالة رياضية ادخالها عبارة عن سلسلة من البيانات ذات طول متغير تعرف بالصورة الاصلية (Pre-Image) والتي تمثل الرسالة او البيانات المراد ايجاد قيمة دالة الترميز لها حيث تقوم دالة الترميز بتحويل الطول المتغير (العشوائي) للبيانات المدخلة الى سلسلة من البيانات ذات طول ثابت (Fixed Length) والتي عادة يكون طولها اصغر من طول

وللتغلب على نقاط الضعف الائمة الذكر وضمان خصوصية المستخدم تم في هذا البحث تحسين خدمة الوثوقية باعتماد التوثيق الحيوي (بصمة قزحية العين) مع الشبكات العصبية الاصطناعية.

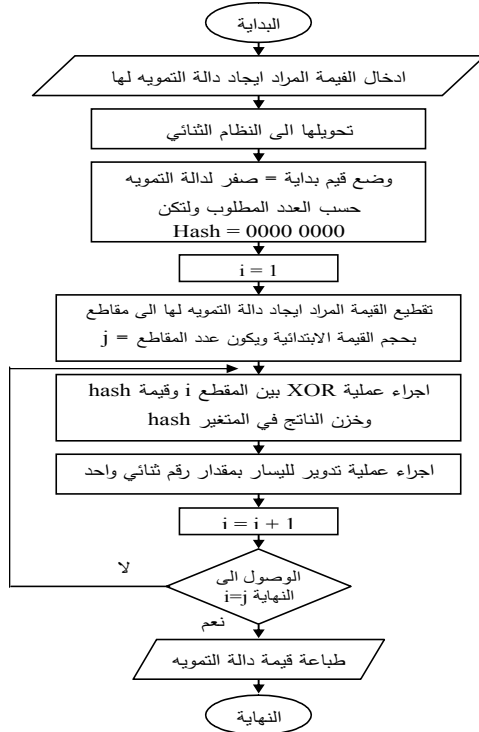
نقد عدد كبير من البحوث في حقل بناء اسلوب الوثوقية باعتماد الصفات الحيوية المستخلصة من المستخدم ، وبحث اخرى طورت اسلوب الوثوقية باعتماد كلمة السر. اما اسلوب الوثوقية باعتماد الصفات الحيوية من جهة والشبكات العصبية الاصطناعية مع كلمة السر من جهة اخرى فقد كان قليل مقارنة بسابقتها. في [2] عرف الباحثون كيفية استخدام الشبكات العصبية الاصطناعية في مجال الوثوقية (التحقق من الشخصية)، حيث تم استخدام شبكة ((Radial Base Function (RBF) لانتاج كلمة السر المشفرة باعتماد الرمز التعريفي للمستخدم. اما في [3] فقد قام الباحثان باستخدام الشبكات العصبية الاصطناعية وتدريبها لتوليد كلمة السر (المعتمدة على التحقق من شخصية المستخدم) في نظام البيت الذكي بدلا من استخدام جدول التحقق، وتم استخدام مقياس نسبة الخطا ((Mean Square Error (MSE) وزمن تدريب الشبكة وعدد مراحل تدريب الشبكة لقياس كفاءة الشبكة. وفي [4] اقترح الباحث نظام وثوقية للمقياس الحيوي بالاعتماد على تمييز الوجه باستخدام تحويل الجيب تمام المنقطع ((2D_ Discret Cosin (DCT) Transform والشبكات العصبية الاصطناعية ، وقد اظهرت نتائج البحث التجريبية تحسين اداء تمييز الوجه وسرية النظام. وفي [5] قدم الباحثون طور تحقق سري باعتماد الشبكة العصبية الاصطناعية مع اتفاقية المفتاح الموثوق باعتماد المقياس الحيوي (بصمة الاصبع).

الادوات المستخدمة

ان كلمة (Authentication) تعني عند الاغريق حقيقي (real) او اصلي (genuine). اما في امن المعلومات فان (Authentication) تعني بان نضمن ان مستخدم الشبكة هو من يدعي او هو المستخدم الاصلي . هذا مهم لأننا لا نريد ان يصل ذلك الشخص الى الشبكة اذا كان لا يفترض السماح له بذلك. توجد عدة طرائق تمكن الاشخاص من تحديد هويتهم وهي استخدام شيء يملكه الشخص (Something the user has) مثل البطاقة الذكية (Smart Card)، او استخدام شيء يعرفه الشخص (Something the user knows) مثل كلمة السر (Password) او رقم التعريف الشخصي (PIN) Personal Identical Number، واستخدام شيء حي يميزه (Something the user is or does) مثل بصمة قزحية

7. تطبيق خوارزمية دالة الترميز على مخرجات الدالة المنطقية لانتاج Hashbio.
8. اجراء عملية XOR بين Hashpassword و Hashbio لانتاج Finalxor.
9. ادخال Finalxor و ID للمستخدم الى الشبكة العصبية.
10. مقارنة نتائج الشبكة العصبية مع الادخال، هل ضمن المسموح.
- أ- نعم: الشخص مخول بالدخول للشبكة.
- ب- لا: الشخص غيرمخول بالدخول للشبكة.
11. اعادة الخطوات السابقة على كل الاشخاص الراغبين باستخدام الشبكة.
12. النهاية.

الإخراجات: قبول او رفض دخول الشخص الى الشبكة. والشكل (3) يوضح المخطط الصندوقي للخوارزمية المقترحة في طور التحقق.



شكل(1):خوارزمية دالة الترميز Hash Function المستخدمة

البيانات المدخلة [6]. في هذا البحث تم الاستفادة من خصائص هذه الدوال لتحقيق مستوى عالي من الوثوقية حيث تم اعتماد دالة ترميز مبسطة (simple hash function) كحل اولي للخوارزمية المقترحة.

الخوارزمية المقترحة في طور التسجيل:

الإدخالات: (نماذج التدريب). الرموز التعريفية للمستخدمين، بصمات قزحية العين، كلمات السر.

1. البداية.
2. قراءة ID للمستخدم.
3. قراءة كلمة السر للمستخدم وتحويله الى النظام الثنائي.
4. تطبيق خوارزمية دالة الترميز على ناتج الخطوة السابقة لانتاج Hashpassword. انظر الشكل(1).
5. استخلاص الخواص من قزحية العين المدخلة باستخدام دالة تحويل الموجة.
6. استخدام الدالة المنطقية NOT لعكس مخرجات الخطوة السابقة.
7. تطبيق خوارزمية دالة الترميز على مخرجات الدالة المنطقية لانتاج Hashbio.
8. اجراء عملية XOR بين Hashpassword و Hashbio لانتاج Finalxor.
9. ادخال Finalxor و ID للمستخدم الى الشبكة العصبية.
10. تدريب الشبكة العصبية لحين الحصول على الاخراج الذي يطابق Finalxor.
11. اخذ قيم الازان Wiegths للشبكة عند الوصول للاخراج المطلوب وخرنه بقاعدة بيانات خاصة.
12. النهاية.

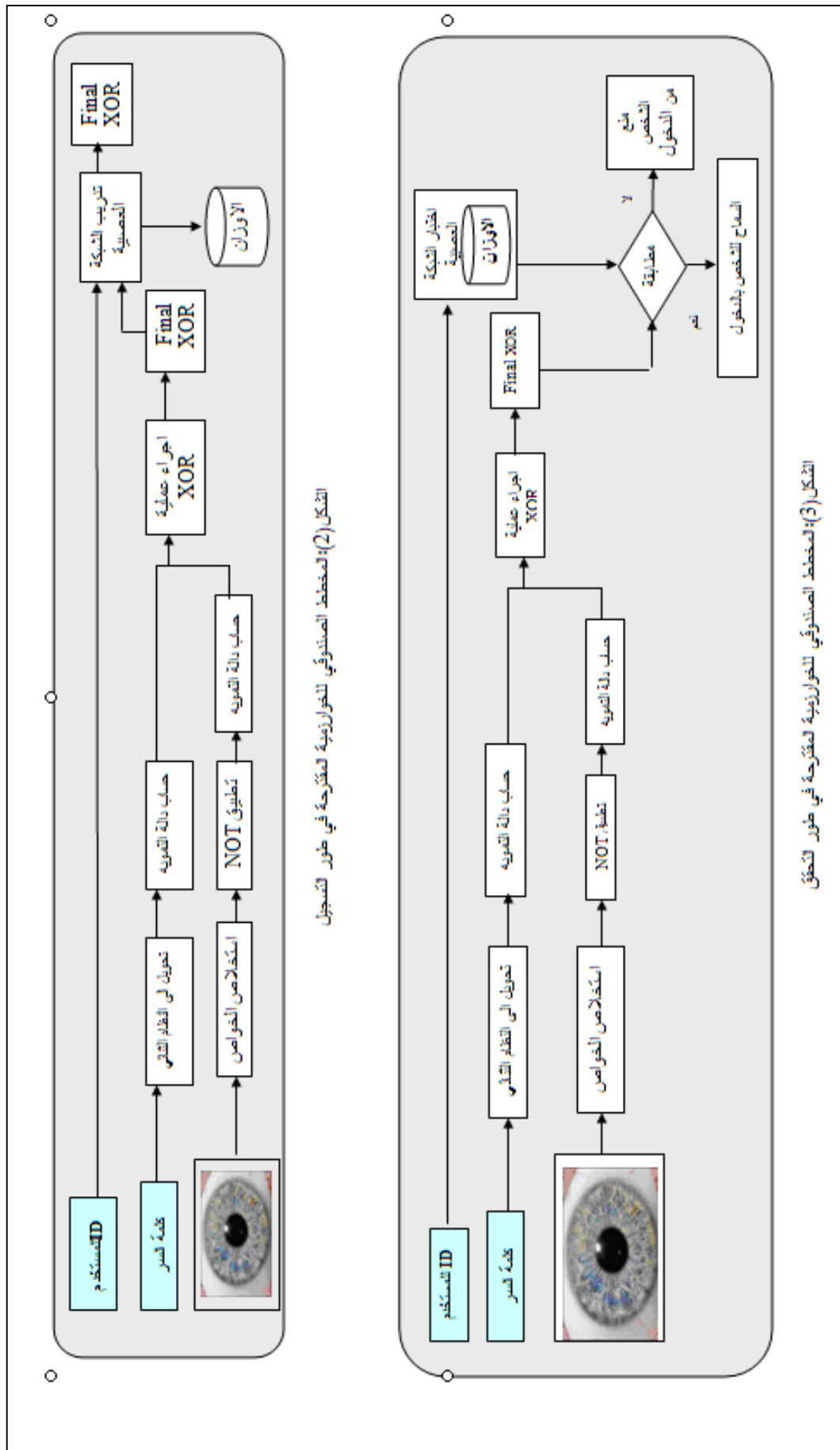
الإخراجات: قاعدة بيانات بقم الازان.

والشكل (2) يوضح المخطط الصندوقي للخوارزمية المقترحة في طور التسجيل

الخوارزمية المقترحة في طور التحقق

الإدخالات: قاعدة بيانات الازان، ID للمستخدم، كلمة السر، قزحية العين.

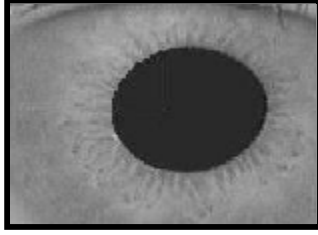
1. البداية.
2. قراءة قيمة ID للمستخدم.
3. قراءة كلمة السر للمستخدم وتحويله الى النظام الثنائي.
4. تطبيق خوارزمية دالة الترميز على ناتج الخطوة السابقة لانتاج Hashpassword.
5. استخلاص الخواص من قزحية العين المدخلة باستخدام دالة تحويل الموجة.
6. استخدام الدالة المنطقية NOT لعكس مخرجات الخطوة السابقة.



الشكل (2): لمخطط الصندوقي للخوارزمية المقترحة في طور التدريب

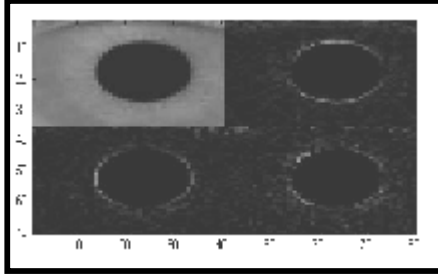
الشكل (3): لمخطط الصندوقي للخوارزمية المقترحة في طور التحقق

لهذا تجمع صورة القرحة من هذه الاجزاء لتكون الصورة الموضحة في الشكل (5).



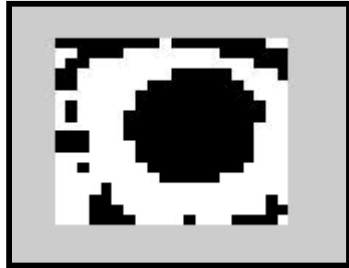
الشكل(5):القرحة بعد اقتصاصها من صورة العين

بعد اقتصاص صورة القرحة من صورة العين تبدأ مرحلة استخلاص الخواص باستخدام دالة تحويل المويجه من نوع (DB1) ولثلاث مستويات لتنتج صورة مصغرة للقرحة ، الشكل (6) يوضح الصورة الناتجة بعد تحويل المويجه.



الشكل(6):صورة القرحة بعد استخلاص خواصها

تحويل الصورة الناتجة الى رمز ثنائي باستخدام طريقة العتبة (thresholding)، ليتسنى تمثيلها بالرقمين (0 او 1) و الشكل (7) يوضح الصورة الثنائية.



الشكل(7):الصورة الثنائية الناتجة من قرحة العين
يتم الان تحويل صورة القرحة الى مصفوفة ثنائية لتسهيل التعامل معها والشكل (8) يوضح جزء من هذه المصفوفة لكبير حجمها:

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	0
0	0	0	0	0	0
0	0	0	0	0	0
0	0	0	0	0	0
0	0	0	0	0	0
0	0	0	0	0	0

الشكل (8):المصفوفة الثنائية لقرحة العين

الجانب العملي

من خلال تتبع خطوات الطورين (التسجيل والتحقق) فان الخطوات العملية تتلخص بما يلي:

طور التسجيل:

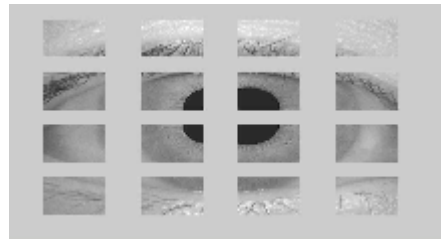
- في بادئ الامر يتم ادخال ID وكلمة السر وفزحية العين للمستخدم ، الجدول (1) يمثل الاشخاص المخولين بالدخول الى الشبكة:

ت	ID المستخدم	كلمة السر	فزحية العين
1	Ahmad	AB2008	
2	aha	allah	
3	saad	Allah-2009	
4	Fahad	Iraqi2008	
5	han-2008	Mbroka	
6	Raseel ha	RH2008	
7	ZENArma	heLo	
8	Sara A S	hadha	
9	Omar ah	O_M_A_R	
10	XYZ-aha	zaid	

جدول (1) الاشخاص المخولين

- يتم اخذ قرحة العين واستخلاص الخواص منها باستخدام دالة تحويل المويجه واتباع الخطوات التالية:

* بما ان الصورة تضم صورة العين باكملها بضمنها جفون ورموش العين وليست القرحة فقط فيجب اولا قطع صورة القرحة ليتم التركيز عليها في عملية استخلاص الخواص، ولذا تقطع الصورة باستخدام التقطيع المنتظم (systematicclassification) الى 16 جزء (4*4) كما في الشكل(4).



الشكل(4):صورة العين بعد تقطيعها الى 16 جزء

* من الشكل(5) نلاحظ استقرار القرحة في وسط الصورة أي الاجزاء الاربعة الداخلية للصورة بعد التقطيع

Finalxor	ID للمستخدم
11110100	Ahmad
10001111	Suha
11011111	Saad
11111001	Fahad
11011111	Ban-2008
01001001	Raseel ha
10111101	ZENAZena
01100000	SaraA.S.
10010101	Omar ali
01001000	XYZ-abc

الجدول (3): جدول التدريب Training table

■ نتائج الخطوة السابقة يمثل قاعدة بيانات الازران للأشخاص المخولين بالدخول الى الشبكة، والذي يعتبر ادخال المرحلة الثانية الممثل بطور التحقق.

طور التحقق:

في هذا الطور يتم ادخال ID ، كلمة السر ، قزحية العين للشخص الراغب بالدخول الى الشبكة اضافة الى قاعدة بيانات الازران الناتج من طور التسجيل ، يتم تطبيق خطوات هذا الطور بالكيفية نفسها التي تم تطبيقها في طور التسجيل مع اختلاف في كيفية استخدام الشبكة العصبية فانه يتم المطابقة فقط اي الاختبار بدون تدريب الشبكة وعلى ضوء المطابقة يصدر قرار اما بالموافقة على دخول الشخص الى الشبكة او لا وحسب الخوارزمية الموضحة بالشكل (3).

المناقشة والاستنتاجات

اعتمدت نظم الوثوقية التقليدية على استخدام جدول كلمات السر او جداول التحقق، في هذا البحث استخدمت خوارزمية الشبكة العصبية ذات الانتشار العكسي مع السمة الحيوية لقزحية العين كطريقة مقترحة للوثوقية والتي يمكن ان تحل بكفاءة محل الطرق السابقة حيث انها تحقق:-

- 1- زيادة ألمان في أنظمة التوثيق الحيوي لاعتمادها على أكثر من وسيلة للتحقق.
- 2- ربطت الشبكة العصبية الاصطناعية كلا من الرمز التعريفي وكلمة السر وبصمة قزحية العين، لذلك فأن اضافة أي زوج مزيف (رمز تعريفي وكلمة سر) تعتبر عملية غير مجدية.
- 3- اعتماد بصمة قزحية العين يؤدي الى فشل هجوم القاموس عندما يستخدم من قبل المتطفل بالاضافة الى التقليل من خطر استخدام كلمات سر اعتيادية والتي يمكن نسيانها، سرقتها ، أو اعتراضها من قبل المتطفل. تطلبت الطريقة المقترحة عمليات حسابية بسيطة لاطهار النتائج مقارنة مع أنظمة الحماية الاخرى. بالاضافة الى وقت قصير لتدريب الشبكة والحصول على الازران.

■ تم استخدام الدالة المنطقية NOT لعكس مخرجات الخطوة السابقة، والشكل (10) يوضح المصفوفة الاخيرة:

1	1	1	1	1	1
1	1	1	1	1	1
1	0	1	1	1	1
1	0	1	1	1	1
1	1	1	1	1	1
1	1	1	1	1	1
0	1	1	1	1	1

الشكل(9):المصفوفة الثنائية بعد تطبيق NOT

■ يتم حساب دالة التمويه لقزحية العين بعد اجراء الخطوات السابقة ، باستخدام الاسلوب المبسط لدالة التمويه وحسب الخوارزمية الموضحة بالشكل (2) ويكون الناتج عبارة عن بايت من النظام الثنائي فقط 10110110

■ تحويل كلمة السر المدخلة الى النظام الثنائي وحساب دالة التمويه لها، وايضا يكون الناتج هو بايت واحد من النظام الثنائي 01001010

■ اجراء عملية XOR بين ناتج الخطوتين السابقتين لينتج لنا Finalxor، والجدول (2) يوضح القيم الناتجة للخطوات السابقة للأشخاص المخولين بالدخول الى الشبكة.

Finalxor	دالة تمويه قزحية العين	دالة تمويه كلمة السر	ID للمستخدم
11110100	10110110	01001010	Ahmad
10001111	01110111	11111000	Suha
11011111	00001011	11100100	Saad
11111001	00111110	11000111	Fahad
11011111	10110000	01101111	Ban-2008
01001001	11100011	10101010	Raseel ha
10111101	00110011	10001110	ZENAZena
01100000	11110001	10010001	SaraA.S.
10010101	10000011	00010110	Omar ali
01001000	00011111	01010111	XYZ-abc

الجدول (2):قيم دالة التمويه لكلمة السر وقزحية العين وقيم Finalxor

ادخال قيم ال Finalxor مع قيمة ID للمستخدم الى الشبكة لتنفيذ طور التدريب لحين الحصول على المخرجات المطلوبة (Finaltest) لاحظ الجدول (3)

- 3- J. A., D.B.L.B. and D.A.A. M. (2009). Application of Neural Network in User Authentication for Smart Home System. *in Proceeding of the World Academy of Sciences, Engineering and Technology* .pp 1293-1300
- 4- M. G. and M. F. (2010). A protection Scheme for Enhancing Biometric Template Security and Discriminability. *Università Politecnica delle Marche, Ancona, Italy.*
- 5- P. E. A. CH., B. EL.-H. and A. M. (2011). An Enhanced Authenticated Key Agreement Protocol with a Neural Network-based Model for Joining-Phase in Mobile Environments. *International Journal of Engineering and Industries*, Vol. 2: NO. 2, June.pp103-112
- 6- الناظر سائد. (2005). التعمية و امن الشبكات. شعاع للنشر والعلوم.
- 7- جاسم سجي، جادر ميلاد و اسامة ايلاف. (2010). التشفير الفوضوي باستخدام مفتاح المقياس الحيوي. مجلة الراقدين لعلوم الحاسوب والرياضيات. المجلد 7: العدد 3 .
- 8- Al- G. M. A.-R. H. (2006). Biometric Identification Based on Improved Iris Recognition Techniques. PhD.Thesis Submitted to the Council of the College of Computer and Mathematics Sciences, University Of Mousl.
- 9- زكي علاء ، عزود. عماد. (2000). الشبكات العصبية (البنية الهندسية، الخوارزميات ، التطبيقات). سورية- حلب.

التوصيات

- على الرغم من كون اسلوب التحقق من الشخصية باعتماد المقاييس الحيوية يعتبر أفضل بمراحل من أساليب الحماية التقليدية الا انه لا يمكن اعتباره اسلوبا مثاليا" لامن المعلومات لاننا لانعرف ما يمكن أن تقدمه لنا الأيام القادمة , خصوصا وان هذا الحقل يعتبر ارض خصبة للبحوث في الوقت الحاضر. ومقترحات مستقبلية يوصى بما يلي:
- 1- دراسة الثغرات والتهديدات الامنية وايجاد الحلول المناسبة لها.
 - 2- تطبيق دوال تمويه تحقق المواصفات المطلوبة مثل MD5, HMAC.
 - 3- زيادة حجم نماذج التعلم و تطبيق شبكات عصبية أخرى لتقليص زمن التدريب والاختبار
 - 4- تشفير قاعدة البيانات باعتماد اسلوب تشفير مناسب.
 - 5- تطوير نموذج ثقة (Trust Model) بالاعتماد على سلوك المستخدم في الماضي والحاضر. يعطي النموذج مستوى ثقة لكل مستخدم قبل مروره بطور التحقق.

المصادر

- 1- D. V. K. (1990). Foiling the cracker: a survey of, and improvements to password security. *Proceedings of the second USENIX UNIX security workshop*, pp. 5-14.
- 2- S. Z. R. and M. M. (2007). User Authentication Using Neural Networks in Smart Home Networks. *International Journal of Smart Home*, Vol. 1: No. 2, July. pp 147-154

An Enhanced Authentication Based on Biometric and Neural Network

Najla Badie

Melad Jader

Nadia Maan

najladabagh@yahoo.com

Abstract: Because of the significant in the field of information technology, increasing means of communication and networks , proliferation of electronic crimes and personality theft, the security of information and verification of the identity of the user became the biggest concerns of institutions and individuals. Hence, several types to verify the reliability of people appeared, some of them relied on traditional means like passwords and smart cards, other modern methods adopted the biometric features for which vital statistics, which depends on the characteristics of natural or unique behavior in people. The artificial neural networks have been used by a large number of researchers to achieve the goals of information security and so as it is ability of learning and modeling of complex relationships between inputs and Outputs.This research suggest a way to improve the user authentication scheme in high security applications in networks. Artificial neural network is used (Back propagation network) to provide privacy to the user and vital feature (fingerprint iris of the eye) being one of the best biometric features to verify the identity of the user as it is the consistency and accuracy in addition to ease of use .