P- ISSN 1991-8941 , E-ISSN 2706-6703
2012 ,(6), (2) :26-32

(*JUAPS*) **مجلة جامعة الانبار للعلوم الصرفة**

Open Access

تحسين الوثوقية باعتماد المقياس الحيوي والشبكات العصبية

نجلاء بديع ابراهيم **ميلاد جادر سعيد** **نادية معن محمد**

جامعة الموصل / كلية علوم الحاسوب والرياضيات

معلومات البحث:

تاريخ التسليم: ٠٠/٠٠/٠٠
تاريخ القبول: ٠٠/٠٠/٠٠
تاريخ النشر: ٩ / ١٢ / ٢٠١٢

DOI: 10.37652/juaps.2012.63374

الكلمات المفتاحية:

الوثوقية ،
المقياس الحيوي ،
الشبكات العصبية.

الخلاصة:

نظرا للتطور الكبير في مجال تكنولوجيا المعلومات وتزايد وسائل الاتصال والشبكات وانتشار جرائم السرقات الالكترونية وانتحال الشخصيّة ، أصبح أمن المعلومات والتحقق من هوية المستخدم من اكبر اهتمامات المؤسسات والافراد. ومن هنا ظهرت عدة انواع للتحقق من وثوقية ألاشخاص ، 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. أقترح هذا البحث طريقة لتحسين اسلوب الوثوقية للمستخدم في التطبيقات عالية الامنية في الشبكات. استّخدمت 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 بالاضافة الى سهولة الاستخدام.

المقدمة

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 فهنالك دائما خشية 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. 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 لخزن الاسم التعريفي المشفر وكلمة السر المشفرة باستخدام دالة التمويه (Hash Function) ليقوم النظام بخزن الاوزان (Weights) بدلا من جدول التحقق [2]. وبالرغم من الفوائد التي قدمتها هذه الطرق مثل عدم قدرة المتطفل من اضافة رقم تعريفي وكلمة سر مزيفتين بالاضافة الى بساطة العمليات الحسابية لاظهار النتائج المطلوبة الا انها بقيت تعاني من بعض نقاط الضعف مثل امكانية تعرضها لهجوم القاموس (Dictionary Attack) الذي يحاول فيه المتطفل بعد حصوله على الاوزان بتجربة كل كلمات السر الممكنة للتحقيق.

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

نّفذ عدد كبير من البحوث في حقل بناء اسلوب الوثوقية باعتماد الصفات الحيوية المستخلصة من المستخدم ، وبحوث اخرى

* Corresponding author at: University of Mosul - College of Computer Science and Mathematics;
E-mail address: najladabagh@yahoo.com

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 Sequare Error (MSE)) وزمن تدريب الشبكة وعدد مراحل تدريب الشبكة لقياس كفاءة الشبكة. وفي [4] أقترح الباحث نظام وثوقية للمقياس الحيوي بالاعتماد على تمييز الوجه باستخدام تحويل الجيب تمام المتقطع (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 الموثق 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 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 والمستخدمة 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 ولايمكن 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 جدا، 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 الإصطناعية (Artificial Neural Network) على أنه العلم الذي يهتم بدراسة أنظمة الضبط والإتصالات 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 [٩].

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 التمويه 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 التمويه لها حيث تقوم دالة التمويه بتحويل الطول المتغير (العشوائي) للبيانات المدخلة الى سلسلة من البيانات ذات طول ثابت (Fixed Length) والتي عادة يكون طولها اصغر من طول البيانات المدخلة [6]. في هذا البحث تم الاستفادة من خصائص هذه الدوال لتحقيق مستوى عالي من الوثوقية حيث تم اعتماد دالة تمويه مبسطة (simple hash function) كحل اولي للخوارزمية المقترحة.

الخوارزمية المقترحة في طور التسجيل:

<u>الادخالات</u> (نماذج التدريب). الرموز التعريفية للمستخدمين، بصمات قزحية العين، كلمات السر.

١. البداية.
٢. قراءة ID للمستخدم.
٣. قراءة كلمة السر للمستخدم وتحويله الى النظام الثنائي.
٤. تطبيق خوارزمية دالة التمويه على ناتج الخطوة السابقة لانتاجHashpassword.انظر الشكل(١).

P- ISSN 1991-8941 , E-ISSN 2706-6703 (*JUAPS*) **مجلة جامعة الانبار للعلوم الصرفة** Open Access
2012 ,(6), (2) :26-32

٥. استخلاص الخواص من قزحية العين المدخلة باستخدام دالة تحويل المويجة.
٦. استخدام الدالة المنطقية NOT لعكس مخرجات الخطوة السابقة.
٧. تطبيق خوارزمية دالة التمويه على مخرجات الدالة المنطقية لانتاج Hashbio.
٨. اجراء عملية XOR بين Hashpassword و Hashbio لانتاج Finalxor.
٩. ادخال Finalxor و ID للمستخدم الى الشبكة العصبية.
١٠. تدريب الشبكة العصبية لحين الحصول على الاخراج الذي يطابق Finalxor.
١١. اخذ قيم الاوزان Wieghts للشبكة عند الوصول للاخراج المطلوب وخزنه بقاعدة بيانات خاصة.
١٢. النهاية.

الاخراجات: قاعدة بيانات بقيم الاوزان.

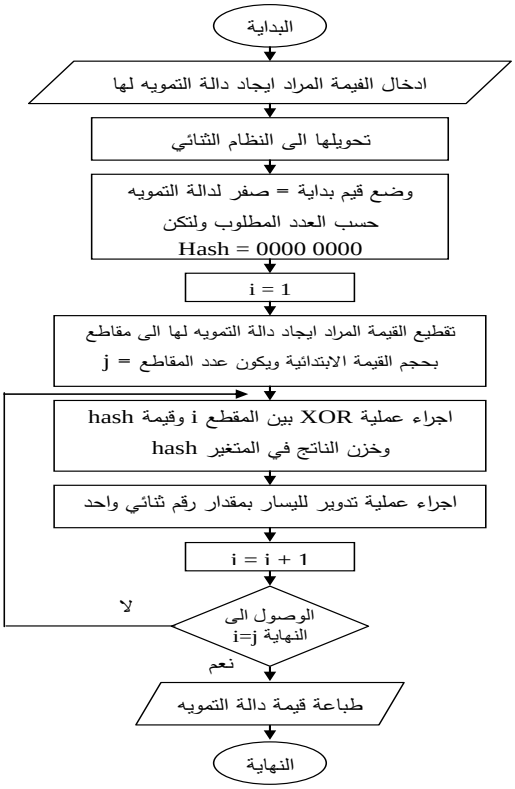
والشكل(٢) يوضح المخطط الصندوقي للخوارزمية المقترحه في طور التسجيل.

الخوارزمية المقترحة في طور التحقق

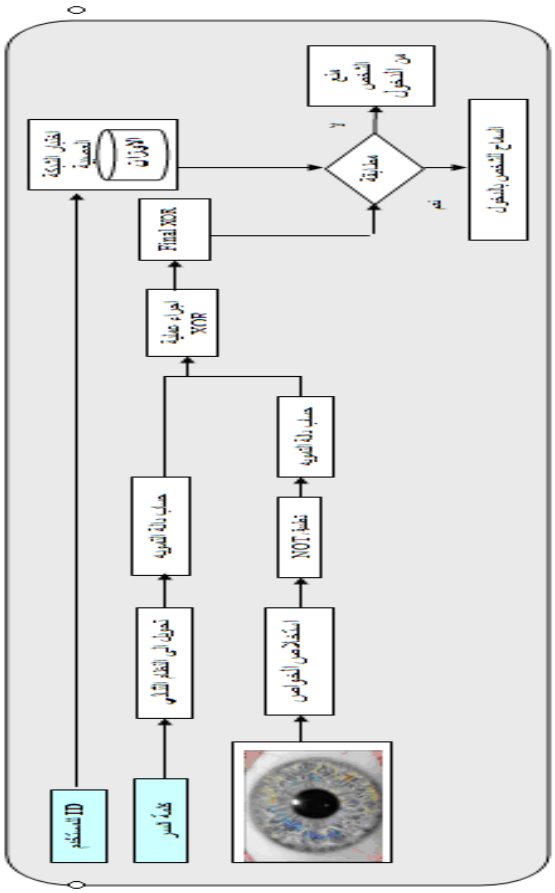
الادخالات: قاعدة بيانات الاوزان،ID للمستخدم، كلمة السر، قزحية العين.

١. البداية.
٢. قراءة قيمة ID للمستخدم.
٣. قراءة كلمة السر للمستخدم وتحويله الى النظام الثنائي.
٤. تطبيق خوارزمية دالة التمويه على ناتج الخطوة السابقة لانتاج Hashpassword.
٥. استخلاص الخواص من قزحية العين المدخلة باستخدام دالة تحويل المويجة.
٦. استخدام الدالة المنطقية NOT لعكس مخرجات الخطوة السابقة.
٧. تطبيق خوارزمية دالة التمويه على مخرجات الدالة المنطقية لانتاج Hashbio.
٨. اجراء عملية XOR بين Hashpassword و Hashbio لانتاج Finalxor.
٩. ادخال Finalxor و ID للمستخدم الى الشبكة العصبية.
١٠. مقارنة نتائج الشبكة العصبية مع الادخال، هل ضمن المسموح.
أ- نعم: الشخص مخول بالدخول للشبكة.
ب- لا: الشخص غيرمخول بالدخول للشبكة.
١١. اعادة الخطوات السابقة على كل الاشخاص الراغبين باستخدام الشبكة.
١٢. النهاية.

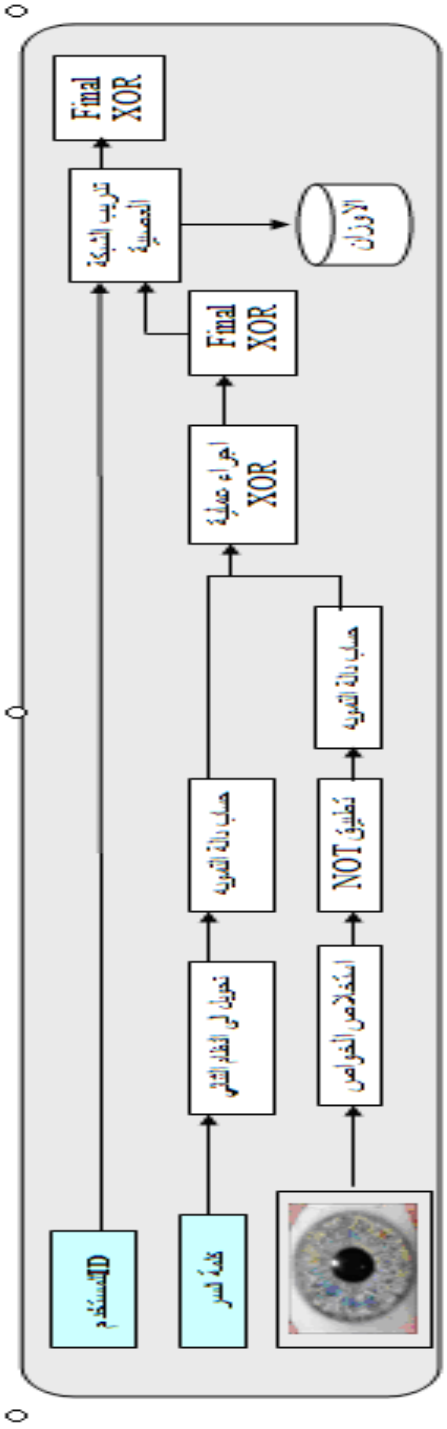
الاخراجات: قبول او رفض دخول الشخص الى الشبكة.والشكل (٣) يوضح المخطط الصندوقي للخوارزمية المقترحه في طور التحقق.



شكل(١):خوارزمية دالة التمويه Hash Function المستخدمة



الشكل(٣)المخطط الصندوقي للخوارزمية المقترحة في طور التحقق



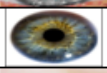
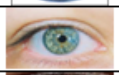
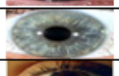
الشكل(2)المخطط الصندوقي للخوارزمية المقترحة في طور التسجيل

الجانب العملي

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

طور التسجيل:

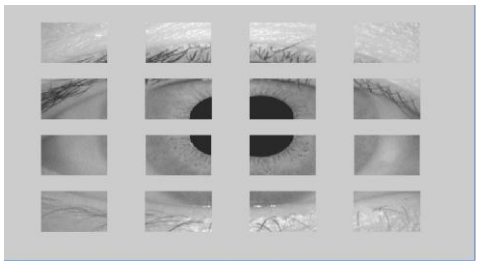
– في بادئ الامر يتم ادخال ID وكلمة السر وقزحية العين للمستخدم ، الجدول (١) يمثل الاشخاص المخولين بالدخول الى الشبكة:

ت	ID للمستخدم	كلمة السر	قزحية العين
1	Ahmad	AB2008	
2	suha	allah	
3	saad	Allah-2009	
4	Fahad	Iraq^2008	
5	Ban-2008	Mbroka	
6	Raseel ha	RH2008	
7	ZENAzena	hello	
8	SaraA.S.	hadba	
9	Omar ali	O_M_A_R	
10	XYZ-abc	ziad	

جدول (1) الاشخاص المخولين

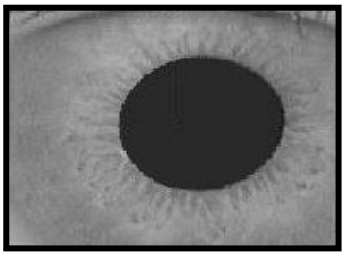
– يتم اخذ قزحية العين واستخلاص الخواص منها باستخدام دالة تحويل المويجة وباتباع الخطوات التالية:

* بما ان الصورة تضم صورة العين باكملها بضمنها جفون ورموش العين وليست القزحية فقط فيجب اولا قطع صورة القزحية ليتم التركيز عليها في عملية استخلاص الخواص، ولذا تقطع الصورة باستخدم التقطيع المنتظم(systematicclassification) الى١٦جزء (٤*٤) كما في الشكل(٤).



الشكل(٤):صورة العين بعد تقطيعها الى ١٦جزء

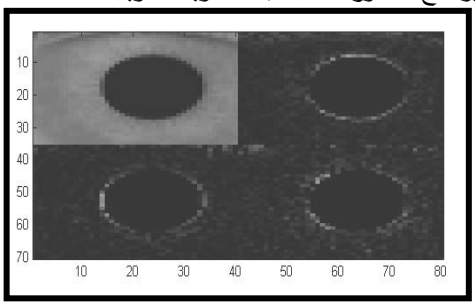
* من الشكل(٥) نلاحظ استقرار القزحية في وسط الصورة أي الاجزاء الاربعة الداخلية للصورة بعد التقطيع لهذا تجمع صورة القزحية من هذه الاجزاء لتكون الصورة الموضحة في الشكل (٥).



الشكل(٥):القزحية بعد اقتصاصها من صورة العين

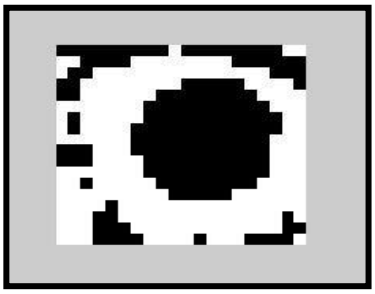
P- ISSN 1991-8941 , E-ISSN 2706-6703 (*JUAPS*) **مجلة جامعة الانبار للعلوم الصرفة** Open Access
2012 ,(6), (2) :26-32

بعد اقتصاص صورة القزحية من صورة العين تبدأ مرحلة استخلاص الخواص باستخدام دالة تحويل المويجه من نوع (DB1) ولثلاث مستويات لتنتج صورة مصغرة للقزحية ، الشكل (٦) يوضح الصورة الناتجة بعد تحويل المويجه.



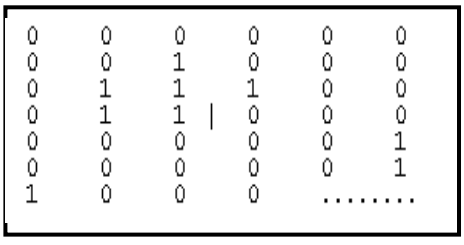
الشكل(٦):صورة القزحية بعد استخلاص خواصها

- تحول الصورة الناتجة الى رمز ثنائي باستخدام طريقة العتبة (thresholding)، ليتسنى تمثيلها بالرقمين (١و٠) و الشكل (٧) يوضح الصورة الثنائية.



الشكل(٧):الصورة الثنائية الناتجة من قزحية العين

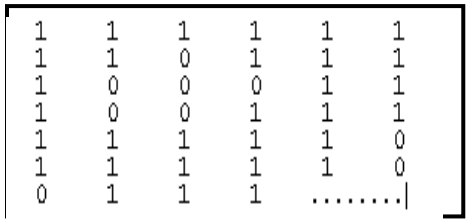
يتم الان تحويل صورة القزحية الى مصفوفة ثنائية لتسهيل التعامل معها والشكل (٨) يوضح جزء من هذه المصفوفة لكبر حجمها:



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	1
0	0	0	0	0	1
1	0	0	0	.....	

الشكل (٨):المصفوفة الثنائية لقزحية العين

تم استخدام الدالة المنطقية NOT لعكس مخرجات الخطوة السابقة، والشكل (١٠) يوضح المصفوفة الاخيرة:



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(٩):المصفوفة الثنائية بعد تطبيق NOT

- يتم حساب دالة التمويه لقزحية العين بعد اجراء الخطوات السابقة ، باستخدام الاسلوب المبسط لدالة التمويه وحسب الخوارزمية الموضحة بالشكل (٢) ويكون الناتج عبارة عن بايت من النظام الثنائي فقط ١٠١١٠١١٠
- تحويل كلمة السر المدخلة الى النظام الثنائي وحساب دالة التمويه لها، وايضا يكون الناتج هو بايت واحد من النظام الثنائي ٠١٠٠١٠١٠
- اجراء عملية XOR بين ناتج الخطوتين السابقتين لينتج لنا Finalxor، والجدول (٢) يوضح القيم الناتجة للخطوات السابقة للاشخاص المخولين بالدخول الى الشبكة.

الجدول (٢):قيم دالة التمويه لكلمة السروقزحية العين وقيم Finalxor

ID للمستخدم	دالة تمويه كلمة السر	دالة تمويه قزحية العين	Finalxor
Ahmad	٠١٠٠١٠١٠	١٠١١٠١١٠	١١١١٠١٠٠
Suha	١١١١١٠٠٠	٠١١١٠١١١	١٠٠٠١١١١
Saad	١١١٠٠١٠٠	٠٠٠٠١٠١١	١١٠١١١١١
Fahad	١١٠٠٠١١١	٠٠١١١١١٠	١١١١١٠٠١
Ban-2008	٠١١٠١١١١	١٠١١٠٠٠٠	١١٠١١١١١
Raseel ha	١٠١٠١٠١٠	١١١٠٠٠١١	٠١٠٠١٠٠١
ZENAzena	١٠٠٠١١١٠	٠٠١١٠٠١١	١٠١١١١٠١
SaraA.S.	١٠٠١٠٠٠١	١١١١٠٠٠١	٠١١٠٠٠٠٠
Omar ali	٠٠٠١٠١١٠	١٠٠٠٠٠١١	١٠٠١٠١٠١
XYZ-abc	٠١٠١٠١١١	٠٠٠١١١١١	٠١٠٠١٠٠٠

ادخال قيم ال Finalxor مع قيمة ID للمستخدم الى الشبكة لتنفيذ طور التدريب لحين الحصول على المخرجات المطلوبة (Finaltest) لاحظ الجدول(٣).

الجدول (٣):جدول التدريب Training table

ID للمستخدم	Finalxor
Ahmad	١١١١٠١٠٠
Suha	١٠٠٠١١١١
Saad	١١٠١١١١١
Fahad	١١١١١٠٠١
Ban-2008	١١٠١١١١١
Raseel ha	٠١٠٠١٠٠١
ZENAzena	١٠١١١١٠١
SaraA.S.	٠١١٠٠٠٠٠
Omar ali	١٠٠١٠١٠١
XYZ-abc	٠١٠٠١٠٠٠

- ناتج الخطوة السابقة يمثل قاعدة بيانات الاوزان للاشخاص 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 الاوزان 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 (٣).

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 ممكن ان تحل بكفاءة محل الطرق السابقة حيث انها تحقق:-

١- زيادة ألامان في أنظمة التوثيق الحيوي لاعتمادها على أكثر من وسيلة للتحقق.

٢- 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.

٣- أعتماد بصمة قزحية العين يؤدي الى فشل هجوم القاموس عندما يستخدم من قبل المتطفل بالاضافة الى التقليل من خطر استخدام كلمات سر اعتيادية والتي ممكن نسيانها، سرقتها ، أو اعتراضها من قبل المتطفل.

تطلبت الطريقة المقترحة عمليات حسابية بسيطة لاظهار النتائج مقارنة مع انظمة الحماية الاخرى. بالاضافة الى وقت قصير لتدريب الشبكة والحصول على الاوزان.

التوصيات

على الرغم من كون اسلوب التحقق من الشخصية باعتماد المقاييس الحيوية يعتبر أفضل بمراحل من أساليب الحماية التقليدية الا انه لايمكن اعتباره اسلوبا مثاليا" لامن المعلومات لاننا لانعرف ما يمكن أن تقدمه لنا ألايام القادمة ، خصوصا وان هذا الحقل يعتبر ارض خصبة للبحوث في الوقت الحاضر. وكمقترحات مستقبلية يوصى بما يلي:

١- دراسة الثغرات والتهديدات الامنية وايجاد الحلول المناسبة لها.

٢- تطبيق دوال تمويه تحقق المواصفات المطلوبة مثل MD5, HMAC.

٣- زيادة حجم نماذج التعلم و تطبيق شبكات عصبية أخرى لتقليص زمن التدريب والاختبار

٤- تشفير قاعدة البيانات باعتماد اسلوب تشفير مناسب.

٥- تطوير انموذج ثقة (Trust Model) بالاعتماد على سلوك المستخدم في الماضي والحاضر. يعطي انموذج 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

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 inMobile Environments. *International Journal of Engineering and Inustries*, Vol. 2: NO. 2, June.pp103-112

٦- الناظر سائد. (٢٠٠٥) . التعمية و امن الشبكات. شعاع للنشر والعلوم.

٧- جاسم سجى، جادر ميلاد و اسامة ايلاف. (2010) . التشفير الفوضوي باستخدام مفتاح المقياس الحيوي. *مجلة الرافدين لعلوم الحاسوب والرياضيات*. المجلد ٧: العدد ٣ .

٨- 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 ، عزو د.عماد.(٢٠٠٠). الشبكات العصبية (البنية الهندسية ،الخوارزميات ، التطبيقات). سورية–حلب.

P- ISSN 1991-8941 , E-ISSN 2706-6703 (*JUAPS*) مجلة جامعة الانبار للعلوم الصرفة Open Access
2012 ,(6), (2) :26-32

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 .