مجلة جامعة تشرين للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (36) العدد (4) 2014
Tishreen University Journal for Research and Scientific Studies - Engineering Sciences Series Vol. (36) No. (4) 2014

التحقق من التواقيع اليدوية باستخدام التوابع الإحصائية لصورة التوقيع

الدكتورة مريم محمد ساعي*
الدكتور محمد مصطفى حجازية**
رلى مريشة***

(تاريخ الإيداع 26 / 3 / 2014. قُبِل للنشر في 23/ 7 / 2014)

□ ملخّص □

يقترح البحث طريقة جديدة تهدف إلى التحقق من صورة التوقيع اليدوي لشخص ما، وتحديد فيما إذا كان التوقيع يعود لهذا الشخص أو أنه توقيع مزور. وتم ذلك بالاعتماد على استخلاص سمات هندسية من صورة التوقيع الموجودة في قاعدة البيانات وإجراء عمليات إحصائية رياضية عليها كطريقة للتحقق من توقيع هذا الشخص.

تم استخلاص السمات من صورة التوقيع على مراحل متعددة حيث تم تحويل صورة التوقيع من الصيغة الرمادية إلى الصيغة الثنائية ثم استخلاص الخصائص الإحصائية للتوقيع الأصلي وهي القيم الأكبر بين القيم الأكثر تكراراً في إحداثيات الواحدات التي تحدد شكل التوقيع، بالإضافة لعدد الواحدات التي تحدد شكل التوقيع، ثم تم تحديد مجالين للقيم المقبولة للتوقيع الأصلي. وبنفس الاسلوب ويتم استخلاص السمات الإحصائية للتواقيع المزورة واختبارها إذا كانت تنتمي إلى مجال القيم المقبولة المحدد.

كما يتضمن البحث مقارنة لنتائج الطريقة المقترحة مع الطرق السابقة في هذا المجال. تم اختبار الطريقة المقترحة باستخدام قاعدة البيانات مكونة من16200 توقيع موزعة على 300 شخص، وكنتيجة لذلك تم التحقق بنسبة جيدة من صورة التوقيع اليدوي.

الكلمات المفتاحية : معالجة الصورة، التعرف على النماذج، صورة التوقيع، كشف التوقيع، سمات من صورة التوقيع، التحقق من صحة الأشخاص باستخدام صورة التوقيع، التوابع الإحصائية.

* مدرس – قسم الحاسبات والتحكم الآلي– كلية الهندسة الميكانيكية والكهربائية– جامعة تشرين– اللاذقية– سورية.
** مدرس – قسم الحاسبات والتحكم الآلي– كلية الهندسة الميكانيكية والكهربائية– جامعة تشرين– اللاذقية– سورية.
*** مهندسة – قسم الحاسبات والتحكم الآلي– كلية الهندسة الميكانيكية والكهربائية – جامعة تشرين– اللاذقية– سورية.

مجلة جامعة تشرين للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (36) العدد (4) 2014
Tishreen University Journal for Research and Scientific Studies - Engineering Sciences Series Vol. (36) No. (4) 2014

Handwritten Signature Verification using Statistical Functions for Signature Image

Dr. mariam M. Saii*
Dr. Mohammed Hijazieh **
Rula Mrishah***

(Received 26 / 3 / 2014. Accepted 23 / 7 / 2014)

□ ABSTRACT □

This research suggests a new method that aims to verify the manual signature image which is written by person, and specify whether this signature back to this person or that forged signature. This was done by extracting geometric features of the signature image and applying statistical functions on them as a way to verify the signature of that person.

The features from the signature image have been extracted on many stages, so a signature image has been transformed from the gray scale to binary format, and then extracting the statistical features from the original signature image which is the maximum value from the most repeated values in the ones' coordination line that determine the signature shape, in addition to the number of ones which also determine the signature shape. Finally two ranges have been identified for the values accepted for original signature image. By the same way, statistical features have been extracted from the foreign signature image and tested if they aggregate within the specified domain of acceptable values. This research also includes the results of the proposed approach that compared with the previous methods in this scope. The proposed method has been tested to the data base consisting of 16200 signatures back to 300 persons, and as a result the signature image has been verified with a good percentage.

Keywords: Image processing, Pattern recognition, Signature image, Signature detection; Signature Image's features, off line Signature verification, statistical functions.

*Assistant Professor, department of Computer and Automatic control Engineering, Tishreen University, Lattakia, Syria.
**Assistant Professor, department of Computer and Automatic control Engineering, Faculty of Mechanical and Electrical Engineering, Tishreen University, Lattakia, Syria.
***Engineer , computer and Automatic control Engineering Department, Faculty of Mechanical and Electrical Engineering, Tishreen University, Lattakia, Syria.

مقدمة :

يعتمد التوقيع اليدوي في توثيق العديد من المستندات الرسمية، ويوجد–حتى يومنا هذا–خبراء في تحليل الخطوط يستطيعون من خلال خبرتهم أن يؤكدوا ما إذا كان التوقيع هو توقيع أصلي (أي أنه يعود صاحب التوقيع بالفعل)، أم أنه مزوّر.كما أنه لا تنطبق ملامح شخصين تمام الانطباق، كذلك لا ينطبق خط شخص على خط شخص آخر تمام الانطباق، بل لابد من وجود تباين ولو طفيف بينهما، والمقصود هنا الانطباق لا التشابه، فمن الممكن جداً أن يتشابه خطّا شخصين لكنهما لا ينطبقان إطلاقاً .وقد أكدت التجارب –ويستطيع كل شخص فرد أن يلمس ذلك– أن الشخص الواحد لا يستطيع أن يكتب شيئاً واحداً مرتين بنفس التطابق ،حتى ولو كان هذا الشيء هو توقيعه، فإذا صادف وجود توقيعين منطبقين بشكل كامل فإنه يؤكد أن أحدهما ،لا ريب، مزور **[1]**.

تصمم الأنظمة البيومترية من أجل هدفين هما التعرف recognition على شخص والتحققverification من هويته، وهما هدفان منفصلان، لكن على الرغم من ذلك لا يوجد نظام مخصص لأحد الهدفين دون الآخر، وإنما حاجات البيئة تملي علينا أي هدف نختار. الاستخدام الأكثر شيوعاً هو التحقق أي– وكما هو واضح من التسمية– التحقق من المستخدم باستخدام البيانات التي يقدمها، على سبيل المثال عندما يدخل المستخدم x اسمه وكلمة السر الخاصة به يقوم نظام التحقق البيومتري بجلب القالب البيومتري له ثم إذا حصل تطابق match بين العينة المدخلة وإحدى العينات الموجودة في قاعدة البيانات التابعة للنموذج عندئذٍ يقر النظام بأن المستخدم x هو فعلاً x وليس شخصاً آخر يقوم بعملية انتحال أو تزوير للمستخدم x [2,3]

بالمقابل يهدف التعرف إلى اتخاذ قرار حول معرفة هوية المستخدم بدون أن يقوم المستخدم بإدخال بيانات خاصة به ،على سبيل المثال تستخدم أنظمة التعرف على التواقيع بشكل رئيسي لأغراض التعرف حيث تتم مقارنة صورة لتوقيع المستخدم من خلال جهاز ما ومن ثم يتم البحث في قاعدة البيانات عن عينة تطابق بياناتها البيانات المدخلة[2,3].

إن الاعتماد على الحاسوب في عمليات التعرّف أو التحقّق من توقيع اليد ليس بالمهمة اليسيرة ،ولهذا فقد درست بشكل مكثّف وقد تم التوصل إلى عدد كبير من الطرق تم طرحها والعمل بها ونشرت أبحاث عديدة في هذا المجال:

تم نشر بحث بعنوان " التحقق من التوقيع اليدوي بشكل غير مباشر باستخدام مصنف الشبكة العصبونية الصنعية" "Off-line Handwritten Signature Verification using Artificial Neural Network Classifier" **[4]**، قدمت هذه الدراسة معالجة مبدئية لصور التواقيع ومن ثم استخلاص ميزات هندسية من شكل التوقيع مثل مركز التوقيع و نسبة طوله إلى عرضه وتقسيم صورة التوقيع إلى أربع مناطق لدراسة توزع كثافة التوقيع في كل منطقة من الصندوق الذي يحدده طول التوقيع وعرضه، ثم تم إدخال القيم الناتجة عن الميزات المستخلصة السابقة إلى شبكة عصبونية لتدريبها **[4]**.

تم نشر بحث بعنوان: " Off-line Signature Verification Based on Pseudo-Cepstral Coefficients"**[5]**. قدم هذا البحث عملية معالجة مبدئية لصور التواقيع ، حيث تم تحويل الصور إلى المستوى الرمادي وتم حساب الهيستوغرام لكل صورة لحساب معاملات Pseudo-Cepstral وبالتالي الحصول على سلسلة فريدة unique sequence لكل توقيع.تم استخدام هذه السلسلة كشعاع ميزات لمقارنته مع أشعة الميزات لصور تواقيع في قاعدة البيانات المؤلفة من 100 شخص **[5]**.

تم نشر بحث بعنوان :"التحقق واستخلاص الميزات من صورة التوقيع باستخدام تقنية العنقدة" **[6]** أو "Features Extraction and Verification of Signature Image using Clustering Technique" . عمل هذا البحث على إجراء معالجة مبدئية لصور التواقيع ومن ثم تم استخلاص ميزات خاصة من شكل التوقيع مثل نسبة طول التوقيع إلى عرضه، ونسبة مشغولية التوقيع و هو نسبة عدد البكسلات التي تمثل شكل التوقيع إلى العدد الكلي لبكسلات الصورة.يتم بعدها تجميع الميزات المستخرجة من صورة التوقيع الأصلي في عدة عناقيد ، عدد هذه العناقيد مساوٍ لعدد الأشخاص في قاعدة البيانات و بعدها يتم استخراج الميزات من صورة التوقيع المراد التحقق منه لنحصل على عدة قيم لهذه الميزات، وبعدها تأتي مرحلة إيجاد العنقود المناسب لهذه القيم فإذا كانت هذه القيم مطابقة لقيم إحدى العناقيد السابقة فهذا يعني أن التوقيع غير مزور أما إذا كانت هذه القيم بعيدة عن القيم السابقة فهذا يعني أن التوقيع مزور**[6]**.

وتم نشر بحث بعنوان: "مقارنة الميزات المختلفة في نماذج ماركوف المخفية وعمل SIFT لقاعدة بيانات صورة التواقيع اليدوية " أو "Invariant Features Comparison in Hidden Markov Model and SIFT for Off-line Handwritten Signature Database". عمل هذا البحث على الحد من الاختلافات الناتجة عن ميل زاوية البدء بالتوقيع والتغييرات الداخلية ضمن محيطه وذلك باستخلاص الميزات من صور التواقيع باستخدام نماذج ماركوف المخفية وتقنية التحويل المويجي المتقطع [7].

وتم نشر بحث بعنوان: "التعرف على التوقيع اليدوي صعوداً من المرحلة الأساسية صعوداً" أو " Handwritten Signature Recognition From the Ground Up " .اعتمد هذا البحث على استخلاص ثلاث ميزات رسومية من صورة التوقيع الأصلي ومقارنتها مع أخرى من التوقيع المزوّر باستخدام طريقة تشابه المجموعات، حيث تم تحديد مركز التوقيع و اختيار32 نقطة متساوية البعد على محيط هذا التوقيع للحصول على الفرق بين مسافات نقطتين محيطتين متجاورتين إلى مركز صورة التوقيع و الزاوية بين الخط المرسوم بين النقطة المحيطة والمركز ومحور السينات بالإضافة إلى عدد البكسلات الموجودة في مثلث مرسوم بين المركز، وكل زوج من النقاط المحيطة المتجاورة [8].

وتم نشر بحث بعنوان:"التحقق غير المباشر من التوقيع اليدوي باستخدام الطرق الحديثة في معالجة الصورة"[9]، اعتمد هذا البحث على استخلاص نفس الميزات الرسومية من صورة التوقيع التي استخدمت في الدراسة [8], ولكن تمت عملية التحقق باستخدام الشبكات العصبونية وقد حسنت من نسبة النتائج السابقة.

وغيرها العديد من الدراسات التي اهتمت بالعمل في هذا المجال. يصنف هذا البحث تحت إحدى الطرق البيومترية التي تهدف إلى التحقق من صورة التوقيع اليدوي الذي يكتبه شخص ما فيما إذا كان هذا التوقيع يعود لهذا الشخص أو أنه توقيع مزور باستخدام طريقة جديدة غير مستخدمة سابقاً.

أهمية البحث وأهدافه :

تعد عملية التحقق من التواقيع اليدوية عملية معقدة جداً، وابتكار نظام عالي الفاعلية والتمييزية غاية في الصعوبة حيث يمضي الخبراء في هذا المجال سنوات من التدرّب على فهم الفروقات الدقيقة والحساسة بين التواقيع [2,3].

نظراً لزيادة البنوك المصرفية وأهمية العمل فيها، تم العمل على إنجاز هذا النظام الذي يمكن تطبيقه في واحدة من هذه النظم البنكية والمصارف حيث يتم أخذ عدة تواقيع للمودع الواحد بغية إدخال هذه التواقيع في قاعدة البيانات

لإمكانية التحقق من هذا الشخص لاحقاً في حال أراد سحب رصيده من البنك، ويمكن للعديد من المؤسسات الحكومية الاستفادة منه وخاصة المؤسسات التي لا يزال موظفوها يقومون بالتوقيع في بداية الدوام الرسمي وفي نهايته.

يقدم البحث نظاماً آلياً للتحقق من صور التواقيع اليدوية للأشخاص (أي تمييزها عن المزورة) عن طريق مقارنة هذه التواقيع مع تواقيع أصلية موجودة في قاعدة البيانات ضمن الحاسوب ،وذلك باستخدام تقنيات معالجة الصور الرقمية والتوابع الإحصائية.

طرائق البحث ومواده :

تصمم أنظمة التحقق من التواقيع اليدوية بطريقتين هما: الأنظمة المباشرة أو الديناميكية On-Line systems والأنظمة غير المباشرة أو السكونية Off-line (static) systems [12] :

1) الأنظمة المباشرة أو الديناميكية (On-line (dynamic) systems): ويتم في هذا النوع من الأنظمة كتابة التوقيع باستخدام قلم خاص على سطح الكتروني لذلك يتطلب عتاداً خاصاً للعمل به، أي تكون هذه الأنظمة على اتصال مع مصدر المعلومات متضمنة الالتقاط الرقمي الفوري للتوقيع. تتميز هذه الأنظمة بأنها تستطيع أن تسجل عدة عناصر هامة بالنسبة للتحقق من التوقيع منها الزمن المستغرق في عملية التوقيع ومقدار ضغط القلم[3].

2) الأنظمة غير المباشرة أو السكونية (Off-line (static) systems): يتم في هذا النوع من الأنظمة العمل على استخلاص سمات معينة من صور تواقيع مخزنة في قاعدة بيانات باستخدام تقنيات معالجة الصورة، أي تكون دون اتصال مباشر مع مصدر المعلومات[3].

يقدم البحث نظاماً غير مباشر للتحقق من صورة التوقيع اليدوي وذلك لأنه أكثر شيوعاً بسبب عدم احتياجه لتوفر عتاد لإدخاله ولا يشترط الاتصال المباشر لمصدر المعلومات مع النظام.

توجد نسبتين تحددان كيفية قياس أداء نظام التحقق وحساب فعاليته هما معدل القبول الخاطئ ومعدل الرفض الخاطئ.

1) معدل القبول الخاطئ False Acceptance Rate :

واختصاراً يشار إليه بـ FAR ويقاس بالنسبة المئوية للمرات التي يقبل فيها النظام شخصاً كان يجب أن يرفضه (عدد التواقيع المزورة التي قبلها النظام) ، فعندما يستطيع مهاجم أن يخترق تطبيقاً أو موقعاً بيومترياً يقل أمن هذا التطبيق لذا يحاول منتجو هذه الأنظمة أن يجعلوا نسبة FAR أقل ما يمكن. ويعطى FAR بالعلاقة [5,6]:

$$FAR = \frac{\text{عدد التواقيع المزورة التي قبلها النظام}}{\text{عدد الأشخاص} \times \text{عدد التواقيع المزورة التي تم اختبارها}}$$

لا بد من الإشارة إلى أن نسبة الخطأ هذه لا بد من أن ترتفع عند تطبيق النظام على أرض الواقع بسبب عدة عوامل مثل عدم تآلف المستخدم مع هذا النوع من التطبيقات أو ظروف البيئة أو إخفاق برمجي أو عتادي و لأسباب تعود إلى حتمية التشابه بين العينات البشرية عند استخدام صفات بيومترية تملك نسبة تخالف منخفضة.

2)معدل الرفض الخاطئ False-rejection Rate:

واختصاراً يشار إليه بـ FRR ويقاس بالنسبة المئوية للمرات التي يرفض فيها النظام شخصاً كان يجب أن يقبله مما قد يؤدي إلى منع الأشخاص من تأدية واجباتهم نتيجة عدم التعرف عليهم من قبل النظام و تعطى بالعلاقة [5,6]:

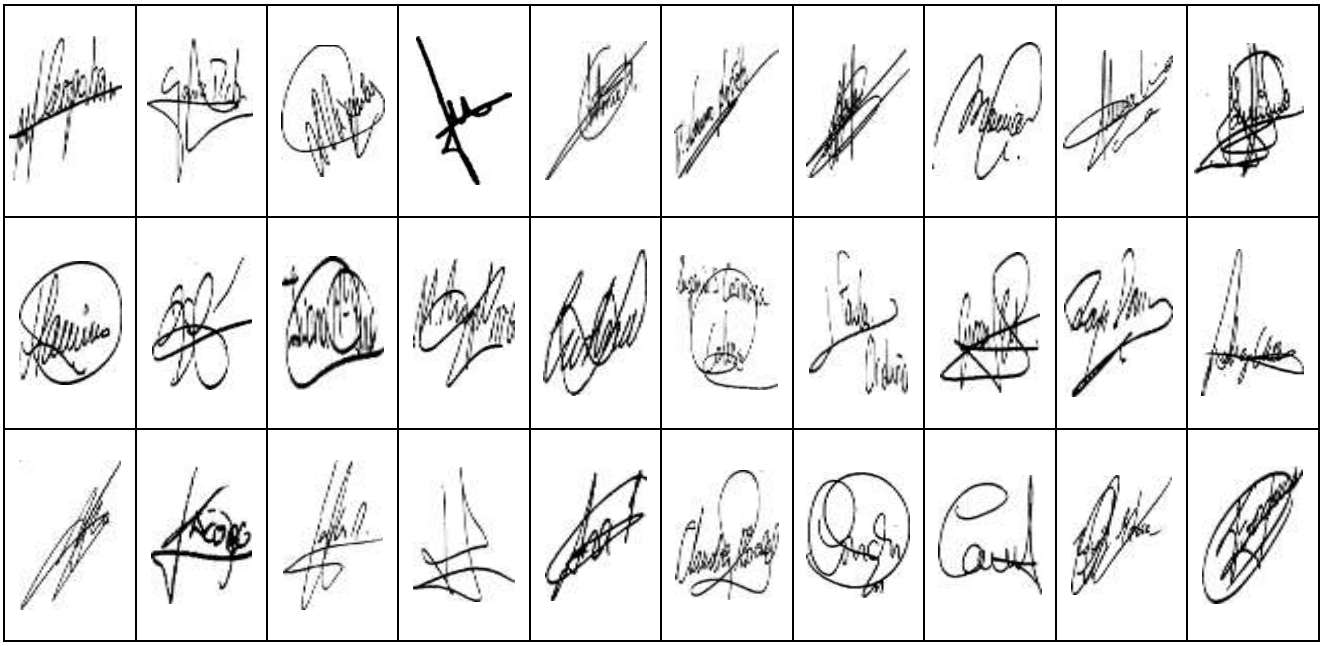
$$FRR = \frac{\text{عدد التواقيع الأصلية التي رفضها النظام}}{\text{عدد الأشخاص} \times \text{عدد التواقيع الأصلية التي تم اختبارها}}$$

1- قاعدة البيانات المستخدمة :

تم استعارة قاعدة بيانات صور التواقيع من قاعدة بيانات متوفرة للاستخدام على موقع جامعة Universidad de Las Palmas de Gran Canaria الإسبانية على الرابط التالي: (http://www.gpds.ulpgc.es/download/)[4]،حيث تحتوي على 16200 توقيع موزعة على 300 شخص يحدد كل شخص برقم ، لكل مستخدم 24 توقيع أصلي و30 توقيع مزور عن التواقيع الأصلية[4].

يبين الجدول (1) أول 30 توقيع يعود لأول 30 مستخدم في قاعدة البيانات المؤلفة من 300 مستخدم.

الجدول (1) أول 30 توقيع يعود لأول 30 مستخدم في قاعدة البيانات



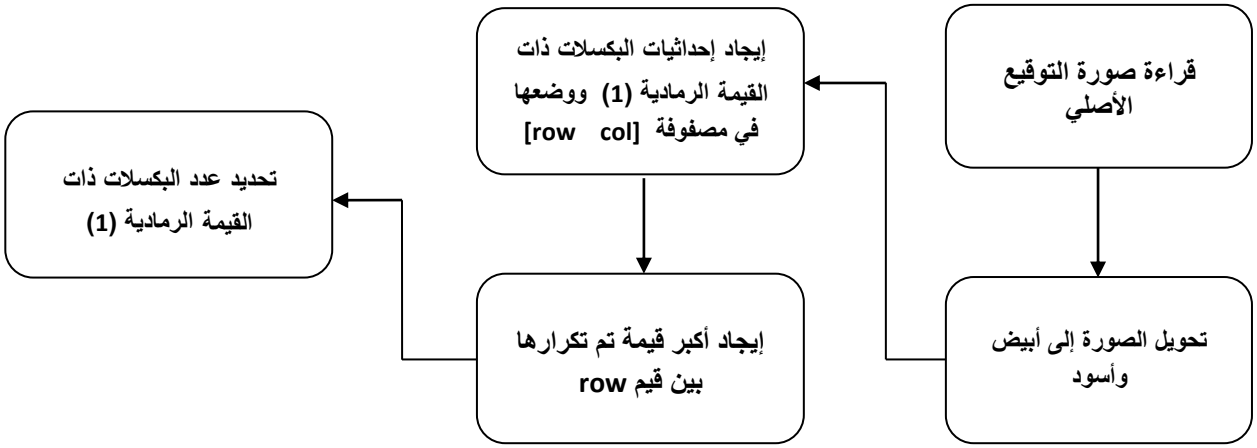
النتائج والمناقشة :

1 – نظام التحقق من صورة التوقيع اليدوي:

يقترح البحث طريقة جديدة للتحقق من صورة التوقيع اليدوي باستخدام تقنيات معالجة الصورة والتوابع الإحصائية وقد تم العمل على تنفيذ خطوات الاستخلاص برمجياً باستخدام تعليمات معالجة الصورة والتوابع الإحصائية في برنامج الماتلاب. وتم العمل على مرحلتين هما استخلاص السمات من صورة التوقيع وتطبيق التوابع الاحصائية عليها ومرحلة تحديد مجال القيم المقبولة.

1-1 المرحلة الأولى: مرحلة استخلاص السمات من صورة التوقيع اليدوي وتطبيق التوابع الإحصائية عليها:

يبين الشكل (1) المخطط الصندوقي للمرحلة الأولى من مراحل نظام التحقق من التوقيع اليدوي وهي استخلاص السمات من صورة التوقيع وتطبيق التوابع الإحصائية عليها.

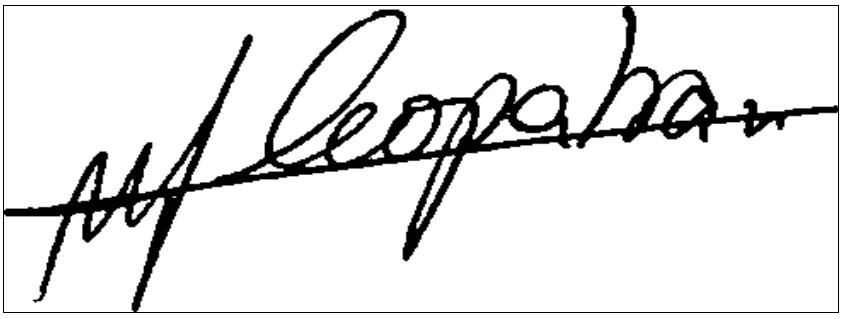


الشكل (1) المخطط الصندوقي لمرحلة استخلاص السمات من صورة التوقيع

الخطوات التفصيلية للمرحلة الأولى من مراحل استخلاص السمات من صورة التوقيع الأصلي:

1-عملية قراءة صورة التوقيع باستخدام التعليمة imread كما في الشكل (2).

2-عملية تحويل الصورة إلى أبيض وأسود باستخدام التعليمة im2bw في الماتلاب كما في الشكل (3).



الشكل (2) صورة توقيع أصلي

الشكل (3) صورة التوقيع الأصلي بعد تحويلها إلى أبيض وأسود

3-إيجاد إحداثيات البكسلات ذات القيم الرمادية المساوية لـ(1) أي البكسلات البيضاء في الصورة، حيث تقوم هذه البكسلات بتحديد شكل التوقيع بين البكسلات السوداء المحيطة وقد تم ذلك باستخدام التعليمة [row col]= find(==1) .

لم يتم العمل على تطبيق عمليات معالجة مثل (Skeleton أو Thinning) للصورة لأن مثل هذه العمليات تعمل على تقليل البكسلات التي تحدد شكل التوقيع وبالتالي تعمل على حذف البكسلات التي تنتج عن مقدار ضغط الشخص على القلم أثناء عملية التوقيع، وعملية الضغط هذه مفيدة جداً في عملية التحقق من تزوير التوقيع لأن المزور قد يعمل على تقليد شكل التوقيع ولكن لن تكون عنده دراية بمقدار ضغط الشخص الأصلي على القلم ولهذا السبب لم يتم العمل على مثل هذه العمليات لنزيد من دقة النظام.

4-إيجاد قيم الإحداثيات الأكثر تكراراً في سطر البكسلات ويتم ذلك باستخدام تابع الإحصاء الوصفي الذي يدعى بالمنوال mode ، ثم نعمل على إيجاد القيمة الأكبر بين هذه القيم الأكثر تكراراً باستخدام التابع max أي تصبح التعليمة max(mode(row)). مثلاً أكبر قيمة إحداثيات تم تكرارها في سطر الإحداثيات للتوقيع الأول الأصلي للمستخدم رقم 10 من قاعدة البيانات هي (199) وهذه القيمة ناتجة عن أكبر قيمة تم تكرارها في سطر إحداثيات البكسلات البيضاء المحددة لشكل التوقيع وليس عن قيم الصورة الثنائية (أبيض=1/أسود=0).

5-إيجاد قيمة عدد البكسلات ذات القيم الرمادية المساوية لـ(1) أي البكسلات البيضاء في الصورة التي تقوم بتحديد شكل التوقيع (يظهر الشكل 3 النقاط البيضاء التي تحدد شكل التوقيع وهي بكسلات ذات سوية رمادية مساوية للواحد ، حيث يكون لكل بكسل إحداثيات أي سطر وعمود) وذلك باستخدام التابع find أيضاً حيث يعطي عدد البكسلات ذات القيمة واحد. مثلاً عدد الواحدات للتوقيع الأول الأصلي للمستخدم رقم 10 من قاعدة البيانات هو (87189).

تم العمل على تكرار المرحلة الأولى (المكونة من الخطوات الأربعة المشروحة بالتفصيل سابقاً) لأول 14 توقيع أصلي لكل شخص في قاعدة البيانات لنحصل في كل مرة على أكبر قيمة تم تكرارها في سطر بيانات التوقيع وعلى عدد الواحدات التي تحدد شكل التوقيع .في نهاية عملية التكرار نحصل على مصفوفتين كل مصفوفة فيها 14 قيمة ،المصفوفة الأولى هي مصفوفة القيم الإحصائية التي تمثل القيمة الأكبر بين القيم الأكثر تكراراً والمصفوفة الثانية هي عدد الواحدات لكل توقيع أصلي. مثلاً المصفوفة الأولى للمستخدم رقم 10 من قاعدة البيانات(القيم الاحصائية لأول 14 توقيع أصلي):

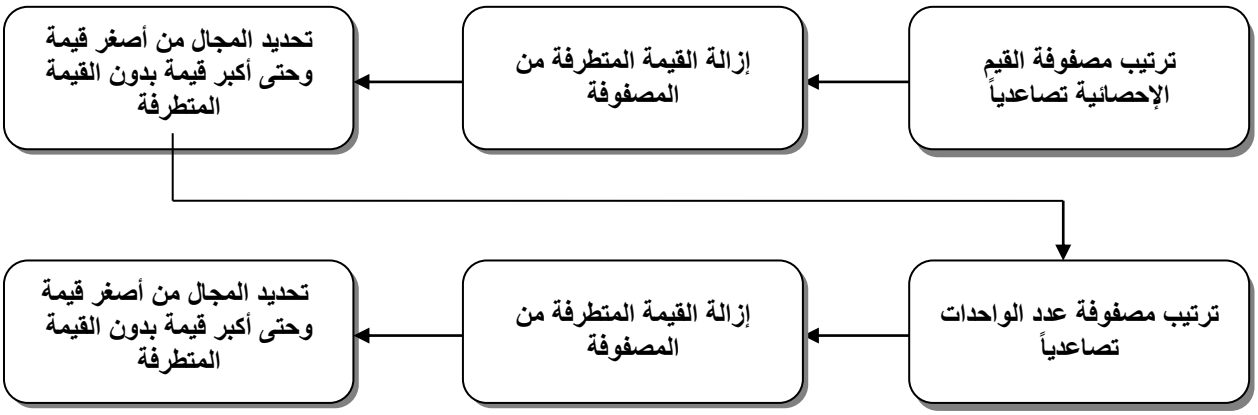
[199 248 227 205 228 223 227 219 192 228 263 218 346 307]

والمصفوفة الثانية للمستخدم رقم 10 من قاعدة البيانات (عدد الواحدات لأول 14 توقيع أصلي):

[87189 115477 110988 106633 116591 103552 106036 119523 103392 119635 134896 121566 182991 155463]

2-1 المرحلة الثانية: مرحلة تحديد مجال القيم المقبولة :

يمثل الشكل (4) المرحلة الثانية من مراحل استخلاص السمات .



الشكل (4) المرحلة الثانية من مراحل استخلاص السمات

الخطوات التفصيلية للمرحلة الثانية من مراحل استخلاص السمات من صورة التوقيع الأصلي:

1-ترتيب المصفوفة القيم الإحصائية المكونة من 14 قيمة تصاعدياً وذلك باستخدام التعليمة sort.

مثلاً تصبح المصفوفة الأولى للمستخدم رقم 10 من قاعدة البيانات:

[192 199 205 218 219 223 227 227 228 228 248 263 307 346]

2-نلاحظ من قيم سمات المصفوفة السابقة بوجود قيمة بعيدة جداً عن قيم السمات الأخرى المتقاربة الموجودة تسمى القيمة المتطرفة ، لذلك نعمل على إزالتها و ذلك بالعمل على إيجاد الفرق بين القيمة الصغرى في المصفوفة المرتبة والقيمة التالية لها ، ثم حساب الفرق بين القيمة الكبرى في المصفوفة والقيمة السابقة لها . يدل الفرق الأكبر على القيمة المتطرفة، فمثلاً إذا كان فرق القيمة الصغرى أكبر من فرق القيمة الكبرى تكون القيمة الصغرى هي القيمة المتطرفة في المصفوفة ويتم حذفها من المصفوفة وإلا تكون القيمة الكبرى. مثلاً تكون القيمة المتطرفة المصفوفة الأولى للمستخدم رقم 10 من قاعدة البيانات (346).

في حال وجود أكثر من قيمة متطرفة (مثلاً لو تكررت القيمة المتطرفة 346) سيكون الفرق بين القيمة العظمى والقيمة السابقة لها هو صفر،وبالتالي سيكون الفرق بين القيمة الصغرى والقيمة التالية لها هو الفرق الأكبر وهذا يؤدي إلى إزالة القيمة الصغرى.وفي حال تساوي قيمتي الفرقين سيتم إزالة إحدى القيمتين ولتكن القيمة المتطرفة العظمى.

3-تعبر أصغر قيمة وأكبر قيمة في المصفوفة الناتجة بعد حذف القيمة المتطرفة [min1 max1] عن مجال قيم السمات المقبولة لشخص معين أي يصبح min1= 192 و max1=307

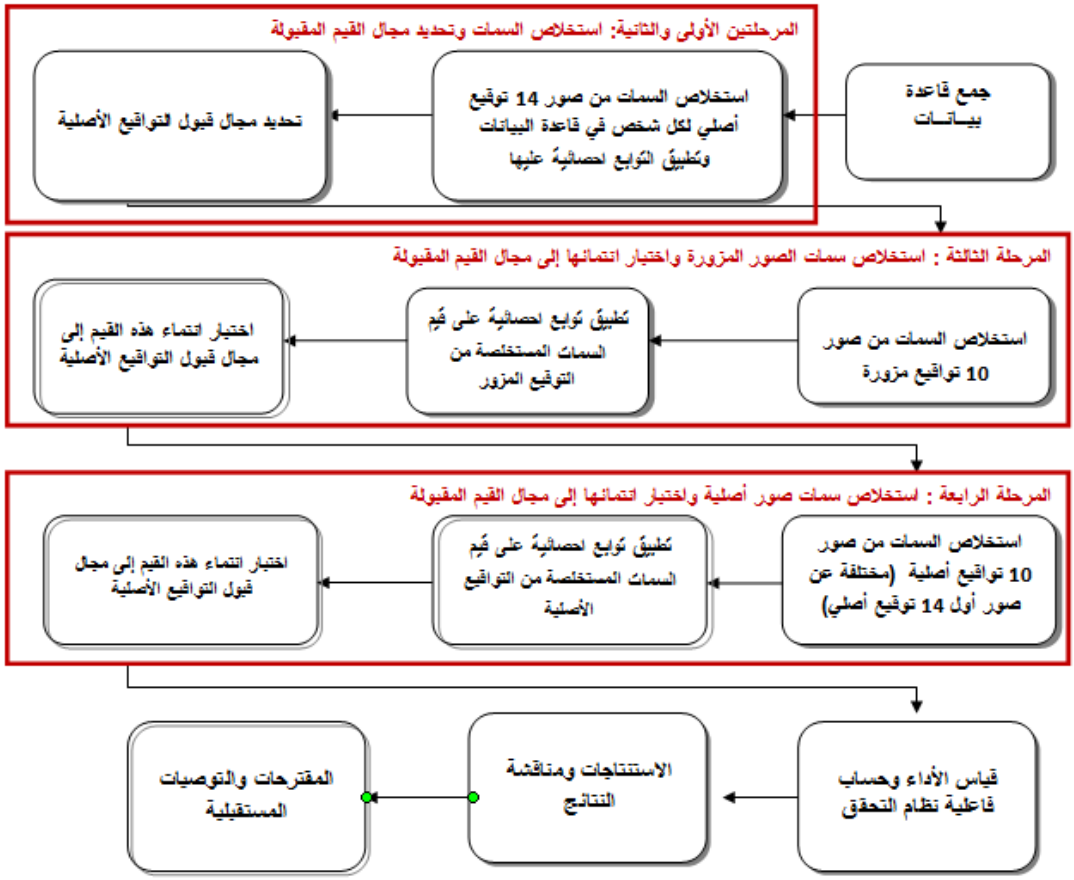
نطبق الخطوات من 1 حتى 3 على مصفوفة الواحدات أيضاً للحصول على مجال آخر لقيم السمات المقبولة لشخص معين [min2 max2]. تصبح min2= 87189 و max2=155463 للمستخدم رقم 10 من قاعدة البيانات.

لاختبار توقيع مُدخل فيما إذا كان يعود للشخص نفسه أو أنه مزور يجب أن تكون قيمة السمة الإحصائية الأولى التي سيتم استخلاصها من صورته تنتمي للمجال الأول و أن تكون عدد واحدات هذا التوقيع تنتمي للمجال الثاني بنفس الوقت.

تم العمل في المرحلتين الأولى والثانية على تحديد مجالات القيم المقبولة لتوقيع أصلي يعود لشخص معين في قاعدة البيانات، نكرر المرحلتين السابقتين لإيجاد مجالات القيم المقبولة لكل من شخص في قاعدة البيانات المؤلفة في هذا النظام من 300 شخص، لأنه لكل توقيع قيم سمات مختلفة تماماً عن التواقيع الأخرى لأشخاص آخرين في قاعدة البيانات ولكن متشابهة مع التواقيع المزورة عنه ويعمل هذا النظام على مقارنة السمات الأصلية مع السمات المزورة .

2- مراحل العمل:

تم العمل على نظام التحقق من صور التواقيع بإجراء الخطوات التي يبينها الشكل(5) التالي:



الشكل (5) المخطط الصندوقي لمراحل العمل التفصيلية

بعد العمل على جمع قاعدة البيانات واستخلاص السمات من صور التواقيع وتطبيق التوابع الإحصائية عليها ثم تحديد مجال القيم المقبولة، نعمل على تمرير 10 تواقيع مزورة و10 تواقيع أصلية للشخص نفسه (مختلفة عن التواقيع الأصلية التي تم منها تحديد مجال القيم المقبولة) وذلك لمعرفة عدد التواقيع المزورة التي سيعمل النظام على رفضها وعدد التواقيع الأصلية التي سيقوم النظام بقبولها.

2-1 المرحلة الثالثة: استخلاص السمات من صور التواقيع المزورة واختبار انتمائها لمجال القيم المقبولة:

تم العمل في هذه المرحلة على استخلاص السمات لـ10 تواقيع مزورة غير أصلية وذلك بتطبيق المرحلة الأولى على صور التواقيع المزورة ،وبنفس الخطوات تم الحصول على مصفوفة السمات الأولى المكونة من 10 قيم إحصائية تمثل كل منها القيمة الأكبر بين القيم الأكثر تكراراً لكل توقيع وعلى مصفوفة السمات الثانية هي عدد الواحدات المكونة أيضاً من 10 قيم. نختبر انتماء كل قيمة من القيم العشرة المزورة المستخلصة في المصفوفة الأولى إلى مجال القيم المقبولة الأول [min1 max1] ونختبر كل قيمة من القيم في المصفوفة الثانية إلى مجال القيم المقبول الثاني [min2 max2]، فإذا كانت القيمتان تقعان ضمن المجالين بنفس الوقت اعتبر التوقيع أصلياً وإلاّ اعتبر مزوراً.

وكمثال القيمة الأكبر بين القيم الأكثر تكراراً للتوقيع رقم 1 المزور للمستخدم رقم 10 هي (245) نجد أنها تنتمي للمجال الأول وعدد الواحدات هو(86748) نجد أنه لا ينتمي للمجال الثاني فالتوقيع يعتبره النظام مزوراً.

2-2 المرحلة الرابعة:استخلاص السمات من صور التواقيع الأصلية واختبار انتمائها لمجال القيم المقبولة:

تم العمل في هذه المرحلة على استخلاص السمات لـ10 تواقيع أصلية مختلفة عن 14 توقيع أصلي الذي تم استنتاج مجال القيم المقبولة منها وذلك بتطبيق المرحلة الأولى على صور التواقيع الأصلية الجديدة ،وبنفس الخطوات تم الحصول على مصفوفة السمات الإحصائية المكونة من 10 قيم ومصفوفة سمات عدد الواحدات المكونة أيضاً من 10 قيم . نختبر انتماء كل قيمة من القيم العشرة الأصلية المستخلصة في المصفوفة الأولى إلى مجال القيم المقبولة الأول [min1 max1] ونختبر كل قيمة من القيم في المصفوفة الثانية إلى مجال القيم المقبول الثاني [min2 max2] ، فإذا كانت القيمتان تقعان ضمن المجالين بنفس الوقت اعتبر التوقيع أصلياً وإلاّ اعتبر مزوراً.

فمثلاً القيمة الأكبر بين القيم الأكثر تكراراً للتوقيع رقم 17 الأصلي للمستخدم رقم 10 هي (296) نجد أنها تنتمي للمجال الأول وعدد الواحدات هو(153604) نجد أنه ينتمي للمجال الثاني فالتوقيع يعتبره النظام أصلياً.

3- قياس الأداء و حساب فاعلية نظام التحقق من التوقيع:

3-1معدل القبول الخاطئ False Acceptance Rate :

وهي نسبة التواقيع المزورة التي رفضها النظام ،عند تطبيق النتائج على العلاقة نحصل على مايلي:

$$FAR = \frac{527}{300 \times 10} = 0.1756 \rightarrow \quad FAR = 17.56\%$$

3-2 معدل الرفض الخاطئ False-rejection Rate:

وهي نسبة التواقيع الأصلية التي رفضها النظام ،عند تطبيق النتائج على العلاقة نحصل على مايلي:

$$FRR = \frac{1749}{300 \times 10} = 0.583 \rightarrow \quad FRR = 58.3\%$$

3-3 مقارنة النتائج مع نتائج دراسات سابقة :

قدمت العديد من الأبحاث طرقاً مختلفة تهدف إلى التحقق من صورة التوقيع اليدوي الذي يكتبه شخص ما فيما إذا كان هذا التوقيع يعود لهذا الشخص أو أنه توقيع مزور-تم ذكر البعض منها في مقدمة هذا البحث-. وتم ذلك بالاعتماد على استخلاص سمات هندسية مختلفة وعديدة جداً من صورة التوقيع الموجودة في قاعدة البيانات وعملت على التحقق من هذا الشخص أيضاً بطرق عديدة منها استخدام الشبكات العصبونية (عدة أنواع من الشبكات

العصبونية) أو باستخدام عملية مطابقة لسمات التوقيع الأصلي مع المزور أو باستخدام التوابع الإحصائية وغيرها العديد من الطرق.

قدمت هذه الدراسة طريقة جديدة في استخلاص سمات من صورة لتواقيع الأصلية واعتمدت على التوابع الإحصائية الرياضية لتحديد التواقيع المقبولة واستخدمت قاعدة بيانات كبيرة جداً معتمدة من جامعة Universidad de Las Palmas de Gran Canaria الإسبانية وهذه القاعدة قد تم استخدامها أيضاً من قبل الدراسة [8]. يبين الجدول (2) نتائج هذه الدراسة بالمقارنة مع نتائج الدراستين السابقتين بحيث كل دراسة استخدمت طرقاً مختلفة في عملية التحقق .

الجدول (2) مقارنة النتائج مع نتائج دراسات سابقة

طريقة التحقق	السمات المستخلصة من صورة التوقيع	حجم قاعدة البيانات	FAR	FRR
باستخدام التوابع الإحصائية	– مجال القيم الأكبر بين القيم الأكثر تكرارا في سطر إحداثيات الواحدات التي تحدد شكل التوقيع بعد استبعاد القيم المتطرفة – مجال لعدد الواحدات للبكسلات التي تحدد شكل التوقيع بعد استبعاد القيم المتطرفة.	10200 توقيع	17,56%	58,3%
باستخدام شبكة عصبونية [8]	Δrt– الاختلاف بين مسافات نقطتين محيطتين متجاورتين إلى مركز الصورة. θt– الزاوية بين الخط المرسوم بين النقطة المحيطة والمركز ومحور السينات. At– عدد البكسلات الموجودة في مثلث مرسوم بين المركز وكل زوج من النقاط المحيطة المتجاورة	10200 توقيع	15,7%	81,3%
باستخدام مطابقة المجموعات[7]	Δrt– الاختلاف بين مسافات نقطتين محيطتين متجاورتين إلى مركز الصورة. θt– الزاوية بين الخط المرسوم بين النقطة المحيطة والمركز ومحور السينات. At– عدد البكسلات الموجودة في مثلث مرسوم بين المركز وكل زوج من النقاط المحيطة المتجاورة	64 توقيع	21,87%	56,25%

الاستنتاجات والتوصيات:

الاستنتاجات:

بمقارنة الدراستين السابقتين مع بعضهما نجد أن إدخال شبكة عصبونية على نفس السمات قد أعطى نتائج أفضل من حيث قبول التواقيع المزورة، ولكن أدى ذلك إلى رفض نسبة كبيرة من التواقيع الأصلية آخذين بالاعتبار الفرق الهائل في قاعدة البيانات المستخدمة .أي إن إدخال الشبكة العصبونية من حيث النتائج التي أعطاها أكثر أمناً، لأن رفض التواقيع الأصلية سيكون أفضل أمنياً من حيث المبدأ من قبول التواقيع المزورة ، وهذا ما يحصل في أغلب

البنوك والمصارف، بحيث يطلب في هذه الحالة من الشخص إعادة عملية التوقيع بحيث تكون ،قدر الإمكان، مماثلة للتواقيع التي تدرب عليها النظام.

استخدمت هذه الدراسة نفس قاعدة البيانات التي اعتمدها الدراسة التي استخدمت الشبكة العصبونية ولكن بالاعتماد على طريقة جديدة باستخدام التوابع الاحصائية فنجد أن نسبة التواقيع المزورة التي قبلها النظام تزيد قليلاً عن سابقتها ولكنها استطاعت تحسين وتقليل نسبة التواقيع الأصلية التي رفضها النظام بشكل كبير وواضح.

التوصيات:

إن عملية التحقق من التواقيع ليست عملية سهلة، كما أن مقدار العمل البحثي المخصص للتقنيات المُصمَّمة لتطوير الطرق المتوفرة سيشهد على صحة ذلك. إن ابتكار نظام عالي الفاعلية هو أمر غاية في الصعوبة. ورغم ذلك إنّ التحقق من تواقيع خطوط اليد سيدرس ويحسّن بشكل كبير في السنوات القادمة.

يقترح للدراسات المستقبلية:

1- استخلاص عناصر وميزات بطريقة أخرى من صورة التوقيع :

يمكن العمل على تقسيم صورة التوقيع إلى أربع مناطق لدراسة توزع كثافة التوقيع (أي عدد البكسلات ذات السوية الرمادية المساوية لـ1) في كل منطقة من الصندوق الذي يحدده طول التوقيع وعرضه ويتم تطبيق الطريقة المقترحة على المناطق الأربعة وبالتالي تصبح المقارنة مع أربع مجالات للقيم المقبولة، و العمل على دراسة أثر زيادة عدد هذه الميزات على دقة النتائج.

2- *زيادة عدد التواقيع الأصلية التي يتم منها تحديد مجال القيم المقبولة:*

أي العمل على زيادة حجم قاعدة البيانات وذلك للعمل على أكثر من 14 صورة للتوقيع الأصلي مما يزيد من مجال القيم المقبولة ،و العمل على دراسة أثر هذه الزيادة على دقة النتائج.

3- *استخدام أنواع أخرى من التوابع الاحصائية للتحقق من صور التوقيع:*

يمكن العمل على تطبيق توابع إحصائية أخرى على صورة التوقيع أو على قيم إحداثيات الواحدات التي تحدد شكل التوقيع، مثل التابع الرياضي الإحصائي المجال Range الذي يحدد الفرق بين أعلى قيمة وأقل قيمة أو تطبيق تابع الانحراف المعياري STD الذي يمثل الجذر التربيعي للتباين، وغيرها الكثير من التوابع الإحصائية.

المراجع:

1. المحامي الأستاذ نجاح حمشو. *الكتابة اليدوية والعوامل المؤدية لاختلاف الخطوط* . فرع دمشق.
2. Shirdhonkar,M.S; Kokare,M .*Off-Line Handwritten Signature Identification Using Rotated Complex Wavelet Filters*, International Journal of Computer Science Issues, Vol. 8, Issue 1, January 2011.
3. Arya,M.S; Inamdar,V.S . *A Preliminary Study on Various Off-line Handwritten Signature Verification Approaches*, International Journal of Computer Applications, Vol. 1, 2010.
4. Sisodia,K; Anand,M.S. *Off-line Handwritten Signature Verification using Artificial Neural Network Classifier* , International Journal of Recent Trends in Engineering, Vol 2, No. 2, November 2009, 205-207 .
5. Ferrer,M.A; Travieso,C.M; Alonso,J.B .*Offline Signature Verification Based on Pseudo-Cepstral Coefficients,* International Conference on Document Analysis and Recognition , Spain, 2009.

6. Biswas,S; Kim,T; Bhattacharyya,D. *Features Extraction and Verification of Signature Image using Clustering Technique* , International Journal of Smart Home Vol.4, July, 2010, 43-56 .
7. Shukla,N ; Shandilya,M . *Invariant Features Comparison in Hidden Markov Model and SIFT for Offline Handwritten Signature Database* , International Journal Of Computer Applications , *Volume 2 – No.7, June 2010.*
8. Sheffield.T.*Handwritten Signature Recognition from the Ground Up*, International Conference on Document Analysis and Recognition, 2009.
9. م. رلى مريشة ،ود. مريم ساعي ود. محمد حجازية *بناء نظام للتحقق غير المباشر من صورة التوقيع اليدوي باستخدام الطرق الحديثة في معالجة الصورة*، رسالة ماجستير ، جامعة تشرين، 2013.
10. Jan.2009.http://www.gpds.ulpgc.es/download/
11. McCabe, A; Trevathan, J; Read,W. *Neural Network-based Handwritten Signature Verification* . Journal of Computers, Vol. 3, NO. 8, AUGUST 2008, 9- 22.
12. Gurney, K . *An Introduction to Neural Networks.* Taylor & Francis, London, 2005,139.
13. Marques de Sá, J.P . *Applied Statistics Using SPSS, STATISTICA MATLAB and R,* 2nd Edition , Springer, New York, 2007,505.
14. Martinez,W.L; Martinez,A.R. *Computational Statistics Handbook with Matlab*, Chapman & Hall/CRC ,USA, 2002.
15. TchSource Systems. *Statistics & Data Analysis using Neural Network, TchSource* Systems SdnBhd, 2005.
16. Sjöberg,J . *Neural Networks*, 1th edition, wolfram Research, Sebtemper 2005.