Application of Chaotic Neural Network for Authentication using the Database

Ammar Thaher Yaseen Abd Alazeez

ammarthaher@yahoo.com

College of Computer Science and Mathematics

University of Mosul, Mosul, Iraq

Received on: 26/02/2013

Accepted on: 03/04/2013

ABSTRACT

In this paper a new algorithm is suggested to encrypt data, since it was to take advantage of properties of the chaotic, so it was entered as a key in encryption and hiding by entering values to the artificial neural network for training as well as hide in the picture, beside use the database for storage and retrieval information and increase the secret system. Through the overlap between the results of stages encryption and hide and artificial neural network algorithm was obtained exciting new strength from where you can not detect secret text only after obtaining random values of the chaotic algorithm and information about neural network algorithm as well as algorithm of work.

Keywords: Neural network, security, database, authentication.

تطبيق الشبكة العصبية الفوضوية للوثوقية باستخدام قاعدة البيانات

عمار ظاهر ياسين عبد العزيز

قسم علوم الحاسوب

كلية علوم الحاسوب والرياضيات

جامعة الموصل

تاريخ قبول البحث : 2013\4\3

تاريخ استلام البحث : 2013\2\26

الملخص

تم في هذا البحث اقتراح خوارزمية جديدة لتشفير البيانات، إذ تم الاستفادة من خصائص الدالة الفوضوية بإدخالها كعامل أساسي بعملية التشفير والإخفاء من خلال إدخال قيمها إلى الشبكة العصبية الاصطناعية للتدريب وكذلك الإخفاء في الصورة، فضلاً عن استخدام قاعدة البيانات لغرض خزن واسترجاع المعلومات وزيادة في سرية النظام. ومن خلال التداخل بين نتائج مراحل التشفير والإخفاء والشبكة العصبية تم الحصول على خوارزمية جديدة تمتاز بقوتها من حيث عدم إمكانية كشف النص السري إلا بعد الحصول على القيم العشوائية للخوارزمية الفوضوية ومعلومات عن الشبكة العصبية فضلاً عن خوارزمية العمل. الكلمات المفتاحية: الشبكة العصبية، السرية، قواعد البيانات، الوثوقية.

1. المقدمة

ظهر في الوقت الراهن اهتمام متجدد بابتكار طرائق موثوقة وسريعة للتمييز الذاتي لهوية الفرد، ومنها هندسة اليد، وطرارز الأوعية الدموية في شبكية العين واليد، وبصمة الصوت وديناميكية التوقيع الشخصي.

إن قدرة الإنسان على التعلم واكتساب الخبرة مما يتدرب عليه، لفت انتباه الكثير من العلماء الذين يعملون في مجال الحواسيب الالكترونية، مما حدا بهم إلى تقليد عمل الدماغ البشري لمحاكاة عمل الخلايا العصبية، مما أدى إلى ظهور علم الشبكات العصبية الاصطناعية (Artificial Neural Network) الذي هو فرع من فروع الذكاء الاصطناعي (Artificial intelligence). أن الشبكة العصبية هي أنموذج حسابي مبني على خواص الشبكة العصبية الحيوية، وتتكون من وحدات مترابطة بعضها ببعض بروابط اعتمادية (Dependencies)، وتقوم هذه الشبكات بمعالجة البيانات باستخدام مبدأ حسابي يسمى بـ (Connectionist Approach). [1],[2].

أما إخفاء البيانات فهي عملية نقل البيانات خلال بيانات أخرى كمضيف أو حامل "Carrier" بطريقة تحافظ على المعلومات المنقولة، هذه الطريقة تخفي وجود أي اتصالات سرية كما تمنع المراقب من اكتشاف وجود بيانات مخفية. أما بالنسبة للحامل فقد يكون صورة أو صوت أو نص أو فيديو... الخ. المعلومات المخفية تحتاج إلى مفتاح إخفاء وهو عبارة عن معلومات سرية إضافية، مثل كلمة المرور "Password".

إن علمي الإخفاء والتشفير يستخدمان (رغم اختلافهما) في تأكيد وثوقية البيانات، ففي التشفير يمكن لأي طرف أن يكتشف إن ثمة طرفين يتصلان بطريقة مشفرة، أما في إخفاء المعلومات فيخفي أصلاً وجود الاتصال فلا يمكن لأحد أن يلاحظ وجود طرفين يتبادلان الرسائل عبر قنوات الاتصال. [3] [4].

أما مصطلح الفوضى Chaotic فيطلق على الأنظمة التي هي في الأساس غير خطية وتعرض سلوك عشوائي لمجموعة من القيم. ومع ذلك فإن الحلول أو مسارات النظام تبقى محددة بمرحلة الفضاء. هذه المرحلة تبقى غير مستقرة، تعتمد بصورة كبيرة على قيم المتغيرات وعلى الطريقة التي يبدأ بها النظام. من هذه المتغيرات " الحساسية للقيمة الابتدائية (Sensitivity To Initial Condition) "، وهي أهم ميزة من مميزات النظم الفوضوية؛ إذ تعتمد النظم الفوضوية بشكل كبير على مقدار القيمة الابتدائية لها، فعند إعطاء قيمة ابتدائية لنظام معين، فمن المعروف انه يمكن توقع الحالة المستقبلية للنظام. إلا أنه في أنظمة الفوضى فان توقع المدى البعيد يستحيل التنبؤ به. [5].

تم في هذا البحث الاستفادة من خواص الشبكة العصبية وعلمي الإخفاء والتشفير والأنظمة الفوضوية فضلاً عن قواعد البيانات في الحصول على نظام جديد للوثوقية يمكن استخدامه في الأنظمة ذات السرية العالية مثل المصارف والمطارات والتي تحتاج إلى الوثوق من الأشخاص التي تتعامل معهم.

2. الدراسات السابقة

في عام 2010 قدم الباحثون سجي القدو وميلاد سعيد وإيلاف عبدالمجيد خوارزمية جديدة للتشفير تعتمد على المقاييس الحيوية للإنسان (قزحية العين) لإنتاج مفتاح التشفير وذلك باستخلاص الخواص من خلال تحويلات الموجية والاستفادة من مميزات الدالة الفوضوية. [5]. كما قدم الباحث كوانك وآخرين في عام 2010 نظاماً للتنبؤ لحالة الطقس، يركز على استخدام الدالة الفوضوية في الشبكات العصبية في مطار هونك كونج الدولي. [6]. أما الباحثان الكر دالكيران وكنان دانيسام فقد قدما في عام 2010 شبكة عصبية تختلف عن سابقتها بطريقة التدريب، حيث اعتمدت نتائج الدالة الفوضوية في التدريب، فضلاً عن اعتماد التشفير وفك التشفير بمرحلتين، الأولى عن طريق الدالة الفوضوية والثانية عن طريق الشبكة العصبية، ثم المقارنة بين نتائج كلا الطريقتين. [7]. وفي عام 2011 قدم الباحثان هاربريت كوار وتربارتجو سنك نظاماً للتشفير، يعتمد على استخدام الدالة الفوضوية مع الشبكة العصبية. [4]. وكذلك في عام 2012 قدم الباحث سوراب باردواج وآخرون طريقة جديدة لتوقع السلاسل

الفوضوية بالاعتماد على نماذج ماركوف، ومن ثم تجميعها لاعتمادها في التدريب للشبكات العصبية لأغراض التمييز بين النماذج. [8].

3. الصور الرقمية

أصبحت الصور الرقمية من الأجزاء الأساسية في أنظمة المعلومات، كذلك اعتمادها في العديد من التطبيقات المختلفة للوسائط المتعددة (التي شاع تداولها بشكل واسع)، ويمكن عدها عرضا بصريا لمصفوفة ثنائية من الأعداد الصحيحة، والتي قيمتها تحدد قيمة تدرج رمادي؛ في حالة الصور ذات التدرج الرمادي، أو لون محدد في حالة الصور الملونة، وكذلك يمكن تعريف الصور الرقمية، بأنها عينات منفصلة في فضاء معين، تضم بيانات رقمية تمثل كل قيمة منها إضاءة نقطة ضوئية في الصورة. تصنف الصور الرقمية حسب التصنيف اللوني إلى أربعة أنواع: الصور الثنائية (Binary Image)، الصور ذات التدرج الرمادي (Gray Level Image)، الصور الملونة (Colored Image)، الصور متعددة الأطياف (X-ray Image). [9].

4. الإخفاء والتشفير وأمنية المعلومات

لعلم الإخفاء أسلوبان هما؛ الأول: العلامة المائية "Water marking" والتي يمكن تعريفها على أنها وسيلة لإيجاد دليل إثبات للملكية، وتعريف نسخة محرمة في التوزيع للمعلومات في الوسائط المتعددة. الثاني: الإخفاء أو نظام التغطية "Steganography"، يُعرف إخفاء المعلومات على أنه عملية تضمين بيانات سرية في أشكال مختلفة من الوسائط الرقمية المتعددة (Digital Multimedia) كملفات النصوص والصور والملفات الصوتية والفيديو. ومع النمو السريع لتقنيات الشبكات والاتصالات، فإن تقنيات إخفاء المعلومات أصبحت تستخدم بصورة واسعة لتحقيق أغراض متعددة، منها حماية حقوق الطبع وتثبيت الملكية وتحقيق الاتصال بصورة سرية [3].

إن الغاية من إخفاء المعلومات ليست منع الآخرين من معرفة المعلومات المخفية، بل لإزالة الشك أصلا في وجود معلومات مخفية، والشيء المميز في تقنيات إخفاء المعلومات أنها تواكب التقنيات الحديثة، ويمكن استخدامها في جميع الوسائط الحاسوبية من صور، نصوص صوت، فيديو، وحزم الشبكة...الخ. [5].

وهذا يعني أن نظام التغطية ليس جزءا من علم التشفير، فالفرق بينهما كبير وعلى سبيل المثال، فإن علم التشفير يترك أثرا واضحا في معالم الرسائل المرسل، ولا يتطلب وسطا ثانيا لإخفاء البيانات، ويمكن القول أن التشفير هو تغيير المعالم الظاهرة للنص المرسل بإحدى خوارزميات التشفير، بحيث يصعب فهمها بعد تشفيرها، إلا من قبل المرسل والمستلم، بينما التضمين كعلم يتطلب وسطا ثانيا يتم إخفاء البيانات داخله، وهذا الذي يجعل هذه التقنية مختلفة عن التشفير "Cryptography"، ففي التشفير يعلم المهاجم بوجود البيانات، وقد يستطيع الوصول إليها، لكنه لا يستطيع قراءتها إلا بعد كسر الشفرة. انظر الشكل (1) لملاحظة تصنيف تقنيات إخفاء المعلومات. [3].

1.4. فوائد نظام التغطية ومساوئه

إن الفوائد المرجوة من نظام التغطية هي إمكانية استخدامه للنقل السري للرسائل من دون اكتشافها. كما إن استخدامه يعزز سرية الاتصالات الشخصية ويعد وسيلة مهمة للاتصال خصوصا عبر الإنترنت.

أما المساوئ فهي أنها تحتاج إلى غطاء كبير الحجم لإخفاء عدد قليل من البيانات. كما إن اكتشاف الرسالة المخفية يعد من عيوب نظام التغطية لأنه بذلك سوف تنتفي الحاجة إلى نظام التغطية وقد يتم اعتراض رسالة سرية ذات أهمية كبيرة. [4],[10],[11].

الشكل (1) تصنيف تقنيات إخفاء المعلومات

5. الفوضى

الفوضى هي إحدى السلوكيات التي تربط الأنظمة غير الخطية، والتي تحدث تطوراً في القيم المحددة لنظام المعلومات؛ إذ اعتبر اكتشاف هذا النظام العشوائي ثورة أدت إلى العديد من القضايا المترابطة، مثل نظرية الاستقرار، والميزات الهندسية الجديدة، وعروض تمييز التوقع. استخدمت الدالة الفوضوية أساساً لتطوير النماذج الرياضية، واجتذبت العديد من الرياضيين، بسبب الحساسية العالية للقيمة الابتدائية، وتطبيقاتها لمشكلات الحياة اليومية؛ منها التنبؤات الجوية، والنظام الشمسي، واقتصاد السوق، وحركة الأسهم المالية والتزايد السكاني وإخفاء المعلومات لزيادة الأمانة ولما امتازت به الدوال الفوضوية من ميزات جيدة، فقد استخدمت في هذا البحث لتشفير وإخفاء الرسالة السرية في محاولة لزيادة سرية المعلومات المنقولة وتأمين عملية النقل.

ظاهرة الفوضى هي ظاهرة حتمية وتناظرية، وهي عملية عشوائية تظهر في النظام الديناميكي، وهي تعتمد على تحديد الشروط البدائية، بسبب الحساسية الشديدة للظروف الأولية خارج مدارات الانتشار على كامل المساحة، هذه الخاصية ولدت ما يسمى بمفهوم (تأثير الفراشة) ونصها "إن التأثير البسيط الذي يولده جناح الفراشة يؤدي بالتالي إلى حدوث أعاصير في أماكن أخرى من العالم بعد فترة من الزمن". [5].

1.5. خصائص نظم الفوضى

يمكن تصنيف حركة ما بأنها فوضوية، إذا أبدت الخواص الآتية: [12]

- الحساسية للشروط الابتدائية (Initial Conditions): وتعني أنه عند إعطاء قيمة ابتدائية لنظام معين فمن المعروف أنه يمكن توقع الحالة المستقبلية له، إلا أنه في أنظمة الفوضى فإن توقع المدى البعيد يستحيل التنبؤ به.

- قابلية التحويل (Transitive): وتعني أنه يمكن تطبيق تابع التحويل على أي فترة زمنية، بحيث يقوم بمطابقتها مع فترة زمنية أخرى.
- المسارات الدورية المتراصة (Periodic Orbits): ويطلق عليها أيضا **Ergodicity** وهي ميزة أنظمة الاحتمالية للمتغيرات العشوائية، أي أن النظام يعمل باستقلالية كما أنه يكون بشكل محدد ومستقل عن الظروف الابتدائية، ويفتقر إلى إمكانية التكهّن به، وله مسارات دورية متراصة مع بعضها، كما أن كثافة القيم ثابتة في وقت محدد، وهذه الخاصية ضرورية في مجال التشفير والإخفاء.
- ميزة الدمج أو الخلط (Mixing): وهي ميزة الأنظمة التي يكون الانتشار في الفضاء ضمن فترة قصيرة بفصل زمني صغير من الشرط الابتدائي، حيث أنه في الأنظمة الفوضوية تكون هذه الفترة غير محددة بشرط، ولكن عملها يكون بشكل اعتباطي من قيم الشرط الابتدائي، حيث يكون المسير قريبا من الشرط الابتدائي ولكن لا يتقاطع معه أبداً.

2.5. الدوال الفوضوية

يوجد العديد من الدوال الفوضوية، منها: Logistic Equation، Rossler Equation، Lorenz Equation. النوعين الأول والثاني (على التوالي)، تستخدمان في الأنظمة الفوضوية ثلاثية البعد، أما الدالة اللوجستية "Logistic function"، فهي من أنواع الدوال الفوضوية المعروفة (وهي الدالة المستخدمة في هذا البحث)، وقد تم دراستها لأول مرة عام 1960 عندما لوحظ اهتمام الكثير بخصائصها. إذ أن القيم المحددة التي تنشأها هذه الدالة، هي قيم عشوائية تماما في صيغتها، على الرغم من أنها تكون بين حدود، وهذه القيم لا تتكرر حتى بعد عدد من الدورات، واهم صفة لهذه الدالة هي حساسيتها للقيمة الابتدائية.

الأبحاث التي أجريت على الأنظمة الديناميكية للفوضى تدل على أن الدالة اللوجستية تقف في حالة من الفوضى عندما تكون $3.5699456 < \mu \leq 4$ والأرقام التي تولدها هذه الدالة تكون غير دورية وغير متقاربة مما جعلها ذات أهمية عالية في مجال التشفير والإخفاء. أما التمثيل الرياضي للدالة فهو:

$$x_{n+1} = \lambda x_n (1 - x_n) \quad (1)$$

حيث أن قيمة x_n تتراوح بين (1,0) وهو الجيل المتوقع، وقيمة المتغير (λ) هي قيمة موجبة تحدد السلوك العشوائي للجيل التالي، أما بالنسبة لقيمة x_0 فتمثل القيمة الابتدائية، والشكل (2) يوضح الرسم البياني التشعبي لسلوك الدالة اللوجستية [4],[12].

شكل (2) الرسم البياني التشعبي للدالة اللوجستية

6. الشبكات العصبية الاصطناعية

يمكن تصنيف الشبكات العصبية إلى نوعين [2] [10] [11]:-

1.6. الشبكات ذات التغذية الأمامية

وفيها يكون اتجاه انتشار الإشارات الداخلة في الشبكة إلى الأمام دائما، وبذلك فإن الإشارة الخارجة من أي خلية تعتمد على الإشارات الداخلة فقط. انظر الشكل (3).

2.6. الشبكات ذات التغذية الخلفية

من الممكن في هذه الشبكات أن يعاد تغذية (كل أو بعض)، الإشارات الخارجة من الشبكة وتحويل اتجاهها لتصبح إشارة داخلة أيضا (إعادة تغذية). وبذلك فإن الإشارة الخارجة من أي خلية، سوف تعتمد على الإشارات الداخلة إليها، فضلا عن الإشارات الخارجة منها في وقت سابق. انظر الشكل (4).

شكل (4) الشبكة العصبية الإرجاعية

شكل (3) الشبكة العصبية الأمامية

إن وحدات المعالجة في الشبكات الأمامية يتم اتصالها بحيث تتدفق باتجاه واحد، وذلك من خلايا الإدخال إلى خلايا الإخراج. أما الشبكات الإرجاعية فتحتوي على وصلات بالاتجاه الأمامي والخلفي. يمكن استخدام الشبكات الأمامية في نمذجة الأنظمة الديناميكية ولكن هذه الشبكات لا تملك ذاكرة ديناميكية، لذلك فهي تستعين بطريقة خطوط التأخير، لإعطاء خاصية نمذجة النظام الديناميكي، مثل هذه الشبكات شبكة الانتشار العكسي **Back propagation** التي تم استخدامها في هذا البحث.

7. الخوارزمية المقترحة

إن المرسل والمستلم سينفقان مسبقا على القيم الابتدائية (μ , X_0) لخوارزمية الفوضى، المستخدمة في عمليتي تدريب الشبكة العصبية والإخفاء داخل الصورة، وذلك عن طريق قناة مخفية ذات سرية جيدة. وإن الخوارزمية المقترحة تتكون من مرحلتين:

المرحلة الأولى: الخوارزمية المقترحة للوثوقية في جهة المرسل وستنفذ كالآتي:

الإدخالات: الصورة الغطاء المستخدمة للإخفاء، والنص السري المطلوب إخفاءه.

- الخطوة (1):** قراءة الصورة الغطاء (Cover)، والنص السري (S).
- الخطوة (2):** تحويل النص السري (S) إلى أرقام بالنظام السداسي عشر (S').
- الخطوة (3):** تكوين رقمين عشوائيين (Chaotic_Train) مفتاح التشفير والتدريب للشبكة العصبية
- Chaotic_Hide**، مفتاح الإخفاء في الصورة) لكل نص مقروء عن طريق تطبيق المعادلة الفوضوية (1).
- الخطوة (4):** إدخال الرقم السري (S') الناتج من الخطوة (2) ك INPUT على الشبكة العصبية لغرض التدريب
- TRAIN مع تحديد الهدف للشبكة TARGET الناتج من الخطوة (3) Chaotic_Train، للحصول
- على الأوزان النهائية (S'').
- الخطوة (5):** تشفير الأوزان النهائية (S''') باستخدام المعادلة الآتية :
- (2) $S''' = S'' \oplus \text{Chaotic_Train}$
- الخطوة (6):** تكرار الخطوات السابقة (من 1 إلى 5) على أكثر من شخص مخول وتكوين قاعدة بيانات خاصة للنظام Create Database CNNFA تكون معلومة بين جهة الإرسال والاستلام.
- الخطوة (7):** إدخال النص السري (S) الناتج من الخطوة (1) والأوزان النهائي (S'') الناتج من الخطوة (4) والأوزان النهائي المشفر (S''') الناتج من الخطوة (5) إلى قاعدة البيانات CNNFA.
- الخطوة (8):** استخدام طريقة إخفاء ابدالية Substitute مقترحه (تعتمد على عملية XOR تتم بين الوزن النهائي للشبكة العصبية ورقم ال Chaotic_Train الناتج من الدالة الفوضوية) لإخفاء الوزن النهائي المشفر (S''') في الجزء LL و HH من الصورة الغطاء والذي يطابق رقم ال Chaotic_Hide بعد تجزئته إلى جزأين الأول LL والثاني HH، للحصول على الصورة بعد الإخفاء (Stego Image)، وعرضها.
- لاحظ الشكل (5).
- المخرجات:** الصورة النهائية بعد إخفاء النص السري داخلها.
- المرحلة الثانية:** خوارزمية الاسترجاع المقترحة للوثوقية في جهة المستلم ستنفذ كالآتي:
- المدخلات:** الصورة بعد إخفاء النص السري داخلها.
- الخطوة (1):** قراءة الصورة بعد الإخفاء (Stego Image).
- الخطوة (2) :** تكوين رقمين عشوائيين (Chaotic_Train , Chaotic_Hide) عن طريق تطبيق المعادلة الفوضوية وباعتماد على قيم (X_0 , μ) المتفق عليها مسبقاً، وذلك للحصول على المواقع العشوائية التي استخدمت في الإخفاء عن طريق Chaotic_Hide.
- الخطوة (3):** استرجاع الوزن النهائي المشفر (S''') من الجزء LL و HH من الصورة الغطاء والذي يطابق موقع رقم ال Chaotic_Hide.
- الخطوة (4):** استخدام Chaotic_Train للحصول على الأوزان النهائية (S'') باستخدام المعادلة الآتية:
- (3) $S'' = S''' \oplus \text{Chaotic_Train}$
- الخطوة (5):** إدخال الأوزان النهائية الناتجة من الخطوة (4) على الشبكة العصبية لغرض الاختبار TEST مع تحديد الهدف للشبكة Target الناتج من الخطوة (2) Chaotic_Train والإدخال INPUT، للحصول على الهدف TARGET والأوزان النهائية الناتجة من التدريب.
- الخطوة (6):** فتح قاعدة البيانات CNNFA والاستعلام عن معلومات الأوزان (S'') الناتج من الخطوة (5) للحصول على النص السري (S) وكافة معلوماته.
- الخطوة (7):** عرض النص السري. لاحظ الشكل (6).

المخرجات: الصورة الغطاء التي استخدمت للإخفاء والنص السري المخفي المطلوب.

الشكل (5) المخطط الانسيابي لخوارزمية الإخفاء المقترحة

الشكل (6) المخطط الانسيابي لخوارزمية الإخفاء المقترحة

8- مثال تطبيقي

تم في هذا البحث تصميم وتنفيذ برنامج على وفق عدة مراحل، يتم فيها تشفير وإخفاء النص، ومن ثم استرجاع وفك شفرة النص؛ والجدول (1) الآتي يمثل الجدول الرئيس في قاعدة البيانات التي يتم الاعتماد عليها لتحديد وثوقية الشخص المعني:

الجدول (1) CNNFA Table الجدول الرئيس في قاعدة البيانات

User_Name	Weight	Encrypt_Weight
Ammar	0.0138	8362

Ali	0.2139	3466
Suha	0.6758	7857
Muna	0.5676	4367
Luma	0.7865	7693
...	...	...

1.8. مرحلة التشفير Encrypt

وفيها يتم قراءة وتشفير النص السري المراد إخفاؤه، حيث يتم أولاً تحويل النص إلى أرقام بالنظام السادس عشر بعد قراءته، مثلاً الإدخال هو كلمة: Ammar، يكون (114 97 109 109 65)، يتم بعد ذلك تطبيق المعادلة الفوضوية على مرحلتين لتكوين رقمين عشوائيين، الأول لتدريب الشبكة العصبية والتشفير Chaotic_Train=0.5280 والثاني للإخفاء داخل الصورة Chaotic_Hide = 0.8224، ولقد تم استخدام $\mu=3,3$ و $X_0=0,2$ كقيم ابتدائية للدالة اللوجستية.

يتم بعد ذلك استدعاء الشبكة العصبية وتدريبها (تم تدريبها لـ 20000 مرة في مثالنا) على قيم الإدخال للنص المطلوب (114 97 109 109 65) كـ INPUT وتحديد الهدف (TARGET=0.5280) للحصول على الوزن النهائي (في مثالنا كان الوزن النهائي هو (0.0138)).

يتم بعد ذلك تطبيق خوارزمية تشفير بسيطة لزيادة السرية العملية من خلال استخدام دالة XOR بين الوزن النهائي والرقم العشوائي الخاص بالإخفاء Chaotic_Hide، للحصول على الوزن النهائي المشفر؛ بعد إلغاء الفارزة العشرية وتجزئة الرقم الناتج إلى رقمين كل منهما بمرتبتين عشريتين ثم تحويل الرقم الناتج إلى النظام الثنائي وتطبيق الدالة XOR ثم إرجاع الرقم الناتج إلى النظام العشري. وكما موضح بالشكل (7) الآتي:

Weight = 0.0138	→ 0138	→ 01 38	→ 0 0 0 0 0 0 1	0 1 0 0 1 1 0
Target = 0.5280	→ 5280	→ 52 80	→ 1 0 1 0 0 1 0	0 0 1 1 0 0 0
Weight XOR Target = 1 0 1 0 0 1 1 0 1 1 1 1 1 0				
Encrypt Weight = 83 62				

شكل (7) عملية تشفير الوزن النهائي للشبكة العصبية

يتم تكوين قاعدة البيانات CNNFA ثم خزن القيم (النص الأصلي، والوزن النهائي، والوزن النهائي المشفر)

```
CREATE USER CNNFA_SYS IDENTIFIED BY CNNFA
CREATE TABLE CNNFA(USER_NAME VARCHAR2(15),
WEIGHT NUMBER(15,6), ENCRYPT_WEIGHT NUMBER(15,6));
INSERT INTO CNNFA VALUES('AMMAR',0.0138,8362);
```

داخلها، وذلك باستخدام الدوال الآتية:

2.8. مرحلة الإخفاء Hide

في هذه المرحلة سيتم إخفاء الوزن النهائي المشفر في داخل الصورة، وذلك باستخدام طريقة إخفاء ابدالية Substitute مقترحة، حيث يتم أولاً قراءة الصورة الغطاء والتي يكون نوعها BMP أو JPG أو JPEG، وبأبعاد مختلفة. لاحظ الشكل (8).

شكل (8) الصورة المراد استخدامها للإخفاء

في هذه المرحلة سوف يتم استخدام الرقم العشوائي الثاني الناتج من الدالة الفوضوية والمسمى Chaotic_Hide، فنقوم بإلغاء الفارزة العشرية وتجزئة الرقم الناتج إلى رقمين كل منهما بمرتبتين عشريتين وكما يأتي:

$$\text{Chaotic_Hide} = 0.8224 \rightarrow 8224 \rightarrow 82 \ 24$$

$$\text{Encrypt Weight} = 83 \ 62$$

وعلى أساس هذه القيمة، سيتم إخفاء أول رقم من الوزن النهائي المشفر (83) في الموقع (82)، والرقم الثاني (62) في الموقع (24) ضمن الصورة الغطاء. ثم عرض الصورة النهائية بعد الإخفاء، وكما في الشكل (9).

شكل (9) الصورة بعد الإخفاء

من خلال ملاحظة الصورة الناتجة بعد الإخفاء وبعد إجراء المقاييس (BER, PSNR, MSE) نلاحظ عدم ظهور أي تشوهات مرئية، وأن نسبة الخطأ ومربع الخطأ كانت قليلة جداً، بينما كانت قيمة PSNR جيدة. أي أن الصورة مقاربة جداً للصورة الأصلية ويمكن قراءة قيم المقاييس حسب الجدول (2) الآتي:

الجدول (2) نتائج مقاييس الكفاءة

ت	اسم الصورة	MSE	PSNR	BER
1	Flower1. Jpg	0.019	61.821	0
2	Flower2.bmp	0.012	65.876	0
3	Flower3. Jpg	0.018	62.433	0
4	Flower4.bmp	0.009	69.543	0
5	Flower5.Jpg	0.006	63.611	0
6	Flower6.bmp	0.009	64.633	0
7	Flower7.jpeg	0.011	64.532	0
8	Flower8.jpeg	0.022	66.321	0
9	Flower9.jpg	0.021	63.769	0
10	Flower10.jpg	0.017	62.765	0

حيث أن:

• **Mean Square Error(MSE)**: وتحسب من القانون التالي:

$$MSE=1/(N*M)* \sum_{i=1}^n \sum_{j=1}^n (C(i,j)-S(i,j)) \dots\dots\dots(4)$$

علما أن: M, N: تمثلان أبعاد الصورة, C: تمثل الصورة الغطاء, S: تمثل الصورة بعد الإخفاء.

• **Peak Signal to Noise Ratio(PSNR)**: تقيس مقدار التشوه بين الصورة الأصلية (الغطاء)

والصورة الناتجة بعد الإخفاء، وتحسب من القانون الآتي:

$$PSNR=10\log_{10}[C_{max}^2 / MSE](in \text{ db}) \dots\dots\dots(5)$$

علما أن: Cmax هي أعلى قيمة لونية في الصورة.

• **BER**: $BER=(\text{no. of wrong bit}/\text{no. of original bit})*100 \dots\dots\dots(6)$

3.8. مرحلة الاسترجاع Retrieve

في هذه المرحلة سيتم استرجاع النص السري (المشفر فوضوياً) باستخدام الدالة الفوضوية والشبكة العصبية، حيث يتم أولاً قراءة الصورة بعد الإخفاء (Stego) لاحظ الشكل (8)، بعد ذلك يتم استخدام الدالة الفوضوية اللوجستية حسب المعلومات المتفق عليها مسبقاً لكل من $\mu, X0$ لتطبيق الدالة اللوجستية للحصول على نفس الأرقام العشوائية $Chaotic_Train = 0.5280$ $Chaotic_Hide = 0.8224$.

ثم نقوم باستخدام Chaotic_Hide لمعرفة مواقع خزن الوزن النهائي المشفر داخل الصورة، فيتم إيجاد الرقمين (83) و(62) التابعين للوزن النهائي المشفر في الموقع الأول (82) والثاني (24) لرقم الإخفاء، ليكون الوزن النهائي المشفر هو (62 83).

ثم بعد ذلك استرجاع الوزن النهائي من خلال تحويل الوزن النهائي المشفر إلى النظام الثنائي، وكذلك تحويل الرقم العشوائي الخاص بالتدريب إلى النظام الثنائي وتنفيذ دالة XOR بينهما، وكما موضح بالشكل(10):

$$\begin{aligned} \text{Encrypt Weight} &= 83 \ 62 = 1 \ 0 \ 1 \ 0 \ 0 \ 1 \ 1 \ 0 \ 1 \ 1 \ 1 \ 1 \ 1 \ 0 \\ \text{Target} &= 0.5280 \rightarrow 5280 \rightarrow 52 \ 80 \rightarrow 1 \ 0 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 1 \ 1 \ 0 \ 0 \ 0 \\ \text{Encrypt Weight XOR Target} &= 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 1 \ 0 \ 0 \ 1 \ 1 \ 0 \\ \text{Weight} &= 0.0138 \leftarrow 0138 \leftarrow 01 \quad 38 \end{aligned}$$

شكل (10) عملية تشفير الوزن النهائي للشبكة العصبية

بعد ذلك يتم إدخال الوزن النهائي مع مجموعة من الإدخالات INPUTs والهدف TARGET على الشبكة العصبية لغرض الاختبار TEST، في حالة تطابق الوزن الناتج مع الإدخال المعني في قاعدة البيانات فان الشخص موثوق أما خلافه فان الشخص غير موثوق. وكالاتي:

SELECT * FROM CNNFA WHERE WEIGHT = 0.0138;

9. الاستنتاجات والأعمال المستقبلية

9.1. الاستنتاجات:

- من خلال تطبيق خطوات الخوارزمية المقترحة تم التوصل إلى ما يأتي :-
1. أثبتت النتائج قوة وكفاءة الطريقة المقترحة مقارنة مع طرائق تقليدية أخرى.
2. أدى استخدام التشفير الفوضوي مع الإخفاء الفوضوي إلى زيادة قوة وسرية الطريقة المقترحة مقارنة مع طرائق تشفير أخرى.
3. من خلال النتائج التجريبية، تبين أن استخدام التشفير والإخفاء لا يؤدي إلى تحطيم الصورة الغطاء من خلال التماثل الكبير بين الصورة قبل وبعد الإخفاء وكما هو ناتج في المقاييس.
4. استرجاع النص السري بنسبة تطابق 100% وهذا ما تم قياسه باستخدام BER.
5. كان للفوضى الأثر الكبير في زيادة سرية الطريقة المقترحة، وذلك من خلال حساسيتها للقيمة الابتدائية لدالة الفوضى المستخدمة (الدالة اللوجستية).
6. كان للفوضى والشبكة العصبية أثر واضح وفعال في الخوارزمية المقترحة إذ أعطت فوضوية في اختيار الهدف للشبكة العصبية وفوضوية أخرى في اختيار مواقع الإخفاء في الصورة الغطاء، بينما أعطت قاعدة البيانات سرعة وسهولة في التعرف على وثوقية الشخص المعني من خلال الاستعلام.
7. من خلال النتائج التي تم الحصول عليها وقيم PSNR و MSE و BER في هذا البحث والموضحة بالجدول (2)، وبعد ملاحظة العمل المذكور في المصدر [5] ومن خلال مقارنة ومناقشة عمله الذي اعتمد على المقاييس الحيوية مع الدوال الفوضوية في قياس الأمانة يتضح أن عمل هذا البحث أكثر كفاءة وهذا ما دل عليه جدول (2) فضلا عن أن استخدام الدالة الفوضوية مع الشبكات العصبية وقواعد البيانات يزيد

من كفاءة وسرية الطريقة لكون هناك نوع هجين من البيانات التي تستخدم في التشفير والإخفاء أفضل من كون نوع واحد (المقياس الحيوي) الذي يعتمد عليه العمل.

9.2. الأعمال المستقبلية

1. استخدام الشبكات العصبية التنافسية مثل SOM و Radial Basis.
2. استخدام دوال فوضوية أخرى مثل دالة Lorenzo.
3. تطوير الخوارزمية بحيث تشمل النصوص والمقاطع الفيديوية.
4. استخدام طرائق إخفاء أخرى مثل تضمين العلامة المائية.

المصادر

- [1] حمدي, محمد عبدالرحيم, ذنون, كرم حاتم, (2009), "تشخيص مرض التدرن الرؤي باستخدام الشبكات العصبية الاصطناعية", مجلة الرافيدين لعلوم الحاسوب والرياضيات المجلد (6) العدد (1).
- [2] Fawziya M. Ramo, Ramadan M. Ramo, (2011), "Face Detection using Neural Networks", College of Computer Science and Mathematics, Computer Science Department, University of Mosul.
- [3] عبدالله, سعدون حسين, (2012), "تسلسلات DNA وسطا لإخفاء المعلومات", رسالة ماجستير, قسم علوم الحاسوب, كلية علوم الحاسوب والرياضيات, جامعة الموصل.
- [4] Kaur H.,Singh T. P., (2011), " Cryptography Using Chaotic Neural Network", International Journal Of Information Technology And Knowledge Management July-December 2011, Volume 4, No. 2, Pp. 417-422.
- [5] القدو, سجي جاسم, سعيد, ميلاد جادر, عبد المجيد , إيلاف أسامة, (2010), "التشفير الفوضوي باستخدام مفتاح المقياس الحيوي", مجلة الرافيدين لعلوم الحاسوب والرياضيات المجلد (7) العدد(3).
- [6] Kwong K. M., (2010)," LIDAR and Chaotic Oscillatory-based Neural Network for Wind Shear Forecasting", Hong Kong Polytechnic University, Hong Kong, China.
- [7] Dalkiran I., Danisman K.,(2010), " Artificial Neural Network Based Chaotic Generator For Cryptology", Department Of Electrical Engineering, Faculty Of Engineering Erciyes University,38039, Kayseri-Turkey.
- [8] Bhardwaj S., Smriti S., Gupta J., (2012), " Chaotic Time Series Prediction Using Combination of Hidden Markov Model and Neural Nets", Netaji Subhas Institute Of Technology, Delhi University, New Delhi, India, 110078.
- [9] برزنجي, فوزي, (2008), "إخفاء البيانات داخل صورة", جامعة السليمانية, العراق.
- [10] Gavrilova M., Ahmadian K.,(2010), "On-demand chaotic neural network for broadcast scheduling problem",Springer Science+Businrss Media,LLC/IVSL.
- [11] Li Y., Xia D., Deng S., (2011)," Improvement and performance analysis of hash function based on chaotic neural network", Springer-Verlag London Limiter/IVSL.
- [12] Bigddi N., Farid Y.,Afshar K.,(2012)," A novel image encryption/decryption scheme based on chaotic neural networks", EE Department, Imam Khomeini International University, Iran,IVSL
- [13] <http://dx.doi.org.tiger.sempertool.dk/10.1016/j.engappai.2012.01.007>