تهجين الخوارزمية الجينية مع الشبكات العصبية في تشفير النصوص الإنكليزية

رضوان يوسف الجوادي
ماجستر علوم حاسبات
الكلية التقنية / الموصل

رائد رافع النعمة
مدرس مساعد
الكلية التقنية/قسم هندسة تقنيات الحاسبات

الخلاصة

يهدف هذا البحث في جزءه الاول الى بناء نظام للتشفير عن طريق اسـتخدام الخوارزميـة الجينـة المهجنة مع الشبكات العصبية ذات الطبقة الواحدة لحماية البيانات ضد الكثير من المخاطر التي تتعرض لهـا اثناء نقل البيانات . اذ اعتبرت الحروف مدخلات للشبكة وتحديد اعداد عشوائية لكل حرف تمثل شفرة الحرف وتم تدريب الشبكة العصبية وتعديل الاوزان بواسطة الخوارزمية الجينية ، واعتبرت هذه الاوزان هي مفتـاح التشفير لدى الطرفين .

اما الجزء الثاني فقد تم فك الشفرة عن طريق عكس استخدام الشبكة العـصبية الجينيـة لاسـترجاع البيانات المشفرة. حيث استخدام معكوس مصفوفة اوزان الشبكة كمفتاح لفك الشفرة .

لقد تم استخدام فكرة التشفير الانسيابي (Stream Cipher) لغرض تغذية مداخل الشبكة في مرحلـة التشفير ، وقد نجحت هذه الطريقة في تشفير وفك تشفير البيانات بدقة وصلت الى ١٠٠% . وقد تم اسـتخدام برنامج MATLAB في بناء النظام .

Hybrid Genetic Algorithm with Neural network in English Language Cipher

Radwan yousif S. Al-jawadi MSC Computer science Technical college / Mosul	Raid R. Al-nima Lecturer Assistant Technical Colleges/ Mosul

E-mail : radwanyousif@yahoo.com

Abstract

This research aims in the first stage to built a cipher system using hybrid Genetic Algorithm with single layer Neural network to prevent any data attack during the transition process , where the ASCII of the letters are used as inputs to the network and the random numbers are used as outputs to the network , then the weights will be constructed after the network training .

In the second stage a decipher process is used to restore the ciphered data by using the inverse of the genetic neural network , where the inverse of weights is used as a key for the decryption process .

Stream cipher method is used to input the data in the network during the ciphering stage. This suggested technique attained 100% success.

All the ciphering and deciphering processes are built under MATLAB ver.(7) .

١- المقدمة

شهد العالم في الآونة الأخيرة تطورا كبيرا في تكنولوجيا المعلومات والاتصالات وقـد دخـل علـم الحاسوب في كافة مجالات الحياة ومنها مجال إرسال واستقبال المعلومات التي تزداد أهميتها بشكل هائـل ، فالمعلومات ترسل وتعالج بشكل آلي، وهذا يتطلب الحرص على الخزن السري للبيانات المراد إرسـالها ، اذ يوجد العديد من الأسباب لحماية المعلومات من التطفل منها أهمية المعلومة نفسها وحماية الاقتصاد وغيرها .

اما علم التشفير (Cryptography) فهو العلم الذي يعنى بالطرق التي تجهزنـا بحمايـة وخـزن المعلومات ونقلها في مجال واسع ، وهذه الطرق تعتمد على مفتاح سري يستخدم لتشفير البيانات [١] .

هنالك العديد من البحوث في هذا المجال منها: في عام (٢٠٠٠) استخدم نظام حماية هجين وطبقـه على النصوص ، حيث تضمن البحث استخدام تقنيات التشفير والإخفاء والكبس للبيانـات النـصية واعتمـد الترتيب الأتي: كبس ملف الغطاء وثم تشفير النص المراد إرساله وثم إخفـاءه ضـمن الغطـاء ، واسـتخدم خوارزمية الكبس (LZ77) لصورة نوع BMP ، خوارزمية التشفير (RSA) وثم إخفاء الشفرة في الصورة [١] . وفي عام (٢٠٠٣) صمم نظام للتشفير ثم تم استخدام الشبكات العصبية الاصطناعية في مهاجمة عمليـة التشفير ، وقد تضمن تنفيذ خوارزمية تشفير البيانات القياسية (RSA) وتحليل الـشفرة باسـتخدام الـشبكات العصبية [٢] . أما في عام (٢٠٠٨) فقد استخدمت شبكة (Hebbian) في التشفير واعتمـد فكـرة التـشفير الانسيابي (Stream Cipher) دون استخدام القواعد المحددة لطريقة التشفير ، اذ تم تغذية شبكة (Hebbian) بإدخالات النص المراد تشفيره واعتبار الاخراجات هي النص المشفر . اما أوزان الشبكة فقد اعتبرت مفتـاح التشفير وفك الشفرة [٣] . وقد ذكر في هذا المصدر: اسـتحالة تهجـين الخوارزميـة الجينيـة مـع شـبكة (Hebbian) لصعوبة ايجاد معادلة دالة اللياقة (Fitness value) [٣] . ومن هنا جاءت فكرة هذا البحث .

يهدف هذا البحث إلى بناء نظام تشفير هجين لتأمين سرية تداول البيانـات حيـث يطبـق مبـادئ تكنولوجيا المعلومات فى تشفير البيانات وفك الشفرة مستخدماً اسلوب يدمج بين الخوارزمية الجينية والشبكات العصبية في تشفير البيانات . حيث يتيح لراسل البيانات التأكد من أن البيانات ستصل فقط للـشخص المـراد إرسالها إليه وبالطريقة الصحيحة وبطريق لا يستطيع أحد فك شفراتها إلا الشخص المستقبل .

٢- علم التشفير (Cryptography)

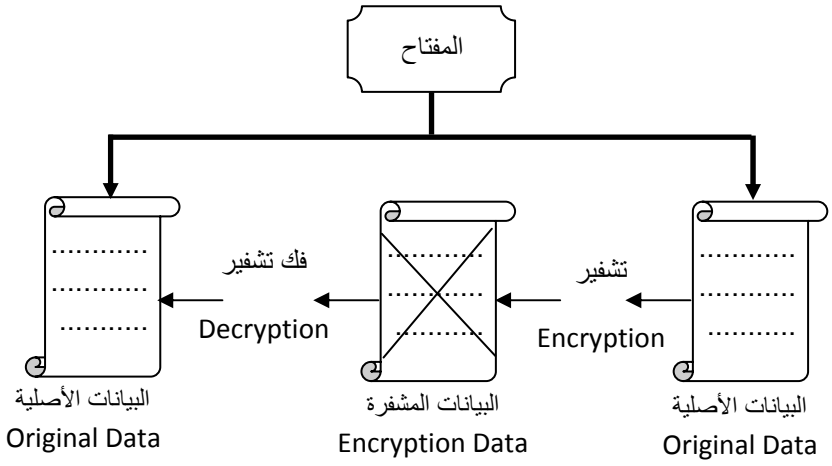
يعرف علم التشفير بأنه عملية تحويل المعلومات الى شفرات غير مفهومة ، لمنع الأشـخاص غيـر المرخص لهم من الاطلاع على المعلومات او فهمها ، ولهذا تنطوي عملية التشفير الى تحويـل النـصوص العادية الى نصوص مشفرة [٣] . وهو الذي يسمح أيضا للمستخدم بالتغيير الجذري للمعلومات لغرض اخفاء محتواها عن طرف ثالث ، ويسمح لمستخدمي شبكات الاتصالات التعامل معها بثقة [١] .

استخدم الإنسان التشفير منذ حوالي الفي عام قبل الميلاد لحماية رسائله السرية ، وبلغ ذروتـه فـي فترات الحروب خوفا من وقوع الرسائل الحساسة في أيدي العدو ، وقام يوليوس قيصر بتطوير خوارزميتـه المعروفة باسم شفرة قيصر (Caeasar Cipher) التي كانت عبارة عن نصا مشفرا (Cipher text) ، لتأمين اتصالاته ومراسلاته مع قادة جيوشه [٣] .

والهدف من التشفير هو ضمان حفظ المعلومات السرية الخاصة ، ولايمكن لاحد ان يفهم مـضمون هذه المعلومات او الرسائل الا من لديه المفتاح البرمجي السري الخاص بها والتي تتم عن طريقه عملية كسر الشفرة (Decryption) اي اعادة البيانات الى صيغتها الاصلية [٣] .

يقسم التشفير بصورة عامة الى طريقتين رئيسيتين هما : -

١ . انظمة التشفير المتماثلة (Symmetric cipher system) والتي تمتاز باستخدامها المفتاح نفسه في جهة الإرسال والاستقبال، وهذا النوع من الانظمة يدعى بنظام تشفير المفتاح الخاص (Private key) او المفتـاح السري (Secret key)، هذا النوع من الخوارزميات يكون سريعا مناسبا لاحظ الـشكل (١)، ومـن اشـهر الخوارزميات المتماثلـة المعروفـة خوارزميـة تـشفير البيانـات القياسـية DES(Data Encryption standard)عام ١٩٧٧، وتستخدم مفتاحا للتشفير يتكون من ٥٦ رقما ثنائيا ،وبسبب كسرها فقد طورت الـى خوارزمية تشفير البيانات العالمية (IDEA)(International Data Encryption Algorithm) والتي تعد من الخوارزميات الاسرع والاكثر سرية اذ تستخدم مفتاحا يتكون من ١٢٨ رقما ثنائيا[١] . وتنقسم انظمـة التشفير المتماثلة الى نوعين هما النوع التقليدي (Classical) الـذي يتـضمن الطـرق الابداليـة والطـرق التعويضية في الحروف . والنوع الثاني وهو الحديث(modern) والتي ينقسم الـى نـوعين همـا التـشفير الانسيابي(Stream Cipher) والتشفير الكتلي (Block Cipher) [١ ، ٣] . تعتمد فكرة التشفير الانـسيابي بتشفير النص حرف بعد حرف (X0,X1,…..,Xn)، وذلك بعد تحويل الحروف الى شـفرة الـ (ASCII code) وثم الى (0,1) والذي يتكون من (7-bit) [٤] .



الشكل (١) التشفير باستخدام المفتاح المتماثل (Symmetric Key Encryption)

٢. أنظمة التشفير غير المتماثلة (Asymmetric Cipher Systems) تمتاز هذه الانظمـة بانهـا تـستخدم مفتاحين في التشفير وكسر الشفرة اذ تستخدم المفتاح العام والمفتاح الخاص ومن امثلة هذا النوع خوارزميـة (RSA) [١ ، ٣] .

٣- الخوارزمية الجينية

تعرف الخوارزمية الجينية بأنها خوارزمية ذكية يمكن استخدامها لايجـاد حـل المـسائل المعقـدة وتحسينها ، وتعد الخوارزمية الجينية من طرق البحث الكفوءة المعتمدة على مبادئ الاختيار الطبيعـي وعلـم الوراثة ، ابتكرها العالم هولاند (John Holland) عام (1975) فـي جامعـة ميـشكان (University of Michigan) ، وكان الهدف منها بناء وتحسين العديد من الخوارزميات والبرمجيات والأنظمة [٥] .

يعتمد أسلوب الخوارزمية الجينية في حل المسائل على افكار مستنبطة من علم الوراثة، والتي تهـتم بشكل عام بكيفية انتاج افراد جديدة تمتلك صفات معينة (مرغوبة او غير مرغوبة) وذلك من خلال التـداخل او التعديل او التبديل الذي يحصل على المجموعات الموروثة بهدف تكوين افراد جديدة تختلف فـي صـفاتها عن الآباء [٥] .

تستخدم الخوارزمية الجينية في تطبيقات مختلفة منها: حل المسائل الصعبة في بحوث العمليات والتحليل العددي والامثلية، و استخدمت في حل مسائل التشفير وكسر الشفرة ومعالجة الصور وتطبيقات الشبكات العصبية (ايجاد العدد الأمثل لطبقات الشبكة او الاوزان) ، وكذلك استخدمت لتصميم الأنظمة المختلفة والدوائر الإلكترونية [٥] .

وتتميز الخوارزمية الجينية بعدة مميزات :

- فهي تعطي حلول جديدة عند كل تنفيذ جديد.
- ومبادئ الخوارزمية سهلة الفهم والتطبيق.
- وتجهز عدة حلول مثلى ، او حلول بديلة .
- وتعتبر خوارزمية عامة لحل مختلف انواع المسائل .

٣- الشبكات العصبية

يمكن القول ان تاريخ دراسة الشبكات العصبية الاصطناعية يعود الى عـام ١٩٤٣ ، اذ بنـي اول نموذج لخلية عصبية من قبل العالم (Mcculloh & pitts) ، وكانت عبارة عن خلية بسيطة ثنائية الحالة وقد امكن من خلالها تمثيل الدوال المنطقية ، وفي عام ١٩٤٩ قدم العـالم (Hebb) اول قاعـدة لتعلـيم الـشبكة العصبية اطلق عليها (Hebbian Learning Rule) اعتمدت كقاعدة اساسية لتطوير خوارزميات التعليم [٣] .

تعتبر الشبكات العصبية الاصطناعية هي نظام معالجة المعلومات له مميزات اداء معينة من خـلال اسلوب يحاكي الشبكات العصبية الحيوية [٣] ، لقد طورت الشبكات العصبية كامثلية رياضية معتمـدة علـى طريقة التفكير البشري وكيفية معالجة الاعصاب للمعلومات [٦] .

تنقسم الشبكات العصبية الإصطناعية من حيث التدريب إلى نوعين رئيسيين: الأول هـو التـدريب بمعلم supervised training والثاني هو التدريب بدون معلم unsupervised training [٦] . تم إعتمـاد النوع الأول في هذا البحث .

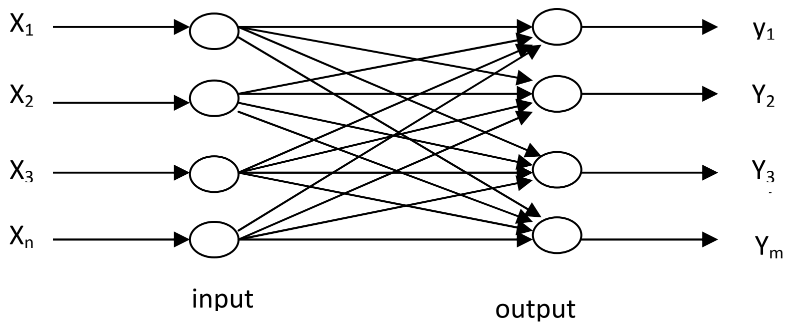
٣-١ شبكة Hebbian

اكتشفت شبكة (Hebbian) من قبل العالم دونالد هيب (Donald Hebb) عام ١٩٤٩ . الهدف من الشبكة هو اعادة تعديل مصفوفة الوزن التي تمثل مصفوفة الارتباط بين العقد .

لقد تم استخدام شبكة (Hebbian) بمعلم (Supervised) في هذا البحث ، اذ تم اعطاء شفرة لكـل حرف ، وتمتاز شبكة (Hebbian) بمعلم بانها تتكون من طبقة واحدة (Single layer)، ان اتجاه تغذية عمل الشبكة يكون إلى الأمام (Feed Forward)، وتمتاز هذه الشبكة بعدم احتواء جسم الخلية على دالة التحفيـز (Activation Function). بينما يحدث التعديل على الوزن (Weight) .

٣-٢ معمارية الشبكة

يبين الشكل (٢) هيكل شبكة (Hebbian) العامة والتي تتكون من طبقـة واحـدة (Single layer) ويتم فيها توضيح الادخالات والاخراجات .



الشكل(٢): مخطط يوضح معمارية شبكة (Hebbian)

لاجل الحصول على الاخراجات في هذه الشبكة العصبية يمكن متابعة المعادلة التالية :

$$Y_j = \sum_{i=1}^{m} X_i W_{ij} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

ولاجل تعديل مصفوفة الوزن فيمكن متابعة المعادلة التالية :

$$W_{ij}(new) = W_{ij}(old) + C X_i Y_j \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2)$$

حيث ان:

X_i: تمثل قيمة الادخال i .

Y_j: تمثل قيمة الاخراج j .

W_{ij}: تمثل قيمة مصفوفة الوزن ij .

C: تمثل معدل التعليم وتتراوح قيمتها بين ($0 < C \leq 1$) .

وقد تم الاستغناء عن معادلة تعديل مصفوفة الوزن والاستعاضة عنها بالخوارزمية الجينية حيث تم حساب مصفوفة الوزن باستخدام الخوارزمية الجينية للوصول الى قيم الاخراجات المطلوبة .

٤- الشبكة العصبية الجينية

إن الخوارزمية الجينية المستخدمة في هذا العمل هي خوارزمية جينية تتعامل مع أوزان الشبكة العصبية للوصول إلى أفضل نتائج وزنية . حيث حورت عملية التدريب التقليدية لشبكة Hebbian العصبية لتتدرب حسب الخوارزمية الجينية وذلك باستخدام الخواص التالية :

١. تتكون الشبكة العصبية من (١٢) عقدة في طبقة الادخال ، و (١٢) عقدة في طبقة الاخراج وبدون اية طبقة خفية ، اذن سوف يكون لدينا مصفوفة اوزان مكونة من (١٤٤) وزن – والتي ستستخدم بعد توليدها على اعتبار أنها كروموسومات - ، تم تدريب مصفوفة الاوزان هذه من خلال خواص التضارب والتبادل والطفرة الموجودة في الخوارزمية الجينية للوصول الى مصفوفة الأوزان الصحيحة التي تؤدي إلى دالة اللياقة (Fitness Function).

٢. إن دالة اللياقة المستخدمة في الخوارزمية الجينية موضحة بالمعادلة التالية رقم (٣) :

$$\delta_k = \sum_{k=1}^{m} |t_k - y_k| \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (3)$$

حيث لكل وحدة اخراج (Y_k, k=1,2,…m) تستلم نمط الهدف (t_k) اعتمادا على نمط التدريب المدخل وذلك لحساب قيمة الخطأ (δ_k) .

٣. استخدمت دالة إختيار الصنف الجيد من نوع (RANK) لكل جيل مولد والذي ساوى (٢٠) فرد لكل جيل ، حيث أن عدد الأفراد هذا قد حقق النتيجة المرجوة منه .

إن دالة (RANK) تعتمد أسلوب جدولة النتائج بحسب رتبة إقترابها من دالة اللياقة (Fitness Function) [٧].

٤. دالة الطفرة (mutation) المستخدمة هي من النوع الناقوسي (Gaussian) لاضافة عدد عشوائي لكل متجه ادخال لكل فرد ، هذه الارقام العشوائية اختيرت من التوزريع الطبيعي حول الصفر [٧]. وقد تم اختيار هذا النوع عوضا عن النوع الثاني وهو الثنائي (binary) لكونه مناسبا للقيم التي اعتمدت في هذا البحث . ومقياس الطفرة المستخدمة هنا يساوي ١,١٥ (لمقياس ناقوسي يتراوح بين ٠–١٠ درجات) حيث أن هذا المقياس كان مناسبا عند التنفيذ والإختبار .

٥. إن عملية التضارب Crossover المستخدمة هي من نوع (Two points) والتي تعتمد مبدأ تبادل الجينات الوراثية إعتمادا على منطقتين عشوائيتين لنفس الجين [٧]. وقد تم اختيار هذا النوع بالتجربة بدلا من (One point) لأن نتائجه كانت أدق ، وكما هو موضح في المثال الآتي:

الجيل الأول (الآباء) :

$$P_1 = [W_1^1 \quad W_2^1 \quad W_3^1 \quad W_4^1 \quad . \quad . \quad . \quad W_{136}^1 - W_{137}^1 \quad W_{138}^1 \quad W_{139}^1 \quad W_{140}^1 \quad W_{141}^1 - W_{142}^1 \quad . \quad . \quad . \quad W_{253}^1 \quad W_{254}^1 \quad W_{255}^1 \quad W_{256}^1]$$

$$P_2 = [W_1^2 \quad W_2^2 \quad W_3^2 \quad W_4^2 \quad . \quad . \quad . \quad W_{136}^2 - W_{137}^2 \quad W_{138}^2 \quad W_{139}^2 \quad W_{140}^2 \quad W_{141}^2 - W_{142}^2 \quad . \quad . \quad . \quad W_{253}^2 \quad W_{254}^2 \quad W_{255}^2 \quad W_{256}^2]$$

الجيل الثاني (الأبناء) :

$$CH_1 = [W_1^1 \quad W_2^1 \quad W_3^1 \quad W_4^1 \quad . \quad . \quad . \quad W_{136}^1 - W_{137}^2 \quad W_{138}^2 \quad W_{139}^2 \quad W_{140}^2 \quad W_{141}^2 - W_{142}^1 \quad . \quad . \quad . \quad W_{253}^1 \quad W_{254}^1 \quad W_{255}^1 \quad W_{256}^1]$$

$$CH_2 = [W_1^2 \quad W_2^2 \quad W_3^2 \quad W_4^2 \quad . \quad . \quad . \quad W_{136}^2 - W_{137}^1 \quad W_{138}^1 \quad W_{139}^1 \quad W_{140}^1 \quad W_{141}^1 - W_{142}^2 \quad . \quad . \quad . \quad W_{253}^2 \quad W_{254}^2 \quad W_{255}^2 \quad W_{256}^2]$$

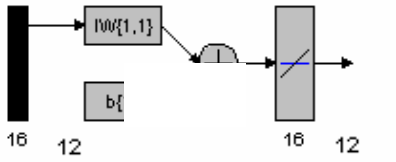
إن مقياس عملية التضارب المستخدمة هنا يساوي ٠,٨ (لمقياس تضارب يتراوح بين ٠-١ درجة).

٥- نظام تشفير البيانات المقترح

ويمكن تمثيل العمل بخوارزميتين :الخوارزمية الاولى هي خطوات تشفير النص المـدخل بتـدريب الشبكة العصبية المهجنة مع الخوارزمية الجينية والحصول على الأوزان ، اما الخوارزميـة الثانيـة : فهـي خطوات فك الشفرة باستخدام معكوس مصفوفة الأوزان التي تم الحصول عليها . حيث اعتبـرت مـصفوفة الاوزان والمكونة من (١٤٤) وزنا مفتاحا للتشفير ومعكوسها (inverse) مفتاحا لفك الشفرة .

لقد تم استخدام شبكة (Hebbian) في التشفير ، ودربت هذه الشبكة عن طريق الخوارزمية الجينية . وتم استخدام الأسلوب الخطي (Linear) لهذه الشبكة في عملية حساب الاخراجات . وكما هـو معلـوم ان هـذه الشبكة لاتحتوي على طبقة خفية (Hidden Layer) مما أدى الى زيادة سرعة التدريب نسبيا .

تم تشفير الحروف بإعطاء شفرة عشوائية لكل حرف كناتج إخراج للشبكة تتكـون مـن ١٢ رقـم عشري، وتم الإعتماد في هذا البحث على الحروف الإنكليزية والتي قيمة الـ ASCII CODE لها تتكون من (12-bit) وهي التي استخدمت كإدخالات للشبكة . إن الأوزان الناتجة من عملية تدريب كـل حـرف لهـذه الشبكة العصبية الجينية قد تم خزنها داخل ملف نوع (xls) . وقد تم استدعاءها ثانية عند عملية فك الـشفرة وذلك بضرب شفرة الحرف بمعكوس مصفوفة أوزانه فرجعت بيانات الحرف التي تم تدريب الشبكة العصبية الجينية عليه (وهي قيمة الـ ASCII CODE لهذا الحرف نفسها) . انظر الشكل (٣) والـذي يبـين شـكل الشبكة التي استخدمت في هذا البحث في برنامج الماتلاب . ونورد فيما يلي الخطوات التفصيلية لخوارزميتي التشفير وفك التشفير .



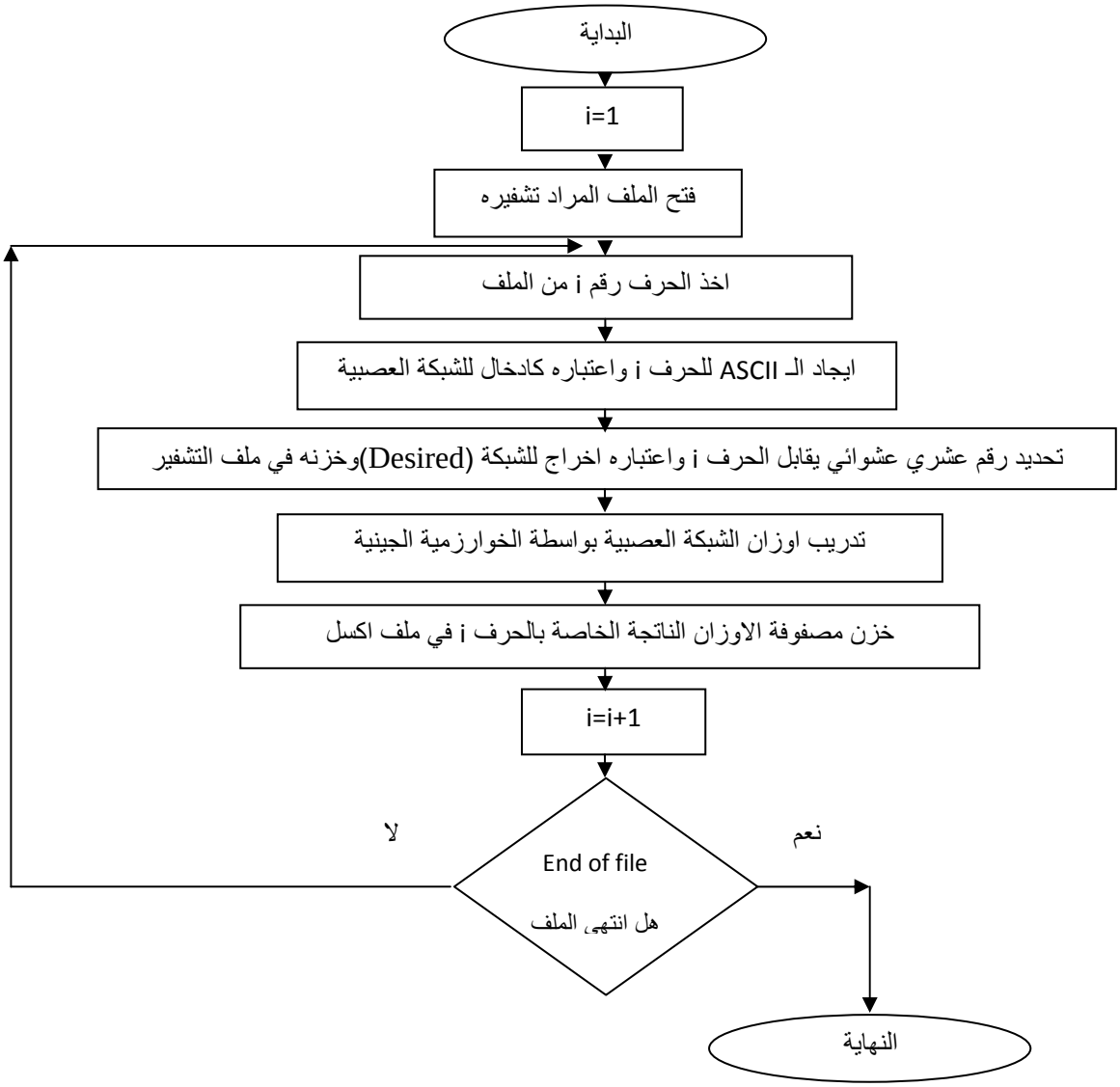
الشكل(٣): شكل الشبكة المستخدمة في برنامج الماتلاب

ان عدد العقد للشبكة المستخدمة في هذا البحث هو عدد قليل مقارنة بالمصدر [٣] الذي استخدم عدد عقد كبير جدا بعدد الـ ASCII CODE لحروف النص المستخدم مما أضفى تعقيدا للشبكة العصبية من حيث زيادة عدد العقد وكمية الأوزان وبالتالي تعقيد للعمليات الحسابية في الشبكة .

٥-١ خوارزمية التشفير

١. تقطيع الملف المراد تشفيره الى حروف .
٢. اخذ الـ ASCII CODE للحرف المراد تشفيره .
٣. تحديد عدد عشوائي لكل حرف مكون من (١٢) رقم عشري ليكون كاخراج للشبكة (Desired output) ، وخزنة في ملف الاخراج (النص المشفر) .
٤. ادخال الـ ASCII CODE للحرف الى الشبكة .
٥. تعديل اوزان الشبكة بواسطة الخوارزمية الجينية للوصول الى للشبكة (Desired output) الخاص بالحرف .
٦. خزن مصفوفة الأوزان الاخيرة والتي تمثل مفتاح تشفير الحرف .
٧. تعاد الخطوات من (٢)- (٦) حتى نهاية الملف .

الشكل (٤) يوضح خطوات خوارزمية التشفير المستخدمة ، وفي الملحق رقم (١) مثال تفصيلي عن تشفير نص .



الشكل (٤) مخطط انسيابي يوضح خوارزمية التشفير

٢-٥ خوارزمية فك الشفرة

تبدا عملية فك الشفرة باستخدام الشبكة العصبية الجينية المقترحة من خلال اعتماد الخوارزمية الآتية :

١. فتح الملف المشفر وتهيئته كادخلات .
٢. تهيئة مصفوفة الوزن الناتجة من الخوارزمية الجينية والتي تمثل مفتاح الحروف واخذ معكوس هذه المصفوفة (إن الأوزان التي لا تناسب شفرة الحرف ستظهر نتائج بعيد عن قيم الـ ASCII CODE) .
٣. حساب اخراجات الشبكة من خلال اعتماد معادلة رقم (٤):

$$X_i = round(Y_j\, W_{ij}^{-1}) \quad ....(٤)$$

حيث ان:

X_i: تمثل قيمة الادخال i.

Y_j: تمثل قيمة الاخراج j.

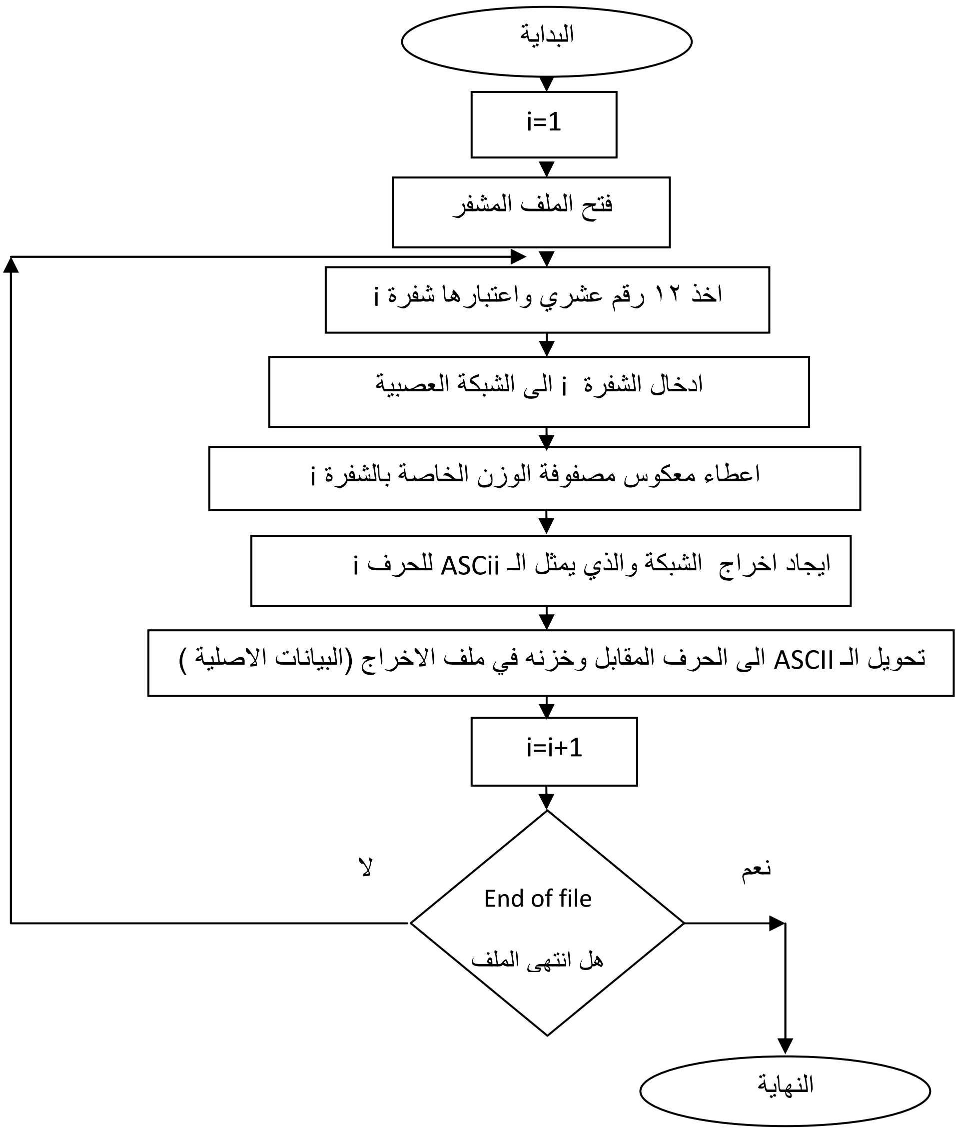
W_{ij}^{-1}: تمثل قيمة معكوس مصفوفة الوزن ij ، المخزنة مسبقا في ملف نوع (xls) .

الدالة (round) تقوم بتقريب الناتج الى اقرب رقم صحيح وهو اما (0) او (1).

٤. مثلت اخراجات الشبكة ١٢ رقم ثنائي (12 -bit) القيم الصريحة للنص الاصلي (ASCII CODE) .

٥. تحويل الـ ASCII CODE الى الحروف المقابلة .

الشكل (5) يوضح آلية عمل خوارزمية فك الشفرة عن طريق مخطط انسيابي، وفي الملحق رقم (٢) مثال تفصيلي عن فك تشفير نص .



الشكل (5) مخطط انسيابي يوضح خوارزمية فك التشفير

٥-٣ الوقت المستغرق لعمليتي التشفير وفك التشفير

تم حساب زمن التشفير للحرف الواحد وكان (31 ms) اما زمن فك الشفرة فقد كان (94 ms) . وكما هو ملاحظ ان زمن فك التشفير أكبر من زمن التشفير وذلك بسبب زيادة حجم النص المشفر عن النص الأصلي وكذلك بسبب العملية الرياضية لحساب معكوس مصفوفة الأوزان . والجدول (١) يبين زمن تنفيذ لملفات ذات أحجام مختلفة .

جدول رقم (١): زمن تنفيذ عمليتي التشفير وفك التشفير لمجموعة ملفات

حجم الملف الأصلي	حجم الملف المشفر	زمن تنفيذ عملية التشفير	زمن تنفيذ عملية فك التشفير	الزمن الكلي لعمليتي التشفير وفك التشفير
35Kbyte	628KByte	713ms	2162ms	2875ms
70Kbyte	1256KByte	1426ms	4324ms	5750ms
105Kbyte	1884KByte	2139ms	6486ms	8625ms

الواضح من الجدول (١) أن زمن التنفيذ يتضاعف بمضاعفة حجم الملف المستخدم والذي يتضاعف بمضاعفة الحروف وذلك لأن لكل حرف شبكة عصبية ثابتة الحجم والخصائص فبمضاعفة عدد الحروف يتضاعف عدد الشبكات العصبية .

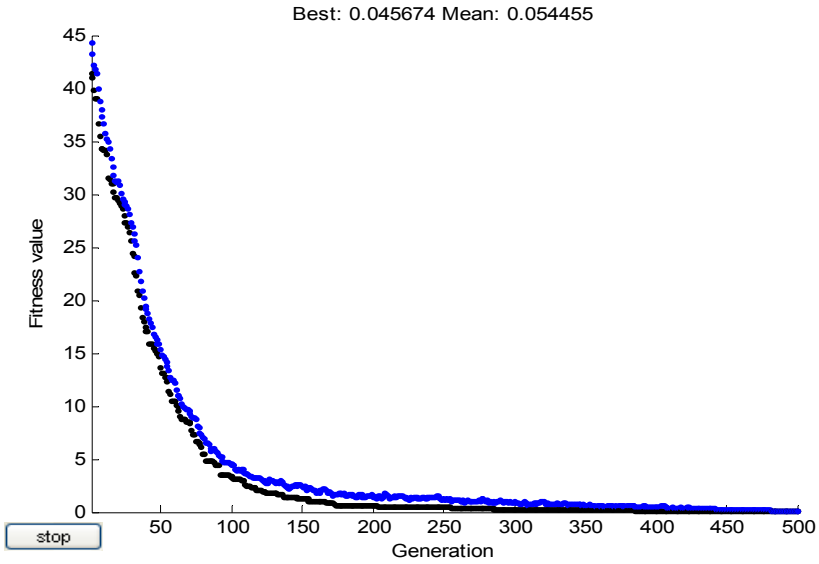
٥-٣ الشبكة العصبية الجينية والشبكة العصبية الإعتيادية

كما ذُكر سابقا بأنه قد تم استخدام شبكة (Hebbian) في عملية التشفير ولكن دربت هـذه الـشبكة حسب الخوارزمية الجينية. فمن المعلوم أن شبكة (Hebbian) هي شبكة عصبية بدائية وبسيطة ولا تحتـوي في خوارزميتها على تكرار إدخال البيانات لحين الحصول على نتائج الأوزان الصحيحة [٦] لهذا فـإن دقـة وصولها لأهدافها ضعيفة، بينما حين تم تهجينها مع الخوارزمية الجينية في عمليـة التـدريب إزدادت دقـة وصولها لأهدافها وحصلت الشبكة على أوزان صحيحة لجميع الإدخالات.

٦- النتائج

١. تم اقتراح شبكة عصبية جينية تقوم بعملية تشفير نصوص، وتحقق ذلك عن طريق تدريب أوزان شبكة عصبية باستخدام الخوارزمية الجينية .
٢. الشبكة العصبية المعتمدة في البحث تكونت من ١٢ عقدة في الإدخال تمثل ASCII CODE الحرف ، والإخراج يتكون كذلك من ١٢ عقدة يمثل أرقام عشرية عشوائية .

٣. دربت الشبكة العصبية باستخدام الخوارزمية الجينية ، حيث تم إعتبار مصفوفة الأوزان الكروموسوم الذي تعتمده الخوارزمية الجينية للحصول على أفضل نتائج .
٤. ان عملية التشفير باستخدام الشبكة العصبية الجينية تتضمن نوعا عاليا من السرية بسبب دقة الخوارزمية الجينية في الوصول إلى معادلة الهدف.
٥. الأوزان الناتجة من عملية تدريب الشبكة العصبية الجينية تكون مشتركة من قبل المرسل والمستلم . حيث استخدمت مصفوفة الأوزان بعملية تشفير ASCII CODE الحرف لمجموعة من الحروف العربية ، واستخدمت معكوس مصفوفة الأوزان بعملية فك الشفرة واسترجاع ASCII CODE الحرف .
٦. الشبكة العصبية الجينية المقترحة حققت نجاحا في عمليتي التشفير وفك التشفير بنسبة وصلت إلى ١٠٠% .
٧. الشكل (6) يبين وصول الخوارزمية الجينية إلى نتائجها في تدريب الشبكة العصبية لأحد الحروف (وهو حرف الـ 'n') مما يدل على نجاح عملية التدريب للحصول على الشفرة .



الشكل (6) نجاح استخدام الخوارزمية الجينية في تدريب الشبكة العصبية لأحد الحروف

المصادر

١. الغريري ، شهد (٢٠٠٣) : "تصميم نظام حماية هجين وتطبيقه على النصوص" ، رسالة ماجستير ، كلية علوم الحاسبات والرياضيات ، جامعة الموصل .
٢. العطيوي ، ريا جاسم عيسى (٢٠٠٠): "استخدام الشبكات العصبية الاصطناعية في مهاجمة التشفير الانسيابي" ، رسالة ماجستير ، كلية علوم الحاسبات والرياضيات ، جامعة الموصل .

٣. بدران ، عامرة استقلال (٢٠٠٩) : "استخدام شبكة (Hebbian) في التشفير "، مجلة الرافدين لعلوم الحاسبات والرياضيات ، كلية علوم الحاسبات والرياضيات ، جامعة الموصل ، المجلد ٦ ، العدد ١ .

4. Alan G. , Computer security & cryptography , Prentice Hall , United States of America 2007 .
http://rapidshare.com/files/107960959/computer-security-and-cryptography.pdf

٥. بشير ، غصون سالم (٢٠٠٣): "استخدام الخوارزمية الجينية في مطابقة الصور"، رسالة ماجستير ، كلية علوم الحاسبات والرياضيات ، جامعة الموصل .

6. L. Fausett, *Fundamental of Neural Networks, Architectures, Algorithms and applications*, Printice Hall Int. Snc., 1994.
7. The Math Works Inc., Genetic Algorithm Toolbox, For Use with MATLAB, Ver. 7.6, 2008, MA, USA.

ملحق (١)

مثال لعملية تشفير مبينة بالتفصيل:

الجدول (٢): مثال لعملية تشفير نص

الجملة المراد تشفيرها	حروف النص الصريح	قيمة الـ ASCII CODE لكل حرف	الرقم العشوائي المقابل لكل حرف (الشفرة)
Technical College in Mosul	'T'	000010000100	746763637891
	'e'	000100000001	372213449107
	'c'	000010011001	008220550027
	'h'	000100000100	868817535961
	'n'	000100010000	425124421273
	'i'	000100000101	450006044938
	'c'	000010011001	008220550027
	'a'	٠٠٠٠١٠٠١٠١١١	372213449107
	'l'	000100001000	105823360909
	' '	٠٠٠٠٠٠١١٠٠١٠	450006044938
	'C'	000001100111	667187261877
	'o'	000100010001	575453752151
	'l'	000100001000	105823360909
	'l'	000100001000	105823360909
	'e'	000100000001	372213449107
	'g'	000100000011	169548725868
	'e'	000100000001	372213449107
	' '	٠٠٠٠٠٠١١٠٠١٠	450006044938
	'i'	000100000101	450006044938
	'n'	000100010000	425124421273
	' '	٠٠٠٠٠٠١١٠٠١٠	450006044938
	'M'	٠٠٠٠٠١١١٠١١١	950123116068
	'o'	000100010001	575453752151
	's'	000100010101	746763637891
	'u'	000100010111	372213449107
	'l'	000100001000	105823360909

ملحق (٢)

مثال لعملية فك التشفير مبينة بالتفصيل:

الجدول (٣): مثال لعملية فك تشفير نص

الرقم العشوائي المقابل لكل حرف (الشفرة)	قيمة الـ ASCII CODE الناتجة	حروف النص الصريح	الجملة بعد فك تشفيرها
746763637891	000010000100	'T'	Technical College in Mosul
372213449107	000100000001	'e'	
008220550027	000010011001	'c'	
868817535961	000100000100	'h'	
425124421273	000100010000	'n'	
450006044938	000100000101	'i'	
008220550027	000010011001	'c'	
372213449107	٠٠٠٠١٠٠١٠١١١	'a'	
105823360909	000100001000	'l'	
450006044938	٠٠٠٠٠٠١١٠٠١٠	' '	
667187261877	000001100111	'C'	
575453752151	000100010001	'o'	
105823360909	000100001000	'l'	
105823360909	000100001000	'l'	
372213449107	000100000001	'e'	
169548725868	000100000011	'g'	
372213449107	000100000001	'e'	
450006044938	٠٠٠٠٠٠١١٠٠١٠	' '	
450006044938	000100000101	'i'	
425124421273	000100010000	'n'	
450006044938	٠٠٠٠٠٠١١٠٠١٠	' '	
950123116068	٠٠٠٠٠١١١٠١١١	'M'	
575453752151	000100010001	'o'	
746763637891	000100010101	's'	
372213449107	000100010111	'u'	
105823360909	000100001000	'l'	