University of Mosul
College of Computer Science
and Mathematics

Design equivalent Blowfish cryptosystem using Backpropagation neural network

Raghad Abdul Hadi Abdul Qader AL-Quseimy

M.Sc. / Thesis

Computer Science

Supervised by

Dr. Auday H. Saeed AL-Wattar
lecturer

2021 A.D. **1443 A.H.**

ABSTRACT

The last decade witnessed a great evolution in the fields of computer science, communication, and data transmission. The necessity of data protection has become more complex and cryptanalysis has evolved to meet the growing complexity of cryptography or the process of encrypting and decrypting messages to ensure data privacy or security.

Various cryptosystems were developed during this time, one of which is the Blowfish, is a feistel network, iterating a simple encryption function 16 times. The block size is 64 bits, and the key can be any length up to 448 bits. The Blowfish is a patent-free algorithm, and anyone can use it without any restrictions. As most of the algorithms present are patented by some or the other agency, it is very important to have at least one algorithm that is available to be used by anyone and is open for all.

The Blowfish algorithms is one of the most popular, but it requires significant computational power with many details that make it prey to many attackers. In this thesis, a Blowfish equivalent cryptosystem was designed using backpropagation.

The proposed system is based on representing the operations that take place on the plaintext/ciphertext by the Blowfish algorithm on the neural network with the reduction of the data (S-Box). To learning the proposed neural network, a "bidirectional system" was used for encryption and decryption. The system accepts input (plaintext or ciphertext) and outputs the equivalent text, with the keys used in both encryption and decryption being the initial weights of the neural network trained using the backpropagation network, then training the network on a smaller number of outputs in parallel from (1-32) bits and (33-64) bits of the so-called series-parallel system. The proposed Neural Network (NN) model was designed and simulated by a medium-performance computer the test results showed

that the accuracy of the classification process using the backpropagation network was 90% and the error rate is 10%, and that the execution time of ANN encryption and decryption is 15% and 16% lesser than that of the Blowfish algorithm, and convergence of results achieved through ANN with Blowfish results.

The proposed system was built using the MATLAB (2018a) language, and a dataset of 2500 was created with two formatting (plaintext and ciphertext).

جامعة الموصل
كلية علوم الحاسوب والرياضيات

تصميم نظام تشفير مكافئ للسمكة المنفوخة باستخدام الشبكة العصبية ذات الانتشار العكسي

رغد عبد الهادي عبد القادر القصيمي

رسالة ماجستير

علوم الحاسوب

بإشراف

د. عدي هاشم سعيد الوتار

١٤٤٣ هـ ٢٠٢١ م

الخلاصة

شهد العقد الاخير تطورًا كبيرًا في مجالات علوم الكمبيوتر والاتصالات ونقل البيانات. أصبحت ضرورة حماية البيانات أكثر تعقيدًا وتطور تحليل التشفير لمواجهة التعقيد المتزايد للتشفير أو عملية تشفير وفك تشفير الرسائل لضمان خصوصية البيانات أو أمانها.

تم تطوير أنظمة تشفير مختلفة خلال هذا الوقت ، أحدها هو السمكة المنفوخة ، وهي شبكة فاستيل ، تكرر وظيفة تشفير بسيطة ١٦ مرة. حجم الكتلة هو ٦٤ بت ، ويمكن أن يصل طول المفتاح إلى ٤٤٨ بت. السمكة المنفوخة هي خوارزمية خالية من براءات الاختراع ، ويمكن لأي شخص استخدامها دون أي قيود. نظرًا لأن معظم الخوارزميات الموجودة مسجلة ببراءة اختراع من قبل وكالة أو وكالة أخرى ، فمن المهم جدًا أن يكون لديك خوارزمية واحدة على الأقل متاحة للاستخدام من قبل أي شخص ومفتوحة للجميع.

تعد خوارزمية السمكة المنفوخة واحدة من أكثر الخوارزميات شيوعًا ، ولكنها تتطلب قوة حسابية كبيرة مع العديد من التفاصيل التي تجعلها فريسة للعديد من المهاجمين. في هذه الأطروحة ، تم تصميم نظام تشفيرمكافئ للسمكة المنفوخة باستخدام الانتشار العكسي.

يعتمد النظام المقترح على تمثيل العمليات التي تتم على النص العادي / النص المشفر بواسطة خوارزمية السمكة المنفوخة على الشبكة العصبية مع تقليل البيانات (S-Box). لتعليم الشبكة العصبية المقترحة ، تم استخدام "نظام ثنائي الاتجاه" للتشفير وفك التشفير. يقبل النظام الإدخال (نص عادي أو نص مشفر) ويخرج النص المكافئ ، حيث تكون المفاتيح المستخدمة في كل من التشفير وفك التشفير هي الأوزان الأولية للشبكة العصبية المدربة باستخدام شبكة الانتشار العكسي، ثم تدريب الشبكة على عدد أقل من المخرجات بالتوازي من (١-٣٢) بت و (٣٣-٦٤) بت مما يسمى بالنظام التسلسلي المتوازي. تم تصميم نموذج الشبكة العصبية المقترح (NN) ومحاكاته بواسطة كمبيوتر متوسط الأداء ، وأظهرت نتائج الاختبار أن دقة عملية التصنيف باستخدام شبكة الانتشار العكسي كانت ٩٠% ومعدل الخطأ ١٠% ، وأن وقت تنفيذ التشفير وفك التشفير لـ ANN أقل بنسبة ١٥% و ١٦% من خوارزمية السمكة المنفوخة ، وتقارب النتائج التي تم تحقيقها من خلال ANN مع نتائج السمكة المنفوخة.

تم بناء النظام المقترح باستخدام لغة ماتلاب (2018a) ، وتم إنشاء مجموعة بيانات من ٢٥٠٠ بتنسيقين (نص عادي ونص مشفر).