وزارة التعليم العالي والبحث العلمي
جامعة الموصل
كلية علوم الحاسوب والرياضيات
قسم البرمجيات

تطبيق خوارزمية RC4 على الصور بالأعتماد على نظام الفوضى

رسالة مقدمة
الى مجلس كلية علوم الحاسوب والرياضيات في جامعة الموصل
كجزء من متطلبات نيل شهادة دبلوم عالي في
البرمجيات

من قبل

نور مؤيد حسين مجيد

إشراف
أ. م. د. نادية معن محمد ثابت

١٤٤٥هـ ٢٠٢٤ م

الخلاصة

في عالم تطورت فيه المعلومات ووسائل نقلها ضمن شبكة تضم العالم بأسره، لابد من وجود طريقة مناسبة للحفاظ على تلك المعلومات لما يتمتع به البعض منها بخصوصية أو سرية توجب حجبها عن البعض الذي قد يلجأ الى العبث بها أو استخدامها بشكل يجلب الضرر للأخرين وجعلها مقصورة على من يحتاجها فكان ذلك واقعا لاختيار موضوع الرسالة والذي يهدف الى تحسين خوارزمية (RC4) لحماية وتشفير البيانات .

تتضمن هذه الرسالة العمل على تحسين خوارزمية (Rivest Cipher 4)(RC4) بزيادة عشوائيتها وتعقيدها من خلال استخدام الدالة اللوجستية الفوضوية في عملية توليد المفتاح وبأطوال مختلفة (64 بت، 128 بت، 256 بت) لجعل الخوارزمية أكثر أماناً في عملية الاتصال وتبادل المعلومات. تم تقييم جودة التشفير للطريقة المحسنة باستخدام عدة مقاييس مثل وقت التشفير (Encryption Time)، ووقت فك التشفير (Decryption Time) وكان قليلا جدا، ونسبة الإشارة إلى الضوضاء (Peak Signal-to-Noise Ratio) (PSNR) وقد كانت تساوي 7.5663dB، ومتوسط مربع الخطأ (Mean Squared Error)(MSE) وكانت تساوي 11387.9، ومعامل التشابه المتقاطع الموحد (Normalized Cross-Correlation) (NCC) وكانت تساوي 0.000676 ، ومؤشر معامل التشابه الهيكلي (Structural Similarity Index Measure) (SSIM)ويساوي 0.010912، فضلاً عن الرسم البياني (Histogram). أظهرت النتائج أن طريقة التشفير المحسنة المعتمدة على الخريطة اللوجستية الفوضوية نجحت في تحقيق توازن بين الصورة والأمان.

Ministry of Higher Education and
Scientific Research
University of Mosul
College of Computer Science and
Mathematics
Department of Software

Applying The RC4 Algorithm To Images Based On The Chaos System

**A Thesis Submitted to the Council of the College of
Computer Science and Mathematics
University of Mosul
as a Partial Fulfillment of Requirements
for the Degree of Higher Diploma of Science
in
Software**

By

Noor Moayed Husain

Supervised by

Assis.Prof.Dr. Nadia Maan Mohammed Thabit

2024 A.D. **1445 A.H.**

Abstract

In a world where information has evolved, and its transmission is facilitated within a network encompassing the entire globe, there must be a suitable method to safeguard such information. Some data possesses privacy or confidentiality, necessitating its concealment from those who might manipulate or misuse it, causing harm to themselves and others. The chosen topic for this thesis addresses the enhancement of the Rivest Cipher (RC4) algorithm for data protection and encryption.

This thesis includes working on improving the Rivest Cipher 4 (RC4) algorithm by increasing its randomness and complexity through the use of the chaotic logistic function in the key generation process with different lengths (64 bits, 128 bits, 256 bits) to make the algorithm more secure in the process of communication and information exchange. The encryption quality of the improved method was evaluated using several metrics such as Encryption Time, Decryption Time which was very little, and Peak Signal-to-Noise Ratio (PSNR) which was equal to 7.5663dB. The Mean Squared Error (MSE) was equal to 11387.9, the Normalized Cross-Correlation Coefficient (NCC) was equal to 0.000676, and the Structural Similarity Index Measure (SSIM) was equal to 0.010912, as well as Histogram. The results showed that the improved encryption method based on the chaotic logistic map succeeded in achieving a balance between image and security.