وزارة التعليم العالي والبحث العلمي، العراق
جامعة بابل
كلية تكنولوجيا المعلومات
قسم شبكات المعلومات
الدراسة: (صباحي)

تشفير الصور باستخدام التوزيع العشوائي للبلوكات

Image Encryption using Random Block Scrambling

مشروع التخرج هو احد متطلبات الحصول على درجة البكالوريوس في تخصص شبكات المعلومات في تكنولوجيا المعلومات.

A Graduate Project Submitted to the department of Information Networks of the College of Information Technology, University of Babylon, in Partial Fulfillment of the Requirements for the Bachelor's degree in the Information Networks of Information Technology.

by

Murtada Alaa Ali

Supervised by

Dr. Rasim Azeez Kadhim

2024

Abstract

Securing digital images against unauthorized access and tampering is increasingly vital in our world. This project introduces an image encryption technique using random block ciphering, implemented in MATLAB, to enhance the security of image data transmissions. The technique employs a block cipher algorithm with a unique adaptation: the introduction of randomness in the encryption key for each image block, thereby improving resistance to cryptographic attacks.

The methodology centers on segmenting the image into fixed-size blocks. This approach ensures that even if one block is decrypted, other blocks remain secure due to the unique key used for each. The robustness of this encryption method was assessed through various statistical analyses, including entropy measurement, correlation coefficients between adjacent pixels, and susceptibility to both known-plaintext and chosen-plaintext attacks, using MATLAB's powerful computational and graphical capabilities. Results indicate a substantial decrease in pixel correlation and enhanced entropy, suggesting a strong encryption framework. The technique displayed significant resistance against sophisticated cryptanalysis, highlighting its potential for secure real-world applications. This study demonstrates that random block ciphering can be efficiently implemented in MATLAB, making it a viable option for developers and researchers looking for accessible yet powerful encryption solutions for multimedia content.

The findings advocate for further integration of this method into broader systems, potentially extending to real-time encryption services. Future studies may also explore optimization of the MATLAB code to enhance speed without compromising security.