Ministry of Higher Education and
Scientific Research University of
Mosul College of Computer Science
And Main thematics Department of
Computer Science

A Secure Method for Data Encryption and Steganography in QR Codes

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 Master of Science in
Computer Science
By

Afraa Zidane younis Al-kawaz

Supervised by

Asst. Prof. Dr. Ahmed Sami Nori

2025 A.D. **1446A.H.**

Abstract

Technology has significantly transformed the transmission of sensitive data in digital networks, making it an integral part of our daily lives. However, this data, including personal information, financial data, trade secrets, and virtual certificates, faces increasing threats, necessitating the implementation of advanced security features to safeguard it, thereby enhancing trust in electronic data transmissions and preventing forgery.

The proposed technique aims to protect data from unauthorized access while maintaining its integrity. It uses the Rubik's Cube Encryption method to encrypt images and generate encryption keys chaotically and randomly. Logistic Chaotic Encryption enhances security by making decryption difficult. The data is encrypted through operations similar to those performed on a Rubik's Cube, such as rotating rows or columns and flipping directions. The encrypted image is uploaded to a Pinata website, where a URL is generated and a QR code is created. In the second stage, the QR codes are used to embed encryption keys securely, hiding the decryption keys. This strategy ensures the QR code remains readable and appears like original QR codes while containing hidden keys. QR codes are used for data hiding, relying on error correction levels to maintain functionality. The Wet Paper Code (WPC) technique is used, embedding information in specific, modifiable "dry" positions to prevent affecting the code's fundamental functionality. The sender is the only one to know this position, making WPC an efficient and secure method. The maximum embedding capacity within the error correction level is half the number of error correction codewords, with a higher value for version 40 in error correction H (9720) bits.

The encryption algorithm's performance was evaluated using various metrics, including Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index Measure (SSIM), and Bit Error Rate (BER). The optimal value of MSE was 50,637, indicating significant differences between the encrypted and original images. The best PSNR was 27.914 dB, lead to structural differences. The Bit Error Rate was 0.501, indicating significant distortion. Entropy analysis showed a significant increase in value, close to 8, indicating high randomness in the encrypted image. This confirms that the encryption eliminated statistical patterns, enhancing overall security.

The study assessed the readability of QR codes after embedding using noise levels of 1%, 2%, 4%, and 6%. QR code versions 7 and 20 showed high robustness to noise, while version 40 remained readable at 1% and 2% noise, but significant issues occurred at 4% and 6%, indicating that higher-density QR codes are more vulnerable to noise.

The QR code's readability was tested under rotation distortions, confirming that rotation has a less critical effect than high noise levels. The code's recognition accuracy was analyzed under normal and dim lighting conditions, with higher levels of darkness causing difficulty in reading. Reading time increased under these conditions, and the QR code was resized to various resolutions. Extreme downscaling, combined with noise or dimming, negatively impacted recognition accuracy. Key sensitivity was evaluated using NPCR and UACI metrics, demonstrating the strength and security of the proposed algorithm.

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

طريقة آمنه لتشفير البيانات وأخفائها في رموز الأستجابة السريعة

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

من قبل

عفراء زيدان يونس الكواز

بإشراف

أ.م.د أحمد سامي نوري

١٤٤٦ هـ ٢٠٢٥ م

الخلاصة

لقد أحدثت التكنولوجيا تحولاً جذرياً في نقل البيانات الحساسة عبر الشبكات الرقمية، مما جعلها جزءاً لا يتجزأ من حياتنا اليومية. ومع ذلك، تواجه هذه البيانات، بما في ذلك المعلومات الشخصية والبيانات المالية والأسرار التجارية والشهادات الافتراضية، تهديدات متزايدة، مما يستلزم تطبيق ميزات أمان متقدمة لحمايتها، مما يعزز الثقة في عمليات نقل البيانات الإلكترونية ويمنع التزوير. تهدف التقنية المقترحة إلى حماية البيانات من الوصول غير المصرح به مع الحفاظ على سلامتها.

تستخدم هذه التقنية طريقة تشفير مكعب روبيك لتشفير الصور وتوليد مفاتيح تشفير بشكل عشوائي. يعزز التشفير الفوضوي اللوجستي الأمان من خلال جعل فك التشفير صعباً. يتم تشفير البيانات من خلال عمليات مماثلة لتلك التي يتم إجراؤها على مكعب روبيك، مثل تدوير الصفوف أو الأعمدة وقلب الاتجاهات. يتم تحميل الصورة المشفرة إلى موقع بيناتا، حيث يتم إنشاء عنوان URL ورمز الاستجابة السريعة. في المرحلة الثانية، تُستخدم رموز الاستجابة السريعة لتضمين مفاتيح التشفير بشكل آمن، وإخفاء مفاتيح فك التشفير. تضمن هذه الاستراتيجية بقاء رمز الاستجابة السريعة (QR) قابلاً للقراءة، ويبدو كرموز الاستجابة السريعة الأصلية، مع احتوائه على مفاتيح مخفية. تُستخدم رموز الاستجابة السريعة لإخفاء البيانات، معتمدةً على مستويات تصحيح الأخطاء للحفاظ على وظائفها. تُستخدم تقنية رمز الورق الرطب (WPC)، حيث تُضمّن المعلومات في مواضع "جافة" محددة وقابلة للتعديل لمنع التأثير على وظائف الرمز الأساسية. المُرسِل هو الوحيد الذي يعرف هذا الموضع، مما يجعل WPC طريقة فعّالة وآمنة. تبلغ أقصى سعة تضمين ضمن مستوى تصحيح الأخطاء نصف عدد كلمات رمز تصحيح الأخطاء، مع قيمة أعلى للإصدار ٤٠ في بت تصحيح الأخطاء H (٩٧٢٠). تم تقييم أداء خوارزمية التشفير باستخدام مقاييس مختلفة، بما في ذلك متوسط الخطأ التربيعي (MSE)، ونسبة ذروة الإشارة إلى الضوضاء (PSNR)، ومقياس مؤشر التشابه الهيكلي (SSIM)، ومعدل خطأ البت (BER). بلغت القيمة المثلى لـ MSE 50,637، مما يشير إلى اختلافات كبيرة بين الصور المشفرة والأصلية. كان أفضل معدل إشارة إلى ضوضاء (PSNR) 27.914 ديسيبل، مما يشير إلى اختلافات هيكلية. بلغ معدل خطأ البت ٠.٥٠١، مما يشير إلى تشوه كبير. أظهر تحليل الإنتروبيا زيادة كبيرة في القيمة، تقارب ٨، مما يشير إلى عشوائية عالية في الصورة المشفرة. وهذا يؤكد أن التشفير أزال الأنماط الإحصائية، مما عزز الأمان العام.

قيّمت الدراسة قابلية قراءة رموز الاستجابة السريعة (QR Codes) بعد التضمين باستخدام مستويات ضوضاء ١٪ و٢٪ و٤٪ و٦٪. أظهرت إصدارات رموز الاستجابة السريعة ٧ و٢٠ مقاومة عالية للضوضاء، بينما ظل الإصدار ٤٠ قابلاً للقراءة عند ١٪ و٢٪ من الضوضاء، ولكن حدثت مشكلات كبيرة عند ٤٪ و٦٪، مما يشير إلى أن رموز الاستجابة السريعة ذات الكثافة الأعلى أكثر عرضة للضوضاء.

تم اختبار قابلية قراءة رمز الاستجابة السريعة في ظل تشوهات الدوران، مما أكد أن للدوران تأثيرًا أقل خطورة من مستويات الضوضاء العالية. تم تحليل دقة التعرف على الرمز في ظروف الإضاءة العادية والخافتة، حيث تسببت مستويات الظلام العالية في صعوبة القراءة. زاد وقت القراءة في ظل هذه الظروف، وتم تغيير حجم رمز الاستجابة السريعة إلى دقة مختلفة. أثر التصغير الشديد، إلى جانب الضوضاء أو التعتيم، سلبًا على دقة التعرف. تم تقييم حساسية المفتاح باستخدام مقاييس NPCR وUACI، مما يدل على قوة وأمان الخوارزمية المقترحة.