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

توليد واختبار مفتاح التشفير بالإعتماد على قزحية العين

رسالة مقدمة

إلى مجلس كلية علوم الحاسوب والرياضيات في جامعة الموصل

وهي جزء من متطلبات نيل شهادة ماجستير علوم في

البرمجيات

من قبل

آلاء عامر عبدالرحيم محمد علي

بإشراف

أ.م. شهد عبدالرحمن حسو مرعي

١٤٤٥ هـ ٢٠٢٤ م

المســـتخلص

تتمتع القياسات الحيوية بميزة فريدة تمكنها من توفير مستوى أعلى من الأمان مقارنة بالطرق التقليدية. بالإضافة إلى ذلك، يقلل استخدام القياسات الحيوية من حاجة المستخدمين إلى تذكر كلمات مرور معقدة أو حمل الرموز المادية(بطاقات الهوية الذكية (Smart Cards),أجهزة التوكن(Tokens) , مفاتيح USB الأمنية)، مما يعزز الراحة للمستخدم. تتضمن عملية توليد المفتاح استخدام القياسات الحيوية مثل بصمة الإصبع والوجه والقزحية وهندسة اليد وغيرها لإنشاء مفتاح فريد مرتبط بالهوية الحيوية للفرد. من بين القياسات الحيوية، كانت القزحية موضوع اهتمام كبير بسبب الملمس الغني للقزحية الذي يوفر معايير قوية لتحديد الأفراد.

في هذه الأطروحة، تم إنشاء مفتاح تشفير يحتوي على مجموعة من الأرقام الثنائية من قزحيتين، وتم التحقق من عشوائية المفتاح الناتج من خلال عدة مقاييس, وللحفاظ على سرية مفتاح التشفير الناتج بين المرسل والمستقبل، تم إنشاء مفتاح التشفير واختباره من القزحية من خلال تنزيل مجموعة من الصور عالية الدقة من الإنترنت واستخدامها في البرنامج, تم أيضًا إنشاء المفتاح من صور حقيقية (تم التقاطها بواسطة الكاميرا). تم اختيار صورتين للعين تمثلان قزحية المرسل والمستقبل بدقة عالية، وتم تحويل (القزحية) إلى تمثيل رقمي، وتم معالجة الصورتين، ومن ثم استخراج السمات داخل قزحية الصورتين باستخدام خوارزميتين، خوارزمية رسم البياني للتدرجات الموجهة (Histogram Oriented Gradient HOG) وخوارزمية تحويل السمات الثابتة للمقياس (Scale Invariant Feature Transform SIFT) لكلا الصورتين، وتم توليد المفتاح من السمات المستخرجة، ومن ثم تم اختبار المفتاح باستخدام مقاييس العشوائية (اختبار مربع كاي، اختبار ENT، مقياس الكتلة، مقياس الكاب). فإذا كان المفتاح الناتج يفي بمعايير العشوائية فإن المفتاح الناتج يكون عشوائيًا، وإذا لم يكن يفي بالمعايير فإنه لا يكون عشوائيًا، وتم الحصول على أفضل النتائج عند استخدام خوارزمية HOG , عندما كان طول المفتاح ٦٤ بت اذ كانت نتائج الاداء افضل من طريقة (SIFT) حيث كان قيمة مربع كاي يساوي ٢٤٨.٠٠ وقيمة المتوسط الحسابي يساوي١٠٣.٨٧٥.

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

Generating and Testing Encryption Key Based on Iris

**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 Software**

By

Alaa Amer Abdul Raheem Mohammad Ali

Supervised by

Assist. Prof. Shahd Abdulrhman Hasso Maree

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

Abstract

Biometrics have a unique advantage of providing a higher level of security compared to traditional methods. In addition, the use of biometrics reduces the need for users to remember complex passwords or carry physical tokens (Smart Cards, Tokens, USB Security Keys), which enhances user convenience. The key generation process involves the use of biometrics such as fingerprint, face, iris, hand geometry, etc. to create a unique key associated with an individual's biometric identity. Among biometrics, the iris has been the subject of great interest due to the rich texture of the iris that provides strong criteria for identifying individuals.

In this thesis, an encryption key containing a set of binary digits was generated from two iris, and the randomness of the resulting key was verified through several measures. To maintain the confidentiality of the resulting encryption key between the sender and the receiver, the encryption key was generated and tested from the iris by downloading a set of high-resolution images from the Internet and using them in the program. The key was also generated from real images (captured by a camera). Two images of the eye were selected to represent the sender and receiver iris with high accuracy, and the (iris) was converted to a digital representation, and the two images were processed, and then the features inside the iris of the two images were extracted using two algorithms, Histogram Oriented Gradient (HOG) algorithm and Scale Invariant Feature Transform (SIFT) algorithm for both images, and the key was generated from the extracted features, and then the key was tested using randomness measures (Chi-square test, ENT test, Block measure, Gap measure). If the resulting key meets the randomness criteria, then the resulting key is random, and if it does not meet the criteria, then it is not random. The best results were obtained when using the HOG algorithm, when the key length was 64 bits, as the performance results were better than the (SIFT) method, as the Chi-square value was equal to 248.00 and the arithmetic mean value was equal to 103.875.