نظام للتعرف آمن ومؤسس على طريقة المشي

إعداد
أشواق محمد عوض المحمدي

إشراف
د. لمياء عبد الله أحمد الرفاعي

مع التقدم الحديث في التكنولوجيا, أصبحت المقاييس الحيوية من التقنيات المستجدة التي تستخدم لتوثيق الأفراد. نظم التعرف على المقاييس الحيوية أو الأنظمة البيومترية (Biometric Recognition System) تحدد أو تتحقق من الشخص بالاعتماد على صفاته

الخاصة سواء كانت فسيولوجية أو سلوكية. نظريا, أي صفة من صفات الشخص سواء كانت فسيولوجية أو سلوكية يمكن ان تستخدم كمعرف للشخص طالما أنها تحقق بعض الخصائص مثل العالمية, الانفراد, الدوام, والقدرة على الحصول عليها. لكن هناك بعض الضعف بقوة النظام البيومتري عند تعرضه لهجمات. نظم تشفير المقاييس الحيوي (Biometric cryptosystems) هي تقنيات تستخدم لتحسين وتعزيز الأمن في أنظمة التعرف على المقاييس الحيوية. في هذا البحث، سنقترح نظام مصادقة يعتمد على المشي باستخدام نظم تشفير المقاييس الحيوية وذلك لتحسين امن النظام. يتكون نظامنا المقترح من مرحلتين: التسجيل والتحقق. كل واحد منهما يتكون من ثلاث مراحل رئيسية وهي: استخراج ميزة، استخراج المكونات الموثوقة، وإضافة الأمن بنظام يسمى (Fuzzy Commitment Scheme). سنقوم باستخراج المميزات من صور المشي باستخدام النمط الثلاثي المحلي (Local Ternary Pattern (LTP)) ثم سنقوم بإيجاد متوسط الصور باستخدام مفهوم صورة طاقة المشية (Gait Energy Image (GEl)) . لتجميع الصور الناتجة من إيجاد المتوسط , سنستخدم الرسم البياني المشترك ثنائي الأبعاد , وسيستخدم محلل المكونات الرئيسية (Principal Component Analysis (PCA)) لتقليل حجم متجه الميزة النهائي. ولزيادة من متانة النظام سوف نستخرج البت الموثوقة فقط من متجه الميزة . وأخيرا سنستخدم (Fuzzy Commitment Scheme) لتأمين متجه الميزة . سنستخدم كود (BCH) لتشفير المفتاح في مرحلة التسجيل ولفك التشفير في مرحلة التحقق فيما بعد . تم اختبار النظام المقترح باستخدام قاعدة بيانات عامة اسمها (CMU MoBo database). ولقد أظهرت النتائج أن أفضل معدل خطأ تم الحصول عليه عندما تم استخدام المشي السريع للتسجيل والتحقق، حيث حصلنا على ٠٪ كنسبة القبول الخاطئة (FAR) و ٠٪ ولنسبة الرفض الخاطئة (FRR) مع مفتاح طوله يساوي ٥٠.

A Secure Gait Based Recognition System

By
Ashwaq Mohammad Awad AL-Mohammady

Supervised By
Dr. Lamiaa Abdallah Ahmad Elrefaei

A Secure Gait Based Recognition System

ABSTRACT

With new advances in technologies, biometrics has become an emerging technology for authentication of individuals. Biometric recognition system identifies or verifies aperson based on his or her physiological or behavioral characteristics. Theoretically, any human physiological or behavioral characteristic can be used to make a personal identification as long as it satisfies features like universality, uniqueness, permanence and collectability. However, there is still some weakness concerning robustness against attacks in the biometric recognition system. Biometric cryptosystems are techniques used to improve and enhance the biometric recognition system security. The most common biometric cryptosystems include: Fuzzy Commitment Scheme, Fuzzy vault, and Shielding functions. In this thesis, a biometric cryptosystem is applied with a gait based biometric system to enhance the system security. The proposed biometric cryptosystem has two phases: enrollment and verification. Each of them comprises three main stages: Feature Extraction, Reliable Components Extraction, and Fuzzy Commitment Scheme. Gait features are extracted from gait images using Local Ternary Pattern (LTP), then the average of one complete gait cycle using Gait Energy Image (GEl) concept is calculated. The average

images are joined using the 2D joint histogram, which is reduced using Principal Component Analysis (PCA) to produce the final feature vector. To enhance the robustness of the system, only highly robust and reliable bits from the feature vector are extracted. Finally, the Fuzzy Commitment Scheme is used to secure feature templates. Bose-Ray-Chaudhuri-Code (BCH) is used for key encoding in the enrollment phase and as decoding in the verification phase. The proposed system is tested using the CMU MoBo database. The experimental results show that the best error rate is obtained when using fast walk for enrollment and verification, where we get 0% for False Acceptance Rate (FAR) and 0% for False Rejection Rate (FRR) for a key length equal to 50.