حماية البيانات البيومترية المتعددة

من بين نماذج أمن الحاسوب تلك القياسات الحيوية، التي تتعلق باستخدام البيانات الفسيولوجية و السلوكية لتحقق من هوية الأفراد. وعلى الرغم من المزايا التي تتمتع بها هذه الأنظمة البيومترية على أنظمة المصادقة التقليدية ، إلا أنها لا تزال عرضة لقيود معينة ، مما أدى إلى ظهور أنظمة مقاييس حيوية متعددة تتضمن استخدام بيانات بيومترية متعددة لتحسين أداء المصادقة. لسوء الحظ ، حتى الأنظمة متعددة القياسات الحيوية الراسخة تعاني من نقاط الضعف.

في هذه الأطروحة اقترحنا نظاما متعدد المقاييس الحيوية قابلا للإلغاء لتأمين بيانات بيومترية متعددة، ركزنا اهتمامنا على طريقة *BioHashing* وهي تقنية حديثة يمكنها حل مشكلة السرية والأمان. وكان هدفنا هو حماية نظام متعدد الوساط، كان علينا أن نحقق نهج يتكون من الاندماج بين نهجين من الاختلاط على مستوى العينات و على مستوى الحالات ، على أساس التهجين بين القياس الحيوي متعدد الوسائط والتحول القابل للانعكاس. ولتحقيق هذا النهج، قمنا بتجميع وظائف بصمات الأصابع متعددة المستشعرين من ثلاث أصابع بشرية قاعدة بيانات ($SDUMLA-HMT$) . نقترح نموذج تقييم يقوم على أساس مجموعة من المعايير والهجمات المحددة لتقييم معايير الأمن والخصوصية.

الكلمات المفتاحية : أنظمة القياسات الحيوية متعددة الوسائط ، حماية النماذج متعددة القياسات الحيوية ، الهجوم ، الأمن ، التحول ، الأداء.

Résumé

Parmi les paradigmes de la sécurité informatique, la biométrie qui concerne à l'utilisation des données physiologiques et / ou comportementales pour vérifier l'identité des individus. Malgré les avantages de ces systèmes biométriques par rapport aux systèmes d'authentification traditionnels, ils sont encore vulnerables aux limitations spécifiques, ce qui a donné naissance aux systèmes multi biométrie qui consiste à utiliser plusieurs données biométriques pour améliorer les performances de l'authentification. Malheureusement, même les systèmes multi biométriques bien établis souffrent de vulnérabilités. Dans cette thèse, nous avons proposé un schéma multi-biométrique révocable pour sécuriser les données multi-biométriques, nous avons focalisé notre attention sur la méthode BioHashing qui est une technique récente capable de répondre à l'inversion du problème de confidentialité et de sécurité. Notre objectif étant de protéger un système multimodale, nous étions mené à réaliser une approche de fusion de scores à deux niveaux : multi échantillons et multi instances, basée sur l'hybridation entre la biométrie multi modale et la transformation révocable. Pour réaliser cette approche nous avons combiné les fonctions multi-capteurs d'empreintes digitales de trois doigts humains (base de données SDUMLA-HMT).Nous proposons un modèle d'évaluation basé sur un ensemble de métriques et des attaques spécifiques, pour évaluer les critères de sécurité et de protection de vie privée.

Mots clés : Systèmes biométriques multimodaux, protection des modèles multi-biométriques, attaque, sécurité, transformation, performance.

Abstract

One of the paradigms of computer security is biometrics, which concerns the use of physiological and/or behavioural data to verify the identity of individuals.Despite the advantages of these biometric systems over traditional authentication systems, Despite the advantages of these biometric systems over traditional authentication systems, they are still vulnerable to specific limitations, which has given rise to multi-biometric systems. which consists of using several biometric data to improve authentication performance. Unfortunately, even well-established multi-biometric systems suffer from vulnerabilities.In this thesis , we proposed a revocable multi-biometric scheme to secure multi-biometric data, we focused our attention on the BioHashing method which is a recent technique that can solve the inversion of the confidentiality and security problem.Our objective being to protect a multimodal system, we had to realize an approache a two-level scoring merging approach: : multi samples and multi instances, based on hybridation between multi modal biometry and revocable transformation. To achievethis approache we have combined the multi-sensor functions of fingerprints from a three human fingers (SDUMLA-HMT database).We propose an evaluation model based on a set of metrics and specific attacks, to evaluate security and privacy criteria.

Keywords : Multi-modal biometric systems, multi-biometric templates protection, attack, security, transformation, Performance.