REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

جامعة محمد بوضياف - المسيلة
Université Mohamed Boudiaf - M'sila

N° d'ordre : .....

UNIVERSITE DE M'SILA

FACULTE DES MATHEMATIQUES ET DE L'INFORMATIQUE

Département des STIC

MEMOIRE de fin d'étude

Présenté pour l'obtention du diplôme de MASTER

Domaine : Mathématiques et Informatique

Filière : Informatique

Spécialité : Technologies de l'information et de la Communication

Par: Elyass KACEM

SUJET

SECURISATION DE DESCRIPTEUR DE MINUTIES DANS LES SYSTEMES D'IDENTIFICATION PAR EMPREINTE DIGITALE

Soutenu publiquement le : / 06 /2015 devant le jury composé de :

Mr.....	**Université de M'sila**	**Président**
Mr Belhadj Foudil	**Université de M'sila**	**Rapporteur**
Mr.....	**Université de M'sila**	**Examinateur**
Mr.....	**Université de M'sila**	**Examinateur**

Promotion : 2013 /2015

TABLE DES MATIÈRES

Chapitre II : RECONNAISSANCE PAR EMPREINTES DIGITALES

Chapitre III : SECURITE DES SYSTEMES BIOMETRIQUES

Chapitre IV : Attaque de l'algorithme "Shell"

Introduction générale

L'accroissement international des communications, tant en ampleur qu'en diversité, implique le besoin de s'assurer de l'identité des individus. L'importance des enjeux, motive les fraudeurs à mettre en échec les systèmes de sécurité existants, d'où l'utilité capitale de vérifier les identités des personnes. Le marché du contrôle d'accès s'est ouvert avec le développement des systèmes, mais aucun ne se révèle efficace contre la fraude et la falsification car tous utilisent un identifiant externe tel que: mot de passe, badge/carte, clé, code, etc. La biométrie s'avère une solution très efficace.

Les systèmes d'identification biométriques reposent sur les caractéristiques comportementales et/ou physiologiques caractérisant un individu pour l'identifier d'une manière unique. Les systèmes biométriques sont sécurisés : « Aucune personne ne peut remplacer une autre pour s'identifier à sa place ! »

La phrase qui vient d'être citée reste-t-elle une « vérité pratique» ? La réponse est NON !

Les systèmes biométriques (SB), malgré leurs grands avantages, présentent plusieurs inconvénients :

1- Les données biométriques, objets d'identification, sont généralement stockées dans une BDD. Cette dernière est toujours exposée à des attaques.
2- Les données biométriques une fois compromises sont inrenouvelables dans le sens des mots de passes.
3- Les données biométriques sont tractables. Un système compromis peut conduire à la vulnérabilité automatique d'un autre puisqu'ils sont basés sur les mêmes données biométriques.

Dans ces dernières années, plusieurs recherches ont été menées dans le but de sécuriser les SB. Une des approches intéressantes proposées est la biométrie résiliables (ou révocables) (cancelable biometry). Le principe est de ne pas stocker les données biométriques originales, mais plutôt sauver des données transformées. Le matching doit être achevé dans le domaine transformé. Ce qui est intéressant encore est qu'à partir un seul modèle biométrique original on doit être capable de générer autant de modèles transformés que l'on veut. Les modèles transformés doivent vérifier :

1) *La révocabilité:* Bien entendu, il doit être facile de révoquer et de remplacer le modèle de référence en se basant sur les mêmes données biométriques.
2) *La diversité:* Pour assurer la protection de la vie privée de l'utilisateur, deux modèles révoqués ne doivent pas être comparés positivement. Cela délimitera le problème de surveillance sur différentes bases de données.
3) *La confidentialité:* Il doit être complexe voire impossible d'inverser le modèle protégé et de recalculer le modèle biométrique original.
4) *La performance: Cette méthode de protection ne devrait pas dégrader la performance du système biométrique (FAR et FRR).*

Dans ce mémoire, nous allons analyser les aspects de sécurité d'un algorithme récent de sécurisation de modèle d'empreinte digitale basée sur la transformation en spirale du modèle biométrique nommé « fingerprint shell securing » proposé en 2014 par Chouaib et al. (Pattern Recognition Letters 45 (2014) 189–196). Les auteurs ont prouvés la sécurisation du template transformé et l'on confirmé par les tests qu'ils ont menés. Cependant, l'algorithme proposé présente plusieurs failles de sécurité.

Nous allons proposer un algorithme d'attaque permettant de récupérer les données biométriques originales à partir de modèle sécurisé par l'algorithm de Shell en exploitant ses

failles de sécurité. Les tests menés sur la base de données FVC2002 confirment la vulnérabilité de cet algorithme.

Le mémoire est structuré en une partie théorique qui présente toutes les informations récoltées et nécessaires à la compréhension de la biométrie et la sécurisation du modèle biométrique. Une deuxième partie est dédiée à des aspects pratiques où sont exposées les différentes étapes de la mise en œuvre de l'algorithme Shell et la réalisation de l'attaque. Afin d'atteindre notre objectif, nous découperons ce mémoire en plusieurs chapitres.

Dans le chapitre I nous donnerons des notions générales sur la biométrie et les systèmes de reconnaissance d'individus.

Le chapitre II présente l'authentification par empreintes digitales, nous expliquerons ainsi les caractéristiques des empreintes et leur classification. Nous citerons les problèmes liés à cette modalité.

Le chapitre III aborde la sécurité des systèmes biométriques où les vulnérabilités et les failles des systèmes biométriques seront exposées.

Le chapitre IV discute la conception et la réalisation de notre algorithme d'attaque.

Nous terminons ce mémoire par une conclusion générale.

Conclusion Générale

La biométrie est proposée comme une solution efficace remédiant aux problèmes posés par les systèmes classiques de sécurisation basés sur les secrets (mots de passe out tokens). Cependant, les données biométriques présentent l'inconvénient de ne pas être renouvelables et sont plus-ou-moins attaquables. Rendre ces données statiques plus sécurisées et révocables en cas où elles sont attaquées est une tâche très importante dans le processus de construction d'un système d'identification biométrique.

Dans ce mémoire, nous avons analysé les aspects de sécurité d'un algorithme récent de sécurisation de modèle d'empreinte digitale basée sur la transformation en spirale du modèle biométrique nommé « fingerprint shell securing ». Nous avons proposé un algorithme d'attaque permettant de récupérer les données biométriques originales à partir de modèle sécurisé en exploitant quelques failles de sécurité. Les tests menés sur la base de données FVC2002 confirment la vulnérabilité de cet algorithme.

Le présent travail peut être encore amélioré en proposant un algorithme de renforcement de l'algorithme « fingerprint shell securing ».

Bibliographie

[4].F.Perronnine, J.L. Dugelay. « *Introduction à la Biométrie* », Revue Traitement du Signal, Vol.19, No. 4, 2002.

[5].Anil K. Jain, Arun Ross et Salil Prabhakar, « *An Introduction to Biometric Recognition* », IEEE Transactions on Circuits and Systems for Video Technology (PDF), vol. 14, N° 1, janvier 2004.

[6].**CLUSIF** « Club de la Sécurité des systèmes d'Information Français ». Commission Techniques de Sécurité Physique TECHNIQUES DE CONTROLE D'ACCES PAR BIOMETRIE juin 2003.

[8].A.K. Jain, S. Pankanti, S. Prabhakar, L. Hong, A. Ross, J.L. Wayman. *"Biometrics: A Grand Challenge"*, International conference on pattern recognition, UK, 2004.

[9].S. Pankanti, S. Prabhakar, and A. Jain. *"On the individuality of fingerprints"*, IEEE Transactions on Pattern Analysis and Machine Intelligence (24:8), 2002, pp. 1010-1025.

[10].Laurent Guyot, « *Attention biométrie* », diffusé sur « ARTE », 2009.

[12].A.K. Jain, S. Prabhakar, L. Hong, S. Pankanti, *"Filterbank-based fingerprint matching"*, IEEE Trans. Image Process, Vol 5, pp. 846–859, 2000.

[13].L. HAMACHE et S. LALLALI « *Conception et réalisation d'une authentification par FingerHashing sur carte à puce* », Mémoire de fin d'études Ecole nationale Supérieure d'Informatique, 2008.

[14].S. Helfroush and H. Ghassemian. *"Non minutiae-Based Decision-Level Fusion for Fingerprint Verification"*, EURASIP Journal on Advances in Signal Processing, 2007.

[15].Patrick Ducrot, « *Sécurité Informatique* », école nationale supérieure d'ingénieurs de Caen & centre de recherche, 6 octobre 2008.

[16].Produced by the Common Criteria Biometric Evaluation Methodology Working Group *"Biometric Evaluation Methodology Supplement [BEM]"*, Common Methodology for Information Technology Security Evaluation, v1.0, **August 2002**.

[17].International Organization for Standardization (ISO), International Electro technical Commission (IEC): ISO/IEC CD 19792: Information technology – Security techniques – Security evaluation of biometrics. (2006-07-14).

[18].B. Schneier, « Attack trees ». Dr. Dobb' s journal Of Soft Tools, December 1999.

[19].I. Buhan, «*Cryptographic keys from Noisy Data Theory and Applications*», PhD thesis at the University of Twente, Netherlands, 2008.

[20].R. Bolle, J. Connell, S. Pankanti, N. Ratha, and A. Senior, *"Guide to Biometrics"*, Springer-Verlag, 2003.

[21].O. henniger, *D. Scheuermann, and T. Kniess, "On security evaluation of fingerprint recognition systems"*, International biometric Performance testing conference, 2010.

[22].M.Sutrop, *"Ethical Issues in Governing Biometric Technologies"*, ICEB, 2010.

[23].N.K. Ratha, J.H. Connell, and R.M. Bolle, *"Enhancing security and privacy in biometrics-based authentication systems"*, IBM Systems Journal (40:03), 2001, pp. 614–634.

[24].J. Feng and A. Jain, *"FM model based fingerprint reconstruction from minutiae template"*, International conference on Biometrics (ICB), 2009.

[25].A. Teoh, D. Ngo, A. Goh, *"An integrated dual factor authenticator based on the face data and tokenised random number"*, ICBA, pp. 117–123, 2004.

[26].N.K. Ratha, S. Chikkerur, J.H. Connell, R.M. Bolle. *"Generating cancelable fingerprint templates"*. IEEE Transactions on Pattern Analysis and Machine Intelligence (29:4), 2007, pp. 561-572.

[27].A. Juels and M. Wattenberg, *"A fuzzy commitment scheme"*, Proceedings of the 6th ACM conference on Computer and communications security, pp.28–36, 1999.

[29] A.k. Jain, K. Nandakumar, A. Nagar, Biometric template security, EURASIP J. Adv. Signal Process. (2008) 1–17.

[30] D. Maltoni, D. Maio, A.K. Jain, S. Prabhakar, Handbook of Fingerprint Recognition, second ed., Springer Publishing Company Incorporated, 2009.

[31] J. Breebaart, B. Yang, I.B. Dulman, C. Busch, Biometric template protection: the need for open standards, Privacy Data Secur. J. 5 (2009) 299–304.

[32] C. Moujahdi ,G.Bebis , S. Ghouzali , M. Rziza Fingerprint shell: Secure representation of fingerprint template Elsevier Pattern Recognition Letters 45 (2014) 189–196

ملخص : قد تكون الإلغائية للقياسات الحيوية نهج أو طريقة جديدة لمعالجة العديد من المخاوف الأمنية للمصادقة البيومترية , وتستخدم بعض التحويلات النقاط الفريدة لتحويل القالب البيومتري الأصلي الى نسخة جديدة من أجل المصادقة.

إن أمن الالغائية للقياسات الحيوية يكمن في صعوبة عكس القالب المحول, اي يجب ان تكون التحويلات غير قابلة لاسترداد واسترجاع القلب الأصلي , ولتحقيق اللاعكسي للقوالب يجب استخدام طريقة (الكل الى واحد) خلال التحويلات .
فكرة الباحث شعيب هي توليد نماذج بصمات الاصابع باستخدام خوارزمية الحلزون , ومع الدراسة تبين في هذا البحث أن شكل التحويلات والمعلمات المختارة (النقاط الفريدة) في تنفيذ و إنشاء القوالب المحمية يعاني من ضعف في الخوارزمية بطريقة (الكل الى واحد) , وهذا يؤدي ما يسمح باستغلالها لاسترجاع القالب المحول المحمي الى البصمة الأصلية .

مفاتيح :

البيومتري , الالغائية , النقاط الفريدة , اللاعكسي , التحويلات , البصمة الرقمية .

Abstract : Cancelable biometrics may be a good approach to address the security and privacy concerns on biometric authentication. It uses some parameterized transforms to convert an original biometric template into a new version for authentication. The security of cancelable biometrics lies on non-invertibility of the transformed template, that is, the transforms should be noninvertible so that the original template cannot be recovered.

One way to achieve the non-invertibilty is through the use of many-to-one transforms.
The idea of the "Shell" scheme of generating a secure fingerprint templates is to transform the original template into one-to-many shell-based representation.
However, it is revealed in this manuscript that the form of the transforms and the parameters (The minutiae) chosen in his implementation weaken the many-to-one property.
This results in the possible recovery of original minutiae from many transformed template.
Keys : Biometrics , Cancelable , minutiae , non-invertibility , transformation , fingerprint .

Résumé : Biométrie résiliables peuvent être une bonne approche pour répondre aux préoccupations de sécurité et de confidentialité sur l'authentification biométrique. Elle utilise des transformations paramétrées pour convertir un modèle biométrique original dans une nouvelle version pour l'authentification. La sécurité de la biométrie résiliable se cache dans la non-invertibilité du modèle transformé, de sorte que le modèle d'origine ne peut pas être récupéré. Une façon d'atteindre cette caractéristique est par l'utilisation d'une fonction de transformation plusieurs-à-un.

Dans ce travail nous avons analysé l'algorithme de sécurisation de modèle d'empreinte digitale proposé par Chouaib et al. (2014) basé sur la conversion des données biométriques en représentation de coque (shell). Cet algorithme présente plusieurs failles de sécurité, nous avons décrit un algorithme d'attaque permettant de récupérer les données originales à partir de modèles protégés par l'algorithme de coque.

Cela se traduit par la récupération possible de minuties d'origine à partir de un modèle transformé.

Mots clés :

Biométrie, résiliablité, minuties, non-inversibilité, transformation, empreinte digitale.