Study of the robustness of a cancelable biometric system

Rima Belguechi, T. Le-Goff, Estelle Cherrier, Christophe Rosenberger

Study of the robustness of a cancelable biometric system

R. Belguechi, T. Le-goff, E. Cherrier, C. Rosenberger
Laboratoire GREYC, ENSICAEN - Université de CAEN - CNRS
6 Boulevard Maréchal Juin, 14000 Caen, France

***Résumé*—Biometrics is an emerging technology for user authentication. However, biometric data is generally non-revocable unlike a password (as it is not possible to change it). To overcome this problem, biometric template protection schemes have been proposed in the last decade. The purpose of this paper is to study the robustness of a popular algorithm carrying out attacks achievable by an attacker. Experimental results on a significant fingerprint benchmark show a good robustness of this protection scheme against personal attacks (identity theft) but also some gaps in identification applications.**

I. Introduction

Littéralement, la biométrie est une science qui mesure les caractéristiques des êtres vivants. Depuis quelques années, la biométrie désigne plus spécifiquement l'identification ou la vérification d'identité de personnes en fonction de données morphologiques (visage, empreintes digitales, iris...) ou comportementales (voix, dynamique de signature, dynamique de frappe ...). De nombreuses applications biométriques ont été développées, on peut citer le contrôle d'identité par un passeport électronique, le contrôle d'accès à des bâtiments sécurisés, ou encore les capteurs d'empreintes digitales présents sur les ordinateurs portables récents. De manière générale, tout usage d'un système biométrique nécessite deux phases :

- une phase d'enrôlement, où les données biométriques (empreinte digitale, visage, iris...) sont capturées, modélisées (pour construire la référence biométrique de l'individu) puis stockées
- une phase de vérification consistant à comparer la nouvelle capture avec la référence de l'individu présumé.

Puisque la biométrie fait appel à ce que l'on est, elle comporte un avantage primordial sur les autres concepts, dans le sens où elle évite l'usage d'un grand nombre de mots de passe complexes, la perte de tokens... Une comparaison de ces techniques est détaillée dans les références [O'G03], [INC06]. Cependant, le recours à la biométrie présente des risques en terme de respect des droits et des libertés fondamentales. Le fait de capturer et de conserver des données biométriques brutes peut constituer une invasion de la vie privée. Ces données sont sensibles et ne sont pas encore protégées par une norme internationale. Parmi les solutions envisagées, on peut rendre les bases de données anonymes, et plus généralement intégrer la notion de respect de la vie privée dès la conception du système biométrique. Un autre problème vient s'ajouter au risque de violation de la vie privée, il s'agit de la non-révocabilité des données biométriques. Contrairement à un mot de passe ou un code PIN, les caractéristiques personnelles ne peuvent pas être changées lorsqu'il y a vol ou falsification.

Le concept de *biométrie révocable* a été défini pour la première fois dans l'article [RCB01]. Il s'agit de transformer les données biométriques brutes, à l'aide d'une fonction choisie, de telle sorte que les données transformées soient sûres, révocables et respectent la vie privée. Le livre [MMJP03] donne les propriétés essentielles d'un bon système de biométrie révocable :

- la révocabilité : on doit pouvoir facilement révoquer les données en cas de compromission,
- la non-inversibilité : à partir des données transformées, on ne doit pas être capable d'obtenir des informations sur les données biométriques brutes,
- la performance : le fait que la biométrie soit révocable ne doit pas détériorer l'efficacité du système de reconnaissance,
- la diversité : on doit pouvoir générer des données différentes pour des applications différentes.

Cet article est organisé de la manière suivante. Nous présentons un bref état de l'art en section II sur les solutions de protection de la donnée biométrique. La section III décrit le principe général du BioHashing ainsi que ses déclinaisons selon la donnée biométrique choisie. Une comparaison des différentes méthodes existantes sera menée. Dans la section IV, on présente les protocoles des différentes attaques ainsi que les outils pour évaluer leurs performances. Les résultats expérimentaux sont détaillés et commentés.

II. Etat de l'art

Afin de protéger une donnée biométrique, il existe plusieurs solutions dans la littérature. Lors de la conception d'un système biométrique, la difficulté à remplir toutes les conditions énoncées précédemment vient du fait que le signal biométrique varie naturellement, par conséquent la cryptographie standard n'est pas

directement adaptée. L'utilisation d'un chiffrement cryptographique est possible mais la vérification nécessite le déchiffrement des données ce qui peut être un problème de sécurité. Il n'est en effet pas possible de comparer des condensés cryptographiques de la référence et de la capture. Un autre problème concerne la durée de vie de ces données (équivalente à celle d'un individu) où il est difficile de garantir que le chiffrement avec les algorithmes classiques tels que RSA ou 3DES avec les tailles de clés usuelles ne sera pas cassé dans plusieurs années (l'attaquant pourra usurper l'identité de l'individu). Il est également possible de stocker la donnée biométrique dans un élément sécurisé tel qu'une carte à puce ou une clef usb sécurisée. Même si ces éléments ont en général un niveau de sécurité élevé (EAL4+), le risque d'attaque existe. Evidemment, ces solutions permettent de résoudre en partie le risque lié au stockage centralisé de données biométriques et évite que la donnée soit transmise (dans les solutions dites de "match on card").

Les schémas de biométrie révocable proposés dans la littérature sont classés en deux catégories : les cryptosystèmes biométriques et les fonctions de transformation. Le point commun à toutes ces méthodes réside dans le fait de ne pas stocker directement dans la base les données biométriques brutes : elles sont soit stockées sur un support externe (carte à puce, token), soit stockées après transformation.

Parmi les cryptosystèmes biométriques, certaines approches nécessitent une clé de chiffrement qui est combinée avec la donnée biométrique. C'est le cas du système de vérification de l'iris développé dans l'article [DFM98], qui utilise les codes correcteurs d'erreur. Mais le schéma proposé ne semble pas applicable et ne répond pas à la condition de révocation. Il est amélioré par la technique de *fuzzy commitment* détaillée dans [JW99], reposant sur le hachage de la donnée biométrique, mais qui ne s'applique qu'à des données binaires stables en taille et ordonnées. Cette condition est relaxée par la technique de *fuzzy vault* (littéralement, *coffre-fort flou*), présentée dans l'article [JS02]. Les auteurs utilisent comme clé un polynôme pour chiffrer les minuties. La vérification se fait par interpolation de Lagrange. Cette méthode a été implémentée dans [CKL03] et modifiée dans [UJ06] par l'ajout de points supplémentaires mais inutiles, dans le but de brouiller les données. Plus récemment, des schémas reposant sur cette technique de fuzzy vault appliquée aux empreintes digitales ont été développés dans [LYC+09] et [NNJ09]. Cependant, l'article [SB07] présente des attaques montrant que ces techniques ne répondent pas au critère de révocabilité. En effet, ce sont les données biométriques qui jouent le rôle de la clé, qui n'est par conséquent pas révocable.

D'un autre côté, les fonctions de transformation représentent une solution intéressante pour compenser la variabilité d'une donnée biométrique. Le point commun à ces techniques est d'exécuter la comparaison entre la donnée capturée et la donnée stockée directement dans le domaine de transformation. L'article pionnier est l'article de Ratha [RCB01], qui présente le principe général du *BioHashing*. Cette méthode introduit une distorsion du signal biométrique à l'aide d'une fonction de transformation choisie. La révocabilité est garantie car, lorsqu'une donnée transformée est compromise, il suffit de changer de fonction de transformation. La diversité est également assurée par le choix de fonctions différentes pour des applications distinctes. Cependant, trouver de telles fonctions n'est pas simple. En effet, outre la non-inversibilité, ces fonctions doivent exhiber deux propriétés essentielles : une robustesse intra-classe (c'est-à-dire une robustesse vis-à-vis des variations d'une donnée biométrique d'un individu) et une sensibilité inter-classe (on doit pouvoir distinguer deux individus différents).

III. Principe général du BioHashing

Des schémas algorithmiques de protection du modèle biométrique ont été proposés dans la dernière décennie [TNG04], [RCCB07], [BHR10]. Le principe général de ces schémas est de générer un BioCode binaire (utilisé pour l'enrôlement et la vérification) à partir de la représentation de la donnée biométrique (comme des paramètres de texture ou les minuties pour les empreintes digitales) et un nombre aléatoire. Ce procédé est employé pour l'enrôlement de l'utilisateur (où seul le BioCode généré est stocké) et pour la vérification (où le BioCode est recalculé à chaque vérification et nécessite le stockage sécurisé de l'aléa). Le résultat de vérification se fait par le calcul d'une simple distance de Hamming entre le BioCode de référence et le BioCode calculé. L'intérêt de cette approche réside dans la possibilité de révoquer le BioCode (en utilisant un autre nombre aléatoire) et même de le diversifier. Il peut être intéressant à partir de la même donnée biométrique (son empreinte digitale par exemple) de générer différents BioCodes pour s'authentifier à différents services. La figure 1 illustre le procédé global.

Plus précisément, la méthode utilisée consiste à projeter la donnée biométrique (normalisée) sur une base orthonormée générée à partir de l'aléa. La dimension résultante est au plus égale à la dimension de représentation de la donnée biométrique. Cette phase consiste donc à cacher en quelque sorte la donnée biométrique dans une partie de l'espace. L'utilisation d'une base orthonormée permet de garantir la conservation des relations de similarité entre deux données biométriques projetées, comme cela a été démontré par le lemme de Johnson-Lindenstrauss (voir la référence [DG99]). La

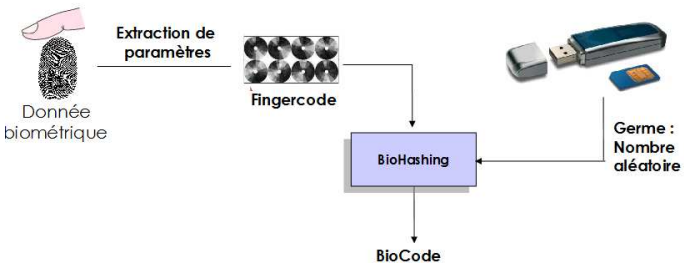


FIGURE 1. Schéma général de protection d'une donnée biométrique

second étape consiste à quantifier ce résultat à l'aide d'un simple seuillage. Cette étape permet de garantir la non inversibilité du procédé (retrouver la donnée biométrique initiale à partir du BioCode) et de rendre robuste le procédé (en autorisant des différences mineures dans le vecteur projeté inhérent à l'acquisition de la donnée biométrique). Le principe général est résumé dans la figure 2.

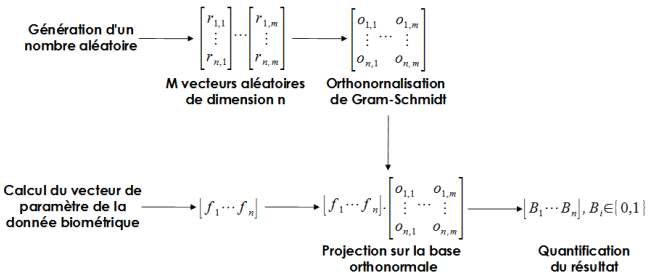


FIGURE 2. Description du procédé de génération d'un BioCode avec la méthode de Ratha

Ce procédé permet de garantir qu'il n'est pas possible de retrouver la donnée biométrique initiale à partir du BioCode. Afin d'éviter l'attaque par force brute (prédiction du BioCode de l'individu), il est nécessaire d'avoir une représentation de la donnée biométrique avec l'entropie la plus importante possible. Les minuties sont couramment utilisées pour représenter une empreinte digitale mais cette représentation est trop compacte pour pouvoir être utilisée telle quelle dans ce type d'algorithme de génération de données biométriques révocables. Dans des travaux antérieurs, nous avons proposé d'utiliser une représentation basée texture (filtres de Gabor) [BHR10] permettant de générer par la méthode de Ratha un BioCode de 384 bits. Dans cet article, nous utilisons un banc de filtres de Gabor pour représenter le FingerCode d'une empreinte digitale. On obtient une dimension de représentation à 128 valeurs numériques.

La méthode BioHashing détaillée précédemment est une méthode générique permettant de révoquer une donnée biométrique. Elle a été utilisée sur plusieurs modalités biométriques (essentiellement les empreintes digitales, le visage [LN07], texture de la paume de la main [CTGN04] ...). L'objet de ces travaux est essentiellement d'augmenter la taille du BioCode (plus il est grand, moins une attaque par force brute sera possible) et d'améliorer les performances. La problématique de protection de données biométriques a été souvent abordée de façon étonnante par le biais de la performance (minimisation du taux d'erreur et maximisation de la taille du BioCode). Mis à part quelques travaux, notamment [TNG04], il existe très peu d'études se focalisant sur la robustesse de ces algorithmes et notamment simulant des attaques visant à être authentifié à la place de l'utilisateur réel à partir du vol de certains éléments ou d'écoutes. Ceci est notre contribution majeure dans cet article.

IV. Etude de la robustesse du Biohashing

Nous décrivons par la suite le protocole mis en place et les attaques qui ont été réalisées.

A. Protocole

D'une manière générale, la fiabilité d'un système biométrique est déterminée à parts égales par :

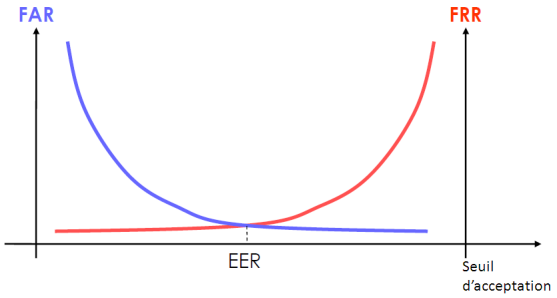
- la qualité du capteur
- l'ergonomie de la capture
- la performance des algorithmes

Dans la suite, on ne s'intéresse qu'au troisième point, on suppose que les deux premières conditions sont remplies. Lorsqu'il s'agit d'authentifier un individu par un mot de passe, la vérification est un procédé dit déterministe, dans le sens où elle est positive (si les deux mots de passe sont identiques), ou négative (si les deux mots de passe sont différents). En revanche, la comparaison de deux données biométriques (transformée ou non) est un procédé statistique. En effet, chaque capture d'une même donnée biométrique est différente : le système essaie alors de déterminer un degré de similarité. On définit deux taux d'erreur classiques :

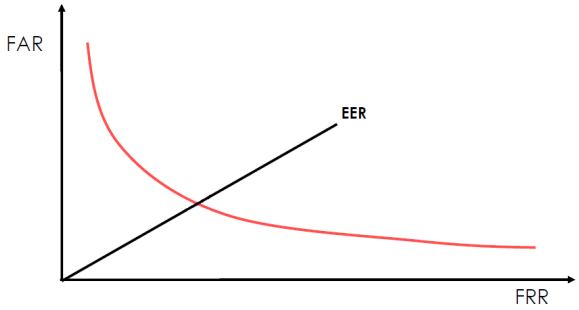
- La fausse acceptation (faux positif) ou FAR (False Acceptance Rate) : c'est la probabilité d'accepter un intrus dans le système pensant qu'il s'agit d'une autre personne qui, elle, est autorisée.
- Le faux rejet (faux négatif) ou FRR (False Rejection Rate) : c'est la probabilité de rejeter, au premier essai, une personne autorisée par le système. Un deuxième essai permet généralement de remédier au problème (la probabilité d'être également rejeté au deuxième essai, et aux suivants, est de plus en plus faible).

La démarche pour évaluer la performance d'un système de biométrie est la suivante. On constate tout d'abord que le FAR et le FRR sont deux données qui évoluent de façon inversement proportionnelle, voir la figure 3(a). Si la sécurité du système est privilégiée, le FAR devra être

bas, tandis qu'un système plus convivial aura un FRR bas. A l'extrême, un système de FAR 0% et de FRR 100% refusera l'accès aux utilisateurs légitimes, mais possédera le niveau de sécurité le plus élevé. Il s'agit donc de trouver un compromis entre FAR et FRR.



(a) Evolution des taux de FAR et FRR en fonction du seuil de similitude



(b) Courbe ROC

FIGURE 3. Evaluation des performances

Pour cela, on fixe un seuil d'acceptation entre 0% et 100% : plus le seuil va vers 0%, plus les fausses acceptations seront nombreuses, plus le seuil va vers 100% plus les faux rejets seront nombreux. On définit une valeur particulière du seuil, notée EER (Equal Error Rate), pour laquelle les deux taux FAR et FRR sont égaux. La courbe ROC, tracée à la figure 3(b), est une représentation du FRR en fonction du FAR. L'intersection de la courbe avec la première bissectrice donne la valeur de l'EER. L'EER n'est pas toujours une valeur pertinente pour juger les performances d'un système biométrique, comme on le verra dans la suite de l'article. Selon l'application considérée, un FAR bas pourra être favorisé, ou au contraire un FRR bas. Si on reprend le raisonnement précédent sur l'interprétation de ces deux taux, une application de type accès physique à une zone ultra sensible devra favoriser un FAR très bas, de sorte qu'un intrus ne puisse pas entrer. En contrepartie, une personne autorisée pourra être amenée à s'authentifier plusieurs fois avant d'être reconnue par le système. Au contraire, une application en recherche criminelle devra favoriser un FRR très bas, pour ne pas laisser passer le criminel. En contrepartie, plusieurs personnes pourront être suspectées à tort.

Les différentes notions introduites précédemment vont maintenant être utilisées pour évaluer les performances de la technique de BioHashing. Les données biométriques testées sont issues de la base de données FVC2002. On dispose ainsi de 8 empreintes digitales de 100 individus. Le FingerCode est généré selon la méthode présentée au paragraphe III, détaillée dans l'article [BHR10], par application d'un banc de filtres de Gabor. Au final, on dispose de 8 FingerCodes pour chaque individu, donc 800 FingerCodes en tout, de longueur 128 bits. Après projection aléatoire et quantification, on obtient 800 BioCodes. Pour chaque individu, on conserve une empreinte de référence, les sept autres serviront à tester les différentes attaques.

B. Evaluation des performances

Dans un premier temps, on teste les performances du FingerCode, puis du BioCode en analysant leurs courbes ROC.

***Test 1 :* FingerCode**

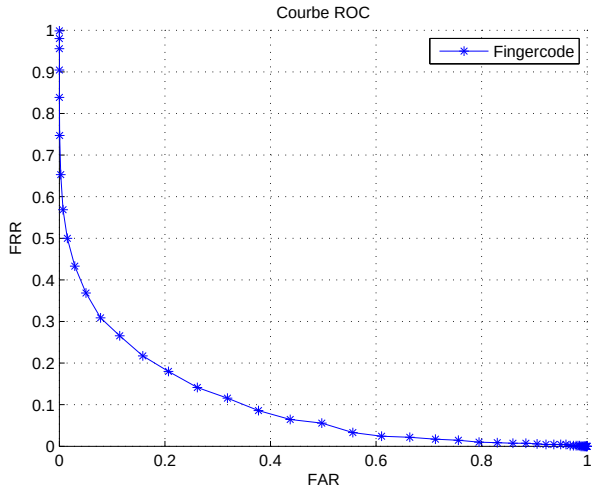
Il s'agit dans ce cas d'un système non révocable, utilisant les empreintes digitales "brutes". Le score traduit la similarité (mesurée à l'aide de la distance de Minkowski) entre les représentations de l'empreinte capturée (ie. le FingerCode) et les empreintes de la base de données. L'EER obtenu est de 19%, voir la figure 4(a). Il est bien évident que cette performance est loin d'être la meilleure de la littérature. Ceci étant, cette valeur permet de fixer une performance initiale du système.

***Test 2 :* BioCode**

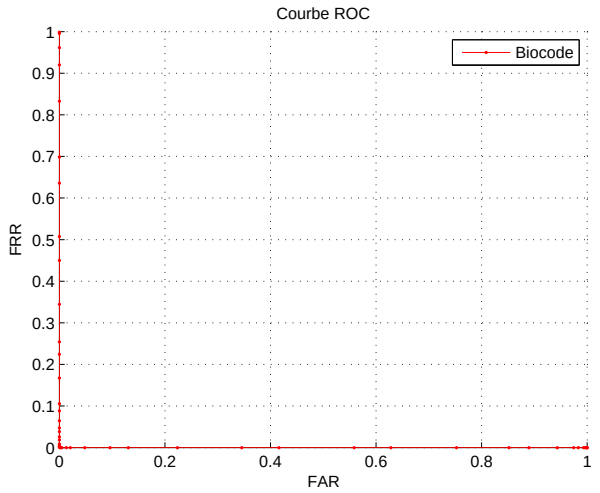
Dans ce cas, on quantifie la performance du système biométrique révocable. On constate que l'EER est nul comme le montre la figure 4(b), ce qui signifie qu'un intrus ne pourra pas se faire passer pour un utilisateur autorisé. La valeur du seuil associé à cet EER est de 0.32. Le gain de performance associé au procédé rendant la donnée biométrique révocable est très intéressant. Il s'explique par le fait que la disparité intra-classe intrinsèque d'une donnée biométrique est lissée par l'utilisation de la valeur aléatoire qui est fixe à chaque utilisation. Au final, la variabilité intraclasse est diminuée ce qui améliore les performances de façon importante.

C. Evaluation de la robustesse

1) Description des différents scénarios: Etudier la robustesse du BioHashing revient à tester la performance du système par rapport aux variations inéluctables de la donnée biométrique d'un individu (robustesse intra-classe), et la sensibilité du BioHashing aux différences entre les données d'individus distincts. On propose de



(a) FingerCode, EER=19%



(b) BioCode, EER=0%

FIGURE 4. Courbes ROC

tester ici des attaques connues (donnée biométrique interceptée, token volé, attaque par force brute). Nous proposons également de nouvelles attaques qui permettront de définir un cadre (ou un niveau de sécurité minimum) pour l'étude des futurs systèmes de biométrie revocable.

On rappelle la configuration de la base de données :
- 100 utilisateurs,
- 1 empreinte de référence par utilisateur,
- 7 autres empreintes de test par utilisateur.

Nous nous intéressons d'abord aux attaques connues mais nous adoptons une approche originale pour quantifier leur impact opérationnel. Pour ces attaques, si on se place du point de vue de l'intrus, la donnée pertinente est le taux de faux rejet, i.e. le FRR, en fonction du seuil. En effet, étant donné le BioCode référence d'un utilisateur légitime, l'attaquant aura pour objectif de générer un BioCode admissible à partir de différentes connaissances à disposition (aléa, FingerCode..). On suppose que le système est paramétré pour avoir les meilleures performances soit un EER à 0% et donc un seuil à 0.32 dans notre cas. L'attaquant a donc comme objectif de générer un BioCode dont la distance avec le BioCode de référence est inférieure à 0.32.

***Test 3 :* Attaque par force brute**

Pour ce test, on suppose que l'intrus ne connaît ni le FingerCode, ni l'aléa. Dans ce contexte, l'attaquant ne dispose d'aucune information hormis la taille du BioCode binaire à présenter. On pourrait croire que ce scénario est le pire des cas mais nous verrons par la suite qu'il n'en est rien. On compare donc des BioCodes générés aléatoirement (avec un FingerCode aléatoire et un aléa différent à chaque fois) aux BioCodes authentiques. La figure 5 illustre les résultats obtenus par comparaison de l'évolution du FRR du BioCode original et du FRR de l'attaque par force brute. On constate bien que cette attaque est inopérationnelle la plupart du temps dans la mesure la valeur du FRR pour l'attaque vaut presque toujours 1 pour un seuil opérationnel du système fixé à 0.32 (par hypothèse). Il y a cependant une zone très limitée (dépendant de la valeur du seuil) pour laquelle la valeur du FRR est différente de 1 rendant cette attaque possible mais peu probable. Nous évaluons cette possibilité d'attaque par la valeur $1 - FRR$ pour le seuil opérationnel de 0.32. Le risque dans ce cas vaut 0.14%.

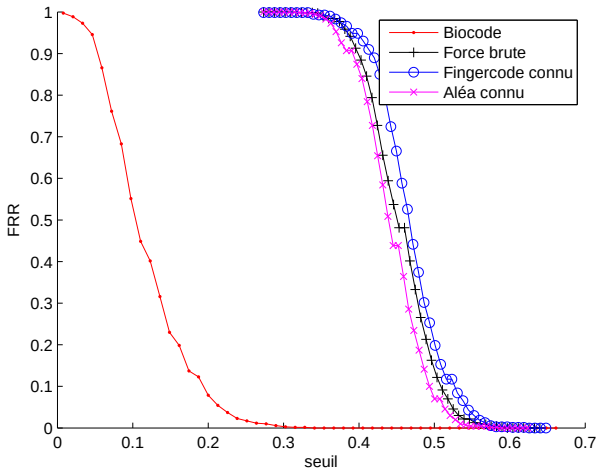


FIGURE 5. Analyse de la robustesse du BioHashing face aux attaques (force brute, capture du fingercode, capture de l'aléa)

***Test 4 :* FingerCode connu**

Pour ce test, on suppose que l'intrus a récupéré une empreinte parmi les 800 de la base de données, et cherche

à se faire reconnaître par le système comme un utilisateur autorisé. L'intrus a donc à sa disposition un FingerCode, et il génère un BioCode avec un aléa différent de celui du BioCode de référence. La figure 5 illustre les résultats de l'attaque avec FingerCode connu. Encore une fois, cette attaque est en général inopérante pour le paramétrage du système. Le risque d'attaque constaté est de 0.14%, il est à noter qu'il équivalent à l'attaque précédente. Ceci montre que la connaissance du fingercode n'est pas significative pour la réalisation d'une attaque (par rapport à l'absence d'information).

***Test 5 :* Aléa connu**

Pour ce test, l'intrus dispose de l'aléa (il a par exemple volé le token), mais pas du FingerCode. Le BioCode va donc être généré avec un FingerCode aléatoire. Pour ce test uniquement, l'aléa est le même pour tous les BioCodes de la base de données. La figure 5 illustre les résultats de ce test. Nous mettons encore une fois en évidence l'inefficacité globale de cette attaque. On montre toutefois que le risque associé est de 0.28% soit deux fois supérieur aux deux attaques précédentes. Ce test met en évidence l'importance de stocker de façon sécurisée cet aléa.

***Test 6 :* attaque personnelle par écoute de N BioCodes**

Les attaques précédentes sont des attaques que l'on peut trouver dans la littérature. On va présenter maintenant un type d'attaques qui, à la connaissance des auteurs, n'a jamais fait l'objet d'une publication. Il s'agit d'attaques adaptées au caractère révocable du BioHashing : on suppose qu'un intrus a intercepté N BioCodes distincts du même utilisateur $\{B_1, .., B_N\}$. On génère alors, sur la base de ces N écoutes, un BioCode dont les bits sont fixés à la valeur (0 ou 1) la plus probable statistiquement. Les tests qui suivent vont permettre d'analyser si le BioCode frauduleux contient suffisamment d'information pour se faire accepter comme BioCode véritable. On teste plusieurs valeurs possibles pour N : $N = 3$, $N = 11$.

On va regarder deux interprétations possibles de ces attaques par écoute du BioCode : d'une part, on va s'intéresser comme précédemment au FRR pour analyser si un intrus peut se faire passer pour un individu précis. On parlera dans ce cas d'une attaque *personnelle*. D'autre part, l'intrus peut se contenter de se faire passer pour l'un des cent utilisateurs autorisés de la base de données : dans ce cas, c'est la courbe ROC qu'il faut tracer, et on s'intéressera à l'EER pour analyser cette attaque *globale*.

Pour ce test, on suppose que l'intrus dispose de 3 ou 11 BioCodes (interceptés après révocation). La figure 6 montre que le système est résistant à l'attaque personnelle par écoute. On peut remarquer qu'entre $N = 3$ et $N = 11$, l'attaque ne progresse pas beaucoup. Ceci se traduit par un risque d'attaque de 0.06% pour $N = 3$ et de 0.16% pour $N = 11$. La valeur du risque montre que l'attaque par écoute n'est pas l'approche la plus efficace pour l'attaquant (il vaut mieux subtiliser l'aléa de l'individu). Il est évident que cette attaque va se révéler plus efficace pour des valeurs de N plus grandes même si d'un point de vue opérationnel, cette attaque est moins facile à réaliser.

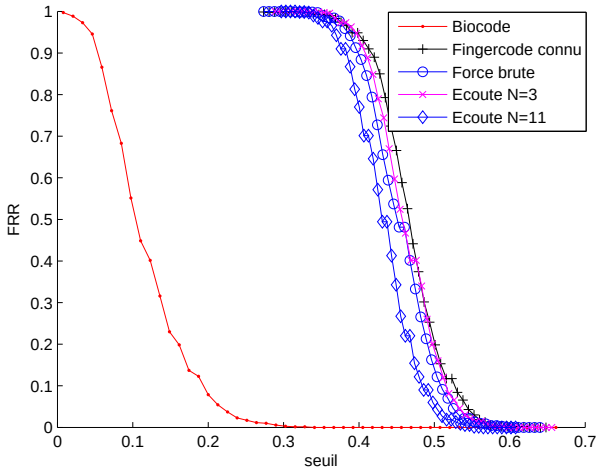


FIGURE 6. Analyse de la robustesse du BioHashing face aux attaques par écoute de N BioCodes

***Test 7 :* Attaque globale**

Une autre attaque à envisager est l'attaque globale définie plus haut : l'intrus peut se contenter de se faire accepter par le système comme l'un des 100 utilisateurs autorisés. Les courbes ROC tracées à la figure 7 dans les cas $N = 3$ et $N = 11$, et en particulier, les EER égaux à 0.5 montrent qu'un intrus a de fortes chances de pouvoir se faire accepter par le système, mais sans savoir de quel utilisateur il usurpe l'identité. En reprenant les attaques précédentes de force brute ou d'interception d'un fingercode, on obtient la même conclusion à savoir une attaque opérationnelle.

D. Synthèse

Nous présentons ici une synthèse des attaques réalisées et leur efficacité. Dans le cas d'une attaque personnelle, tous les scénarios ont permis de mettre en évidence une faille du système biométrique révocable avec un risque d'attaque faible. Le tableau I donne la valeur du risque des différents scénarios. Ceci permet également de dresser un classement de l'efficacité des attaques de ce type de sytème. On peut constater que l'attaque la plus efficace est celle consistant à voler l'aléa d'un individu. Cette attaque a malgré tout un risque faible de 0.28%.

Dans le cas d'une attaque globale, les attaques sont opérationnelles et posent des problèmes de protection de

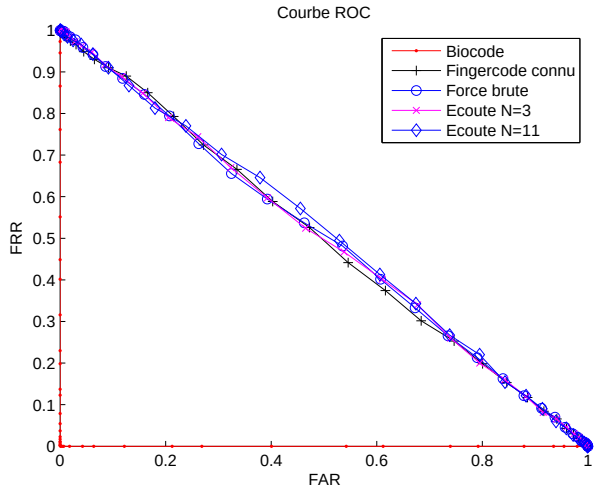


FIGURE 7. Attaque globale par écoute de N BioCodes

Force brute	Fingercode connu	Aléa connu	3 écoutes	11 écoutes
0.14%	0.14%	0.28%	0.06%	0.16%

TABLE I
VALEUR DU RISQUE D'ATTAQUE (1-FRR) POUR UN SYSTÈME BIOMÉTRIQUE RÉVOCABLE PARAMÉTRÉ AVEC LE SEUIL PERMETTANT UN EER À 0% EN MODE OPÉRATIONNEL (SANS ATTAQUE)

la vie privée. Dans ce type d'attaque, l'attaquant ne peut pas prédire à qui il va être identifié.

V. CONCLUSION

La biométrie révocable est enjeu majeur à l'heure actuelle. Malgré une recherche active ces dernières années dans la proposition de schémas de protection de données biométriques, peu d'études se sont focalisées sur la sécurité et la robustesse des protocoles. Ceci est pourtant essentiel dans un domaine comme la biométrie qui concerne la manipulation de données très sensibles. La principale contribution de cet article est de proposer une démarche expérimentale d'analyse de la robustesse de ces algorithmes dans différents scénarios. Ce travail a été réalisé sur un protocole populaire en biométrie révocable sur une base significative d'empreintes digitales de la littérature. L'étude proposée a montré une bonne robustesse du schéma dans un contexte d'usurpation d'identité. Le risque identifié pour l'attaque la plus sévère n'est que de 0.28%. Il a été également montré qu'un attaquant est en mesure de générer assez facilement un BioCode admissible par le système d'identification montrant une faille importante de ce type de protection.

Les perspectives de cette étude sont l'élaboration d'attaques plus complexes pour la partie usurpation d'identité. Des pistes concernant l'analyse de la répartition des bits du BioCode sont à l'étude pour définir des heuristiques de recherche pour la génération d'attaques d'usurpation d'identité.

RÉFÉRENCES

[BHR10] R. Belguechi, B. Hemery, and C. Rosenbergern. Authentification révocable pour la vérification basée texture d'empreintes digitales. In *Congrès Francophone en Reconnaissance des Formes et Intelligence Artificielle (RFIA*, 2010.

[CKL03] T.C. Clancy, N. Kiyavash, and D. J. Lin. Secure smartcard-based fingerprint authentication. In *ACM Multimedia, Biometrics Methods and Applications Workshop*, pages 45–52, 2003.

[CTGN04] T. Connie, A. Teoh, M. Goh, and D. Ngo. Palmhashing : a novel approach for dualfactor authentication. *Pattern analysis application*, 7 :255–268, 2004.

[DFM98] G.I. Davida, Y. Frankel, and B. J. Matt. On enabling secure applications through off-line biometric identification. In *IEEE Symposium on Security and Privacy*, pages 148–157, 1998.

[DG99] S. Dasgupta and A. Gupta. An elementary proof of the Johnson-Lindenstrauss Lemma, 1999. UTechnical Report TR-99-006, International Computer Science Institute, Berkeley, CA.

[INC06] Study report on biometrics in e-authentication, 2006. Technical Report M1/06-0693, International Committee for Information Technology Standards.

[JS02] A. Juels and M. Sudan. A fuzzy vault scheme. In *IEEE International Symposium on Information Theory*, page 408, 2002.

[JW99] A. Juels and M. Wattenberg. A fuzzy commitment scheme. In *6th ACM Conf. Computer and Comm. Security*, pages 28–36, 1999.

[LN07] A. Lumini and L. Nanni. An improved biohashing for human authentication. *Pattern Recognition*, 40 :1057–1065, 2007.

[LYC+09] P. Li, X.Y. Yang, K. Cao, S. Peng, and J. Tian. *Security-Enhanced Fuzzy Fingerprint Vault Based on Minutiae's Local Ridge Information*, volume 5558 of *Lecture Notes in Computer Science*. Springer Berlin / Heidelberg, 2009.

[MMJP03] D. Maltoni, D. Maio, A.K. Jain, and S. Prabhakar. *Handbook of Fingerprint Recognition*. Springer, 2003.

[NNJ09] A. Nagar, K. Nandakumar, and A.K. Jain. A hybrid biometric cryptosystem for securing fingerprint minutiae templates. *Pattern Recognition Letters*, 33(8) :733–741, 2009.

[O'G03] L. O'Gorman. Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE*, 91(12) :2021 – 2040, 2003.

[RCB01] N.K. Ratha, J.H. Connelle, and R. Bolle. Enhancing security and privacy in biometrics-based authentication system. *IBM Systems J.*, 37(11) :2245–2255, 2001.

[RCCB07] N.K. Ratha, S. Chikkerur, J.H. Connell, and R.M. Bolle. Generating cancelable fingerprint templates. *IEEE Trans. Pattern Anal. Mach. Intell.*, 29(4) :561–572, 2007.

[SB07] W. Scheirer and T. Boult. Cracking fuzzy vaults and biometric encryption. In *Proc. of Biometrics Symposium*, 2007.

[TNG04] A.B.J. Teoh, D. Ngo, and A. Goh. Biohashing : two factor authentication featuring fingerprint data and tokenised random number. *Pattern recognition*, 40, 2004.

[UJ06] U. Uludag and A.K. Jain. Securing fingerprint template : fuzzy vault with helper data. In *Computer Vision and Pattern Recognition Workshop*, 2006.