Authentification multi-biométrique sur mobile respectueuse de la vie privée

Alexandre Ninassi, Sylvain Vernois, Christophe Rosenberger

Authentification multi-biométrique sur mobile respectueuse de la vie privée

A. Ninassi S. Vernois C. Rosenberger

Normandie Univ, UNICAEN, ENSICAEN, CNRS, GREYC, 14000 Caen, France
{alexandre.ninassi, sylvain.vernois, christophe.rosenberger}@ensicaen.fr

Résumé

Les smartphones sont de plus en plus utilisés pour différents services numériques tels que les réseaux sociaux ou le commerce électronique. L'authentification de l'utilisateur avec des mots de passe sur ces appareils n'est pas conviviale et n'offre pas un niveau de sécurité élevé de l'utilisateur. La biométrie devient une solution populaire pour atteindre cet objectif avec notamment l'intégration de capteurs d'empreintes digitales dans les smartphones. Dans cet article, nous proposons un nouveau protocole combinant l'empreinte digitale et une biométrie comportementale pour améliorer la sécurité de l'authentification des utilisateurs tout en préservant la facilité d'usage et le respect de la vie privée. Le comportement lors de la saisie d'une authentification d'un motif sur l'écran tactile du smartphone est considéré comme une solution rapide et simple d'usage. Nous pensons que la solution proposée offre de nombreux avantages en termes de sécurité, d'usage et de respect de la vie privée. Nous montrons au travers des résultats expérimentaux l'efficacité de la méthode proposée même en cas d'attaque.

Mots clefs

Authentification, biométrie révocable, multi-biométrie.

1 Introduction

Un sondage récent en 2016 [1] a montré que plus de 50% des utilisateurs de smartphones l'utilisent immédiatement après leur réveil. À mesure qu'un smartphone intègre de plus en plus d'informations personnelles (contacts, contenu du courrier, média ...) et est utilisé comme périphérique privilégié pour accéder à des services distants, une authentification forte de l'utilisateur devient nécessaire. L'authentification par code PIN est une solution simple, néanmoins, elle ne constitue pas une preuve d'identité solide car facile à contourner. Afin de résoudre ce problème, la biométrie est de plus en plus utilisée pour augmenter le niveau de confiance de l'authentification des utilisateurs. Néanmoins, les données biométriques sont sensibles et nécessitent une attention particulière en termes de sécurité et de respect de la vie privée. La protection des données biométriques doit être réalisée pendant le cycle de vie des données, du stockage à la manipulation. La cryptographie standard n'est pas en mesure d'assurer la protection des données lors de l'étape de comparaison (déchiffrement nécessaire). Plusieurs solutions sont proposées dans la littérature pour assurer la protection des données biométriques dont les algorithmes de crypto-biométrie [2, 3] ou les algorithmes de transformation [4, 5]. Pour plus de détails sur ces schémas, nous renvoyons le lecteur à ce papier [6].

En général, une authentification biométrique se réalise en deux étapes : l'enrôlement et vérification. La première consiste à générer la référence biométrique d'un utilisateur et à la stocker. Au cours de la vérification, une capture biométrique est comparée à la référence biométrique de l'individu présumé pour décision. Afin d'améliorer la sécurité de l'authentification des utilisateurs, il faut généralement combiner différents facteurs d'authentification. Cela peut être réalisé en utilisant différentes données biométriques pour définir un système multi-biométrique.

La principale contribution de cet article est de proposer un système multi-biométrique efficace et utilisable pour améliorer la sécurité de l'authentification des utilisateurs sur les smartphones. Nous combinons deux modalités biométriques, à savoir l'empreinte digitale et une biométrie comportementale. Nous supposons dans ce travail que le smartphone utilisé possède un capteur d'empreintes digitales. Cette hypothèse est réaliste car une enquête récente estime que 67% des smartphones en 2018 disposeront d'un capteur d'empreintes digitales [7]. L'empreinte digitale de référence de l'individu est stockée dans un élément sécurisé du smartphone pour en assurer sa protection. Nous utilisons également une modalité biométrique comportementale (façon de saisir un motif sur un écran tactile) avec un schéma de protection du modèle. Cette solution présente l'avantage d'être très simple à utiliser et très rapide. La référence biométrique est stockée dans le smartphone protégée sous la forme d'un BioCode (code binaire lié à la donnée biométrique) révocable en cas d'attaque.

Ce papier est organisé comme suit. La section 2 fournit un

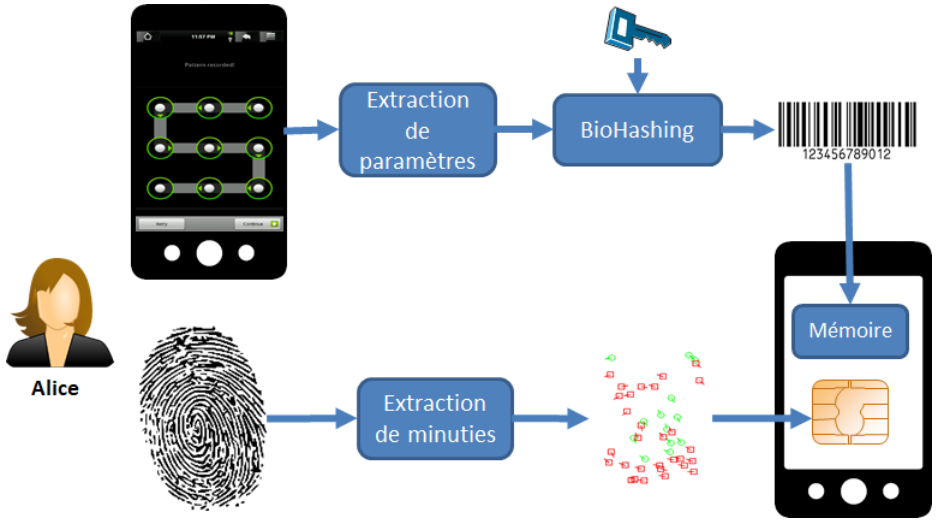

Figure 1 – *Enrôlement d'Alice*

bref état de l'art sur les solutions existantes pour l'authentification des utilisateurs sur un smartphone. La méthode proposée est décrite dans la section 3. La section 4 illustre la performance de la solution proposée à partir de résultats expérimentaux. Enfin, nous concluons et donnons des perspectives dans la section 5.

2 Travaux antérieurs

L'authentification biométrique sur mobile est un problème émergent, avec des références relativement croissantes. Un rapport du NIST [8] propose plusieurs recommandations concernant l'acquisition de données biométriques sur un smartphone et considère les modalités suivantes : l'empreinte digitale, le visage et l'iris. La plupart des papiers de la littérature sont consacrés à une modalité particulière. On peut citer par exemple les références [9, 10] sur la reconnaissance du locuteur. Plusieurs articles [11, 12] traitent de la reconnaissance basée sur la dynamique de frappe. De nombreux articles proposent d'utiliser l'écran tactile pour capturer des données biométriques [13]. La plupart de ces études utilisent des méthodes utilisées pour la dynamique de frappe au clavier ou de signature. Par exemple, la notion de TapPrint a été proposée par Miluzzo et al. [14] où la notion de dynamique de frappe est généralisée à l'écran tactile. La méthode proposée est basée sur le comportement de saisie d'un texte sur un écran tactile et exploite des informations de l'accéléromètre du smartphone. L'efficacité de la reconnaissance est comprise entre 80% et 90%. Le travail réalisé par Luca et al. [15] est très intéressant car il combine le mot de passe à base de motif et la biométrie. Ils ont proposé un système et l'ont testé avec 34 utilisateurs. Ils ont obtenu une performance de 19% pour la valeur FRR (faux taux de rejet) et 21 % pour le FAR (Fausse Acceptation). En 2013, une méthode a été proposée [16] combinant plusieurs informations avec le facteur de corrélation ou la DTW comme méthode de mesure de similarité. Le taux d'erreur égal (EER) est proche de 17 %.

Outre la littérature consacrée aux solutions biométriques pour l'authentification sur mobile liées à une modalité spécifique, plusieurs articles ou thèses récents proposent un aperçu complet du sujet [17, 18]. Même si l'utilisation de plusieurs modalités biométriques permet de limiter le taux d'erreur (notamment le taux de fausse acceptation), l'utilisation de données biométriques supplémentaires pose le problème de la protection de la vie privée. Peu de contributions considèrent ce problème sur un mobile. Nous proposons dans ce papier une nouvelle solution d'authentification combinant l'empreinte digitale et une modalité comportementale. La première modalité est présente dans la plupart des smartphones et le modèle de référence biométrique est stocké en toute sécurité dans un élément sécurisé. L'utilisation de l'approche comportementale permet d'améliorer le niveau de sécurité tout en fournissant une solution d'authentification pratique (interaction rapide) et facile à protéger.

3 Méthode proposée

Le principe général de la méthode proposée est donné par les figures 1 et 2. Pendant la phase d'enrôlement, Alice doit fournir son empreinte digitale au capteur du smartphone pour générer son template de référence. Le modèle calculé (ensemble des minuties détectées) est stocké sur un élément sécurisé dédié. Alice doit également entrer un chemin secret sur l'écran tactile. L'application calcule plusieurs paramètres en fonction de son comportement de saisie (vitesse, pression, façon de tenir le smartphone). Nous utilisons ensuite l'algorithme de BioHashing pour protéger ce modèle. Pour cet algorithme, nous avons besoin d'une clé secrète pour pouvoir révoquer le BioCode généré en cas d'attaque. Cette clé secrète peut

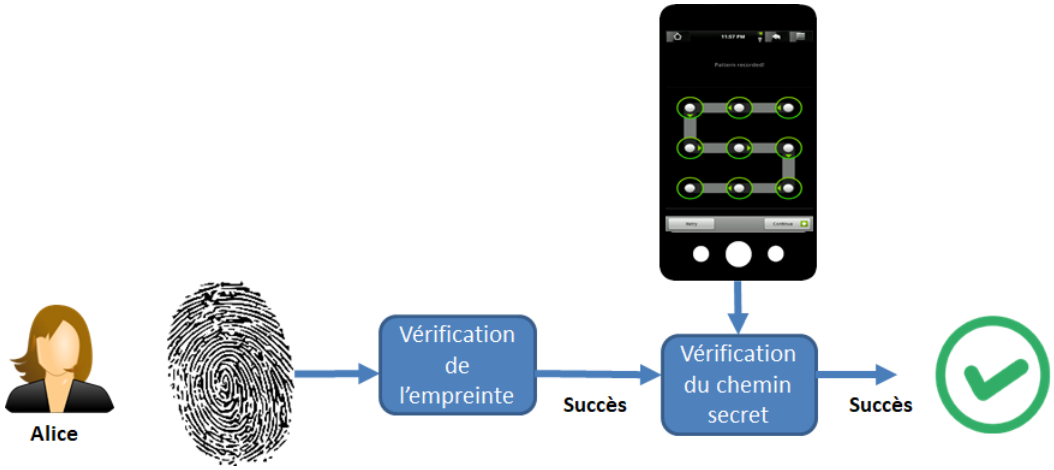

Figure 2 – *Vérification multi-biométrique*

être une représentation binaire du chemin dessiné et peut être concaténée avec d'autres informations telles que le numéro IMEI du smartphone (identifiant du mobile), le nom d'Alice, une valeur aléatoire ...

Au cours de la phase de vérification, Alice doit fournir son empreinte digitale pour s'authentifier. L'empreinte digitale capturée est comparée à la référence d'Alice stockée dans l'élément sécurisé du smartphone. Si son identité est vérifiée, elle doit entrer le motif sur l'écran tactile. Un BioCode est calculé et comparé au BioCode de référence d'Alice dans le smartphone. Si les deux systèmes biométriques acceptent la preuve d'Alice, elle est authentifiée. Nous sommes ici dans un cas de fusion de décision (n'ayant pas accès au score de comparaison de l'algorithme de comparaison des empreintes digitales).

3.1 Vérification de l'empreinte digitale

Nous proposons d'utiliser dans cet article l'empreinte digitale comme première modalité biométrique. La plupart des smartphones intègrent un capteur d'empreinte digitale. Alice doit s'enrôler en fournissant une ou plusieurs captures de son empreinte digitale. Le modèle de référence (un ensemble de minuties) est stocké dans l'élément sécurisé (SE) associé au smartphone ou au matériel du capteur d'empreintes digitales. La comparaison entre une nouvelle capture d'empreinte digitale et le modèle de référence d'Alice est également réalisée en SE et une valeur de décision est fournie (le score n'est pas disponible pour des raisons de sécurité).

Concernant le respect de la vie privée, cette solution est appropriée, la référence biométrique est stockée dans le SE. En terme de sécurité, la solution est intéressante même si le processus d'enrôlement est réalisé par l'utilisateur sans aucun contrôle. Nous pouvons nous attendre à ce qu'un smartphone soit un objet personnel, le processus d'enrôlement devrait être effectué par le propriétaire du smartphone (Alice dans ce cas). En ce qui concerne la performance, il est décrit par la valeur du taux de Fausse acceptation (FAR) correspondant au pourcentage d'attaques réussies par un imposteur. Pour les smartphones, le niveau ciblé du FAR est de 0.005% [19], correspondant au niveau de sécurité 3. Il est difficile de vérifier cette valeur sans le score fourni par l'algorithme correspondant. Le taux de faux rejet associé (FRR) correspondant aux problèmes de reconnaissance des utilisateurs légitimes est censé être inférieur à 2 $\%$. Aucune étude n'existe dans l'état de l'art sur l'évaluation des capteurs commerciaux d'empreintes digitales sur smartphones. La raison est qu'il faudrait avoir un nombre d'utilisateurs très important pour fournir des résultats significatifs.

3.2 Chemin secret biométrique

Le système biométrique que nous proposons d'utiliser dans cette étude a pour but d'accroître la sécurité pour un contrôle d'accès logique rapide sur un smartphone. Nous proposons de reconnaître l'utilisateur par la connaissance d'un mot de passe représenté par un chemin secret. Cette approche pour entrer un mot de passe est plus rapide et plus conviviale pour un appareil mobile. Deuxièmement, le comportement de l'utilisateur lors de la saisie du chemin est analysé. De nombreuses informations peuvent être collectées lors du processus de capture :

- Position X : la position horizontale du doigt sur l'écran tactile est enregistrée pendant la capture,
- Position Y : la position verticale du doigt sur l'écran tactile est également enregistrée,
- Pression : la pression du doigt sur l'écran tactile est capturée (fournie par le système d'exploitation),
- Taille du doigt : nombre de pixels où le doigt est en contact avec l'écran tactile,
- Accéléromètres : trois angles correspondant à l'orientation du smartphone.

Dans cette étude, nous n'avons utilisé que les informations

de position X et Y en calculant également la dérivée première et seconde de chaque signal. Comme le temps nécessaire pour dessiner le même chemin peut être différent pour chaque capture, les signaux sont sous-échantillonnés à une longueur fixe. Une description de taille constante est nécessaire pour utiliser ce modèle comme entrée pour l'algorithme de BioHashing que nous détaillons dans la section suivante.

3.3 Protection par BioHashing

L'algorithme Biohashing est appliqué aux données biométriques représentées par un vecteur à valeur réelle de longueur fixe et génère un modèle binaire appelé BioCode de longueur inférieure ou égale à la taille d'origine. Cet algorithme a été initialement proposé pour le visage et les empreintes digitales par Teoh *et al.* dans [4]. L'algorithme de biohashing peut être appliqué sur toutes les modalités biométriques, qui peuvent être représentées par un vecteur de valeurs réelles de longueur fixe. Cette transformation nécessite un secret lié à l'utilisateur. La comparaison des BioCodes est réalisée par le calcul de la distance de Hamming. L'algorithme de Biohashing transforme le modèle biométrique $T = (T_1, \dots T_n)$ dans un modèle binaire appelé BioCode $B = (B_1, \dots B_m)$, avec $m \leq n$, comme suit :

1. m vecteurs aléatoires orthonormés $V_1, \dots, V_m$ de la longueur n sont générés à partir d'un secret servant de germe du tirage aléatoire (typiquement avec l'algorithme de Gram Schmidt).
2. Pour $i = 1, \dots, m$, calcul du produit scalaire $x_i =< T, V_i >$.
3. Calcul du BioCode $B = (B_1, \dots, B_m)$ avec le processus de quantification :

$$B_i = \begin{cases} 0 & \text{si} \quad x_i < \tau \\ 1 & \text{si} \quad x_i \geq \tau, \end{cases}$$

Où τ est un seuil donné, généralement égal à 0.

La performance de cet algorithme est assurée par le produit scalaire avec les vecteurs orthonormés, comme c'est détaillé dans [20]. Le processus de quantification garantit la non-inversibilité des données (même si $n = m$), car chaque coordonnée de l'entrée T est une valeur réelle, alors que le BioCode B est binaire. Enfin, le germe aléatoire garantit la diversité et les propriétés de révocabilité.

4 Validation du système

Dans cette section, nous présentons des résultats expérimentaux pour la validation du système proposé.

4.1 Protocole

Nous détaillons le protocole que nous avons suivi dans cette étude. Dans ce travail, nous avons d'abord utilisé un ensemble de données biométriques capturées lorsque les utilisateurs dessinent un seul chemin. Les données ont été collectées sur un téléphone portable Nexus 4 avec un écran tactile d'une résolution de 800 x 1280 pixels. Le motif était le même pour tous les utilisateurs et est défini par le code de modèle suivant "1235987". Cette configuration expérimentale peut être considérée comme le pire cas où un attaquant connaît le modèle à dessiner. 34 utilisateurs ont participé à cette expérience et chaque utilisateur a fourni 15 échantillons décrits par 8 signaux sous-échantillonnés à 200 valeurs (normalisation du temps), nous avons utilisé la première et la deuxième dérivée des signaux X et Y. Nous avons également ajouté le temps total pour dessiner le chemin secret. Ainsi, la taille du modèle biométrique comportemental est 1601 (en concaténant tous les signaux sous-échantillonnés et le temps de saisie). Au total, nous avons un sous-ensemble de $34\ fois 15 = 510$ captures biométriques de taille 1601 à valeurs réelles pour le modèle biométrique. Compte tenu de la configuration du BioHashing, nous définissons les valeurs des paramètres comme suit :

- Taille des paramètres d'entrée : n = 1601,
- Taille du BioCode : m = 750 (choix arbitraire, il faut $m < n$ pour garantir la non inversibilité),
- Comme le chemin est le même pour tous les utilisateurs, dans le calcul du BioCode de référence, le code de motif est défini sur "1235987" pour tous les utilisateurs,
- Algorithme de comparaison : distance de Hamming.

En ce qui concerne l'empreinte digitale, nous avons utilisé les bases d'empreintes digitales FVC2002 DB2, FVC2004 DB1 et FVC2004DB3 [21]. La figure 3 présente une image de chaque base de données. On peut voir que les empreintes digitales sont très différentes et représentatives des différents types d'empreintes digitales (acquises avec des capteurs utilisant différentes technologies). Ces bases de données ont des empreintes digitales de 100 individus avec 8 échantillons par personne. Afin de constituer une base chimérique de données multi-biométriques, nous avons pris en compte les empreintes digitales des 34 premiers individus. Pour chaque jeu de données FVC, nous disposons de $34 \times 8 = 272$ échantillons d'empreintes digitales.

(a) (b) (c)

Figure 3 – *Un exemple de chaque base : (a) FVC2002 DB2, (b) FVC2004 DB1, (c) FVC2004 DB3*

Afin d'évaluer la performance de la méthode proposée,

nous utilisons la méthodologie suivante. Nous utilisons le premier échantillon de chaque utilisateur comme modèle de référence, pour le chemin secret, nous utilisons ces données pour calculer le *BioCode de Référence*. Comme nous n'avons pas accès au matériel du capteur d'empreinte digitale (c'est-à-dire la valeur du score correspondant), nous simulons le résultat du score en considérant l'algorithme Bozorth3 fourni par le NIST [22]. Cet algorithme ne fournit pas une performance équivalente aux algorithmes de comparaison commerciale (OCC), la performance est donc sous-estimée. Nous calculons les résultats légitimes comme suit. Nous considérons toutes les empreintes de référence et nous les comparons avec chaque échantillon disponible appartenant au même individu. Nous considérons deux fois ces scores parce que le modèle biométrique comporte 14 échantillons. Pour le chemin secret biométrique, nous comparons le Biocode de référence avec tous les autres BioCodes du même individu. Nous obtenons $14 \times 34 = 476$ scores légitimes pour chaque base de données FVC. Nous avons un processus similaire pour simuler une attaque d'imposteur en considérant tous les échantillons biométriques appartenant à un autre utilisateur. Nous obtenons $14 \times 34 \times 33 = 15708$ scores d'imposture pour chaque base de données FVC. Compte tenu de ces deux ensembles de scores, nous pouvons calculer leur distribution afin d'estimer dans quelle mesure les scores des imposteurs sont différents des légitimes. Deuxièmement, nous calculons la valeur du taux d'erreur égal (EER) qui est une mesure bien connue en biométrie qui mesure le comportement du système biométrique lorsque le seuil de décision est configuré pour avoir le même nombre du taux de faux rejetés et les faux acceptés.

4.2 Résultats

Tout d'abord, nous essayons d'estimer l'efficacité de chaque système biométrique que nous combinons. La figure 4 fournit les courbes DET (de l'anglais Detection Error Trade Off)) du système d'empreintes digitales sur les trois bases de données. La valeur EER est entre 5,2 % et 8 %. Nous pourrions nous attendre en utilisant un système commercial une performance nettement meilleure, cette valeur estime une borne supérieure de l'erreur. En ce qui concerne la performance de reconnaissance par le chemin secret biométrique, avec une simple distance euclidienne, nous obtenons un EER de 27.4 %. En appliquant le BioHashing dans le meilleur des cas (secret seulement connu par l'utilisateur légitime), nous obtenons une reconnaissance parfaite avec une valeur EER de 0 % (voir Figure 5). Dans le pire des cas (secret connu par l'imposteur), la performance est similaire à celle obtenue sans protection.

La figure 6 fournit la distribution du score en combinant l'empreinte digitale et le chemin de secret biométrique dans le meilleur scénario. Nous obtenons pour chacun une reconnaissance parfaite pour toutes les bases de données d'empreintes digitales. C'est évidemment un excellent ré-

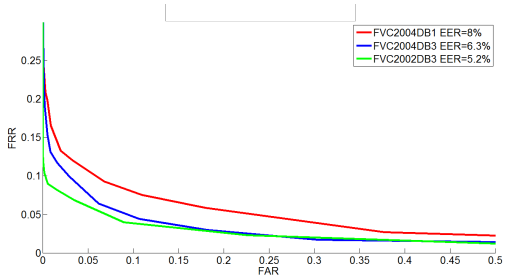

Figure 4 – *Courbe DET de la performance de la reconnaissance d'empreintes digitales sur les 3 bases FVC avec Bozorth3 comme algorithme de comparaison.*

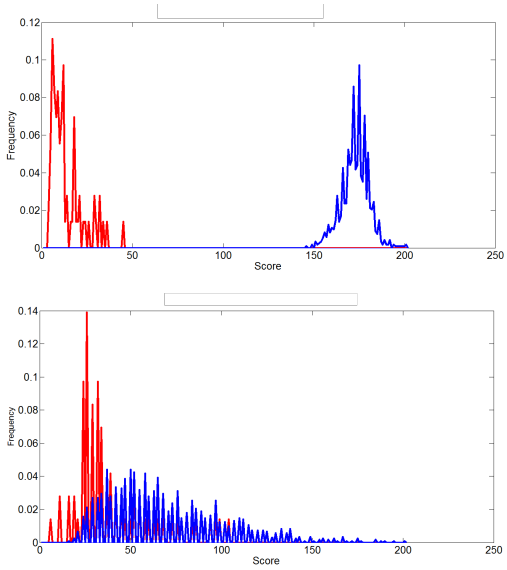

Figure 5 – *Distribution des scores après protection (haut) sans attaque, (bas) secret connu.*

sultat et améliore les résultats en appliquant uniquement le système d'empreinte digitale (voir Figure 4).
Maintenant, nous devons considérer le scénario du pire des cas lorsque l'imposteur a obtenu le secret associé à l'algorithme de BioHashing. Nous supposons que le seuil fixé pour le système d'empreinte digitale est celui associé à la valeur EER (il pourrait être plus strict). Par exemple, pour la FVC2004DB1, nous obtenons un FAR égal à 8 %. Nous fixons la valeur de seuil pour le chemin secret biométrique avec la même approche. Nous avons calculé le taux de fausse acceptation dans le pire des cas et il vaut 28.7%. Cela signifie que si l'imposteur connaît le secret, il a 28.7% de chance de casser le système. En considérant le système multi-biométrique, il a 8% chances de casser le système d'empreinte digitale (sur FVC2004DB1) et 28.7 % pour le chemin secret biométrique. Comme ces événements sont indépendants, nous pouvons estimer le taux de fausse acceptation (FAR) du système multi-biométrique sur FVC2004DB1 à $8\% \times 28.7\% = 2.3\%$. Pour tous les ensembles de données d'empreinte digitale, le FAR est entre

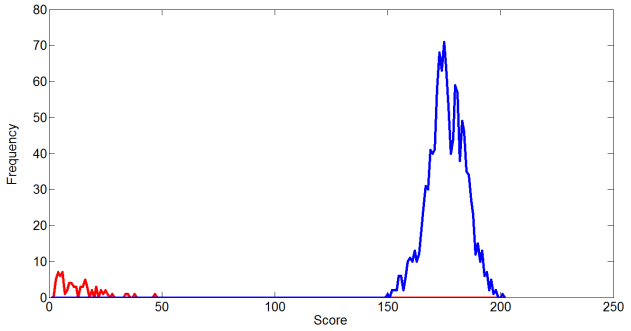

Figure 6 – *Distribution des scores du système multi-biométrique sur la base 2002DB3.*

1.5 % à 2.3 % pour le système multi-biométrique si l'imposteur connaît le chemin secret et le secret. Nous pouvons considérer ce résultat comme très intéressant compte tenu de toutes les informations nécessaires à l'imposteur pour cette attaque (possession temporaire du téléphone, fourniture d'une empreinte digitale proche de celle de l'utilisateur légitime, connaissance du chemin secret, fourniture d'une saisie du chemin proche de celle de l'utilisateur légitime).

5 Conclusion et perspectives

Dans cet article, nous proposons un système multi-biométrique d'authentification pour smartphones en combinant la reconnaissance de l'empreinte digitale à l'aide de son capteur intégré et d'un système biométrique comportemental. Le système proposé est très rapide et simple d'usage pour les utilisateurs car tous ces systèmes de vérification sont couramment utilisés. L'utilisation de la reconnaissance de l'empreinte digitale permet de limiter l'attaque possible du chemin secret lorsque le secret associé à l'algorithme BioHashing est obtenu par l'imposteur. L'utilisation du second système biométrique permet d'augmenter la sécurité de l'authentification des utilisateurs. Dans le meilleur des cas, nous obtenons une reconnaissance parfaite sur les bases de données testées et un taux de fausse acceptation inférieur à 2.3% dans le pire des cas (l'imposteur doit avoir accès au smartphone, connaît le chemin secret et la clé secrète associée à l'algorithme BioHashing).

Nous avons l'intention, à l'avenir, d'intégrer d'autres systèmes biométriques tels que les systèmes de reconnaissance vocale et faciale.

Remerciements

Les auteurs souhaitent remercier la société United Biometrics pour son soutien financier.

Références

[1] Ramona Sukhraj. 31 mobile marketing statistics to help you plan for 2017, 2016.

[2] H. Chabanne, J. Bringer, G. Cohen, B. Kindarji, et G. Zemor. Optimal iris fuzzy sketches. Dans *IEEE first conference on biometrics BTAS*, 2007.

[3] M. Barni, T. Bianchi, D. Catalano, M. Di Raimondo, R. Donida Labati, P. Failla, D. Fiore, R. Lazzeretti, V. Piuri, A. Piva, et Fabio Scotti. A privacy-compliant fingerprint recognition system based on homomorphic encryption and fingercode templates. Dans *BTAS 2010*, 2010.

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

[5] A. Nagar, K. Nandakumar, et A. K. Jain. Biometric template transformation : A security analysis. *Proceedings of SPIE, Electronic Imaging, Media Forensics and Security XII*, 2010.

[6] C. Rathgeb et A. Uhl. A survey on biometric cryptosystems and cancelable biometrics. *EURASIP J. on Information Security*, 3, 2011.

[7] Statista. Penetration of smartphones with fingerprint sensors worldwide from 2014 to 2018, 2016.

[8] S. Orandi et R. M. McCabe. Mobile id device. best practice recommendation. NIST Special Publication 500-280, 2009. Available from : http ://www.nist.gov/itl/iad/ig/upload/MobileID-BPRS-20090825-V100.pdf.

[9] A. Kounoudes, A. Antonakoudi, V. Kekatos, et P. Peleties. Combined speech recognition and speaker verification over the fixed and mobile telephone networks. Dans *Proceedings of the 24th IASTED International Conference on Signal processing, Pattern Recognition, and Applications*, pages 228–233, 2006.

[10] A. Roy, M. Magimai.-Doss, et S. Marcel. A fast parts-based approach to speaker verification using boosted slice classifiers. *IEEE Trans. on Information Forensics and Security*, 7 :241–254, 2012.

[11] S. Hwang, S. Cho, et S. Park. Keystroke dynamics-based authentication for mobile devices. *Computer & Security*, 28 :85–93, 2009.

[12] T.-Y. Changa, C.-J. Tsaib, et J.-H. Lina. A graphical-based password keystroke dynamic authentication system for touch screen handheld mobile devices. *The Journal of Systems and Software*, 85 :1157 ?1165, 2012.

[13] N. Sae-Bae, N. Memon, et K. Isbister. Investigating multi-touch gestures as a novel biometric modality. Dans *IEEE Fifth International Conference on Biometrics : Theory, Applications and Systems (BTAS)*, 2012.

[14] E. Miluzzo, A. Varshavsky, S. Balakrishnan, et R. Choudhury. Tapprints : your finger taps have fingerprints. Dans *Proceedings of the 10th international conference on Mobile systems, applications, and services*, 2012.

[15] A. De Luca, A. Hang, F. Brudy, C. Lindner, et H. Hussmann. Touch me once and i know it's you ! : implicit authentication based on touch screen patterns. Dans *Proceedings of the 2012 ACM annual conference on Human Factors in Computing Systems*, 2012.

[16] Michael Beton, Vincent Marie, et Christophe Rosenberger. Biometric secret path for mobile user authentication : A preliminary study. Dans *Computer and Information Technology (WCCIT), 2013 World Congress on*, pages 1–6. IEEE, 2013.

[17] Abdulaziz Alzubaidi et Jugal Kalita. Authentication of smartphone users using behavioral biometrics. *IEEE Communications Surveys & Tutorials*, 18(3) :1998–2026, 2016.

[18] Attaullah Buriro. *Behavioral Biometrics for Smartphone User Authentication*. Thèse de doctorat, University of Trento, 2017.

[19] William E. Burr, Donna F. Dodson, Elaine M. Newton, Ray A. Perlner, W. Timothy Polk, Sarbari Gupta, et Emad A. Nabbus. Nist special publication 800-63-2 : Electronic authentication guideline. Rapport technique, NIST, 2013.

[20] A. B.J. Teoh, Y. W. Kuan, et S. Lee. Cancellable biometrics and annotations on biohash. *Pattern Recognition*, 41 :2034–2044, 2008.

[21] Davide Maltoni, Dario Maio, Anil Jain, et Salil Prabhakar. *Handbook of fingerprint recognition*. Springer Science & Business Media, 2009.

[22] Kenneth Ko. Users guide to export controlled distribution of nist biometric image software (nbisec). *NIST Interagency/Internal Report (NISTIR)-7391*, 2007.