Construction et analyse de passe-partout biométriques

Tanguy Gernot, Patrick Lacharme

▶ **To cite this version:**

Tanguy Gernot, Patrick Lacharme. Construction et analyse de passe-partout biométriques. Symposium sur la sécurité des technologies de l'information et des communications, Jun 2023, Rennes, France. hal-04114342

HAL Id: hal-04114342
https://hal.science/hal-04114342

Submitted on 1 Jun 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution - NonCommercial - NoDerivatives 4.0 International License

Construction et analyse de passe-partout biométriques

Tanguy Gernot et Patrick Lacharme
tanguy.gernot@unicaen.fr
patrick.lacharme@ensicaen.fr

Normandie Univ, UNICAEN, ENSICAEN, CNRS, GREYC, 14000 Caen, France

Résumé. Dans cet article, nous introduisons la notion de passe-partout biométriques afin d'usurper de nombreux individus à partir d'une même donnée. Un premier scénario décrit la construction d'un tel passe-partout depuis une fuite de données biométriques et son utilisation sur d'autres données. Un second scénario au dessein plus éthique permet à un passe-partout fixé d'usurper tout le monde. Des analyses supplémentaires montrent qu'utiliser plusieurs données biométriques minutieusement choisies d'un individu permet de conserver sa capacité d'usurpation avec ses futures données biométriques.

1 Introduction

La biométrie est une science dont l'objectif est de reconnaître des individus. Cette problématique est centrale dans notre société, notamment pour le domaine judiciaire, pour la signature de contrat, ou bien pour effectuer du contrôle d'accès.

L'objectif étant de reconnaître des individus, un schéma de reconnaissance biométrique se divise en deux étapes principales :

— La phase d'enrôlement, où un individu s'inscrit dans un système en y enregistrant ses caractéristiques biométriques de référence.
— Les phases de reconnaissance, où un individu tente d'être reconnu en fournissant de nouvelles caractéristiques biométriques, qui sont comparées à la référence enregistrée à la phase d'enrôlement.

Pour une vue générale de la biométrie, nous redirigeons le lecteur vers [10]. Il est important de noter que les captures de modalités biométriques issues d'un individu, tout comme les vecteurs de caractéristiques extraits, sont différentes d'une capture à une autre, mais espérées proches.

Ces données biométriques sont à caractère personnel et donc sensibles. C'est pourquoi de nombreux travaux s'intéressent à leur protection tout en maintenant les performances de reconnaissances. Une des techniques les plus utilisées en biométrie est l'utilisation de transformations biométriques

pour protéger ces données. Néanmoins, la sécurité de ces transformations est parfois faible et c'est cette faiblesse qui va être mise en évidence dans un premier temps avec la construction de préimages communes à de multiples données, puis dans un second temps cette faiblesse va être utilisée pour d'autres applications. Plus précisément, les travaux présentés dans cet article portent sur la construction et l'évaluation de passe-partout biométriques, permettant d'usurper l'identité de nombreux individus, c'est-à-dire être reconnu à tort comme eux.

De tels passe-partout ont de nombreuses applications, comme l'attaque de bases, la mise en place d'un système de contrôle d'accès beaucoup plus fin qu'un simple système biométrique ou encore la mise en place d'un système avec une porte dérobée.

Dans un premier temps nous présentons dans la section 2 quelques rappels sur les systèmes biométriques et leur sécurité. Ensuite, dans la section 3, nous décrivons la construction de passe-partout biométriques dans un scénario d'attaque, puis dans la section 4 dans un autre scénario, plutôt orienté contrôle d'accès. Enfin, nous conclurons ces travaux dans la section 5.

2 Sécurité des systèmes biométriques

2.1 Système biométrique

Une donnée biométrique est récupérée grâce à un capteur, généralement sous forme d'une image. Ensuite, une extraction de caractéristiques est réalisée depuis cette image. Il existe différents algorithmes d'extraction de caractéristiques, spécifiques ou non à une modalité donnée. Dans notre cas, ces caractéristiques extraites sont sous la forme d'un vecteur, dit de caractéristiques, de taille fixe à valeur réelle.

Une base de données biométriques est composée d'une ou plusieurs données de référence obtenues lors de la phase d'enrôlement pour chaque utilisateur du système et la nouvelle donnée obtenue lors de la phase de reconnaissance est comparée avec celles de la base. La qualité d'une base de données biométriques est estimée par deux taux qui évoluent en fonction du seuil utilisé : le taux de fausses acceptations, c'est-à-dire le pourcentage d'imposteurs illégitimement reconnus, et le taux de faux rejets, c'est-à-dire le pourcentage d'individus légitimes non reconnus.

Lorsque le seuil est petit, c'est-à-dire que les vecteurs doivent être très proches pour être reconnus, le taux de fausses acceptations est très faible, mais le taux de faux rejets est important. Ce cas correspond à un besoin en sécurité important. À l'inverse, lorsque le seuil est grand, et que des

vecteurs largement différents sont reconnus, alors le taux de faux rejets est très faible, mais le taux de fausses acceptations est important. Ce cas correspond à un besoin en utilisabilité important. Un intermédiaire, compromis entre sécurité et utilisabilité, est de fixer le seuil de sorte que les deux taux soient égaux : le taux d'erreurs égales.

2.2 Protection des données biométriques

Les données biométriques sont sensibles, et il ne devrait pas être possible pour un attaquant de pouvoir récupérer un vecteur de caractéristiques, voir la capture de modalité biométrique dont il est issu. En effet, les algorithmes d'extraction de caractéristiques ne sont pas conçus pour être non-inversibles ni pour assurer une quelconque sécurité des données. C'est pourquoi un tel vecteur de caractéristiques doit être protégé en un gabarit (terme proposé par la CNIL en [4, 5]). Contrairement au cas des mots de passe, où celui saisi à l'étape d'identification doit être strictement similaire à celui de l'étape d'inscription, la variabilité des données biométriques associée à leur nécessaire protection impose de nouveaux schémas de protection, robustes à cette variabilité. Elle impose aussi de fixer un seuil en dessous duquel deux vecteurs sont proches et considérés comme provenant du même individu.

Il existe de nombreux mécanismes de protection des données biométriques. Certains sont basés sur la cryptographie et d'autres utilisent des transformations plus spécifiques, comme présentées dans l'étude [17]. Une telle transformation utilise une graine, secrète ou publique, et doit respecter plusieurs propriétés telles que :

- L'indistinguabilité : un attaquant ayant volé deux gabarits ne doit pas pouvoir déterminer s'ils proviennent du même individu.
- La non-inversibilité : à partir d'un gabarit, un attaquant ne doit pas pouvoir reconstruire le vecteur de caractéristiques dont il est issu.
- Performance : la protection des données biométriques ne doit pas significativement dégrader les performances du système.

Les transformations permettant la protection des données biométriques, doivent conserver globalement les distances. Or, pour permettre une reconnaissance des individus dans l'espace transformé, tout en considérant la variabilité des données biométriques, les transformations non-inversibles ne peuvent pas simplement être des fonctions de hachage cryptographique classique comme SHA-256. En effet, il faut que la notion de proximité persiste dans l'espace transformé, ce qui n'est pas le cas pour ces fonctions de hachage.

Une version faible de la propriété de non-inversibilité considère la construction de préimage, c'est-à-dire la possibilité de construire, depuis un gabarit et sa graine, un vecteur de caractéristiques qui une fois transformé avec cette même graine donne un gabarit proche. Plusieurs travaux ont pour but de calculer des préimages sur des transformations, Par exemple, les travaux de [16] qui proposent une attaque linéaire spécifique à une transformation, appelée biohashing [18] ou encore les travaux de [11] qui utilisent un algorithme génétique sur la même transformation, décrite en section 3.2. Dans la suite de cet article, nous allons utiliser des transformations de données biométriques où nous pouvons facilement calculer des préimages pour construire des passe-partout biométriques.

3 Passe-partout sous forme d'attaque

Dans un premier temps, nous considérons un attaquant ayant corrompu une base de données biométriques, lui permettant d'avoir à sa disposition des couples gabarit/graine. Chaque couple correspond à un individu dont le vecteur de caractéristiques obtenu à l'étape d'enrôlement a été transformé avec la graine en gabarit, qui est lui stocké de manière persistante comme référence. L'objectif est de construire un unique vecteur de caractéristiques, dit passe-partout, depuis de nombreux couples gabarit/graine, qui une fois transformé avec chaque graine donne un gabarit proche de celui en entrée correspondant à la graine.

Pour construire ce passe-partout, nous utilisons une transformation (le biohashing) où il est possible de calculer des préimages, que l'on construit à l'aide d'un algorithme génétique qui s'avère beaucoup plus efficace que la force brute.

3.1 Algorithme génétique

L'objectif d'un algorithme génétique est de minimiser le retour d'une fonction d'évaluation en construisant son paramètre. En quelques mots, un algorithme génétique est inspiré de la reproduction naturelle avec une population d'individus se reproduisant et évoluant sur plusieurs générations. Pour une vue générale des algorithmes génétiques, nous redirigeons le lecteurs vers [15].

De manière plus détaillée, nous avons une population initiale qui va évoluer sur plusieurs générations, en restant de taille fixe. Dans notre cas, cette population initiale est composée de 200 individus. Chaque individu est représenté par un vecteur de caractéristiques, généré aléatoirement, par tirage borné de chaque valeur.

À chaque nouvelle génération, nous sélectionnons 100 individus de la génération précédente, qui vont être des parents reproducteurs et vont persister dans cette génération. Pour sélectionner ces parents, nous utilisons la fonction d'évaluation. Dans notre cas, un individu est évalué par la somme des distances de Hamming avec les gabarits non encore usurpés. Nous utilisons la méthode de sélection par rang, c'est-à-dire que nous sélectionnons les 100 individus ayant les plus faibles scores retournés par la fonction d'évaluation. Ces 100 individus parents vont persister dans cette nouvelle génération, qui est de taille 200 aussi. Ils vont donc se reproduire pour donner 100 individus enfants qui vont compléter cette population. Nous piochons par couple les individus parents, et chaque couple produit deux enfants. Les enfants sont des vecteurs de caractéristiques dont chaque valeur provient d'un parent ou de l'autre. Finalement, les valeurs des vecteurs enfants sont perturbées en appliquant des mutations aléatoires avec probabilité 0,1.

Pour que l'algorithme génétique fonctionne, il faut que des parents ayant de bons scores produisent des enfants ayant de bons scores. Il doit avoir une corrélation entre la proximité de deux vecteurs de caractéristiques, les individus, et leurs scores. Idéalement, la fonction d'évaluation doit être convexe.

3.2 Algorithme du biohashing

Nous allons décrire l'algorithme du biohashing. L'objectif est de transformer un vecteur de caractéristiques x de taille N en un gabarit binaire de taille M. Pour cela, nous générons depuis la graine s une matrice pseudo-aléatoire M_s de taille $N \times M$. Cette matrice est orthonormalisée avec l'algorithme de Gram-Schmidt. Elle va servir à la projection du vecteur de caractéristiques.

Soit la fonction $D : \mathbb{R}^M \to \{0,1\}^M$, permettant la binarisation par seuillage, définie par $D(t_1, \ldots, t_M) = (u_1, \ldots, u_M)$ où

$$u_i = \begin{cases} 0 & \text{si} \quad t_i < 0 \\ 1 & \text{si} \quad t_i \geq 0 \end{cases}$$

Finalement, l'algorithme du biohashing transforme le vecteur x avec la graine s par la fonction de transformation $\mathcal{T}$ définie par $\mathcal{T}(x, s) = D(xM_s)$.

Dans ces travaux, nous utilisons $N = 512$ pour les bases d'empreintes digitales et de visages, et $N = 990$ pour la base d'électrocardiogrammes. Pour les trois bases, nous utilisons $M = 128$.

3.3 Données biométriques utilisées

Les expériences ont été menées sur trois bases de données biométriques très différentes :

— LFW issue de visages [9] : l'extraction de caractéristiques est effectuée avec le réseau profond InsightFace [6]. Le taux d'erreurs égales est de 0,2%. L'utilisation des visages permet une acquisition simple par photographie, une bonne performance de reconnaissance, mais le visage évolue significativement au cours de la vie, ce qui nécessite des adaptations.

— FVC issue d'empreintes digitales [12] : l'extraction de caractéristiques est effectuée avec des filtres de Gabor [2]. Le taux d'erreurs égales est de 10%. L'utilisation d'empreintes digitales est historique, largement acceptée, et procure de bonne performance de reconnaissance tout en était globalement stable dans le temps, hors blessures.

— PTB issue d'électrocardiogrammes (ECG) [3] : l'extraction de caractéristiques est effectuée par délimitation d'ondes [13,14]. Le taux d'erreurs égales est de 11%. L'utilisation d'électrocardiogrammes est récente et permet une bonne reconnaissance des individus, mais l'acquisition est complexe et l'acceptabilité mitigée.

Pour simplifier la lecture de cet article, les différentes bases sont représentées dans les résultats par leur modalité biométrique.

3.4 Résultats des expériences

Les résultats de nos expériences de construction de passe-partout à partir de nombreux couples gabarit/graine sont donnés dans la figure 1. On y trouve pour chacune des bases de données biométriques utilisées, l'évolution de la couverture du meilleur passe-partout construit au fur et à mesure des itérations de l'algorithme génétique. La couverture d'un passe-partout correspond au pourcentage d'individus de la base qui sont usurpés par le passe-partout. Nous constatons une croissance rapide de la couverture, qui converge ensuite lentement jusqu'à environ 400 itérations dans l'algorithme génétique.

Les résultats finaux, à la fin des 500 itérations, sont détaillés dans le tableau 1, où sont décrits pour les 3 bases le taux de couverture optimale (TCO), c'est-à-dire le pourcentage d'usurpation du meilleur passe-partout. La taille optimale de dictionnaire (TOD) y est aussi indiquée et correspond au nombre minimum de passe-partout distincts nécessaires pour que chaque individu de la base soit usurpé par au moins un des passe-partout. Ce

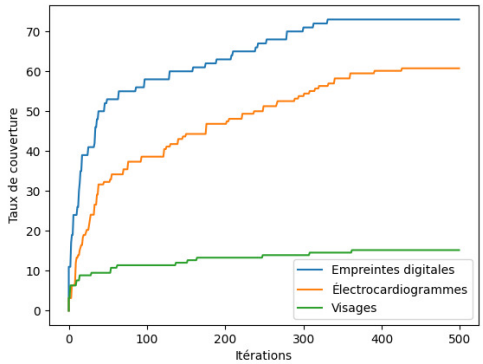

Fig. 1. Évolution du taux de couverture

TOD doit être mis en lien avec le nombre d'individus qui composent les 3 bases, ce qui peut influer sur le TOD.

Base	TCO (%)	TOD	#pers
Empreintes digitales	73	5	100
Visages	15.2	18	158
Électrocardiogrammes	61	12	158

Tableau 1. Performances des passe-partout

Dans un second temps, nous avons mené des expériences de ce scénario d'attaque sous des contraintes plus réalistes. Cette fois un attaquant a obtenu des couples gabarit/graine issus de vecteurs de caractéristiques toujours transformés avec l'algorithme biohashing. L'attaquant construit un passe-partout à partir de ces données, puis tente d'usurper d'autres couples gabarit/graine.

Ce cas d'usage est plus réaliste, car un attaquant prépare le passe-partout à partir d'une fuite de données biométriques pour attaquer d'autres données biométriques dont il n'a pas connaissance, sauf leur type. Les résultats sont présentés dans le tableau 2. Nous constatons que le passe-partout construit à partir d'un premier lot de données biométriques dont la couverture initiale est donnée dans la colonne *Report TCO* procure une capacité d'usurpation importante sur un autre lot de données biométriques

de même type. Cette capacité d'usurpation est donnée dans la colonne *TCO*, et le passe-partout conserve environ la moitié de sa couverture initiale, ce qui en fait un passe-partout réutilisable.

Base	TCO (%)	Report TCO (%)
Empreintes digitales	42	73
Visages	6.3	15.2
Électrocardiogrammes	44.3	61

Tableau 2. Performances des passe-partout réutilisables

Ce scénario a deux limites. La première est que la recherche de passe-partout est liée à la possibilité de trouver rapidement des préimages sur la transformation. Même si la stratégie utilisée (algorithme génétique) est indépendante d'éventuelles faiblesses de la transformation, il n'y a pas de garanties que des préimages puissent être trouvées efficacement. La seconde limite est qu'il est difficile de trouver des passe-partout qui couvrent un grand nombre de données. Au-delà d'attaques potentielles, les applications sont donc limitées à de petits groupes de données biométriques. On peut toutefois envisager des applications où un petit nombre de personnes donnent une délégation à une personne (le propriétaire du passe-partout). Néanmoins, si l'on veut obtenir un tel système, il vaut mieux le concevoir en amont, pour pouvoir obtenir facilement les propriétés désirées. C'est ce qui est présenté dans la section suivante.

4 Passe-partout au dessein éthique

Désormais, nous considérons que l'on a accès à la base de données biométriques, c'est-à-dire directement aux vecteurs de caractéristiques. On se place ainsi plus en amont du processus d'un schéma biométrique et implique un cas d'usage plus éthique, même si ce scénario peut aussi être vu comme une porte dérobée. Nous nous mettons donc dans la peau de l'administrateur par exemple, qui peut agir avant la transformation des données biométriques, notamment dans le choix de la graine qui paramètre la transformation. Le principe est donc de fixer le passe-partout, que l'on va utiliser pour choisir la graine afin que le gabarit produit soit usurpable par ce passe-partout, fixé et connu à l'avance.

4.1 Construction de passe-partout

La construction ne se fait pas par la recherche de préimages comme pour la section précédente, mais se fait par la recherche de graines permettant au passe-partout d'usurper toute la base. L'algorithme utilisé est un algorithme en ligne / incrémental qui traite chaque donnée biométrique indépendamment l'une de l'autre. Pour chaque vecteur de caractéristiques, une graine est choisie par force brute en connaissance du passe-partout de telle sorte que les transformations du passe-partout et du vecteur de caractéristiques avec cette graine procurent des gabarits similaires, et donc permettent au passe-partout d'usurper l'individu.

Nous allons décrire les transformations utilisées pour ces travaux. En effet, dans ce cas d'usage, l'administrateur peut choisir la transformation qu'il souhaite avec pour critère la facilité de calculer des préimages. Les deux matrices $N \times M$ de projection aléatoire sont proposées par [1], avec les mêmes valeurs N et M que précédemment.
Dans le premier cas, appelé JL1, les coefficients de la matrice M_s sont

$$\begin{cases} 1/\sqrt{M} \text{ avec probabilité } 1/2 \\ -1/\sqrt{M} \text{ avec probabilité } 1/2 \end{cases}$$

Dans le second cas, appelé JL2, les coefficients de la matrice M_s sont

$$\begin{cases} \sqrt{3/M} \text{ avec probabilité } 1/6 \\ 0 \text{ avec probabilité } 2/3 \\ -\sqrt{3/M} \text{ avec probabilité } 1/6 \end{cases}$$

Dans ce cas, la transformation $\mathcal{T}$ est définie par $\mathcal{T}(x, s) = D(xM_s)$, où s sert de graine au générateur pseudo-aléatoire utilisé pour générer les coefficients de M_s, et où D est la fonction de binarisation par seuillage précédemment décrite. L'avantage principal de ces transformations est le temps de génération de matrice qui est largement inférieur à l'utilisation de l'algorithme de Gram-Schmidt dans le biohashing.

Ce nouveau scénario permet d'obtenir un taux de couverture optimale de 100%, c'est-à-dire que le passe-partout peut usurper l'intégralité des couples gabarit/graine. De plus les performances de la base de données biométriques transformées sont similaires à celles obtenues avec des graines aléatoires, c'est-à-dire à celles que l'on obtiendrait avec la base de données transformées. Il est donc important d'utiliser une transformation qui ne dégrade pas trop les performances du système. La figure 2 représente le temps de recherche, exprimé en nombre de cycles d'horloge processeur,

pour trouver une telle graine pour chaque individu de la base. Les deux courbes *JL1* et *JL2* correspondent aux deux transformations précédemment décrites. On constate que la durée de recherche de graines est variable d'un facteur de six environ selon les individus.

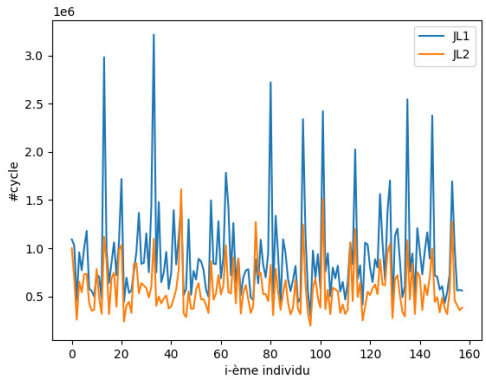

Fig. 2. Temps de recherche de graine pour chaque individu (Visages)

4.2 Individu passe-partout

Dans cette section, nous définissons l'individu passe-partout comme un individu qui possède plusieurs vecteurs de caractéristiques issus de ses captures de modalité biométrique, et qui souhaite pouvoir usurper les autres individus avec de futures captures. L'objectif est d'étendre les travaux précédents et d'évaluer si le nombre et la couverture des vecteurs de caractéristiques, issus d'un même individu passe-partout, utilisés pour la recherche de graines, influent sur ces performances d'usurpation futures. Pour cela, deux ensembles composés de vecteurs de caractéristiques de l'individu passe-partout sont définis. Le premier ensemble, dit ensemble de recherche, est utilisé pour la recherche de graines. Le second ensemble, dit ensemble de test, est utilisé pour analyser les performances d'usurpation d'autres captures de l'individu passe-partout.

La figure 3 représente sous forme de courbes cumulées décroissantes les couvertures de ces deux ensembles dans deux cas : les courbes bleue et orange correspondent au cas où seul un vecteur est utilisé pour la recherche de graine et les autres pour les tests de couvertures, alors que les courbes verte et rouge correspondent au cas où quatre vecteurs sont utilisés pour

la recherche de graines, et les autres pour les tests de couvertures. Nous constatons un glissement de la courbe rouge vers la droite par rapport à la courbe orange, ce qui signifie que lorsqu'on utilise quatre vecteurs au lieu d'un pour la recherche de graines, alors les autres captures de modalité biométrique usurpent plus d'individus de la base. Plus précisément, on constate que lorsqu'un seul vecteur est utilisé pour la recherche de graines, 50% des vecteurs de tests usurpent au moins 50% des individus de la base. Dans le cas où on utilise quatre vecteurs pour la recherche de graines, cette fois c'est 80% des vecteurs de tests qui usurpent au moins 50% de la base. Ces expériences démontrent qu'il faut utiliser plusieurs vecteurs de caractéristiques pour choisir les graines, afin d'améliorer les performances de couverture de futures captures de l'individu passe-partout.

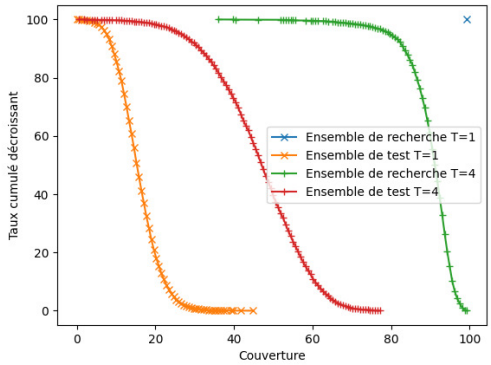

Fig. 3. Courbes cumulées décroissantes de couvertures des ensembles (Visages)

Nous avons aussi souhaité vérifier si la capacité de couverture des vecteurs de l'ensemble de recherche influait sur les performances d'usurpation futures. La figure 4 représente la corrélation de couvertures moyennes entre l'ensemble de recherche et l'ensemble de test. Il s'agit d'un nuage de points, et chaque point représente un individu. L'abscisse d'un point correspond à la couverture moyenne des quatre vecteurs de caractéristiques de l'ensemble de recherche, et l'ordonnée à la couverture moyenne de ceux de l'ensemble de test. On constate une corrélation importante entre ces deux performances, indiquant qu'en plus d'utiliser plusieurs vecteurs pour la recherche de graines, il faut les choisir minutieusement selon leur capacité de couverture pour maximiser l'espérance de capacité d'usurpation d'autres vecteurs.

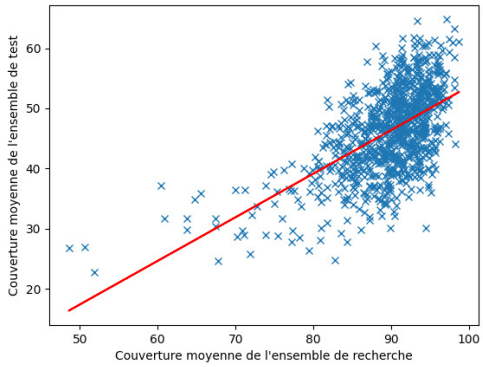

Fig. 4. Corrélation de couvertures (Visages)

5 Conclusion

Dans cet article nous avons introduit la notion de passe-partout biométrique, une donnée biométrique permettant d'usurper de nombreux individus. Dans un premier temps ces passe-partout sont construits par des préimages obtenues avec un algorithme génétique depuis des gabarits. Nous avons proposé des indicateurs de réutilisabilité du passe-partout afin de s'ancrer dans un scénario d'attaque réaliste où les passe-partout conservent la moitié de leur capacité d'usurpation.
Dans l'objectif d'augmenter la capacité d'usurpation, nous avons développé un second scénario qui nécessite d'être actif à la phase d'enrôlement, notamment pour le choix de graine paramétrant la transformation. Ce cas d'usage est principalement le contrôle d'accès, mais peut aussi être considéré comme une porte dérobée. Ces nouvelles contraintes nous permettent d'avoir des passe-partout usurpant l'intégralité des individus cibles.
Nous avons démontré qu'un individu utilisant plusieurs données biométriques minutieusement choisies pour la recherche de graines possède d'importantes capacités d'usurpation avec ses futures données biométriques, non utilisées dans le choix de graines. Notons que la transformation choisie n'a pour but que de construire des bases biométriques avec des propriétés de contrôle d'accès choisies, et non de garantir la sécurité des données. Celle-ci doit être assurée par d'autres moyens.

Postface

Ces travaux ont été effectués durant ma thèse et ont été publiés dans le journal Computers & Security en [8] et ils sont détaillés plus précisément dans mon manuscrit de thèse [7]. Ils sont résumés dans cet article à titre de partage et d'accessibilité à un public francophone averti en sécurité informatique, mais non expert du domaine de la biométrie.

Références

1. Dimitris Achlioptas. Database-friendly random projections : Johnson-lindenstrauss with binary coins. *Journal of Computer and System Sciences (JCSS)*, 66(4) :671–687, 2003.
2. Rima Belguechi, Adel Hafiane, Estelle Cherrier, and Cristophe Rosenberger. Comparative study on texture features for fingerprint recognition : application to the biohashing template protection scheme. *Journal of Electronic Imaging*, 25(1), 2016.
3. R. Bousseljot, D. Kreiseler, and A. Schnabel. Nutzung der EKG-signaldatenbank cardiodat der PTB über das internet, 1995.
4. CNIL. Biométrie : un "gabarit" biométrique, c'est quoi ?
5. CNIL. Délibération n° 2019-001 du 10 janvier 2019 portant règlement type relatif à la mise en œuvre de dispositifs ayant pour finalité le contrôle d'accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travai.
6. Jiankang Deng, Jia Guo, Niannan Xue, and Stefanos Zafeiriou. Arcface : Additive angular margin loss for deep face recognition. In *IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, pages 4685–4694, 2019.
7. Tanguy Gernot. *Passe-partout biométriques*. Theses, Normandie Université, November 2022.
8. Tanguy Gernot and Patrick Lacharme. Biometric masterkeys. *Computers & Security*, 116 :102642, 2022.
9. Gary B. Huang, Manu Ramesh, Tamara Berg, and Erik Learned-Miller. Labeled faces in the wild : A database for studying face recognition in unconstrained environments. Technical Report 07-49, University of Massachusetts, Amherst, 2007.
10. Anil K Jain, Patrick Flynn, and Arun A Ross. *Handbook of biometrics*. Springer Science & Business Media, 2007.
11. Patrick Lacharme, Estelle Cherrier, and Christophe Rosenberger. Preimage attack on biohashing. In *International Conference on Security and Cryptography (SECRYPT)*, pages 363–370, 2013.
12. Dario Maio, Davide Maltoni, Raffaele Cappelli, James L. Wayman, and Anil K. Jain. FVC2002 : Second fingerprint verification competition. In *International Conference on Pattern Recognition (ICPR)*, volume 3, pages 811–814, 2002.
13. Dominique Makowski, Tam Pham, Zen J. Lau, and Jan C. Brammer. Neurokit2 : The python toolbox for neurophysiological signal processing, 2021.

14. Juan Pablo Martínez, Rute Almeida, Salvador Olmos, Ana Paula Rocha, and Pablo Laguna. A wavelet-based ecg delineator : evaluation on standard databases. *IEEE Transactions on Biomedical Engineering*, 51(4) :570–581, 2004.
15. Melanie Mitchell. *An introduction to genetic algorithms*. MIT press, 1998.
16. Abhishek Nagar, Karthik Nandakumar, and Anil K Jain. Biometric template transformation : a security analysis. In *Media Forensics and Security II*, volume 7541, pages 237–251. SPIE, 2010.
17. C. Rathgeb and A. Uhl. A survey on biometric cryptosystems and cancelable biometrics. *EURASIP J. on Information Security*, 3, 2011.
18. Andrew BJ Teoh, David CL Ngo, and Alwyn Goh. Personalised cryptographic key generation based on facehashing. *Computers & Security*, 23(7) :606–614, 2004.