Les attaques par présentation des systèmes biométriques

Quand la réalité rejoint James Bond

Joannes Falade,
Chercheur post-doctoral – GREYC
Christophe Charrier,
Maître de conférences HDR à l'UNICAEN - GREYC
Christophe Rosenberger,
Professeur à l'ENSICAEN - GREYC

Un système biométrique vise en général à sécuriser l'accès à une ressource logique ou physique. Attaquer un système biométrique est malgré tout possible de différentes façons. L'attaque par présentation est spécifique à la biométrie, elle a été rendue populaire dans un film de James Bond en 1971.

Introduction

La biométrie est souvent considérée comme la méthode ultime pour authentifier un individu. La relation entre une personne et sa preuve d'identité peut difficilement être plus étroite. En effet, une donnée biométrique peut correspondre à une partie du corps de l'individu (visage, empreinte digitale,...). Les systèmes biométriques, sous différentes formes, font partie de notre quotidien pour sécuriser l'accès à nos objets intelligents (ordinateur, smartphone) et à des bâtiments (son entreprise par exemple). Malheureusement, comme toute technologie de sécurité, des attaques sont réalisables à plusieurs fins.

Pourquoi attaquer un système biométrique ?

Le premier objectif d'un attaquant vise évidemment à usurper l'identité d'une personne pour accéder à des ressources logiques (ordinateur, smartphone…) ou physiques (comme un bâtiment). Il faut noter que cette attaque peut être réalisée avec le consentement de l'individu (par exemple, lors du pointage horaire au sein d'une entreprise). Un attaquant peut également avoir l'intention de mettre à mal la disponibilité du système, en le rendant défaillant pour simplifier de futures attaques. Un autre type d'attaque consiste à berner le système biométrique afin qu'il ne puisse pas reconnaître une personne. Il peut ●●●

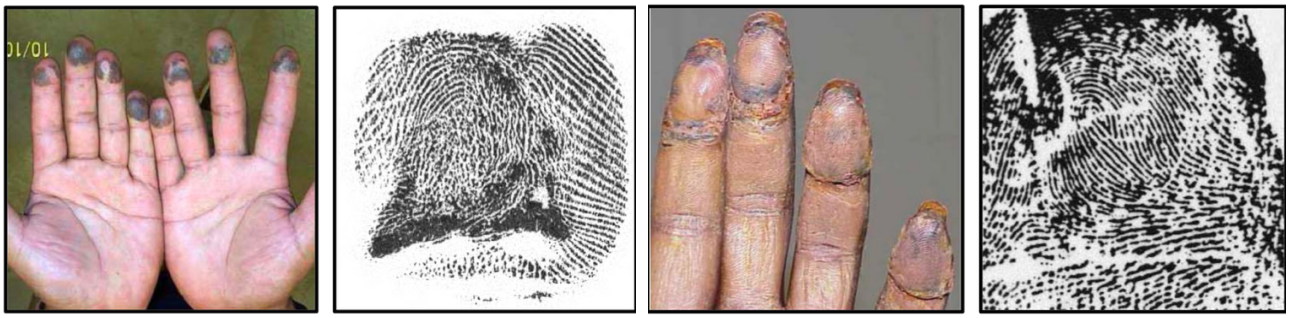

Figure 1 : Exemples d'empreintes digitales volontairement altérées par un individu pour ne pas être identifié par un système biométrique (source [1]).

●●● s'agir de personnes recherchées par la police par exemple. La figure 1 présente deux illustrations de tels procédés concernant l'empreinte digitale (altération par morsure ou transplantation de morceaux de peau).

Comment définit-on l'attaque par présentation ?

Elle consiste à présenter au capteur biométrique une donnée visant à interférer le fonctionnement du système biométrique. Cette attaque se focalise donc essentiellement sur la phase de capture de la donnée biométrique. Bien souvent, le cinéma présente des innovations qui n'existaient pas encore à l'époque de sortie du film. Dans le film de James Bond « Les diamants sont éternels » en 1971, des attaques par présentation sont utilisées pour usurper l'identité d'espions (empreinte digitale et visage), comme le montre la figure 2. A cette époque, l'attaque consistant à copier une empreinte digitale n'était pas déployée de façon opérationnelle par les services gouvernementaux internationaux (voir vidéo [2]).

Dans la suite de cet article, nous allons revenir en détail sur les attaques des systèmes biométriques et les solutions développées par les chercheurs académiques et industriels afin de les détecter.

Les attaques d'un système biométrique

D'une façon générale, il existe huit points d'attaque sur les systèmes biométriques comme présenté sur la figure 3 illustrant le modèle de Ratha en 2001.

"Dans le film de James Bond « Les diamants sont éternels » en 1971, des attaques par présentation sont utilisées pour usurper l'identité d'espions (empreinte digitale et visage)."

L'attaque par présentation, encore appelée « attaque de niveau 1 » est celle qui nous intéresse dans cet article car c'est la seule qui corresponde à une attaque spécifique à la biométrie. En effet, pour réaliser une attaque de niveau 1, l'attaquant présente une fausse donnée biométrique qui est en réalité, une copie de plus ou moins bonne qualité de la donnée biométrique d'un utilisateur légitime et connu par le système biomé-

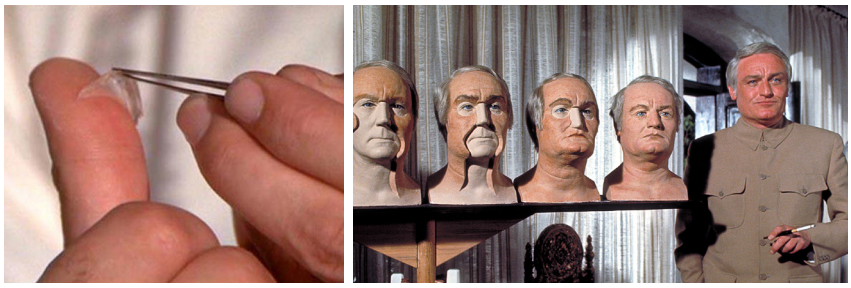

Figure 2 : Attaques par présentation (source : James Bond - "Les diamants sont éternels" (1971)

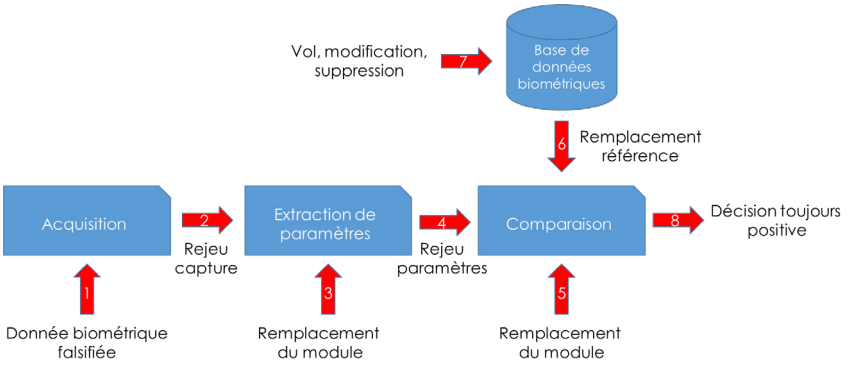

Figure 3 : Les différentes attaques d'un système biométrique (modèle de Ratha 2001) .

trique. Les attaquants ont recours à une attaque par présentation dans le cas où, dans un premier temps lors de l'enrôlement, ils ont pu utiliser leurs données biométriques réelles pour être connu du système. Puis, dans un second temps, ils s'emploient à dissimuler leur identité réelle suite à des restrictions d'accès concernant leur propre personne ou lorsqu'ils souhaitent collaborer avec d'autres personnes ayant connu également de telles restrictions. Par exemple, dans un contexte d'état d'urgence où les contrôles aux frontières sont renforcés pour éviter que les terroristes ou des personnes recherchées à risque n'accèdent sur le territoire afin de commettre des crimes, les attaquants utilisent les attaques de niveau 1 par présentations. Ces personnes, sachant qu'elles sont recherchées et fichées dans les données d'État, ont l'habitude de coopérer avec des individus de leur entourage non ciblés par des restrictions. Ainsi, dans le cas où la donnée biométrique est l'empreinte digitale, ils peuvent reproduire une copie du faux doigt correspondant à celui de leur complice afin de se faire passer pour ce dernier.

Dans la suite de cet article, nous utilisons l'empreinte digitale comme donnée biométrique pour expliquer les attaques par présentation sur les systèmes biométriques.

Méthodes de création de fausses empreintes digitales

Le schéma de la figure 4 présente les différentes techniques utilisées par un attaquant pour réaliser une attaque par présentation en utilisant un faux doigt sur le capteur d'empreintes digitales. On parle également d'empreintes digitales artificielles dans la littérature spécialisée.

Méthode coopérative

En ce qui concerne la méthode coopérative, l'attaquant collabore avec l'individu dont il veut obtenir l'empreinte digitale artificielle. Ainsi, le porteur légal de l'empreinte digitale, pose son doigt sur un matériel (pâte à modeler, colle…) afin de créer un moule de son empreinte digitale. Ensuite, dans ce moule, on y verse de la colle à bois ou de la gélatine pour reproduire la copie de l'empreinte digitale. Les différentes étapes peuvent être observées sur la figure 5.

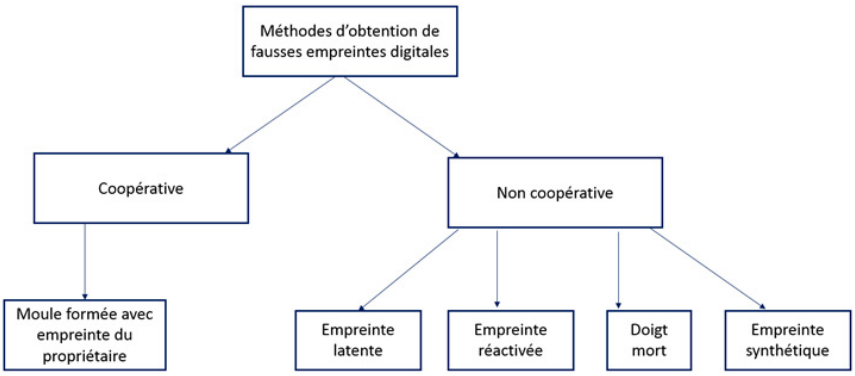

Figure 4 : Les différentes méthodes d'obtention de fausses empreintes digitales.

Figure 5 : Les étapes pour la création d'une fausse empreinte digitale par la méthode coopérative (extrait de [3]) .

"D'autres méthodes comme l'utilisation de doigts morts récupérés chez des cadavres ou des empreintes synthétiques sont également envisageables."

Méthode non-coopérative

S'agissant de la méthode non-coopérative, l'attaquant réussit à reproduire l'empreinte digitale de celui dont il désire usurper l'identité sans l'accord de ce dernier. Pour ce faire, il met en place un dispositif plus complexe pour réactiver ce qu'on appelle une empreinte latente qui représente les traces que nous laissons quand nous touchons des objets ou que nous y posons les doigts. La figure 6 présente un dispositif complexe destiné à réactiver une empreinte latente. D'autres méthodes comme l'utilisation de doigts morts récupérés chez des cadavres ou des empreintes synthétiques sont également envisageables.

Compte tenu des conditions quasi parfaites de fabrication des empreintes digitales artificielles par la méthode coopérative, la détection de ce type d'attaque présente un niveau de difficulté supé- ●●●

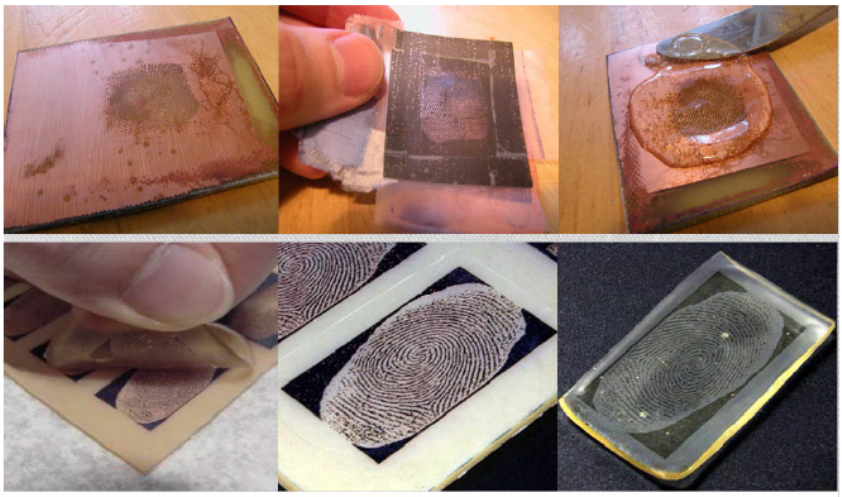

Figure 6 : Les étapes pour la création d'une empreinte artificielle en récupérant une empreinte latente avec un circuit imprimé (extrait de [3]).

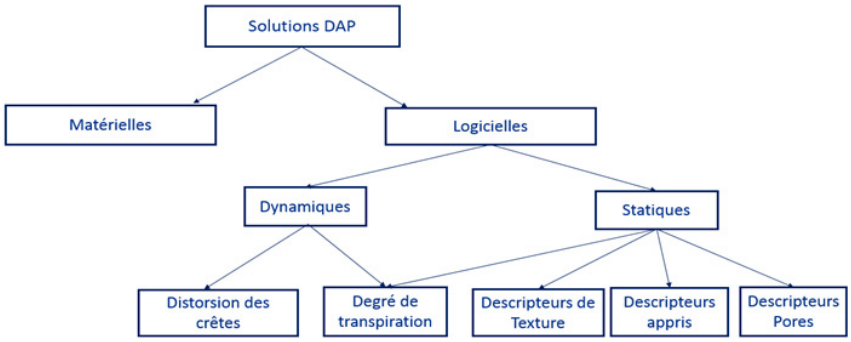

Figure 7 : Différentes solutions de l'état de l'art pour la détection d'attaque par présentation.

rieur à celui des méthodes non coopératives.

Les contre-mesures

Pour contrer les attaques par présentation sur un système biométrique d'empreintes digitales, il existe deux solutions de détection d'attaque par présentation (DAP) : logicielles et matérielles, comme indiquées sur la figure 7.

Qu'il s'agisse de l'approche matérielle ou logicielle, la détection d'attaque consiste à relever des descripteurs discriminants qui qualifient l'état réel ou artificiel de l'empreinte digitale posée sur un capteur. L'approche matérielle nécessite l'utilisation de composants spécifiques sur les capteurs d'acquisition d'empreintes digitales. Les solutions sont très coûteuses et pas très généralisables pour contrer plusieurs modes d'attaque.

L'approche logicielle est la solution la plus explorée de l'état de l'art et peut être dynamique ou statique. Les solutions dynamiques nécessitent des mouvements du bout du doigt de l'utilisateur afin d'évaluer les mouvements de crêtes et les niveaux de transpiration engendrés sur le doigt. Ceci rallonge le temps d'acquisition de l'empreinte digitale en raison des mouvements que la méthode exige. D'autre part, l'attaquant peut se douter de l'existence d'une solution de type DAP et changer son comportement en conséquence.

Solutions logicielles statiques de DAP

Les solutions logicielles statiques ont pour but de de détecter une attaque par présentation à partir d'une seule image d'empreinte digitale acquise sur un capteur. Ces solutions sont les plus explorées de l'état de l'art car elles sont moins coûteuses, ne nécessitent aucune consigne supplémentaire pour l'utilisation du capteur et correspondent au cas d'utilisation courant des systèmes biométriques. Elles sont basées sur l'utilisation de descripteurs de texture, de descripteurs appris par apprentissage profond ou enfin de descripteurs de pores. Les pores nécessitent des capteurs de très haute résolution différents de ceux couramment utilisés aujourd'hui et ne sont donc pas des descripteurs très répandus dans l'état de l'art des solutions logicielles statiques de DAP.

Descripteurs de texture

La figure 8 présente les différentes étapes pour construire un modèle de

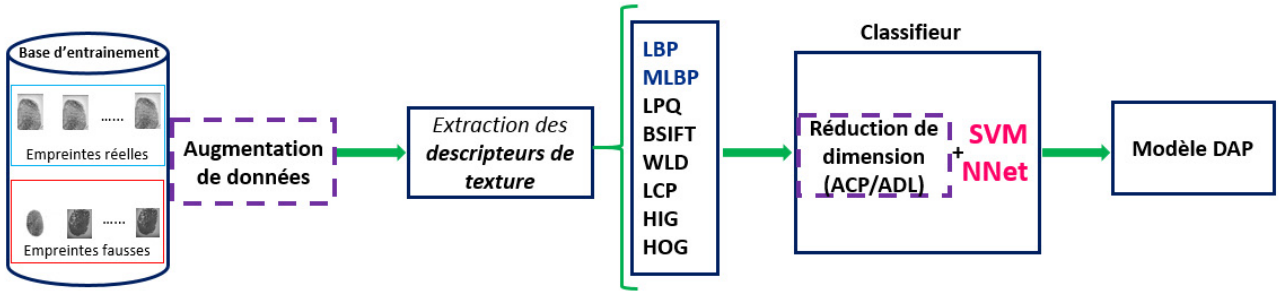

Figure 8 : Méthodes statiques basées sur l'utilisation des descripteurs de texture d'image.

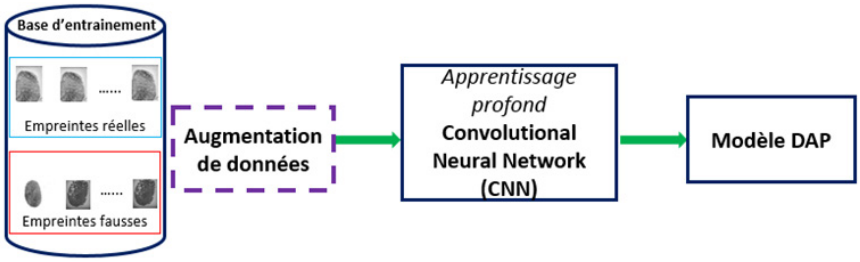

Figure 9 : Méthodes statiques basées sur l'utilisation des descripteurs appris par apprentissage profond.

" Avec les descripteurs appris apparus depuis 2015 dans les compétitions Livdet, les taux de précision se sont globalement améliorés atteignant même 99% et démontrant ainsi l'importance des CNN. "

DAP en utilisant les descripteurs de textures. Ces descripteurs, d'une façon générale, calculent les variations d'intensité des pixels sur une image dans un bloc de pixels de l'image. Ils sont très utilisés en traitement et classification d'images et ont donc été transposés à la problématique de DAP qui consiste à différencier une image d'empreinte digitale réelle d'une image d'empreinte digitale artificielle.

En effet, pour construire un modèle de DAP, on part d'une base de données d'images d'empreintes labellisées contenant des empreintes réelles ainsi que des empreintes fausses puis on extrait des descripteurs de textures tels d'images pour ces images. Ces descripteurs sont par la suite insérés dans les classifieurs de type SVM ou réseau de neurone (NNet) pour permettre la construction de modèles de DAP. Ces classifieurs sont des algorithmes d'apprentissage machine qui déterminent les facteurs discriminants parmi les descripteurs soumis lors de la phase d'entraînement et permettant de construire le modèle de DAP. Les étapes d'augmentation de données puis de réduction de leur dimension sont utilisées dans la chaîne d'apprentissage pour obtenir un modèle plus fiable.

Descripteurs appris

La figure 9 présente les différentes étapes pour construire un modèle de DAP en utilisant les descripteurs appris. Avec cette approche, les descripteurs sont générés automatiquement par les algorithmes d'apprentissage profond que sont les CNN (*Convolutional Neural Network*). Cette approche nécessite une base de données d'exemples que l'on souhaite différentier (ici, les empreintes légitimes des falsifiées).

Ces solutions sont donc très utilisées depuis les années 2015 suite à l'essor des solutions d'apprentissage profond lors de la compétition en classification d'images comme décrit dans [4].

Discussions

Il faut remarquer que les bases de données d'empreintes digitales jouent un rôle très important dans la détection d'attaque car elles permettent l'apprentissage de modèle de DAP puis font avancer les travaux de recherches associés. Pour cela, les compétitions internationales de LivDet apparues depuis 2009 jusqu'à ce jour permettent aux différents concurrents de soumettre leurs solutions de DAP sur un *benchmark* commun.

Les auteurs

Joannes Falade a obtenu son master en Algorithmique et Modélisation à l'interface des sciences de l'université Paris Saclay en 2017. Il a réalisé une thèse CIFRE au sein de l'IN groupe en collaboration avec le laboratoire GREYC entre 2017 et 2020. Ses intérêts de recherche concernent la représentation des empreintes digitales pour l'indexation et la détection d'attaques par présentation.

Christophe Charrier a obtenu son doctorat en informatique de l'Université de Saint-Etienne en 1998. De 1998 à 2001, il a été assistant de recherche au LRTS à Université Laval, à Québec. En 2001, il rejoint l'IUT Grand Ouest Normandie sur le site de Saint-Lô en tant qu'enseignant-chercheur. En 2008, il rejoint le laboratoire GREYC. En 2008, il a été chercheur invité à l'Université du Texas à Austin. De 2009 à 2011, il a été professeur invité à l'Université de Sherbrooke, Canada. Ses intérêts de recherche actuels incluent le traitement des images et de vidéos, l'évaluation de la qualité, la vision par ordinateur et la biométrie. Depuis 2016, il est le responsable de l'équipe de recherche SAFE. Il est l'auteur ou le co-auteurs de plus de 150 publications.

Christophe Rosenberger a obtenu son doctorat en informatique de l'Université de Rennes 1 en 1999. De 2000 à 2007, il a été maître de conférences à l'ENSI de Bourges (INSA Centre Val de Loire depuis 2014). En 2007, il rejoint l'ENSICAEN comme professeur des universités. Depuis, il fait partie de l'équipe de recherche SAFE (Sécurité, Architecture, Forensique, biomEtrie) au sein laboratoire GREYC. Ses intérêts de recherche concernent la biométrie (définition et évaluation de systèmes, protection des données biométriques). Depuis 2019, il est le directeur du laboratoire GREYC. Il est le co-auteur de plus de 200 publications au niveau international.

Ainsi, sur les bases Livdet, on remarque que les solutions utilisant la texture ont été très utilisées jusqu'en 2014. Sur ces bases connues comme difficiles, les descripteurs de texture arrivent globalement à une précision de 90% de détection d'attaque par présentation en testant près de 4000 images d'empreintes digitales contenant autant d'empreintes réelles que d'images artificielles. Avec les descripteurs appris apparus depuis 2015 dans les compétitions Livdet, les taux de précision se sont globalement améliorés atteignant même 99% et démontrant ainsi l'importance des CNN. Cependant, les CNN nécessitent un temps d'apprentissage plus long et moins explicable à un expert du métier car toute la chaîne d'extraction et d'apprentissage du modèle est automatisée, donc abstraite, si on la compare à l'extraction manuelle faite avec la texture.

" Les descripteurs de texture arrivent globalement à une précision de 90% de détection d'attaque par présentation en testant près de 4000 images d'empreintes digitales contenant autant d'empreintes réelles que d'images artificielles. "

Conclusion

Dès lors que l'on utilise la biométrie à des fins d'identification ou de reconnaissance, force est de constater que les systèmes biométriques sont soumis à des attaques pour les leurrer et permettre ainsi d'accéder à des données non autorisées ou bien de ne pas se faire reconnaître. Comme cela a été mentionné précédemment, le principal point de compromission est l'attaque physique ou logicielle sur le capteur. Cependant, des contre-mesures efficaces existent afin de se prémunir contre ce type d'attaque par présentation. Celles-ci nécessitent le recours soit à des ressources matérielles supplémentaires (par exemple caméra infra-rouge dans le cas des empreintes digitales) soit à l'analyse des données biométriques par un logiciel de détection d'intrusion. L'objectif étant d'avoir un taux de détection le plus haut possible, en fonction du niveau de sécurité que l'on souhaite atteindre. ■

Résumé

La biométrie utilise les caractéristiques morphologiques et comportementales pour la reconnaissance des individus bien souvent à des fins de sécurité. L'utilisation de systèmes biométriques peut subir plusieurs types d'attaques. L'attaque par présentation consistant à présenter au capteur biométrique une fausse donnée biométrique peut avoir comme but d'usurper l'identité d'un individu connu du système. Dans cet article, nous nous intéressons aux attaques par présentation sur les empreintes digitales. Nous décrivons les motivations d'un attaquant puis les différentes techniques utilisées par ce dernier pour la fabrication de fausses empreintes digitales. Nous donnons également les grands axes des méthodes existantes pour contrer les attaques sur les systèmes biométriques d'empreintes digitales. ■

Abstract

Biometrics use morphological and behavioral characteristics for the recognition of individuals, often for security purposes. The use of biometric systems can be subject to different types of attacks. The presentation attack consisting in presenting a false biometric data to the biometric sensor aims at impersonating an individual known by the system. In this article, we focus on presentation attacks on fingerprints. We describe the motivations of an attacker and then the various techniques he/she can use to create false fingerprints. We also give the main existing methods to counter attacks on biometric fingerprint systems. ■

Références

[1] S. Yoon, J. Feng, and A. K. Jain, "Altered fingerprints: Analysis and detection," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 34, no. 3, pp. 451–464, 2012.

[2] https://www.youtube.com/watch?v=yP5ku2IJgAY&ab_channel=IntlSpyMuseum

[3] Marasco, E. and Ross, A. "A survey on Anti-Spoofing Schemes for Fingerprint Recognition Systems," ACM Computing Surveys, vol. 47

[4] Alex Krizhevsky and Sutskever, Ilya and Hinton, Geoffrey E "ImageNet Classification with Deep Convolutional Neural Networks," Advances in Neural Information Processing Systems 25, pp. 1097-1105, 2012.