Système automatique de reconnaissance d'empreintes digitales. Sécurisation de l'authentification sur carte à puce.

Christel-Loïc TISSE[1], Lionel MARTIN[1], Lionel TORRES[2], Michel ROBERT[2]

[1]**A**dvanced **S**ystem **T**echnology Laboratory

STMicroelectronics – ZI Rousset – 13106 Rousset, France

[2]Université de Montpellier, UMR 5506, L.I.R.M.M.

161, rue Ada -34392 Montpellier, France

christel-loic.tisse@st.com, lionel.martin@st.com, torres@lirmm.fr, robert@lirmm.fr

Résumé – La reconnaissance d'empreintes digitales est une technique biométrique mature pour toute application d'identification ou de vérification d'individus. Dans cet article, nous décrivons la conception et le développement d'un système automatique d'authentification d'identité par empreintes digitales. Ce système automatique de reconnaissance d'empreintes digitales est basé sur une série d'algorithmes complexes apparentés aux domaines du traitement d'images et/ou de la reconnaissance de motifs (nuages de points). Son originalité repose sur le portage de la phase de comparaison sur une carte à puce *SmartJ*^{TM} 32-bit pour assurer une authentification rapide et sécurisée.

Abstract *– Fingerprint recognition is an important biometric technique for personal identification or verification. In this paper, we describe the design and implementation of an automatic identity authentification system that uses fingerprints to authenticate the identity of an individual. This Automated Fingerprint Identification System (A.F.I.S.) contains a series of complex algorithms, such as advanced image processing for fingerprint enhancement and/or point pattern matching. Our approach is based on a platform, which combines several innovative hardware and software developments to provide identification using a fast matching algorithm executed on a safe and secure 32-bit SmartJ*^{TM} *smart card.*

1. Introduction

1.1 Généralités

Les récents progrès des technologies informatiques ont favorisé le développement des systèmes biométriques. Ces systèmes sont de plus en plus présents dans les applications liées à la sécurisation tel que le contrôle d'accès. Le marché de l'identification par biométrie est évalué à plus de 4 milliards de dollars en 2002 [1].

Concernant l'empreinte digitale, c'est le Britannique F.Galton qui démontra le premier en 1888 la permanence du dessin papillaire de la naissance à la mort, ainsi que son inaltérabilité. Cet arrangement particulier des lignes papillaires forme des points caractéristiques, nommés *minuties* qui sont à l'origine de l'individualité des dessins digitaux. A ce jour, on considère qu'il faut 8 à 17 de ces points sans discordance pour qu'on estime établie l'identification. Un chiffre inférieur au seuil minimum aboutit à l'exclusion de l'empreinte digitale comme élément de preuve.

On recense 13 types différents de *minuties* permettant de classifier les empreintes digitales et d'en assurer leur unicité, dont les 6 plus fréquents sont présentés sur la figure 1. D'un point de vue statistique, Osterburg [2] analyse en 1977 la fréquence d'apparition de chacun des types de *minuties*, et met en évidence que les *minuties* du type « branche » et « terminaison » constituent majoritairement la signature d'une empreinte digitale.

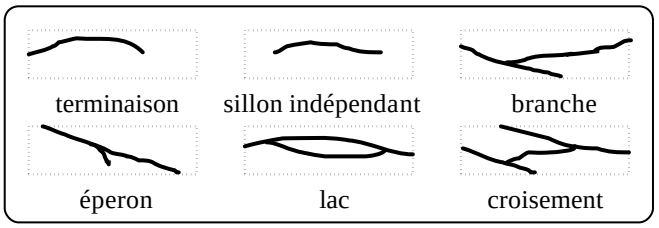


FIG. 1 : les 6 principaux types de *minuties*

1.2 Aperçu des différentes approches

Si chaque A.F.I.S. (Automated Fingerprint Identification System) emploie des terminaux biométriques d'acquisition (capteur optique, capacitif, thermique, à ultrason) et des méthodes d'analyses différentes, le principe d'identification reste sensiblement le même ; il s'agit toujours d'extraire certaines caractéristiques (*minuties* ou autres) sous forme d'information codée : on ne conserve jamais toute l'information originale.

D'une manière générale on distingue dans la littérature deux catégories d'algorithmes de reconnaissance d'empreintes digitales : la première catégorie concerne les algorithmes plutôt « conventionnels » qui s'appuient sur la position relative des *minuties* entre elles, alors que la seconde regroupe les algorithmes visant à extraire d'autres particularités de l'empreinte digitale telles que la direction

locale des sillons [3] et [4], ou encore les composantes fréquentielles locales de la texture au cœur de l'image [5].

L'approche retenue, appartenant à la première catégorie, est celle proposée par A.K Jain [6] qui est vraisemblablement la plus connue. On réalise successivement le filtrage directionnel et la binarisation de l'image, l'amincissement (ou squelettisation) des sillons (figure 2), puis on détermine la position des minuties au sein de l'image pour quantifier les caractéristiques de ressemblance entre deux gabarits par « point pattern matching ». On notera par ailleurs l'alternative proposée par D. Maio [7] qui permet la localisation des *minuties* d'une manière plus directe en utilisant des réseaux de neurones.

FIG. 2 : synopsis du pré-traitement des images d'empreintes digitales en vue de l'extraction des *minuties*

1.3 Vue d'ensemble sur l'article

Nous proposons dans cet article la description d'un AFIS dont la phase de comparaison est sécurisée en s'effectuant sur carte à puce. Il en résulte une solution adaptée au contrôle d'accès, alliant confort, rapidité et fiabilité. Dans un premier temps, les différentes étapes de l'algorithme de reconnaissance d'empreintes digitales sont expliquées. La méthodologie de pré-traitement des images jusqu'à extraction des *minuties* et la description de l'algorithme d'authentification proprement dite sont abordées. Dans un second temps, nous discutons de l'intérêt d'une sécurisation hardware d'une part du procédé d'authentification (algorithme de « *matching* »), et d'autre part du stockage du gabarit associé à une empreinte digitale de référence. Enfin, dans une dernière partie sont présentées les performances de l'AFIS ainsi réalisé.

2. L'algorithme de reconnaissance d'empreintes digitales

Le capteur utilisé est le «*TouchChip*™ » [15], capteur capacitif qui enregistre la forme de l'empreinte digitale à partir des variations électriques produites par les monts et les vallées du doigt avec une qualité d'image en 256 niveaux de gris, et une résolution de 256*360 pixels. L'enrôlement, processus par lequel l'identité d'une personne et son image biométrique sont utilisées pour constituer une base de données, se décomposent en deux parties: le traitement de l'image de l'empreinte, et l'extraction de la position des *minuties*. Le premier algorithme de traitement des images d'empreintes permet de s'affranchir du bruit lié à la mesure, perturbations désignées sous le terme de bruit image (provenant essentiellement de l'imperfection de la peau et des poussières entre le doigt et le capteur), mais aussi de mettre en évidence l'information relative aux sillons en les synthétisant sous forme filaire par leur squelette. La méthodologie globale retenue pour ce pré-traitement est tout à fait classique. Toutefois, dans un souci de portabilité, nous nous sommes orientés vers le développement d'algorithmes bas niveaux, autorisant un maximum de parallèlisation au niveau pixel. Autrement dit, si nous affections un CPU par pixel de l'image, nous serions en mesure de réaliser l'ensemble des traitements plus rapidement. Nous avons par ailleurs évalué les performances de deux procédés de squelettisation, « Zhang » [8] et « Shapori » [9], appliqués à notre problème d'affinement de sillon.

2.1 Pré-traitement des images d'empreintes digitales

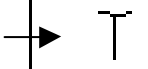
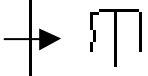
La première étape en vue de l'amélioration de l'image de l'empreinte digitale est le calcul de *l'image directionnelle* [10]. L'objectif de ce traitement est d'obtenir une image de l'orientation des sillons de l'empreinte. Autrement dit, on attribue à chacun des pixels de l'image l'orientation du sillon auquel il appartient. Le calcul de l'orientation s'effectue de la manière suivante:

$$K(i,j)=\min \sum_{k=1}^{n} |C(i,j) - Cd(i_k,j_k)| \quad d=0,1,\ldots.N-1 \quad (1)$$

K(i,j) est l'orientation du pixel (i,j) dans *l'image directionnelle* résultat, *C(i,j)* l'intensité du point (i,j) dans l'empreinte originale, $Cd(i_k,j_k)$ l'intensité de chaque pixel dans une direction donnée, *N* le nombre de directions (N = 8 dans notre exemple), *n* le nombre de pixels à tester dans chacune des directions (déterminé en considérant les largeurs minimales et maximales des sillons et des vallées : n=13 dans notre cas) .

La seconde étape consiste à partager *l'image directionnelle* en sous blocs (13*13 pixels) et de les caractériser par une orientation moyenne (parmi les 8 directions définies) et une seule, en déterminant par calcul d'histogramme quelle est la direction qui apparaît le plus fréquemment au sein de chacun des blocs. Ensuite, on filtre l'image originale en appliquant en chaque point une *convolution directionnelle* [11] (filtres de Gabor 2D) en fonction de la direction moyenne des sillons (bloc directionnel) précédemment calculée. Après filtrage, on différencie sillons et vallées par *binarisation*. Il s'agit d'une *binarisation locale* (un seuil par sous bloc de 13*13 pixels) afin de s'affranchir de la non-uniformité de l'intensité sur l'ensemble de l'image. Pour finir le pré-traitement de l'image d'empreinte digitale, on réalise une *squelettisation*, comparable à une opération d'*amincissement*. L'efficacité d'un tel algorithme d'*amincissement* étant bien difficile à quantifier, notre choix a été guidé par les expérimentations résumées dans le tableau 1 : elles comparent deux algorithmes semblables (basés sur des méthodes morphologiques itératives) de squelettisation et mettent en évidence les nombreux avantages de l'approche de « Zhang » [8] par rapport à celle de « Shapori » [9].

Tab. 1 : comparaison expérimentale des algorithmes de squelettisation de « Zhang » et de « Shapori »

	« **Shapori** »	« **Zhang** »
		
		
Temps d'exécution (image 256*360, P133 MHz)	# 1.6 s	# 1.3 s
Mémoire nécessaire (en taille image)	2	1

2.2 Extraction des minuties

Les *minuties* de l'empreinte digitale sont extraites à partir de son squelette en calculant la « connectivité » *CN* en chaque point de l'image *P* de la manière suivante :

$$CN = 0.5 \sum_{i=1}^{8} |P_i - P_{i+1}| \quad (2)$$

$P_9 = P_1$, Pi est la valeur des pixels dans le voisinage 3*3 de P

En effet le coefficient *CN* présente des caractéristiques (tableau 2) qui permettent d'identifier la nature d'une *minutie* en fonction du résultat obtenu lors du calcul de *CN*.

Tab. 2 : Identification d'une *minutie* à partir du calcul de *CN*

CN	Nature de la minutie en P
0	*Erreur* => Point isolé
1	Terminaison
2	*Erreur* => Point € Sillon
3	Divergence
4	*Erreur*=>Minutie à 4 branches

Dans un premier temps on repère l'emplacement de toutes les *minuties* présentes au sein de l'image de l'empreinte digitale, que l'on sauvegarde dans un liste *L1* en associant à chacun d'entre eux la position absolue (x_P,y_P) correspondante et le type de *minutie* dont il s'agit (*terminaison* ou *divergence*).

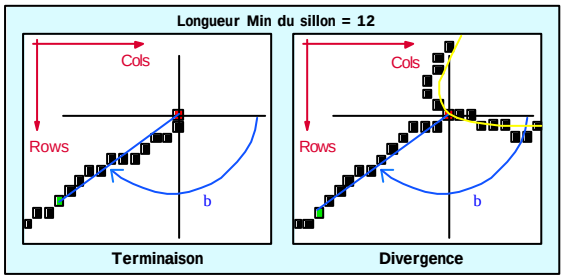


FIG. 3 : détermination de la direction des *minutie*

Afin de conserver une liste de *minuties* plus représentative de l'empreinte digitale d'un individu donné, on s'affranchit dans un second temps des *minuties* appartenant à des sillons de longueur relativement réduite par rapport à l'ensemble des principaux sillons de l'empreinte digitale. On se ramène ainsi à une liste de *minuties L2* dont la taille évolue approximativement entre 30 et 100 *minuties* (66% de *terminaisons* et 34% de *divergences* en moyenne) pour une image d'empreinte digitale peu bruitée, que l'on complémente en dernier lieu par une information supplémentaire propre à la nature des minuties: leur direction, déterminée comme indiqué sur la figure 3.

2.3 Comparaison des minuties

La phase de comparaison des *minuties* s'apparente à du « point pattern matching ». Le problème majeur des nombreux algorithmes proposés dans ce domaine, c'est la croissance exponentielle de leur complexité en fonction du nombre de points à traiter. Certaines améliorations ont été apportées en [12] par A.K. Jain avec le développement d'un algorithme réduisant la comparaison de nuages de points à un problème hiérarchique de minimisation d'énergie, basé sur une *Transformée de Hough Généralisée* (T.H.G.).
L'algorithme que nous proposons s'appuie sur la recherche d'un chemin orienté suivant le parcours vertical de l'image, permettant une comparaison rapide des nuages de minuties *Nr* et *Ni* appartenant respectivement aux empreintes digitales de *R*éférences et à *I*dentifier. Cette rapidité est liée à la non-exhaustivité de la comparaison, et le nombre moyen de comparaisons observé est typiquement 60 fois inférieur au nombre total de possibilités. Chaque chemin orienté est en fait constitué d'une série de vecteurs unissant les *minuties* deux à deux. Ce chemin est caractérisé par l'ensemble des angles aigus formés par deux vecteurs adjacents, et par les normes (distance euclidienne entre deux minuties) des différents vecteurs. L'orientation du chemin dans le sens vertical de l'image signifie que la minutie origine de chacun des vecteurs doit posséder une ordonnée plus petite que celle de la minutie terminaison. Chaque vecteur ne peut posséder qu'un unique successeur. On considère que *m* minuties sont communes à *Nc* et *Ni* si *m-1* vecteurs constituent un chemin comparable. En pratique, on commence par classer les minuties suivant leurs coordonnées croissantes : liste *Lr* pour les n_r minuties appartenant à *Nr, et* liste *Li* pour les n_i minuties appartenant à *Ni*. Puis on recherche à partir des n_r*–t (t étant le nombre de minuties fixé comme seuil de décision)* premières minuties de *Lr* s'il existe au moins n_l*-1* (n_l seuil d'accrochage) vecteurs similaires entre *Nc* et *Ni*. La rapidité de l'algorithme de comparaison dépend du choix du nombre minimum n_l de *minuties* pour poursuivre la recherche de chemin orienté à l'ensemble des *minuties* restantes appartenant aux listes *Lr* et *Lc*. Sa pertinence a été évaluée en le comparant à l'approche par THG, notamment en mesurant leur performance respective pour différentes variations de position angulaire du doigt par rapport au capteur lors de la saisie des images (test effectué sur environ 100 images). La figure 4 montre que notre procédé de comparaison a des performances sensiblement identiques à la THG lorsque la rotation entre l'empreinte digitale de référence et celle à identifier est inférieure à 4 degrés, et un

temps de calcul moyen de 60 ms (sur un PIII à 550 Mhz) au lieu de 4,5 s pour la THG.

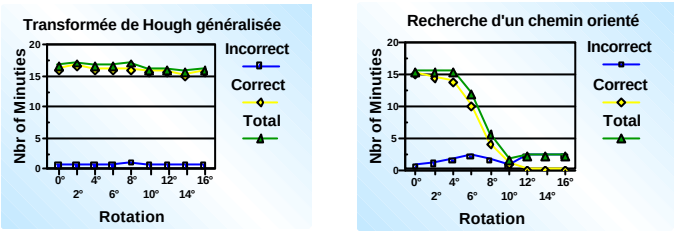


FIG. 4 : Performance des algorithmes de comparaison de *minuties* par THG & par recherche de chemin orienté.

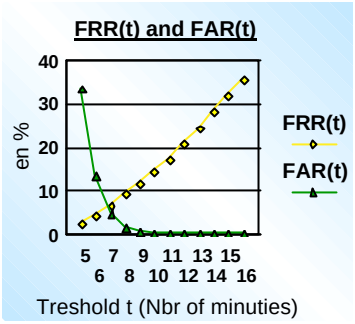


FIG. 5 : FRR et FAR en fonction du seuil de décision *t*

3. Sécurisation de l'authenfication sur carte à puce

L'intérêt d'associer la technologie des cartes à puces aux AFIS pour les sécuriser a déjà largement été discuté [13], [14]. En effet, dès lors que le protocole de comparaison des *minuties* s'effectue sur la carte à puce et que le gabarit de l'empreinte digitale de référence est stocké sur cette dernière, nous sommes assurés du minimum de sécurisation hardware nécessaire pour éviter toute attaque du système à ce niveau. La plate-forme biométrique est conçue autour d'un calculateur (PC) qui traite l'image d'empreinte digitale fournie par le « *TouchChip*™ » via USB et en extrait la liste de *minuties* caractéristiques. Ce fichier de *minuties*, d'une taille inférieure à 2 kO, est alors crypté, puis transféré sur la carte à puce « SmartJ™ » qui réalise la comparaison des gabarits (gabarit de référence chargé en EEPROM), et accepte ou non l'identité du prétendant. L'architecture du « SmartJ™ » repose sur un CPU RISC 32 bits, qui lui procure une puissance de calcul avoisinant les 25 MIPS à 33 Mhz (Pics à 40 MIPS). De plus, dotée d'un jeu d'instructions « Javacard™ », la « SmartJ™ » offre un maximum de flexibilité et de simplicité pour le développement de ce type d'applications biométriques.

4. Résultats et conclusion

Les travaux biométriques présentés dans cet article ont conduit à l'élaboration d'un système d'identification d'individus par reconnaissance d'empreintes digitales dont la phase d'authentification proprement dite (comparaison des nuages de *minuties*) a été sécurisée sur une carte à puce « SmartJ™ ». L'algorithme par recherche de chemin orienté, implanté pour cette phase de comparaison, effectue l'appariement des minuties en moins de 2 s (valeur maximale relevée). Sur une base de données comprenant plus de 600 images d'empreintes digitales, suivant le seuil de décision *t* fixé (de 8 à 12 *minuties*), le système global présente un tau de fausse acceptation (False Acceptance Ratio = F.A.R.) variant de 0.1 à 1%, pour un tau de faux rejet (False Reject Ratio = F.R.R.) variant de 9 à 18% : FAR(t) et FFR(t) en figure 5. Ces résultats démontrent qu'il y a bien adéquation entre la complexité de l'algorithme de comparaison par recherche de chemin orienté et les capacités offertes à ce jour par une carte à puce.

Références

[1] Y. Belgnaoui, J-C. Guézel et T. Mahé. *La biométrie, sésame absolu*. Industries et techniques, Juillet 2000.

[2] Osterburg, Parthasarathy, Raghanvan et Slove. *Development of a mathematical formula for the calculation of fingerprint probabilities based on individual characteristics*. Journal of the American statistical association, Vol. 72, n° 360.

[3] U. Halici et G. Onguin. *Fingerprint classification through self-organizing feature maps modified to treat uncertainties*. Proceedings of the IEEE, Vol. 84, n° 10, Octobre 1996.

[4] R. Capelli, A. Lumini, D. Maio et D. Maltoni. *Fingerprint classification by directional image partitioning*. IEEE Transactions on pattern analysis and machine intelligence, Vol. 21, n° 5, Mai 1999.

[5] A.K. Jain et S. Pankanti. *FingerCode : a filterbank for fingerprint representation and matching*. IEEE, 1999.

[6] A.K. Jain, L. Hong, S. Pankanti et R. Bolle. *An identity-authenfication system using fingerprints*. Proceedings of the IEEE, Vol. 85, n° 9, Septembre 1997.

[7] D. Maio et D. Maltoni. *Neural Network based minutiae filtering in fingerprints*. IEEE, 1998.

[8] J.R. Parker. *Algorithms for image processing and computer vision*. Wiley & Sons, Novembre 1996.

[9] Haralick, Robert et Shapiro. *Computer and robot vision*. Vol. 1, Addison-Wesley, 1992.

[10] Y. Emyrodlu. *Fingerprint image: enhancement and recognition*. Rapport de thèse, Université d'Herdforshire, Octobre 1997.

[11] J.G. Daugman. *Uncertainty relation for resolution in space, spatial frequency, and orientation optimized by two-dimensional visual cortical filters*. J. Opt. Soc. Am., Vol. 2, n° 7, Juillet 1985.

[12] A.K. Jain, S. Shaoyun, K. Karu, N.K. Ratha. *A real-time matching system for large fingerprint databases*. IEEE Trans. on pattern analysis and machine intelligence, Vol. 18, n° 8, Août 1996.

[13] G. Hachez, F. Koeune et JJ. Quisquater. *Biometrics, acces control, smart cards : a not simple combination*. European IST project BANCA report.

[14] D. Guinier. *Towards a future security bio-smart card*. 10th Annuel Canadian Information Technology Security Symposium, Ottawa, Juin 1998.

[15] www.st.com