Sécurité des systèmes biométriques : révocabilité et protection de la vie privée

Rima Ouidad Belguechi

Résumé

En référence à la sécurité informatique, la biométrie concerne l'utilisation des caractéristiques morphologiques ou comportementales pour déterminer ou vérifier l'identité d'un utilisateur.

Récemment, des discussions sur la sécurité des systèmes biométriques ont émergé. Le stockage des données de référence pose de sérieux problèmes de sécurité et d'invasion de vie privée : manipulation d'informations sensibles, reconstruction de la biométrie d'origine à partir du modèle stocké, construction d'un échantillon biométrique falsifié, utilisation secondaire des informations biométriques (surveillance, discrimination, etc.) ou l'impossibilité de révoquer l'identifiant biométrique lorsqu'un vol d'identité à eu lieu. La sécurité du modèle biométrique est l'une des tâches les plus cruciales dans la conception d'un système biométrique sécurisé. Considérant la modalité d'empreintes digitales, nous proposons dans cette thèse deux types de solution à ce problème. La première au niveau algorithmique et la seconde au niveau architectural.

Dans l'approche fonctionnelle ou algorithmique, nous traitons des schémas de protection des modèles biométriques. Il s'agit d'un nouveau concept dont le but est de générer une biométrie révocable en appliquant des transformations, idéalement à sens unique. Plusieurs schémas de biométrie révocable ont été proposés dans la littérature, mais pour l'heure, des efforts sont attendus pour améliorer leur fiabilité. Un schéma de biométrie révocable est une chaine de traitement qui inclut les phases d'extraction des caractéristiques, de transformation et de comparaison. Toutes ces phases sont traitées dans cette thèse. Principalement, nous nous intéressons aux descripteurs de texture d'empreintes digitales. Un premier schéma révocable, en utilisant une description de la texture globale de l'empreinte est proposé. Pour améliorer les résultats, ce schéma est étendu aux minuties. Une approche de transformation par projection aléatoire est ensuite opérée.

L'une des difficultés est d'évaluer correctement le schéma de biométrie révocable généré. Nous proposons un modèle d'évaluation basé sur un ensemble de métriques quantitatives, pour mesurer les critères de sécurité et de protection de vie privée souhaités.

Dans la seconde solution, nous proposons d'utiliser une architecture fermée pour le système de vérification biométrique. Les cartes à puce sont utilisées pour une meilleure gestion des données d'authentification de l'utilisateur. Un système de biométrie révocable avec un algorithme de comparaison sur la carte est proposé. Un tel système offre des avantages combinés de révocabilité et de confidentialité du modèle biométrique. Nous utilisons une JavaCard que nous gérons conformément à la norme PKCS15 pour plus d'interopérabilité.

Nous proposons ensuite d'étudier les possibilités de menaces de vie privée dans l'application des passeports biométriques. Nous concluons par le fait que la biométrie révocable serait souhaitable pour améliorer la protection des données biométriques contenues dans la puce du passeport.

Bibliographie

[1] Andy Adler. Handbook of biometrics, chapter Biometric system security. 2007.

[2] T. Ahmad, J. Hu, and S. Wang. Pair-polar coordinate-based cancelable fingerprint templates. Pattern recognition, 44(1), January 2011.

[3] ANSI-INCITS. Ansi-incits fingerprint minutia format for data interchange, 2008.

[4] A. Arakala, J. Je_ers, and K. J. Horadam. Fuzzy extractors for minutiae-based fingerprint authentication. In 2nd International Conference on Biometrics, 2007.

[5] G. Avoine, K. Kalach, and J.J. Quisquater. Epassport : Securing international contacts with contactless chips. In Springer-Verlag, editor, Proceedings of FC'08, Lecture Notes in Computer Sciences, volume 5143, pages 141–155, 2008.

[6] R. Ang, S.N. Rei, and L. McAven. Cancellable key-based fingerprint templates. In Information Security and Privacy : 10th Australasian Conference, ACISP 2005, Brisbane, Australia, pages 242–252, 2005.

[7] F. Benhammadi, M.N. Amirouche, H. Hentous, K. Bey Beghdad, and M. Aissani. Fingerprint matching from minutiae texture maps. Pattern recognition, 40 :189–197, 2007.

[8] M. Barni, T. Bianchi, D. Catalano, M. D. Raimondo, R. D. Labati, P. Failla, D. Fiore, R. Lazzeretti, V. Piuri, F. Scotti, and A. Piva. Privacy-preserving fingercode authentication. In 12th ACM Multimedia and Security Workshop, 2010.

[9] J. Breebaart, C. Busch, J. Grave, and E. Kindt. A reference architecture for biometric template protection based on pseudo identities. In Proceedings of the Special Interest Group on Biometrics and Electronic Signatures (BIOSIG), Germany, 2008.

[10] J. Bringer and H. Chabanne. An authentication protocol with encrypted biometric data. In AfricaCrypt'09, 2009.

[11] R. Bolle, J. Connell, S. Pankanti, N. Ratha, and A. Senior. Guide to Biometrics. 2003.

[12] R. M. Bolle, J. H. Connell, and N. K. Ratha. Biometric perils and patches. Pattern Recognition, 35(12) :2727–2738, 2002.

[13] J. Bringer and V. Despiegel. Binary feature vector fingerprint representation from minutiae vicinities. In Fourth IEEE International Conference on Biometrics : Theory Applications and Systems (BTAS), 2010.

[14] R. Belguechi. Reconnaissances des empreintes digitales par une approche hybride. Master's thesis, Ecole nationale superieure d'informatique, 2006.

[15] R. Belguechi, V. Alimi, C. Rosenberger. "Secure and Privacy Preserving Management of Biometric Templates". In The third Norsk Information security conference (NISK). Norway. 2010.

[16] R. Belguechi, B. Hemery, C. Rosenberger. "Authentification révocable pour la vérification basée texture d'empreintes digitales". In Congrès Francophone en Reconnaissance des Formes et l'Intelligence Artificielle (RFIA). France, 2010.

[17] D. Petrovska-Delacrétaz, S. Kanade, R. Belguechi, C. Rosenberger, B. Dorizzi. "L'usage de la biométrie est il contradictoire avec le respect de la vie privée ?". In Workshop Interdisciplinaire sur la Sécurité Globale (WISG). France. 2010.

[18] R. Belguechi, C. Rosenberger, S. Ait-Aoudia. "BioHashing for securing fingerprint minutiae templates". In the 20th International Conference on Pattern Recognition (ICPR). Istanbul. p. 1168-1171, 2010.

[19] R. Belguechi, C. Rosenberger, S. Ait-Aoudia. "Cancelable authentication based on fingerprints texture". In International congress on models, optimization and security of systems (ICMOSS).Tiaret, Algérie. 2010.

[20] R. Belguechi, T. Le Gof, E. Cherrier, C. Rosenberger. "Etude de la robustesse d'un système de biométrie révocable". In Conférence sur la sécurité des architectures réseaux et des systèmes d'information (SAR SSI). La Rochelle, France. 2011.
[21] R. Belguechi, E. Cherrier, M. El Abed and C. Rosenberger. "Evaluation of Cancelable Biometric Systems : Application to Finger-Knuckle-Prints". In IEEE International Conference on Hand-Based Biometrics (ICHB). Hong Kong. p. 1-6, 2011.
[22] R. Belguechi, E. Cherrier, C. Rosenberger. "Texture based Fingerprint BioHashing: Attacks and Robustness". In IEEE/IAPR International Conference on Biometrics (ICB). New Delhi. p. 196-201, 2012.
[23] R. Belguechi, E. Cherrier, C. Rosenberger. "How to Evaluate Transformation Based Cancelable Biometric Systems ?". In NIST International Biometric Performance Testing Conference (IBPC). Gaithersburg, United states. 2012.
[24] R. Belguechi, P. Lacharme, C. Rosenberger and S. Ait-Aoudia. "Enhancing the privacy of electronic passports". In International Journal of Information Technology and Management (IJITM). Special Issue on : "Advances and Trends in Biometrics". Inderscience. vol. 11, p. 1-16, 2012.
[25] R. Belguechi, E. Cherrier, C. Rosenberger and S. Ait-Aoudia. "Operational Bio-Hash to Preserve Privacy of Fingerprint Minutiae Templates". In IET journal on Biometrics. Vol. 2(2), p. 76-84, June 2013.
[26] R. Belguechi, E. Cherrier, C. Rosenberger C and S. Ait-Aoudia. "An integrated framework combining Bio-Hashed minutiae template and PKCS15 compliant card for a better secure management of fingerprint cancelable templates". In Elsevier Journal on Computers & Security. Vol. 39, p. 325-399, November 2013.
[27] I. Buhan, E. Kelkboom, and K. Simoens. A survey of the security and privacy measures for anonymous biometric authentication systems. In Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2010.
[28] I. Buhan. Cryptographic keys from Noisy Data Theory and Applications. PhD thesis, University of Twente, Netherlands, 2008.
[29] D. Gafurov B. Yang, C. Busch and P. Bours. Renewable minutiae templates with tunable size and security. In International Conference on Pattern Recognition, 2010.
[30] A. Cavoukian. Privacy and biometrics. In Proceedings of International Conference on Privacy and Personal Data Protection, Hong Kong, China, 1999.
[31] Ann Cavoukian. Fingerprint biometrics: Address privacy before deployment. Technical report, Information and privacy commissioner, Ontario, November 2008.
[32] S. Chikkerur, A.N. Cartwright, and V. Govindaraju. K-plet and coupled bfs : A graph based fingerprint representation and matching algorithm. In Proc. Int. Conf. on Biometrics, LNCS 3832, page 309U″ 315, 2006.
[33] S. Chikkerur, A.N. Cartwright, and V. Govindaraju. Fingerprint enhancement using stft analysis. Pattern Recognition, 40(1) :198–211, 2007.
[34] R. Cappelli, M. Ferrara, and D. Maltoni. On the operational quality of fingerprint scanners. IEEE Transactions on Information Forensics and Security, 3(2) :192–202, 2008.
[35] R. Cappelli, M. Ferrara, and D. Maltoni. Minutia cylinder-code : A new representation and matching technique for fingerprint recognition. IEEE transactions Pattern Analysis and Machine Intelligence, 32 :2128–2141, 2010.
[36] T.C. Clancy, N. Kiyavash, and D. J. Lin. Secure smartcard-based fingerprint authentication. In ACM SIGMM 2003 Multimedia, Biometrics Methods and Applications Workshop, pages 45–52, 2003.

[37] R. Cappelli, A. Lumini, D. Maio, and D. Maltoni. Evaluating minutiae template vulnerability to masquerade attack. In 5th Workshop on Automatic Identification Advances Technologies (AutoID2007), Alghero, June 2007.
[38] R Cappelli, A Lumini, D. Maio, and D. Maltoni. Fingerprint image reconstruction from standard templates. IEEE Transactions on Pattern Analysis and Machine Intelligence, 29(9) :1489–1503, September 2007.
[39] Privacy Commissioners. Privacy by design resolution. In 32nd international conference of data protection and privacy commissioners, 2010.
[40] T. Chotia and V. Smirnov. A traceability attacks against e-passports. In Proceedings of FC'10, Lecture Note in Computer Sciences, Springer-Verlag, 2010.
[41] R. Chaabouni and S. Vaudenay. The extended access control for machine readable travel documents. In Proceedings of BIOSIG'09, volume 155, pages 93–103, 2009.
[42] J. Daugman. The importance of being random : statistical principles of iris recognition. Pattern Recognition, 36(2) :279–291, 2003.
[43] G. I. Davida, Y. Frankel, and B. J. Matt. On the relation of error correction and cryptography to an on line biometric based identification scheme. In WCC99, Workshop on coding and cryptography, 1999.
[44] S. Dasgupta and A. Gupta. An elementary proof of the johnson-lindenstrauss lemma. Technical Report TR-99-006, International Computer Science Institute, Berkeley, CA, 1999.
[45] R.O. Duda, P.E. Hart, and D.G. Stork. Pattern classification. Wiley interscience, 2000.
[46] S.C. Draper, A. Khisti, E. Martinian, A. Vetro, and J.S. Yedidia. Using distributed source coding to secure fingerprint biometrics. In IEEE International Conference on Acoustics, Speech and Signal Processing, 2007.
[47] V. Domnesque. Carte d'identit électronique & conservation des données biométriques. Master's thesis, Université de Lille, 2004.
[48] Y. Dodis, L. Reyzin, and A. Smith. Fuzzy extractors : How to generate strong keys from biometrics and other noisy data ? in Adv. in Cryptology Eurocrypt 2004, LNCS, 3027 :523–540, 2004.
[49] C. Domeniconi, S. Tari, and P. Liang. Direct gray scale ridge reconstruction in fingerprint images. In ICASSP, 1998.
[50] Mohammed El-Abed. Evaluation des systèmes biométriques. PhD thesis, Université de Caen, 2011.
[51] J. Feng. Combining minutiae descriptors for fingerprint matching. Pattern Recognition, 41(1) :342–352, 2008.
[52] J. Feng and A. Jain. Fm model based fingerprint reconstruction from minutiae template. In International conference on Biometrics (ICB), 2009.
[53] M. Ferrara, D. Maltoni, and R. Cappelli. Non-invertible minutia cylinder-code representation. IEEE Trans. Inf. Forensics Secur., 7 :1727–1737, 2012.
[54] Bundesalt fur Sicherheit in der Informationstechni. Advanced security mechanism for machine readable travel documents. Technical report, 2008.
[55] M. Govan and T. Buggy. A computationally e_cient fingerprint matching algorithm for implementation on smartcards. In in Proc. Int. Conf. on Biometrics : Theory, Applications, and Systems (BTAS 07), pages 1–6, 2007.
[56] J. Galbally, R. Cappelli, A. Lumini, D. Maltoni, and J. Fierrez-Aguilar. Fake fingertip generation from a minutiae template. In 19th International Conference on Pattern Recognition (ICPR2008), Tampa, Florida, USA, pages 1–4. IBM Best Student Award, December 2008.
[57] Common Criteria Working Group. Biometric evaluation methodology supplement, 2002.

[58] International Biometric group. Biometrics market and industry report 2009-2014. Technical report, 2013.
[59] M.D. Garris, C.I. Watson, R.M. McCabe, and C.L. Wilson. Users guide to nist fingerprint image software (nfis). Technical report, National Institute of Standards and Technology, 2002.
[60] C.J. Hill. Risk of masquerade arising from the storage of biometrics. Bachelor of science, Australian National University, 2001.
[61] W Hoffmann. Iterative algorithms for gram-schmidt orthogonalization. Computing, 41(4) :335–348, 1989.
[62] M. Hlavac and T. Rosa. A note on the relay attacks on e-passport : the case of czech e-passport. Technical report, 2007.
[63] O. Henniger, D. Scheuermann, and T. Kniess. On security evaluation of fingerprint recognition systems. In International biometric Performance testing conference, 2010.
[64] L. Hong, Y.Wan, and A. Jain. Fingerprint image enhancement : Algorithm and performance evaluation. IEEE transactions on Pattern Analysis and Machine Intelligence, 20 :777–789, 1998.
[65] A. Hafiane and B. Zavidovique. Local relational string and mutual matching for image retrieval. Inf. Process. Manage., 44 :1201–1213, 2008.
[66] Tanya Ignatenko. Secret-Key Rates and Privacy Leakage in Biometric Systems. PhD thesis, Eindhoven : Technische Universteit Eindhoven, 2009.
[67] ISO/IEC. Iso/iec 19795. information technology - biometric performance testing and reporting -, 2006.
[68] ISO/IEC. Iso/iec cd 19792 : Information technology - security techniques – security evaluation of biometrics, 2006.
[69] ISO/IEC. International standard iso/iec 19794-2 information technology – biometric data interchange formats - part 2 : Finger minutia data, 2008.
[70] ISO/IEC. Iso/iec 15408. security techniques - evaluation criteria for it security -, 2009.
[71] ISO/IEC. Iso/iec 24745 :2011 information technology - security techniques – biometric information protection., 2011.
[72] A Jain, L Hong, S Pankanti, and R Bolle. An identity-authentification system using fingerprints. Proceedings of The IEEE, 85(9), 1997.
[73] A.T.B. Jin, D.N.C. Ling, and O.T. Song. An e_cient fingerprint verification system using integrated wavelet and fourier-mellin invariant transform. Image and Vision Computing, 22(6) :503–513, 2004.
[74] A. Juels, D. Molnar, and D. Wagner. Security and privacy issues in e-passports. In IEEE SecureComm, 2005.
[75] A. K. Jain, K. Nandakumar, and A. Nagar. Biometric template security. EURASIP Journal on Advances in Signal Processing, pages 1–17, 2008.
[76] A.K. Jain, S. Prabhakar, L. Hong, and S. Pankanti. Filterbank based fingerprint matching. IEEE Trans Image Process, 9(5) :846–859, 2000.
[77] A. Juels and M. Sudan. A fuzzy vault scheme. In Proceedings of IEEE International Symposium on Information Theory, Lausanne, Switzerland. IEEE Press, 2002.
[78] Z Jin, A.B.J. Teoh, T.S. Ong, and C. Tee. Fingerprint template protection with minutiae-based bit-string for security and privacy preserving. Expert systems with applications, Elsevier, 39 :6157–6167, 2012.
[79] A. Juels and M. Wattenberg. A fuzzy commitment scheme. In Sixth ACM Conference on Computer and Communications Security, pages 28–36. ACM Press, 1999.
[80] S. Kaski. Dimensionality reduction by random mapping. In Int. Joint Conf. on Neural Networks, volume 1, pages 413–418, 1998.

[81] A. Kong, K.H. Cheung, D. Zhang, M. Kamel, and J. You. An analysis of biohashing and its variants. Pattern Recognition, 39, 2005.
[82] G Kumar, S Tulyakov, and V. Govindaraju. Combination of symmetric hash functions for secure fingerprint matching. In International conference on pattern recognition, 2010.
[83] C. Lee, J.Y. Choi, K.A. Toh, S. Lee, and J. Kim. Alignment-free cancelable fingerprint templates based on local minutiae information. IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS, 37(4), August 2007.
[84] C. Li and J. Hu. Attacks via record multiplicity on cancelable biometrics templates. Concurrency Computat. : Pract. Exper, 2013.
[85] E. Lim, X. Jiang, and W. Yau. Fingerprint quality and validity analysis. In IEEE ICIP, 2002.
[86] C. Lee and J. Kim. Cancelable fingerprint templates using minutiae-based bit-strings. Journal of Network and Computer Applications, 33 :236–246, 2010.
[87] A. Lumini and L. Nanni. Empirical tests on biohashing. NeuroComputing, 69(16) :2390–2395, October 2006.
[88] A. Lumini and L. Nanni. An improved biohashing for human authentication. Pattern recognition, 40 :1057–1065, 2007.
[89] J. Lei, Q. Peng, X. You, H. Jabbar, and P. Wang. Fingerprint enhancement based on wavelet and anisotropic filtering. International journal of pattern recognition and artificial intelligence, 26, 2012.
[90] J.M.G. Linnartz and P. Tuyls. New shielding functions to enhance privacy and prevent misuse of biometric templates. In 4th International Conference on Audioand Video-Based Biometric Person Authentication, volume 2688, pages 393–402, 2003.
[91] G. Madlmayr, O. Dillinger, J. Langer, and C. Scha_er. The benefit of using sim application toolkit in the context of near field communication application. In ICMB, 2007.
[92] E. Mordini and S. Massari. Body, biometrics and identity. Bioethics journal, 2008.
[93] D. Maltoni, D. Maio, A.K. Jain, and S. Prabhakar. Handbook of Fingerprint Recognition. Springer, 2009.
[94] T Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino. Impact of artificial gummy fingers on fingerprint systems. Proceedings of SPIE , Optical Security and Counterfeit Deterrence Techniques IV, 4677, 2002.
[95] R.M. McCabe and E.M. Newton. Data format for the interchange of fingerprint, facial and other biometric information, 2007.
[96] A. Nagar and A.K. Jain. On the security of non-invertible fingerprint template transforms. In WIFS, 2009.
[97] K. Nandakumar, A.K. Jain, , and S. Pankanti. Fingerprint-based fuzzy vault: Implementation and performance. IEEE Transactions on Information Forensics and Security, 2 :744–757, December 2007.
[98] L. Nanni and A. Lumini. Descriptors for image-based fingerprint matchers. Expert Systems With Applications, 36(10), 2009.
[99] A. Nagar, K. Nandakumar, and A.K. Jain. Biometric template transformation : A security analysis. Proceeding of SPIE, Electronic Imaging, Media Forensics and Security, Sans Jose, January 2010.
[100] A. Nagar, K. Nandakumar, and A.K. Jain. A hybrid biometric cryptosystem for securing fingerprint minutiae templates. Pattern Recognition Letters, 31(8) :733–741, 2010.

[101] A. Nagar, S. Rane, and A. Vetro. Privacy and security of features extracted from minutiae aggregates. In International Conference on Acoustics, Speech and Signal Processing, 2010.
[102] International Civil Aviation Organization. Doc 9303 : Machine readable travel documents. Technical report, 2004.
[103] N. Otsu. A threshold selection method from gray level histograms. IEEE Transactions on Systems, Man and Cybernetics, 9 :62–66, 1979.
[104] PKCS11. Pkcs11 : Cryptographic token interface standard, 2000.
[105] PKCS15. Pkcs15 : Cryptographic token information format standard, 2000.
[106] S. Pankanti, S. Prabhakar, and A. Jain. On the individuality of fingerprints. IEEE Transactions on Pattern Analysis And Machine Intelligence, 24(8) :1010–1025, 2002.
[107] F. Quan, S. Fei, C. Anni, and Z. Feifei. Cracking cancelable fingerprint template of ratha. In International Symposium on Computer Science and Computational Technology, 2008.
[108] L. Qiong, L. Zhaoping, and N. Xiamu. Analysis and problems on fuzzy vault scheme. In International conference on intelligent information hiding and multimedia signal processing, 2006.
[109] A.R. Rao. A Taxonomy for Texture Description and Identification. Springer-Verlag, New York, 1990.
[110] N. K. Ratha, J. H. Connell, and R. M. Bolle. Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal, 40(03) :614–634, 2001.
[111] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle. Generating cancelable fingerprint templates. IEEE Transactions on Pattern Analysis and Machine Intelligence, 29(4) :561–572, 2007.
[112] N Ratha, S Chen, and A Jain. Adaptive flow orientation based texture extraction in fingerprint images. Pattern recognition, 28(11) :1657–1672, Nov 1995.
[113] N.K. Ratha, K. Karu, S. Chen, and A.K. Jain. A real-time matching system for large fingerprint databases. IEEE Transactions on Pattern Analysis Machine Intelligence, 18(8) :799–813, 1996.
[114] H. Richter, W. Mostowski, and E. Poll. Fingerprinting passports. In Spring Conference on Security, 2008.
[115] A. Ross, J. Shah, and A.K. Jain. From template to image : reconstructing fingerprints from minutiae points. IEEE Transactions on Pattern Analysis and Machine Intelligence, Special Issue on Biometrics, 29(4) :544–560, 2007.
[116] Christian Rathgeb and Andreas Uhl. A survey on biometric cryptosystems and cancelable biometrics. EURASIP Journal on Information Security, 3, 2011.
[117] W. J. Scheirer and T. E. Boult. Cracking fuzzy vaults and biometric encryption. In Proceedings of Biometrics Symposium, 2007.
[118] W.J. Scheirer and T.E. Boult. Bio-cryptographic protocols with bipartite biotokens. In Proc. Biometric Symposium, 2008.
[119] B. Schneier. The uses and abuses of biometrics. In Comm. ACM, volume 42, page 136, Aug 1999.
[120] L.L. Shen, A. Kot, and W.M. Koo. Quality measures of fingerprint images. In 3rd international conference AVBPA, pages 182–271, June 2001.
[121] A. Smith. Maintaining secrecy when information leakage is unavoidable. PhD thesis, Massachusetts institute of technology, 2004.
[122] B.G. Sherlock, D.M. Monro, and K. Millard. Fingerprint enhancement by directional fourier filtering. In Visual Image Signal Processing, 141 :87–94, 1994.
[123] D.J. Solove. Understanding privacy. Harvard university press, 2008.

[124] R. Sanchez-Reillo. Including biometric authentication in a smart card operating system. In AVBPA, 2001.
[125] B. Struif and D. Scheuermann. Smartcards with biometric user verification. In IEEE International Conference on Multimedia and Expo, 2002.
[126] J. Stapleton. American national standard x9.84-2001 biometric informatio, management and security, 2002.
[127] K. Simoens, P. Tuyls, and B. Preneel. Privacy weaknesses in biometric sketches. 30th IEEE Symposium on Security and Privacy, pages 188–203, 2009.
[128] K Simoens, B Yang, X Zhou, F Beato, C Busch, E.M. Newton, , and B. Preneel. Criteria towards metrics for benchmarking template protection algorithms. In International conference on biometrics, 2012.
[129] P. Tuyls, A.H.M. Akkermans, T.A.M. Kevenaar, G.J. Schrijen, A.M. Bazen, and R.N.J. Veldhuis. Practical biometric authentication with template protection. In International Conference on Audio- and Video-Based Biometric Person Authentication, volume 3546, pages 436–446, 2005.
[130] S. Tulyakov, F. Farooq, and V. Govindaraju. Symmetric hash functions for fingerprint minutiae. In ICAPR, 2005.
[131] P. Tuyls and J. Goseling. Capacity and examples of template protection biometric authentication systems. In LNCS, editor, Biometric authentication workshop, volume 3087, pages 158–180, 2004.
[132] K. Takahashi and S. Hirata. Parameter management schemes for cancelable biometrics. In Computational Intelligence in Biometrics and Identity Management, 2011.
[133] Michael Thieme. Identifying and reducing privacy risks in biometric systems. In 13th annual conference on computers, freedom & privacy, 2003.
[134] M. Tuceryan and A.K. Jain. The Handbook of Pattern Recognition and Computer Vision (2nd Edition), chapter Texture analysis (2.1), pages 207–248. 1998.
[135] M. Tico and P. Kuosmanen. Fingerprint matching using an orientation-based minutia descriptor. Pattern Analysis and Machine Intelligence, 25(8) :1009–1014, 2003.
[136] A.B.J. Teoh, Y.W. Kuan, and T. Kar-Ann. Cancellable biometrics and user-dependent multi-state discretization in biohash. Pattern analysis & applications, 13 :301–307, 2010.
[137] Andrew B.J. Teoh, YipWai Kuanb, and Sangyoun Leea. Cancellable biometrics and annotations on biohash. pattern recognition, 41 :2034–2044, 2007.
[138] A. B.J. Teoh and D. C.L. Ngo. Cancellable biometerics featuring with tokenised random number. Pattern Recognition Letters, 26 :1454–1460, 2004.
[139] A. Teoh, D. Ngo, and A. Goh. Biohashing : two factor authentication featuring fingerprint data and tokenised random number. Pattern recognition, 37(11), 2004.
[140] D. Harwood T. Ojala, M. Pietikeinen. A comparative study of texture measures with classification based on feature distributions. Pattern Recognition, 29 :51–59, 1996.
[141] A.O. Thomas, N. Ratha, J. Connell, and R. Bolle. Comparative analysis of registration based and registration free methods for cancelable fingerprint biometrics. In 19th International Conference on Pattern Recognition, 2008.
[142] A. Tabassi, C. L.Wilson, and C. IWatson. Fingerprint image quality. Technical report, National Institute of Standards and Technology (NIST), August 2004.
[143] U. Uludag and A.K. Jain. Attacks on biometric systems : A case study in fingerprints. In Proc. Int'l Soc. Optical Eng. (SPIE), Security, Steganography, and Watermarking of Multimedia Contents VI, pages 622–633, June 2004.
[144] U. Uludag and A.K. Jain. Securing fingerprint template : Fuzzy vault with helper data. In Computer Vision and Pattern Recognition Workshop (CVPR), June 2006.

[145] M Upmanyu, A Namboodiri, K Srinathan, and C. V. Jawahar. Blind authentication : A secure crypto-biometric verification protocol. IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, 5(2), June 2010.
[146] S. Wang and J. Hu. Alignement-free cancellable fingerprint template design : a densely infinite-to-one mapping (ditom) approach. pattern recognition, Elsevier, 45(12) :4129–4137, December 2012.
[147] L. Wolf, T. Hassner, and Y. Taigman. Descriptor based methods in the wild. In Real-Life Images workshop at the European Conference on Computer Vision (ECCV), October 2008.
[148] W.J. Wong, A.B.J. Teoh, M.L.D. Wong, and Kho. Y.H. Enhanced multi-line code for minutiae-based fingerprint template protection. Pattern Recognition Letters, 34 :1221–1229, 2013.
[149] Y. Wang W. Zhang. Core-based structure matching algorithm of fingerprint verification. In 16th International Conference on Pattern Recognition, 2002.
[150] H. Xu, R. N. J. Veldhuis, A. M. Bazen, T. A. M. Kevenaar, T. A. H. M. Akkermans, and B. Gokberk. Fingerprint verification using spectral minutiae representations. Transaction on Information Forensics and Security, 4(3) :397–409, 2009. [cité p. 45]
[151] N. Yager and A. Amin. Coarse fingerprint registration using orientation fields. EURASIP Journal on Applied Signal Processing, 13 :2043–2053, 2005.
[152] B. Yang, D. Hartung, K. Simeons, and C. Busch. Dynamic random projection for biometric tempalte protection. In BTAS, 2010.
[153] S. Ye, Y. Luo, J. Zhao, and S. Cheung. Anonymous biometric access control. EURASIP J, 2009.
[154] Xuebing Zhou. Privacy and security assessment of biometric template protection. PhD thesis, Fachbereich Informatik Universitat Darmstadt, Germany, 2012.
[155] X. Zhou, A. Kuijper, R. Veldhuis, and C. Busch. Quantifying privacy and security of biometric fuzzy commitment. In IEEE Proc in International Joint Conference on Biometrics (IJCB), 2011.
[156] W. Zhang and Y. Wang. Core-based structure matching algorithm of fingerprint verification. In Proc. 16th IEEE International Conference on Pattern Recognition, 2002.
[157] X. Zhou, S.D. Wolthusen, C. Busch, and A. Kuijper. Feature correlation attacks on biometric privacy protection scheme. In IEEE Proc in 5th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2009.
[158] X Zhou, S.D. Wolthusen, C Busch, and A. Kuijper. A security analysis of biometric template protection schemes. Lecture Notes in Computer Science, Springer-Verlag, pages 429–438, 2009.