TokenSign: Using Revocable Fingerprint Biotokens and Secret Sharing Scheme as Electronic Signature

Fahad Alsolami
Department of Information Technology
King Abdulaziz University , KSA

***Abstract*—Electronic signature is a quick and convenient tool, used for legal documents and payments since business practices revolutionized from traditional paper-based to computer-based systems. The growing use of electronic signature means they are used in many applications daily, both in government and private organizations such as financial services, where an electronic signature is taken from group of people at once to cash checks or perform a transaction approval. However, non-repudiation and authentication issues remain highlighted concerns for electronic signature. To overcome these obstacles, we propose a TokenSign system that uses revocable fingerprints biotokens with Secret Sharing as electronic signature. TokenSign maintains two layers of security. First, TokenSign scheme transforms and encrypts a user fingerprint data. Second, TokenSign embeds a shared secret inside the encrypted fingerprints. Then, TokenSign Scheme distributes all shares of electronic signatures over multiple clouds. During the matching/signing process, TokenSign utilizes threading to do parallel matching for the fingerprints in its secure encrypted form without decrypting the data. Finally, TokenSign scheme applies Secret Sharing scheme to compute the shared secret, producing an electronic signature. As a result, our experiments show that TokenSign scheme achieves comparable accuracy and improves performance comparing to the two baselines.**

***Keywords*—Signature; Fingerprint; Electronic; Security**

I. Introduction

Electronic signature affords many benefits for individuals and organizations regarding signing documents or filing and electronic payment. Online document signing has been used in many applications daily, either in governments or private organizations [1]. These services have obvious advantages such as speeding up the work process and allowing for high production [2]. Electronic payment, such as Apple pay, Samsung pay, etc., is considered the most growing technology in financial services and has impacted the business revolution and increase the online e-commerce [3]. The growth of electronic payment has many reasons behind it. For an organization, it is a trusted, easy, fast and convenient way to receive payment from customers; for an individual, it provides convenience in that customers do not need to carry cash for shopping. Therefore, these huge benefits attract many technology companies and researchers to invent more and more tools/applications for financial services [4].

While electronic signature provides a great verity of advantages, the non-repudiation and authentication issues remain a research challenge. Because a signature is not performed face-to-face, there is a concern about non-repudiation issues in electronic signature when one party denies his/her signature [5]. Regarding electronic payment system, according to Abrazhevich et al [6], there are some limitations in electronic payment systems such as usability, security, and trust. Kahn et al [7] shed light on the effect of theft incidents on online banking and how it could limit the electronic payment systems. On the other hand, authentication issues remain a research challenge in electronic signature and electronic payment. The invention [8] implemented an authentication method of electronic signature by generating a digital work fingerprint and a representation file which were transmitted to the client to be signed. In terms of electronic payment authentication, Kalakota et al [9] describes the fraud against e-commerce which increase the cyberattacks. Thus, electronic payment needs authentication methods that are secure and reliable [9]. Biometrics have been suggested as a replacement for the traditional username/password in electronic payment [10]. Biometrics provide a unique identity which enhance the security and build trust to a greater degree [11]. However, despite the biometrics advantages, there are some concerns regarding privacy and security, especially if biometric data get compromised [12].

To address the privacy and security issues, particularly the non-repudiation and authentication of electronic signature, we propose the TokenSign scheme. TokenSign is a new electronic signature for legal documents and financial services using a fingerprint as a signature. Fingerprints are suggested as each is unique; no two people share the same fingerprint pattern. TokenSign scheme utilizes the revocable fingerprint biotokens (Biotope) [13], Bipartite token [14], and the secret-sharing scheme [15] while performing an electronic signature online for legal documents and financial services. Particularly, our aim is designing, implementing, and evaluating a TokenSign system. Then comparing our system with the approaches used in the underlying algorithm wherein the biometric data (i.e. fingerprint) is not encrypted for matching. TokenSign utilizes the revocable fingerprint biotokens (Biotope) [13] to perform matching in secure encryption form without decrypting biometric data (i.e. fingerprint), using shares to separately protect the shared secret (transaction reference numbers/user ID) to perform electronic signature for legal documents and financial services. During the enrollment process, TokenSign transforms the biometric data (i.e. fingerprint) into encrypted data using the revocable fingerprint biotokens (Biotope) [13]. Then, TokenSign embeds a shared secret (i.e. reference numbers/user ID) inside the encrypted fingerprint data using Bipartite token [14] and secret sharing scheme [15]. During the matching/signing process, TokenSign matches the fingerprint data in encoded mode, which provides confidentiality and non-repudiation. TokenSign also provides authentication when the threshold shares of secret (i.e. reference numbers/user ID) return a valid secret (token). In sum, this combination of the

two layers of security ensure no attacks are successful against the fingerprint data nor the embedded shared data inside the fingerprint data.

The remainder of this paper is organized as follows: First, we describe the previous literature review in section II. The objectives of TokenSign are discussed in section III. In section IV, we present the proposed TokenSign algorithm. We describe the experimental design in section V. While in section VI, we discuss and evaluate the experimental results. Finally, we conclude the paper in section VII.

II. Background

A. Non-Repudiation

Non-repudiation is a situation where an action cannot be denied from both parties (sender and receiver). In the other word, non-repudiation is the ability to prove something happen between two parties, especially in electronic signature for legal document or financial transactions. McCullagh et al [5] discusses the non-repudiation concerns of electronic signature when a signature is not performed face-to-face. Also, they addressed the legal and crypto meaning of non-repudiation and model law for trusted system. McCullagh et al [5] concluded that the electronic signature can be secure and trusted if it is equivalent to paper-based environment. In terms of electronic payment system, Abrazhevich et al [6] outlines the important role of electronic payment system in the future and addresses the limitations such as usability, security, and trust. They concluded their study with recommended design for electronic payment system which has better insight of a users perspective. Kahn et al [7] focus on the effect of theft incidents on online banking. In particular, their study analyzed the difference between two types of identity theft with payment security assessments to capture the effect of safety on payment [7].

B. Authentication

Authentication here is to prove that the person who is performing the electronic signature is the right person. The authentication issue is not a new research problem; in fact, it has been studied deeply. The invention [8] outlines their authentication method where the client received digital work fingerprint and a representation file to sign, while in electronic payment authentication, Kalakota et al [9] describes the fraud in e-commerce. These frauds increase the cyberattacks against electronic payments. To have more efficient tool for authentication in electronic payment, Clodfelter et al [10] suggests biometrics. Kaleist et al [11] outlines that biometric as a unique identity in order to enhance the security and trust for electronic payment.

C. Security and Privacy

Even though biometrics data (i.e. fingerprints) afford a wide variety of advantages such as non-repudiation and authentication, the privacy and security of biometrics data itself is the main concern [12]. Biometrics data considered a very sensitive and has been targeted for many attacks, including the adversary attack and the intrinsic failure [13] [12]. Also, biometric data is vulnerable for doppelganger attacks and biometric dilemma [13] [16]. To protect biometrics data from such attacks, many approaches proposed in the literature. Some of these schemes use encryption methods to provide security and privacy for biometric [17]. These approaches are vulnerable for attacks in the matching process when the biometric data needs to be decrypted for matching [12] [18]. On the other hand, template protection approaches have been introduced to secure the biometrics data. These template approaches are classified into four distinct categories: non-invertible transform [19], salting [20], key generating biometrics cryptosystems [21] [22], and key binding biometrics cryptosystems [23] [24].

III. TokenSign Objectives

The main goal of TokenSign scheme is to introduce a new electronic signature by considering the fingerprint a signature to replace the common handwriting signature. In this section we explore the objectives of TokenSign in non-repudiation, authentication, security, and privacy.

A. Non-Repudiation and Authentication

TokenSign scheme provides non-repudiation and authentication by using Biometric data (fingerprint), the revocable fingerprint biotokens (Biotope) [13], Bipartite token [14], and Secret Sharing Scheme [15]. Any time a user wants to perform a signature, a user must provide his/her fingerprint data. In this case, a user cannot deny his/her signature. From the point of view of a government or other organization, the biometric data is a highly acceptable tool for authentication as they can verify who signed, meaning the signer is the right/authenticated user. TokenSign scheme utilizes Secret Sharing Scheme [15] to authenticate the biometric data (fingerprint) belongs to the same person, providing another layer of authentication. To achieve this goal, TokenSign schemes hide a secret inside an encrypted fingerprint data. In the matching/signing process, this secret must be released and computed to match the secret on record.

B. Security and Privacy

TokenSign scheme provides security and privacy for the biometric (fingerprint) by utilizing the revocable fingerprint biotokens (Biotope) [13] and Bipartite token [14]. In this case, TokenSign scheme does not use the biometric data (fingerprint) raw data, providing more security and privacy for the fingerprint data. Moreover, all fingerprint data stored in TokenSign system are revocable biotokens, meaning they can be revoked at any time by a user or its organization. In addition, TokenSign scheme hides a time stamp for each biotoken; this time stamp gives more security by indicating how long a biotoken has been in use. That means each biotoken can be valid only for a time period as specified by organizations. For usability, TokenSign scheme can create new biotokens for expired biotokens without taking the fingerprint raw data again from users.

IV. Design of TokenSign Scheme Algorithm

In our design, we present the architecture of TokenSign scheme in enrollment and matching/signing process. The TokenSign scheme consist of two protocols: single protocol and group protocol. Single protocol is used to perform a signature for one person while group protocol is used to perform a signature for a group of people.

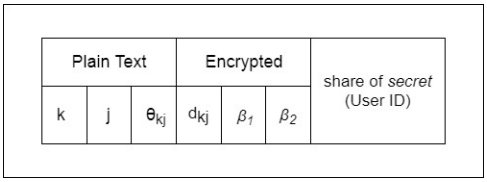

Fig. 1. The layout of the pair table data store in the cloud. Each row of the pair table data contains of d_{k_j}, β_1, β_2, k, j, θ_{kj} combined with share of secret of the user ID.

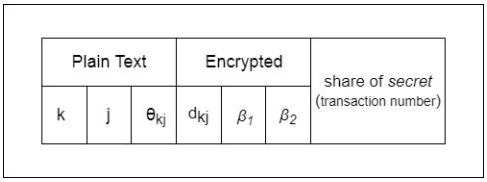

Fig. 2. The layout of the pair table data store in the cloud. Each row of the pair table data contains of d_{k_j}, β_1, β_2, k, j, θ_{kj} combined with share of secret of the transaction number.

A. Enrollment Process

TokenSign scheme algorithm has two protocols: single signature and group signature. Single signature is used for one user while group signature is used for multiple users. Algorithm 1 and 2 explain the details of TokenSign process.

First to occur in single signature protocol, TokenSign scheme takes multiple gallery fingerprint images (N) from each user to extract the minutia points files. Second, TokenSign scheme creates a gallery pair table, as in the NIST Bozorth Matcher Algroithm [25], for each minutia points file. Third, TokenSign scheme uses the revocable fingerprint biotokens (Biotope) [13] to encrypt the gallery pair table. Then TokenSign scheme takes the user ID and applies Secret Sharing Scheme [15] in order to split the user ID into multiple shares equal to the number of a users images (N) while determining the threshold number to recover the user ID where N is always greater than or equal to K. Finally, TokenSign scheme uses a Bipartite token [14] to hide each share of secret (the user ID) inside the encrypted fingerprint data (i.e. pair table). Figure 1 shows the structure of single signature protocol.

Data: Gallery fingerprint image g_i, Where i=1,2,3,. . . ,n
Result: Encrypted gallery fingerprint (pair-table t_i)
for (*each gallery fingerprint impression* g_i) {
  extract minutia points m_i from fingerprint image g_i;
  compute minutia file mf_i from minutia points m_i;
  create the gallery pair table t_i from the minutia file mf_i;
  encrypt the gallery pair table t_i using Biotope [13];
  create a secret and determine all shares and the threshold using SSS [15] ;
  hide a secret inside the encrypted gallery pair-table t_i using Bipartite [14] ;
  upload the encrypted gallery fingerprint (pair-table t_i) over multiple clouds;

Algorithm 1: Algorithm of enrollment operation of TokenSign for single and group protocols. For single protocol, the algorithm creates a secret (user ID) and hides it inside one user fingerprint data. While in group protocol, the algorithm creates a secret (transaction number as a random) and hides it inside multiple users fingerprint data.

In group signature protocol, the same steps are followed, but with minor modification to how they are executed. First, TokenSign scheme takes gallery fingerprint images from group of users (N fingerprints from N users) to extract the minutia points files. Then, TokenSign scheme creates a secret (transaction number) for all users in a group and applies Secret Sharing Scheme [15] in order to split this secret into multiple shares equal to all users in a group while determine the threshold number (K) to recover the secret key back, where N is always greater than or equal to K. Finally, TokenSign scheme using Bipartite token [14] to hide each share of the secret inside each encrypted fingerprint data of each user in a group. Figure 2 shows the structure of group signature protocol.

Data: Probe fingerprint image p_i where i=1,2,3,. . . ,n
Result: Electronic Signature (Print the secret (transaction number/user ID) and (time/data)
for (*each probe fingerprint impression* p_i) {
  extract minutia points m_i from fingerprint image p_i;
  compute minutia file mf_i from minutia points m_i;
  construct the probe pair-table t_i from the minutia file mf_i;
  encrypt the probe pair-table t_i using Biotope [13];
for (*all encrypted probe pair-table* t_i) {
  match each encrypted probe pair-table t_i in parallel against all encrypted gallery pair-table t_i ;
  if *match == true* **then**
    release the threshold secret hidden inside all encrypted gallery pair-table t_i;
    compute the threshold secret using SSS [15] ;
  if *threshold secret shares in gallery == right secret* **then**
    confirm the two fingerprints (probe and gallery) belongs to the same person;
    perform the electronic signature by printing the user ID/transaction number;

Algorithm 2: Algorithm of matching/signing operation of TokenSign for single and group protocols. For single protocol, the algorithm matches one user probe fingerprint data against his/her all gallery fingerprint data and releases the threshold shared secret (user ID). Meanwhile, in group protocol, the algorithm matches multiple users probe fingerprint data against their all gallery fingerprint data and releases the threshold shared secret (transaction number shared by the group). For both protocols, the TokenSign algorithms print the secret number and time/data.

B. Matching Process

In the matching/signing process, TokenSign scheme will follow the same steps in enrollment process to construct an

encrypted probe pair table. In the single signature, TokenSign scheme matches the encrypted probe pair table against the threshold of the encrypted gallery pair tables for one user fingerprint data in parallel. The matching/signing process performs in encrypted space. If the matching is successful, TokenSign scheme computes the secret (Shared users ID) from the threshold shares by applying the Sharing Secret Scheme [15]. Then, the TokenSign scheme can perform the single signature for a user by printing user ID, time, and date. In the group signature, TokenSign scheme matches a group encrypted probe pair tables against the threshold of group encrypted gallery pair tables in parallel. The matching process performs in encrypted space. If the matching is successful, TokenSign scheme computes the secret (shared secret/transaction number) from the threshold shares by applying the Sharing Secret Scheme [15]. Then the TokenSign scheme can perform the group signature for group of users by printing the secret (transaction number), time and, date.

V. Experimental Design

The main objective of our experiment is to compare three systems: TokenSign (group protocol) scheme against two baselines named the revocable fingerprint biotokens (Biotope) [13] and our design baseline called TokenSign (single protocol). We conduct the experiment using threading for parallel matching and using C++ and Python as the programming languages. We use the Amazon cloud to do our experiment. We use the dataset (FV C2002Db2 a) [26] and upload all encrypted gallery fingerprint data into Amazon AWS S3 using Python Amazon S3 API. For storage, we use Paris, N. Virginia, London, N. California, Sydney, Ireland, Ohio, and Tokyo. During the matching process, we transfer our executable files using FileZilla to Amazon EC2 servers. Then we use the Python boto library to connect Amazon S3 with Amazon EC2 instance. Finally, we match in parallel between probe encrypted fingerprint against gallery encrypted fingerprint. The result of this experiment is the average of twenty runs.

A. Baseline Setup

We use two baselines in our experiment: TokenSign (single protocol) scheme and the revocable fingerprint biotokens (Biotope) [13]. For the Biotope [13] baseline, we implement and conduct our experiment in the Amazon cloud instead of local storage. By conducting our scheme in the cloud, we have a fair experiment. For the second baseline, we design our baseline similar to our scheme (TokenSign for group protocol). In this baseline (TokenSign for single protocol), we match a single user against his/her encrypted fingerprints data in the cloud in parallel, calculate the time cost, and compare it to our scheme (TokenSign for group protocol).

B. TokenSign (Group Protocol) Setup

For the TokenSign (group protocol), our designed is similar to baseline (TokenSign for single protocol). In our scheme (TokenSign for group protocol), we matched multiple of users against their encrypted fingerprint data in the cloud in parallel and calculated the time cost and compared it to both baselines.

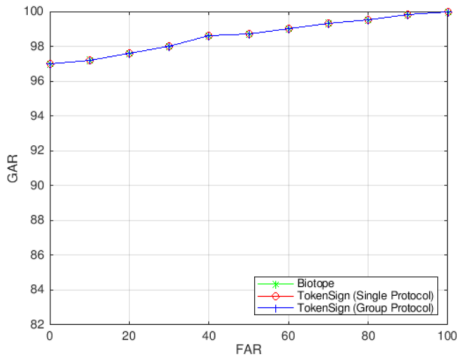

Fig. 3. The ROC curve comparing TokenSign and baseline scheme accuracy.

TABLE I. The Comparison of the Two Algorithms (TokenSign and Biotope [13])

P-value	TokenSign (Single protol)	TokenSign (Group Protocol)
Biotope	2.10E-16	2.10E-16

VI. Experiment Evaluation

In this experiment, the main goal is to prove that TokenSign maintains compatible accuracy while increasing the matching speed. To prove this claim, we conducted two experiments: accuracy evaluation and speed evaluation. When then evaluate if the TokenSign achieves its goal in increasing speed and compatible accuracy. Lastly, we conclude if the result support or reject the hypothesis claim.

A. Accuracy Evaluation

In this section, we evaluated TokenSign (Group Protocol) against the revocable fingerprint biotokens (Biotope) [13] and our designed baseline TokenSign (Single Protocol). We ran the experiment and evaluated the genuine acceptance rate (GAR) and the false acceptance rate (FAR) to prove our scheme maintained compatible accuracy comparing to both baselines. Figure 3 shows that TokenSign (Group Protocol) scheme achieved promising results when compared to both baselines where GRA is equal to 97 while FAR is equal to zero. Thus, this result support our hypothesis claim. Figure 3 shows the ROC curve comparing TokenSign scheme with both baselines.

B. Speed Evaluation

In the speed evaluation, we evaluated TokenSign (Group Protocol) with the revocable fingerprint biotokens (Biotope) [13] and our designed baseline TokenSign (Single Protocol). We ran the experiment of identification (1:N) in parallel to prove our scheme maintained increased speed when compared to both baselines. For the statistical test, the null hypothesis Ho is that the time for the baseline is less than or equal to TokenSign (Group Protocol). Table I illustrates the p-values from the ANOVA F-test, which rejects the null hypothesis of 20 runs, using a one-way ANOVA test. Table II and Figure 4 show the increased speed results when TokenSign scheme is compared with Biotope baseline.

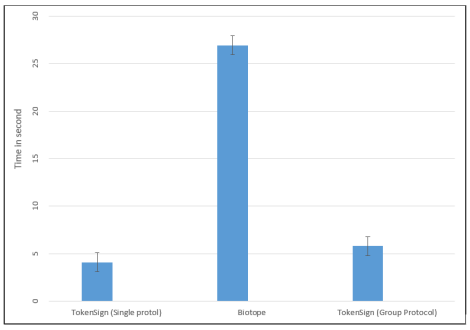

Fig. 4. The average matching time (with the error bars represent the standard deviation) comparing the two algorithms (TokenSign and Biotope [13])

TABLE II. THE AVERAGE MATCHING TIME AND STANDARD DEVIATION OF THE TWO ALGORITHMS (TOKENSIGN AND BIOTOPE [13])

	Biotope	TokenSign (Single protol)	TokenSign (Group Protocol)
AVE	26.93	4.09	5.81
STD	0.307	0.209	0.202

VII. CONCLUSION

This paper represents the design, implementation, and evaluation of a TokenSign system, comparing it with the approaches used in underlying algorithm. TokenSign is a new electronic signature for legal documents and financial services that uses a fingerprint as a signature. TokenSign shows a significant improvement in performance besides providing non-repudiation, authentication, security, and privacy. Our experiments show that applying Bipartite token algorithm and secret sharing scheme to underling algorithm of electronic signature was statistically faster and accurate comparing to the two baselines. In addition, TokenSign scheme utilizes cloud computing to process and compute big data like biometrics data of electronic signature to provide scalability. Future work is to use different fingerprint matcher algorithm for electronic signature and deploy these electronic signature systems on smart devices platforms.

REFERENCES

[1] M. J. Moon, "The evolution of e-government among municipalities: Rhetoric or reality?" *Public Administration Review*, vol. 62, no. 4, pp. 424–433, 2002.

[2] T. Anderson, L. Peterson, S. Shenker, and J. Turner, "Overcoming the internet impasse through virtualization," *Computer*, vol. 38, no. 4, pp. 34–41, April 2005.

[3] O. Ogbanufe and D. J. Kim, "Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment," *Decision Support Systems*, vol. 106, pp. 1 – 14, 2018.

[4] J. Bughin, M. Chui, and J. Manyika, "Clouds, big data, and smart assets: Ten tech-enabled business trends to watch," p. 7586, 2010.

[5] A. McCullagh and W. Caelli, "Non-repudiation in the digital environment," *First Monday*, vol. 5, no. 8, 2000.

[6] D. Abrazhevich, "Electronic payment systems: a user-centered perspective and interaction design," 2004.

[7] C. Kahn and J. Linares Zegarra, "Identity theft and consumer payment choice: Does security really matter?" *Journal of Financial Services Research*, vol. 50, no. 1, pp. 121–159, 8 2016.

[8] R. Daouphars, J.-M. Desperrier, and L. Fourni, "Electronic signature authentication," Jun 2014.

[9] R. Kalakota and A. B. Whinston, *Electronic Commerce: A Manager's Guide*. Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc., 1997.

[10] R. Clodfelter, "Biometric technology in retailing: Will consumers accept fingerprint authentication?" *Journal of Retailing and Consumer Services*, vol. 17, no. 3, pp. 181 – 188, 2010, new Technologies and Retailing: Trends and Directions.

[11] V. F. K. Ph.D., "Building technologically based online trust: Can the biometrics industry deliver the online trust silver bullet?" *Information Systems Management*, vol. 24, no. 4, pp. 319–329, 2007.

[12] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP J. Adv. Signal Process*, vol. 2008, pp. 113:1–113:17, Jan. 2008.

[13] T. E. Boult, W. J. Scheirer, and R. Woodworth, "Revocable fingerprint biotokens: accuracy and security analysis," in *2007 IEEE Conference on Computer Vision and Pattern Recognition*, June 2007, pp. 1–8.

[14] W. J. Scheirer and T. E. Boult, "Bipartite biotokens: Definition, implementation, and analysis," in *Advances in Biometrics*, M. Tistarelli and M. S. Nixon, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 775–785.

[15] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979.

[16] W. J. Scheirer, B. Bishop, and T. E. Boult, "Beyond pki: The biocryptographic key infrastructure," in *The IEEE International Workshop on Information Forensics and Security (WIFS)*, December 2010.

[17] [Online]. Available: http://www.griaulebiometrics.com/enus/ biometric-framework

[18] W. J. Scheirer and T. E. Boult, "Cracking fuzzy vaults and biometric encryption," in *2007 Biometrics Symposium*, Sept 2007, pp. 1–6.

[19] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 561–572, Apr. 2007. [Online]. Available: http://dx.doi.org/10.1109/TPAMI.2007.1004

[20] A. B. J. Teoh, A. Goh, and D. C. L. Ngo, "Random multispace quantization as an analytic mechanism for biohashing of biometric and random identity inputs," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 28, no. 12, pp. 1892–1901, Dec 2006.

[21] Y.-J. Chang, W. Zhang, and T. Chen, "Biometrics-based cryptographic key generation," pp. 2203–2206 Vol.3, June 2004.

[22] C. Vielhauer, R. Steinmetz, and A. Mayerhofer, "Biometric hash based on statistical features of online signatures," pp. 123–126 vol.1, 2002.

[23] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *Proceedings of the 6th ACM Conference on Computer and Communications Security*, ser. CCS '99. New York, NY, USA: ACM, 1999, pp. 28–36. [Online]. Available: http://doi.acm.org/10.1145/319709.319714

[24] K. Nandakumar, A. Nagar, and A. K. Jain, *Hardening Fingerprint Fuzzy Vault Using Password*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 927–937.

[25] C. I. Watson, M. D. Garris, E. Tabassi, C. L. Wilson, R. M. McCabe, S. Janet, and K. Ko, "User's guide to non-export controlled distribution of nist biometric image software," 2004.

[26] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, "Handbook of fingerprint recognition," 2009.