Towards Automated Transactions Based on the Offline Handwritten Signatures

George S. Eskander, Robert Sabourin, and Eric Granger

Laboratoire d'imagerie, de vision et d'intelligence artificielle
Ecole de technologie supérieure, Université du Québec, Montréal, Canada
geskander@livia.etsmtl.ca, robert.sabourin@etsmtl.ca,
eric.granger@etsmtl.ca

Abstract. Automating business transactions over the Internet relies on digital signatures, a replacement of conventional handwritten signatures in paper-based processes. Although they guarantee data integrity and authenticity, digital signatures are not as convenient to users as the manuscript ones. In this paper, a methodology is proposed to produce digital signatures using off-line hand-written signatures. This methodology facilitate the automation of business processes, where users continually employ their handwritten signatures for authentication. Users are isolated from the details related to the generation of digital signatures, yet benefit from enhanced security. First, signature templates from a user are captured and employed to lock his private key in a fuzzy vault. Then, when the user signs a document by hand, his handwritten signature image is employed to unlock his private key. The unlocked key produces a digital signature that is attached to the digitized document. The verification of the digital signature by a recipient implies authenticity of the manuscript signature and integrity of the signed document. Experimental results on the Brazilian off-line signature database (that includes various forgeries) confirms the viability of the proposed approach. Private keys of 1024-bits were unlocked by signature images with Average Error Rate of about 7.8%.

Keywords: Automated Transactions, Digital Signatures, Handwritten Signatures, Offline Signatures, Bio-Cryptography, Fuzzy Vault.

1 Introduction

Nowadays, online financial transactions and business agreements are replacing the conventional paper-based processes. One important aspect to accomplish a transaction is to guarantee authenticity of its parties. For the paper-based processes, handwritten signature is the most universally accepted method of authentication. However, identity of the signer is another important aspect to prove, especially for critical agreements and transactions. Various means are applied to check a signer identity in the paper-based processes. For instance, a signer shows his identity card where a signature is done in front of a legal officer and/or a witness co-signs with the main signer. For the online processes,

these conventional methods are not applicable. Instead, the digital signatures can replace the handwritten signatures to authenticate involved parties. The public key infrastructure (PKI) technology is employed for realizing the digital signature concept [1]. Two asymmetric keys are generated: a private (signing) key is given for a signer, and a public (verification) key is published to the other parties. To sign a document, the user private key is employed to encrypt some message and attach it to the document. Any party involved in this process can verify the authenticity of the received document. To this end, the recipient extracts the encrypted message from the document, decrypts it by means of the sender's public key, and compares the result with the corresponding plain message. The document is considered authentic, if the two messages are identical. This approach also provides a measure of integrity, as identical messages imply that the document is not tempered while being transfered. On the other hand, integrity of the paper-based processes is hard to proof as document contents can be changed after being signed.

Despite of the enhanced security of the digital signature compared to the handwritten signatures, it has some practical drawbacks. First, digital signatures employ long private keys that is hard to memorize. This problem is alleviated through storing the key in a secure place, e.g., a smart card, and a user retrieves his key by entering a simple password. This scenario, although guarantee authenticity of the digital signature, it does not prove the identity of the signer. Any person, who gets access to the smart card and knows the password, can produce a valid digital signature. Moreover, the security level of the process is degraded, as whatever strong is the signing key, the actual security is determined by the password length. This is known as the cryptographic key management problem. Second, the additional security measures used for digital signatures, like smart cards and passwords, are not as convenient to users as the traditional manuscript signatures. Moreover, some electronic processes employ paper-based steps that rely on handwritten signatures. For instance, remote bank check deposits imply signing a paper-based check, scan it and submit it remotely to the bank system. Such applications need some integration between the traditional way of authentication and the new technology, which is not offered by the card-password scenario.

In literature, the cryptographic key management problem is alleviated by introducing the bio-cryptography concept [2]. Biometrics, that are physical or behavioral human characteristics, are used to control the access to the cryptographic keys. Hence, authenticity of the signer is proved by his traits, instead of something he knows like a password that can be stolen or forgotten. The published bio-cryptographic implementations mostly employed physical biometrics, like fingerprint [3], iris [4], etc. However, few bio-cryptographic implementations are proposed based on the handwritten signatures. These systems concerned mostly with online systems, where signatures are acquired using special pens and tablets, e.g., [5]. These bio-cryptographic implementations, although alleviates the key management problem of digital signatures, they cannot be integrated in applications where the traditional manuscript signatures are employed.

This paper proposes a digital signature framework based on the offline handwritten signature images. Recently, we introduced a method to secure the cryptographic keys by means of the signature images [6]. Here, this method is employed for digital signature key management. To this end, the fuzzy vault (FV) scheme is implemented [12], where signature representations are selected through a boosting feature selection (BFS) process [13]. We show that the proposed method can be employed to manage large keys, e.g., 1024-bits keys, as that involved in the RSA signature schemes [1].

The rest of this paper is organized as follows. The next section reviews the biometric-based digital signature schemes in the literature. The proposed manuscript signature-based digital signature framework is illustrated in section 3. The experimental methodology is illustrated in section 4. The experimental results are presented and discussed in section 5.

2 Biometrics-Based Digital Signatures

In literature, some of the aforementioned bio-cryptographic implementations are employed to design biometric-based digital signatures. The employed bio-cryptographic schemes are categorized into three main types: 1) key-release, 2) key-generation, and 3) key-binding schemes. In key-release systems, the biometric templates and cryptography keys are stored separately, and the crypto-key is released to genuine users based on classical biometric authentication. To secure both of the key and the template, tamper-resistant storage is needed. In key-generation systems, crypto-keys are generated directly from the biometric traits. This technique is secure, as there is no need to store neither the key nor the biometric template. A drawback of the key-generation approach is that it is hard to generate robust and random keys from unstable and correlating biometric signals. It is also not easy to integrate these biometric-based keys with standard cryptographic algorithms like RSA. Moreover, as private keys are gerenated directly from the biometric signals, these keys are not revocable (if either the key or the biometric signal is compromised, no new key can be generated). In key-binding systems, classical crypto-keys generated by standard cryptographic keys, e.g., RSA, are coupled with biometric keys. They cannot be decoupled without applying a genuine sample of the biometric trait. Accordingly, reliability and security of key-binding techniques surpasses other cryptography schemes, as they protect the biometric templates and produce typical cryptographic keys.

Janbandhu et al., [7] proposed an Iris-based digital signature framework based on 512-bytes Iris templates and a key generation bio-cryptographic scheme. To overcome the irrevocability of the key generation approach, randomly generated numbers are employed to modify the iris template. To integrate this scheme with standard public key infrastructures (PKI), e.g., DSA and RSA, the random prime numbers generated by the PKI (to produce the public and private keys), are adjusted to be as close as possible to the Iris template. Mohammadi et al., [8] proposed a similar approach, where Iris templates are integrated with Elliptic Curve Cryptography (ECC). Orvos., [9] introduced a key-binding scheme,

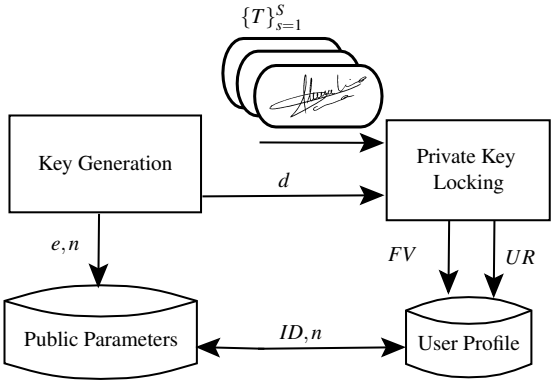

Fig. 1. User enrollment process.

where keys of the digital signatures can be encrypted by means of fingerprints. However, this scheme is abstract and no details of the employed key-binding methodology is presented. Kwon [10] et al., propsed a fingerprint-based digital signature framework based on a key-binding scheme. The authors employed the concept of key encryption proposed by Soutar et al., [11], where no features are extracted from the fingerprint, but rather an image processing method is applied to lock the private key by the template.

For most of the aforementioned biometric-based digital signature proposals, accuracy of generated keys by means of genuine and forgery biometric signals are not reported. Moreover, the employed biometrics, like iris and fingerprint, might not be user convenient, costly, and not suitable for some business applications. For instance, it is not practical to accomplish a remote bank check deposit by means of the customer fingerprint, instead signing checks by hand would be more convenient and compatible with the already existing paper-based processes.

3 Handwritten Signature-Based Digital Signature

3.1 Overview

The proposed system employs the fuzzy vault scheme (FV) [12], as a key-binding mechanism for digital signature key management. Typical cryptographic keys are generated through standard public key infrastructures (PKI), and the private key is locked in a secure FV by means of the user handwritten signature image. Later, a user signs his document digitally by providing a genuine handwritten signature sample. Also, a user can delegate a third party for producing digitally signed documents, based on his handwritten signed documents. Any party involved in the transaction, who has the user public key, can validate the digital signature, and hence the authenticity and integrity of the document. The proposed framework consists of three main processes: 1) user enrollment, 2) signing, and 3) verification.

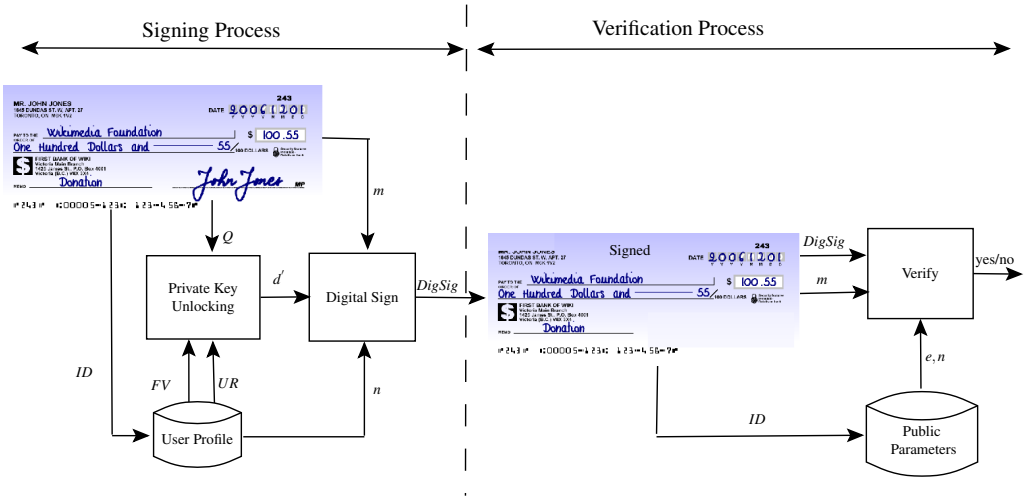

Fig. 2. Framework of the proposed digital signature method based on the handwritten signature images.

3.2 Enrollment Process

Figure 1 illustrates the user enrollment process. The cryptographic keys are generated according to the employed public key infrastructure (PKI). For instance, for the RSA scheme, a private (signing) key d, a public key e and a shared parameter n are generated for a user. Parameters e and n are published to parties, who are supposed to receive and verify documents belonging to the specific user. The private key d is locked by means of some features, extracted from user's handwritten signature templates $\{T_s\}_{s=1}^{S}$, and constitutes a user fuzzy vault FV. A user profile contains the FV and user identification data is constituted. This profile might be sent to the user, so he can digitally sign his documents on his own. Also, the user profile might be sent to a trusted party, that can issue digital signatures on behalf of the user. This party extracts the handwritten signatures embedded in the user document, unlocks the user private key d from the FV by means of the extracted signature image, and then produces a digital signature and attach it to the digitized document. This last scenario simulates the witness party in paper-based agreements or transactions.

3.3 Signing Process

Figure 2 (see the left side) illustrates the signing process. To digitally sign a document, the embedded handwritten signature image Q is extracted and used to decode the user FV. If Q is genuine, it correctly unlocks the signing key $d^{'}$ from the FV, where $d^{'}$ and the original private key d are identical. The document is then signed by means of $d^{'}$ and n. A specific message m is extracted from the

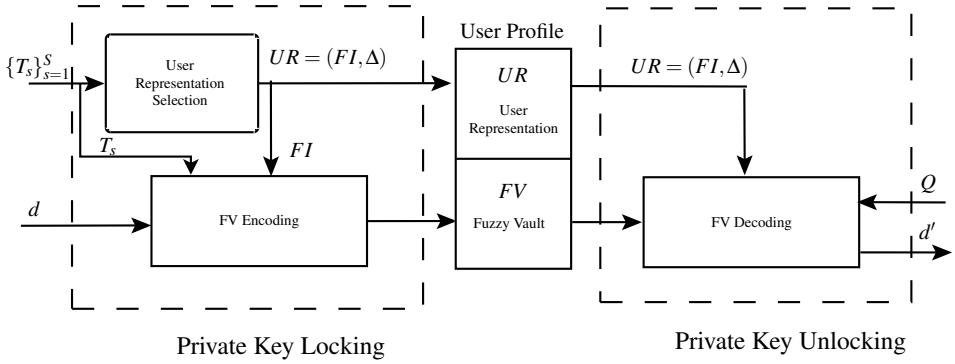

Fig. 3. Locking and unlocking of the digital signature private keys within secure FV tokens, by means of the user offline handwritten signature samples.

document, e.g., for bank check applications, m could be the value of the check. Then, m is encrypted by means of $d^{'}$ to constitute a digital signature $DigSig$, and it is attached to the digitized document.

3.4 Verification Process

Figure 2 (see the right side) illustrates the verification process. A recipient, who has the user public key e, can verify the attached digital signature. $DigSig$ is decrypted by means of e and n, and retrieves the message $m^{'}$. The original plain message m is extracted from the document. The digital signature passes the validation test, if both m and $m^{'}$ are identical. In this case, the recipient is sure that the original document is authentic (contains a genuine handwritten signature). Also, this indicates integrity of the document (e.g., the check amount is not changed after the check is signed).

3.5 Private Key Locking and Unlocking

Figure 3 illustrates how the private keys are locked and unlocked in/from secure FV tokens. To lock a private key d, the enrollment handwritten signature templates $\{T\}_{s=1}^{S}$ are used to learn a user representation UR. This representation consists in vectors FI and Δ. Vector $FI = \{fI_i\}_{i=1}^{t}$ consists in the indexes of the best t features, that discriminate between genuine and forgery signatures. Vector $\Delta = \{\delta_i\}_{i=1}^{t}$ consists in feature dissimilarity thresholds. Assume δf_i^{QT} is the dissimilarity between two samples Q and T, measured by feature f_i. The dissimilarity feature threshold $\{\delta_i\}$ is selected so that: $\delta f_i^{Q_{gen}T} \leq \delta_i$ and $\delta f_i^{Q_{fr}T} > \delta_i$, $\forall$ genuine sample Q_{gen} and forgery sample Q_{fr}. In a preliminary version of our FV implementation based on the offline handwritten signatures [6], boosting

feature selection approach (BFS)[13] is employed to select the most discriminative feature FI. Recently, this feature representation is enhanced by learning the feature dissimilarity vector Δ [14], in a dissimilarity representation space [1]. The features indexes vector FI is used to extract a feature representation $F^T = \{F_i\}_{i=1}^{t}$ from a prototype signature T_s. Then, F^T locks the private key d in a FV. To this end, d is used to generate an encoding polynomial p, by splitting d of size KS-bits into $k+1$ equal chunks (c) of size l-bits. These chunks are used as polynomial coefficients. So that the encoding polynomial p is given by:

$$p(a_i) = c_k {a_k}^k + c_{k-1} {a_{k-1}}^{k-1} + ... + c_1 a + c_0. \quad (1)$$

The extracted features F^T are quantized in elements of l-bit, to constitute a locking vector $A = \{a_i\}_{i=1}^{t}$. Genuine FV points $\{A, P(A)\}$ are constituted by computing the polynomial, given by Eq.1, for all elements of A. To hide the genuine points, z chaff (noise) points $\{\hat{A}, \hat{P}\}$ are generated, so that they do not collide with the genuine points. Finally both genuine and chaff points are merged to constitute r FV points $\{\tilde{A}, \tilde{P}\}$, where $r = t + z$.

To unlock the private key d, a query handwritten signature image Q is extracted from the document, and used to decode the FV. A query feature vector F^Q is extracted from Q, based on the pre-selected feature indexes FI. Feature quantization is done, as that for the FV encoding process, and the FV unlocking vector $B = \{b_i\}_{i=1}^{t}$ is constituted. Elements of B are matched against all points of the FV, so that the chaff points are filtered out. For the preliminary version of our FV implementation [6], elements of A and B are strictly matched. Two elements are considered matching if they have exact quantized values. In this work, the modeled dissimilarity threshold vector Δ is used for adaptively matching elements based on their expected dissimilarities [14]. Two elements are considered matching if their dissimilarity is less than the corresponding dissimilarity threshold. The resulting vector $\{\bar{A}, \bar{P}\}$ is used to reconstruct the polynomial $p^{'}$, by applying the Reed-Solomon error correction codes [17]. Finally, the coefficients of $p^{'}$ are assembled to constitute the key $d^{'}$. If the FV is correctly decoded, the unlocked key $d^{'}$ is identical to the user private key d. For more details about the FV encoding and decoding processes and the dissimilarity representation, see [6] and [14].

4 Experimental Methodology

The Brazilian database [20] is used for proof-of-concept simulations. This DB contains three types of signature forgery: random, simple and simulated. Random

[1] Details of the BFS and dissimilarity learning is out of the scope of this paper. For more details, see [6] and [14]. This method relies on recent works proposed by Rivard et al., [15] and Eskander et al., [16], for designing writer-independent and writer-dependent offline signature verification systems, respectively.

forgeries do not know neither the writer's name nor the signature morphology. For simple forgery, the forger knows the writer's name and he produces a simple forgery using his writing style. A simulated forgery has access to a sample of the signature and imitates the genuine signature. The signatures were provided by 168 writers. Signatures of first 60 writers include: 40 genuine signatures, 10 simple forgeries and 10 simulated forgeries per writer. Of them, 30 genuine signatures, besides some of signatures selected from the last 108 users (that represents random forgeries), are used for the user representation (UR) selection task. For performance evaluation, the rest 10 genuine samples, 10 simple, 10 simulated forgeries, and 10 random forgeries (belong to the last 108 users) are used.

In the preliminary version of this work [6], we employed Extended-Shadow-Code (ESC) features [18]. Here, we investigate a multi-type feature extraction approach, where Directional Probability Density Function (DPDF) [19] is also employed. Features are extracted based on 30 different grid scales producing 60 different single scale feature representations. These representations are then fused to produce a feature representation of huge dimensionality $(30, 201)$ [15].

For digital signature key generation, the RSA scheme is employed [1]. Keys of different sizes are generated, where the private key d is locked in a FV. Digital signatures is produced by means the private key $d^{'}$, unlocked from the FV by means of query signatures. Verification of the digital signatures is done by means the public key e.

The FV parameters are set as follows: the quantization size l is set to 16-bits. Different key sizes (KS) are employed (128, 256, 512, 1024-bits). Number of genuine FV locking points t is determined experimentally for the different key sizes.

The Average Error Rate (AER) is employed for performance evaluation and computed as follows:

$$AER = (FRR + FAR_{random} + FAR_{simple} + FAR_{simulated})/4. \quad (2)$$

False Reject Rate (FRR) is the ratio of genuine query signatures that failed to decode the FV, and produce valid digital signatures. FAR_{random}, FAR_{simple} and $FAR_{simulated}$ are the ratio of random, simple, and simulated forgeries, respectively, that succeed to decode the FV, and produce valid digital signatures.

5 Experimental Results

Table 1 reports the experimental results for different key sizes. In [6], only ESC features are employed and features are matched strictly. Here, when the DPDF features are added and features are matched adaptively, the performance is enhanced as AER is reduced from 17.75% to 10.08%. It is found that the proposed FV method could secure large keys with acceptable accuracy, so it could be integrated in practical digital signature schemes like RSA. However, the size of the

Table 1. Performance of the proposed manuscript signature-based digital signatures.

Parameters	KS-bits	128(previous work[6])	128	256	512	1024
	t	20	20	40	140	200
	z	180	180	360	1260	1800
Measure %	FRR	25	11.53	13.55	5.31	11.26
	FAR_{random}	3	2.05	2.00	2.71	0.98
	FAR_{simple}	7	2.39	2.28	3.31	1.31
	$FAR_{simulated}$	36	24.38	19.28	29.26	17.43
	AER	17.57	10.08	9.27	10.14	7.75

FV locking vector t should be increased for the large keys. Also, two important aspects are noticed: 1) different key sizes result in different performance for the different users. This motivate future investigation for adapting the key length for each user, 2) the performance differs for the different signature templates that locks the FV. This motivates further work to address prototype selection for FV encoding [14].

6 Conclusions and Future Work

A framework for digital signature by means of the handwritten signature images is proposed. The private keys are locked by the user signature templates and released only when a user provides a genuine signature sample. This framework facilitates various industrial applications like remote bank check transactions, ATM and credit card transactions, automation of business procedures including legal agreements, etc. Also, the proposed system permits delegation of authority, as a third party who stores the user profile, can generate signed digitized documents on behalf of a user based on his embedded handwritten signature. A fuzzy vault system is designed to protect the signature keys, where boosting feature selection process is employed in a dissimilarity representation space. Accuracy of FV decoding is increased through applying multi-type feature extraction and matching the FV encoding and decoding features adaptively, based on the modeled feature dissimilarity. Decoding accuracy of genuine, random and simple forgeries is acceptable, even with large cryptography keys. Resistance of the system against simulated forgeries needs enhancement, and further work is needed to detect this type of forgery. Also, future work should be conducted to increase the system accuracy, through adapting the FV parameters and select the signature prototypes for the specific users [14].

Acknowledgments

This work was supported by the Natural Sciences and Engineering Research Council of Canada and BancTec Inc.

References

1. Rivest, R., Shamir, A., Adleman, L., A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, vol.21, pp.120-126, 1978.
2. U. Uludag, S. Pankanti, S. Prabhakar and A.K. Jain., Biometric Cryptosystems: Issues and Challenges. *Proceedings of the IEEE*, vol.92, issue.6, pp.948-960, 2004.
3. K. Nandakumar A. K. Jain and S. Pankanti., Fingerprint based Fuzzy Vault: Implementation and Performance. *IEEE TIFS*, vol.2, no.4, pp.744-757, 2007.
4. Y. J. Lee and K. R. Park, S. J. Lee, K. Bae, and J. Kim., A new method for generating an invariant iris private key based on the Fuzzy Vault system. *IEEE TSMC-part B:Cybernetics*, vol.38, no.5, pp.1302-1313, 2008.
5. M. Freire-Santos, J. Fierrez-Aguilar and J. Ortega-Garcia., Cryptographic key generation using handwritten signatures. *proc of SPIE*, vol.6202, pp.225-231, 2006.
6. Eskander, G.S., Sabourin, R. and Granger, E., Signature based Fuzzy Vaults with boosted feature selection. *IEEE Workshop on Computational Intelligence and Identity Management (SSCI-CIBIM 2011)*, pp.131-138, Paris, 2011.
7. Janbandhu, P., Siyal, M., Novel biometric digital signatures for Internet-based applications. *IMCS*, vol.9, no.5, pp.205-212, 2001.
8. Shahriar Mohammadi, Sanaz Abedi., ECC-Based Biometric Signature: A New Approach in Electronic Banking Security. *Proceedings of the International Symposium on Electronic Commerce and Security*, pp.763-766, DC, USA, 2008.
9. Orvos, P., Towards biometric digital signatures. *Net workshop, Eszterhazy College, Eger*, pp.26-28, 2002.
10. Kwon, T., Lee, J., Practical digital signature generation using biometrics. *LNCS, Springer*, vol.3043, pp.728-737, 2004.
11. C. Soutar, D. Roberge, A. Stoianov, R. Golroy, and B. Vijaya Kumar., Biometric Encryption. *ICSA Guide to Cryptography*, McGraw-Hill, 1999.
12. A. Juels and M. Sudan., A Fuzzy Vault scheme. *In proc. IEEE int. Symp. Inf. Theory*, Switzerland, pp.408, 2002.
13. K. Tieu and P. Viola., Boosting image retrieval. *International Journal of Computer Vision*, vol.56, no.1, pp.17-36, 2004.
14. Eskander, G.S., Sabourin, R. and Granger, E., On the Dissimilarity Representation and Prototype Selection for Signature-Based Bio-Cryptographic Systems. *2nd Intel. Workshop on Similarity-Based Pattern Analysis and Recognition (SIMBAD2013)*, York, UK, 3-5 July 2013, LNCS, vol.7953, pp.265-280, In press.
15. Rivard, D, Granger, E and Sabourin, R., Multi-Feature extraction and selection in writer-independent offline signature verification. *International Journal on Document Analysis and Recognition*, vol.16, no.1, pp.83-103, 2013.
16. Eskander, G.S., Sabourin, R. and Granger, E., Adaptation of writer-independent systems for offline signature verification. *The 13th International Conference on Frontiers in Handwriting Recognition (ICFHR-2012)*, pp.432-437, Bari, Italy, 2012.
17. Berlekamp and Elwyn R., Algebraic Coding Theory. *McGraw-Hill*,NY,USA,1968.
18. R. Sabourin and G. Genest., An Extended-Shadow-Code based Approach for Off-Line Signature Verification. *Proc of the 12th international conference on PR*, Jerusalem, vol.2, pp.450-453, 1994.
19. J. Drouhard, R. Sabourin and M. Godbout., A neural network approach to off-line signature verification using directional pdf. *PR*, vol.29, no.3, pp.415-424, 1996.
20. C. Freitas, M. Morita, L. Oliveira, E. Justino, A. Yacoubi, E. Lethelier, F. Bortolozzi, and R. Sabourin., Bases de dados de cheques bancarios brasileiros. *XXVI Conferencia Latinoamericana de Informatica*, Mxico, 2000.