Visualizing key authenticity: turning your face into your public key.

Joan Arnedo-Moreno and Àgata Lapedriza

Universitat Oberta de Catalunya,
Rambla de Poblenou 156, 08018 Barcelona, Spain
{jarnedo,alapedriza}@uoc.edu

Abstract. Biometric information has become a technology complementary to cryptography, allowing to conveniently manage cryptographic data. Two important needs are fulfilled: first of all, making such data always readily available, and additionally, making its legitimate owner easily identifiable. In this work we propose a signature system which integrates face recognition biometrics with and identity-based signature scheme, so the user's face effectively becomes his public key and system ID. Thus, other users may verify messages using photos of the claimed sender, providing a reasonable trade-off between system security and usability, as well as a much more straightforward public key authenticity and distribution process.

Key words: digital signature, identity-based, face hashing, biometrics, signature validation, key generation

1 Introduction

At the present time, many transactions on the Internet, such as online banking or shopping, are carried out assuming some degree of security. This is possible by using secure schemes reliant on cryptographic data during the process, even when the user is not tech-savvy or knowledgeable about it. Nevertheless some requirements must be fulfilled in order for such schemes to actually be effective: secret cryptographic data must be safely stored and it must be possible to clearly establish a link between such cryptographic data and an identity. Even though anybody may be able to generate a proper cryptographic key, some means must exist to ensure who is its legitimate owner. Due to the nature of cryptographic data, in many instances, such requirements directly work against the usability of the system and require a minimum effort by end users. As the breadth of Internet applications with security requireents starts to encompass much more casual users, such as social networks, a compromise between usability and security mus be reached.

To address these issues, biometric information, such as voice, face, iris or fingerprint data, has become a complementary technology to cryptography [8, 9], offering a solution to the requirements of a secure system while, at the same

time, making the technology more accessible and convenient. It may be possible to forget a password or a shared key, but not to fail to recognize a friend's face or voice.

Most applications of biometric data in secure systems make special emphasis in access control and data encryption. In such cases, biometrics are either compared to a template database, or used to establish shared secret keys, assuming that the legitimate user is the only one who holds that particular biometric data. For example, a very common case is the use of fingerprint data, which is becoming a staple in some laptop models as a means for login or data encryption. However, secret key encryption cannot be applied to obtain other useful security services such as non-repudiation or convenient authentication in a multi-party environment, which require digital signature.

Signature schemes usually rely on public key cryptography, where each user keeps a secret key for himself and distributes a public key among the other users. However, one of the main issues in this kind of systems is precisely key authentication, ensuring who is the owner of a particular public key. A very common solution to this issue is the use of PKI (Public Key Infrastructure) and digital certificates [7]. This approach requires that users are, at least, able to understand what the certificate's content means and discern valid ones from invalid ones. On the other hand, another interesting approach is the use of identity-based schemes [10]. In such scheme, public keys are not randomly generated, but are the user's identifier itself (for example, the e-mail address). Therefore, the link between any public key and the legitimate owner is immediate and does not require any deep understanding of the underlying security system.

In this paper we present our work combing both approaches, biometrics and identity-based systems, to get both of their advantages. Specifically, we have chosen face biometrics as the user's system identifier, and thus, the public key. The main reason for this choice is the fact that, in contrast with other biometric data, a face is public information which can be easily retrieved by means of a simple photo. This is specially true now that most mobile phones already include a digital camera and social networks are attaining a high degree of popularity. Thus, it is feasible to locate someone's image, endorsed by all his contacts. Therefore, under this system, public keys can be easily distributed and managed with a high degree of usability. Furthermore, identifying who is the legitimate owner becomes straightforward. However, the main interest in using this approach is, precisely, that face information access is not limited to the real owner. Anyone may acquire it, in contrast with other biometric data.

We would like that absolutely any face picture of the claimed user could be used as his public key. However, this is currently imposible. For this goal, we would need a system to get the same bit string from all the face images from a particular person, as well as getting different ones from images from diffrent subjects. Unfortunately, visual data, such face images, are highly unstable because of the acquisition conditions. For example, the presence of some highlights or complements, such as glasses, make a face image to be very different to another one of the same person. Because of these drawbacks we propose in this

initial approach to use as public key a specific face image per subject, or, at least, very similar ones taken under the same conditions. In this context, the requirements of the face hashing system are the following: (*i*) to obtain different strings for images of different subjects and (*ii*) to use just the face image as information of the subject to get the bits string of the user. Furthermore we would like the system to be fast and with low computational demands. Thus, it could be implemented in portable devices. In this context, we found in the literature interesting approaches for face hashing [26, 25, 27], although they do not fulfil all the above specified conditions. For this reason we developed a simple face hashing algorithm that takes the desired conditions into account.

The paper is organized as follows. Section 2 provides an overview of the current work in combining biometrics with signature schemes and identity-based systems, highlighting some of their strong points and limitations. Section 3 presents our approach to face biometrics data acquisition and the proposed face hashing algorithm. An overview of the chosen identity-based scheme is provided in Section 4. Some experimental results from the face hashing algorithm are exposed in Section 5. Finally, Section 6 outlines the conclusions and further work.

2 Related work

Currently, biometrics has many applications within the field of security. In general, the research of this topic is focussed in two main issues: the generation of symmetric keys which may be used to encrypt sensitive data [5, 6], and the developement of access control systems via pattern recognition techniques [11, 12]. In the first case, biometric data usually acts as a replacement to passwords and relies in the easy acquisition of data. In this context, we can find some approaches based on fingerprints or face biometrics [1], although the latter are less common. In contrast, in the case of access control systems, we find a broader set of choices on biometric data, mainly encompassing fingerprint, eye iris and face recognition.

Nevertheless, we can find just a few attempts for signature schemes based on biometric data. In [13], a general framework of digital signature generation based on applying a fuzzy vault [16] scheme to biometric data is presented. Even though the authors propose the use of fingerprints, it could be applied to any kind of biometrics. However, upon closer inspection, the biometric data is only used to provide standard access control via pattern matching to a keystore. No biometric data is actually used to generate the secret key itself, or during signature processing. Once the keystore content is available, standard RSA [17] or ElGamal [18] signature methods proceed, with biometric data having no additional role during the encrytion process.

Proposals which actually generate RSA secret keys from biometric data may be found in [15, 14]. Instead of using random prime numbers to search for a suitable RSA secret key, an iris reading is used. The former paper exposes the general method, whereas the later proposes an actual implementation. Each time a signature must be generated, the secret key is obtained from the biometric data.

Apart from that, the scheme follows the standard RSA algorithm. In this case , it is at the validation stage where biometric data plays no role. Following the same principles, we can find approaches using ECC (Elliptic Curve Cryptography)[20] instead of RSA [15].

Notice that the exposed biometric signature schemes use different approaches and different kinds of data to generate secret keys. However, they share a common requirement: they need a PKI to link any user's public key to his or her actual identity. In particular, biometric data is only used at the signing stage, but not at the validation stage.

In this context, Shamir [10] proposed identity-based systems as an alternative to PKI as a means to link public keys to identities. Instead of generating a secret key from which the public key is inferred, the process is just the opposite. The user chooses an identifier unique to him, which directly becomes his public key, and then obtains the secret key from it. The chosen identifier is then made publicly available. This is an approach which may be applied to biometrics if we consider that some types of biometric data are a publicly available unique identifier under some contexts, such as the face. Up to our knowledge, the current literature on biometric identity-based systems do not take faces into account as a mechanism to transmit the public key.

The notion of a biometric identity-based system signature scheme is proposed in [2], which provides a complete description, including implementation details, of how this goal may be achieved. However, the main biometric data the authors' have in mind is fingerprints, since, under their scheme, anybody who has access to the biometric data may generate valid secret keys. In fact, biometrics are used at both the signature and validation stage, acting as both secret and public key. Therefore, signature validation assumes collaboration of the signer, who must be present in person during the process and requires an arbitrator who corroborates the validity of the acquired data each time. Such requirement is a very big constraint, and thus, the system does not fulfill our requirement that biometric information can be easily accessed during validation.

A brief extension to the previous proposal is presented [3], still based on fingerprints. Its main contribution is eliminating the need for an arbitrator at the validation stage. This is achieved by proposing a scheme where it is possible to deduce the original biometrics from the validating public key. Nevertheless, signer presence is still required, since fingerprints must be read at the validation stage. Following the idea of using fingerprint data, an authentication scheme, also under an identity-based system, is proposed in [4].

3 Hashing Algorithm for Face Images

In this paper we propose to use face images as the user's public key. However, it is not feasible to directly use the face images because of their size. Notice that the scheme proposed by Shamir accounted for ID's characters strings with the size of an standard username or an e-mail address. Therefore, each face image

must be previously processed to obtain a face hash, with a much smaller size, which will be the actual input for the validation algorithm.

This section describes the proposed method for face hashing. In this first approach, our goal is to obtain a binary string from a face image such that

- Face image strings obtained from different subjects have to be different
- The hash function has to use just the face image as user-specific information. Non additional user-specific data can be used for the binary string generation, given that the public key of our system is specifically the face image.

Furthermore, for our future work, we would like to obtain highly correlated bit strings for different face images of the same person.

The proposed hashing method uses Principal Component Analysis (PCA) [22] to reduce the initial data dimensionality. Next subsection briefly describes PCA and then we detail the our face hashing proposal.

3.1 Principal Component Analysis

Principal Component Analysis (PCA) is a non-supervised linear feature extraction technique. It is frequently applied in classification and clustering problems given its simplicity and optimality.

The method seeks a linear transformation of the data keeping as much information as possible under the Euclidean reconstruction criterion. Concretely, it finds an orthogonal set of projection vectors computed as the first eigenvectors of the data covariance matrix. These eigenvectors are sorted by their respective eigenvalues, to preserve the maximum possible amount of the data variance.

In this context, all the data can be projected to the lower dimensional feature space generated by the first eigenvectors. This new data representation is called *eigenrepresentation*, while the new feature space is called *eigenprojections space* or *eigenspace*.

The use of these technique is specially suitable to process visual data, in order to reduce redundancy and noise. For this reason we transform the face images using this method for the bit string computation.

3.2 Face Hashing Method

Our face hasing algorithm is inspired by the work of Goh and Ngo [23]. Briefly, their procedure is based on iterated inner-products between pseudorandom and user-specific eigenprojections. Thus, given a face image, they project the image in the eigenprojection space and segment this new representation computing inner products with subject-specific random normalized vectors. Then, using empirical thresholds, they binarize each of these inner products in 0/1, to construct the hash string.

We chose this bio-hash algorithm as our starting point due to its functional advantages compared to other methods in terms of consistency and simplicity.

However, we can not directly apply this system for our purpose, given that we do not want to use additional user-specific information except of the face image to construct the hash code. More concretely, we want the public key to be just the face image, and not both the face image and some additional information of the user. Thus, we need a bio-hashing algorithm that uses just the face image to obtain the bits string.

Taking into account the requirements of our signature scheme, in this first approach we propose to construct the bit string from a face image computing inner products between the eigenrepresentation of the face image and a general set of random vectors. After that, another set of general random vectors will be used to compute specific thresholds for binarizing the inner products.

Following we detail the proposed method to get the bits string of a face image $\mathbf{I}$ in grey intensities. In particular, we supose that the size of the image $\mathbf{I}$ is $n \times m$ pixels and denote $D = nm \in \mathbb{R}$.

Parameters of the algorithm:

- Eigenspace dimensionality $d \in \mathbb{N}$, and the corresponding PCA transformation found previously using face images. This new dimensionality has to verify that $d < D$.
- Predefined bits string length, $N \in \mathbb{N}$
- A set of random vectors: $\mathbf{U} = \{\mathbf{u}_1, \ldots, \mathbf{u}_N\}$; $\mathbf{u}_i \in \mathbb{R}^d$, for all $i = 1, ..., N$.

Algorithm:

1. Express $\mathbf{I}$ as a features vector $\mathbf{x} \in \mathbb{R}^D$, where $D = nm$, concatenating the different columns of $\mathbf{I}$. This process is illustrated in Figure 1.
2. Project $\mathbf{x}$ to the eigenspace of dimensionality d, using the previously learned PCA transformation, obtaining $\mathbf{y} \in \mathbb{R}^d$.
3. Compute $a_1, ..., a_N$ calculating the following inner products

$$a_i =< \mathbf{y}, \mathbf{u}_i > \in \mathbb{R}$$

   for all $i, = 1, ..., N$.
4. Compute each bit b_i of the hash string by

$$b_i = \begin{cases} 1 \text{ if } a_i \geq 0 \\ 0 \text{ otherwise} \end{cases}$$

   for $i = 1, ..., N$.

Output: The algorithms returns the bits string of the input image $\mathbf{I}$,

$$(b_1, ..., b_N)$$

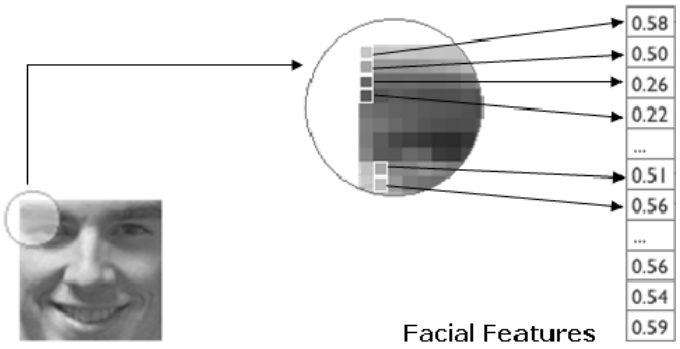


Fig. 1. Initial features vector construction from the face image in grey intensities.

4 Identity-based scheme

In this section we describe the identity-based signature and validation scheme (IBS), once we are able to process the face image of a system user u to calculate a proper face hash, BIO_u. The face image used to derive BIO_u directly becomes user u's public key in the scheme, being made publicly available to other system users. A face image conforms to the identity-based system requirement that it uniquely identifies a user and can be undeniably associated with him.

The scheme is formalized as a set of algorithms:

$IBS = (Setup, KeyDer, Sign, Vf)$.

- The $Setup$ algorithm produces the master secret and public parameters (MSP, MPP) from a security parameter K.
- The $KeyDer$ algorithm is able to generate a user u's secret key, SK_u, from MSP and BIO_u.
- The $Sign$ algorithm is the signature one, which produces a signature σ given the input of a message M and SK_u.
- The Vf algorithm is the signature validation process, returning true if it is deemed valid, or false if invalid.

IBS should conform to the following requirements and properties:

- *Correctness:* Any signature produced by a signing user u must be accepted by the validating algorithm using the biometric hash from u, BIO_u. Thus, $Vf(MPP, BIO_u, Sign(M, SK_u))$ must return true.
- *Uniqueness:* Any given signature produced by u may only validate using BIO_u.
- *Unforgeability:* Only using the system's master public parameters, MPP, it is not feasible for anyone else but u to construct signature which will validate using BIO_u
- *Non-repudiation:* A signing user u cannot deny he produced any signature which validates using BIO_u.

The last property, non-repudiation, is actually a consequence of the former three ones. However, we explicitly state it since it is the main goal of our proposal. Users in the system may prove signature ownership to third parties, without the need for direct arbitration from a trusted entity.

4.1 Signature processing

The signature processing method based on face hashing can be divided in four stages, one for each algorithm in IBS: Setup, Key Derivation, Signature and Validation. For our system, we have decided to use the original scheme proposed by Shamir, as it is a simple one which allows us to easily test how an approach based on face biometrics responds to an identity-based system.

Setup: This is the first step before the identity-based system may be used. it requires the deployment of a trusted entity, the Key Generation Center (KGC) which initializes the system parameters, (MSP, MPP). In the context of a social network, the administrator would take the role of the KGS.

1. Two large primes are chosen, their product being n.
2. Two integers e and d, so that $gcd(e, \varphi(n)) = 1$ and $ed = 1 \mod \varphi(n)$, are chosen.
3. A hash function $h : \{0,1\}^* \rightarrow Z_{\varphi(n)}$ is chosen.
4. The system parameters are considered initialized: $MSP = (d)$ and $MPP = (n, e, h)$.

Key Derivation: Whenever a new user u joins the system, his secret key must be derived from the public biometric data (the face), using the $KeyDer$ algorithm, before he can sign data. This step implies that, apart from the required personal information, he also provides a photo at registration, which will be processed by the KGS. Once the photo is available, this process follows.

1. The face image is processed according to the method presented in Section 3. The user biohash BIO_u is obtained, in the form of a bit array.
2. The user secret key is calculated using the following operation: $SK_u = {BIO_u}^d \mod n$
3. Once registration has been successfully completed, the user is provided with SK_u and MPP, the latter already generated at the Setup stage.

Signature: Whenever a user u wants to sign message m to some other user within the system, the following calculations are completed.

1. The user chooses a random number r.
2. Value $t = r^e \mod n$ is calculated.
3. Value $s = SK_u * r^{h(t||m)} \mod n$ is calculated.
4. (t, s) is considered the signature.

Validation: Before signed message validation may occur, users must exchange their images. In the context of a social network, this may be automatically achieved by accessing the contact's profile, or just directly sending the image file. At an in person meeting, a photo may be taken with a mobile phone and stored for later usage.

Whenever a user recieves a signed message from another user u, it may be validated in the following manner.

1. User u's photo is retrieved.
2. The claimed identity is checked by looking and the photo and corroborating that the person who appears is, in fact, u. This step can be completed by the validating user himself.
3. The BIO_u is derived from the image using the method described in Section 3.
4. The signature is validated evaluating the expression $s^e = BIO_u * t^{h(t||m)} \mod n$. If the expression is valid, then so is the signature.

5 Experiments

We tested the proposed system with the FRGC [21] database. Concretely, we used the subset of images acquired under controlled conditions. It is composed of 3772 images from 275 subjects, having from 2 to 16 images per person. The faces have been aligned according to the eyes and resized at a resolution of 81×77 pixels. Notice that this process can be performed automatically using eye detection algorithms [24].

For this experimental validation, we used just the *internal face features*, composed by eyes, nose and mouth. Figure 2 includes some examples of images in the FRGC database after being aligned, resized and cropped.

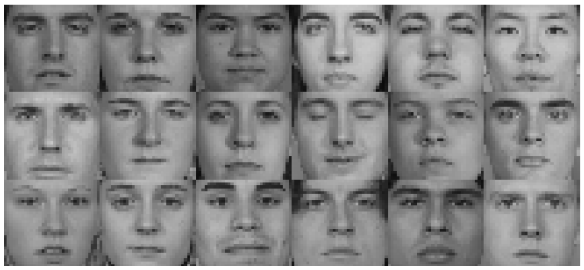


Fig. 2. Examples of images from the FRGC database after being aligned, resized and cropped.

The experiments are performed to show that the proposed procedure produces different codes for different subjects. Furthermore, we also want to evaluate the choice of parameters d and N. For this goal, we randomly selected

one image per each of the 275 subjects and compute the Hamming distances between their corresponding bit string, using different parameters. These values are called the *inter class* Hamming distances.

First, we make an experiment to explicitly evaluate the choice of parameters d and N. For this aim we computed the *inter class* Hamming distances for different values of d and N. Tables 1 are detailed the the mean and the standard deviation of these distances.

Table 1. Mean(*mean*) and standard deviation (*std*) of the inter-class Hamming distances for different values of d and N.

	N	1000	2000	3000	4000	5000
$d = 50$	*mean*	250.2	500.4	750.6	1001.0	1251.3
	std	55.2	109.5	160.5	214.6	270.1
$d = 100$	*mean*	250.3	500.5	750.9	1001.2	1251.4
	std	49.4	100.9	153.5	197.5	249.0
$d = 150$	*mean*	250.3	500.7	750.9	1001.3	1251.5
	std	50.8	97.1	146.3	194.8	245.6
$d = 200$	*mean*	250.3	500.7	751.1	1001.1	1251.7
	std	49.5	96.3	143.5	198.4	236.6
$d = 250$	*mean*	250.3	500.6	751.1	1001.3	1251.4
	std	47.6	95.2	143.9	191.5	240.1

Notice that the Hamming distances are most dependant of N than of d. In particular, for a fixed d the distances increase depends linearly on N. This can be more easily seen in Figure 3, where we show the evolution of the maximum, the minimum and the mean inter-class Hamming distances for $d = 250$. Concretely, we observe in this case that the inter-class Hamming distances are, at least, 10% of N.

5.1 Intra-Class Hamming Distances

In this first approach our system uses always the same image per subject as a public key. However, in the future, we want that the public key of the user could be any image of his or her face. For this aim, we need to find a face hashing function that produces exactly the same bit string for different images from the same person, which is currently an open problem.

In this context, we have performed one experiment to evaluate the intra-class Hamming distances obtained with the proposed algorithm. That is, the Hamming distances of strings obtained with different images of the same subject.

Thus, for all the images of subject in the database we computed the corresponding strings following the proposed algorithm. Then, for each subject, we compute the different Hamming distances among the strings obtained with his or her images. After that we computed the mean, the minimum and the maximum

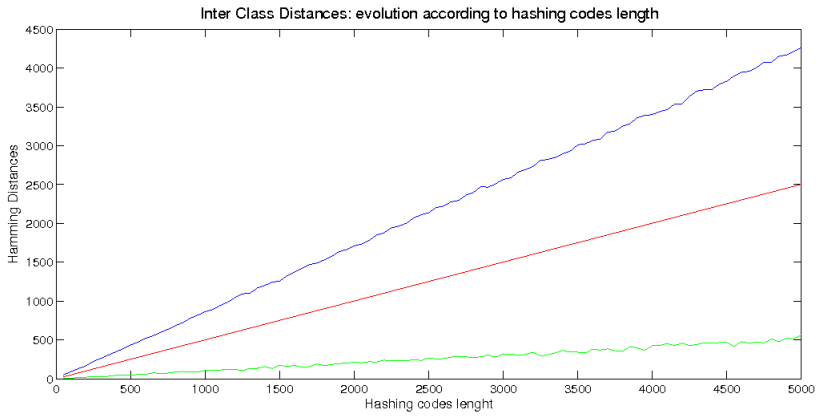


Fig. 3. Evolution of the inter-class Hamming distances in function of the code length N, for $d = 250$.

Hamming distances per subject. The parameters selected for this experiment where $d = 250$ and $N = 3000$.

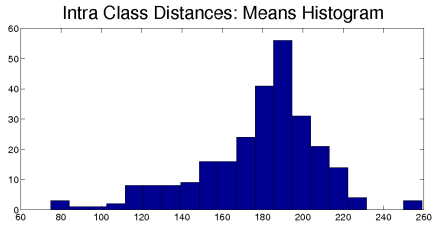
In Figure 4 we show the histograms of these distances.

As expected, our method never gets the same string for different images from the same person. However, the intra-class Hamming distance is always less than 423. Notice that, using the same parameters, the inter-class Hamming distance was always higher than 304 (see Figure 3). Then, comparing these results, we can see that, with our system, the intra-class Hamming distance is in general significantly lower than the inter-class Hamming distance.

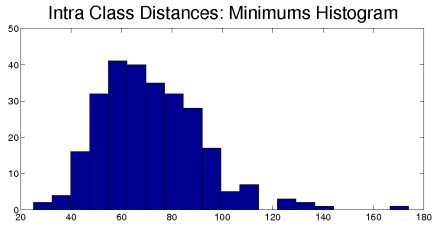
6 Conclusions

This paper proposes a basic framework for digital signature generation and validation reliant of face biometrics. This is achieved by using an identity-based system. The main novelty of our approach is the fact that, in this case, it is not based in private biometric data, difficult to access or requiring the signer's collaboration at the validation stage. On the contrary, it relies on easily available data. Up to our knowledge, no other identity-based biometric signature system uses face data, just fingerprints.

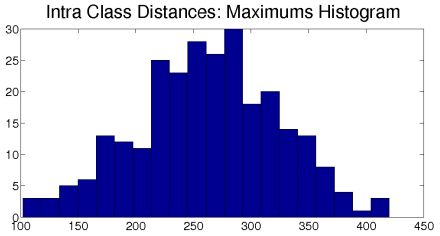
The main advantage of our system is providing a very intuitive method to link personal identities to public keys, which meshes well with current popular systems such as social networks, where friends already share their photos as part of their daily activities. Furthermore, for human beings, a face is easier to retrieve and recognize than random data. It must be also taken into account that face biometric data is much easier to acquire than any other sample type, even by non tech-savvy users in impromptu situations. A phone camera, an increasingly common element, is enough. In fact, a public key/certificate keystore may not



(A)



(B)



(C)

Fig. 4. Histograms of the mean (A), minimum (B) and maximum (C) Intra-Class Hamming distances.

need be necessary, in contrast with traditional systems. Whenever a friend's public key must be retrieved, the key's authenticity is implicit.

For our aims we proposed a fast algorithm for face image hashing. The method can manage large amounts of images and may be easily implemented with low computational loads in portable devices. We made some experiments to test the performance of the method. The results showed that our method produces different bits strings for different subjects, while the obtained strings of different images from the same subjects are highly correlated.

Further work includes improving the data acquisition process to increase the breadth of image types which can be processed by our system to generate proper secret keys. Additionally, more modern identity-based signature schemes, such as the ones based on well pairings, could be tested. We also feel it would be important to study how the system can be further integrated with the current social networks' workings. For example, how a complete stranger may guarantee that someone's photo belongs to the claimed identity, instead of assuming a former personal relationship.

Acknowledgements

This work has been supported by the Spanish Ministry of Science and Innovation, the FEDER funds under the grants TSI2007-65406-C03-03 E-AEGIS, CONSOLIDER-INGENIO CSD2007-00004 ARES.

References

1. B. Chen, V. Chandran: Biometric Based Cryptographic Key Generation from Faces. Proceedings of the 9th Biennial Conference of the Australian Pattern Recognition Society on Digital Image Computing Techniques and Applications, pp. 394–401 (2007).
2. A. Burnett, A. Duffy, T. Dowling and N. Maynooth: A Biometric Identity Based Signature Scheme. Report (2004).
3. X. Liu, Q. Miao and D. Li: A Biometric Identity Based Signature Scheme with Convenient Verification. Future Generation Communication and Networking 1, pp. 113–117 (2007).
4. W. Jiang, Z. Huang, Y. Yang, J. Tian, L. Li: ID-based authentication scheme combined with identity-based encryption with fingerprint hashing, The Journal of China Universities of Posts and Telecommunications, vol. 15, no. 4, pp. 75–80.
5. Y. Chang, W. Zhang and T. Chen: Biometrics-Based Cryptographic Key Generation. IEEE International Conference on Multimedia and Expo 38 (5), pp. 2203–2206 (2004).
6. H. Chen, H. Sun and K. Lam: Key Management Using Biometrics. Proceedings of the The First International Symposium on Data, Privacy, and E-Commerce, pp. 321–326 (2007).
7. CCITT: The Directory Authentication Framework. Recommendation (1988).
8. J. Daugman: Biometric Decision Landscapes. Technical Report UCAM-CL-TR-482, Computer Laboratory, Univ. of Cambridge, (2000).

9. F. Hao, R. Anderson and J. Daugman: Combining cryptography with biometrics effectively, IEEE Trans. Comput. 55 (9), pp. 1081-1088 (2006).
10. A. Shamir: Identity-Based Cryptosystems and Signature Schemes. Advances in Cryptology: Proceedings of CRYPTO 84, Lecture Notes in Computer Science, 7, pp. 47–53, (1984).
11. A. Lapedriza, D. Masip, J. Vitri: On the Use of External Face Features for Identity Verification. Journal of Multimedia, Vol 1, No 4, pp. 11–20 (2006).
12. Y.Zhu, T. Tan, Y. Wang: Biometric Personal Identification Based on Iris Patterns. 15th International Conference on Pattern Recognition (ICPR'00), pp. 2801 (2000).
13. J. Jo, J. Seo, H. Lee: Biometric Digital Signature Key Generation and Cryptography Communication Based on Fingerprint. Lecture Notes in Computer Science, vol. 4613, pp. 38–49 (2007).
14. P.K. Janbandhu, M.Y. Siyal: Novel biometric digital signatures for Internet-based applications. Information Management & Computer Security, vol. 9, no. 5, pp. 205–212 (2001).
15. M. Peyraviana, S. M. Matyasa, A. Roginskya, N. Zunica: Generation of RSA Keys That Are Guaranteed to be Unique for Each User, Computers & Security, vol. 19, no. 3, pp. 282–288 (2000).
16. A. Juels, M. Sudan: A Fuzzy Vault Scheme. Designs, Codes and Cryptography, vol. 38, no. 2, pp. 237–257 (2006).
17. R. Rivest, A. Shamir, L. Adleman: A method for obtaining digital signatures and public-key scryptosystems. Communications of the ACM, no. 21, pp. 120-126 (1978).
18. T. ElGamal, A. Public: Key Cryptosystem and a Signature Scheme based on Discrete Logarithms. IEEE Transactions on Information Theory, vol 30, no. 4, pp. 469–472 (1985).
19. S. Mohammadi, S. Abedi: ECC-Based Biometric Signature: A New Approach in Electronic Banking Security. Proceedings of the 2008 International Symposium on Electronic Commerce and Security, pp. 736–766 (2008).
20. N. Koblitz: Elliptic curve cryptosystems. Mathematics of Computation, no. 48, pp. 203209 (1987).
21. P. J. Phillips and P. J. Flynn and T. Scruggs and K.W. Bowyer and J. Chang and K. Hoffman and J. Marques and J. Min and W. Worek: The 2005 IEEE Workshop on Face Recognition Grand Challenge Experiments, Proceedings of the 2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05) - Workshops (2005).
22. M. Kirby and L. Sirovich : Application of the Karhunen-Loeve Procedure for the characterization of human faces. IEEE Transactions on Pattern Analysis and Machine Intelligence, vol 12, no. 1, pp. 103–108 (1990).
23. A. Goh and D.C.L. Ngo: Computation of cryptographic keys from face biometrics. In International Federation for Information Processing, volume 2828 of LNCS, 2003.
24. Wang, P. and Green, MB and Ji, Q. and Wayman, J.: Automatic eye detection and its validation. IEEE Computer Society Conference on Computer Vision and Pattern Recognition, pp. 164–168, 2005.
25. Chen, B. and Chandran, V.: Biometric based cryptographic key generation from faces. 9th Biennial Conference of the Australian Pattern Recognition Society on Digital Image Computing Techniques and Applications, pp. 394–401, 2007.
26. Ngo, DCL and Teoh, ABJ and Goh, A.:Biometric hash: high-confidence face recognition. IEEE transactions on circuits and systems for video technology, vol. 16, no. 6, pp. 771–775, 2006.

27. Zhao Zeng and Paul A. Watters: A Face Hashing Algorithm using Mutual Information and Feature Fusion. Proceedings of the 2007 IEEE International Conference on Networking, Sensing and Control, pp. 15–17, 2007.