IET Biometrics

Research Article

IET Journals
The Institution of Engineering and Technology

SEMBA: secure multi-biometric authentication

ISSN 2047-4938
Received on 7th June 2018
Revised 19th March 2019
Accepted on 11th June 2019
E-First on 23rd August 2019
doi: 10.1049/iet-bmt.2018.5138
www.ietdl.org

Mauro Barni[1], Giulia Droandi[1] ✉, Riccardo Lazzeretti[2], Tommaso Pignata[1]

[1]*Department of Information Engineering and Mathematics, University of Siena, Siena, Italy*
[2]*Department of Computer, Control, and Management Engineering 'Antonio Ruberti', Sapienza University of Rome, Rome, Italy*
✉ *E-mail: giulia.droandi@gmail.com*

Abstract: Biometrics security is a dynamic research area spurred by the need to protect personal traits from threats like theft, non-authorised distribution, reuse and so on. A widely investigated solution to such threats consists of processing the biometric signals under encryption, in order to avoid any leakage of information towards non-authorised parties. In this study, the authors propose to leverage on the superior performance of multimodal biometric recognition to improve the efficiency of a biometric-based authentication protocol operating on encrypted data under the malicious security model. In the proposed protocol, authentication relies on both facial and iris biometrics, whose representation accuracy is specifically tailored to the trade-off between recognition accuracy and efficiency. From a cryptographic point of view, the protocol relies on Damgård *et al.* SPDZ. Experimental results show that the multimodal protocol is faster than corresponding unimodal protocols achieving the same accuracy.

1 Introduction

In the digital and increasingly interconnected world we live in, establishing individuals' identity is a pressing need [1, 2]. For this reason, in the last decades, we are witnessing an increasing interest in biometric-based recognition systems. Biometric recognition can be split into two main categories: authentication and identification. In the first scenario, also referred to as *verification*, the user is interested in demonstrating that he/she is who he/she claims to be, while in the second one, referred to as *identification*, the goal is to determine the identity of the user submitting the biometric template among those *known by the system*. Usually, in both verification and identification protocols, a single biometric trait is used to extract a biometric template, usually represented as a feature vector. The feature vector then is matched with one or more templates stored in the system database.

Under the EU GDPR (General Data Protection Regulation) [3], biometrics are considered a special category of personal data that requires both a special legal basis for processing and an accompanying data protection impact assessment. Applications using biometrics usually ask for the user consent, but this is not sufficient to prevent the damage caused by a data breach. Hence, recently, the security of biometric systems has become a very active research area, due to the necessity of impeding newly emerging cybercrimes like identity theft, privacy violation, unauthorised access to sensitive information and so on [4].

Protocols allowing to process encrypted biometric signals without decrypting them are among the most widely studied solutions to enhance the security of biometric systems [5, 6]. According to such an approach, verification or identification is carried out by the system relying exclusively only on encrypted biometric templates, thus preventing the risk for sensitive information leakage during the protocol.

The possibility of processing and comparing encrypted biometric templates rely on a number of cryptographic tools [7–10], broadly referred to as multi-party computation (MPC) [11]. Generally speaking, MPC protocols can be classified according to the adopted security model. The most common distinction considers protocols which are secure only against *semi-honest* adversaries, and those which can be proven to be secure also against *malicious adversaries*. To be specific, in the *semi-honest* model, all the parties execute the protocol without deviating from it, but meanwhile they try to obtain as much information as possible about the other parties' data. Protocols developed in the semi-honest model are very efficient and, for this reason, are adopted in the majority of the works proposed so far [5, 6]. On the contrary, in the *malicious* model, the parties can arbitrarily deviate from the protocol in their attempt to get access to sensitive information. While security against malicious parties would be desirable in many real-world applications, the resulting protocols have a very high complexity and their use in real systems is often impractical. The great majority of the attempts are made so far to devise efficient biometric recognition protocols in the malicious setting, focused on the development and use of innovative and efficient MPC and cryptographic primitives. A less investigated approach consists of the adoption of biometric recognition protocols which are better suited to be implemented in a MPC framework. Yet, as highlighted in [6], working on the signal processing side of the problem may help to reduce significantly the complexity of the MPC protocol, e.g. by efficiently trading off between accuracy and complexity.

1.1 Contribution

In this work, we focus on an authentication protocol and, following the above strategy, we present SEMBA: a SEcure Multi-Biometric Authentication protocol which achieves a better trade-off between efficiency and accuracy with respect to the single modality subsystems composing it. This represents a major deviation from most works on multimodal biometric systems, in which the availability of multiple biometric modalities is exploited to decrease interclass variability and improve intra-class similarity in the presence of acquisition noise and any other kind of distortion [12]. In this framework, the main contributions of the paper are as follows:

(i) We design SEMBA, a multimodal biometric system that combines face and iris templates and that can be easily implemented by relying on secure multi-party computation protocols;
(ii) We propose a privacy-preserving multi-biometric authentication protocol secure against a malicious party. SEMBA is based on the SPDZ tool [1, 2] and discloses only the final binary decision;

(iii) We compare our multi-biometric protocol with single biometric protocols, showing that by using a properly simplified representation of the two biometric traits, backed by a rigorous signal processing analysis, the multimodal protocol can reach the same accuracy of the corresponding single-modality systems based on more accurate – and more complicated – representations of iris and face templates, but with significantly lower computational complexity. In particular, SEMBA obtains the same accuracy of the stand-alone iris authentication protocol described in [13]. Nevertheless, system designers could also decide to exploit the better performance allowed by multimodal authentication to improve authentication accuracy with the same complexity of the single modality protocols, according to ISO\IEC TR 24722:2015 [14].

1.2 Outline of the paper

In Section 2, we briefly discuss the state of art of privacy-preserving biometrics systems, focusing on face and iris biometrics. In Section 3, we introduce the cryptographic and biometric protocols we use in our implementation. In Section 4, we describe the SPDZ-based iris, face and multi-biometrics authentication protocols. In Section 5, we present the results of tests carried out in the plain domain. The results of such tests are then used to set the parameters for the tests in the encrypted domain, whose results are presented in Section 6. Finally, in Section 7 we compare SEMBA with the state of the art and in Section 8, we draw our conclusions.

2 Prior works

In the last years, many cryptographic tools, including oblivious transfer [7], homomorphic encryption [9, 15], secret sharing [16] and garbled circuits [8, 17], have been used for privacy protection of biometric templates. In most works, such tools are used in such a way to achieve security in the semi-honest model. Many privacy-preserving authentication protocols have been proposed in the literature making use of a wide variety of biometric traits. Since, in this work, we present a privacy-preserving multi-biometric authentication protocol based on face and iris, we focus on the state of art relative to those biometries, then we discuss the few works achieving privacy protection in the malicious model and finally we discuss the main characteristics of multimodal (or *fusion*) biometric systems.

2.1 Biometric recognition in the semi-honest model

As pointed in [5, 6], many prior works on biometric recognition are designed to be secure against semi-honest adversaries. However, protocols operating in the encrypted domain have high complexity, and they require optimisation by working at different levels. First of all, the biometric algorithm needs an efficient implementation in the encrypted domain, thus algorithms with low implementation complexity appear more suitable, even if they have a (slightly) lower accuracy. As an example, Blanton and Gasti [18] have compared the fingercode- and minutia-based implementations for finger recognition showing that, despite the highest accuracy, the fingercode representation results in a more efficient protocol than the one based on minutiae, whose complexity is almost impractical. For this reason, eigenface [19] and iriscode [20] representations are commonly used for face and iris, respectively. Then the protocol should be optimised to avoid complex operations, again at expense of accuracy, and finally there is the necessity to operate at feature level, accurately choosing the number of features and bits used for their representation, to decrease the complexity while guaranteeing high accuracy. We underline that protocols operating in the encrypted domain have the same accuracy of the same protocol operating in the plain domain where the same optimisations have been applied and using the same feature representation.

Several works have been proposed to evaluate iris recognition and face recognition in the encrypted domain. As far as face recognition is concerned, some examples can be found in [21–24], while with respect to iris recognition, protocols are provided in [18, 25–29].

2.2 Biometric recognition in malicious setting

All the works referred to in the previous section are designed to be secure against semi-honest adversaries. However, there is the need to guarantee higher security to fulfil the requirements imposed by the GDPR, because as pointed out by Simoens *et al.* [30], biometric templates are usually the target of malicious attackers.

There are few works on privacy-preserving biometric authentication secure under a malicious model. Kantarcioglu and Kardes [31] present a way to implement some primitives, specifically the dot product and equality check, in the malicious model, by also analysing the corresponding computational cost. Even if this work is not directly related to biometrics protection, the proposed solutions can be adapted to such an aim. In [32], Abidin illustrates a general framework for biometric authentication that uses a homomorphic encryption scheme to evaluate the distance between two encrypted biometric templates. In his work, Abidin proves security against malicious attacks, but he does not provide any results about the practical implementation of the protocol. In [33], Pathak and Raj describe two speech-based authentication protocols. One of them is a non-interactive protocol which is secure against malicious attacks. In both protocols, the output is a probability value and the client checks if such a value is equal to zero or not in the plain domain.

Several approaches [34–38] have been proposed to make Yao's garbled circuit techniques secure in the malicious model through zero knowledge proof, cut and choose, or other techniques. Such approaches can also be used for biometric authentication protocols, however their high complexity makes them impractical. Gasti *et al.* [39] proposed a lightweight biometric authentication protocol based on simple garbled circuits and secure against malicious adversaries by relying on an untrusted third party (the cloud). In the protocol, the biometric owner acts as circuit constructor, the cloud as circuit evaluator, while the server verifies the correctness of the circuit. The approach is secure against colluding biometric owner and cloud, but not against colluding server and cloud.

2.3 Private multimodal biometric recognition

Given the recent technological advances, new devices are often equipped with numerous sensors, opening the way to multi-biometric authentication. In [40], Ross *et al.* present an overview of the possible fusion scenarios and their applications in real life. For our protocol, we choose a *multimodal* system that combines information from face and iris.

Biometric signals are usually processed in four stages. First, a sensor captures the traits of an individual as raw biometric data. Second, raw data is processed and a compact representation of the physical traits, called *features*, is extracted. Then, the feature template is matched with the templates stored in a database. Finally, the matching score is used to determine an identity or to validate a claimed identity. Information can be merged at any time during a multi-biometric recognition protocol [40]. The choice of a specific fusion strategy depends on the intended application, its specific characteristics and the MPC tool chosen to guarantee privacy. Fusing the biometric signals at an early stage results in a higher accuracy of the protocol at the expenses of a higher complexity. For this reason, the most used approach, and the one we use in this paper, is score level fusion, whereby the match scores from each biometric trait involved in the process are combined to obtain the final result. Score level fusion combines good accuracy and relatively easy implementation.

To the best of our knowledge, Gomez-Barrero *et al.* [41] have proposed the only previous work on multi-biometric privacy protection operating in the encrypted domain.

In [41], the authors present a general framework for multi-biometric template protection based on Pailler cryptosystem, in which only encrypted data is handled. The authors examine the outcome of the fusion of on-line signature and fingerprints, at three different levels of fusion: feature, score and decision levels. During the enrolment phase, the client, $\mathscr{C}$, acquires the probe and extracts the template $\boldsymbol{T}_r$. $\mathscr{C}$ encrypts $\boldsymbol{T}_r$ and sends it to the server, $\mathscr{S}$. $\mathscr{S}$ holds only encrypted templates in the database and a pair (sk, pk) of public and secret keys. During verification, $\mathscr{S}$ sends the

encryption of the reference template $E(\boldsymbol{T}_r)$ to $\mathscr{C}$. The client computes the encrypted distance between $E(\boldsymbol{T}_r)$ and the new probe $\boldsymbol{T}_p$. Since $\boldsymbol{T}_p$ is available only on the client side, it does not need to be encrypted. Moreover, $\mathscr{C}$ does not know sk and has no access to $\boldsymbol{T}_r$. Finally, the server decrypts the distance score and computes the final decision. Gomez *et al.* system is secure in the semi-honest model, therefore all the parties involved follow the protocol honestly. For this reason, the score computed by $\mathscr{C}$ can be assumed correct. However, a drawback of the system is that final comparison is carried out on plain data by the server, thus introducing a breach into the security of the system.

Other secure multi-biometric solutions: While in this paper we focus on privacy-preserving multi-biometric recognition protocols based on secure multi-party computation algorithms, we underline that other secure solutions have been proposed in the literature. Sowkarthika and Radha [42] have proposed a protocol for joint iris and fingerprint authentication where fusion is performed at feature level and security is based on fuzzy vaults. As other biometric fuzzy vault solutions [43], the proposed protocol has an efficient encoding protocol, while decoding is based on Reed-Solomon error-correcting code. Given the protocol simplicity, fuzzy vault based protocols are more efficient than MPC-based authentication protocols. On the other side, fuzzy vault has shown weaknesses against correlation attacks [44], attacks via record multiplicity, blended substitution attacks [45] and other attacks, which cannot be performed in the encrypted domain if the protocol is secure against active adversaries.

Some works [46–48] exploited fuzzy commitment schemes for multi-biometric protection. In fuzzy commitment scheme, biometrics are protected by xoring them with a secret key chosen during an enrolment procedure in which biometric data are observed for the first time. This key is to be reconstructed after these biometric data are observed again during an attempt to obtain access (authentication). Since biometric measurements are typically noisy, reliable biometric secrecy systems also extract so-called helper data from the biometric observation at the time of enrolment. Despite the efficiency of the fuzzy commitment schemes, the helper data are assumed to be public, and therefore they should not contain information on the secret, hence secrecy leakage should be negligible, as shown in [49]. To solve the problem, Failla *et al.* [50] proposed to implement fuzzy commitment scheme in the encrypted domain.

In [51], authors propose an anti-spoofing multispectral biometric cloud-based identification approach for privacy and security of cloud computing. The approach offers a protocol based on a different multi-biometric representation. Authors are not leveraging on multiple biometrics, but on multiple representations of the same biometric. Their solution uses multi-spectral palmprint to generate features and then encrypts them by relying on unpadded RSA Cryptosystem. Encrypted features collected during the enrolment phase are used to train a regularised extreme learning machine classifier able to handle the variations in the encrypted biometrics and recognising the user. Unfortunately, unpadded RSA is deterministic and hence weak against chosen plaintext attacks. For this reason, the protocol cannot provide sufficient security.

3 Tools

In literature, some frameworks that secure only against a passive adversary have been proposed. Among them, we highlight Sharemind [52], ABY [53] and SPDZ [1, 2]. ShareMind is a commercial framework developed at the University of Tartu which derives its efficiency from the great variety of protocols for integer, fix- and floating-point operations, as well as for shuffling the arrays. ABY [53] is a novel framework that allows a flexible design process for developing highly efficient applications. It has been developed by applying several state-of-art MPC techniques and using exiting protocols in a novel fashion. ABY supports three different sharing methods (Arithmetic, Boolean and Yao) and also allows efficient conversion from one to another. SPDZ is a two- or multi-party computation protocol secure against an active adversary corrupting up to $n-1$ of the n players.

Among them, we chose SPDZ because of its security against active adversaries and high efficiency. SPDZ is not only the secret sharing tool that can be used for secure multi-party computation with active adversaries, but it is best suited to our purpose. For example, the system presented in [54] provides perfect security against an active, adaptive adversary corrupting $t < n/3$ players, which is not optimal for our scope.

In the remaining of this section, we present the SPDZ protocol and biometric tools used in our protocol.

3.1 Cryptographic tools: SPDZ system

Damgård *et al.* [1, 2] proposed the MPC framework named SPDZ, a two- or multi-party computation protocol secure against an active adversary corrupting up to $n-1$ of the n players. This method uses multiplicative triples generated offline by using somewhat homomorphic encryption (SHE) to efficiently perform online secret sharing operations.

We assume that all computations are performed over a fixed finite field $\mathbb{F}_p$ of characteristic p; where p is a prime number. Each player P_i has an uniform share $\alpha_i \in \mathbb{F}_p$ of a secret key α such that $\alpha = \sum_{i=1}^{n} \alpha_i \bmod p$ (in the following we omit the indication of the modulus operation for simplicity). In this paper, we focus on secure two-party computation protocols, then $n = 2$ and $\alpha = \alpha_1 + \alpha_2$. An item $a \in \mathbb{F}_p$ is $\langle \cdot \rangle$-shared if the player P_i holds a tuple $\langle a_i, \gamma(a)_i \rangle$ such that $a = a_1 + a_2$ and $\gamma(a) = \gamma(a)_1 + \gamma(a)_2$. In other words, a_i and $\gamma(a)_i$ are additive secret shares of a and $\gamma(a)$. The value $\gamma(a)$ represents the message authentication code (MAC) of a. Any operation involving some variables is also performed on their MAC, so that, at the end of the protocol, the MAC is checked before revealing the outcome. If one of the parties has a different MAC from the others, the procedure aborts. During the description of the protocol, we say that a $\langle \cdot \rangle$-shared value is *partially opened* if each party reveals to the other one the value a_i but not the associated $\gamma(a)_i$.

An SPDZ protocol can be divided into two major phases. The preprocessing phase, sometimes referred to as the offline phase, where the system is set up, and the online phase, where the actual computation is performed.

3.1.1 Preprocessing phase: In the offline phase, the parties generate a public key and a shared secret key for the SHE scheme. Then, relying on the homomorphic properties of SHE, the preprocessing protocol generates α and α's shares, input shares, shares of tuples for multiplications and squares, and the random share values necessary to evaluate the comparison [2]. As in [2], we assume that the shares of a common key of a homomorphic encryption scheme have been distributed to all the parties, along with the share of the MAC key and an encryption of the MAC itself.

The offline phase of SPDZ protocol has two distinct sub-phases. In the first one, random data are encrypted and used to create multiplication tuples, square tuples and shared bits, by exploiting the homomorphic properties of the cryptosystem. Tuples and bits are over-produced with respect to the quantity needed by the online protocol (the total tuples number is doubled). Since an adversary could induce an error during tuples construction, and therefore compromise the whole following computation, in the second sub-phase a random subset of the material previously produced is consumed in order to verify if tuples and shared bits have been built correctly. The check is done by *sacrificing* techniques, i.e. half of the tuples are partially opened and then the MACs are checked without revealing the MAC key. The detail of this last operation is described in [2].

In this paper, we assume that the generation of tuples and inputs has already been carried out in the encrypted domain before the protocol starts and we focus on the analysis of the online part of the system.

3.1.2 Online phase: Operations in SPDZ: By using SPDZ, linear operations, such as additions and scalar multiplications (see

Table 1), can be performed on the $\langle\cdot\rangle$-shares without interaction; while products between ciphertexts and comparisons need data transmission and proper sub-protocols using the multiplication triples generated during the preprocessing phase.

Multiplication: Here, we show how to securely evaluate the product between two ciphertexts and the square of a ciphertext [2]. During the offline phase, several *multiplication triples* are produced. If $a, b, c \in \mathbb{F}_p$ are such that $c = a \cdot b$, then a multiplication triple is the set $\{\langle a\rangle, \langle b\rangle, \langle c\rangle\}$. In the online phase, to multiply two shared $\langle x\rangle$ and $\langle y\rangle$, we take a multiplication triple $\{\langle a\rangle, \langle b\rangle, \langle c\rangle\}$ and we partially open $\langle x\rangle - \langle a\rangle$ and $\langle y\rangle - \langle b\rangle$, disclosing $\varepsilon = x - a$ and $\delta = y - b$ to both parties. Now the shares of $z = x \cdot y$ can be computed as $\langle z\rangle = \langle c\rangle + \varepsilon \cdot \langle b\rangle + \delta \cdot \langle a\rangle + \varepsilon \cdot \delta$. and δ.

Similarly, during the offline phase, we prepare a list of pairs of $\langle\cdot\rangle$-shared values $\{\langle d\rangle, \langle e\rangle\}$ such that $e = d^2$ $(d, e \in \mathbb{F}_p)$. This arrangement allows to efficiently compute the square of a shared value x using only one transmission. Since the square protocol is similar to multiplication, we refer to [2] for details.

Complexity: Each multiplication requires two transmissions between the parties to partially open ε and δ, while each square operation requires only one transmission.

Comparison: Here we describe the computation of a secure comparison $x < y$, for any two elements $x, y \in \mathbb{F}_p$. We rely on the protocol proposed in [55] that has the lowest computational complexity among all the secure comparison protocols proposed so far.

The comparison computation is based on the observation that $\langle x < y\rangle$ is determined by the truth values of $\langle x < (p/2)\rangle$, $\langle y < (p/2)\rangle$ and $\langle (x - y) \bmod p < (p/2)\rangle$, where $\langle x < y\rangle$ indicates the share values of the outcome of $x < y$. By choosing p large enough to guarantee that both inputs are lower than $\frac{p}{2}$, only $\langle (x - y) \bmod p < (p/2)\rangle$ needs to be evaluated.

Given $z = x - y$, then $\langle x < y\rangle$ can be easily computed as $1 - \langle z < (p/2)\rangle$. We observe that if $z > (p/2)$, then $2z > p$. Since we work on $\mathbb{F}_p$, we have that $2z \bmod p = 2z - p$ and it is odd; else if $z < (p/2)$ then $2z < p$ and it will be even because we do not need any modular operation. Therefore, to establish if z is larger or smaller than $p/2$ we need to determine only the last significant bit of $2z$. To compute the last significant bit of $2z$, we use a value $\langle r\rangle$ shared by the parties both as integer and as a bit array. The value r along with its bit decomposition is pre-computed off line. We indicate by $r_0 r_1 \ldots r_\ell$ the bits of r and with $\langle r_i\rangle$ the corresponding shared values.

First of all we compute $\langle s\rangle = \langle 2z + r\rangle$, then s is partially opened. If $s < p$ then the last significant bit of $2z$ is equal to $s_0 \oplus r_0$, otherwise it is equal to $1 - (s_0 \oplus r_0)$. Since we work in the field $\mathbb{F}_p$, $s < p$ iff $s < r$. By recalling that s is known to both parties, we can easily obtain a $\langle\cdot\rangle$-share of δ, the truth value of $\langle s < r\rangle$ (i.e. $\langle\delta\rangle = \langle s < r\rangle$) working on the bits of s and on the shared bits of r. Then we use the following procedure to calculate $\langle\delta\rangle = \langle s < r\rangle$.

If $s_0 = 0$ then $\langle\delta\rangle = \langle r_0\rangle$ else $\langle\delta\rangle = \langle 0\rangle$.

For all $i < \ell - 1$ if $s_i = 0$ then $\langle\delta\rangle = \langle r_i\rangle + \langle\delta\rangle \cdot \langle 1 - r_i\rangle$ else $\langle\delta\rangle = \langle r_i\rangle \cdot \langle\delta\rangle$.

Now $\langle z < (p/2)\rangle$ can be easily calculated as

$$\langle\delta \oplus s_0 \oplus r_0\rangle = \langle\delta\rangle - \langle s_0 \oplus r_0\rangle - \langle\delta\rangle \cdot \langle s_0 \oplus r_0\rangle . \tag{1}$$

Since s_0 is known in our implementation

$$\langle\delta \oplus s_0 \oplus r_0\rangle = \begin{cases} \langle\delta\rangle + \langle r_0\rangle - 2 \cdot \langle\delta\rangle \cdot \langle r_0\rangle & \text{if } s_0 = 0, \\ 1 + 2\langle\delta\rangle \cdot \langle r_0\rangle - \langle r_0\rangle - \langle\delta\rangle & \text{if } s_0 = 1. \end{cases} \tag{2}$$

Complexity: This protocol requires one multiplication for each iteration plus one for the last step in (1). Therefore, the complexity depends on the bit length of r and it is equal to ℓ multiplications, which require 2ℓ transmissions.

3.2 Biometrics tools

In our work, we compare two different authentication systems: an iris authentication protocol and a multimodal system relying on the fusion at the score level of iriscode and eigenfaces. As shown in Section 4, both protocols can be implemented efficiently in the encrypted domain by relying on the SPDZ framework. In the following subsections, we first describe the stand-alone iris (Section 3.2.1) and face (Section 3.2.2) recognition protocols in the plain domain, and then we focus on the main characteristics of a general multimodal recognition protocol (Section 3.2.3).

3.2.1 Iris recognition: In our implementation, we use the iriscode template proposed for the first time by Daugman in [20] and then modified by Masek in [13]. The description of the entire extraction process is out of the scope of this paper, therefore we are only giving an overview of the process, focusing mainly on the details which are relevant for the current work.

An iriscode is a bit vector whose length N depends on the radial (r) and angular (θ) resolutions used during template extraction. The extraction process outputs also a bitwise noise mask. The noise mask represents the regions of the iris altered by noise, e.g. by eyelashes end eyelids. To compare two templates (the query and the probe enrolled in the database) the authentication process uses the weighted Hamming distance (HD), where the weights depend on the noise mask bits. In this way only significant bits are used to calculate the distance between the two templates. Given the template length $N = 2 \cdot r \cdot \theta$, we indicate by $\boldsymbol{F}_1 = f_{1,1} \ldots f_{1,N}$ and $\boldsymbol{F}_2 = f_{2,1} \ldots f_{2,N}$ the iris templates and $\boldsymbol{M}_1 = m_{1,1} \ldots m_{1,N}$ and $\boldsymbol{M}_2 = m_{2,1} \ldots m_{2,N}$ the corresponding noise masks. We assume that the value $m_i = 1$ in the mask vector indicates that the bit is affected by noise and must be excluded from the computation. Moreover, we indicate with $\overline{a} = 1 - a$ the negation of a feature bit a. The weighted HD can be calculated as

$$\begin{aligned} \mathrm{HD} &= \frac{\| (\boldsymbol{F}_1 \oplus \boldsymbol{F}_2) \wedge (\overline{\boldsymbol{M}}_1 \wedge \overline{\boldsymbol{M}}_2) \|}{N - \| \boldsymbol{M}_1 \vee \boldsymbol{M}_2 \|} \\ &= \frac{\sum_j^N \left[(f_{1,j} \oplus f_{2,j}) \wedge (\overline{m}_{1,i} \wedge \overline{m}_{2,i}) \right]}{N - \sum_{j=1}^N m_{1,j} \vee m_{2,j}} . \end{aligned} \tag{3}$$

3.2.2 Face recognition: Face templates can be generated by relying on the *eigenfaces* method proposed by Tuck and Pentland in [19] providing a set of facial characteristics that can be used to describe all the faces into the database (the *face-space*), as eigenvectors do in linear algebra. The template associated to a face Γ is the projection of Γ on the face space $\boldsymbol{\Omega} = [\omega_1 \ldots \omega_k]$. Each ω_j describes the contribution of the corresponding eigenface, e_j, in representing the input image. In order to find the image that best matches Γ, the algorithm looks for the projection vector $\boldsymbol{\Omega}_j$ among all database images that minimises the Euclidean distance (ED)

$$\mathrm{ED} = \| \boldsymbol{\Omega} - \boldsymbol{\Omega}_j \| = \sqrt{\sum_{i=0}^{k} \left(\boldsymbol{\Omega}_i - \boldsymbol{\Omega}_{j,i} \right)^2} . \tag{4}$$

3.2.3 Multi-biometric score level fusion: In this work, we choose to use multimodal fusion (face and iris) at score level. This is motivated by the fact that, on the basis of what illustrated in Section 2.2, face and iris recognition protocols allow to easily compute the match score in the encrypted domain. Moreover, we underline that both iris and face can be acquired at the same time in real applications, for example by using a smartphone camera. We summarise our fusion system in Fig. 1.

Match scores generated by iris and face subsystems are characterised by a different range of values: the output of the iris protocol is a real number in [0, 1], while the output of the face recognition protocol is a squared number in $[0, M], M \in \mathbb{R}$. Many ways have been proposed to overcome the problems generated by the differences between the scores provided by different biometric recognition systems (see [40] for more details). Among them, due to the characteristics of our MPC system, we choose a linear

Table 1 Linear operation in SPDZ

Operation	Party 1	Party 2
$\langle a\rangle + \langle b\rangle$	$\langle a\rangle_1 + \langle b\rangle_1$	$\langle a\rangle_2 + \langle b\rangle_2$
$\langle a\rangle - \langle b\rangle$	$\langle a\rangle_1 - \langle b\rangle_1$	$\langle a\rangle_2 - \langle b\rangle_2$
$\alpha \cdot \langle a\rangle$	$\alpha \cdot \langle a\rangle_1$	$\alpha \cdot \langle a\rangle_2$
$c + \langle a\rangle$	$c + \langle a\rangle_1$	$\langle a\rangle_2$

$\langle a\rangle$ indicates the pair $\langle a, \gamma(a)\rangle$, $\langle a\rangle_i$ indicates the pair $\langle a_i, \gamma(a)_i\rangle$.

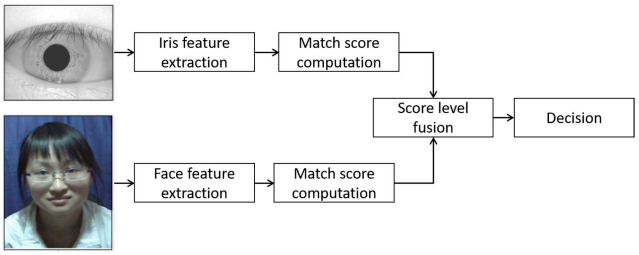

Fig. 1 *General scheme of our fusion protocol*

Table 2 Correspondence table between binary and integer operations

Binary	Integer
$a \oplus b$	$a + b - 2 \cdot a \cdot b$
$a \wedge b$	$a \cdot b$
$a \vee b$	$a + b - a \cdot b$
$\overline{a}$	$1 - a$

combination of the scores. Furthermore, to normalise the face matching score, we choose to use a min–max normalisation method [40]

$$\text{face\_score\_norm} = \frac{\text{score} - \min_{\text{face}}}{\max_{\text{face}} - \min_{\text{face}}}, \tag{5}$$

where $\min_{\text{face}}, \max_{\text{face}}$ indicate the minimum and maximum values of the face range. Since $\min_{\text{face}} = 0$, if $i \in [0, 1]$ is the HD resulting from iris match, f is the ED between faces and R is the maximum value of the face recognition system, multimodal recognition corresponds to checking if the following inequality holds:

$$\alpha \cdot i + \beta \cdot \frac{f}{R} < t \tag{6}$$

where $\alpha, \beta \in [0, 1]$ are proper weights and $t \in [0, 1]$ is the decision threshold. The choice of the parameters α, β, T determines the trade-off between equal error rate (EER) and computational complexity (Section 5.1). As in [41, 56] we choose $\beta = 1 - \alpha$ for the tests in the plain domain. More details are provided in Section 4.

4 Proposed protocol

In this section, we describe the details of SEMBA implementation. We start by presenting the security model (Section 4.1), and then we present the implementation of the iris and face authentication protocols (Sections 4.3 and 4.4) and the multimodal biometric protocol (Section 4.5). Finally, we discuss the security of the SPDZ protocols in Section 4.6.

4.1 Security model

All the protocols involve a client (the biometric owner) and a server that authenticates the identity of the client. Since in our computation we have only two parties, from now on, the SPDZ protocol is described for $n = 2$. We assume that $\mathcal{S}$ and $\mathcal{C}$ have already run the preprocessing phase. We also assume that the server owns a shared reference template of the client. During the online phase, the client could be interested to be authenticated by the server without revealing neither his identity nor his biometric templates. It may also be interested in obtaining records stored by the server for some malicious purpose, e.g. in order to perform spoofing attacks. On the other hand, the server does not want to dislocate its records, while can be interested to collect new biometric templates or identify the user that is authenticated. Hence, both client and server can be malicious, i.e. they may be interested in gaining as much information as possible on the other party even by deviating from the protocol. Considering that the SPDZ protocol involving n parties is secure up to $n - 1$ malicious parties, we assume that only one, either the client or the server, can act maliciously. It is to be pointed out that if both act maliciously, they obtain no real information about the counterpart. We finally assume that the parties are connected through a secure channel providing privacy against eavesdroppers and any third party that can compromise the transmission.

4.2 Biometric representation

To operate in the encrypted domain, we need a version of the authentication protocol that works only with integer numbers. This is a necessary step since the cryptosystem underlying secure protocol can handle only integer numbers. Few solutions operating on floating point exist [57–59], but have higher complexity. For this reason, we must adapt the biometric algorithms of Section 3.2 to let them work with integer numbers. Passing from an algorithm implemented in floating-point arithmetic to one working with integer numbers (fixed-point arithmetic with no truncation) requires that the inputs and the parameters of the protocol are quantised and represented by a suitable number of bits, so that the final output does not differ significantly from the results that would have been obtained with a floating-point implementation. Generally speaking, given a positive floating-point number, we can construct its quantised version multiplying it by a positive integer value and rounding the result to the nearest integer, as specified by the following mapping:

$$a \to a_q = \lfloor qa \rceil$$

where we have indicated explicitly that $\lfloor qa \rceil$ is an integer number that requires a number of bits for the representation chosen in order to have in the new fixed-point protocol negligible accuracy loss with respect to the original floating-point protocol. In our protocol, iris features are binary values and do not need quantisation, while eigenfaces, weights and acceptance threshold are values that must be correctly quantised. We also underline that a protocol operating in the encrypted domain does not introduce any further accuracy loss compared to the corresponding fixed-point plain protocol.

4.3 Iris authentication protocol in the encrypted domain

The SPDZ protocol supports operations modulo p. Each binary element of an iris feature is encrypted as a modulo p integer $\langle a\rangle$-share. For this reason, to implement the HD computation as in (3), we must implement logical operations $\oplus$, $\vee$, $\wedge$ as a combination of integer operations $+$, $-$, $\cdot$. The correspondence between binary and integer operations is detailed in Table 2.

Let $\boldsymbol{F}_1 = f_{1,1}, f_{1,2}, \cdots, f_{1,N}$ and $\boldsymbol{F}_2 = f_{2,1}, f_{2,2}, \cdots, f_{2,N}$ be two binary iris feature templates, where N is the number of features, we indicate with $\langle \boldsymbol{F}_i\rangle$ the vector containing the shares of each element, i.e. the vector $\langle f_{i,1}\rangle, \langle f_{i,2}\rangle, \cdots \langle f_{i,n}\rangle$ for $i = 1, 2$.

Since $\overline{M}_1 \wedge \overline{M}_2$ is equivalent to $\overline{\boldsymbol{M}_1 \vee \boldsymbol{M}_2}$, the HD in (3) can be computed as

$$\frac{\sum_{i=1}^{N} \{(f_{1,i} + f_{2,i} - 2 \cdot f_{1,i} \cdot f_{2,i}) \cdot [1 - (m_{1,i} \vee m_{2,i})]\}}{N - \sum_{j=1}^{N} (m_{1,i} \vee m_{2,i})}, \tag{7}$$

where $m_{1,i} \vee m_{2,i} = m_{1,i} + m_{2,i} - m_{1,i} \cdot m_{2,i}$.

In SPDZ, as well as in other MPC protocols, division is a very expensive operation. Hence, instead of evaluating the division and

then comparing the distance with the decision threshold, the denominator is multiplied by the threshold before the comparison. By letting

$$\text{num} = \sum_{i=1}^{N} \{(f_{1,i} + f_{2,i} - 2f_{1,i}f_{2,i})[1 - (m_{1,i} \vee m_{2,i})]\} \quad (8)$$

and

$$\text{den} = N - \sum_{j=1}^{N} (m_{1,i} \vee m_{2,i}), \quad (9)$$

the authentication check corresponds to

$$\text{num} < t \cdot \text{den}. \quad (10)$$

As it can be seen from (8), many share multiplications are needed to calculate the numerator, namely, N multiplications for each $\boldsymbol{F}_1 \oplus \boldsymbol{F}_2$, $\boldsymbol{M}_1 \wedge \boldsymbol{M}_2$ and $(\boldsymbol{F}_1 \oplus \boldsymbol{F}_2) \wedge (\boldsymbol{M}_1 \wedge \boldsymbol{M}_2)$. To compute the denominator, we can reuse the $m_{1,i} \vee m_{2,i}$ that has already been computed for the numerator. Multiplication between shares requires data transmission, slowing down the computation. To optimise the protocol, we split the multiplication protocol into two parts. First, we calculate $\langle \epsilon_i \rangle = \langle f_{1,i} \rangle - \langle a \rangle$ and $\langle \delta_i \rangle = \langle f_{2,i} \rangle - \langle b \rangle$, for all $i = 1 \ldots N$. Then, to partially open the values, both server and client exchange shares by using a packet for all ϵ's and one for all δ's. In this way, we need only two transmissions for N multiplications.

Complexity: Computing $\boldsymbol{F}_1 \oplus \boldsymbol{F}_2$ and $\boldsymbol{M}_1 \wedge \boldsymbol{M}_2$ requires N multiplications each, one for each element of the template; moreover, N multiplications are required to compute $(\boldsymbol{F}_1 \oplus \boldsymbol{F}_2) \wedge (\boldsymbol{M}_1 \wedge \boldsymbol{M}_2)$. The total cost associated to the computation of num is $3N$ multiplications but, as we explained above, we need only six transmissions. Computing den (9) has a negligible complexity since $m_{1,i} + m_{2,i} - m_{1,i} \cdot m_{2,i}$ has already been calculated for all i in (8). Moreover, we need a multiplication between *den* and t, and ℓ multiplications for the comparison, where ℓ is the number of bits necessary to represent a modulo p integer (see Section 3.1.2). Consequently, we need $3N + \ell + 1$ multiplications but only $2\ell + 7$ transmissions for the iris protocol.

4.4 Face authentication in the encrypted domain

As for the iris, we assume that face features have already been computed according to the protocol described in Section 3.2.2, obtaining a set of k real features $\boldsymbol{\Omega}_i$ that have been rounded (we have chosen $q = 1$, however different values can be chosen to increase accuracy) to represent them in $\mathbb{F}_p$ (in the following we do not indicate the rounding operator for simplicity).

Given the projection $\boldsymbol{\Omega}$ of the query face image, the face-based biometric authentication protocol must evaluate the ED as in (4), and check if the distance is lower than a threshold t. Considering that the square root cannot be evaluated efficiently in SPDZ, we instead compare the squared Euclidean distance (SED) against the squared threshold

$$\sum_{i=1}^{k} (\boldsymbol{\Omega}_i - \boldsymbol{\Omega}_{j,i})^2 < t^2. \quad (11)$$

In (11), $\boldsymbol{\Omega}_i$ indicates an element of the face $\boldsymbol{\Omega}$ and $\boldsymbol{\Omega}_{j,i}$ the ith element of the projection $\boldsymbol{\Omega}_j$. Moreover, as we did for the HD, we separate the square computation into two parts, so we need only one transmission to calculate SED.

Complexity: The computation of the SED requires the evaluation of k squares that can be parallelised, hence only one transmission is necessary. For the comparison, we need ℓ products, as in the iris authentication protocol. Considering that squares and products have similar complexity, the complexity of the protocol is given by $k + \ell$ products.

4.5 Fusion in the encrypted domain

We now describe our solution to implement the fusion protocol in the encrypted domain. As outlined in (6), we use a linear combination of the matching scores; to avoid performing divisions, we evaluate

$$\alpha \cdot \text{num} \cdot R + \beta \cdot \text{SED} \cdot \text{den} < T \cdot \text{den} \cdot R, \quad (12)$$

where num and den stand for the numerator and denominator of the iris HD, i in (6), while SED, R and T stand for squared Euclidean distance score, face maximum range and threshold.

The SPDZ framework does not allow the use of non-integer numbers, so α, β and T are scaled and approximated to integers in the interval [0, 10]. We chose this interval because it is accurate enough to obtain the same results achieved in the plain domain, and the resulting bit-length is small enough to make it possible to represent $\alpha \cdot \text{num} \cdot R + \beta \cdot \text{SED} \cdot \text{den}$ and $T \cdot \text{den} \cdot R$ in $\mathbb{Z}_p$.

Complexity: The previous formula requires three multiplications and six transmissions that cannot be run in parallel. Moreover, it needs ℓ multiplications for the comparison. In total, the linear fusion requires $\ell + 6$ multiplications and $2\ell + 12$ transmissions, plus the multiplications necessary to compute the HD and the SED. The total complexity of the full multimodal protocol is $3N + \ell + 6$ multiplications and k squares, while it requires only $2\ell + 19$ transmissions.

4.6 Protocol security

As outlined in Section 4.1, the client or the server could act maliciously to obtain private information of the other party. It is hence necessary that SEMBA provides security against at least an active party. When both the parties are malicious, any secure protocol rarely outputs some information useful to the parties. The whole protocol is developed within the SPDZ framework, and hence our protocol is secure in the UC model if at least one of the two parties is honest. In fact, according to [2], our SPDZ-based protocol is secure against $n - 1$ malicious adversaries, where $n = 2$ in our two-party computation scenario. The offline phase does not depend on the functionality evaluated and its security demonstration against active adversaries in the UC model is provided in [2].

The security demonstration of the online protocol is provided in the following theorem:

Theorem 1: **:** The online SPDZ implementation of SEMBA is computationally secure against any static adversary corrupting at most 1 party if p is exponential in the security parameter.

Proof: The proof follows the security demonstration of the online SPDZ protocol in [2]. We rely on the simulator $\mathcal{S}_{\text{ONLINE}}$ defined in [2] to work on top of the ideal multi-biometric authentication functionality $\mathcal{F}_{\text{ONLINE}}$, such that the adversary cannot distinguish among the simulator using the real function $\mathcal{F}_{\text{ONLINE}}$ and the real SPDZ-based implementation using multiplication triples generated offline. Input values broadcasted by both the simulator and honest players are uniform and it is not possible to distinguish among them. During execution, interaction with player is performed only during multiplication and squaring where partial opening reveals uniform values for both the honest parties and the simulator. Also MACs have similar distribution in both the protocol and the simulation. If the protocol does not abort due to a cheat detection, both the real and the simulated runs output the decision bit. In the simulation, the decision bit is obtained by a correct evaluation of the multi-biometric function on the inputs provided by the player. In real SPDZ-based implementation, the adversary can cheat in the MAC check with probability $2/p$. Hence, the probability that the adversary can distinguish the simulated environment from the real one is negligible if p is exponential. The adversary is not able to obtain the inputs of the honest player because if the protocol does not abort, he can observe only its input, the input shares received by the other party and the final result. To obtain the original inputs of the honest party, the

Table 3 Iriscode EER (%) without shifting, as a function of different values of r and θ

r	Angular resolution θ					
	100	120	140	160	180	200
4	8.19	6.43	4.37	3.34	3.31	3.10
6	6.88	5.05	3.01	2.45	2.71	3.01
8	6.13	4.42	2.69	2.19	2.58	4.36
10	6.31	4.03	2.64	2.44	2.54	3.92
12	5.96	4.10	2.56	2.14	2.59	3.71
14	5.71	3.85	2.54	2.17	2.58	3.27
16	5.49	3.79	2.32	2.13	2.51	3.31
18	5.71	3.61	2.46	2.31	2.41	3.18
20	5.77	3.74	2.20	2.08	2.41	3.13

Table 4 Eigenface EER (%) values, as a function of the number of projections

k	EER, %	k	EER, %
1	28.77	6	17.01
2	17.37	7	16.19
3	16.62	8	16.51
4	16.59	9	16.38
5	16.08	10	16.09

adversary should be able to solve the inequality in (6), which has $N_i + N_f$ unknown variables for the server and $N_i + N_f + 3$ for the client, where N_i and N_f are the number of features used to represent iris and face, respectively.□

5 System tuning

In this section, we present the results of the tests performed on plain data. We will use such results to choose the best parameters to build an efficient protocol working in the encrypted domain. Tests have been carried out on the 'CASIA-IrisV1' database for irises and 'CASIA-FaceV5 part 1' database for faces, both collected by the Chinese Academy of Sciences' Institute of Automation (CASIA) [60, 61].

The CASIA-IrisV1 database for irises [60] contains 756 grey-scale eye images with 108 unique irises (or classes) and 7 images for each of them. As in [13], we used a subset of the database for the tests, retaining only those images in which the algorithm has well-separated iris region from sclera and pupil. The resulting database contains 625 eye images.

The CASIA-FaceV5 Databases for faces part 1 [61] contains 500 face images of 100 subjects. The face images are captured using Logitech USB camera in one session. All face images are 16 bit colour BMP files and the image resolution is 640×480 pixels.

We implemented and tested our SPDZ-based iris and multi-biometric protocols on a desktop equipped with 8 GB RAM processor Intel Core i3 CPU 550 @ 3.20 GHz Quad-Core running Ubuntu 14.04 LTS (64 bit) operative system. We developed the test using C++ language with GMP free library for arbitrary precision arithmetic, operating on signed integers, rational numbers and floating-point numbers.

To implement the SPDZ protocol, we chose the 46 bit prime number $p = 67280421310721$, which is big enough to allow all the needed modular operations and comparisons, and guarantee the security of the protocol. Is a matter of fact, in iriscode authentication, both num and den are integer values lower than N and hence can be correctly represented in $\mathbb{F}_p$, as well as $t \cdot \text{den}$ that need few bits more. Similarly, in face recognition protocol, eigenfaces are represented with 8 bits and hence the upperbound for SED is $R = (2^8)^2 * k$, where the maximum k is 10 eigenfaces. Hence in our experiments R is lower or equal to 655,360 and it can be represented in $\mathbb{F}_p$. Finally, in multi-biometrics authentication we assume that α, β and T are scaled by multiplying them with the factor 100, and R is equal to the maximum SED. Again, in the worst case $R = 655,360$ when $= 100$, hence the maximum value that the left side of (12) can assume is $100 \times 6400 \times 655,360 + 100 \times 655,360 \times 6400 = 838860800000$, which can be correctly represented in $\mathbb{F}_p$. We can observe that such values are also lower than $p/2$, allowing efficient evaluation of the comparison, as described in Section 3.1.2.

Server and client run on the same computer, and we used a socket to simulate the transmission channel. We assume that all the communications are carried on secure channels (Section 4.1), in order to prevent eavesdroppers and man-in-the-middle attacks.

We assume that in the precomputation phase, before the online iris protocol starts, at least $3N + \ell + 1$ multiplication triples have been generated, one for each multiplication in the protocol, along with ℓ share bits. For the fusion protocol we need $3N + \ell + 6$ multiplication tuples, k square tuples and ℓ share bits.

5.1 Parameter optimisation

We performed tests on plain data, running the authentication protocol on each single biometric and then by fusing the scores obtained on eigenfaces and iriscodes.

Iris: In order to test the iris authentication protocol, we have chosen a radial resolution r ranging from 4 to 20 and an angular resolution θ between 100 and 200 (Table 3). As said above, we tested the protocol on 625 eye images and each one has been compared with all the others. To perform the tests in the plain domain, we used the Matlab code provided by L. Masek (iris recognition source code [62]) as part of his work [13]. As we can see from Table 3, the best accuracy is achieved by letting the angular resolution be equal to 160 angles and radial resolution equal to 20 corresponding to an iris feature vector of length 6400 bits.

To reduce the EER, Masek [13] shifts n times the iris templates keeping the lowest HD score. In SPDZ, this operation is computationally very expensive, so we could not afford it.

Face: We have implemented the eigenface protocol by using the Open Source Computer Video (openCV) library (http://opencv.org/about.html) and Matlab. Face images are 640×480 pixel and we transformed them in 256 bit images. The protocol has been tested on 500 images. We used the algorithm provided in the openCV library to build k eigenfaces with $k = 1 \ldots 10$. Each image is thus represented by a projection vector of length k. Each projection element is a 16-bit integer and the SED has been calculated by using Matlab. We observed that the use of more than five projections does not provide any significant improvement (see Table 4).

Multimodal: We have evaluated the efficiency of the fusion protocol in the plain domain, by fusing the outcomes of face and iris sub-algorithms. From Table 3, we have chosen some relevant iris configurations, based on the achieved EER or number of features. First of all, to better compare with the best iris result, we chose $r = 20$ and $\theta = 160$ resulting in $N = 6400$, then for each θ, we looked for the best accuracy under 4%, and finally we chose those configurations with EER similar to the previous ones but less features. Moreover, we varied α in the interval [0, 1] and the number of eigenfaces k from 1 to 10. Table 5 shows the EER for each N and k.

As shown in Table 5, the same accuracy of the 6400 stand-alone iris protocol (2.08%) can be reached with many different multi-

Table 5 EER of the multimodal biometric authentication protocol

Iris parameters			Iris	Number of eigenfaces (k)									
N	r	θ		1	2	3	4	5	6	7	8	9	10
6400	20	160	2.08	1.17	**1.15**	1.02	1.25	1.25	1.24	1.31	1.37	1.4	1.41
5760	16	180	2.51	1.26	**0.98**	1.01	1.22	1.38	1.36	1.43	1.47	1.49	1.50
5600	20	140	2.20	1.20	1.08	1.19	1.18	1.34	1.28	1.36	1.38	1.39	1.40
4800	20	120	3.74	1.90	1.97	1.65	1.98	2.04	2.15	2.11	2.17	2.2	2.21
3840	12	160	2.14	1.84	1.52	1.50	1.45	1.63	1.74	1.76	1.77	1.78	1.78
3600	10	180	2.54	1.36	1.23	**0.97**	1.65	1.82	1.99	2.07	2.15	2.17	2.19
3360	12	140	2.56	1.51	1.32	1.38	1.31	1.56	1.61	1.58	1.63	1.67	1.69
2560	8	160	2.19	1.50	1.24	1.19	1.15	1.39	1.49	1.59	1.6	1.61	1.62
2400	6	200	3.01	2.01	1.83	1.89	2.13	2.37	2.56	2.66	2.7	2.72	2.73
2160	6	180	2.71	1.92	1.74	1.82	1.98	2.04	2.09	2.07	2.13	2.16	2.18
1920	6	160	2.45	1.47	1.42	1.43	1.57	1.66	1.95	1.92	1.95	1.96	1.97
1600	4	200	3.10	**2.01**	**1.87**	1.85	2.41	2.37	2.56	2.67	2.69	2.71	2.71
1280	4	160	3.34	2.29	1.89	2.22	2.26	2.51	2.80	2.80	2.92	2.98	3.01

The first three columns show iris's parameters: feature's number (N), radial resolution (r) and angular resolution θ. The fourth column shows the EER of the iris authentication system (%). All the others columns contain the EER's obtained by fusing an iris template of length N and a face template with $k \in \{1\ldots10\}$ eigenfaces. We highlighted in bold the configurations that we have selected for the tests under encryption.

Table 6 Complexity summary

	Multiplications	Squares	Transmissions
iris	$3N + \ell + 1$	0	$2\ell + 7$
face	ℓ	k	$2\ell + 1$
multimodal	$3N + \ell + 6$	k	$2\ell + 19$

We underline that transmission number depends only on p's bitlength ℓ.

Table 7 Communication complexity for the iris and multimodal protocols

Iris	Bandwidth, kB			Face
N	Iris	Multimodal	Overhead	k
1600	53.24	53.30	0.06	1
3600	119.16	119.23	0.07	3
5760	190.35	190.42	0.07	2
6400	211.44	211.51	0.07	2

It is important to notice that adding few eigenfaces increases the bandwidth by a few bytes only.

biometric configurations, e.g. by using $N = 3600$ and $k = 7$ or even by using only 1600 iris features and $k = 1$. For the tests in the encrypted domain, between the two configurations with the same accuracy, we chose the last one, since it has lower bandwidth and computational complexity (see Tables 6 and 7). We can also notice that keeping $N = 1600$, but using two features for face representation, we can lower both accuracy and complexity. Generally, by using two eigenfaces, the best possible accuracy is provided with 5760 iris features. However, the same performance is obtained also by the combination of 3600 iris features and three face features. For this reason, we tested several configurations in the encrypted domain, as summarised in Table 8.

5.2 Validation with other datasets

We have also validated the results of our analysis on the IIT Delhi Iris database [63] and the ORL Database of Faces [64]. The IIT Delhi Iris database is composed by ten eye images (five for each eye) of 224 individuals. In the ORL Database of Faces there are ten different images of 40 distinct subjects. The size of each image is 92×112 pixels, with 256 grey levels per pixel.

By relying only on iriscode, we still obtain the lowest EER with 6400 features ($r = 20$ and $\theta = 160$), where we observed EER = 7.52%. This result is indeed higher than the one obtained with the CASIA dataset. We observed some segmentation problems that affected classification accuracy. However, optimal segmentation is out of the scope of our paper and we have overlooked it to focus on the advantages provided by using multi-biometrics in privacy preserving authentication. Again we can distinguish two goals: (i) if we desire higher accuracy we can combine a 6400-bit iriscode with one eigenface, decreasing the EER to 3.46%; (ii) if we wish to decrease protocol complexity, we can rely on 1280-bit iriscodes ($r = 4$ and $\theta = 160$) and 1 eigenface, which guarantees an EER = 7.57%, really close to the original iriscode-based authentication EER.

6 Complexity of the SPDZ protocol

We evaluated the computational complexity of the SPDZ protocol (Section 4), by using the parameters chosen in the previous section (see Tables 3 and 8). We here focus on the parameter configuration identified with the CASIA-IrisV1 and CASIA-FaceV5 datasets. However, we underline that in our validation tests in Section 5.2, we obtained similar configurations. Execution times are heavily affected by the number of multiplications. As we said in Section 4.3, when possible, we performed a single transmission, by packing data. To calculate the execution time, reported in Table 9, we used the *clock* function, measuring the CPU time of the process.

We assume that the preprocessing phase has already been completed, therefore we assume to have generated enough multiplication and square tuples to complete the authentication protocols (see Table 10) and at least 46 shares bits for comparison. Since the number of bits depends only on p's bit length, the number of share bits remains constant in all the protocols, while the number of multiplication and square tuples depends on the parameters set.

In SEMBA, the number of transmission rounds depends only on the bitlength ℓ of the prime number p and not on the feature configuration, as it can be seen from Table 6. On the contrary, the amount of data transmitted by each party also depends on the number of features used in the protocol. In fact, the iris authentication protocol has a bandwidth of $(6N + 2\ell + 2) \cdot \ell$ bits, while the multimodal protocol bandwidth is $\ell \cdot (6N + k + 2\ell + 12)$ bits. Since the complexity of the iris protocol is much higher than that of the face-based authentication protocol, the overhead introduced by the multimodal biometric authentication is of few bytes, as it can be seen from Table 7. For this reason, the communication complexity remains almost constant switching from the iris to the multimodal protocol.

The main goal of our work was exploiting multimodality to reduce complexity while maintaining the same accuracy of the iris-based protocol. Moreover, our analysis shows that the multimodal protocol can also be used to lower the EER without a significant loss in terms of complexity. In the following, we discuss both cases.

Improved efficiency: The running time of the stand-alone iris authentication protocol ranges from 0.03 s for 1600 bits, up to 0.12 s for a 6400 bit-long template in the malicious setting (see Table 9),

Table 8 EER of iris and multimodal biometric authentication protocols for different settings

Iris	EER		Face	Fusion parameters	
N	Iris, %	Fusion, %	k	α	t
1600	3.10	2.01	1	0.80	0.35
1600	3.10	1.87	2	0.55	0.25
3600	2.54	0.97	3	0.55	0.25
5760	2.51	0.98	2	0.80	0.35
6400	2.08	1.15	2	0.80	0.35

α, t, respectively, stand for fusion coefficient and threshold.

Table 9 Iris protocol time in SPDZ system

Iris	CPU time		Face
N	Iris, s	Multimodal, s	k
1600	0.029	0.030	1
1600		0.030	2
3600	0.048	0.049	3
5760	0.11	0.109	2
6400	0.12	0.120	2

Table 10 Number of multiplications and square triples needed

Iris	Multiplicative tuples		Squares tuples
N	Iris	Fusion	k
1600	4847	4852	1
1600	4847	4852	2
3600	10,847	10,852	3
5760	17,327	17,332	2
6400	19,247	19,252	2

while Luo *et al.* protocol [26] with masks needs 2.5 s for 9600 bits and 0.56 s for 2048 bits in the semi-honest setting. Moreover from Tables 8 and 9, it is evident that SEMBA can provide the same accuracy of the best stand-alone iris protocol, but with lower execution time and computational complexity. As a matter of fact, the best EER for the stand-alone iris protocol is 2.08% for 6400 features corresponding to 19,246 multiplications (Table 6) in 0.12 s, while in the fusion configuration for 1600 iris features and 1 eigenface feature, we need only 8744 multiplications (see Table 6, where we consider squares as multiplications) to obtain an EER equal to 2.01% in about 30 ms. On the contrary, the number of required transmissions increases from $2\ell + 7$ to $2\ell + 19$ (Table 6), but it depends only on the bit length of p.

Improved accuracy: As an alternative to improve the computational complexity, the use of two biometrics instead of one can be exploited to achieve a higher accuracy, at the cost of a slight increase of complexity with respect to the iriscode protocol. In fact, as shown in Table 6, complexity depends heavily on the number of iris features, however by adding two eigenfaces it is possible to decrease the EER rate, while the number of multiplications increases only from $3N + \ell + 1$ to $3N + \ell + 6 + k = 3N + \ell + 8$ (as usual we consider squaring to be equivalent to multiplication). More generally, when we move to multimodal authentication, the total CPU time slightly increases with respect to the unimodal iris protocol, but the EER always decreases; by adding one more eigenface ($k = 2$) to the 1600 iris feature configuration considered above, we can have a better EER (1.87%) with the same time complexity (30 ms). For the case of 5760 bit long iris template, the EER passes from 2.1% for the unimodal authentication to 0.98% for the bimodal case with $k = 2$ (Table 8). Finally, keeping 0.98% as target accuracy, we highlight that we can reduce N to 3600 at the cost of an additional feature in the face representation ($k = 3$). In this case, computational complexity goes from 36,926 to 19,596 multiplications and time complexity decreases from 0.109 to 0.05 s (Tables 7 and 9).

7 Comparison with the state of the art

SEMBA improves that state of the art by proposing for the first time a multi-biometric protocol based on secure multi-party computation, also secure against active adversaries. Our proposal is based on the fusion of iriscode and eigenface at the score level. Iriscode has been used in literature in [18, 25–27] for privacy preserving iris recognition. Luo *et al.* [25] present one of the first protocols for iris authentication and their rough protocol requires around 480 s. Blanton and Gasti [18] have proposed a protocol that, thanks to several optimisations, requires around 240 ms for the online part of iris identification. Both the previous works focus on the cryptographic aspects of the implementation, overlooking the accuracy. Bringer *et al.* [27] proposed a two-step identification protocol that, according the parameters configuration, provides a false rejection rate ranging between 21 and 3.1%. The protocol requires a runtime of around 2.6 s per candidate. Luo *et al.* [26] presented an iris authentication protocol having an EER of around 1.45% and an online runtime of 573 ms in the worst case. In our experiments we have reached similar accuracy and an online runtime ranging between 30 and 120 ms, improving all the iris recognition protocols proposed so far. Moreover, we underline that SEMBA is secure against malicious parties, providing higher security level. Such significant improvement is indeed due to the excellent performances of the SPDZ protocol, but also to our smart multi-biometrics feature optimisation.

The only MPC-based privacy preserving multi-biometric scheme provided in literature is the system presented by Gomez-Barrero *et al.* [41], which relies on signature and fingerprint and ensures a good accuracy (EER = 0.12%). It is based on fully homorphic encryption and has a computational cost (one decryption on the server side and no encryptions at verification time) lower than our protocol with a required time for a single comparison of about 0.5 ms. However, a drawback of the system is that final comparison is carried out on plain data by the server, thus introducing a breach into the security of the system. On the contrary, SEMBA also implements the final comparison step within the SPDZ framework, to prevent any security loss, even if this choice has a non-negligible cost in terms of complexity (see Section 6). As a further difference, in [41] an ED computation (in

case of two-modal system) requires $M \cdot F + 2$ exponentiations, where M is the number of enrolled samples for each subject and F the feature's total number considering all the modalities. In our work, instead, thanks to the SPDZ system and to the possibility of using integer numbers, we need only k (the length of the feature vector) squares, one of our most expensive operations. Last but not least, thanks to the SPDZ system, SEMBA is secure under the assumption that one between the server and the client acts maliciously, while Gomez-Barrero *et al.* assume the semi-honest model.

8 Conclusions

In this paper, we have proposed SEMBA, a multimodal authentication protocol based on SPDZ [1, 2]. The protocol is secure against a malicious party. We have shown that by using a multi-modal system it is possible to improve the efficiency of the recognition process in terms of number of multiplications and evaluation time, without any loss of accuracy. In the same way, it is also possible to improve accuracy at the cost of a negligible increase of complexity. As an additional contribution, we adapted the iris and face authentication protocols to work in the SPDZ setting. A further additional complexity reduction is achieved by resorting to packed transmission of encrypted data involved in the secure multiplication protocol.

As future work, we plan to extend our approach to even more biometric traits, like fingerprints, behavioural biometric and many others. Another interesting research direction could be to look for different algorithms and more efficient fusion rules to merge the match scores. Due to the recently widespread use of biometric authentication on laptops and smartphones, it would also be interesting to evaluate the possibility to apply SEMBA to mobile devices. In those devices, fingerprint or face readers and extractors are often already in place, but since their only scope is to confirm owner identification, templates are matched in plain domain. Readers on mobile devices could also be used to access remote services through biometric authentication. In this scenario, SEMBA could be used to enhance security during match computation.

9 Acknowledgment

This work has been partially supported by a grant of La Sapienza University of Rome Bando Ricerca 2017 within the project *Security and Privacy of Biometrics for Mobile Authentication (SPoB-MA)* – Protocol n. RM11715C7878B045.

10 References

[1] Damgård, I., Pastro, V., Smart, N., *et al.*: 'Multiparty computation from somewhat homomorphic encryption'. Advances in Cryptology–CRYPTO 2012, California, USA, 2012, pp. 643–662

[2] Damgård, I., Keller, M., Larraia, E., *et al.*: 'Practical covertly secure MPC for dishonest majority–or: breaking the SPDZ limits'. European Symp. on Research in Computer Security, Egham, UK, 2013, pp. 1–18

[3] Voigt, P., Von dem Bussche, A.: 'The EU general data protection regulation (GDPR)', in '*A practical guide*' (Springer International Publishing, Cham, 2017, 1st edn.), pp. 1–249

[4] Evans, N., Marcel, S., Ross, A., *et al.*: 'Biometrics security and privacy protection [from the guest editors]', *IEEE Signal Process. Mag.*, 2015, **32**, (5), pp. 17–18

[5] Bringer, J., Chabanne, H., Patey, A.: 'Privacy-preserving biometric identification using secure multiparty computation: an overview and recent trends', *IEEE Signal Process. Mag.*, 2013, **30**, (2), pp. 42–52

[6] Barni, M., Droandi, G., Lazzeretti, R.: 'Privacy protection in biometric-based recognition systems: a marriage between cryptography and signal processing', *IEEE Signal Process. Mag.*, 2015, **32**, (5), pp. 66–76

[7] Michael, O.R.: 'How to exchange secrets by oblivious transfer'. Technical Report TR-81, Aiken Computation Laboratory, Harvard University, 1981

[8] Yao, A.C.: 'How to generate and exchange secrets'. Annual IEEE Symp. on Foundations of Computer Science, Toronto, Canada, 1986, pp. 162–167

[9] Paillier, P.: 'Public-key cryptosystems based on composite degree residuosity classes'. Advances in Cryptology – EUROCRYPT, Prague, Czech Republic, 1999, pp. 223–238

[10] Gentry, C., Halevi, S.: 'Implementing gentry's fully-homomorphic encryption scheme'. Advances in Cryptology–EUROCRYPT 2011, Tallinn, Estonia, 2011, pp. 129–148

[11] Goldreich, O.: 'Secure multi-party computation'. Manuscript. Preliminary Version, 1998, pp. 86–97

[12] Ross, A., Nandakumar, K., Jain, A.K.: 'Introduction to multibiometrics', in '*Handbook of biometrics*', (Springer, USA, 2008), pp. 271–292

[13] Masek, L.: '*Recognition of human iris patterns for biometric identification*', vol. **2** (The University of Western Australia, Australia, 2003)

[14] ISO/IEC TR 24722:2015: '*Information technology – biometrics – multimodal and other multibiometric fusion*' (International Organization for Standardization, Switzerland, 2015). [Online]. Available at: https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:24722:ed-2:v1:en

[15] Pisa, P.S., Abdalla, M., Duarte, O.C.M.B.: 'Somewhat homomorphic encryption scheme for arithmetic operations on large integers'. Global Information Infrastructure and Networking Symp. (GIIS), Choroni, Venezuela, 2012, pp. 1–8

[16] Shamir, A.: 'How to share a secret', *Commun. ACM*, 1979, **22**, (11), pp. 612–613

[17] Lazzeretti, R., Barni, M.: 'Private computing with garbled circuits [applications corner]', *IEEE Signal Process. Mag.*, 2013, **30**, (2), pp. 123–127

[18] Blanton, M., Gasti, P.: 'Secure and efficient protocols for iris and fingerprint identification'. European Symp. on Research in Computer Security – ESORICS, Leuven, Belgium, 2011, pp. 190–209

[19] Turk, M.A., Pentland, A.P.: 'Face recognition using eigenfaces'. Conf. on Computer Vision and Pattern Recognition – CVPR, Hawaii, USA, 1991, pp. 586–591

[20] Daugman, J.: 'How iris recognition works', *IEEE Trans. Circuits Syst. Video Technol.*, 2004, **14**, (1), pp. 21–30

[21] Erkin, Z., Franz, M., Guajardo, J., *et al.*: 'Privacy-preserving face recognition', in '*Privacy enhancing technologies*', (Springer, Germany, 2009), pp. 235–253

[22] Sadeghi, A.-R., Schneider, T., Wehrenberg, I.: 'Efficient privacy-preserving face recognition'. Information, Security and Cryptology–ICISC 2009, Seoul, Korea, 2010, pp. 229–244

[23] Osadchy, M., Pinkas, B., Jarrous, A., *et al.*: 'Scifi-a system for secure face identification'. IEEE Symp. on Security and Privacy (SP), California, USA, 2010, pp. 239–254

[24] Troncoso-Pastoriza, J.R., Gonzalez-Jimenez, D., Perez-Gonzalez, F.: 'Fully private noninteractive face verification', *IEEE Trans. Forensics Sec.*, 2013, **8**, (7), pp. 1101–1114

[25] Luo, Y., Sen-ching, S.C., Ye, S.: 'Anonymous biometric access control based on homomorphic encryption'. Int. Conf. on Multimedia and Expo – ICME 2009, Cancun, Mexico, 2009, pp. 1046–1049

[26] Luo, Y., Cheung, S.-C.S., Pignata, T., *et al.*: 'An efficient protocol for private iris-code matching by means of garbled circuits'. Int. Conf. on Image Processing – ICIP. IEEE, Florida, USA, 2012, pp. 2653–2656

[27] Bringer, J., Favre, M., Chabanne, H., *et al.*: 'Faster secure computation for biometric identification using filtering'. IAPR Int. Conf. on Biometrics – ICB, New Delhi, India, 2012, pp. 257–264

[28] Droandi, G.: 'Non-interactive privacy preserving protocol for biometric recognition based on somewhat homomorphic encryption'. Proc. of the 14th European Conf. on Cyber Warfare and Security 2015 (ECCWS). Academic Conf.s Limited, London, UK, 2015, p. 355

[29] Droandi, G., Lazzeretti, R.: 'She based non interactive privacy preserving biometric authentication protocols'. IEEE 9th Int. Symp. on Intelligent Signal Processing (WISP), Siena, Italy, 2015, pp. 1–6

[30] Simoens, K., Bringer, J., Chabanne, H., *et al.*: 'A framework for analyzing template security and privacy in biometric authentication systems', *IEEE Trans. Inf. Forensics Sec.*, 2012, **7**, (2), pp. 833–841

[31] Kantarcioglu, M., Kardes, O.: 'Privacy-preserving data mining in the malicious model', *Int. J. Inf. Comput. Secur.*, 2008, **2**, (4), pp. 353–375

[32] Abidin, A.: 'On privacy-preserving biometric authentication'. Int. Conf. on Information Security and Cryptology – Inscrypt, Seoul, South Korea, 2016, pp. 169–186

[33] Pathak, M.A., Raj, B.: 'Privacy-preserving speaker verification and identification using Gaussian mixture models', *IEEE Trans. Audio, Speech, Lang. Process.*, 2013, **21**, (2), pp. 397–406

[34] Kiraz, M., Schoenmakers, B.: 'A protocol issue for the malicious case of Yao's garbled circuit construction'. Symp. on Information Theory in the Benelux, Brussels, Belgium, 2006, pp. 283–290

[35] Lindell, Y., Pinkas, B., Smart, N.P.: 'Implementing two-party computation efficiently with security against malicious adversaries'. Int. Conf. on Security and Cryptography for Networks, Porto, Portugal, 2008, pp. 2–20

[36] Pinkas, B., Schneider, T., Smart, N.P., *et al.*: 'Secure two-party computation is practical', in '*Asiacrypt*', vol. **9** (Springer, Germany, 2009), pp. 250–267

[37] Nielsen, J.B., Nordholt, P.S., Orlandi, C., *et al.*: 'A new approach to practical active-secure two-party computation', in '*CRYPTO*', vol. **7417** (Springer, Germany, 2012), pp. 681–700

[38] Lindell, Y.: 'Fast cut-and-choose-based protocols for malicious and covert adversaries', *J. Cryptol.*, 2016, **29**, (2), pp. 456–490

[39] Gasti, P., Šeděnka, J., Yang, Q., *et al.*: 'Secure, fast, and energy-efficient outsourced authentication for smartphones', *IEEE Trans. Inf. Forensics Sec.*, 2016, **11**, (11), pp. 2556–2571

[40] Ross, A.A., Nandakumar, K., Jain, A.: '*Handbook of multibiometrics*', vol. **6** (Springer Science & Business Media, USA, 2006)

[41] Gomez-Barrero, M., Maiorana, E., Galbally, J., *et al.*: 'Multibiometric template protection based on homomorphic encryption', *Pattern Recognit.*, 2017, **67**, pp. 149–163

[42] Sowkarthika, S., Radha, N.: 'Securing iris and fingerprint templates using fuzzy vault and symmetric algorithm'. Int. Conf. on Intelligent Systems and Control (ISCO), Coimbatore, India, 2013, pp. 189–193

[43] Nandakumar, K., Jain, A.K., Pankanti, S.: 'Fingerprint-based fuzzy vault: implementation and performance', *IEEE Trans. Inf. Forensics Sec.*, 2007, **2**, (4), pp. 744–757

[44] Kholmatov, A., Yanikoglu, B.: 'Realization of correlation attack against the fuzzy vault scheme', in '*Security, forensics, steganography, and*

watermarking of multimedia contents X', vol. **6819** (International Society for Optics and Photonics, USA, 2008), p. 68190O
[45] Scheirer, W.J., Boult, T.E.: 'Cracking fuzzy vaults and biometric encryption'. Biometrics Symp., Baltimore, USA, 2007, pp. 1–6
[46] Sutcu, Y., Li, Q., Memon, N.: 'Secure biometric templates from fingerprint-face features'. IEEE Conf. on Computer Vision and Pattern Recognition, Minneapolis, USA, 2007, pp. 1–6
[47] Kelkboom, E., Zhou, X., Breebaart, J.*, et al.*: 'Multialgorithm fusion with template protection'. IEEE Int. Conf. on Biometrics: Theory, Applications, and Systems (BTAS), Washington, USA, 2009, pp. 1–8
[48] Rathge, C., Uhl, A., Wild, P.: 'Reliability-balanced feature level fusion for fuzzy commitment scheme'. Int. Joint Conf. on Biometrics (IJCB), Washington, USA, 2011, pp. 1–7
[49] Ignatenko, T., Willems, F.M.: 'Information leakage in fuzzy commitment schemes', *IEEE Trans. Inf. Forensics Sec.*, 2010, **5**, (2), pp. 337–348
[50] Failla, P., Sutcu, Y., Barni, M.: 'Esketch: a privacy-preserving fuzzy commitment scheme for authentication using encrypted biometrics'. Proc. of the 12th ACM Workshop on Multimedia and Security, Rome, Italy, 2010, pp. 241–246
[51] Gumaei, A., Sammouda, R., Al-Salman, A.M.S.*, et al.*: 'Anti-spoofing cloud-based multi-spectral biometric identification system for enterprise security and privacy-preservation', *J. Parallel Distrib. Comput.*, 2019, **124**, pp. 27–40
[52] Bogdanov, D., Laur, S., Willemson, J.: 'Sharemind: a framework for fast privacy-preserving computations'. European Symp. on Research in Computer Security, Malaga, Spain, 2008, pp. 192–206
[53] Demmler, D., Schneider, T., Zohner, M.: 'ABY-a framework for efficient mixed-protocol secure two-party computation'. Network and Distributed System Security Symp. (NDSS), California, USA, 2015
[54] Beerliová-Trubíniová, Z., Hirt, M.: 'Perfectly-secure MPC with linear communication complexity'. Theory of Cryptography Conf., New York, USA, 2008, pp. 213–230
[55] Veugen, T., de Haan, R., Cramer, R.*, et al.*: 'A framework for secure computations with two non-colluding servers and multiple clients, applied to recommendations', *IEEE Trans. Inf. Forensics Sec.*, 2015, **10**, (3), pp. 445–457
[56] Connaughton, R., Bowyer, K.W., Flynn, P.J.: 'Fusion of face and iris biometrics', in '*Handbook of Iris recognition*' (Springer, UK, 2013), pp. 219–237
[57] Aliasgari, M., Blanton, M., Zhang, Y.*, et al.*: 'Secure computation on floating point numbers'. Network and Distributed System Security Symp. (NDSS), California, USA, 2013
[58] Kamm, L., Willemson, J.: 'Secure floating point arithmetic and private satellite collision analysis', *Int. J. Inf. Secur.*, 2015, **14**, (6), pp. 531–548
[59] Pullonen, P., Siim, S.: 'Combining secret sharing and garbled circuits for efficient private IEEE 754 floating-point computations'. Int. Conf. on Financial Cryptography and Data Security, San Juan, Puerto Rico, 2015, pp. 172–183
[60] C. A. of Sciences' Institute of Automation: 'Casia-Irisv1'. [Online]. Available at: http://biometrics.idealtest.org/
[61] C. A. of Sciences Institute of Automation: 'Casia-Facev5'. [Online]. Available at: http://biometrics.idealtest.org/
[62] Libor Masek, P.K.: '*Matlab source code for a biometric identification system based on iris patterns*' (The School of Computer Science and Software Engineering, The University of Western Australia, Australia, 2003)
[63] Kumar, A., Passi, A.: 'Comparison and combination of iris matchers for reliable personal authentication', *Pattern Recognit.*, 2010, **43**, (3), pp. 1016–1026
[64] Samaria, F.S., Harter, A.C.: 'Parameterisation of a stochastic model for human face identification'. Proc. of 1994 IEEE Workshop on Applications of Computer Vision, Florida, USA, 1994, pp. 138–142