# Hill-Climbing Attacks on Multi-Biometrics Recognition Systems

Emanuele Maiorana, *Member, IEEE*, Gabriel Emile Hine, and Patrizio Campisi, *Senior Member, IEEE*

***Abstract*—Biometric recognition systems, despite the advantages provided with respect to traditional authentication methods, have some peculiar weaknesses which may allow an attacker being falsely recognized or accessing users' personal data. Among such vulnerabilities, in this paper we speculate on the hill-climbing attack, that is the possibility for an attacker to exploit the scores produced by the matcher with the goal of generating synthetic biometric data which could allow a false acceptance. More in detail, we focus on multi-biometrics systems and investigate about the robustness of different system architectures, both parallel and serial fusion schemes, against the hill-climbing attack. Non-uniform quantization is also evaluated as a possible countermeasure for limiting the effectiveness of the considered attacks in terms of recognition success rate and average number of required attempts without affecting the recognition performance.**

***Index Terms*—Hill-Climbing Attacks, Multi-Biometrics Recognition Systems, Biometrics Protection, Electroencephalography, On-line Signature, Fingerprint**

## I. Introduction

Biometrics are becoming more and more popular as preferred identifiers to be used in automatic people recognition systems, mainly thanks to the potential higher user's comfort, convenience, and security they can provide with respect to traditional recognition techniques. Nonetheless, biometric systems posses peculiar weaknesses which may affect their security, and put in peril the users' privacy [1]. Specifically, fake synthetic biometrics can be presented to the acquisition sensor, while previously eavesdropped biometrics can be replayed to the feature extractor module. This latter can be compromised to produce templates preset by the attacker in order to fool the system. Synthetic templates can be directly fed to the matcher module, which is also vulnerable to attacks overriding its output to produce an arbitrarily high matching score. The threshold of the decision module can be modified according to the attacker's needs. Attacks can also be perpetrated against the database containing the users' templates, with the purpose of adding a new template, modifying or removing an existing one, or acquiring relevant information about the enrolled users [2]. Eventually, the channels connecting the different modules can be attacked to intercept and alter the transmitted information.

It is therefore evident that, besides analyzing biometric recognition systems in terms of achievable recognition rates, also their security against potential attacks needs be properly evaluated. Within this framework, the present paper investigates the resilience of different architectures implementing multi-biometrics systems [3] against hill-climbing attacks [4]. This threat is based on the assumption that the scores produced by the matcher can be accessed by an attacker and exploited for driving the generation of either synthetic biometric samples used as inputs of the feature extractor module or synthetic biometric templates used as inputs to the matcher. The hill-climbing attack is performed iteratively, each time updating the data generated at a given step trying to improve the resulting matching output, till a successful recognition is achieved. It is worth remarking that, to carry out this strategy, the attacker does not need any specific *a priori* knowledge about the biometrics of the targeted user. In fact, differently from a spoofing attack, only statistical information about the overall distributions of the considered features needs to be available. Our analysis focuses on multi-biometrics systems, which in recent years gained increasing popularity for practical applications, mainly due to the increased recognition performance and enhanced level of security they can provide. Actually, multi-biometrics systems have been recently analyzed also in terms of their resistance against specific menaces like spoofing attacks [5]. The increased security provided by template protection schemes applied to multi-biometrics systems is discussed for instance in [6], where a biometric cryptosystem using a fuzzy vault with fingerprint and iris templates is presented.

However, an analysis on the robustness of multi-biometrics systems against hill-climbing strategies is still missing in literature. In this paper we try to fill this gap, considering multi-biometrics systems based on both parallel and serial fusion schemes. Their performance are analyzed in terms of both the achievable recognition rates and the security provided against several hill-climbing attacks, and compared with those associated to uni-modal biometric systems. Moreover, non-uniform quantization is here proposed as a novel countermeasure to limit the effectiveness of hill-climbing strategies when applied to the multi-biometrics architectures here considered, without affecting the achievable recognition accuracy.

The paper is organized as follows. A brief review on the state of the art on hill-climbing attacks is given in Section II, while the general attack strategies employed in this paper are introduced in Section III. The architectures considered for implementing multi-biometrics recognition systems, including both parallel as well as serial schemes, are described in Section IV. Countermeasures against hill-climbing attacks are analyzed in Section V, where non-uniform score quantization is proposed to counteract the employed attack strategies. The performed experimental tests, assessing the robustness of the considered fusion schemes against hill-climbing attacks, are then reported in Section VI. Eventually, conclusions are drawn in Section VII.

The authors are with the Section of Applied Electronics, Department of Engineering, Roma Tre University, Via V. Volterra 62, 00146 Roma, Italy (e-mail: emanuele.maiorana@uniroma3.it, gab.hine@stud.uniroma3.it, patrizio.campisi@uniroma3.it)

## II. State Of The Art On Hill-Climbing Attacks

Hill-climbing attacks are performed by iteratively submitting synthetic representations of the attacked user's biometrics until successful recognition is achieved. At each step the employed data are modified according to the results of previous attempts, expressed in terms of matching scores, assumed to be known to the attacker, with the aim of improving the resulting matching output. No specific information regarding the target user needs to be known *a priori* in order to perform this strategy: only statistical information about the characteristics of the employed templates are in fact needed. Such attacks can be perpetrated both at the feature extraction module and at the matcher module. When considering the former scenario, hill-climbing attacks generate data resembling the originally acquired biometrics. Such approach is for instance proposed in [7], where artificial raw on-line signatures are created and employed as forgeries. However, these methods are typically highly dependant on the selected biometrics and on the acquisition modality, being thus hard their generalization for different applications.

In alternative, hill-climbing attacks can be also performed by targeting the matcher module, with the aim of generating synthetic templates allowing successful recognition. Specifically, binary iris templates based on the Daugman's rubber-sheet model are synthetically generated and pixel-wise modified until successful recognition in [8]. A binary genetic algorithm is evaluated in [9] for the same purpose. Fingerprint templates represented in terms of minutiae location and angle information are analyzed in [4], by defining attacks where a random template composed by a set of minutiae points is perturbed with different possible modifications such as displacements or erasures. Only the changes leading to a score improvement are kept during the iterations. The initial conditions of the algorithms as well as the best possible modifications are further analyzed in [10]. Also in this case, all the described approaches are designed for attacking a specific biometric representation and cannot be generalized.

Conversely, several approaches in the literature are designed to attack generic biometric recognition systems with the unique requirement of using a fixed-length parametric representation for the employed biometric templates. This is the case of the attacks based on a Bayesian method performed against on-line signature templates in [11], and of the application of the Nelder-Mead algorithm to face biometrics in [12] and to on-line signatures in [13]. Several strategies are tested for performing hill-climbing attacks against a recognition system based on electroencephalography (EEG) in [14], where it is shown that the simultaneous perturbation stochastic approximation (SPSA) method [15] can provide the best performance in terms of attack success rate.

In this paper we focus on the robustness analysis of different multi-biometrics architectures against hill-climbing attacks when fixed-length parametric representations for biometric templates are considered. This approach allows us guaranteing the possibility of comparing the behaviors of both uni- and multi-modal approaches against the same hill-climbing attack. Specifically, the employed attack strategies are outlined in Section III, while in Section IV their application against the considered multi-biometrics systems is detailed.

## III. Hill-Climbing Attacks For Fixed-Length Templates

As outlined in Section II, the hill-climbing attacks we consider can be applied to any generic biometric recognition system, given that the employed templates are expressed through a finite set of $N$ parametric features $\mathbf{x}[i]$, $i = 1, \ldots, N$. Under this hypothesis, several attack strategies can be taken into account. Specifically, as in [13] and [14], algorithms defined within the field of unknown function optimization [16] can be exploited. In fact, the purpose of these methods consists in finding a local optimum point for an *objective function* $\mathcal{F}(\cdot)$, whose arguments are given by the determinations $\mathbf{x}$ of an $N$-dimensional random variable $\mathbf{X}$. The sought optimum typically corresponds to a local or global maximum of the function $\mathcal{F}(\cdot)$, that is, the set of values $\hat{\mathbf{x}}$ for which $\mathcal{F}(\hat{\mathbf{x}}) = \max_{\mathbf{x} \in \mathcal{X}} \mathcal{F}(\mathbf{x})$, being $\mathcal{X}$ the domain in which $\mathbf{X}$ takes values. Such problems are also often referred to as Derivative Free Optimization (DFO), since the objective function is usually assumed to be not differentiable, i.e. it is not possible or not convenient in terms of computational complexity to measure local gradients of the functions slope. Besides finding the desired optimum, the algorithms are typically designed in order to reach it with the minimum possible amount of evaluation attempts, since the evaluations of the objective function $\mathcal{F}(\cdot)$ can be highly computationally demanding. These methods have been exploited in many different applications, ranging from astrophysics to nanotechnology [16].

In order to carry out a comprehensive analysis on the robustness of different multi-biometrics systems against hill-climbing attacks, several DFO-based strategies are evaluated in this paper. Specifically, both deterministic and stochastic DFO approaches are considered. The SPSA [15] and the Implicit Filtering (IF) [17] methods, both based on the estimation of the function gradient, are described in Sections III-A and III-B respectively. Moreover, an enhanced version of the deterministic Nelder-Mead (NM) [18] method, among the most well-known DFO approaches, is described in Section III-C, while the Hooke-Jeeves (HJ) algorithm [19] is detailed in Section III-D. It is worth reporting that the employed approaches are defined by assuming, for the sake of simplicity, that the features represented in the $N$-dimensional random variable $\mathbf{X}$ are mutually statistically independent. Moreover, some *a priori* knowledge about the statistics of $\mathbf{X}$, such as its estimated mean $\boldsymbol{\mu}_{\mathbf{X}}$ and the standard deviation of its components $\boldsymbol{\sigma}_{\mathbf{X}}$, is assumed to be available at the attacker side, because of the availability of a training data set. The Bayesian approach proposed in [11] is not considered here due to its significantly lower performance with respect to the aforementioned methods, as shown in [14]. When the considered algorithms are used to attack a uni-modal biometric recognition system, the values of the objective function $\mathcal{F}(\cdot)$ are given by the similarity scores produced by the matching module fed with a parametric template $\mathbf{x}$ as recognition probe. The input biometric representation $\mathbf{x}$ is then modified according to the selected strategy until either the maximum number of allowed iterations is reached or the maximum evaluated similarity score is above the chosen system threshold $t$, thus granting the recognition of the attacker. More details on the use of the considered methods to attack multi-biometrics systems are given in Section IV.

### A. SPSA Algorithm

The SPSA optimization procedure [15] computes approximations of unknown functions' gradient with a limited number of measurements. As in [13], a starting point $\mathbf{x}_{(1)} = \boldsymbol{\mu}_{\mathbf{X}}$ is selected, and at the generic $k$-th iteration, with $k \geq 1$:

- an $N$-dimensional perturbation vector $\mathbf{p}_{(k)}$ is randomly generated for determining the direction along which $\mathcal{F}(\cdot)$ is evaluated. Its statistical characterization is commonly given by a Bernoulli $\pm 1$ distribution, characterized by mutually statistically independent elements, with a zero-mean and with finite inverse moments [15];
- two evaluations of $\mathcal{F}(\cdot)$ are taken along the selected direction for approximating the gradient as $\hat{\mathbf{G}}_{\mathbf{X}} = \mathbf{p}_{(k)} \cdot [\mathcal{F}(\mathbf{x}_{(k)} + c_{(k)} \cdot \mathbf{p}_{(k)}) - \mathcal{F}(\mathbf{x}_{(k)} - c_{(k)} \cdot \mathbf{p}_{(k)})]/[2c_{(k)}]$. The scale parameter $c_{(k)}$ is then updated as $c_{(k+1)} = (\frac{k+1}{k})^{\lambda} \cdot c_{(k)}$, with $\lambda$ controlling its evolution;
- the base point is updated $\mathbf{x}_{(k+1)} = \mathbf{x}_{(k)} - a_{(k)} \cdot \hat{\mathbf{G}}_{\mathbf{X}}$. The evolution of the projection parameter $a_{(k+1)} = (\frac{A+k+1}{A+k+2})^{\kappa} \cdot a_{(k)}$ depends on the initial choice of $A$ and $\kappa$. Typically, the parameters $\lambda$ and $\kappa$ can be adjusted for a specific application, while practical guidelines for setting $c_{(1)}$, $a_{(1)}$, and $A$ are provided in [15].

If the estimated gradient is below a threshold $\varsigma$, the process is restarted. The performance of the algorithm can be improved by evaluating the objective function in more than a single pair of points and then considering the average of the obtained estimations. In our implementation we evaluate three pairs at each iteration.

### B. Implicit Filtering Algorithm

Similarly to the SPSA algorithm, the implicit filtering algorithm [17] is based on a gradient estimate, performed considering two simplexes each with $N$ points. Specifically, given an initial base point $\mathbf{x}_{(1)} = \boldsymbol{\mu}_{\mathbf{X}}$ and a scale factor $\varrho_{(1)} > 0$, at the generic $k$-th iteration, with $k \geq 1$:

- an approximated gradient is evaluated with central differences. Its $\nu$-th component, $\nu = 1, \ldots, N$, is equal to $\hat{\mathbf{G}}_{\mathbf{X}}[\nu] = [\mathcal{F}(\mathbf{x}_{(k)} + \varrho_{(k)} \cdot \mathbf{u}_{\nu}) - \mathcal{F}(\mathbf{x}_{(k)} - \varrho_{(k)} \cdot \mathbf{u}_{\nu})]/[2\varrho_{(k)}]$;
- a line search process along the direction defined by the estimated gradient is performed, by determining the value of $\phi$ for which the sufficient increase condition $[\mathcal{F}(\mathbf{x}_{(k+1)}) - \mathcal{F}(\mathbf{x}_{(k)})] > \varphi \cdot \phi \cdot ||\hat{\mathbf{G}}_{\mathbf{X}}||^2$ is satisfied, with $\mathbf{x}_{(k+1)} = \mathbf{x}_{(k)} - \phi \cdot \hat{\mathbf{G}}_{\mathbf{X}}$, and $\varphi > 0$;
- if the line search cannot update the base point, or if the estimated gradient $\hat{\mathbf{G}}_{\mathbf{X}}$ is lower than a given threshold, the employed scale $\varrho_{(k)}$ is halved: $\varrho_{(k+1)} = \varrho_{(k)}/2$.

The use of different scales in the algorithm simulates a filter which, at each iteration, removes the high frequencies contribution in the objective function, thus avoiding local maximum during the search. However, if the algorithm goes into stagnation, it has to be restarted from the latest working point with the largest considered scale.

|  | Type | Measure | Evaluation attempts |  |  |
|---|---|---|---|---|---|
|  |  |  | Initialization and restarts | $k$-th step | Further direction anal. |
| SPSA | stochastic | gradient | $2 \cdot 3$ | $2 \cdot 3$ | 1 |
| IF | determin. | simplex + gradient | $2 \cdot N$ | $2 \cdot N$ | line search |
| NM | determin. | simplex | $N$+1 | 1 | 1 |
| HJ | determin. | sequential search | $N$ | $N$ | 1 |

TABLE I
MAIN CHARACTERISTICS OF THE CONSIDERED DFO APPROACHES.

Although the strategy followed in the IF algorithm is similar to the one implemented in the SPSA method, the two approaches differ in the selection of the points employed for estimating the gradient, in the use of a sufficient increase condition along the search direction, and in the update modality of the scale and the projection parameters. Such variations result in differet performance as discussed in Section VI-B.

### C. Nelder-Mead Algorithm

The Nelder-Mead algorithm [18] is based on the iterative update of a simplex, defined as a group of $N+1$ vertices $\mathbf{x}_{\nu}$, $\nu = 1, \ldots, N+1$ in an $N$-dimensional space. As described in [13] for the algorithm's enhanced version, such simplex is initialized with a vertex $\mathbf{x}_1$ as the feature estimated mean $\boldsymbol{\mu}_{\mathbf{X}}$, and with other $N$ vertices each having just a single element different from the first vertex. Specifically, we set $\mathbf{x}_{\nu+1} = \boldsymbol{\mu}_{\mathbf{X}} + \varepsilon \cdot \mathbf{u}_{\nu}$, with $\nu = 1, \ldots, N$, being $\mathbf{u}_{\nu} = [0 \ \ldots \ 1 \ \ldots \ 0]^T$ a unit vector with $N$ coefficients, having its $\nu$-th element equal to 1, and $\varepsilon$ an algorithm parameter. At each iteration:

- the objective function is evaluated at the $N+1$ vertices of the simplex. The vertices $\mathbf{x}_L$ and $\mathbf{x}_H$ having respectively the lowest and the highest values are determined. Moreover, the centroid $\mathbf{c}$ of the $\beta \cdot (N-1)$ vertices with the highest values is evaluated, being $\beta \in [0, 1]$;
- the reflection of $\mathbf{x}_L$ with respect to $\mathbf{c}$ is computed as $\bar{\mathbf{x}} = (1+\gamma) \cdot \mathbf{c} - \gamma \cdot \mathbf{x}_L$. Then:
  - if $\mathcal{F}(\mathbf{x}_L) < \mathcal{F}(\bar{\mathbf{x}}) < \mathcal{F}(\mathbf{x}_H)$ the vertex $\mathbf{x}_L$ is substituted with $\bar{\mathbf{x}}$ (reflection);
  - if $\mathcal{F}(\bar{\mathbf{x}}) > \mathcal{F}(\mathbf{x}_H)$ then $\bar{\bar{\mathbf{x}}} = (1+\vartheta) \cdot \bar{\mathbf{x}} - \vartheta \cdot \mathbf{c}$ is evaluated, with $\vartheta > 1$. If $\mathcal{F}(\bar{\bar{\mathbf{x}}}) > \mathcal{F}(\bar{\mathbf{x}})$, then $\mathbf{x}_L$ is substituted with $\bar{\bar{\mathbf{x}}}$ (expansion), otherwise it is substituted with $\bar{\mathbf{x}}$;
  - if $\mathcal{F}(\bar{\mathbf{x}}) < \mathcal{F}(\mathbf{x}_L)$, then $\check{\mathbf{x}} = (1-\eta) \cdot \mathbf{c} + \eta \cdot \bar{\mathbf{x}}$ is computed, with $0 < \eta < 1$. If $\mathcal{F}(\check{\mathbf{x}}) > \mathcal{F}(\mathbf{x}_L)$ the worst vertex $\mathbf{x}_L$ is substituted with $\check{\mathbf{x}}$, otherwise the simplex is contracted by substituting each vertex $\mathbf{x}_{\nu}$ with $(\mathbf{x}_{\nu} + \mathbf{x}_H)/2$, $v = 1, \ldots, N+1$.

As in [13], the simplex is restarted if the difference between $\mathcal{F}(\mathbf{x}_H)$ and $\mathcal{F}(\mathbf{x}_L)$ is below a given parameter $\zeta$. The new simplex has one vertex corresponding to the maximum point so far evaluated, and the others obtained as during initialization.

### D. Hooke-Jeeves Algorithm

The Hooke-Jeeves method [19] is an iterative approach whose initialization consists in selecting a base point $\mathbf{x}_{(1)}$, typically corresponding to the estimated feature mean $\boldsymbol{\mu}_{\mathbf{X}}$, and an initial scale parameter $\omega_{(1)}$. The generic $k$-th step, with $k \geq 1$, can be summarized as follows:

- a local search around the base point $\mathbf{x}_{(k+1)} = \mathbf{x}_{(k)}$ is made by selecting a direction $\nu$, and evaluating the objective function in $\mathbf{x}_{(k+1)} \pm \omega_{(k)} \cdot \mathbf{u}_{\nu}$. The actual

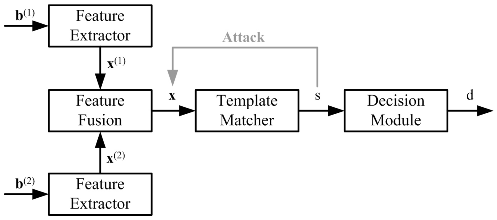


Fig. 1. Feature-level parallel fusion and corresponding hill-climbing attack.

point $\mathbf{x}_{(k+1)}$ is updated with the one giving the highest measured value, and the process is performed for all the $N$ directions $\nu = 1, \ldots, N$;

- if $\mathcal{F}(\mathbf{x}_{(k+1)}) > \mathcal{F}(\mathbf{x}_{(k)})$, then a further explorative move is made by checking the objective function at $\bar{\mathbf{x}}_{(k+1)} = \mathbf{x}_{(k+1)} + \psi \cdot (\mathbf{x}_{(k+1)} - \mathbf{x}_{(k)})$. If $\mathcal{F}(\bar{\mathbf{x}}_{(k+1)}) > \mathcal{F}(\mathbf{x}_{(k+1)})$ then $\mathbf{x}_{(k+1)} = \bar{\mathbf{x}}_{(k+1)}$;
- if no improvement is found, the scale parameter is lowered. In common applications, it is halved thus having $\omega_{(k+1)} = \frac{\omega_{(k)}}{2}$.

The algorithm is restarted from the latest base point with the original scale $\omega_{(1)}$ in case it goes into stagnation, that is, it reaches the lowest admitted scale without having found a maximum greater than the system threshold $t$.

An overview of the main characteristics of each considered DFO approach is given in Table I. All of them estimate, at each step, the best direction to be investigated in the $N$-dimensional space and then evaluate $\mathcal{F}(\cdot)$ along it. Specifically, the SPSA approach performs a stochastic search of the preferable direction, with a complexity relatively independent on the size of the considered templates. The HJ method implements a sequential inspection of the available dimensions. On the contrary, the NM and IF approaches evaluate the entire $N$-dimensional space before performing an update.

## IV. Hill Climbing Attacks Against Multi-Biometrics Recognition Systems

The methods described in Section III can be easily applied to a uni-modal biometric recognition system as attack strategies, being the produced similarity scores exploited as evaluations of the unknown objective function, upon which the generation of synthetic biometric representations $\mathbf{x}$ can be driven. However, their application to a multi-biometrics system is not necessarily straightforward, and it is therefore detailed for each of the considered multi-biometrics system architectures in the following.

Parallel and serial fusion approaches are detailed in Section IV-A and IV-B, together with the hill-climbing strategies which can be used effectively applied. Without any loss of generality, we refer to a bi-modal scenario, which is also used for the experimental tests described in Section VI.

### A. Parallel Fusion

In parallel fusion approaches, all the employed biometrics have to be acquired and processed simultaneously to perform user recognition. Specifically, the available information can be integrated at the feature level as illustrated in Section IV-A1. Alternatively, the scores obtained from the independent matching of each employed modality can be combined as discussed in Section IV-A2. Eventually, systems performing user recognition by evaluating the decisions separately taken on the available biometrics are considered in Section IV-A3. Fusion at the sensor level is not considered in this paper, because the biometric modalities used to implement this architecture should necessarily share the same format for the acquisition of the raw data and contain comparable information, which limits the generality of the approach [20].

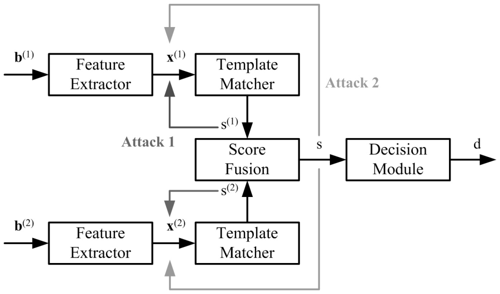


Fig. 2. Score-level parallel fusion and corresponding hill-climbing attacks.

*1) Feature Fusion:* The fusion process at feature level is depicted in Figure 1 for a bi-modal system. Such architecture has been significantly investigated as a mean for improving the achievable recognition accuracy: actually, pattern recognition systems exploiting information coming from multiple sources are often more effective if data fusion is made at an early stage of processing. The most common methodology for performing feature-level fusion consists in concatenating the feature sets independently extracted from the considered modalities [21]. A feature selection process, or a transformation to a domain with a reduced dimensionality such as principal component analysis (PCA), may be then performed as in [22]. During the fusion process, depending on the characteristics of the matcher, it may also be necessary to normalize the variance of the involved features to a common value, in order to make the considered representations compatible before their combination. A final decision mostly dependent on a subset of the employed biometric traits can be thus avoided. When applying an hill-climbing strategy against these systems, the single score $s$ generated by the matcher has to be employed for deriving the combined representation $\mathbf{x}$ comprising the features belonging to all the employed biometric modalities. The attacker can then either submit to the system the combined feature vector $\mathbf{x}$ or extract from it the templates characterizing each original biometric representation and input them separately into the system. It is worth pointing out that a single source of information has to be employed to simultaneously derive an estimation of all the involved biometric data.

*2) Score Fusion:* The fusion process at the score level is depicted in Figure 2, with reference to a bi-modal system. This approach represents the preferred modality to combine information derived from different biometrics [3]. In fact, score-level fusion is a relatively easy operation, not requiring any specific knowledge about the underlying feature extraction and matching algorithms. Since the output of a generic biometric matcher can be expressed in terms of either similarity scores or dissimilarity distances, or may cover different ranges of admissible values with significantly different distributions, score fusion typically requires a two-phase processing:

- a *normalization* step managing potentially not homogeneous matching scores. We resort to fixed score normalization, where it is assumed that a set of matching scores

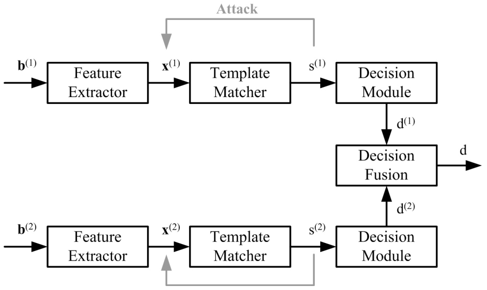


Fig. 3. Decision-level parallel fusion and corresponding hill-climbing attack.

is made available during the training phase of the fusion module. By analyzing such scores, a suitable statistical model, which has to fit the available data, is determined. The parameters to be employed for normalizing the scores computed during the system operative phase are then evaluated on the basis of the estimated model. Several approaches can be evaluated for carrying out this task, such as *min-max*, *z-score*, *median*, *double sigmoid* or *tanh-estimator* normalization techniques [3];

- a *fusion rule* combining the available normalized scores. The use of the *sum* or the *product* between the available measures, or the selection of their *minimum* or *maximum*, are possible strategies [3]. A *weighted sum* of the available scores, where each modality contributes proportionally on its accuracy [23], can be also performed to this aim, while a framework based on a likelihood ratio test has been proposed in [6].

Two distinct scenarios can be considered for hill-climbing attacks against systems based on score-level fusion. Specifically, with reference to Figure 2, it is possible to separately exploit the available scores $s^{(1)}$ and $s^{(2)}$ to independently generate, through an iterative process, the employed biometric representations $\mathbf{x}^{(1)}$ and $\mathbf{x}^{(2)}$. In this case we have to assume that an attacker is able to access the scores before their fusion is performed. On the other hand, it is also possible to assume that an attacker can only access the fused score $s$ and tries to exploit this limited information to reconstruct the templates associated to the different modalities. In order to achieve this goal, similarly to the approach employed in the case of feature fusion, the attacker can perform one of the attack strategies detailed in Section III, using $s$ as the output of an objective function having the feature vector $\mathbf{x}^T = [\mathbf{x}^{(1)^T} \ \mathbf{x}^{(2)^T}]$ as argument. Attacks exploiting either distinct or fused scores are compared in Section VI-B.

*3) Decision Fusion:* Decision-level fusion consists in combining the decisions taken by systems working independently as in Figure 3, where a bi-modal system is shown. Common decision-level fusion strategies consist in the application of either the AND or the OR rule [24]. The output of the AND rule is a match only when all the performed comparisons confirm that the acquired biometrics belong to the same user who provided the stored templates. The output of the OR rule is a match as long as at least one matcher decides that the input sample is acquired from the legitimate enrolled user.

It is worth observing that, when employing both the AND and the OR fusion strategies, the thresholds controlling the accuracy of the individual recognition processes can be selected in multiple ways for providing a given level of False Acceptance Rate (FAR) or False Rejection Rate (FRR). For this reason, similarly to what has been proposed in [25], a threshold-selection process has to be carried out during a training phase, to determine the best combinations of thresholds allowing a given operating point. In the performed experiments, data available for training are therefore exploited for selecting which system thresholds are able to guarantee a specific value of FAR while minimizing the corresponding FRR. The obtained combinations are then employed to test the accuracy of the considered system during the recognition phase. When applied to practical implementations, this thresholds selection strategy may result in Receiver Operating Characteristics (ROCs) which are not monotonic, because the minimum FRR achievable for a given FAR with the combined selection of two thresholds may be lower than the best obtainable at higher FAR conditions, even because the threshold selection process is carried out on a data set different from the one employed for testing the verification performance.

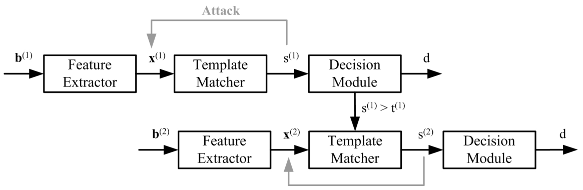


Fig. 4. Serial fusion and corresponding hill-climbing attack.

An hill-climbing attack against a decision-level-fusion multi-biometrics scheme requires the knowledge of both the scores $s^{(1)}$ and $s^{(2)}$ generated by the matchers. In this case, the attacker can exploit the presented strategies for independently deriving the templates $\mathbf{x}^{(1)}$ and $\mathbf{x}^{(2)}$, in the same way followed for two independent uni-modal systems. For systems based on the OR rule, a successful recognition is obtained once one of the two processes produces a score greater than the corresponding threshold. The attack mostly depends on the biometrics whose convergence can be achieved faster. Conversely, when using the AND rule the overall performance is regulated by the biometrics more difficult to be attacked.

### B. Serial Fusion

Within the framework of multi-biometrics, serial fusion has received much less attention than parallel fusion [22] so far. We take a broader prospective and analyze it also in comparison with the other considered multi-biometrics architectures. A serial fusion scheme for a bi-modal biometric system is depicted in Figure 4. As detailed in [22], a system where the considered biometrics are acquired sequentially may provide some benefits in terms of processing time. In fact, allowing subjects recognition according only to a subset of the employed biometrics may speed up the process with respect to the mandatory simultaneous analysis of all the employed data as in a parallel system. Moreover, systems relying on the serial acquisition of biometric traits can also be perceived as less user inconvenient than parallel systems. Therefore a wider acceptability of serial schemes may be therefore encountered for services whose frequency of access request is especially high.

An analytical description of the performance achievable using a serial multi-biometrics system is provided in [26], together with a guideline for selecting the preferable input order of the considered biometrics to guarantee optimal recognition performance. Specifically, in case a bi-modal system is implemented using a serial scheme, the biometrics providing the best recognition accuracy is first processed, and its representation $\mathbf{b}^{(1)}$ is matched with the corresponding template, thus generating the matching score $s^{(1)}$. Then:

- if $s^{(1)}$ is below a given threshold $t_1^{(1)}$, the user is immediately rejected as an impostor;
- if the computed similarity score $s^{(1)}$ is above a given threshold $t_2^{(1)}$, the user is accepted as legitimate;
- if $t_1^{(1)} < s^{(1)} < t_2^{(1)}$, the second biometric trait is acquired and processed for determining a matching score $s^{(2)}$, which is compared against a threshold $t^{(2)}$. If $s^{(2)} > t^{(2)}$, the user is authenticated, otherwise he is rejected.

In [26], the thresholds $t_1^{(1)}$ and $t_2^{(1)}$ are selected in correspondence of the *zeroFRR* and the *zeroFAR* for the first employed modality, respectively. Such operating points are estimated in the training stage. As for the attacks which can be perpetrated against a serial fusion scheme, we assume the availability of two independent scores $s^{(1)}$ and $s^{(2)}$ associated with the employed biometrics. However, no information can be derived about the modality employed in the latter stage till a similarity score greater than the first threshold $t_1^{(1)}$ is obtained in the first stage. Therefore, an attacker has to successfully accomplish this task before starting to attack the second biometrics. Then the attacker can also exploit $s^{(2)}$ to derive information about the second biometrics. A successful recognition can be achieved by either obtaining a score $s^{(1)}$ greater than $t_2^{(1)}$ for the first modality, or producing a template $\mathbf{x}^{(2)}$ for which $s^{(2)} > t^{(2)}$. Obviously, less attempts will be therefore performed for achieving a successful recognition thanks to the second biometrics, which according to [26] should be selected as the less discriminative one.

It is worth remarking that, regardless the specific attack strategy or fusion architecture, the computational effort required to perform hill climbing attack a multi-biometrics system is higher than what is required to attack a uni-modal system. This is the case even if the same number of attempts would be required to obtain illegitimate access, since, in the case of multi-biometric systems, more than a single template has to be processed at each step of the hill-climbing attack.

## V. A Countermeasure Against Hill-Climbing Attacks: Non-Uniform Score Quantization

Due to the increasing interest in the security of biometric recognition systems, significant efforts have been recently devoted to the design of countermeasures protecting users from the vulnerabilities described in Section I. As for the hill-climbing attacks, uniform score quantization has been proposed in [12] as a possible countermeasure. In fact, the effectiveness of hill-climbing attacks such as those described in Section III is in general negatively affected by the loss of some information about the outcome of the matching process, as it happens when the produced scores are quantized to a limited set of admissible values. However, the application of uniform score quantization may not be sufficient to significantly decrease the hazard of hill-climbing attacks [12], [13].

On the other hand, as discussed in [14], the application of a non-uniform quantization to the matching scores can actually limit the effectiveness of hill-climbing attacks. Being possible to adopt such countermeasure in all the multi-biometrics architectures here detailed, in Section VI-B we evaluate its effectiveness in increasing the robustness level of multi-biometrics systems without significantly affecting the achievable recognition rates. However, as pointed in Section VI-B the adoption of score quantization reduces the number of admissible operating points, yet still allowing the resulting biometric systems to work in a wide range of conditions.

Non-uniform quantization can be performed using a Lloyd-Max quantizer [27]: having set the number $L$ of desired quantized score levels, the non-uniform quantization intervals can be determined by minimizing the mean-square-error (MSE) between a given similarity score distribution and its quantized version. The employed score distribution is obtained collecting data during a training phase and performing comparisons among genuine biometric data. The estimated genuine score distribution is employed to this aim for two main reasons. First, as remarked by the experimental results in Section VI-B, hill-climbing attacks are specifically relevant when working at operating conditions characterized by a low FAR, while a brute-force approach may represent a preferable choice in high FAR conditions. Low FARs are typically obtained by setting the system threshold to high values, that is, within the range of similarity scores mostly covered by the genuine distribution. The minimization of the MSE between the genuine score distribution and its quantized version results in a finer quantization of the range interested for the foreseen operative conditions, therefore allowing to not significantly affect the system recognition performance. Second, it is also worth noticing that hill-climbing attacks are commonly initiated from evaluation points randomly selected or associated with the inter-class features mean, therefore resulting in low similarity scores which cannot be assimilated within the distribution of genuine scores. If a coarse quantization process is applied to the range of scores produced by the first attempts of an hill-climbing strategy, the evolution of the considered attacks will be hindered, therefore inducing more often the attacks into stagnation.

An extensive experimental analysis of non-uniform score quantization as deterrent against hill-climbing attacks is given in Section VI, where the systems recognition accuracy and robustness against hill-climbing attacks are evaluated and compared with those of systems using unquantized scores.

## VI. Experimental Tests

The experimental tests performed to evaluate the performance of the considered hill-climbing attacks against the multi-biometrics architectures detailed in Section IV are here described. Specifically, the employed experimental setup is first presented in Section VI-A, then the obtained results are given in Section VI-B in terms of both achievable recognition accuracy and robustness against the employed attacks.

### A. Experimental Setup

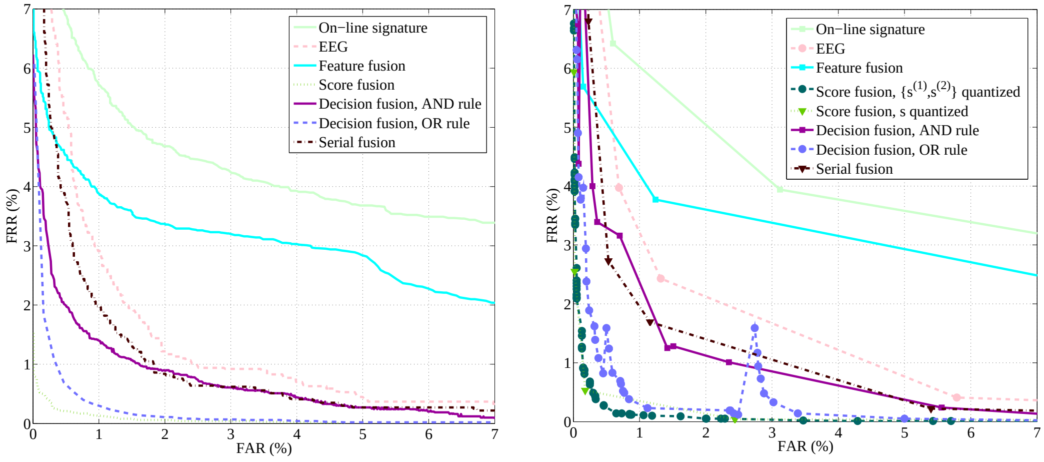
As already mentioned, without any loss of generality, we focus on bi-modal architectures for implementing the considered multi-biometrics systems. More specifically, a detailed analysis comprising all the presented attack strategies is first conducted on bi-modal systems based on on-line signature and EEG, which represent quite independent modalities characterized by significantly different recognition accuracies. Moreover, as an additional proof-of-concept for corroborating the observed outcomes, further evaluations are also carried out considering schemes relying on combinations of on-line signature and fingerprint biometrics. A very brief introduction on the employed biometric modalities is given hereafter, together with the associated representations exploited in the considered implementations. Section VI-A4 then introduces the employed data sets, and illustrates how the considered multi-biometrics systems are simulated.

*1) On-line Signature:* This modality is based on the acquisition of the signature dynamic behavior by means of a graphic tablet or a pen-sensitive computer display. The considered signature representation is based on the extraction of parametric features [28], which can express either static information such as the height and the width of the signatures, or dynamic information like the number of strokes, the mean signature velocity, and so forth. More specifically, not being feature extraction the focus of our contribution, we employ 40 global features, chosen among the ones proposed in [29] by means of the selection process described in [30], which determines the most discriminative feature set among the possible selections. The employed matcher module relies on the computation of the Mahalanobis distance between the feature vector provided during the authentication phase and the distributions estimated during the users enrollment, expressed in terms of the estimated intra-class means and standard deviations. The chosen features are assumed to be independent to simplify the evaluation of the covariance matrix as well as the computation of the Mahalanobis distance. In order to generate similarity scores, the inverse of the computed distance is employed as the output of the considered uni-modal matcher.

*2) Electroencephalography:* EEG-based biometrics exploits the possibility of recognizing individual using the brain electrical activity recorded on the scalp of a user by means of non-invasive electrodes placed in specific spatial configurations. Although brain waves have been typically investigated for medical purposes, in the last few years they have also been proposed as a biometrics for recognition purposes [31]. In the considered scenario, EEG signals are recorded from subjects in relaxed state with closed eyes. In these conditions the so-called alpha activity, mainly pronounced in the parieto-occipital region and in the frequency range 8–14 Hz, is the most dominant rhythm. Three channels (P7-Pz-P8) are employed for performing recognition as in [32]. An auto-regressive (AR) modelization with an order equal to 12 is then employed to represent each acquired channel [33], therefore resulting in 36 parametric features employed to represent each EEG sample. As for a uni-modal system relying on on-line signature, also the matcher for EEG signals is based on the evaluation of the Mahalanobis distance between the stored template and a single query EEG sample. The inverse of the computed distance is employed also in this case to provide the similarity measure produced by the considered matcher.

*3) Fingerprint:* Fingerprint is undoubtedly the most widely employed modality in biometric recognition systems. Its processing involves the analysis of ridge and valley patterns on the surface of a finger, which traditionally consists in the extraction of local ridge anomalies such as bifurcations or endings, called minutiae points [34]. When adopting such approach, the resulting fingerprint templates may have variable sizes and the matching phase is typically computationally expensive due to the need of aligning the unregistered minutiae patterns of different acquisitions. However, it is also possible to generate compact fixed-length parametric fingerprint templates. Specifically, without any loss of generality, the *FingerCode* representation proposed in [35] is here taken into account. A reference point, characterized by the maximum curvature of the concave ridges, is first determined. The fingerprint region around this point is then divided in different sectors, each processed through a bank of Gabor filters to capture both local and global fingerprint details. According to the processing described in [35], 640 features can be generated for each fingerprint. Among them, the most discriminative ones can be determined through the selection method proposed in [30] in order to derive the employed fingerprint templates. As detailed in Section VI-B2, two different fingerprint template sizes are considered to perform an in-depth evaluation on the performance of the considered hill-climbing algorithms. The comparison between two fingerprints is performed by computing the Euclidean distance of the associated templates, with its inverse being the output of the considered matcher.

*4) Multi-modal Systems:* The experimental tests performed on multi-modal systems using on-line signature and EEG are carried out by taking biometric data from two independent databases. Specifically, signatures are taken from the public MCYT corpus [36], that contains 25 genuine signatures as well as 25 skilled forgeries for each user, for a total of 100 users. A database collected in our institution, containing data taken from 40 different users, is considered for providing EEG data: the signals acquired from users in a relaxed state are segmented into patterns, named “frames”, each lasting three seconds, taken as biometric acquisition samples. For each user 77 frames of EEG signals are available. The two databases are employed to generate *chimerical* data sets simulating the simultaneous acquisition of on-line signature and EEG signals. As remarked in [3], building chimerical data sets is a widely used approach in experimental investigations on multi-modal biometrics. Moreover, chimerical databases are considered as more “realistic” as less correlated are its components [37]. Therefore, the use of two biometric identifiers with low correlation such as signature and EEG signals acquired in closed-eyes resting conditions makes the creation of chimerical users realistic. The adoption of two independent biometrics with notably different recognition rates also allows to clearly define the configuration of the serial scheme described in Section IV-B according to [26] and to better appreciate the contribution of the different fusion schemes for the computed performance, reported in Section VI-B. The signatures taken from 20 users in the MCYT corpus, together with the EEG signals acquired from 10 subjects, are employed for a training phase when some statistics of the employed modalities are estimated, while



(a) (b)

Fig. 5. Recognition accuracy of systems with on-line signatures and EEG biometrics. Random forgeries used as signature impostor attempts. (a): FAR/FRR with unquantized scores; (b): FAR/FRR with quantized scores.

the remaining data are used for testing the considered multi-biometrics systems and the analyzed hill-climbing attacks on a disjoint data set. In both training and testing conditions, the enrollment of a user is simulated by randomly associating 10 signatures of a given subject in MCYT with 52 frames taken from a user in the EEG database. This way, during the testing phase we are able to generate a large number of user templates, namely 10000, for estimating the performance of the considered systems in terms of recognition rates and robustness against hill-climbing attacks.

Additionally, we complement our experiments with the evaluation of biometric systems characterized by real multi-modal data sets, exploiting the availability of fingerprints in the MCYT database. Specifically, for each user whose signatures are collected, 12 impressions of each finger are also captured with an optical scanner [36]. Signatures and fingerprints of 20 users are used to carry out the systems training phases, while the remaining 80 users are employed for testing purposes. Specifically, the enrollment of a subject is performed by associating a right index fingerprint with 10 randomly selected signatures, thus generating with the available data overall 80×12 = 960 different templates for performance estimation.

Focusing on the training phase of the considered multi-biometrics systems, the available data sets are exploited to define the normalization process required in a score-level fusion scheme, as described in Section IV-A2. Specifically, in our experiments we consider a tanh-estimator approach [3] which, having indicated as $s^{(i)}$ the score produced by the $i$-th classifier, returns a normalized value $\bar{s}^{(i)}$ equal to

$$\bar{s}^{(i)} = \frac{1}{2}\Big\{tanh\big[0.02 \cdot \big(\frac{s^{(i)} - \mu}{\sigma}\big)\big] + 1\Big\}. \tag{1}$$

The values $\mu$ and $\sigma$ are respectively the mean and the standard deviation of the genuine scores distribution estimated during the training phase, once the Hampel influence function has been applied to the computed scores $s$ as:

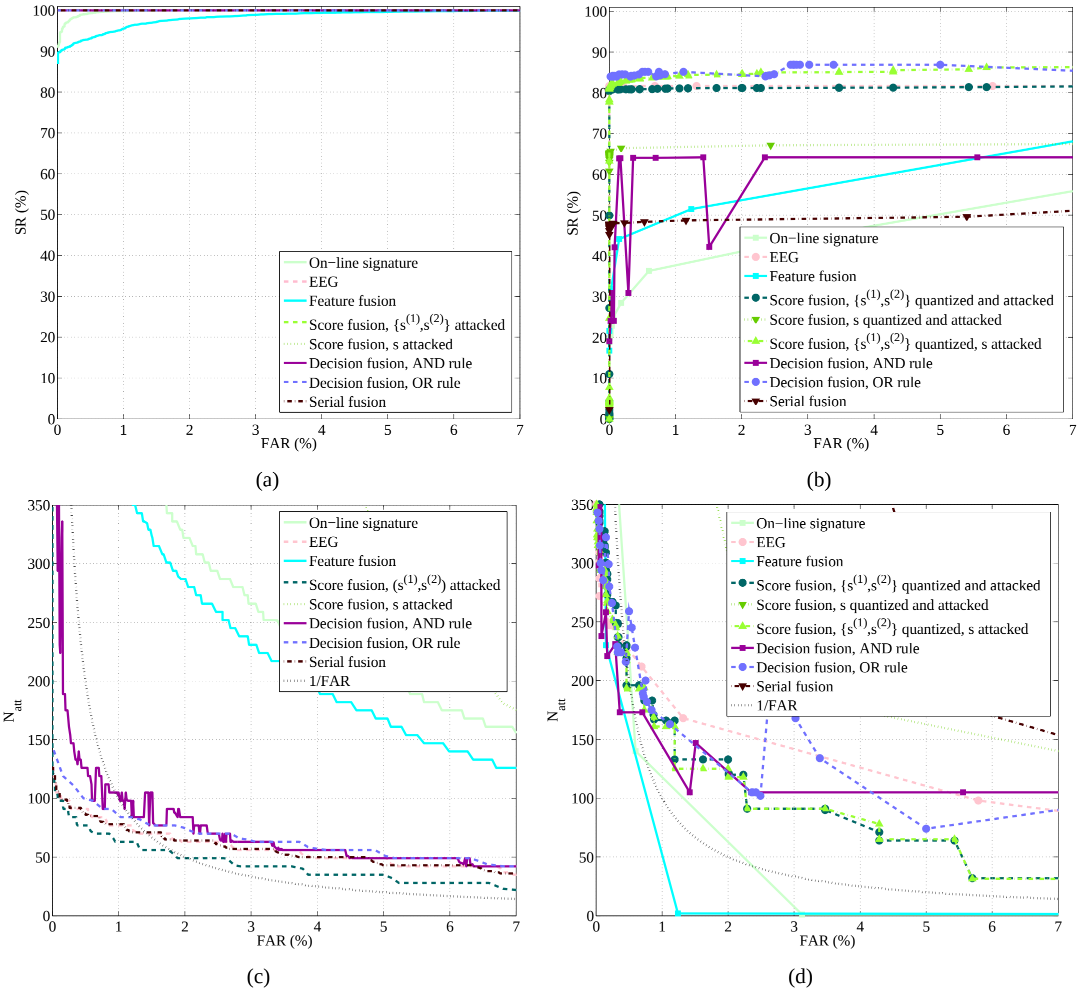
$$\psi(s) = \begin{cases} s & , \ 0 \leq |s| < a, \\ a \cdot sign(s) & , \ a \leq |s| < b, \\ a \cdot sign(s) \cdot \big(\frac{c-|s|}{c-b}\big) & , \ b \leq |s| < c, \\ 0 & , \ |s| \geq c. \end{cases} \tag{2}$$

Normalized scores are comprised between 0 and 1, with the distribution of genuine normalized scores having a mean of 0.5 and a standard deviation of 0.01. The function $\psi(\cdot)$ is employed for limiting the influence of the score distribution's tails in the normalization process through a proper setting of the parameters $a, b$ and $c$, thus making this process highly robust against outliers. We set $a = 95\%$, $b = 0.97\%$, and $c = 0.99\%$ of the maximum observed score in the performed experiments, having assumed a limited presence of outliers in the score distributions of the considered biometrics.

Training data are also employed for the features normalization process, still based on the tanh-estimator. As reported in Section IV-A1, combined vectors whose coefficients share similar characteristics such as an equal variance can be thus generated, avoiding performance being mainly dependent only on one of the involved biometrics. The classifier employed for fingerprint biometrics can be therefore implemented through a Mahalanobis distance as for signature and EEG, even if the fingerprint enrollment phase requires just one sample. A constant standard deviation equal to 0.01 is used for all the features of every user. The parameters employed for the Hampel influence function are the same as those adopted for score normalization. No further processing is applied to the concatenated vectors, whose size is therefore equal to the sum of the lengths of the contributing representations. Obviously, the threshold-selection process described in Section IV-A3, defining the operating conditions of a decision-level fusion scheme, is carried out on the training data. The available information is also employed to determine the most discriminative biometrics among the considered ones, thus allowing to follow the suggestions given in [26]. In the serial system based on signature and EEG, this latter is employed in the first stage, whereas when using fingerprint and signature, the former identifier is exploited first. Eventually, the training data sets are employed to determine the quantization intervals of the scores produced in systems implementing the countermeasures described in Section V to increase their strength against hill-climbing attacks.

## B. Results and Discussion

A detailed analysis of multi-modal systems based on signature and EEG biometrics is first performed in Section VI-B1. Systems using signature and fingerprint biometrics are then



(a) (b) (c) (d)

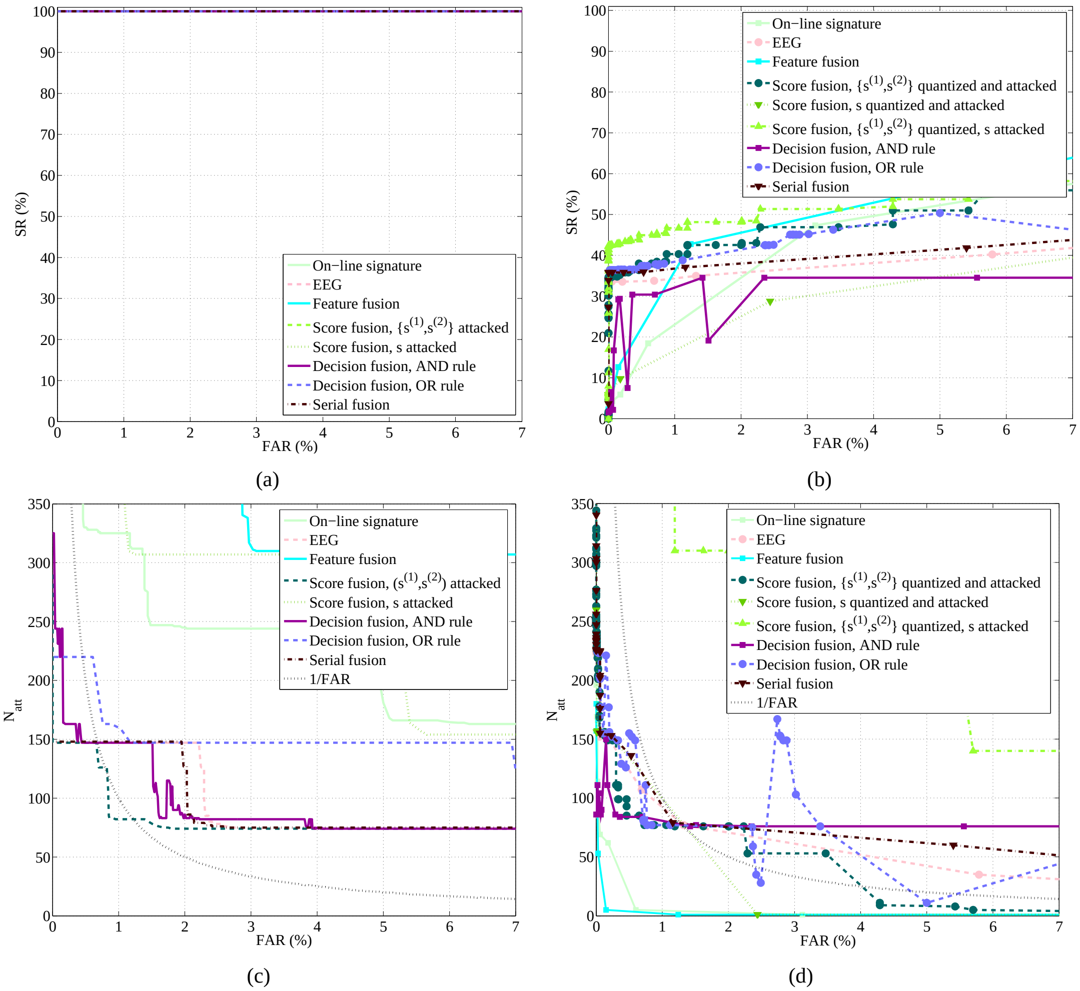
Fig. 6. Performance of SPSA hill-climbing attacks against multi-biometrics systems based on on-line signatures and EEG. (a): SR (in %) using unquantized scores; (b): SR (in %) using quantized scores; (c): $N_{att}$ using unquantized scores; (d): $N_{att}$ using quantized scores.

analyzed in Section VI-B2 to further strengthen our findings.

*1) Bi-modal systems - Signature and EEG:* Figures 5.(a) and 5.(b) show the recognition rates achievable for uni- and multi-modal systems based on on-line signature and EEG biometrics, when dealing respectively with unquantized and quantized matching scores. Specifically, random forgeries are employed as signature impostor attempts when evaluating the FAR performance, in order to properly compare the effectiveness of a random guessing attack with the efficacy of a hill-climbing approach. This latter is in fact performed without knowing any specific information about the targeted user, therefore data strictly correlated with the interested identity, such as skilled forgeries, cannot be considered for the sake of a fair comparison. As can be seen, the system guaranteeing the best recognition performance is the one based on score-level parallel fusion, achieving an Equal Error Rate (EER) of 0.3% when using unquantized scores. It is worth specifying that all the fusion rules mentioned in Section IV-A2 for combining normalized scores are considered for score-level-fusion-based multi-biometrics systems. However, observing that all the employed fusion rules result in similar performance, at least from the point of view of the desired analysis, only the outcomes achieved when employing the *sum* rule are given in the reported figures. Decision-level fusion represents the second most preferable scheme in terms of verification accuracy, with the OR rule outperforming the AND approach. Serial fusion is able to provide a slight improvement with respect to the use of a uni-modal scheme relying on EEG, which often provides better results than those achieved when it is used together with on-line signatures in a feature-level fusion approach. As for the adoption of quantized scores, it is possible to observe that, apart from allowing less operating points, represented with markers in the reported figures, the employed non-uniform quantization strategy does not significantly alter the achievable system accuracy. It is worth observing that, when considering a score-level fusion scheme, we can quantize the produced scores either before or after their fusion. The latter strategy results in a reduced number of admissible operating points with respect to the use of quantization before fusion, nevertheless it can still guarantee verification rates better than those associated with other fusion schemes.

The effectiveness of the considered hill-climbing in attacking uni-modal biometric systems, as well as the multi-modal systems described in Section IV, is described through Figures 6 - 9, each associated with one of the considered attack strategy. Systems using both unquantized and quantized scores are taken into account in the performed experiments. Specifically, the attacks are evaluated in terms of indicators [10] commonly used in literature to assess hill-climbing attacks, namely:

- the associated success rate (SR), that is, the percentage



(a)

(b)

(c)

(d)

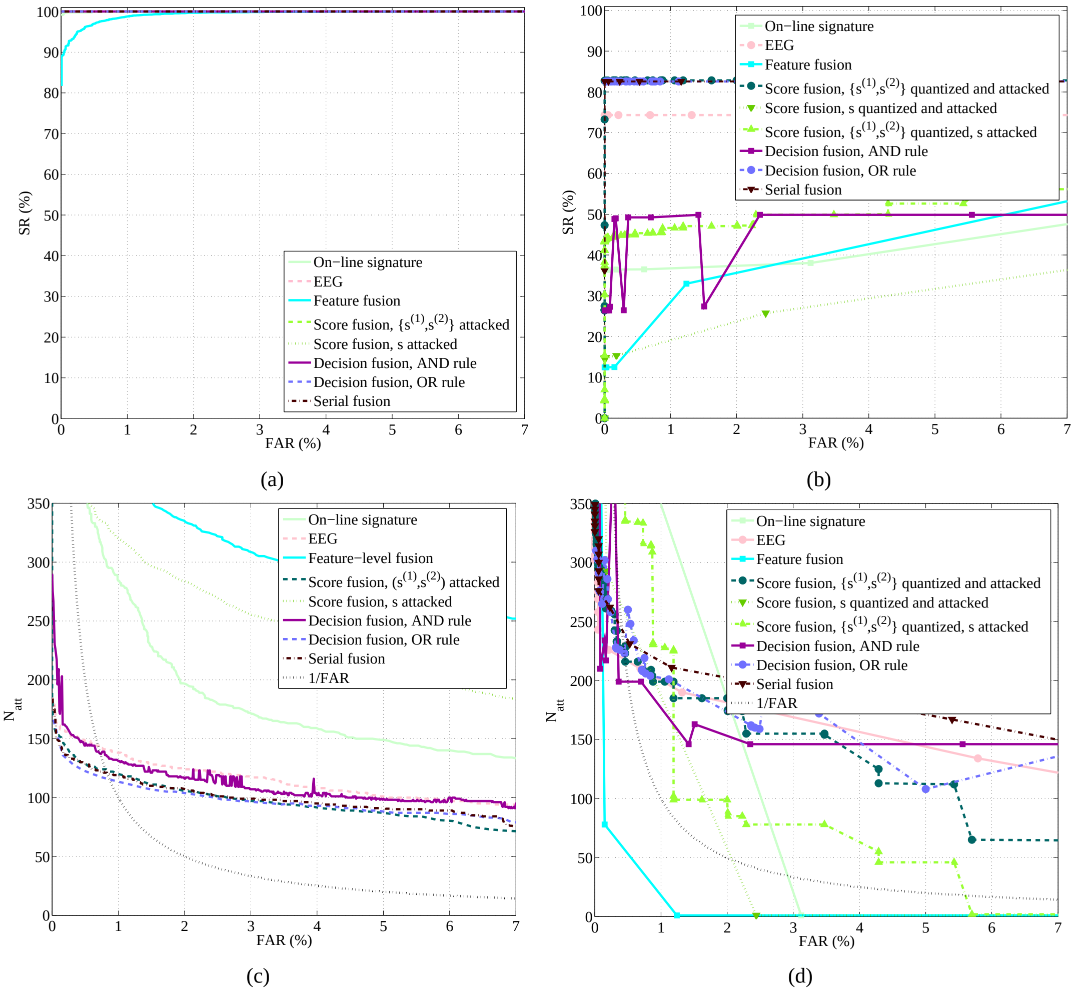
Fig. 7. Performance of Implicit Filtering hill-climbing attacks against multi-biometrics systems based on on-line signatures and EEG. (a): SR (in %) using unquantized scores; (b): SR (in %) using quantized scores; (c): $\mathrm{N_{att}}$ using unquantized scores; (d): $\mathrm{N_{att}}$ using quantized scores.

of users whose account can be accessed with less than a maximum number of attempts, here set to 5000;

- the attack efficiency, given by the average number of matching attempts $\mathrm{N_{att}}$ needed to break an account. The lower $\mathrm{N_{att}}$, the faster the algorithm is in succeeding.

It is worth pointing out that the SR is commonly introduced to limit the computational complexity of hill-climbing attacks to a given maximum, thus avoiding situations with infinite loops during the simulations, due to persisting stagnation of the algorithms. The initial conditions of attacks at systems with both unquantized and quantized scores are determined by estimating means and standard deviations of the original features distributions over the training data set. Due to the significant dependency of the algorithms performance on the parameters selected for running each attacks, several tests are performed in order to obtain, for each considered method, the conditions resulting in the highest percentages of success rate SR together with the lowest number of attacks $\mathrm{N_{att}}$. Such optimization is performed at the operating point corresponding to FAR = 0.3%, since the analysis of hill-climbing attacks is particularly important at low FAR conditions, as already outlined. The behavior of each attack is reported with reference to the FAR corresponding to a given threshold in the analyzed systems. Adopting this approach for displaying the observed behaviors allows us easily comparing the considered multi-biometrics systems with respect to their robustness against all the investigated hill-climbing strategies. Furthermore, we can also directly compare the performance of hill-climbing attacks, in terms of $\mathrm{N_{att}}$, with those associated to brute-force approaches. These latter can be in fact represented, for all the considered uni- and multi-modal systems, with a single curve reporting the 1/FAR behavior, which is indeed the average number of attempts an attacker should perform by randomly submitting biometric samples before obtaining a successful recognition. Moreover, we would like to point out that three different scenarios are taken into account when analyzing score-level fusion schemes: in the first one, the scores are non-uniformly quantized prior to the fusion and the attacker can access the quantized scores to drive his hill-climbing strategy; in the second one, the scores are fused and then the final output is non-uniformly quantized according to its estimated distribution, being also accessible to the attacker; in the last one, non-uniform quantization is applied to the original scores $\{s^{(1)}, s^{(2)}\}$, while the attacker is able to capture only the fused score $s$.

From the reported results it is possible to notice that, when dealing with systems relying on unquantized scores, the most important figure of merit is given by the value of $\mathrm{N_{att}}$, since the SR of all the considered methods is close or equal to 100% for almost all the evaluated operating conditions. By



(a)

(b)

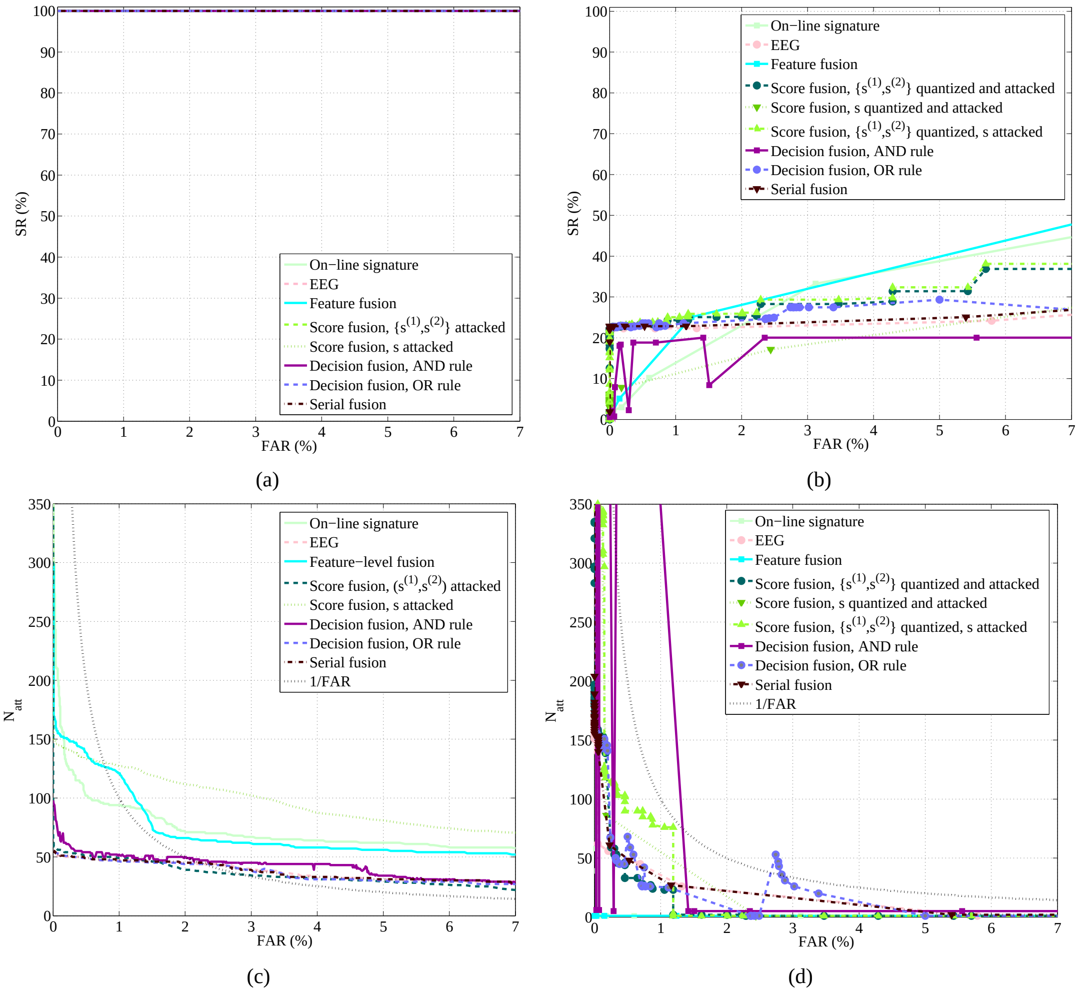
(c)

(d)

Fig. 8. Performance of Nelder-Mead hill-climbing attacks against multi-biometrics systems based on on-line signatures and EEG. (a): SR (in %) using unquantized scores; (b): SR (in %) using quantized scores; (c): $N_{att}$ using unquantized scores; (d): $N_{att}$ using quantized scores.

a joint analysis of the recognition performance reported in Figure 5 and the efficiency of the considered attacks given in Figures 6 - 9, it is also possible highlighting a specific trade-off between achievable recognition capabilities and vulnerability against hill-climbing attack. In fact, for a given robustness against impostors random guessing attacks, that is, for a specific FAR value, multi-biometrics systems guaranteeing better recognition rates in terms of FRR are more vulnerable to hill-climbing attacks. In more detail, from a comparison of the considered fusion strategies, feature-level fusion seems to be the most resilient strategy. In fact, this is the only system resulting in a success rate lower than 100% in some operating conditions, at least for the SPSA and the Nelder-Mead approaches as evident from Figures 6.(a) and 8.(a). Additionally, the number of attempts $N_{att}$ needed to achieve a successful recognition in a feature-level-based architecture is typically much higher than that required in other multi-biometrics systems (see Figures 6.(c), 7.(c), 8.(c) and 9.(c)). A score-level fusion approach is typically less secure than a serial or a decision-level fusion scheme, while these latter two are normally characterized by a similar resilience against hill-climbing attacks. As for the decision-level fusion schemes we observe that, in general, a system using the AND rule is commonly more difficult to be attacked than one based on the OR rule, and both are often more vulnerable than uni-modal systems relying on the individual modalities. It is also worth observing that, given the assumption an attacker may access the scores produced in a biometric system, schemes based on score-level fusion can be considered secure only if the accessible information relates to the fused score and not the original scores related to the employed modalities. Under such condition, the achieved robustness is usually in the same order of magnitude of a feature-level fusion scheme. Moreover, we notice that hill-climbing attacks may represent a more serious threat than brute-force approaches when working at low FAR conditions: for the multi-modal systems considered in our experiments, an SPSA strategy achieves successful recognition with less attempts than random data submission for FAR $<$ 1%, while the Hooke-Jeeves approach represents a significant threat for FAR $<$ 2%.

When considering non-uniform score quantization as a possible countermeasure against hill-climbing attacks, we observe a dramatic decrease in the resulting success rate with respect to systems using unquantized scores, as evident when for example comparing Figure 6.(a) with Figure 6.(b), 7.(a) with 7.(b), 8.(a) with 8.(b), or 9.(a) with 9.(b). Within this scenario, the SR therefore represents the most important figure of merit. The reported experimental results show that the SPSA and the Nelder-Mead attacks seem to perform better than the other considered approaches, with the former method especially



(a) (b) (c) (d)

Fig. 9. Performance of Hooke-Jeeves hill-climbing attacks against multi-biometrics systems based on on-line signatures and EEG. (a): SR (in %) using unquantized scores; (b): SR (in %) using quantized scores; (c): $\mathrm{N_{att}}$ using unquantized scores; (d): $\mathrm{N_{att}}$ using quantized scores.

effective at high FAR values, both in terms of SR and $N_{att}$. We can also observe that the most resilient multi-modal system is still the one relying on a feature-level fusion, followed by the serial scheme and the decision-level parallel approach. For this latter, the use of the AND fusion rule makes the system slightly more robust than the adoption of the OR rule, which is however more effective in terms of recognition accuracy. The trade-off between recognition accuracy and security against hill-climbing attacks, for a given FAR, is therefore confirmed also in this case. As for the implemented score-level fusion strategies, the case in which the fused score is quantized and made available to the attacker is the most resilient against hill-climbing attacks. This condition would be therefore the most preferable one for simultaneously providing acceptable robustness against hill-climbing attacks, while guaranteeing proper verification performance, although few operating conditions would be available, as observed in Figure 5.(b). When quantizing the original scores $\{s^{(1)}, s^{(2)}\}$, similar results in terms of SR are typically achieved when either their quantized values are given to the attacker, or when the fused scores are made available. Nonetheless, the latter case typically require more attempts for a successful attack, therefore representing a more secure condition.

It is worth specifying that the 1/FAR behavior is reported as a continuous curve in all the figures reporting $\mathrm{N_{att}}$ in case of quantized scores, although only a limited subset of FAR values can be actually achieved in this scenario, not to mention also that distinct FAR operating conditions can be guaranteed in different multi-biometrics architectures, as shown in Figure 5.(b). Moreover, we would like to point out that a monotonic behavior for SR and $\mathrm{N_{att}}$ can be hardly obtained in systems based on decision-level fusion strategy. This is due to the modality employed for determining the corresponding operating points, e.g., by selecting the operative system thresholds during a training phase, and then using them for obtaining the displayed experimental results as described in Section IV-A3.

A brief summary providing a comparison between the performance of different hill-climbing strategies applied to the considered multi-modal systems is given in Table II. Specifically, the most significant measures for systems based on unquantized and quantized scores are here reported: the $\mathrm{N_{att}}$ computed at FAR = 0.3% is given for systems using unquantized scores, while the SR estimated at the available operating points closer to FAR = 0.3% is shown for systems exploiting score quantization.

*2) Bi-modal systems - Signature and Fingerprint:* An additional proof-of-concept is provided by considering systems based on signature and fingerprint biometrics. Specifically, being one of the best performing among the adopted meth-

|  |  |  | Parallel Fusion |  |  |  |  | Serial Fusion |
|---|---|---|---|---|---|---|---|---|
|  | Sign. | EEG | Feature | Score |  | Decision |  |  |
|  |  |  |  | $\{s^{(1)},s^{(2)}\}$ | $s$ | AND | OR |  |
| $\mathrm{N_{att}}$ at FAR = 0.3% for systems using unquantized scores |  |  |  |  |  |  |  |  |
| SPSA | 686 | 92 | 609 | 84 | 1329 | 148 | 112 | 92 |
| IF | 398 | 150 | 613 | 148 | 460 | 163 | 220 | 154 |
| NM | 403 | 151 | 570 | 128 | 387 | 151 | 136 | 133 |
| HJ | 121 | 50 | 148 | 48 | 140 | 57 | 52 | 50 |
| SR (in %) at FAR $\simeq$ 0.3% for systems using quantized scores |  |  |  |  |  |  |  |  |
| SPSA | 28.4 | 81.2 | 44.1 | 80.8 | 66.4 | 64.1 | 84.2 | 48.1 |
| IF | 5.9 | 33.5 | 12.6 | 37.5 | 9.7 | 30.3 | 36.2 | 36.4 |
| NM | 36.4 | 74.3 | 12.5 | 82.5 | 15.3 | 49.3 | 82.3 | 82.1 |
| HJ | 2.9 | 22.4 | 5.2 | 23.8 | 7.8 | 18.3 | 22.7 | 23.0 |

TABLE II

SUMMARY OF THE ACHIEVABLE ATTACK PERFORMANCE FOR SYSTEMS USING UNQUANTIZED SCORES (AT FAR = 0.3%) AND QUANTIZED SCORES (AT THE OPERATING POINT CLOSER TO FAR = 0.3%).

| Parallel Fusion |  |  |  |  | Serial Fusion |
|---|---|---|---|---|---|
| Feature | Score |  | Decision |  |  |
|  | $\{s^{(1)},s^{(2)}\}$ | $s$ | AND | OR |  |
| +++ | - | +++ | ++ | + | + |

TABLE III

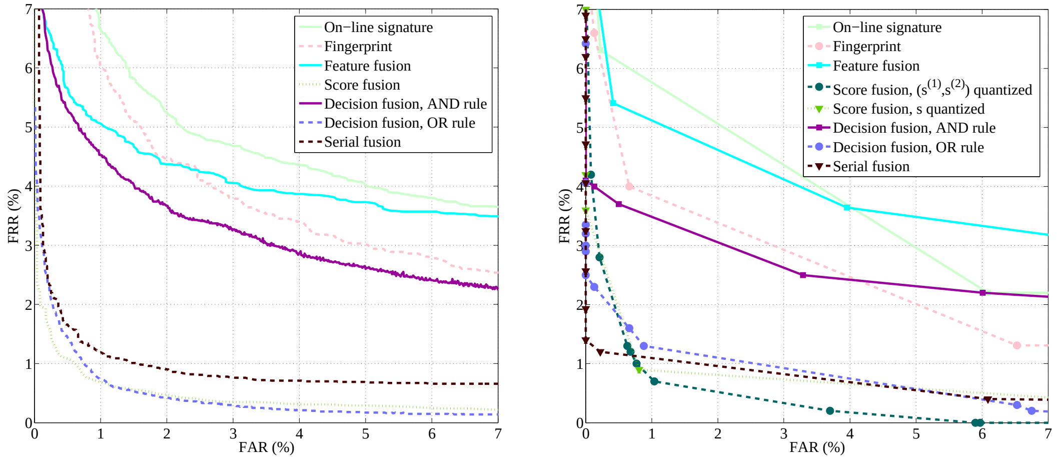
QUALITATIVE EVALUATION OF THE SECURITY AGAINST HILL-CLIMBING ATTACKS.

ods, only the SPSA approach is employed in the following discussion for evaluating the robustness of the considered fusion strategies when applied to signature and fingerprint data. Furthermore, as already mentioned, the experiments on the considered real bi-modal data set are carried out exploiting two different representations for the parametric templates characterizing fingerprint biometrics. In the first set of experiments, fingerprint templates are represented by 36 features, that is the same size of the EEG templates considered in Section VI-B1. This way we can analyze the performance of the considered hill-climbing attacks when applied to biometric modalities with different characteristics, yet represented through templates with comparable sizes. While the recognition performance achievable with the evaluated multi-biometrics systems based on on-line signature and fingerprint are reported in Figure 10, the effectiveness of the considered SPSA strategy in attacking such systems is described in Figure 11. As evident, the observed behaviors are definitely similar to those outlined in Figure 6, highlighting once again the trade-off between the achievable recognition accuracy and the corresponding security against hill-climbing attacks for a given FAR: the feature-level fusion scheme provides the highest robustness against the adopted attack strategy, followed by a decision-level fusion approach using the AND rule. The OR decision rule and the serial fusion strategy represent the most vulnerable systems, together with the score-level approach, which is secure only if the individual scores are not accessible. Such qualitative evaluations, in agrement with what observed in Section VI-B1, are summarized in Table III. It is worth mentioning that also a "hybrid" procedure, where an attacker first performs some attempts with a brute-force approach (with either 10 or 20 random guesses), and then launches an hill-climbing attack starting from the best result so far obtained, has been tested. Nonetheless, no significant improvement in the observed attacks' effectiveness has been noticed *wrt* an hill-climbing strategy starting from the estimated feature mean. Actually, a similar result has been already pointed out in [13], where it has been observed that launching Nelder-Mead-based hill-climbing attacks from the estimated feature mean vectors would result in an efficiency improvement, with respect to starting the attack from random points.

Furthermore, an additional set of tests is performed by considering a fingerprint representation with an increased template size, with the dual objective of analyzing the performance of the used hill-climbing strategies in higher-dimensional spaces, and verifying the trade-off between achievable recognition rates and security against hill-climbing attacks in highly accurate real multi-biometrics systems. In fact, while the fingerprint representation so far considered allows achieving an EER = 3.5% for a uni-modal fingerprint system, the exploitation of 72 features selected among the available 640 allows achieving an EER = 1.2%. It is worth pointing out that no significant further improvement can be obtained, with the considered data, for even larger sizes of the fingerprint templates. The best performance in real multi-biometrics systems exploiting such longer fingerprint representation is still achieved with a score-level fusion strategy, reaching an EER = 0.4% as shown in Figure 12. Nonetheless, the results reported in Figure 13 still show that hill-climbing approaches may represent strategies more efficient than brute-force approaches for significant operating conditions, typically characterized by low FAR, if countermeasures such as score quantization are not adopted. Moreover, the effectiveness of the SPSA approach is not significantly affected by the modified biometric template size, especially when considering systems using unquantized scores. The reported results confirm the trade-off between achievable recognition rates and vulnerability against hill-climbing attacks at a given FAR, also for highly accurate multi-modal systems based on real multi-biometrics data.

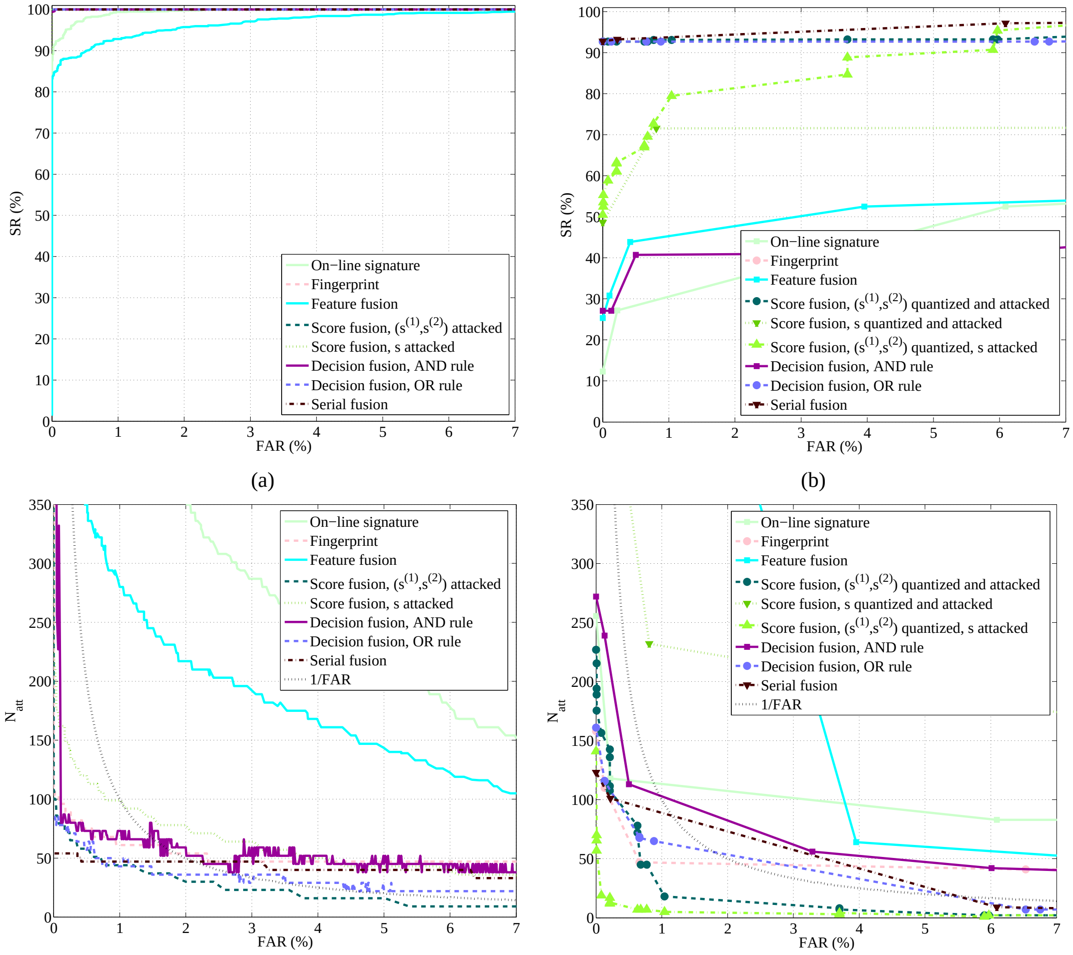
## VII. CONCLUSIONS

An analysis on the performance of hill-climbing attacks against multi-modal biometric recognition systems has been presented in this paper. Specifically, attack strategies relying on the exploitation of matching outputs for generating parametric fixed-length biometric templates have been considered for testing the behavior of both parallel and serial fusion schemes. As proof-of-concept and without any loss of generality, bi-modal systems based on on-line signature and EEG, and on on-line signature and fingerprint, have been considered in the performed experimental tests, showing a trade-off relationship between the achievable recognition accuracy and the security against the considered hill-climbing strategies for a given FAR. It has been noticed that hill-climbing attacks may represent a significant threat for biometric systems operating at low FAR, requiring less effort than a brute-force attack for successfully breaking the system. Non-uniform score quantization has also been analyzed as a possible countermeasure to hill-climbing attacks, observing its effectiveness in increasing the systems robustness without a significant worsening of the verification performance. Among the considered attack strategies, the Hooke-Jeeves approach turns out to be the most effective approach when dealing with unquantized scores, while the SPSA outperforms the other considered methods when adopting score quantization in the considered schemes. According to the obtained experimental results, in order to



(a) (b)

Fig. 10. Recognition accuracy of systems with on-line signatures and fingerprint biometrics (with 36 features). (a): FAR/FRR with unquantized scores; (b): FAR/FRR with quantized scores.



(a) (b)

(c) (d)

Fig. 11. Performance of SPSA hill-climbing attacks against multi-biometrics systems based on on-line signatures and fingerprint biometrics (with 36 features). (a): SR (in %) using unquantized scores; (b): SR (in %) using quantized scores; (c): $\mathrm{N_{att}}$ using unquantized scores; (d): $\mathrm{N_{att}}$ using quantized scores.

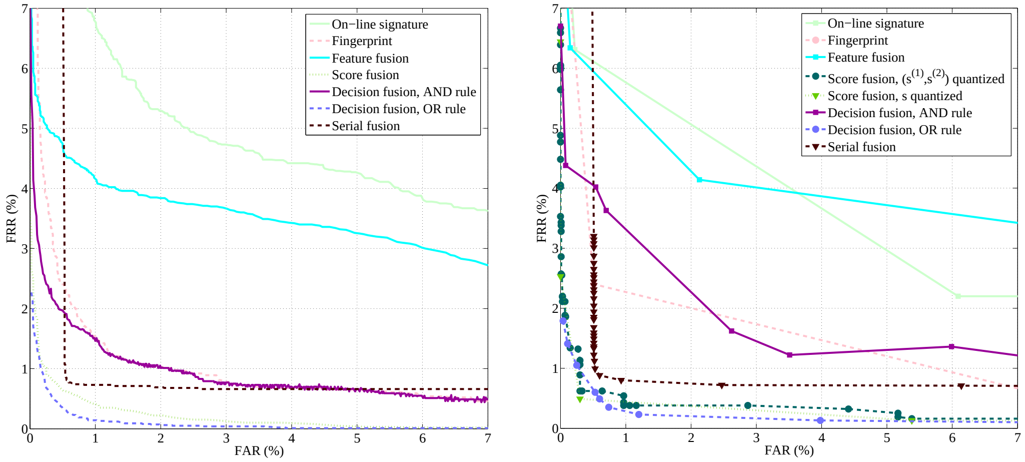
simultaneously guaranteeing high recognition accuracy and proper robustness against hill-climbing attacks, a score-level fusion scheme could be adopted, provided that an attacker should access only the quantized fused score for driving his hill-climbing strategy. Such observations should be taken into account when implementing custom multi-biometric systems with commercial off-the-shelf components whose modules need to be interconnected each other.

## References

[1] P. Campisi, Ed., *Security and Privacy in Biometrics*. Springer, 2013.

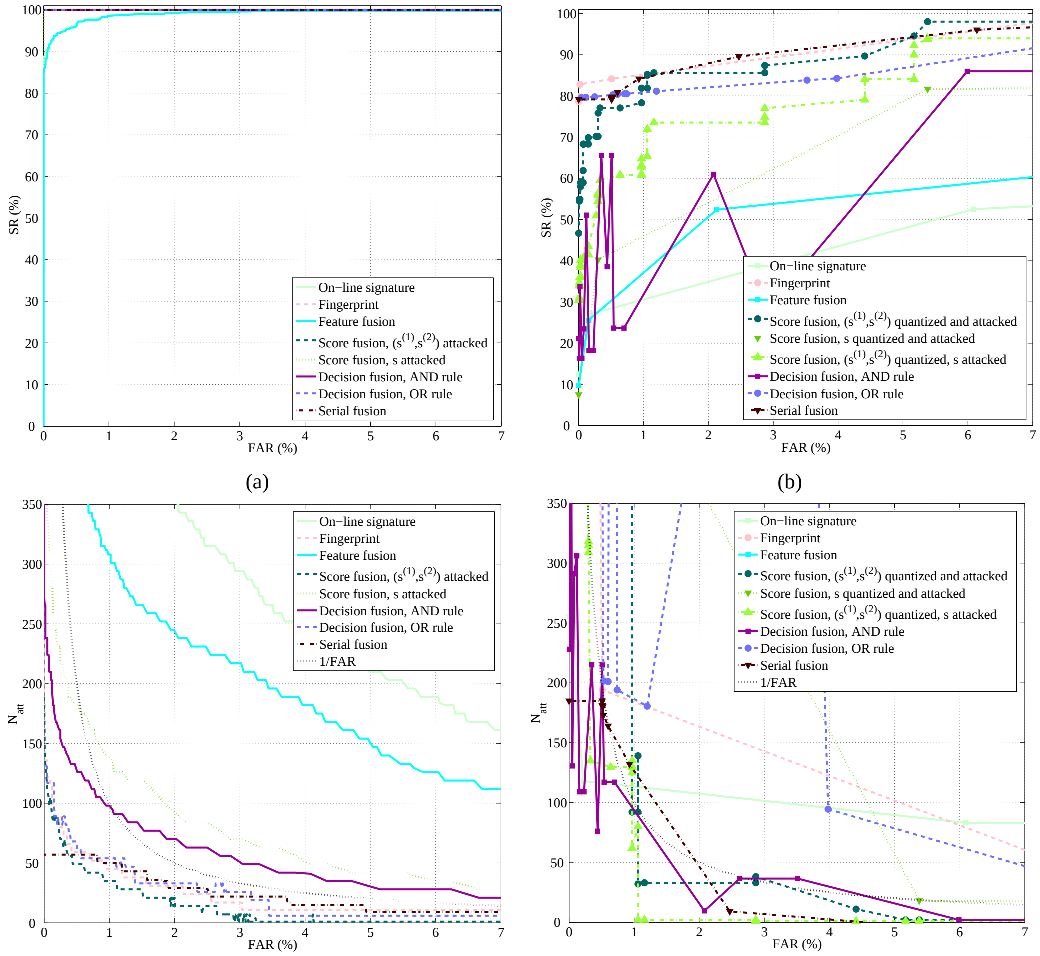
[2] E. Maiorana, P. Campisi, J. Fierrez, J. Ortega-Garcia, and A. Neri, "Cancelable templates for sequence-based biometrics with application to on-line signature recognition," *IEEE Transactions on System Man and Cybernetics Part A*, vol. 40, no. 3, pp. 525–538, 2010.

[3] A. Ross, K. Nandakumar, and A. Jain, *Handbook of Multibiometrics*. Springer, 2006.



(a) (b)

Fig. 12. Recognition accuracy of systems with on-line signatures and fingerprint biometrics (with 72 features). (a): FAR/FRR with unquantized scores; (b): FAR/FRR with quantized scores.



(a) (b)

(c) (d)

Fig. 13. Performance of SPSA hill-climbing attacks against multi-biometrics systems based on on-line signatures and fingerprint biometrics (with 72 features). (a): SR (in %) using unquantized scores; (b): SR (in %) using quantized scores; (c): $\mathrm{N_{att}}$ using unquantized scores; (d): $\mathrm{N_{att}}$ using quantized scores.

[4] M. Martinez-Diaz *et al.*, "Hill-climbing and brute force attacks on biometric systems: a case study in match-on-card fingerprint verification," in *ICCST*, 2006.

[5] R. Rodrigues, N. Kamat, and V. Govindaraju, "Evaluation of biometric spoofing in a multimodal system," in *IEEE BTAS*, 2010.

[6] K. Nandakumar and A. K. Jain, "Multibiometric template security using fuzzy vault," in *IEEE BTAS*, 2008.

[7] D. Muramatsu, "Online signature verification algorithm using hill-climbing method," in *IEEE/IFIP Internation Conference on Embedded and Ubiquitous Computing*, 2008.

[8] C. Rathgeb and A. Uhl, "Online signature verification algorithm using hill-climbing method," in *IEEE ICPR*, 2010.

[9] M. Gomez-Barrero, J. Galbally, P. Tome, and J. Fierrez, "On the vulnerability of iris-based systems to a software attack based on a genetic algorithm," in *CIARP*, 2012.

[10] M. Martinez, J. Fierrez, J. Galbally, and J. Ortega, "An evaluation of indirect attacks and countermeasures in fingerprint verification systems," *Elsevier Pattern Recognition Letters*, vol. 32, no. 12, pp. 1643–1651, 2011.

[11] J. Galbally, J. Fierrez, and J. Ortega, "Bayesian hill-climbing attack and

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIFS.2014.2384735, IEEE Transactions on Information Forensics and Security

its application to signature verification," in *IEEE ICB*, 2007.

[12] M. Gomez-Barrero, J. Galbally, J. Firrez-Aguilar, and J. Ortega-Garcia, "Face verification put to test: A hill-climbing attack based on the uphill-simplex algorithm," in *IEEE ICB*, 2012.

[13] E. Maiorana, G. Hine, and P. Campisi, "Hill-climbing attack: Parametric optimization and possible countermeasures. An application to on-line signature recognition," in *IEEE ICB*, 2013.

[14] E. Maiorana, G. Hine, D. La Rocca, and P. Campisi, "On the vulnerability of an EEG-based biometric system to hill-climbing attacks. algorithms' comparison and possible countermeasures," in *IEEE BTAS*, 2013.

[15] J. Spall, "Implementation of the simultaneous perturbation algorithm for stochastic optimization," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 34, no. 3, pp. 817–823, 1998.

[16] A. R. Conn, K. Scheinberg, and L. N. Vicente, *Introduction to Derivative-Free Optimization*. MPS-SIAM Series on Optimization, 2008.

[17] P. Gilmore and C. Kelley, "An implicit filtering algorithm for optimization of functions with many local minima," *SIAM Journal on Optimization*, vol. 5, pp. 269–285, 1995.

[18] J. Nelder and R. Mead, "A simplex method for function minimization," *Computer Journal*, vol. 7, pp. 313–368, 1965.

[19] R. Hooke and T. Jeeves, "Direct search solution of numerical and statistical problems," *Journal of the ACM*, vol. 8, no. 2, pp. 212–229, 1961.

[20] J.-G. Wang, W.-Y. Yau, A. Suwandya, and E. Sung, "Person recognition by fusing palmprint and palm vein images based on "laplacianpalm" representation," *Elsevier Pattern Recognition*, vol. 41, no. 5, pp. 1514–1527, 2003.

[21] X. Zhou and B. Bhanu, "Feature fusion of side face and gait for video-based human identification," *Elsevier Pattern Recognition*, vol. 41, no. 3, pp. 778–795, 2008.

[22] J. Yang, J. Yang, D. Zhang, and J. Lu, "Feature fusion: parallel strategy vs. serial strategy," *Elsevier Pattern Recognition*, vol. 38, no. 6, pp. 1369–1381, 2003.

[23] B. Biggio, Z. Akthar, G. Fumera, G. Marcialis, and F. Roli, "Robustness of multi-modal biometric verification systems under realistic spoofing attacks," in *IEEE IJCB*, 2011.

[24] S. Prabhakar and A. Jain, "Decision-level fusion in fingerprint verification," *Elsevier Pattern Recognition*, vol. 35, no. 4, pp. 861–874, 2002.

[25] Q. Tao and R. Veldhuis, "Threshold-optimized decision-level fusion and its application to biometrics," *Elsevier Pattern Recognition*, vol. 42, no. 5, pp. 823–836, 2009.

[26] G. Marcialis, F. Roli, and L. Didaci, "Personal identity verification by serial fusion of fingerprint and face matchers," *Elsevier Pattern Recognition*, vol. 42, no. 11, pp. 1076–1088, 2009.

[27] S. Lloyd, "Least squares quantization in PCM," *IEEE Transactions on Information Theory*, vol. 28, no. 2, pp. 129–137, 1982.

[28] J. Fierrez, D. Ramos-Castro, J. Ortega-Garcia, and J. Gonzalez-Rodriguez, "HMM-based on-line signature verification: feature extraction and signature modeling," *Pattern Recognition Letters*, vol. 28, no. 16, pp. 2325–2334, 2007.

[29] J. Fierrez-Aguilar *et al.*, "An on-line signature verification system based on fusion of local and global information," in *AVBPA*, 2005.

[30] E. Maiorana, P. Campisi, and A. Neri, "Feature selection and binarization for on-line signature recognition," in *IEEE ICB*, 2009.

[31] P. Campisi and D. La Rocca, "Brain waves for automatic biometric based user recognition," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 5, pp. 782–800, May 2014.

[32] D. La Rocca, P. Campisi, and G. Scarano, "EEG biometrics for individual recognition in resting state with closed eyes," in *IEEE BIOSIG*, 2012.

[33] P. Campisi, G. Scarano, F. Babiloni, F. D. Fallani, S. Colonnese, E. Maiorana, and L. Forastiere, "Brain waves based user recognition using the "eyes closed resting conditions" protocol," in *IEEE WIFS*, 2011.

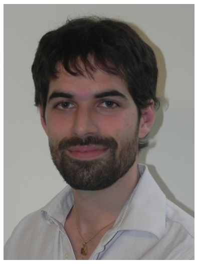
[34] A. Jain, F. Jianjiang, and K. Nandakumar, "Fingerprint matching," *IEEE Computer*, vol. 43, no. 2, pp. 36–44, 2010.

[35] A. Jain, S. Prabhakar, L. Hong, and S. Pankanti, "Filterbank-based fingerprint matching," *IEEE Transactions on Image Processing*, vol. 9, no. 5, pp. 846–859, 2000.

[36] J. Ortega-Garcia *et al.*, "MCYT baseline corpus: A bimodal biometric database," *IEE Proceedings Vision, Image and Signal Processing*, vol. 150, no. 6, pp. 395–401, 2003.

[37] N. Poh and S. Bengio, "Can chimeric persons be used in multimodal biometric authentication experiments?" ser. Lecture Notes in Computer Science, vol. 3869. Springer, 2005, pp. 87–100.

**Emanuele Maiorana** (S'06-M'08) received the Ph.D. degree in telecommunication engineering with European Doctorate Label from the Roma Tre University, Rome, Italy, in 2009. He is the recipient of the Lockheed Martin Best Paper Award for the Poster Track at the IEEE Biometric Symposium 2007, and of the Honeywell Student Best Paper Award at the IEEE Biometrics: Theory, Applications and Systems conference 2008. He was the Program Chair for the 2014 IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications, October 2014, Italy. His research interests are in the area of digital signal and image processing with applications to multimedia communications and security of telecommunication systems. Specifically, he worked on biometric recognition and protection of biometric templates, high dynamic range images imaging and watermarking, synthesis of video textures, and stereo image analysis and enhancement.



**Gabriel Emile Hine** is currently pursuing his Master degree in Communication and Information Technologies Engineering at the Roma Tre University, Rome, Italy. In 2013, he got the Bachelor's degree (cum laude) in Electronic Engineering at the same University, with a thesis in biometric systems security. His research interests are in the area of signal and image processing. Specifically, he has been working on biometrics, 3D ultrasonic imaging, and digital watermarking.

**Patrizio Campisi** (IEEE SM) received the Ph.D. degree in electrical engineering from the Roma Tre University, Rome, Italy, where he is currently a Full Professor with the Section of Applied Electronics, Department of Engineering. His research interests are in the area of secure multimedia communications. Specifically, he has been working on secure biometric recognition, digital watermarking, image deconvolution, image analysis, stereo image and video processing, blind equalization of data signals, and secure data communications. He is the General Chair of the Seventh IEEE Workshop on Information Forensics and Security, WIFS 2015, Novemer 2015, Rome, Italy. He was the General Chair for the 2014 IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications, October 2014, Rome, Italy and of the 12th ACM Workshop on Multimedia and Security, September 2010, Rome, Italy. He was the Technical Co-chair of the 1st ACM Workshop on Information Hiding and Multimedia Security, June 2013, France, and of the Fourth IEEE Workshop on Information Forensics and Security, WIFS 2012, December 2012, Spain. He is the editor of the book Security and Privacy in Biometrics (Springer, 2013). He is coeditor of the book Blind Image Deconvolution: Theory and Applications (CRC Press, 2007). He is corecipient of an IEEE ICIP06 and the IEEE BTAS 2008 Best Student Paper Award and an IEEE Biometric Symposium 2007 Best Paper Award. He is Associate Editor of the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY. He has been an Associate Editor of the IEEE SIGNAL PROCESSING LETTERS. He is currently Senior Associate Editor of the IEEE SIGNAL PROCESSING LETTERS. He is a member of the IEEE Certified Biometric Program Learning System Committee and the IEEE Technical Committee on Information Assurance and Intelligent Multimedia- Mobile Communications, System, Man, and Cybernetics Society. He is IEEE SP Director Student Services (Jan. 2015 - Dec. 2017)