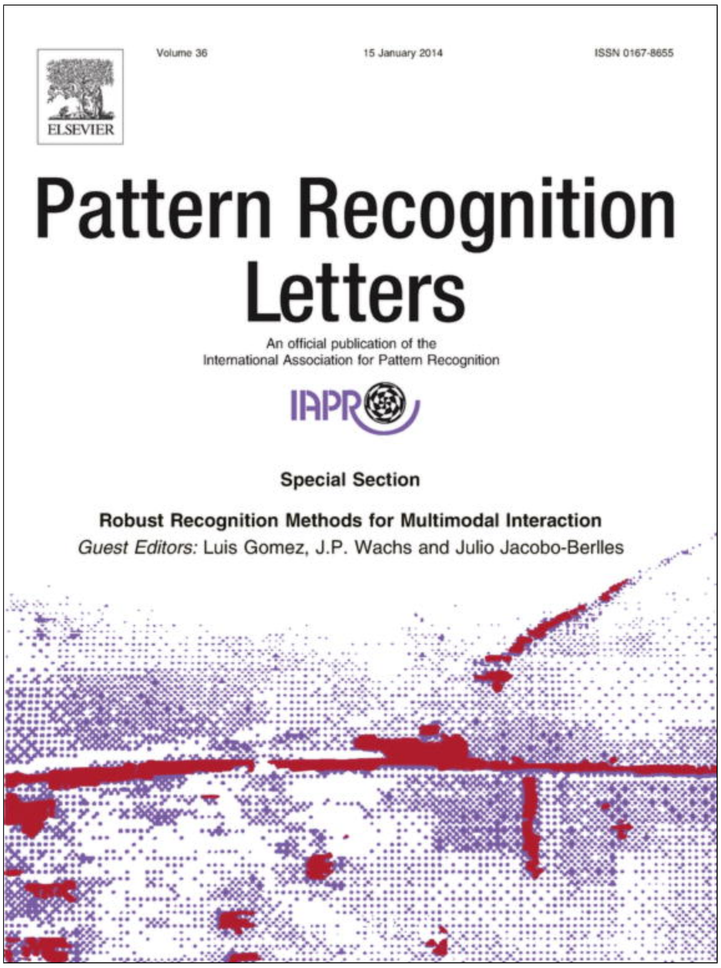


Volume 36 15 January 2014 ISSN 0167-8655

ELSEVIER

Pattern Recognition Letters

An official publication of the
International Association for Pattern Recognition

IAPR

Special Section

Robust Recognition Methods for Multimodal Interaction
Guest Editors: Luis Gomez, J.P. Wachs and Julio Jacobo-Berlles

Pattern Recognition Letters 36 (2014) 243–253

Contents lists available at SciVerse ScienceDirect

Pattern Recognition Letters

journal homepage: www.elsevier.com/locate/patrec

Efficient software attack to multimodal biometric systems and its application to face and iris fusion

Marta Gomez-Barrero [*,1], Javier Galbally [1], Julian Fierrez [1]

Biometric Recognition Group – ATVS, EPS, Universidad Autonoma de Madrid, C/ Francisco Tomas y Valiente 11, 28049 Madrid, Spain

ARTICLE INFO

Article history:
Available online 10 May 2013

Communicated by Luis Gomez Deniz

Keywords:
Multimodal system
Security
Vulnerabilities
Hill-climbing
Countermeasures

ABSTRACT

In certain applications based on multimodal interaction it may be crucial to determine not only *what* the user is doing (commands), but *who* is doing it, in order to prevent fraudulent use of the system. The biometric technology, and particularly the multimodal biometric systems, represent a highly efficient automatic recognition solution for this type of applications.

Although multimodal biometric systems have been traditionally regarded as more secure than unimodal systems, their vulnerabilities to spoofing attacks have been recently shown. New fusion techniques have been proposed and their performance thoroughly analysed in an attempt to increase the robustness of multimodal systems to these spoofing attacks. However, the vulnerabilities of multimodal approaches to software-based attacks still remain unexplored. In this work we present the first software attack against multimodal biometric systems. Its performance is tested against a multimodal system based on face and iris, showing the vulnerabilities of the system to this new type of threat. Score quantization is afterwards studied as a possible countermeasure, managing to cancel the effects of the proposed attacking methodology under certain scenarios.

1. Introduction

Multimodal systems represent a new direction for computing that embraces users' natural behaviour as the center of human–computer interaction (Oviatt and Cohen, 2000). As with any other novel discipline, the research community is just beginning to understand how to design robust and well integrated multimodal systems. But only trough multidisciplinary cooperation among those with expertise in individual component technologies can multimodal systems reach its final aim: building more general and robust systems that will reshape daily computing tasks and have significant commercial impact (Oviatt, 1999).

One of the main areas of research in multimodal interaction, where specific expertise is needed, is *recognition*, generally regarded as a form of processing users' commands. However, for certain applications based on multimodal interaction, a second form of recognition is crucial: it is not only necessary to distinguish *what* the user is doing, but *who* is doing it, so that non-authorized individuals cannot use the system. For these cases, a robust personal automatic recognition solution such as the one provided by *biometrics* is required. Although being relatively young compared to other mature and long-used security technologies, biometrics have emerged in the last decade as a pushing alternative for applications where automatic recognition of people is needed. Certainly, biometrics are very attractive and useful for the final user: forget about PINs and passwords, you are your own key (Jain et al., 2006; Wayman et al., 2005). However, we cannot forget that as any technology aimed to provide a security service, biometric systems are exposed to external attacks which could compromise their integrity (Schneier, 1999). Thus, it is of special relevance to understand the threats to which they are subjected and to analyse their vulnerabilities in order to prevent possible attacks and increase their benefits for the users.

External attacks to biometric systems are commonly divided into: *direct attacks* (also known as *spoofing attacks*), carried out against the sensor, and *indirect attacks*, directed to some of the inner modules of the system. In the last recent years important research efforts have been conducted to study the vulnerabilities of biometric systems to both direct and indirect attacks (Galbally et al., 2010, 2011; Matsumoto, 2004; Uludag and Jain, 2004).

This new concern which has arisen in the biometric community regarding the security of biometric systems has led to the appearance of several international projects, like the European Tabula Rasa (2010), which base their research on the security through transparency principle (Schneier, 2000; Kerckhoffs, 1883): in order to make biometric systems more secure and reliable, their vulnerabilities need to be analysed and useful countermeasures need to be developed.

[*] Corresponding author. Tel.: +34 91 497 33 63.
E-mail addresses: marta.barrero@uam.es (M. Gomez-Barrero), javier.galbally@uam.es (J. Galbally), julian.fierrez@uam.es (J. Fierrez).

[1] This work has been partially supported by projects Contexts (S2009/TIC-1485) from CAM, Bio-Challenge (TEC2009-11186) and Bio-Shield (TEC2012-34881) from Spanish MINECO, TABULA RASA (FP7-ICT-257289) and BEAT (FP7-SEC-284989) from EU, and *Cátedra UAM-Telefónica.*

0167-8655/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.patrec.2013.04.029

In this scenario, biometric multimodality has been regarded as an effective way of increasing the robustness of biometric-based security systems to external attacks. Combining the information offered by several traits would force an eventual intruder to successfully break several unimodal modules instead of just one. However, it has already been proven that this is not necessary in spoofing attacks: breaking into the module based on the most accurate biometric trait grants access to the multimodal system in many occasions (Akhtar et al., 2011; Chetty and Wagner, 2005; Rodrigues et al., 2009).

In addition to research works which address the vulnerabilities of multimodal systems to spoofing attacks (Akhtar et al., 2011; Chetty and Wagner, 2005; Rodrigues et al., 2009, 2010; Akhtar and Alfarid, 2011; Hämmerle-Uhl et al., 2011; Johnson et al., 2010; Marasco, 2010), different studies may be found in the literature regarding the analysis of indirect attacks against unimodal systems (Galbally et al., 2010; Uludag and Jain, 2004; Martinez-Diaz et al., 2011). However, the problem of whether multimodal approaches are vulnerable or not to software-based attacking methodologies still remains unexplored.

In the present work we propose and analyse a general multimodal indirect attack, which can be used to study the vulnerabilities of biometric systems based on different number of traits, different fusion strategies and different types of templates (e.g., real valued, binary). Without loss of generality, the attack is applied to the particular case of a face- and iris-based recognition system. This trait combination is regarded as one of the most popular and user-friendly, since the acquisition of both traits can be transparent to the user (Wang et al., 2003; Zhang et al., 2010; Gan and Liu, 2009; Gan and Liang, 2006). This provides a straight-forward integration of both modalities, a complex topic on multimodal computation (Oviatt et al., 2003). Furthermore, the experimental protocol used is fully replicable, so that the results obtained can be fairly compared.

Score quantization is studied afterwards as a possible countermeasure against the proposed attack. Two different approaches are analysed: quantizing the score before and after the fusion of the partial face and iris scores. While the second scheme barely reduces the success rate and efficiency of the attack, the first one succeeds in preventing an intruder from breaking into the system.

Thus, following the same transparency principle which is starting to prevail in the biometric community through European Projects such as Tabula Rasa (Schneier, 2000; Kerckhoffs, 1883), the main objectives and contributions of the present work are: (*i*) proposal of a fully novel software-based attacking methodology against multimodal systems, (*ii*) study of the vulnerabilities of a realistic multimodal system to the previous attack under a replicable scenario, (*iii*) comparison of the performance of the attack to that obtained against the unimodal modules in order to determine if the multimodal approach increases the security of the system against this type of threat, and (*iv*) study of some biometric-based countermeasures which may prevent such an attack.

The paper is structured as follows. Related works are summarised in Section 2. The novel multimodal attacking algorithm used to evaluate the system is presented in Section 3. Then the multimodal verification system evaluated is described in Section 4. The database and experimental protocol followed are presented in Section 5. In Section 6 we describe and analyse the results obtained. Score quantization is studied as a possible countermeasure in Section 7. Conclusions are finally drawn in Section 8.

2. Related works

In 2001, Ratha et al. identified and classified in a biometric recognition system eight possible points of attack (Ratha et al., 2001). These vulnerable points can be broadly divided into direct and indirect attacks.

2.1. Direct attacks

Also known as spoofing-attacks, these are attacks at the sensor level, carried out with synthetic biometric traits, such as gummy fingers or high quality printed iris images, and thus requiring no knowledge for the attacker of the inner parts of the system (matching algorithm used, feature extraction method, template format, etc.) Some research regarding the vulnerabilities of multimodal systems to these attacks has been carried out over the last recent years: in 2005, Chetty and Wagner (2005) tested the performance of spoofing attacks against a novel multimodal system based on face and voice; in 2009, Tan (2009) investigated methods for increasing the security of multimodal systems based on face and voice against spoofing attacks; in 2010, Rodrigues et al. (2010) and 2011, Rodrigues et al. (2009), evaluated the vulnerabilities of a multimodal system based on face and fingerprint, using different fusion techniques and proposing new ones; in Johnson et al. (2010) analysed the effect of spoofing attacks against a multimodal system based on face and iris, proposing a method for the vulnerabilities assessment of these systems; later in 2010, Marasco (2010) analysed the security risks in multimodal biometric systems based on face and fingerprint coming from spoofing attacks; in 2011, Akhtar et al. (2011) and Akhtar and Alfarid (2011) used real rather than simulated spoof samples for the evaluation of the vulnerabilities of a multimodal system based on fingerprint, face and iris, proposing a new learning algorithm able to improve the security offered by the system against spoofing attacks. All these works have proven that combining several traits in one system for person authentication does not necessarily increment the security offered against spoofing attacks, since the system can be bypassed by breaking only one of the unimodal traits.

2.2. Indirect attacks

These attacks are directed to the inner modules of the system and can be further divided into three groups, namely: (*i*) attacks to the communication channels between modules of the system, extracting, adding or changing information; (*ii*) attacks to the feature extractor and the matcher may be carried out using a Trojan Horse that bypasses the corresponding module; and (*iii*) attacks to the system database which manipulate it in order to gain access to the application, by changing, adding or deleting a template. While for direct attacks the intruder needed no knowledge about the inner modules of the system, this knowledge is a main requisite here, together with access to some of the system components (database, feature extractor, matcher, etc.). Most of these indirect attacks are based on some variation of a hill-climbing algorithm, consisting on iteratively changing some synthetically generated templates until access to the system is granted. Even though some research has been done in this area using unimodal systems (Galbally et al., 2010; Uludag and Jain, 2004; Martinez-Diaz et al., 2011; Adler, 2004), to the best of our knowledge there is no previous analysis of the vulnerabilities of multimodal biometric systems to this kind of attacks.

3. Proposed attack

Until now, only the vulnerabilities of unimodal systems to indirect attacks have been analysed. In this section we present the first algorithm for the evaluation of the vulnerabilities of multimodal systems to this type of threat. As can be observed in Fig. 1 (top), the input to the algorithm are the scores given by the matcher, and the output the templates to be compared to the client account.

For simplicity, the attacking methodology is described here for the particular case of a multimodal system based on the score fusion of a real valued (e.g. face) and a binary (e.g. iris) matcher. However, the proposed approach is general and may be applied with very small modifications to attack multimodal systems working on: (*i*) more than two traits represented with real-valued or binary templates (by adding new blocks after the switch in Fig. 1), or (*ii*) feature-based fusion strategies (by rearranging the template disposition).

In order to attack a multimodal biometric system where one of the biometric traits is represented with real values and the other is binary (most iris recognition systems work on binary templates), the algorithm here presented combines two sub-algorithms. Each of them attacks one segment of the template: the real-valued or the binary segment. In the following subsections, each of the individual sub-algorithms is described. Finally, the multimodal attacking algorithm based on the previous two models is presented.

3.1. Sub-Algorithm 1: hill-climbing based on the Uphill Simplex Algorithm

3.1.1. Problem statement

Consider the problem of finding a K-dimensional vector of real values x_{face} which, compared to an unknown template $\mathcal{C}_{\text{face}}$ (in our case related to a specific client), produces a similarity score bigger than a certain threshold δ_{face}, according to some matching function J_{face}, i.e., $J_{\text{face}}(\mathcal{C}_{\text{face}}, x_{\text{face}}) > \delta_{\text{face}}$. The template can be another K-dimensional vector or a generative model of K-dimensional vectors.

3.1.2. Assumptions

Let us assume:

- That there exists a statistical model G (K-variate Gaussian with mean $\boldsymbol{\mu}_G$ and a diagonal covariance matrix $\boldsymbol{\Sigma}_G$, with $\boldsymbol{\sigma}_G^2 = \text{diag}(\boldsymbol{\Sigma}_G)$), in our case related to a background set of users, overlapping to some extent with $\mathcal{C}_{\text{face}}$.
- That we have access to the evaluation of the matching function $J_{\text{face}}(\mathcal{C}_{\text{face}}, x_{\text{face}})$ for several trials of x_{face}.

3.1.3. Algorithm

The problem stated above can be solved by adapting the Downhill Simplex algorithm first presented in Nelder and Mead (1965) to maximize instead of minimize the function J_{face}. We iteratively form new simplices by reflecting one point, x^l_{face}, in the hyperplane of the remaining points, until we are close enough to the maximum of the function. The point to be reflected will always be the one with the lowest value given by the matching function, since it is in principle the one furthest from our objective. Thus, as can be observed in Fig. 2, the different steps followed by the sub-Algorithm 1 are:

1. Compute the statistical model $G(\boldsymbol{\mu}_G, \boldsymbol{\sigma}_G)$ from a development pool of users.
2. Take $K+1$ samples (x^i_{face}) defining the initial simplex from the statistical model G and compute the similarity scores $J_{\text{face}}(\mathcal{C}_{\text{face}}, x^i_{\text{face}}) = s^i_{\text{face}}$, with $i = 1, \ldots, K+1$.
3. Compute the centroid $\bar{x}_{\text{face}}$ of the simplex as the average of $x^i_{\text{face}} : \bar{x}_{\text{face}} = \frac{1}{K+1}\sum_i x^i_{\text{face}}$.
4. Reflect the point x^l_{face} according to the next steps, adapted from the Downhill Simplex algorithm (Nelder and Mead, 1965). In the following, the indices l and h are defined as $h = \arg\max_i(s^i_{\text{face}}),\ l = \arg\min_i(s^i_{\text{face}})$.
    (a) *Reflection*: Given a constant $\alpha > 0$, the *reflection coefficient*, we compute:

$$a = (1+\alpha)\bar{x}_{\text{face}} - \alpha x^l_{\text{face}}.$$

Thus, a is on the line between x^l_{face} and $\bar{x}_{\text{face}}$ being α the ratio between the distances $[a\bar{x}_{\text{face}}]$ and $[x^l_{\text{face}}\bar{x}_{\text{face}}]$. If $s^l_{\text{face}} < s^a_{\text{face}} < s^h_{\text{face}}$ we replace x^l_{face} by a. Otherwise, we go onto step 4b.

(b) *Expansion or contraction.*

i. *Expansion*: If $s^a_{\text{face}} > s^h_{\text{face}}$ (i.e., we have a new maximum) we expand a to b as follows:

$$b = \gamma a + (1-\gamma)\bar{x}_{\text{face}},$$

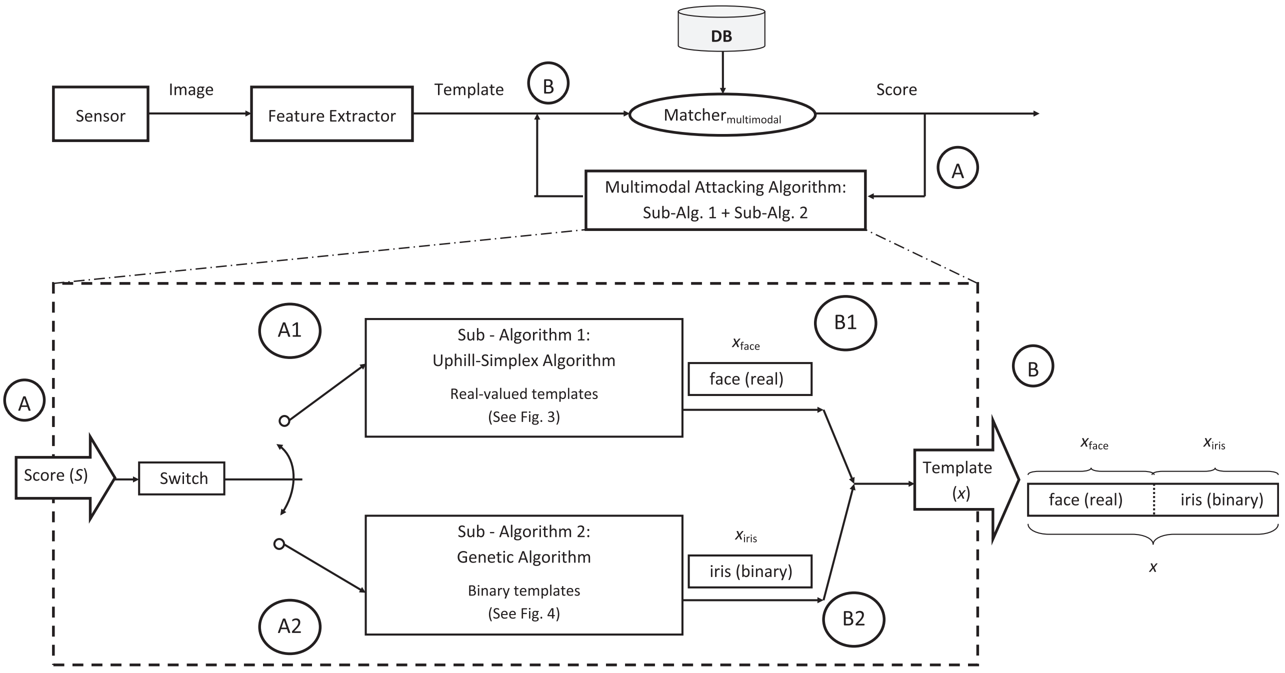


Fig. 1. Diagram of a general hill-climbing attack (top), with the specific modification scheme for the combined algorithm (bottom).

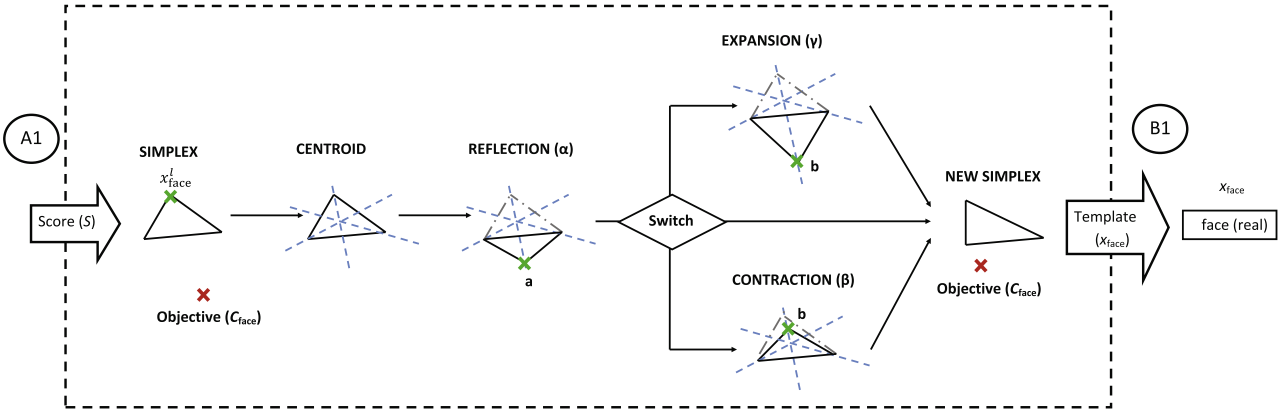


Fig. 2. Diagram of the modification scheme for the Sub-Algorithm 1, based on the Uphill-Simplex.

where $\gamma > 1$ is another constant called *expansion coefficient*, which represents the ratio between the distances $[b\bar{x}_{\text{face}}]$ and $[s\bar{x}_{\text{face}}]$. If $s^b_{\text{face}} > s^h_{\text{face}}$, we replace x^l_{face} by b. Otherwise, we have a failed expansion and replace x^l_{face} by a.

ii. *Contraction*: If we have reached this step, then $s^a_{\text{face}} \leqslant s^l_{\text{face}}$ (i.e. replacing x^l_{face} by **a** would leave s^a_{face} as the new minimum). We compute

$$b = \beta x^l_{\text{face}} + (1 - \beta)\bar{x}_{\text{face}},$$

where $0 < \beta < 1$ is the *contraction coefficient*, defined as the ratio between the distances $[b\bar{x}_{\text{face}}]$ and $[x^l_{\text{face}}\bar{x}_{\text{face}}]$. If $s^b_{\text{face}} > \max(s^l_{\text{face}}, s^a_{\text{face}})$, then we replace x^l_{face} by b; otherwise, the contracted point is worse than x^l_{face}, and for such a failed contraction we replace all the x^i_{face}'s by $(x^i_{\text{face}} + x^h_{\text{face}})/2$.

5. With the new x^l_{face} value, update the simplex and return to step 3.

3.1.4. Stopping criteria

The algorithm stops when: (*i*) the maximum similarity score of the simplex vertices is higher than the threshold δ_{face} (i.e., the account is broken), (*ii*) the variation of the similarity scores obtained in a number of iterations is lower than a certain threshold or (*iii*) a maximum number of iterations is reached.

3.1.5. Additional note

It is important to notice for the computation of the Efficiency (defined in Section 5.3) of this sub-algorithm that at each iteration (except for the initial one) a maximum of 2 matchings will be performed (i.e., s^a_{face} + s^b_{face}). On average, the number of matchings computed per iteration will be lower than 2 and greater than 1.

The hill-climbing based on the Uphill Simplex algorithm was first presented in Gomez-Barrero et al. (2011), where it was used to successfully attack a signature verification system. The performance of the proposed algorithm showed a clear improvement in the attacking capabilities with respect to previously proposed state-of-the-art approaches, which motivated its choice for the present multimodal vulnerability study.

3.2. Sub-Algorithm 2: indirect attack based on a genetic algorithm

3.2.1. Problem statement

Consider the problem of finding an L-dimensional binary vector x_{iris} which, compared to an unknown template $\mathcal{C}_{\text{iris}}$ (in our case related to a specific client), produces a similarity score bigger than a certain threshold δ_{iris}, according to some matching function J_{iris}, i.e., $J_{\text{iris}}(\mathcal{C}_{\text{iris}}, x_{\text{iris}}) > \delta_{\text{iris}}$. The template can be another L-dimensional vector or a generative model of L-dimensional vectors.

3.2.2. Assumptions

Let us assume:

- That we have access to the evaluation of the matching function $J_{\text{iris}}(\mathcal{C}_{\text{iris}}, x_{\text{iris}})$ for several trials of x_{iris}.

3.2.3. Algorithm

The problem stated above may be solved by using a genetic algorithm, which has shown a remarkable performance in binary optimization problems (Brindle, 1981), to optimize the similarity score given by the matcher, that is, the fitness value for an individual is $s_{\text{iris}} = \mathcal{J}_{\text{iris}}(x_{\text{iris}}, \mathcal{C}_{\text{iris}})$. As can be seen in Fig. 3 the steps followed by the sub-Algorithm 2 are:

1. Generate an initial population P_i with N individuals of length L, L being the length of the iris code.
2. Compute the similarity scores s^i of the individuals (x^i_{iris}) of the population $P_i, s_i = J(x^i_{\text{iris}}, \mathcal{C}_{\text{iris}})$ with $i = 1, \ldots, N$.
3. Four rules are used at each iteration to create the next generation P_n of individuals from the current population:
   (a) *Elite*: the two individuals with the maximum similarity scores are kept unaltered for the next generation.
   (b) *Selection*: certain individuals, the *parents*, are chosen by stochastic universal sampling (Baker, 1987). This way, the individuals with the highest fitness values (similarity scores) are more likely to be chosen as parents for the next generation: one subject can be selected from 0 to many times. From the original N individuals, $N/2 - 1$ *fathers* and $N/2 - 1$ *mothers* are chosen.
   (c) *Crossover*: parents are combined to form the $N - 2$ *children* of the next generation, following a scattered crossover method. A random binary vector is created and the genes (bits) of the child are selected from the first parent where the value of the random vector is 1, and from the second when it is 0 (vice versa for the second child).
   (d) *Mutation*: random changes are applied to the bit values of the new children with a mutation probability p_m.
4. Redefine $P_i = P_n$ and return to step 2.

3.2.4. Stopping criteria

The algorithm stops when: (*i*) the best fitness score is higher than the threshold δ_{iris} (i.e., the account is broken), (*ii*) the variation of the similarity scores obtained in a number of generations is

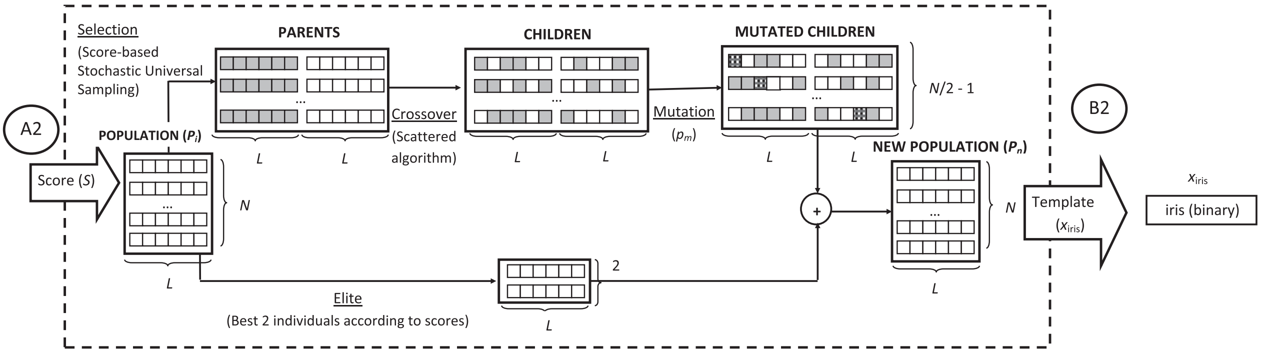


Fig. 3. Diagram of the modification scheme for the Sub-Algorithm 2, based on a Genetic Algorithm.

lower than a previously fixed value, or (*iii*) when the maximum number of generations is reached.

3.2.5. Additional note

It is important to notice for the computation of the Efficiency (defined in Section 5.3) of this sub-algorithm that at each iteration (i.e., generation) N matchings are performed (one for each of the members of the population).

This particular implementation of a genetic algorithm was first presented in Gomez-Barrero et al. (2012), where it was used to analyse the vulnerabilities of the same iris recognition system considered in this work. The performance of the proposed algorithm showed a very high attacking potential with very encouraging results and was the first one, to our knowledge, working on a binary input (such as the iriscodes). Therefore, its use as part of the global multimodal attack presented here seemed like a promising choice.

3.3. Multimodal attack: combination of Sub-Algorithms 1 (Uphill-Simplex) and 2 (Genetic-Algorithm)

3.3.1. Problem statement

Consider the problem of finding a $(K+L)$-dimensional vector x of real and binary values which, compared to an unknown template $\mathcal{C}$ (in our case related to a specific client), produces a similarity score bigger than a certain threshold δ, according to some matching function J, i.e., $J(\mathcal{C},x) > \delta$. The template can be another $(K+L)$-dimensional vector or a generative model of $(K+L)$-dimensional vectors.

3.3.2. Assumptions

Let us assume:

- That we know the distribution of the two subtemplates (real-valued x_{face} and binary x_{iris}) within the multimodal template x.
- That we have access to the evaluation of the matching function $J(\mathcal{C},x)$ for several trials of x.

3.3.3. Algorithm

The problem stated above may be solved by dividing the template x into its real-valued (x_{face}) and binary parts (x_{iris}) and alternately optimize each of them as can be seen in Fig. 1. In order to optimize each of the parts, the algorithms described in the previous subsections are used: the Sub-Algorithm 1 for the real-valued segment (face) and the Sub-Algorithm 2 for the binary segment (iris). Thus, the steps followed are:

1. Generate a synthetic template (x) randomly initializing the real-valued (x_{face}) and binary (x_{iris}) segments, and compute the similarity score $S = J(\mathcal{C},x)$, which will be used as optimization criterion.
2. Leaving one of the segments unaltered, optimize the other segment of the template using the appropriate sub-algorithm until one of the stopping criteria of the sub-algorithm is fulfilled.
3. Change the optimization target to the segment which was previously left unaltered and go back to step 2.

3.3.4. Stopping criteria

The algorithm stops when: (*i*) the verification threshold is reached (i.e., access to the system is granted) or (*ii*) the total number of iterations (i.e., changes between the optimized segments) exceeds a previously fixed value (i.e., the attack has failed).

3.3.5. Additional note

As will be analysed in the experimental section this algorithm may present different results depending on whether it starts attacking the real-valued or binary part of the template.

It is very important to notice that the multimodal attacking algorithm does not have access at any point to the partial scores of the unimodal modules (s_{face} and s_{iris}) but only uses the final fused score given by the system (S). This way, in the description of the previous two sub-algorithms, s_{face} ad s_{iris} should be changed by S when they are used as part of the multimodal attack and not individually.

Both attacking sub-algorithms stop when the improvement of the final multimodal score saturates (i.e., the variation of the multimodal similarity scores obtained in a number of iterations or generations is lower than a certain threshold). This “switching” methodology is preferred over a “sequential” approach based on the assumption that once the algorithm has saturated attacking one of the unimodal subsystems, further changes in the other modality will lead to new improvements in the final multimodal score.

4. Multimodal verification system attacked

The multimodal verification system evaluated in this work is the fusion of two unimodal systems, namely: (*i*) a modified version of the iris recognition system developed by Masek and Kovesi (2003),[2] which is widely used in many iris related publications; and (*ii*) an Eigenface-based face verification system (Turk and Pentland, 1991), used to present initial face verification results for the recent Face Recognition Grand Challenge (Phillips et al., 2005).

[2] The source can be freely downloaded from www.csse.uwa.edu.au/pk/studentprojects/libor/sourcecode.html.

4.1. Face verification system

The system evaluated uses Multi-Layer Perceptron (MLP) and a cascade of Haar-like classifiers in order to segment the faces in the images, together with the position of the eyes on them. Principal Component Analysis (PCA) is used afterwards so that face images can be represented in a lower dimensional space (Galbally et al., 2010). 80% of the variance is retained when training the PCA vector space with cropped face images of size 64 × 80, reducing the original 5120-dimensional space to only 100 dimensions or eigenvectors.

Finally, the similarity scores are computed in this PCA vector space using the Euclidean distance.

4.2. Iris verification system

The system comprises four different steps, namely: (*i*) *segmentation*, where the method proposed in Ruiz-Albacete et al. (2008) is followed, modelling the iris and pupil boundaries as circles; (*ii*) *normalization*, using a technique based on Daugman's ruber sheet model that maps the segmented iris region into a 2D array (Daugman, 2004); (*iii*) *feature encoding*, which produces a binary template of $20 \times 480 = 9600$ bits and the corresponding noise mark (representing the eyelids areas) by convolving the normalized iris patter with 1D Log-Gabor wavelets; and (*iv*) *matching*, where the inverse of a modified Hamming distance is used, which takes into account the noise mask bits.

This way, the similarity score between two templates is computed as $1/HD$ (so that a higher score implies a higher degree of similarity):

$$HD = \frac{\sum_{j=1}^{L} X_j (XOR) Y_j (AND) \bar{X}n_j (AND) \bar{Y}n_j}{L - \sum_{k=1}^{L} Xn_k (OR) Yn_k}$$

where X_j and Y_j are the two bitwise templates to compare, Xn_j and Yn_j are the corresponding noise masks for X_j and Y_j, and L is the number of bits comprised in each template. $\bar{X}n_j$ denotes the logical not operation applied to Xn_j.

4.3. Multimodal verification system

Given an input vector x, the system performs the following tasks in order to obtain the final score, S, as can be seen in Fig. 4:

1. Compute the similarity scores obtained by the face (s_{face}) and iris (s_{iris}) traits, as given by the matchers described in Sections 4.1 and 4.2.
2. Normalize the scores s_k, with $k = \{\text{face}, \text{iris}\}$, using hyperbolic tangent estimators (its robustness and high efficiency are proven in Jain et al. (2005)):

$$s'_k = \frac{1}{2}\left\{\tanh\left(0.01\frac{s_k - \mu}{\sigma}\right) + 1\right\}$$

where s_k is the original similarity score obtained by the iris (respectively face) section of the template, μ and σ the mean and standard deviation of the scores distribution of the iris (respectively face), and s'_k the normalised score. This way, both partial scores (face and iris) lie in the interval $[0,1]$.

3. Finally, both normalised scores are fused with a sum, given the very good results that this fusion rule has presented even when compared with more sophisticated methods like decision trees (Ross and Jain, 2003) or neural networks (Wang et al., 2003):

$$S = s'_{\text{iris}} + s'_{\text{face}}$$

There may be other fusion strategies that can improve the performance of the multimodal system. However, simple summation gives very good results, and it is not the scope of the paper to find the optimal fusion strategy.

5. Database and experimental protocol

Prior to any vulnerability assessment study a performance evaluation of the systems being attacked should be carried out. The performance evaluation will permit to determine how good is the system and, more important, the operating points where it will be attacked as the success chances of this kind of attacking algorithms are, in principle, highly dependent on the False Acceptance and False Rejection rates of the system. While the FRR measures the probability of rejecting a genuine user, the FAR gives a measure of the probability of an impostor being taken as a genuine user. Therefore, in general, the higher the FAR, the easier for an eventual attacker to break into the system. Moreover, for the particular case of the proposed method, attacking the system at a lower FAR implies reaching a higher threshold, which leads to a decrease on the success chances of the algorithm.

Furthermore, defining the operating points will enable us to compare, in a more fair fashion, the vulnerabilities of the different systems to the same attack (i.e., we can determine for a given FAR or FRR which of them is less/more robust to the attacking approach).

Both the database and the protocol used for the performance and security evaluations of the multimodal system are the same ones used for the evaluation of the unimodal subsystems, so that the results are fully comparable. This way, we will be able to determine whether the multimodality enhances the system security against the proposed attacking approaches with respect to the unimodal traits.

5.1. Database

The experiments are carried out on the face and iris subcorpora included in the Desktop Dataset of the multimodal BioSecure database (Ortega-Garcia et al., 2010), which comprises voice, fingerprints, face, iris, signature and hand of 210 users, captured in two time-spaced acquisition sessions. This database was acquired thanks to the joint effort of 11 European institutions and has become one of the standard benchmarks for biometric performance and security evaluations (Mayoue et al., 2009). It is publicly available through the BioSecure Foundation.[3]

The database comprises three datasets captured under different acquisition scenarios, namely: (*i*) Internet Dataset (DS1, captured through the Internet in an unsupervised setup), (*ii*) Desktop Dataset (DS2, captured in an office-like environment with human supervision), and (*iii*) the Mobile Dataset (DS3, acquired on mobile devices with uncontrolled conditions). The face subset used in this work includes four frontal images (two per session) with an homogeneous grey background, and captured with a reflex digital camera without flash ($210 \times 4 = 840$ face samples), while the iris subset includes four grey-scale images (two per session as well) per eye, all captured with the Iris Access EOU3000 sensor from LG. In the experiments only the right eye of each user has been considered, leading this way as in the face case to $210 \times 4 = 840$ iris samples.

5.2. Performance evaluation

As the iris and face subcorpus present identical sample distributions, the protocol followed for the performance evaluation of the unimodal modules and the multimodal system is the same. As can

[3] http://biosecure.it-sudparis.eu/AB.

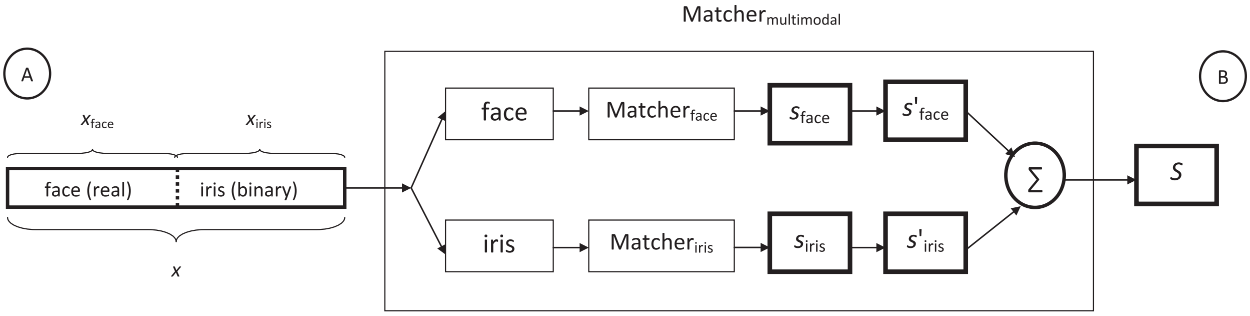
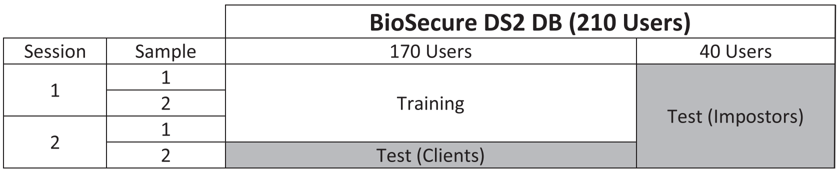


Fig. 4. Similarity score obtained from one multimodal template (x) consisting of two different segments, containing: face features (x_{face}, real values) and the iris code (x_{iris}, binary). The unimodal verification subsystems give the corresponding scores (s_{face}, s_{iris}), which are then normalised (s'_{face}, s'_{iris}) and fused to obtain the final output of the global system: S.



		BioSecure DS2 DB (210 Users)	
Session	Sample	170 Users	40 Users
1	1	Training	Test (Impostors)
	2		
2	1		
	2	Test (Clients)	

Fig. 5. Partition of the BioSecure DS2 DB according to the performance evaluation protocol defined.

Table 1
EER of the unimodal and multimodal systems, based on face and iris, before and after the normalization of the scores.

	EER (%)		
	Face	Iris	Multimodal
Before norm.	6.55	4.11	–
After norm.	6.61	4.04	0.83

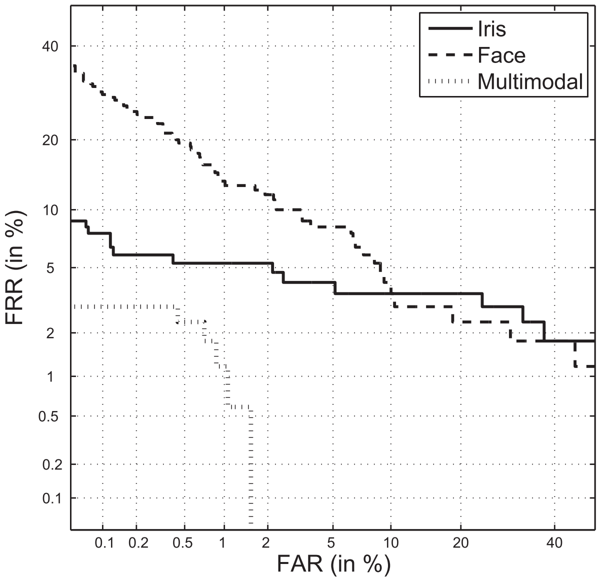


Fig. 6. DET curves of the unimodal and multimodal systems.

be seen in Fig. 5, each subcorpus of the database is divided in two sets, namely: (i) a training set comprising the first three samples of 170 clients, used as the enrolment templates; (ii) a test set formed by the fourth image of the 170 clients above (used to compute the genuine scores) and the 4 images of the remaining 40 users (used to compute the impostor scores).

As a result of: (i) using the same subjects for PCA training and client enrolment for the face verification subsystem, and (ii) manually segmenting those eyes that were not successfully segmented automatically (3.04%), the system performance is optimistically biased, and therefore harder to attack than in a practical situation (in which the enrolled clients may not have been used for PCA training and the image segmentation would be fully automatic). This means that the results presented in this paper are a conservative estimate of the attack's performance.

The final score given by the system is the average of the scores obtained after matching the input template to the three face and iris templates of the client model $\mathcal{C}$. Table 1 shows that the ERR of the unimodal face and iris modules and of the whole multimodal system computed according to the protocol described above. In this chart we can observe that: (i) the performance of the unimodal modules is not noticeably affected by score normalization (i.e., the EER barely changes after normalising the scores), and (ii) the performance of the multimodal system (0.83% EER) clearly improves that of the unimodal systems (4% and 6% respectively). In Fig. 6 the Detection Error Tradeoff (DET) curves of the unimodal and multimodal systems obtained using the described protocol are shown. As can be seen, the multimodal system clearly outperforms both unimodal systems at all points.

5.3. Experimental protocol for the attacks

The user accounts to be attacked by the algorithm are generated with the training set defined in the performance evaluation protocol (i.e., the first three samples of the 170 users in Fig. 5). The performance of the attack is evaluated in terms of: (i) its Success Rate (SR) or expected probability of bypassing the system, computed as the ratio $\mathrm{SR} = A_B/A_T$, where A_B is the number of broken accounts and A_T is the total number of attacked accounts; and (ii) its Efficiency (Eff), or inverse of the average number of comparisons needed to break an account, $\mathrm{Eff} = 1/\left(\sum_{i=1}^{A_B} n_i/A_B\right)$, where n_i is the number of comparisons made to bypass the ith account, with $i = 1, \ldots, A_B$.

It has to be emphasized that the Eff is computed in terms of the number of *matchings* performed by the attacking algorithm and not according to the number of *iterations* needed (i.e., two algorithms performing the same number of iterations to break an account do not necessarily have the same Eff).

The SR gives an estimation of how dangerous the attack is: the higher the SR, the bigger the threat. On the other hand, the Eff tells us how easy it is for the attack to bypass the system in terms of speed: the higher the Eff, the faster the attack.

The different attacks have been evaluated at three operating points which correspond to FAR = 0.1%, FAR = 0.05% and FAR = 0.01%, which, according to ANSI (2001), offer a low, medium and high security level.

6. Results: attack performance

The objectives of this first study of the vulnerabilities of a multimodal system to an indirect attack are: (*i*) to evaluate the performance of the proposed attacking methodology, and (*ii*) to test whether the use of two different biometric traits increments the security level and robustness of the system to this kind of attacks.

In the first set of experiments, the performance of the two attacking sub-algorithms against the unimodal systems is studied, so that later a comparison between the unimodal and the multimodal systems can be established. In the second set, the performance of the attack against the multimodal system is tested. Score quantization is afterwards analysed as a possible countermeasure, studying its impact in the SR and the Eff of the multimodal attacking scheme.

6.1. Sub-Algorithm 1 vs face verification system

The performance of the Sub-Algorithm 1 against the unimodal system based on eigenfaces is tested at the three operating points mentioned before, namely: (*i*) FAR = 0.10%, (*ii*) FAR = 0.05%, (*iii*) FAR = 0.01%. The results of the experiments are detailed in Table 2, where we can observe that the algorithm successfully breaks all the attacked accounts. Also worth noting that for this attack the efficiency remains almost invariant, regardless of the operating point considered.

It should also be emphasized that in the present work the hill-climbing attack is initialized from a normal distribution of zero mean and unit variance, that is, the first simplex is generated without needing any training faces, contrary to what happened in other state of the art attacking methods (Galbally et al., 2010). Furthermore, the parameters α, β and γ used here are the same that were optimized in Gomez-Barrero et al. (2011) to break a signature verification system, which proves the robustness of the algorithm: it is able to break totally heterogeneous systems working on different biometric traits without adjusting its parameters.

6.2. Sub-Algorithm 2 vs iris verification system

As before, the performance of the Sub-Algorithm 2 against the unimodal system based on iris is tested at the three operating points mentioned before, namely: (*i*) FAR = 0.10%, (*ii*) FAR = 0.05%, (*iii*) FAR = 0.01%. The results of the experiments are also shown in Table 2, where we can observe that the algorithm is able to successfully break more than 90% of the accounts for the point of operation corresponding to a low security level, and more than 60% for the point corresponding to a high security level. As in the previous case the efficiency of the attack remains almost invariant, slightly decreasing, as would be expected, for higher security points where the attack needs more iterations to break the system (i.e., it becomes slower).

6.3. Combined attack vs multimodal system

We run two sets of experiments, namely: (*i*) the algorithm starts attacking the face section of the template (Sub-Algorithm 1), and (*ii*) the algorithm starts attacking the iris section (Sub-Algorithm 2). Between 40% and 60% of the times that the algorithm starts attacking the iris section of the template it is able to break the account without changing to the face segment. This does not happen when the algorithm starts attacking the face segment. This way, as it was already proven for spoofing attacks in Akhtar et al. (2011), Rodrigues et al. (2009) and Johnson et al. (2010), attacking only the best individual matcher (i.e., the unimodal system with the lowest EER, the iris one in our case) grants in many cases access to the system under attack.

Secondly, in Table 2 we also show the results obtained by the multimodal approach when it starts attacking the face segment (randomly initializing the iris section) or iris segment (randomly initializing the face section). As can be observed, in both cases the SR is as high as 100% for all the operating points tested. However, the Eff of the attack decreases about 25% when starting with the Sub-Algorithm 2 (Genetic Algorithm) compared to the case of starting with the Sub-Algorithm 1 (Uphill-Simplex). The reason lies on the Eff of the individual Sub-Algorithms. On the left columns of Table 2 (Unimodal Attacks) we can observe that the Eff of the Sub-Algorithm 1 is between 15 and 20 times higher than the Eff of Sub-Algorithm 2 (for a similar number of iterations performed to break an account the number of matchings carried out is significantly higher for the binary attack as was presented in Sections 3.1 and 3.2). When the multimodal algorithm starts attacking the iris segment, in many occasions it is able to break the system without changing to the face segment. This way, the multimodal attacking algorithm can not benefit from the higher Eff of the Sub-Algorithm 1, and has a lower Eff than that achieved when the attack is started against the face section.

From the previous observations none of the two main vulnerability scenarios considered for the multimodal attack is clearly better than the other. On the one hand, when it starts attacking the face segment, it is faster but it needs to use both sections of the template to break the system (i.e., face and iris). On the other hand, when it starts attacking the iris segment, it becomes slower but it has a good chance of gaining access to the system using just one of the template sections (i.e., iris) with the advantage that this may entail in terms of simplification of the attack.

In Table 2 we can also observe that the most robust system in terms of Eff and SR is the unimodal system based on iris and not

Table 2
Eff and SR for the Sub-Algorithm 1 (Uphill-Simplex) and Sub-Algorithm 2 (Genetic Algorithm) attacks carried out against the corresponding unimodal systems, and for the multimodal attack against the multimodal system.

FAR (%)	Unimodal attacks				Multimodal attack			
	Sub-Alg. 1 vs face		Sub-Alg. 2 vs iris		Starts face		Starts iris	
	SR (%)	Eff ($\times 10^{-4}$)	SR (%)	Eff ($\times 10^{-4}$)	SR (%)	Eff ($\times 10^{-4}$)	SR (%)	Eff ($\times 10^{-4}$)
0.10	100	22.472	91.18	1.400	100	1.9372	100	1.4180
0.05	100	22.124	80.89	1.255	100	1.8218	100	1.3585
0.01	100	21.930	62.36	1.102	100	1.3702	100	1.1112

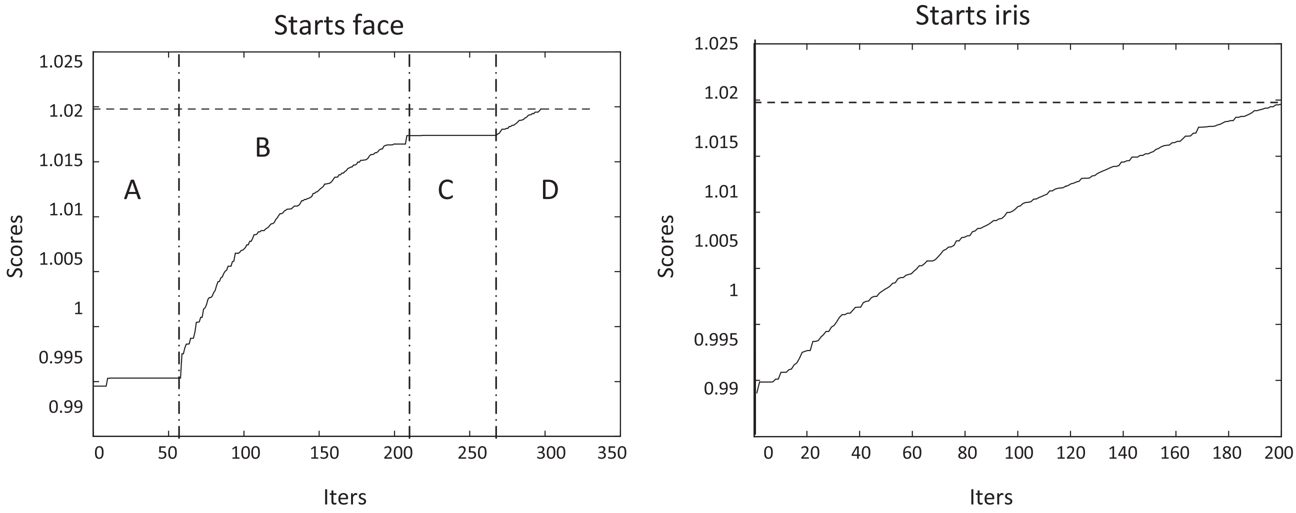


Fig. 7. Evolution of the score in each iteration for two broken accounts in the two different scenarios studied: the algorithm starts attacking the face section of the template (left) or the iris section (right). The verification threshold is represented with a dashed horizontal line. In the left plot, the different phases of the algorithm, alternatively attacking the face and iris sections, are marked with letters A–D.

the multimodal approach as would be expected. This shows that, as already demonstrated for spoofing attacks (Akhtar et al., 2011; Rodrigues et al., 2009; Johnson et al., 2010), although in general multimodal systems offer a better performance than their unimodal subsystems (for our particular case the EER decreases from 5% to 0.8%), they are not necessarily less vulnerable to software attacks. These results reinforce the importance of reporting the SR of the attack always in terms of the operating point at which it was evaluated (i.e., FAR), so that a fair comparison across different recognition systems may be established.

Finally, in Fig. 7 the evolution of the score for each iteration of the algorithm can be observed. On the left, the face section of the template is first attacked, and several areas with different slopes can be observed (marked with letters A, B, C and D), depending on what part of the template is being attacked. In segments A and C, it can also be observed that the algorithm switches to attack the other section of the template after the score remains almost constant for a fixed number of iterations. On the other hand, on the graph on the right, no "steps" can be observed on the curve: the attack started attacking the iris section and never changed to the face segment as the template was successfully broken using only the iris part.

7. Countermeasuring the attack: score quantization

Given the high vulnerability of the multimodal system evaluated to the combined attacking algorithm proposed, some attack protection needs to be incorporated in order to increase the robustness of the system. When a countermeasure is introduced in a biometric system to reduce the risk of a particular attack, it should be statistically evaluated considering two main parameters:

- Impact of the countermeasure in the system performance. The inclusion of a particular protection scheme might change the FAR and FRR of a system, and these changes should be evaluated and reported (other performance indicators such as speed or computational efficiency might also change, but are not considered here).
- Performance of the countermeasure, i.e. impact of the countermeasure in the SR and Eff of the attack.

It is often argued that a simple account lockout policy (i.e., blocking the user accounts after a number of consecutive unsuccessful access attempts) would be enough to prevent an attack such as the one proposed in the present work. However, such countermeasures still leave the system vulnerable to a spyware-based attack that interlaces its false attempts with the attempts by genuine users (successful attempts) and collects information over a period of time (i.e. piggyback attack). Furthermore, it may be used by the attacker to perform an account lockout attack (i.e., the intruder tries to illegally access a great amount of accounts blocking all of them and collapsing the system).

In this scenario, a specific design of the matching algorithm can also be implemented in order to reduce the effects of this type of threats, providing this way an additional level of security through a biometric-based protection scheme complementary to other possible non-biometric countermeasures.

Among the biometric-based approaches to reduce the effects of hill-climbing attacks, score quantization has been proposed as an effective countermeasure (Adler, 2004). In fact, the BioApi Consortium (BioAPI, 2009) recommends that biometric algorithms emit only quantized matching scores. Such quantization means that small changes in the randomly generated templates will normally not result in a modification of the matching score, so that the attack does not have the necessary feedback from the system to be carried out successfully.

With this precedents, in this section we analyse the performance of score quantization as a possible countermeasure against the proposed attack. In the experiments we will consider the multimodal system operating at a medium security operating point (FAR = 0.05%). For the combined attack we will assume the same configuration used in the vulnerability assessment experiments.

Since the global score in this multimodal system is obtained from two previous partial (face and iris) scores that are normalised and then fused, the quantization can take place either before or after this sum or fusion. Both possible schemes are studied in this section.

In order to select the appropriate quantization step according to the trade-off that should be met in terms of its impact on the system performance (ideally as small as possible) and on the attack performance (as big as possible), several Quantization Steps (QS) are tested in terms of their corresponding Positive Increment, PI (i.e., percentage of iterations that produced an increase in the similarity score higher than the quantization step considered). The EER of the system with the different QS is computed when the quantization is applied before and after the score fusion. The QS

Table 3
Performance (in terms of SR and Eff) of the combined attack against the system considering different quantization steps (QS), applied before and after the fusion of the scores.

QS		10^{-4}	10^{-3}	10^{-2}	10^{-1}
Before fusion	SR (%)	100	100	0	0
	Eff ($\times 10^{-4}$)	1.8932	1.6113	–	–
After fusion	SR (%)	100	100	100	0
	Eff ($\times 10^{-4}$)	1.7806	1.7921	1.7470	–

considered range from 10^{-8} and 10^{-1}. For the last QS (10^{-1}), the EER increases considerably (i.e., the QS is too big), while for the remaining values the performance of the system is not significantly affected. The multimodal attack is therefore repeated applying four QS values, namely: (i) QS = 10^{-4}, (ii) QS = 10^{-3}, (iii) QS = 10^{-2}, and (iv) QS = 10^{-1}. The first three QS values guarantee a similar performance of the system, while the last one can be useful for very high-security applications, when a lower performance of the system might be acceptable if it leads to a much higher protection against the analysed attacks.

In Table 3 the results of these experiments are shown. As can be seen, the quantization of the scores is effective as a countermeasure against the combined attacking algorithm presented in this work when it is applied:

- Before the fusion with a QS = 10^{-2}. Since the rounding effect of quantizing the scores and then summing them is bigger than that obtained when fusing the scores before applying the quantization, the performance of the attack decreases more when applying the quantization before the fusion. This leads to a SR = 0% for the QS = 10^{-2} when the partial scores are quantized before fusing them.
- Before or after the fusion with a QS = 10^{-1}. With this QS, the system is able to stop the attack regardless of the point where the scores are quantized. As in the previous case, the attack does not receive the necessary feedback from the system on whether it has managed to increase or not the similarity score, and thus fails to achieve its objective.

In both cases listed above, no account is broken, while for the remaining trials the SR of the attack is still 100%, only decreasing its Eff (i.e., more comparisons are needed to break an account). However, while the performance of the system is not considerably affected in the first case (EER = 1.37%), it is barely acceptable with a QS = 10^{-1}: the EER is as high as 32.06%.

8. Conclusions

In this work, we have presented and evaluated the first software attack against multimodal biometric systems. As case study, we have tested it on a system based on face and iris, a trait combination regarded as user-friendly: the features of both traits may be extracted from images the can be captured at the same time, being the acquisition process transparent to the user. The attacking algorithm shows a remarkable performance, thus proving the vulnerabilities of multimodal systems to this type of attacks. Furthermore, the multimodal system has not presented an improvement in the security level against this kind of attack compared to the face and iris modules on their own. This fact confirms what previous studies on spoofing attacks pointed out: even though multimodal systems recognition performance is higher, they do not necessarily increase the robustness of unimodal approaches to external attacks.

The quantization of the scores given by the matcher is analysed as a possible countermeasure. Two different approaches are studied and compared: the partial scores can be quantized before fusing them, or the final score can be quantized after the fusion. The first scenario leads to a null success rate without affecting the verification performance of the system, being thus a suitable countermeasure for the proposed attack. The second case also protects the system against the attack but at the cost of drastically reducing its verification performance.

Research works such as the one presented in this article pretend to bring some insight into the difficult problem of biometric security evaluation through the systematic study of biometric systems vulnerabilities and the analysis of effective countermeasures that can minimize the effects of the detected threats, in order to increase the confidence of the final users in this rapidly emerging technology.

References

Adler, A., 2004. Images can be regenerated from quantized biometric match score data. In: Proc. Canadian Conference on Electrical and Computer Engineering (CCECE), pp. 469–472.

Akhtar, Z., Alfarid, N., 2011. Secure learning algorithm for multimodal biometric systems against spoof attacks. Proc. International Conference on Information and Network Technology (IPCSIT), 2011, vol. 4. IACSIT Press, pp. 52–57.

Akhtar, Z., Kale, S., Alfarid, N., 2011. Spoof attacks in mutimodal biometric systems. Proc. International Conference on Information and Network Technology (IPCSIT), 2011, vol. 4. IACSIT Press, pp. 46–51.

ANSI, 2001. ANSI X9.84-2001, Biometric Information Management and Security.

Baker, J.E., 1987. Reducing bias and inefficiency in the selection algorithm. In: Proc. International Conference on Genetic Algorithms and their Application (ICGAA), 1987. L. Erlbaum Associates Inc., pp. 14–21.

BioAPI, 2009. The BioAPI consortium, <http://www.bioapi.org>.

Brindle, A., 1981. Genetic Algorithms for Function Optimization. Ph.D. Thesis, University of Alberta, Edmounton.

Chetty, G., Wagner, M., 2005. Audio-visual multimodal fusion for biometric person authentication and liveness verification. In: Proc. NICTA-HCSNet Multimodal User Interaction Workshop (MMUI).

Daugman, J., 2004. How iris recognition works. IEEE Transactions on Circuits and Systems for Video Technology 14, 21–30.

Galbally, J., McCool, C., Fierrez, J., Marcel, S., 2010. On the vulnerability of face verification systems to hill-climbing attacks. Pattern Recognition 43, 1027–1038.

Galbally, J., Fierrez, J., Alonso-Fernandez, F., Martinez-Diaz, M., 2011. Evaluation of direct attacks to fingerprint verification systems. Telecommunication Systems, Special Issue on Biometrics 47, 243–254.

Gan, J.-Y., Liang, Y., 2006. A method for face and iris feature fusion in identity authentication. International Journal of Computer Science and Network Security (IJCSNS) 2, 135–138.

Gan, J.-Y., Liu, J.-F., 2009. Fusion and recognition of face and iris feature based on wavelet feature and kfda. In: Proc. of the International Conference on Wavelet Analysis and, Pattern Recognition (ICWAPR).

Gomez-Barrero, M., Galbally, J., Fierrez, J., Ortega-Garcia, J., 2011. Hill-climbing attack based on the uphill simplex algorithm and its application to signature verification. In: Proc. European Workshop on Biometrics and Identity Management (BioID), 2011, LNCS, vol. 6583, pp. 83–94.

Gomez-Barrero, M., Galbally, J., Tome-Gonzalez, P., Fierrez, J., 2012. On the vulnerability of iris-based systems to software attacks based on genetic algorithms. In: Proc. Iberoamerican Conf. on Pattern Recognition (CIARP).

Hämmerle-Uhl, J., Raab, K., Uhl, A., 2011. Attack against robust watermarking-based multimodal biometric recognition systems. In: Proc. of the COST 2101 European conference on Biometrics and ID management (BioID), 2011, LNCS, vol. 6583, 2011, pp. 25–36.

Jain, A.K., Nandakumar, K., Ross, A., 2005. Score normalization in multimodal biometric systems. Pattern Recognition 38, 2270–2285.

Jain, A.K., Ross, A., Pankanti, S., 2006. Biometrics: a tool for information security. IEEE Transactions on Information Forensics and Security 1, 125–143.

Johnson, P., Tan, B., Schuckers, S., 2010. Multimodal fusion vulnerability to non-zero effort (spoof) attacks. In: Proc. Workshop on Information Forensics and Security (WIFS).

Kerckhoffs, A., 1883. La cryptographie militaire. Journal des Sciences Militaires 9, 5–83. Available on-line at: <http://www.petitcolas.net/fabien/kerckhoffs>.

Marasco, E., 2010. Secure Biometric Systems. Ph.D. Thesis, University of Naples Federico II.

Martinez-Diaz, M., Fierrez, J., Galbally, J., Ortega-Garcia, J., 2011. An evaluation of indirect attacks and countermeasures in fingerprint verification systems. Pattern Recognition Letters 32, 1643–1651.

Masek, L., Kovesi, P., 2003. MATLAB Source Code for a Biometric Identification System Based on Iris Patterns, Master's thesis, School of Computer Science and Software Engineering, University of Western Australia.

Matsumoto, T., 2004. Artificial irises: importance of vulnerability analysis. In: Proc. Second Asian Biometrics, Workshop, 2004.

Mayoue, A., Dorizzi, B., Allano, L., Chollet, G., Hennebert, J., Petrovska-Delacretaz, D., Verdet, F., 2009. Guide to Biometric Reference Systems and Performance Evaluation. Springer, pp. 327–372.

Nelder, J.A., Mead, R., 1965. A simplex method for function minimization. Computer Journal 7, 308–313.

Ortega-Garcia, J., Fierrez, J., Alonso-Fernandez, F., Galbally, J., Freire, M.R., Gonzalez-Rodriguez, J., Garcia-Mateo, C., Alba-Castro, J.-L., Gonzalez-Agulla, E., Otero-Muras, E., Garcia-Salicetti, S., Allano, L., Ly-Van, B., Dorizzi, B., Kittler, J., Bourlai, T., Poh, N., Deravi, F., Ng, M.W.R., Fairhurst, M., Hennebert, J., Humm, A., Tistarelli, M., Brodo, L., Richiardi, J., Drygajlo, A., Ganster, H., Sukno, F.M., Pavani, S.-K., Frangi, A., Akarun, L., Savran, A., 2010. The multi-scenario multi-environment BioSecure multimodal database (BMDB). IEEE Transactions on Pattern Analysis and Machine Intelligence 32, 1097–1111.

Oviatt, S., 1999. Ten myths of multimodal interaction. Communications of the ACM 42, 74–81.

Oviatt, S., Cohen, P., 2000. Multimodal interfaces that process what comes naturally. Communications of the ACM 43, 45–53.

Oviatt, S., Coulston, R., Tomko, S., Xiao, B., Lunsford, R., Wesson, M., Carmichael, L., 2003. Toward a theory of organized multimodal integration patterns during human-computer interaction. In: Proc. Int. Conf. on Multimodal Interaction.

Phillips, J., Flynn, P. et al., 2005. Overview of the face recognition grand challenge. In: Proc. IEEE Conf. on Computer Vision and Pattern Recognition (CVPR), pp. 947–954.

Ratha, N., Connell, J.H., Bolle, R.M., 2001. An analysis of minutiae matching strength. In: Proc. IAPR on Audio- and Video-Based Person Authentication (AVBPA), 2001. LNCS, vol. 2091. Springer, pp. 223–228.

Rodrigues, R.N., Ling, L.L., Govindaraju, V., 2009. Robustness of multimodal biometric fusion methods against spoof attacks. Journal of Visual Languages and Computing 20, 169–179.

Rodrigues, R., Kamat, N., Govindaraju, V., 2010. Evaluation of biometric spoofing in a multimodal system. In: Proc. IEEE International Conference on Biometrics: Theory Applications and Systems (BTAS).

Ross, A., Jain, A.K., 2003. Information fusion in biometrics. Pattern Recognition Letters 24, 2115–2125.

Ruiz-Albacete, V., Tome-Gonzalez, P. et al., 2008. Direct attacks using fake images in iris verification. In: Proc. European Workshop on Biometrics and Identity Management (BioID), 2008, LNCS, vol. 5372, pp. 181–190.

Schneier, B., 1999. Inside risks: the uses and abuses of biometrics. Communications of the ACM 42, 136.

Schneier, B., 2000. Secrets and lies. Wiley.

Tabula Rasa, 2010. Trusted biometrics under spoofing attacks (tabula rasa).

Tan, B., 2009. Assessing and recducing spoofing vulnerability for multimodal and fingerprint biometrics. Ph.D. Thesis, Clarkson University.

Turk, M.A., Pentland, A.P., 1991. Face recognition using eigenfaces. In: Proc. IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp. 586–591.

Uludag, U., Jain, A., 2004. Attacks on biometric systems: a case study in fingerprints. In: Proc. SPIE Seganography and Watermarking of Multimedia Contents VI, vol. 5306, pp. 622–633.

Wang, Y., Tan, T., Jain, A.K., 2003. Combining face and iris biometrics for identity verification. In: Proc. of Int. Conf. on Audio- and Video-Based Person Authentication (AVBPA), pp. 805–813.

Wayman, J., Jain, A., Maltoni, D., Maio, D., 2005. Biometric Systems. Technology, Design and Performance Evaluation. Springer.

Zhang, X., Sun, Z., Tan, T., 2010. Hierarchical fusion of face and iris for personal identification. In: Proc. International Conference on Pattern Recognition (ICPR).