Hill-Climbing Attack based on the Uphill Simplex Algorithm and its Application to Signature Verification

Marta Gomez-Barrero, Javier Galbally, Julian Fierrez, Javier Ortega-Garcia

Biometric Recognition Group–ATVS, EPS, Universidad Autonoma de Madrid,
C/ Francisco Tomas y Valiente 11, 28049 Madrid, Spain
{marta.barrero, javier.galbally, julian.fierrez, javier.ortega}@uam.es

Abstract. A general hill-climbing attack to biometric systems based on a modification of the downhill simplex algorithm is presented. The scores provided by the matcher are used in this approach to adapt iteratively an initial estimate of the attacked template to the specificities of the client being attacked. The proposed attack is evaluated on a competitive feature-based signature verification system over both the MCYT and the BiosecurID databases (comprising 330 and 400 users, respectively). The results show a very high efficiency of the hill-climbing algorithm, which successfully bypassed the system for over 90% of the attacks with a remarkably low number of scores needed.

1 Introduction

Biometric security systems are nowadays being introduced in many applications, such as access control, sensitive data protection, on-line tracking systems, etc., due to their advantages over traditional security approaches [1]. Nevertheless, they are also susceptible to external attacks that can decrease their security level. Therefore, it is of the utmost importance to analyse the vulnerabilities of biometric systems so that their weaknesses can be found and useful countermeasures against foreseeable attacks can be developed.

There are two main types of attacks that may put at risk the security offered by a biometric system: (*i*) *direct attacks*, carried out against the sensor using synthetic traits, such as printed iris images or gummy fingers [2]; and (*ii*) *indirect attacks*, carried out against some of the inner modules of the system [3, 4], and thus requiring for the attacker to have some knowledge about the system (e.g., storage format or matcher used). A more detailed analysis of the vulnerable points of biometric systems is made by Ratha *et al.* in [5]. In this work 8 possible points of attack are identified, the first corresponding to direct ones and the remaining seven to indirect attacks.

Several works have already studied the robustness of biometric systems against direct attacks, specially fingerprint- and iris-based, including [2, 3, 6]. In the case of indirect attacks, most of the studies use some kind of variant of the hill-climbing algorithm [4]. Some examples include an indirect attack to a face-based

system in [7], and to a PC and Match-on-Card minutiae-based fingerprint verification systems in [8] and [9], respectively. These attacks iteratively change a synthetic template, according to the scores given by the matcher, until the similarity score exceeds a fixed decision threshold. This way, the access to the system is granted. These hill-climbing approaches, except for the one proposed in [10], are all highly dependent of the technology used, only being usable for very specific types of matchers.

In the present paper, a hill-climbing algorithm based on an adaptation of the downhill simplex algorithm [11], is presented. The main contribution of the work lies in the fact that this general approach can be applied to any system working with fixed length feature vectors, regardless of the biometric trait being used. The proposed method uses the scores provided by the matcher to adapt an initial simplex, computed from a development set of users, to the local specificities of the client being attacked. The performance of the attack is evaluated on a feature-based signature verification system using the MCYT [12] and the BiosecurID [13] databases (comprising 330 and 400 users, respectively). In the experiments, the attack showed a remarkable performance, similar with both databases, being able to bypass over 90% of the accounts attacked for the best configuration of the algorithm found.

The paper is structured as follows. The general hill-climbing algorithm is described in Sect. 2, while the case study in signature verification is reported in Sect. 3. In Sect. 3.1 we present the attacked system, and the database and experimental protocol followed are described in Sect 3.2. The results are detailed in Sect. 3.3. Conclusions are finally drawn in Sect. 4.

2 Hill-Climbing based on the Uphill Simplex Algorithm

Consider the problem of finding a K-dimensional vector $\mathbf{y}$ 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.: $J(\mathcal{C}, \mathbf{y}) > \delta$. The template can be another K-dimensional vector or a generative model of K-dimensional vectors.

Let us consider a simplex, that is, a polygon defined by $K + 1$ points in the K-dimensional space, obtained randomly from a statistical model G (a K-variate Gaussian with mean $\boldsymbol{\mu}_G$ and diagonal covariance matrix $\boldsymbol{\Sigma}_G$, with $\boldsymbol{\sigma}_G^2 = \text{diag}\boldsymbol{\Sigma}_G$, related to a background set of users, overlapping to some extent with $\mathcal{C}$), and let us assume that we have access to the evaluation of the matching function $J(\mathcal{C}, \mathbf{y})$ for several trials of $\mathbf{y}$. Then, the problem stated above can be solved by adapting the downhill simplex algorithm first presented in [11] to maximize instead of minimize the function J. We iteratively form new simplices by reflecting one point, $\mathbf{y}_l$, 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, the different steps followed by the attacking hill climbing algorithm are:

1. Compute the statistical model $G(\boldsymbol{\mu}_G, \boldsymbol{\sigma}_G)$ from a development pool of users.
2. Take $K+1$ samples $(\mathbf{y}_i)$ defining the initial simplex from the statistical model $G(\boldsymbol{\mu}_G, \boldsymbol{\sigma}_G)$ and compute the similarity scores $J(\mathcal{C}, \mathbf{y}_i) = s_i$, with $i = 1, \ldots, K+1$.
3. Compute the centroid $\bar{\mathbf{y}}$ of the simplex as the average of $\mathbf{y}_i$:

$$\bar{\mathbf{y}} = \frac{1}{K+1} \sum_i \mathbf{y}_i$$

4. Reflect the point $\mathbf{y}_l$ according to the next steps, adapted from the downhill simplex algorithm [11]. In the following, the indices l and h are defined as:

$$h = \arg\max_i (s_i)$$
$$l = \arg\min_i (s_i)$$

4.a. **Reflection**: Given a constant $\alpha > 0$, the *reflection coefficient*, we compute:

$$\mathbf{a} = (1+\alpha)\bar{\mathbf{y}} - \alpha \mathbf{y}_l.$$

Thus, $\mathbf{a}$ is on the line between $\mathbf{y}_l$ and $\bar{\mathbf{y}}$ being α the ratio between the distances $[\mathbf{a}\bar{\mathbf{y}}]$ and $[\mathbf{y}_l\bar{\mathbf{y}}]$. If $s_l < s_a < s_h$ we replace $\mathbf{y}_l$ by $\mathbf{a}$. Otherwise, we go on to step 4b.

4.b. **Expansion or contraction**.

4.b.1 **Expansion**: If $s_a > s_h$ (i.e., we have a new maximum) we expand $\mathbf{a}$ to $\mathbf{b}$ as follows:

$$\mathbf{b} = \gamma \mathbf{a} + (1-\gamma)\bar{\mathbf{y}},$$

where $\gamma > 1$ is another constant called *expansion coefficient*, which represents the ratio between the distances $[\mathbf{b}\bar{\mathbf{y}}]$ and $[\mathbf{a}\bar{\mathbf{y}}]$. If $s_b > s_h$, we replace $\mathbf{y}_l$ by $\mathbf{b}$. Otherwise, we have a failed expansion and replace $\mathbf{y}_l$ by $\mathbf{a}$.

4.b.2 **Contraction**: If we have reached this step, then $s_a \leq s_l$ (i.e. replacing $\mathbf{y}_l$ by $\mathbf{a}$ would leave s_a as the new minimum). Afterwards we compute

$$\mathbf{b} = \beta \mathbf{y}_l + (1-\beta)\bar{\mathbf{y}},$$

where $0 < \beta < 1$ is the *contraction coefficient*, defined as the ratio between the distances $[\mathbf{b}\bar{\mathbf{y}}]$ and $[\mathbf{y}_l\bar{\mathbf{y}}]$. If $s_b > \max(s_l, s_a)$, then we replace $\mathbf{y}_l$ by $\mathbf{b}$; otherwise, the contracted point is worse than $\mathbf{y}_l$, and for such a failed contraction we replace all the $\mathbf{y}_i$'s by $(\mathbf{y}_i + \mathbf{y}_h)/2$.

5. With the new $\mathbf{y}_l$ value, update the simplex and return to step 3.

The hill climbing algorithm stops when $s_h \geq \delta$ or when the maximum number of iterations M is reached.

The iterative optimization algorithm used here as core of the proposed hill-climbing attack is an adaptation of the downhill simplex first presented in [11], which has been modified in order to maximize a given function and where several redundant conditions have been discarded. From now on, this modified version of the original algorithm will be referred to as *uphill simplex*.

3 Case study: Attacking a Feature-Based On-Line Signature Verification System

3.1 Signature Verification System

The proposed hill-climbing method attack based on the uphill simplex algorithm is used to attack the feature-based on-line signature verification system considered in [10] so that the results on the performance of the two hill-climbing attacks (i.e., that proposed in [10], and the one presented here) may be compared. The signatures are parametrized using the set of features described in [14]. In that work, a set of 100 global features was proposed, and the individual features were ranked according to their individual discriminant power. A good operating point for the systems tested was found when using the first 40 parameters. In the present contribution we use this 40-feature representation of the signatures, normalizing each of them to the range [0,1] using the tanh-estimators described in [15]:

$$p_k^{'} = \frac{1}{2}\left\{\tanh\left(0.01\left(\frac{p_k - \mu_{p_k}}{\sigma_{p_k}}\right)\right) + 1\right\}, \tag{1}$$

where p_k is the kth parameter, $p_k^{'}$ denotes the normalized parameter, and μ_{p_k} and σ_{p_k} are respectively the estimated mean and standard deviation of the parameter under consideration.

The similarity scores are computed using the Mahalanobis distance between the input vector and a statistical model $\mathcal{C}$ of the attacked client, using a number of training signatures (4 or 5 in our experiments). Thus,

$$J(\mathcal{C}, \mathbf{y}) = \frac{1}{\left((\mathbf{y} - \boldsymbol{\mu}^{\mathcal{C}})^T (\boldsymbol{\Sigma}^{\mathcal{C}})^{-1} (\mathbf{y} - \boldsymbol{\mu}^{\mathcal{C}})\right)^{1/2}}, \tag{2}$$

where $\boldsymbol{\mu}^{\mathcal{C}}$ and $\boldsymbol{\Sigma}^{\mathcal{C}}$ are respectively the mean vector and covariance matrix obtained from the training signatures (i.e., the statistical model of the client) and $\mathbf{y}$ is the 40-feature vector used to attack the system.

3.2 Databases and Experimental Protocol

In order to avoid biased results, two different databases were used in the experiments: the MCYT database [12] and the BiosecurID database [13].

The first of them, MCYT, is used as development set in order to compute the best parameter values of the attack and to obtain a first estimation of its performance, which may be compared to that of the hill climbing attack proposed in [10]. The findings obtained on the MCYT database are then used to analyse the algorithm performance on a totally different database (BiosecurID), in order to get to a realistic overall evaluation of the attacking capabilities and efficiency of the proposed hill climbing technique. Next, the experimental protocol followed with each of the databases is presented.

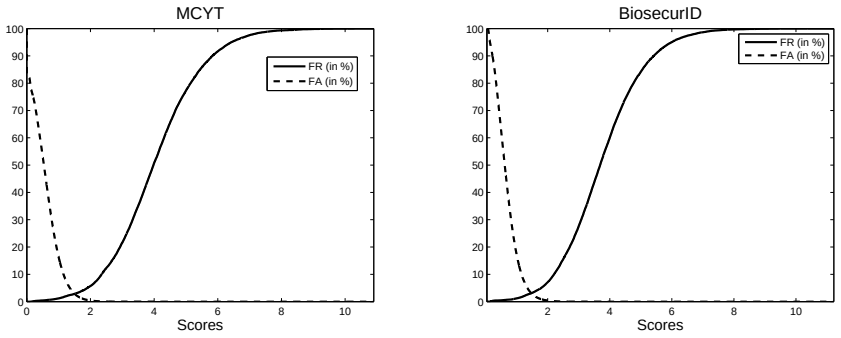

Fig. 1. FA and FR curves the MCYT (left) and BiosecurID (right) databases.

MCYT experimental protocol. The initial evaluation experiments are carried out on the MCYT signature database [12], comprising 330 users. The database was acquired in 4 different sites with 5 time-spaced capture sets. Every client was asked to sign 5 times in each set, thus capturing 25 genuine signatures per user.

The experimental protocol is the same followed in [10], so that the final results are fully comparable. Thus, the database is divided into a training set (used to estimate the distribution G from which the initial simplex is taken) and a test set (containing the user's accounts being attacked), which are afterwards swapped (two-fold cross-validation). The training set initially comprises one signature from the genuine ones of the odd users in the database, and the test set the genuine samples of the even users. This way, the donors captured in the 4 sites are homogeneously distributed over the two sets.

For each user, five different genuine models are computed using one training signature from each acquisition set, so that the temporal variability of the signing process is taken into account. With this approach, a total $330 \times 5 = 1,650$ accounts are attacked (825 in each of the two-fold cross-validation process).

In order to set the threshold δ, where we consider that the attack has been successful, the False Acceptance (FA) and False Rejection (FR) curves of the system are computed. Each of the 5 estimated models of every user is matched with the remaining 20 genuine signatures ($5 \times 20 \times 330 = 33,000$ genuine scores), while the impostor scores are generated comparing the 5 statistical models with one signature of the remaining donors, making a total of $5 \times 330 \times 329 = 542,850$ random impostor scores. The FA and FR curves are depicted in Fig. 1 (left), together with three different realistic operating points used in the attack experiments (FA = 0.05%, FA = 0.01%, and FA = 0.0025%).

BiosecurID Experimental Protocol. In order to check whether the algorithm is equally effective with different databases, we established an analogous experimental protocol to the one defined for MCYT using the BiosecurID database [13]. This database comprises 400 users and was acquired in 4 different

sessions in a 6 month time-span. Every client was asked to sign 4 times in each set, leading to 16 genuine signatures per user.

Analogously to the MCYT database, 4 different models are computed for each client using one signature from each acquisition set (i.e., 4 different signatures) so that the temporal variability is taken into account.

As before, the threshold δ is fixed after computing the FA and FR curves. The set of genuine and impostor scores are generated respectively matching each of the 4 estimated models of every user against the remaining 12 genuine samples of each subject ($4 \times 12 \times 400 = 19,200$ genuine scores), and against one signature of the other donors (leading to $4 \times 399 \times 400 = 638,400$ impostor scores). The FA and FR curves forgeries are depicted in Fig. 1 (right), together with three different realistic operating points used in the attack experiments (FA = 0.05%, FA = 0.01%, and FA = 0.0025%).

In order to assure that the hill-climbing performance results obtained on the BiosecurID database are in no way data-adapted, the initial G distribution in this experimental protocol is estimated on the MCYT database (i.e., part of the users in MCYT are used as training set), while BiosecurID is used only as test set.

3.3 Results

The goal of the experiments is to analyse in an objective and replicable manner the attacking skills of the proposed hill-climbing algorithm. With this objective, the performance of the attack will be evaluated in terms of the success rate and efficiency, defined as [16]:

- **Success Rate (SR)**: it is the expected probability that the attack breaks a given account. It is computed as the ratio between the number of broken accounts (A_B) and the total number of accounts attacked (A_T):

$$\mathrm{SR} = \frac{A_B}{A_T}$$

  This parameter indicates how dangerous the attack is: the higher the SR, the bigger the threat.
- **Efficiency (Eff)**: it indicates the average number of matchings needed by the attack to break an account. It is defined as

$$Eff = \sum_{i=1}^{A_B} \frac{n_i}{A_B},$$

  where n_i is the number of matchings computed to bypass each of the broken accounts. This parameter gives an estimation of how easy it is for the attack to break into the system in terms of speed: the lower the Eff, the faster the attack.

A direct comparison between the attack performance results obtained on the MCYT database and those presented in [10] will also be given in this section.

Analysis of α, γ and β. The goal of the initial experiments carried out on the MCYT database is to study the effect of varying the three parameters of the algorithm (α, γ and β) on the performance of the attack. As described in Sect. 2, these parameters affect how the new point of the simplex is computed at each iteration and denote: α the reflection coefficient, γ the expansion coefficient, and β the contraction coefficient.

The main objective of this experiment is not to search for the optimal values of $[\alpha, \gamma, \beta]$, but rather to understand their effect on the attack behaviour and to find a general suboptimal set of values for which the algorithm may present a good performance under different attacking scenarios. To do so, we will perform three successive steps fixing in each of them two of the parameters and sweeping the other in a given range. According to the original downhill simplex algorithm [11], the best values for the parameters are $\alpha = 1$, $\gamma = 2$ and $\beta = 0.5$. Thus, we run the experiments in ranges centred on those values, taking always into account the constraints explained in Sect. 2, namely: $\alpha > 0$, $\gamma > 1$ and $0 < \beta < 1$. The operating point chosen was FA = 0.05% and FR = 11.80%, for a maximum number of iterations $M = 5,000$.

- **Step 1: α.** First we vary α with $\gamma = 2$ and $\beta = 0.5$. As can be seen in Fig. 2,a good performance point is reached for $\alpha = 1.1$.
- **Step 2: γ.** Then, with $\alpha = 1.1$ and $\beta = 0.5$ fixed, we sweep γ from 1 to 2.5. This second plot reaches a maximum at 1.1.
- **Step 3: β.** Finally, with those two fixed values ($\alpha = 1.1$ and $\gamma = 1.1$), we find a maximum for β at 0.8.

This will be the set of parameter values that will be used in the rest of the experiments, $[\alpha, \gamma, \beta] = [1.1, 1.1, 0.8]$.

Analysis of different operating points. In this experiment, the suboptimal set of parameter values found in the previous section $[\alpha, \gamma, \beta] = [1.1, 1.1, 0.8]$ is used here to analyse the performance of the attack for different operating points of the automatic signature verification system, namely: FA = $[0.05\%, 0.01\%, 0.0025\%]$, which correspond to those considered by Galbally et al. [10]. Therefore, results of both works (shown in Table 1) may be directly compared. The SR difference between both attacks is less than 8%, while the efficiency improved about 75% with our proposed method. This way, the hill-climbing based on the uphill simplex proves to be highly competitive, breaking the accounts remarkably faster than the Bayesian hill-climbing, at the cost of a small loss of accuracy.

Analysis of the initial G distribution. In this last development experiment, also carried out on the MCYT database, the number of users employed for the estimation of the initial distribution G is varied from 5 to 165 in order to study its impact on the attack performance. The SR improvement was lower than 3% in terms of SR and Eff for all operating points, as can be observed in Fig. 3. Thus, the attack proves to be highly competitive with as few as 5 different training signatures compared to over 150 needed by the algorithm proposed in [10].

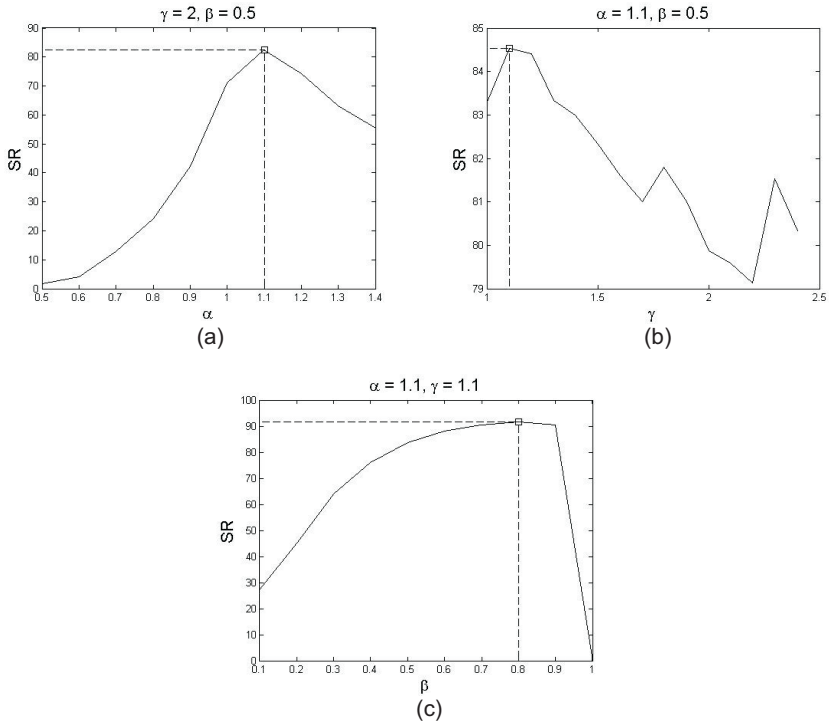

Fig. 2. (a) Success rates for $\alpha \in [0.5, 1.4], \gamma = 2, \beta = 0.5$. Maximum at $\alpha = 1.1$. (b) Success rates for $\gamma \in [1, 2.4], \alpha = 1.1, \beta = 0.5$. Maximum at $\gamma = 1.1$. (c) Success rates for $\beta \in [0.1, 1], \alpha = 1.1, \gamma = 1.1$. Maximum at $\beta = 0.8$.

Analysis of the performance on the BiosecurID database. Finally, the knowledge acquired in the previous experiments was applied to study the dependency of the attack performance on the data being used. Thus, the parameter values fixed in the MCYT database (i.e., $[\alpha, \gamma, \beta] = [1.1, 1.1, 0.8]$) are deployed to attack the accounts of the subjects comprised in the BiosecurID database. As mentioned in Sect. 3.2, the initial distribution G is computed using one signature from each of the initial 5 users in MCYT. This way, the training set (MCYT) and test set (BiosecurID) are totally independent, leading to fully unbiased results.

As shown in Table 2, the performance of the attack is very similar, both in terms of the efficiency and the success rates for both datasets. Even though Eff is a little higher for all the three different operating points, it must be taken into account that in the case of MCYT, the parameters of the algorithm were specifically adjusted for the dataset, while they remained the same for this second database. On the other hand, the SR is about 2% higher in the case of BiosecurID, proving that the algorithm has a high adaptation capability, performing well under different operating conditions.

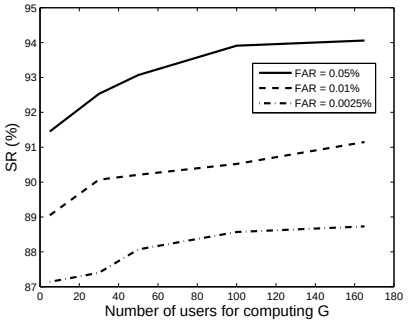

Fig. 3. Success rates for the three operating points tested (FA = 0.05%, FA = 0.01%, FA = 0.0025%), for an increasing number of subjects used to compute the distribution G from which the initial simplex is taken.

FA	Uphill simplex		Gal. et al. [10]	
	SR	Eff	SR	Eff
0.05%	91.76%	1,556	98.12%	5,712
0.01%	89.58%	1,678	96.60%	6,076
0.0025%	87.82%	1,805	94.90%	6,475

Table 1. Efficiency and SR (in %) for each operating point, compared to the performance results given in Galbally et al. [10].

Graphical example. An execution of the attack at the FA = 0.05% operating point and using the best algorithm configuration for the database MCYT is shown in Fig. 4. The signature was successfully attacked in less than 500 iterations. At the top of the figure, we can see a signature of the client being attacked as well as the successive best similarity scores in each iteration until the threshold δ is reached. At the bottom, the evolution of the simplices corresponding to the scores marked with a vertical line are shown for two pairs of parameters (1 and 2 on the left, 3 and 4 on the right). A darker colour denotes a previous

FA	BiosecurID		MCYT	
	SR	Eff	SR	Eff
0.05%	92.69%	2,051	91.32%	1,178
0.01%	87.94%	2,440	88.43%	1,353
0.0025%	83.44%	2,611	86.77%	1,661

Table 2. Success rate (in %) and Efficiency for each operating point tested, using 5 subjects from MCYT for the training of the initial simplex, for both the MCYT and the BiosecurID databases.

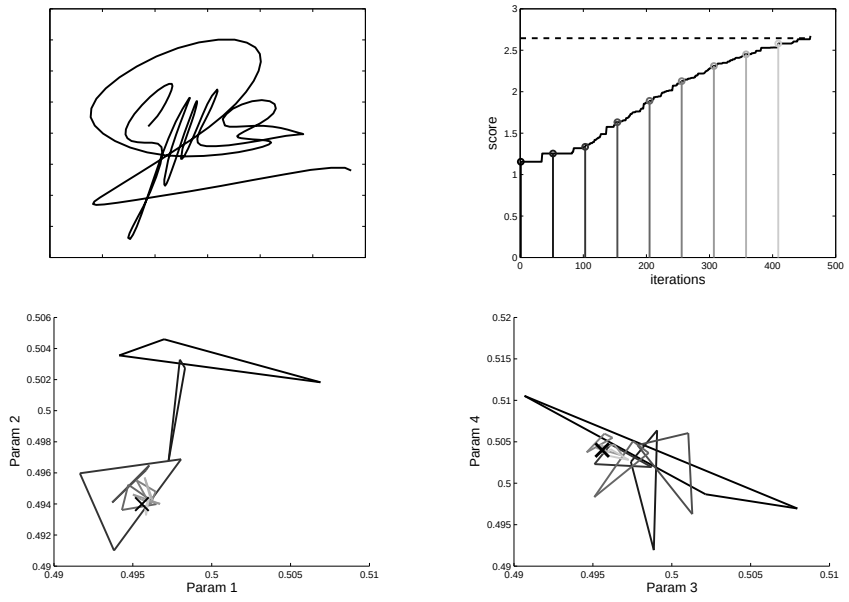

Fig. 4. Evolution of the algorithm in a successful attack. On the top we show one signature of the client attacked (left) and the scores reached for every iteration of the hill-climbing algorithm (right). On the bottom appear the simplices corresponding to the scores marked with a vertical line for parameters one and two (left) and three and four (right). A darker colour denotes a previous iteration while the cross shows the target being attacked.

iteration and the cross is the target being attacked. It can be observed that the simplices quickly approach the target, diminishing their area at the same time.

4 Conclusions

In the present work, a hill-climbing attack based on the uphill simplex algorithm, an adaptation of downhill simplex, was presented and evaluated on a feature-based signature verification system using two different databases comprising 330 and 400 users, respectively. Several experiments proved its high efficiency, reaching success rates over 90% for the best configuration found.

The algorithm performance was also compared to that of the Bayesian hill-climbing attack [10], resulting in very similar success rates but with a convergence speed which is around four times faster (it needs a quarter of the number of matchings to break the same amount of accounts). Furthermore, the proposed algorithm only requires 5 different real signatures to be initialized, in opposition to the Bayesian-based attack, where over 150 samples were used.

The experiments have also shown that the performance of the proposed attack is independent of the data being used, as the results obtained in both databases (MCYT and BiosecurID) were almost identical although the attack parameters had been specifically fixed for the MCYT database.

It should finally be emphasized that the proposed attack can be applied to the evaluation of the vulnerabilities of any biometric system based on fixed length templates of real numbers, regardless of the matcher or biometric trait being used.

5 Acknowledgements

This work has been partially supported by projects Contexts (S2009/TIC-1485) from CAM, Bio-Challenge (TEC2009-11186) from Spanish MICINN, TABULA RASA (FP7-ICT-257289) from EU, and *Cátedra UAM-Telefónica*.

References

1. Jain, A.K., Ross, A., Pankanti, S.: Biometrics: a tool for information security. IEEE Trans. on Information Forensics and Security **1** (2006) 125–143
2. Van der Putte, T., Keuning, J.: Biometrical fingerprint recognition: don't get your fingers burned. In: Proc. Conference on Smart Card Research and Advanced Applications (CARDIS). (2000) 289–303
3. Pacut, A., Czajka, A.: Aliveness detection for iris biometrics. In: Proc. IEEE Int. Carnahan Conf. on Security Technology (ICCST). Volume 1. (2006) 122–129
4. Soutar, C., Gilroy, R., Stoianov, A.: Biometric system performance and security. In: Proc. IEEE Automatic Identification Advanced Technologies (AIAT). (1999)
5. Ratha, N., Connell, J.H., Bolle, R.M.: An analysis of minutiae matching strength. In: Proc. IAPR Audio- and Video- Based Person Authentication (AVBPA), Springer LNCS-2091 (2001) 223–228
6. Galbally, J., Fierrez, J., Rodriguez-Gonzalez, J., Alonso-Fernandez, F., Ortega-Garcia, J., Tapiador, M.: On the vulnerability of fingerprint verification systems to fake fingerprint attacks. In: Proc. IEEE Int. Carnahan Conf. on Security Technology (ICCST). (2006) 130–136
7. Adler, A.: Sample images can be independently restored from face recognition templates. In: Proc. Canadian Conference on Electrical and Computer Engineering (CCECE). Volume 2. (2003) 1163–1166
8. Uludag, U., Jain, A.: Attacks on biometric systems: a case study in fingerprints. In: Proc. SPIE Seganography and Watermarking of Multimedia Contents VI. Volume 5306. (2004) 622–633
9. Martinez-Diaz, M., Fierrez, J., Alonso-Fernandez, F., Ortega-Garcia, J., Siguenza, J.A.: Hill-climbing and brute force attacks on biometric systems: a case study in match-on-card fingerprint verification. In: Proc. IEEE Int. Carnahan Conf. on Security Technology (ICCST). Volume 1. (2006) 151–159
10. Galbally, J., Fierrez, J., Ortega-Garcia, J.: Bayesian hill-climbing attack and its application to signature verification. In: Proc. IAPR International Conference on Biometrics (ICB), Springer LNCS-4642 (2007) 386–395
11. Nelder, J.A., Mead, R.: A simplex method for function minimization. Computer Journal **7** (1965) 368 – 313

12. Ortega-Garcia, J., Fierrez-Aguilar, J., et al.: MCYT baseline corpus: a bimodal biometric database. IEE Proc. Vis. Image Signal Process. **150** (2003) 395–401
13. Fierrez, J., Galbally, J., Ortega-Garcia, J., Freire, M.R., Alonso-Fernandez, F., Ramos, D., Toledano, D.T., Gonzalez-Rodriguez, J., Siguenza, J.A., Garrido-Salas, J., Anguiano, E., de Rivera, G.G., Ribalda, R., Faundez-Zanuy, M., Ortega, J.A., Cardeoso-Payo, V., Viloria, A., Vivaracho, C.E., Moro, Q.I., Igarza, J.J., Sanchez, J., Hernaez, I., Orrite-Uruuela, C., Martinez-Contreras, F., Gracia-Roche, J.J.: BiosecurID: a multimodal biometric database. Pattern Analysis and Applications **13** (2009) 235–246
14. Fierrez-Aguilar, J., Nanni, L., et al.: An on-line signature verification system based on fusion of local and global information. In: Proc. of AVBPA, LNCS-3546 (2005)
15. Jain, A.K., Nandakumar, K., Ross, A.: Score normalization in multimodal biometric systems. Pattern Recognition **38** (2005) 2270–2285
16. Galbally, J.: Vulnerabilities and Attack Protection in Security Systems Based on Biometric Recognition. PhD thesis (2009)