ARTICLE IN PRESS

Information Sciences xxx (2013) xxx–xxx

Contents lists available at SciVerse ScienceDirect

Information Sciences

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

A novel hand reconstruction approach and its application to vulnerability assessment

Marta Gomez-Barrero [a,*], Javier Galbally [a], Aythami Morales [b], Miguel A. Ferrer [b], Julian Fierrez [a], Javier Ortega-Garcia [a]

[a] Biometric Recognition Group – ATVS, EPS, Universidad Autonoma de Madrid, C/ Francisco Tomas y Valiente 11, 28049 Madrid, Spain
[b] Instituto Universitario para el Desarrollo Tecnológico y la Innovación en Comunicaciones (IDeTIC), Universidad de Las Palmas de Gran Canaria, Campus de Tafira s/n, E35017 Las Palmas de Gran Canaria, Spain

ARTICLE INFO

Article history:
Available online xxxx

Keywords:
Biometric system
Hand recognition
Hand reconstruction
Security
Vulnerability

ABSTRACT

The present work proposes a novel probabilistic method to reconstruct a hand shape image from its template. We analyse the degree of similarity between the reconstructed images and the original samples in order to determine whether the synthetic hands are able to deceive hand recognition systems. This analysis is made through the estimation of the success chances of an attack carried out with the synthetic samples against an independent system. The experimental results show that there is a high chance of breaking a hand recognition system using this approach. Furthermore, since it is a probabilistic method, several synthetic images can be generated from each original sample, which increases the success chances of the attack.

1. Introduction

Biometrics are nowadays being introduced into many applications as an alternative to traditional security mechanisms [38,75]. The main advantage of biometric systems is that you no longer need to carry a key or remember a PIN code: you are your own key.

One of the most popular biometric traits deployed by these systems is the hand [61,77]. In the last 30 years, hand recognition devices have been installed in airports, nuclear plants or hotels [49,79]. These systems offer a reliable [30,41,73], low-cost (acquisition can be made by means of commercial low-resolution scanners or cameras) and user-friendly [32,42] solution for a wide range of access control applications.

However, as any other security device, these systems are also vulnerable to external attacks that may compromise their security [62]. Therefore, it is of the utmost importance to understand and analyse these eventual threats in order to increase the security offered by biometric systems.

One of the areas that is more directly related to the vulnerabilities evaluation of biometric systems and that presents a high potential impact in their security, is the reconstruction of a biometric trait starting from the original user template, or *inverse biometrics*. If such an inverse engineering process is possible, an eventual attacker that manages to obtain a template belonging to a certain user (e.g. the iriscode or minutiae template) would be able to reconstruct the original biometric sample and could use it to illegally access the system.

* Corresponding author. Tel.: +34 914973363.
E-mail addresses: marta.barrero@uam.es (M. Gomez-Barrero), javier.galbally@uam.es (J. Galbally), amorales@gi.ulpgc.es (A. Morales), mferrer@dsc.ulpgc.es (M.A. Ferrer), julian.fierrez@uam.es (J. Fierrez), javier.ortega@uam.es (J. Ortega-Garcia).

0020-0255/$ - see front matter © 2013 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.ins.2013.06.015

In this context, the ultimate question is: are we able to generate synthetic images whose templates are similar enough to those of the original user? That would mean that given just a template, we are able to reconstruct an image with which we can deceive a recognition system or even steal someone's identity.

In the past, it has been a common belief that templates do not comprise enough information in order to reconstruct the original sample from them [35]. However, recent studies have arisen several concerns regarding the soundness of this widely spread belief for traits such as the fingerprint [12], the iris [67] or the face [26].

In this work, we address for the first time these questions and concerns for the hand trait. For this purpose, we present a novel probabilistic approach based on the Uphill Simplex algorithm and a hand-shape generator for the reconstruction of hand shape images from their templates. Three main objectives are pursued in the present work:

- Analyse the feasibility of such a reverse engineering process for the hand geometry trait.
- Study whether the reconstructed images obtained with the proposed method are able to deceive state-of-the-art hand recognition systems. This will also serve as validation for the new reconstruction technique.
- Determine if it is possible to generate not just one, but several different synthetic images which yield templates very similar to the genuine one.

In this new scenario, the results presented in this contribution show the necessity to include in hand-shape applications efficient countermeasures to repel the studied attacks [19,21].

In order to follow a fully reproducible experimental protocol which permits the comparison of the results with future studies, experiments are carried out on three publicly available databases. Furthermore, the hand recognition systems used for development and testing are well known and state-of-the-art systems which may be easily obtained by any interested party.

The article is structured as follows. After the introduction, a selection of the most important related works may be found in Section 2. Hand recognition is briefly summarized in Section 3. The novel probabilistic hand reconstruction algorithm is presented in Section 4. Then, the experimental protocol together with the databases and hand recognition systems used are described in Section 5. In Section 6 the development and validation results, as well as a quality assessment of the real and the synthetic samples, are presented. Conclusions are finally drawn in Section 7.

2. Related works

A growing interest has arisen in the biometric community over the last decade for the generation of synthetic biometric traits such as voice [18], fingerprints [11], iris [80], handwriting [47], face [57] or signature [58].

One of the first research lines in this field was the generation of the so-called *duplicated samples*. In these methods the generation algorithm starts from one or more real samples of a given person and, through different transformations, produces different synthetic (or duplicated) samples corresponding to the same subject. This type of algorithms is useful to increase the amount of already acquired biometric data which can be helpful, for instance, to synthetically augment the size of the enrolment set of data in identification and verification systems, a critical parameter for instance in signature biometrics [22]. This approach has been applied to signature [52,55], handwriting [51,69] or face synthesis [57,68,70].

Based on those initial works, researchers have also focused their efforts on a second and more complex problem: the generation of *fully synthetic biometric individuals*. In this case, some kind of a priori knowledge about a certain biometric trait (e.g., minutiae distribution, iris structure, signature length, etc.) is used to create a model that characterizes that biometric trait for a population of subjects. New synthetic individuals can then be generated sampling the constructed model. In a subsequent stage of the algorithm, multiple samples of the synthetic users can be generated by any of the procedures for creating duplicated samples. Different model-based algorithms have been presented in the literature to generate synthetic individuals for biometric traits such as iris [15,64,80], fingerprint [11], or speech [40,56].

All the previous works have been mainly focused on the generation of new synthetic data, intended in general to overcome the limitation of assembling large biometric databases for performance assessment purposes. However, none of these very valuable efforts addresses directly the main objective raised in the present work referred to as *inverse biometrics*, that is, the reconstruction of a synthetic biometric sample from a genuine template and the evaluation of the ensuing security implications.

One of the first works that addressed the problem posed by inverse biometrics was carried out by Hill [31]. This work, focused on fingerprint recognition, proves that the information stored in the minutiae template allows the reconstruction of images similar to the original fingerprint. After him, other researches have generated fingerprint images [12,59] or gummy fingers [25] given only the minutiae template. However, not only fingerprints have been successfully reconstructed: in [1,2,26] face images are recovered from their templates, and in [67] iris images are generated starting from the iriscodes.

In our particular case study, hand shape recognition, to our knowledge, only our previous work [28] addresses the inverse biometrics problem, proposing the first reconstruction approach to recover hand geometry samples from their templates. In that work, only the theoretical framework was proposed and some preliminary experiments were carried out. In the present contribution we significantly extend that initial work with: (i) a more thorough and comprehensive description of the

Please cite this article in press as: M. Gomez-Barrero et al., A novel hand reconstruction approach and its application to vulnerability assessment, Inform. Sci. (2013), http://dx.doi.org/10.1016/j.ins.2013.06.015

algorithm, (ii) a very much improved experimental protocol with the use of different databases and recognition systems, (iii) new and more reliable experimental findings, *iv*) an exhaustive analysis of the results, and (v) a quality assessment of the synthetic hand shape images generated.

3. Summary of hand recognition

In this section the main aspects of the hand recognition problem directly related to the present study are briefly summarized. For a more comprehensive review of hand-shape recognition the reader is referred to specific works on the topic [16,17,39,41,45,61,76,79].

In order to perform recognition of individuals through their hands, different features may be used, namely: hand geometry [61], shape [41], the palm texture [77], or fusions of those features [43,44]. Only the first two sets are studied in the present work:

- *Hand geometry*: since the length and width of the fingers are relatively simple to extract and present a significative discriminative power, they are suited for verification purposes. Some examples can be found in [8,37,46,71].
- *Hand shape*: hand shapes contain very rich information which exhibits a big variation between individuals. Therefore, many hand-based recognition systems make their decisions relying on this kind of information [7,13,23,36,41,73]. In the present work, these systems will be referred to as *appearance-based systems*.
- *Silhouette alignment*: the coordinates of the silhouette of the hand contains discriminative information which can be used for person recognition by aligning the silhouettes. Some examples are presented in [16,17,19,37].

Another problem related to hand verification is the acquisition device. Wong et al. discuss in [72] the advantages and disadvantages of the two main possible scenarios:

- *Camera*: its main advantages are its acquisition speed and the use of a contactless setup, so that no plastic deformation is produced in the hand shape and its features.
- *Scanner*: scanners offer a higher image resolution and a more comfortable acquisition scenario to the user, as well as an homogeneous background that makes the hand segmentation easier. However, in this case some amount of deformation is introduced as a consequence of the contact between the hand and the scanner surface, which increases the intra-user variability.

As it is described in Section 5, databases acquired both with a camera and a scanner are used in the experiments. Furthermore, the experimental protocol includes four completely different systems, two based on geometric features, one on the global hand shape appearance, and a last one on the hand silhouette. The objective of this experimental setup is to perform a study as general as possible regarding the state-of-the-art on hand recognition systems and databases.

4. The reconstruction method

Problem statement. Consider the problem of finding a real-valued matrix (in our case representing a hand geometry image) $\mathbf{I_R}$ which, compared to an *unknown* template $\mathbf{T}$ (related to a specific client), produces a similarity score bigger than a certain threshold δ, according to some unknown function $\mathcal{V}$, i.e.: $s = \mathcal{V}(\mathbf{I_R}, \mathbf{T}) > \delta$. The mapping function $\mathcal{V}$ is internally divided into two sub-functions, also unknown: $\mathcal{F}(\mathbf{I_R}) = \mathbf{T_R}$ extracts the features from the input image $\mathbf{I_R}$ and obtains the corresponding template $\mathbf{T_R}$, and $\mathcal{J}(\mathbf{T_R}, \mathbf{T}) = s$ computes the similarity score between $\mathbf{T_R}$ and the target template $\mathbf{T}$. That is: $\mathcal{V}(\mathbf{I_R}, \mathbf{T}) = \mathcal{J}(\mathcal{F}(\mathbf{I_R}), \mathbf{T}) = \mathcal{J}(\mathbf{T_R}, \mathbf{T}) = s$.

Assumptions. Let us assume that we have access to the evaluation of the function $\mathcal{V}(\mathbf{I_R}, \mathbf{T})$ for several trials of $\mathbf{I_R}$.

Algorithm. The problem stated above may be solved combining the hill-climbing approach based on the Uphill Simplex algorithm first presented in [27] to optimize the input of a generator of hand shape images, according to the general diagram presented in Fig. 1.

Hand-shape generator. The generator used to obtain the matrices $\mathbf{I_R}$ (hand shape images) that will be compared with the target, $\mathbf{T}$, is based on the Active Shape Model approach [13,14]. A general diagram of the generator is shown in Fig. 2. The first step is to train the ASM model using the aligned hand contours from the development set GPDS2 DB, as will be presented in Section 6.1. The process of aligning the contours can be divided in four stages: (i) for each hand image, we automatically locate 14 landmarks (see crosses in Fig. 2) using the methodology proposed in [19]; (ii) the contours are aligned by placing the hand geometric center as the coordinate origin, and rotating the hand contour by an angle equal to the slope of the line between the 1st and 3rd finger-web: this allows to reduce the effects of translation and rotation; (iii) the envelope line between landmarks is sampled with a number of points equal to average envelope length in GPDS2 DB divided by five; (iv) finally, the hand contour is represented as a $2n$ element vector composed by the coordinates (x and y) of $n = 630$ selected contour points.

As we enforce a common number of points between landmarks, the alignment in the positioning of landmarks inside the sampled vector is ensured for all the contours.

Please cite this article in press as: M. Gomez-Barrero et al., A novel hand reconstruction approach and its application to vulnerability assessment, Inform. Sci. (2013), http://dx.doi.org/10.1016/j.ins.2013.06.015

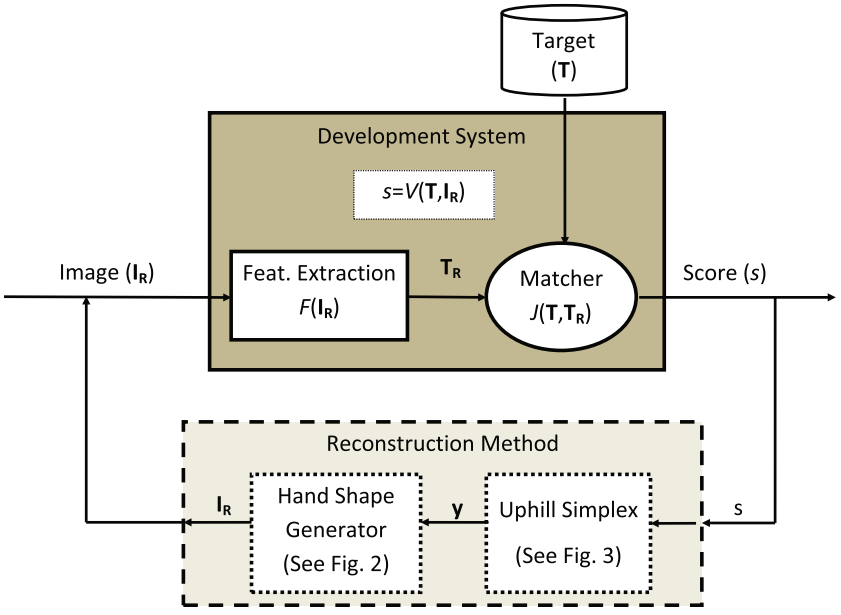

Fig. 1. General structure of the image reconstruction method proposed in this work.

Let $\bar{x}$ be the hand mean contour obtained as $\bar{x} = \frac{1}{100}\sum_{i=1}^{100} x_i$, being $x_i \in \mathbb{R}^{2n\times 1}$ the vector that represents the contour of the ith GPDS2 DB user. Principal Component Analysis (PCA) is applied to determine the k main directions of variation of the development set. A reconstructed hand-contour can be then generated as:

$$\mathbf{I_R^c} = \bar{x} + P\mathbf{y}$$

where $P \in \mathbb{R}^{2n\times k}$ is the projection matrix, whose columns are the eigenvectors of the covariance matrix, and $\mathbf{y} = [y_0,\ldots,y_{k-1}]$ is the vector of parameters defining the hand-shape contour, which will be optimized by the Uphill Simplex. $\mathbf{I_R^c}$ is the contour vector of the generated hand. The reconstructed binary hand-shape, $\mathbf{I_R}$, is obtained ensuring the continuity of the contour points by lineal interpolation and applying a flood-fill operation on background pixels of the binary contour image generated with $\mathbf{I_R^c}$.

Uphill Simplex. Development experiments are carried out on the GPDS2 DB in Section 6.1 to determine the four initialization parameters of the hand shape generator [13,14] and the Uphill Simplex.

In order to optimize the input of the hand shape generator, as depicted in Fig. 1, the proposed reconstruction approach uses the Uphill Simplex algorithm [27]. Let us consider a simplex, that is, a polygon defined by $k+1$ points $\mathbf{y}_i$ in the k-dimensional space, obtained from randomly sampling a statistical model G (computed from a development pool of users). Each of these $\mathbf{y}_i$ k-dimensional points (with $i = 1,\ldots,k+1$) is transformed into a hand shape image $\mathbf{I_R}$ using the hand shape generator (see Fig. 2). We iteratively form new simplices by reflecting one point, $\mathbf{y}_l$, in the hyperplane of the remaining points, in order to increase at each iteration the value of the mapping function $\mathcal{V}(\mathbf{I_R},\mathbf{T})$. The point to be reflected will always be the one with the lowest score s, since it is, in principle, the one furthest from our objective (see Fig. 3). The algorithm stops when one of the $\mathbf{I_R^i}$ images produces a score higher than the threshold δ.

In particular, the different steps followed by the reconstruction algorithm are:

1. Compute empirically the statistical model G from a development pool of users.
2. Take randomly $k+1$ samples ($\mathbf{y}_i$) defining the initial simplex from the statistical model G and generate the corresponding matrices $\mathbf{I_R}^i$, with $i = 1,\ldots,k+1$, using the hand shape generator (see Fig. 2).
3. Compute the similarity scores $\mathcal{V}\left(\mathbf{T},\mathbf{I_R^i}\right) = s_i$.
4. Compute the centroid $\bar{\mathbf{y}}$ of the simplex as the average of $\mathbf{y}_i$.
5. Reflect the point $\mathbf{y}_l$ according to the next steps, where the indices l and h are defined as (see Fig. 3):

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

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

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

Please cite this article in press as: M. Gomez-Barrero et al., A novel hand reconstruction approach and its application to vulnerability assessment, Inform. Sci. (2013), http://dx.doi.org/10.1016/j.ins.2013.06.015

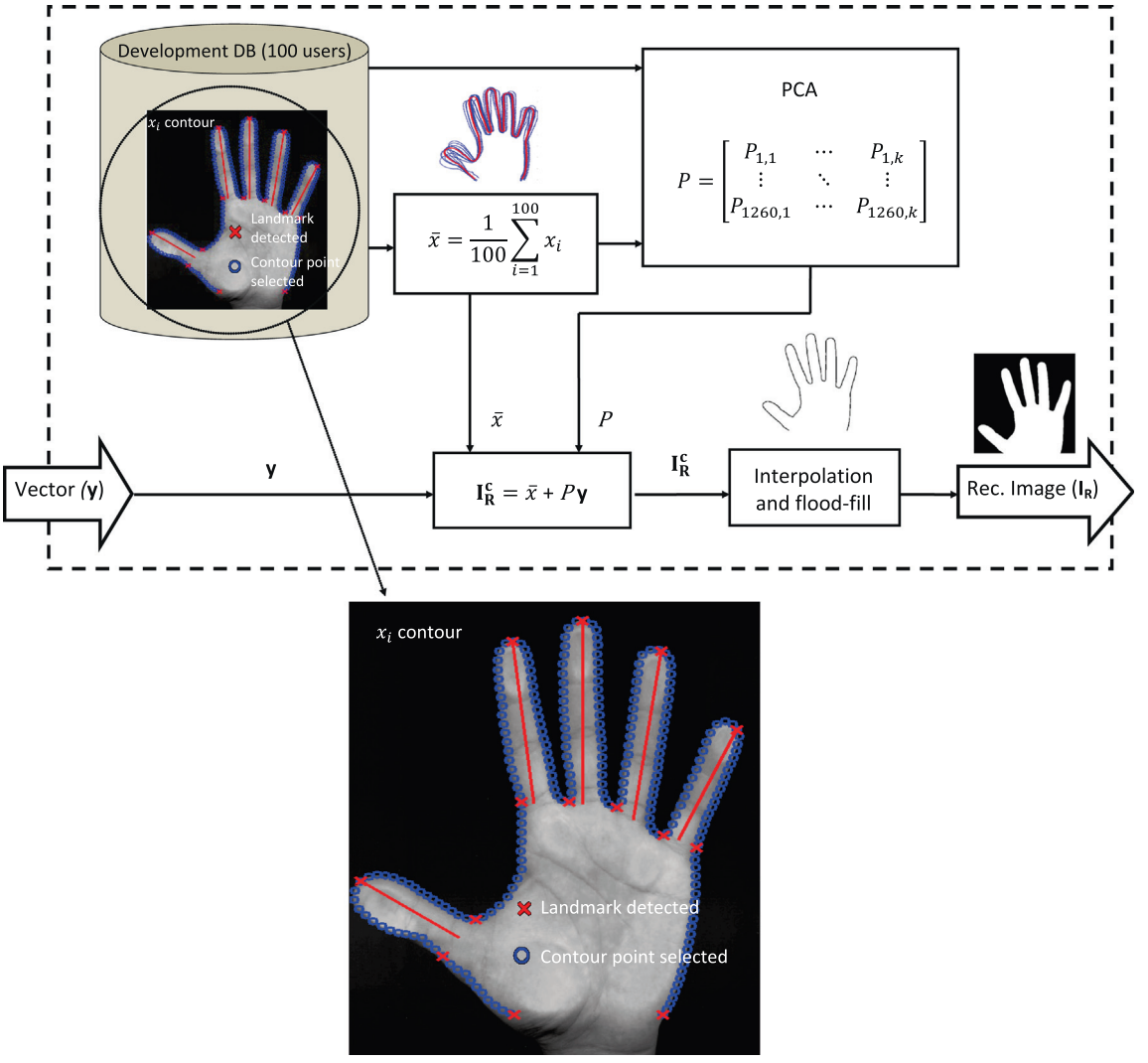

Fig. 2. General diagram of the hand shape generator used in the hand shape reconstruction method, with a zoom on the hand landmarks and contour.

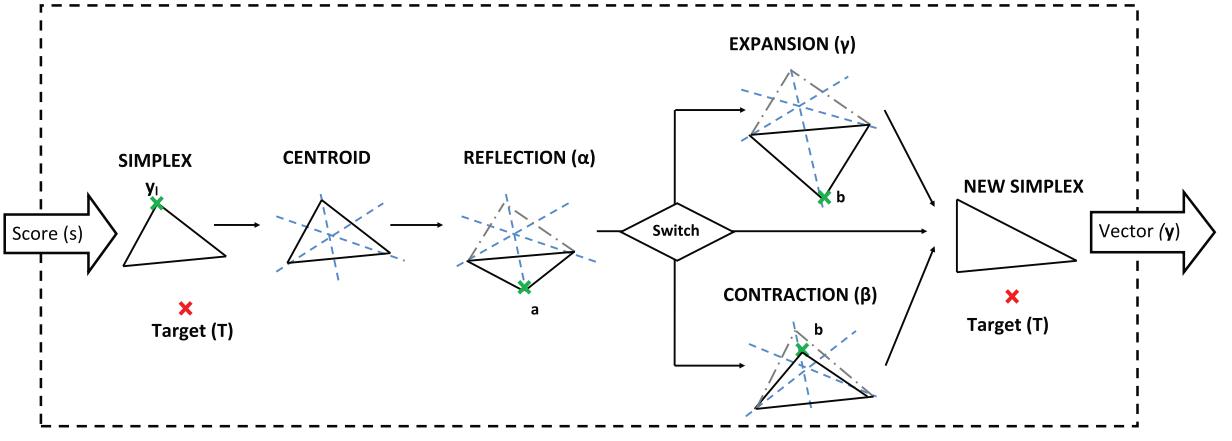

Fig. 3. General diagram of the Uphill Simplex algorithm used in the hand shape reconstruction method.

Please cite this article in press as: M. Gomez-Barrero et al., A novel hand reconstruction approach and its application to vulnerability assessment, Inform. Sci. (2013), http://dx.doi.org/10.1016/j.ins.2013.06.015

Thus, $\mathbf{y}_a$ is on the line between $\mathbf{y}_l$ and $\bar{\mathbf{y}}$ being α the ratio between the distances $[\mathbf{y}_a\bar{\mathbf{y}}]$ and $[\mathbf{y}_l\bar{\mathbf{y}}]$.
Generate $\mathbf{I_R}^a$ and compute $s_a = \mathcal{V}(\mathbf{T}, \mathbf{I}_\mathbf{R}^a)$.
If $s_l < s_a < s_h$ we replace $\mathbf{y}_l$ by $\mathbf{y}_a$. Otherwise, we go to step 5b.

5.b. *Expansion or contraction.*

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

$$\mathbf{y}_b = \gamma\mathbf{y}_a + (1-\gamma)\bar{\mathbf{y}}$$

where $\gamma > 1$ is another constant called *expansion coefficient*, which represents the ratio between the distances $[\mathbf{y}_b\bar{\mathbf{y}}]$ and $[\mathbf{y}_a\bar{\mathbf{y}}]$.
Generate $\mathbf{I_R}^b$ and compute $s_b = \mathcal{V}\left(\mathbf{T}, \mathbf{I}_\mathbf{R}^b\right)$.
If $s_b > s_h$, we replace $\mathbf{y}_l$ by $\mathbf{y}_b$. Otherwise, we have a failed expansion and replace $\mathbf{y}_l$ by $\mathbf{y}_a$.

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

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

where $0 < \beta < 1$ is the *contraction coefficient*, defined as the ratio between the distances $[\mathbf{y}_b\bar{\mathbf{y}}]$ and $[\mathbf{y}_l\bar{\mathbf{y}}]$.
Generate $\mathbf{I_R}^b$ and compute $s_b = \mathcal{V}(\mathbf{T}, \mathbf{I}_\mathbf{R}^b)$.
If $s_b > \max(s_l, s_a)$, then we replace $\mathbf{y}_l$ by $\mathbf{y}_b$; 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 $(\mathbf{y}_i + \mathbf{y}_h)/2$.

6.With the new $\mathbf{y}_l$ value, update the simplex and return to step 4.

Rationale behind the algorithm. As stated in [48], when we move from the worst vertex ($\mathbf{y}_l$) towards any of the other vertices, the function value sincreases. Hence, assuming a continuous fitness function $\mathcal{V}$ with a relatively smooth surface following a general commanding gradient (which is the usual case for unencrypted biometric systems), it is feasible that a point $\mathbf{y}_a$ lying on the line $[\bar{\mathbf{y}}\mathbf{y}_l]$ on the opposite side of $\mathbf{y}_l$ with respect to the hyperplane defined by the other k points (i.e., outside the simplex) achieves higher values of $\mathcal{V}$. If the function value s_a is higher than the value of all vertices, then we have most likely moved in the correct direction, and the maximum may lie ahead. This is the case in step 5.b.1, when the point is further expanded in the same direction. On the other hand, if the new point $\mathbf{y}_a$ results in a new minimum (i.e., its function value s_a is lower than in any other vertex), the maximum is probably close to $\mathbf{y}_l$. Therefore, the simplex is contracted by finding a new point in the $[\mathbf{y}_l\bar{\mathbf{y}}]$ line inside rather than outside the simplex, as in case 5.b.2. If this new point achieves no improvement over $\mathbf{y}_l$, the only remaining option is contracting the whole simplex: the maximum probably lies inside the simplex. All these scenarios are depicted in Fig. 3 for clarity in only two dimensions, where the simplex is a triangle.

Stopping criteria. The hill climbing algorithm stops when $s_h \geqslant \delta$ (i.e., the image has been successfully reconstructed) or when the maximum number of iterations is reached (i.e., the reconstruction has failed).

Important notices. It has to be emphasized that the Uphill Simplex is not used to optimize the templates $\mathbf{T}$ deployed by the development recognition system, but the vectors $\mathbf{y}$ needed by the hand shape generator (which do not coincide with $\mathbf{T}$). This way, the proposed approach is general as it can be used to reconstruct the hand shape images independently of the template $\mathbf{T}$ (e.g., size, format, information stored, ...) used by the system.

It should also be noted that, due to the probabilistic nature of the algorithm initialization (i.e., step 2: *random* sampling of the statistical model G), the method produces different solutions at each execution. This permits the reconstruction of more than one hand image ($\mathbf{I_R}$) with very similar templates ($\mathbf{T_R}$) to the target ($\mathbf{T}$).

Furthermore, the algorithm does not require any information about:

- The mapping function $\mathcal{F}$ between the hand shape images ($\mathbf{I_R}$) and their corresponding templates ($\mathbf{T_R}$).
- The matching function $\mathcal{J}$.
- The function $\mathcal{V}$, only needing access to its outcome for given inputs.

Lastly, it should be beard in mind that, as will be explained in Section 6, a development pool of users is necessary to determine the initialization parameters of the hand shape generator and the Uphill Simplex, namely: (i) the dimensionality (k) of the vector $\mathbf{y}$, (ii) the PCA matrix P, (iii) the mean $\bar{x}$ of the development set of hand shape images, and (iv) the statistical model G for the Uphill Simplex.

5. Experimental protocol and databases

As it is shown in Fig. 4, the experimental protocol is divided into a development and a validation stage:

- *Development*. The purpose of this stage is twofold: on the one hand, complete the training of the hand synthesizer and fix the initialization parameters (k, P, G and $\bar{x}$) of the reconstruction algorithm; on the other hand, once the training phase has been completed, generate the synthetically reconstructed datasets (S-GPDS and S-UST) that will be used in the validation stage.

Please cite this article in press as: M. Gomez-Barrero et al., A novel hand reconstruction approach and its application to vulnerability assessment, Inform. Sci. (2013), http://dx.doi.org/10.1016/j.ins.2013.06.015

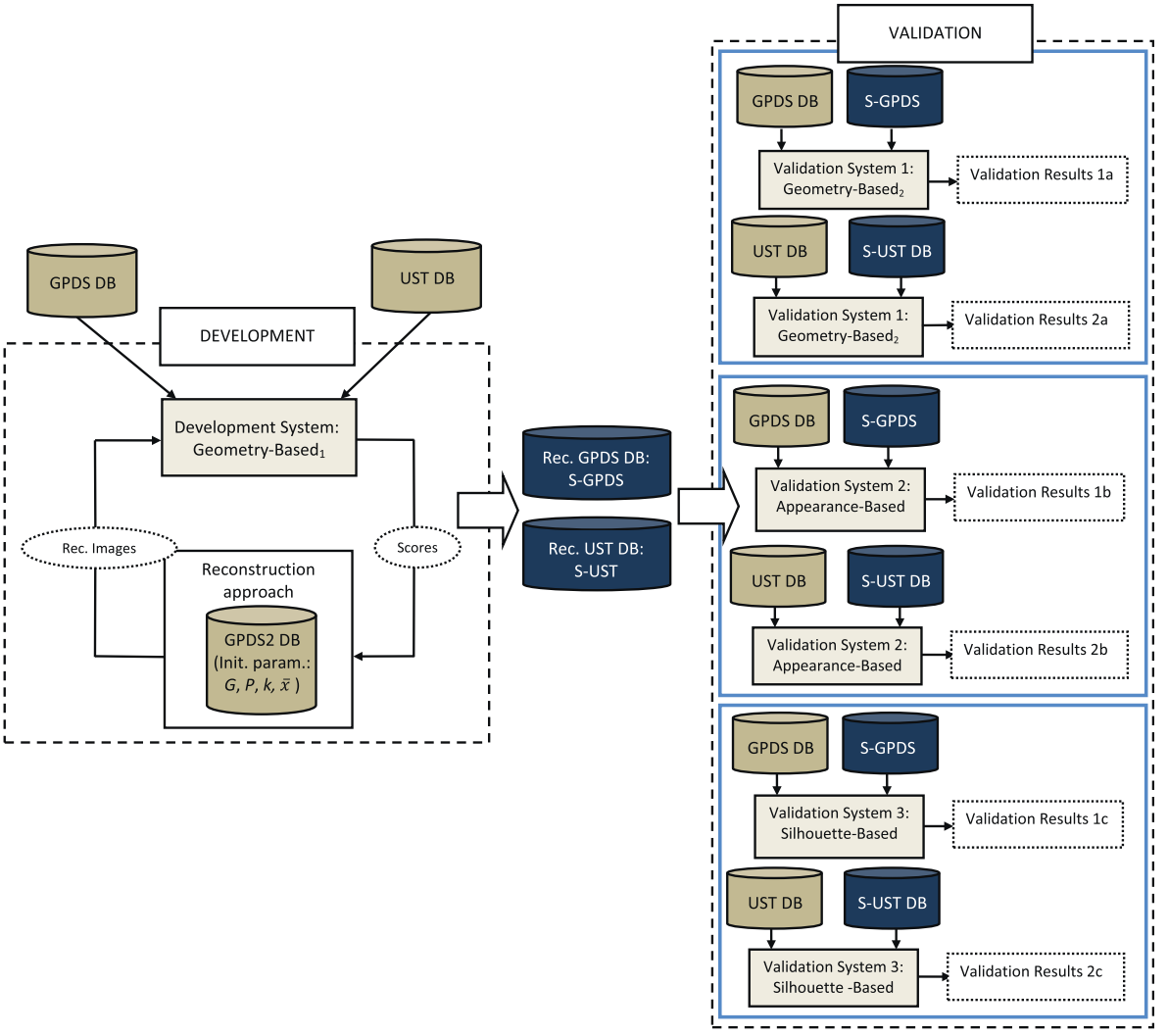

Fig. 4. Diagram of the experimental protocol followed in the present work. Both the real and the synthetic databases, as well as the systems used, are highlighted with a darker shade.

- *Validation*. The objective of this stage is to validate the proposed reconstruction scheme and to estimate its performance. For this purpose, the synthetically reconstructed samples generated in the development stage are presented to three different hand recognition systems to determine if they are positively matched to the genuine original images (which would mean the reconstruction approach is successful).

For the development and validation stages three different databases and four different hand recognition systems (described respectively in Sections 5.1 and 5.2) have been used in order to avoid biased results. All of them are either publicly available or well described in the literature so that the experiments are fully reproducible and the results here presented may be compared with future similar works.

5.1. Databases

The images used to train the hand generator and to compute the initialization parameters are taken from the GPDS2 database [50], while the real hand shape samples to be reconstructed are taken from the GPDS [20] and the UST [63] databases. It is important to notice that the images used to train the generator are independent and belong to completely different users than those being reconstructed. That way, the results obtained with the reconstruction method are not optimistically biased:

Please cite this article in press as: M. Gomez-Barrero et al., A novel hand reconstruction approach and its application to vulnerability assessment, Inform. Sci. (2013), http://dx.doi.org/10.1016/j.ins.2013.06.015

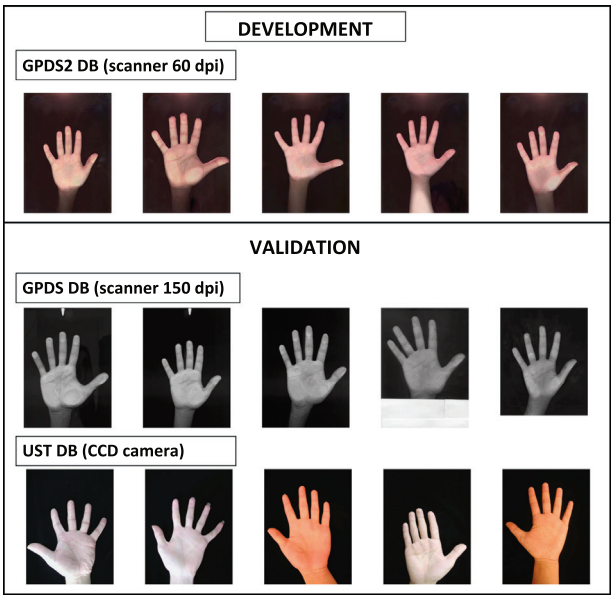

Fig. 5. Typical samples of the real databases used in the development (GPDS2 DB) and validation (GPDS DB and UST DB) steps of the experimental protocol.

- *Development: GPDS2 DB*. In order to train the hand-shape generator and initialize the Uphill Simplex (i.e., compute the initialization parameters G, P, k, $\bar{x}$), the GPDS2 DB [50] is used. This database comprises one sample of the right hand of 100 users, captured with a 60 dpi commercial scanner in one session. It should be noted that with such resolution (60 dpi) the hand shape is not very accurately defined, making it harder for the generator to learn the hand characteristics and compute high quality reconstructions.

Once the hand shape generator has been trained, it is combined with the Uphill Simplex algorithm as described in Section 4 to reconstruct the hand images from the real databases: GPDS DB and UST DB. As shown in Fig. 4, in the validation step each of the two synthetically reconstructed datasets (named S-GPDS DB and S-UST DB respectively) is used to evaluate the performance of the proposed reconstruction method: we try to access the three different recognition systems used for validation presenting a synthetic sample from the reconstructed database instead of a real image. The system will perform the comparison with the user model comprising only real images and output its decision: if access is granted it means that the synthetic reconstruction was positively matched to the genuine sample and that our goal of reverse engineering hand shape images from their templates was achieved. Therefore, the datasets used for validation are:

- *Validation: GPDS DB*.[1] The first set of images reconstructed using the proposed approach come from the GPDS dataset, which comprises 144 users with 10 images per user (only right hand of each subject). All of them were acquired in one session with a commercial digital scanner of 150 dpi at the University of Las Palmas de Gran Canaria [20], placing the right hand flat on the glass platen.
- *Validation: UST DB*. The second database used in the validation experiments comprises 564 users (right and left hands belonging to the same person are regarded as different users) with 10 images per user. Images were captured using a CCD camera (1280×960 pixels) by the Hong Kong University of Science and Technology [63]. The final version of this database has not been published yet and includes a small number of duplicates.
- *Validation: S-GPDS DB*. It comprises three synthetic reconstructed samples of each of the original 144 users in the GPDS DB. All the reconstructions are generated from the same randomly selected original sample as will be explained in Section 6.1.
- *Validation: S-UST DB*. It comprises three synthetic reconstructed samples of each of the original 564 users in the UST DB. As in the previous case, all the reconstructions are generated from the same randomly selected original sample.

It is important to notice that the capturing devices used in the acquisition of the two real databases to be reconstructed are completely different: the GPDS DB was captured using a digital scanner and the UST DB using a CCD camera. Thus, while hands are placed on a glass platen in the first case, leading to a certain distortion on the acquired image, hands belonging to the UST DB are captured using a contactless protocol so that no distortion is produced. This way we will be able to determine to what extent the proposed reconstruction approach is able to generate samples acquired under totally different conditions.

[1] Publicly available at http://www.gpds.ulpgc.es/download/index.htm.

Please cite this article in press as: M. Gomez-Barrero et al., A novel hand reconstruction approach and its application to vulnerability assessment, Inform. Sci. (2013), http://dx.doi.org/10.1016/j.ins.2013.06.015

We can observe the plastic distortion in the two databases captured with a scanner in Fig. 5: the GPDS2 DB (development stage) and the GPDS DB (validation stage). The difference in terms of resolution between the scanners used in both cases is also noticeable, especially in the distorted areas. On the other hand, the effect of different illumination conditions during the acquisition of the images of the UST DB (validation step) can be also observed in the last row of Fig. 5.

5.2. Hand recognition systems

Four different hand based recognition systems are used in the experiments, as can be seen in Fig. 4. In the development step, a geometry-based system is used to reconstruct the hand images, while in the validation step three systems based in different sets of features (namely, geometry-, appearance- and silhouette-related) are used to test whether the images obtained in the previous stage are positively matched to real samples of the genuine user by completely independent systems.

- *Development: geometry-based system* [19]. Geometric features of the hands (48 widths and 4 lengths from the little, ring, middle and index fingers) are obtained by measuring the widths and lengths of each finger. For verification, a least squares support vector machine (LS-SVM) is used to model each hand [65]. This system does not take into account any features obtained from the thumb as, due to their high variability, it has been demonstrated that they do not improve the performance of the geometry-based hand recognition systems [16].
- *Validation*. In order to prove the efficiency of the proposed approach, three different systems, based on distinct and independent features, are used for validation.
  - *Geometry-based system* [9]. Taking measures of the four fingers (excluding the thumb) lengths and widths, this system computes a dissimilarity measure, the Manhattan distance, between hand feature vectors.
  - *Appearance-based system* [74]. This system makes its decisions based on the whole hand shape, including the thumb, considering independent component features (ICA2) and images normalized after pose correction.
  - *Silhouette-based system* [19]. The method employed on this paper is based on direct silhouette alignment of 50 equal spaced samples of the finger contour of the hands excluding the thumb. The matching score is computed estimating the modified Hausdorff distance between the silhouettes of the fingers of two hands after an alignment that includes translation and rotation with no shape deformation.

It should be noted that according to Jain et al. [37], geometric features are somewhat correlated. Therefore, this kind of features are in some cases not sufficiently discriminative and for more demanding applications in terms of performance other additional independent features such as hand global shape or appearance should be considered. Since in the experiments described in the present work a geometry-based system is used at the development stage and an appearance-based system, among others, using independent and uncorrelated features, in the validation step, the results obtained are not positively biased.

6. Results

As it was already described in Section 5, experiments are carried out in two steps. First of all, in the development step, two completely different databases (GPDS DB and UST DB), acquired with different devices and conditions, are reconstructed using a geometry-based hand recognition system, thus leading to the generation of two synthetic databases (S-GPDS DB and S-UST DB). Afterwards, using three different systems, the validation experiments are performed: the synthetic images obtained in the development step are presented to each of the validation systems to determine if they are accepted as original or not.

The experimental framework has been designed not only to avoid biased results, but also to estimate the degree of compliance of the proposed reconstruction approach with the main objectives set in this work: (i) determine the feasibility of recovering a hand shape image from its template, (ii) evaluate to what extent the hand reconstructed images are able to compromise the security of hand recognition systems, and (iii) determine if it is possible to generate different synthetic samples from one given template.

Finally, a quality assessment study has been carried out. All the images of both the real and the synthetic databases are examined in order to determine if they are valid or non-valid hand images. Then the results of the real and the synthetic databases are compared, in order to determine the feasibility of developing a countermeasure against the detected vulnerability based on the quality of the presented images.

6.1. Development experiments: geometry-based system

Exhaustive development experiments were carried out on the GPDS2 DB to determine the four initialization parameters of the hand shape generator [13,14], namely: (i) the dimensionality (k) of the vector $\mathbf{y}$, which was finally set to $k = 50$ dimensions, thus taking into account 99.9% of the variance in the trained model; (ii) the PCA matrix P; (iii) the statistical model G, which was defined as a uniform distribution within the limits $\left[-3\sqrt{\lambda_j}, 3\sqrt{\lambda_j}\right]$, being λ_j the eigenvalue corresponding to the jth eigenvector of matrix P (with $j = 1,\ldots,k$); and iv) the mean $\bar{x}$ of the development set of hand shape images.

Please cite this article in press as: M. Gomez-Barrero et al., A novel hand reconstruction approach and its application to vulnerability assessment, Inform. Sci. (2013), http://dx.doi.org/10.1016/j.ins.2013.06.015

Table 1
Reconstruction rate and average number of comparisons needed to reconstruct a hand (in brackets) for the two databases reconstructed in the experiments (GPDS DB and UST DB). Results are given for the reconstruction method proposed in the present article and for an eventual brute force reconstruction (as baseline).

	GPDS DB	UST DB
Rec. method	100% (109)	100% (215)
Brute force	52% (15,746)	31% (17,562)

In [27], an exhaustive set of experiments was carried out in order to select the best possible values for the parameters of the Uphill Simplex (α, β and γ). Since the goal of the present work is not finding the optimal parameter set, but proving the efficiency and feasibility of the proposed reconstruction method as well as providing an estimation of the hand recognition systems vulnerabilities to the reconstruction scheme, no further experiments were carried out to determine new values for these parameters. Furthermore, by using the same feature values, we are also testing the robustness of the Uphill Simplex algorithm against different biometric traits.

In our previous work [27], we performed 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 [53], the best values for the parameters are $\alpha = 1$, $\gamma = 2$ and $\beta = 0.5$. Thus, the selected ranges were centred on those values, taking always into account the constraints explained in Section 4, namely: $\alpha > 0$, $\gamma > 1$ and $0 < \beta < 1$. Finally, the parameters values (that will be used in the experiments in the present research work) were set to $[\alpha, \gamma, \beta] = [1.1, 1.1, 0.8]$.

In order to determine the positive matching threshold δ at which a hand shape sample is considered to have been successfully reconstructed, the geometry-based recognition system performance was evaluated on the GPDS DB. Each of the 100 users comprised in the database was modelled with four samples randomly selected from the 10 samples available, and the matching process was repeated 10 times training the user models with four different samples (random selection) each time. In each of the 10 iterations of this process, genuine scores were computed matching the remaining six samples with the user model (i.e., $144 \times 6 \times 10 = 8640$ genuine scores), while impostor scores were generated comparing these same six samples of each user to the remaining users' models (i.e., $144 \times 143 \times 6 \times 10 = 1{,}235{,}520$ impostor scores). The threshold δ was finally fixed at the operating point corresponding to FAR = 0.01%, since the probability of having an impostor score at that point is very low: only one impostor in 10,000 would access the system. Thus, two hand shape images producing a similarity score greater than δ may be considered to belong to the same user.

After the initialization parameters were fixed, we reconstructed the hand shapes contained in the two real validation databases: GPDS DB and UST DB. Each user was modelled in the development system with just one randomly selected hand image, and three synthetic samples were generated using the reconstruction method proposed. Those synthetic samples constitute the synthetic validation databases: S-GPDS DB and S-UST DB.

For completeness and also as baseline result with which to compare the performance of our reconstruction method, a brute force reconstruction approach (i.e., an exhaustive search through a very large number of hand shape images) was also carried out. For this purpose, 20,000 synthetic hand shapes were randomly generated with the hand generator ($\mathbf{I_R}^m$ with $m = 1, \ldots, 20{,}000$). As the development system is working at an operating point where, on average, one *real* hand image in 10,000 would produce a false positive, it seems that 20,000 may be a reasonable amount of *synthetic* samples to find one that is assigned to a given real identity. Therefore, those images were matched to the users of each database (GPDS DB and UST DB) until one of the synthetic samples produced a score greater than δ. The number of comparisons needed by the brute force strategy to reconstruct a given hand is M, being $\mathbf{I_R}^M$ the first image that produced the winning score.

The results of both reconstruction approaches (the one proposed in the present article and the brute force method) are shown in Table 1, in terms of the reconstruction rate (i.e., percentage of successfully reconstructed hands) and the average number of comparisons necessary to reconstruct a hand image. We can observe that only around 40% of the hand shapes were recovered by the brute force scheme, while all of them were successfully reconstructed using the method proposed in the present work. Furthermore, the Uphill Simplex-based method is over 100 times faster than the brute force strategy. Therefore, not only the hand shapes are reconstructed with a considerably lower number of comparisons by the Uphill Simplex-based approach, but it also guarantees success in the reconstruction, in contrast to the brute force scheme.

Finally, in Fig. 6 the evolution of the hand shapes ($\mathbf{I_R}$) through the iterative reconstruction process for one user of each validation database is depicted. The score evolution is also shown, where the horizontal dashed line represents the objective threshold (δ). Starting from a random hand (iteration A), it can be seen that the successive synthetically generated samples evolve towards the original user hand (iterations B-E), until the score given by the development recognition system is higher than δ: the hand image has been successfully reconstructed (iteration F).

6.2. Validation experiments

As explained in Section 5, the reconstructed images (S-GPDS DB and S-UST DB) are used to try to access (i.e., attack) the validation systems. Since several systems are used in this validation step, and the appearance- and silhouette-based systems work on independent features with respect to the ones used by the development system (geometry-based), the results obtained in this validation stage for each database permit to evaluate in an objective way the ability of the proposed reconstruction approach to recover the hand-shape images from their templates.

Please cite this article in press as: M. Gomez-Barrero et al., A novel hand reconstruction approach and its application to vulnerability assessment, Inform. Sci. (2013), http://dx.doi.org/10.1016/j.ins.2013.06.015

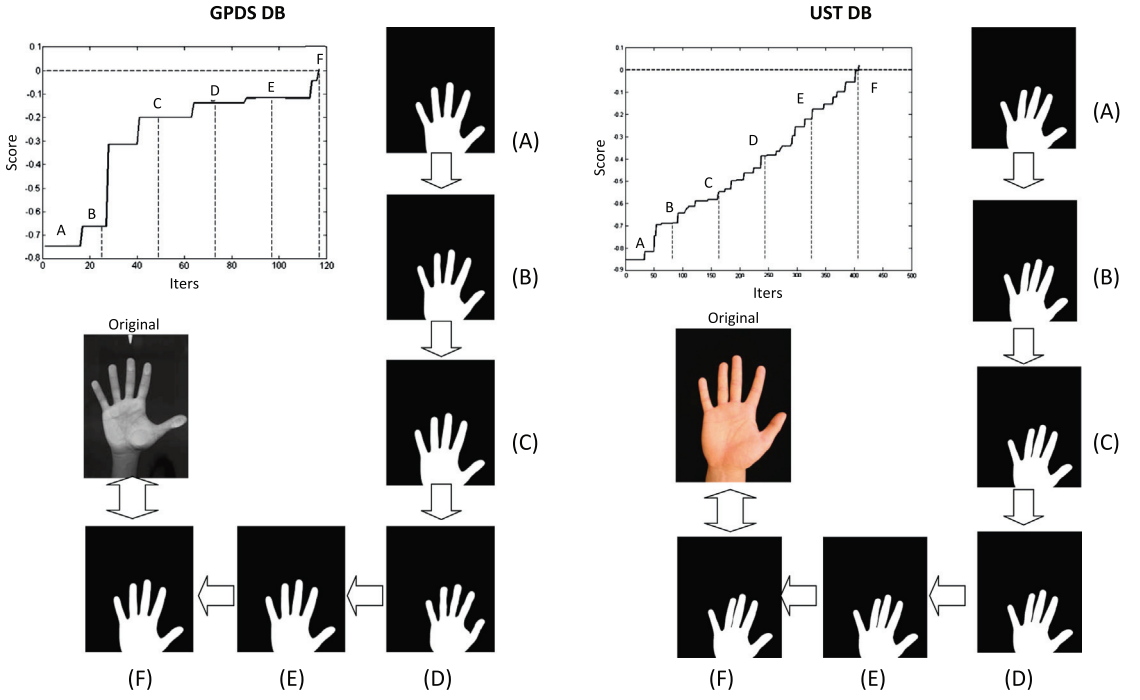

Fig. 6. Examples of the evolution of the score and the synthetic hand shapes through the iterations of the proposed algorithm for a successfully reconstructed hand shape of the GPDS DB (left) and of the UST DB (right). The horizontal dashed line represents the objective threshold (δ) where a sample is considered to have been successfully reconstructed.

The performance of the attacks is measured in terms of its Success Rate (SR), which is defined as the expected probability of bypassing the attacked system. It is computed as the ratio $SR = A_B/A_T$, where A_B is the number of broken accounts and A_T is the total number of attacked accounts. The SR thus gives an estimation of how dangerous the attack is: the higher the SR, the bigger the threat. The key factor to compute the SR is to define what constitutes an attack and when it is considered to be successful. In the experiments, three representative attacks will be considered in order to estimate the performance of the proposed reconstruction method:

Attack 1: 1 reconstruction *vs* 1 real. In this case the attack is carried out on a 1 on 1 basis. That is, one reconstructed image is matched against one real image and, if the resulting score exceeds the fixed matching threshold, the attack has been successful. Two possible scenarios may be distinguished in this case depending on the real image being attacked:

1.a. The real image being attacked is the original sample from which the synthetic images were reconstructed. In this scenario the total number of attacks performed which will be used to compute SR_{1a} is $A_{T1a} = 144 \times 3 = 432$ for the GPDS DB and $A_{T1a} = 564 \times 3 = 1692$ for the UST DB.

1.b. The real image being attacked is one of the other nine samples of the same user present in the corresponding validation DB. For this experiment the total number of attacks performed which will be used to compute A_{T1b} is $A_{T1b} = 144 \times 3 \times 9 = 3888$ for the GPDS DB and $A_{T1b} = 564 \times 3 \times 9 = 15{,}228$ for the UST DB.

Attack 2: 3 reconstructions *vs* 1 real. In this case all three reconstructions are matched against the real sample. The attack is successful if at least one of the synthetic images is able to access the system. This represents the most likely attack scenario analysed in other related vulnerability studies [12]: the template of the legitimate user is compromised and the intruder makes different reconstructions of the hand shape to try to break the system. The attacker will gain access if any of the reconstructions obtains a positive score. The same two scenarios as in attack 1 can be considered here, being the total number of attacks carried out in each of them $A_{T2a} = 144$ for the GPDS DB and $A_{T2a} = 564$ for the UST DB; $A_{T2b} = 144 \times 9 = 1296$ for the GPDS DB and $A_{T2b} = 564 \times 9 = 5076$ for the UST DB. The resulting success rates will be noted as SR_{2a} and SR_{2b}, respectively.

Attack 3: 3 reconstructions *vs* model (4 real). It is a common practice in many biometric recognition systems to match the test sample against a model trained with several stored templates. To emulate this scenario each reconstructed hand shape image is matched to the user model comprising four samples (randomly selected) of the real user in the corresponding database. The attack is successful if the final score returned by the system of any of the three reconstructions is higher than the given operating threshold. Thus, in this case, the total number of attacks performed in order to compute SR_3 is $A_{T3} = 144$ for the GPDS DB and $A_{T3} = 564$ for the UST DB.

Please cite this article in press as: M. Gomez-Barrero et al., A novel hand reconstruction approach and its application to vulnerability assessment, Inform. Sci. (2013), http://dx.doi.org/10.1016/j.ins.2013.06.015

In general, the success chances of an attack are highly dependent on the False Acceptance Rate (FAR) of the system. Thus, the vulnerability of the validation systems to the attacks with the reconstructed images is evaluated at three operating points corresponding to: FAR = 0.1%, FAR = 0.05%, and FAR = 0.01%, which, according to [4], correspond to a low, medium and high security application, respectively. For completeness, the system is also tested at a very high security operating point corresponding to FAR $\ll$ 0.01%.

Depending on the experiment at hand, these operating points are estimated (on the GPDS DB or the UST DB), considering user models computed with either one hand image (for attacks 1 and 2) or four hand images (attack 3) for each of the validation systems tested.

Several observations can be made from the results of the validation experiments shown in Tables 2–7:

The high performance of the reconstruction algorithm is confirmed. As expected, the performance of the synthetic images is higher when a system based on the same kind of features as the ones used in the development stage (hand geometry) is used. However, the SR for the other validation systems, based on completely independent sets of features, remains considerably high:

- In the case of the geometry-based recognition system, the SR reaches an average SR of over 85% for the three usual operating points considered and over 90% for the most likely attacking scenario for the UST DB (i.e., SR_{2a}).
- For the other two validation systems (appearance- and alignment-based), the SR remains between 50% and 60% on average for the three usual operating points considered.

Even for an unrealistically high security point (i.e., FAR $\ll$ 0.01%), the reconstructed images would have, on average,

- Around 80% chances of entering the geometry-based system for both databases tested.
- Between 30% and 45% chances of breaking the system for the GPDS DB and over 35% for the UST DB under the appearance- and silhouette-based systems.

The results are very similar for the appearance- and silhouette-based systems. The only significant difference is the decrease of the SR for the latter when working on the UST DB. The reason behind this worsening is a decrease in the performance of the system: silhouette alignment is not as competitive as in the case of the GPDS DB due to projection distortions caused by the camera acquisition scenario, which leads to a higher EER. Thus, for identical FAR operating points, the FRR is higher and therefore more hand images within the intra-user variability are rejected.

Table 2
SR of the different attacking scenarios considered against the *geometry-based system* using the GPDS DB at the four operating points tested.

FAR (%)	GPDS DB – Geometry-based system					
	SR_{1a}	SR_{1b}	SR_{2a}	SR_{2b}	SR_3	*Average*
0.1	90.26	87.52	90.26	87.52	92.58	89.63
0.05	88.96	85.89	88.96	85.89	90.61	88.06
0.01	85.41	83.27	85.41	83.27	87.37	84.95
$\ll$0.01	78.97	75.96	78.97	75.96	81.05	78.20

Table 3
SR of the different attacking scenarios considered against the *appearance-based system* using the GPDS DB at the four operating points tested.

FAR (%)	GPDS DB – Appearance-based system					
	SR_{1a}	SR_{1b}	SR_{2a}	SR_{2b}	SR_3	*Average*
0.1	58.82	53.38	58.82	53.38	60.78	57.04
0.05	52.94	41.39	52.94	41.39	58.82	49.50
0.01	50.98	36.60	50.98	36.60	54.90	46.01
$\ll$0.01	31.37	23.97	31.37	23.97	43.14	30.76

Table 4
SR of the different attacking scenarios considered against the *silhouette-based system* using the GPDS DB at the four operating points tested.

FAR (%)	GPDS DB – Silhouette-based system					
	SR_{1a}	SR_{1b}	SR_{2a}	SR_{2b}	SR_3	*Average*
0.1	62.52	61.28	62.52	61.28	65.27	62.57
0.05	60.26	51.02	60.26	51.02	63.57	57.23
0.01	58.92	40.65	58.92	40.65	61.49	52.13
$\ll$0.01	45.25	34.97	45.25	34.97	55.66	43.22

Please cite this article in press as: M. Gomez-Barrero et al., A novel hand reconstruction approach and its application to vulnerability assessment, Inform. Sci. (2013), http://dx.doi.org/10.1016/j.ins.2013.06.015

Table 5
SR of the different attacking scenarios considered against the *geometry-based* system using the UST DB at the four operating points tested.

FAR (%)	UST DB – Geometry-based system					
	SR_{1a}	SR_{1b}	SR_{2a}	SR_{2b}	SR_3	*Average*
0.1	93.29	90.59	93.29	90.59	95.68	92.69
0.05	92.58	88.95	92.58	88.95	94.56	91.52
0.01	90.15	86.21	90.15	86.21	92.98	89.14
$\ll$0.01	80.27	78.51	80.27	78.51	85.24	80.56

Table 6
SR of the different attacking scenarios considered against the *appearance-based system* using the UST DB at the four operating points tested.

FAR (%)	UST DB – Appearance-based system					
	SR_{1a}	SR_{1b}	SR_{2a}	SR_{2b}	SR_3	*Average*
0.1	63.58	57.97	63.58	57.97	66.21	61.86
0.05	57.25	43.46	57.25	43.46	63.25	52.93
0.01	54.69	40.65	54.69	40.65	59.82	50.10
$\ll$0.01	38.25	29.52	38.25	29.52	51.29	37.37

Table 7
SR of the different attacking scenarios considered against the *silhouette-based system* using the UST DB at the four operating points tested.

FAR (%)	UST DB – Silhouette-based system					
	SR_{1a}	SR_{1b}	SR_{2a}	SR_{2b}	SR_3	*Average*
0.1	52.36	50.28	52.36	50.28	53.24	51.70
0.05	50.53	47.52	50.53	47.52	51.98	49.62
0.01	48.27	44.59	48.27	44.59	50.37	47.22
$\ll$0.01	35.67	33.28	35.67	33.28	45.29	36.64

The probabilities of accessing the system in the scenarios 1.a and 2.a, 1.b and 2.b are the same for each validation system considered. This means that the validation system is quite robust to several initializations of the Uphill Simplex algorithm (i.e., reconstructions of the same template). This way, the scores given by the system do not vary significantly among reconstructions, which means that either all three or none of them are able to access the system.

As expected, it is more probable that the synthetic samples are positively matched to the original image from which they were reconstructed than to other real images of the same user (see the decrease in the SR between SR_{1a} *vs* SR_{1b} and between SR_{2a} *vs* SR_{2b}).

Even so, the reconstructed images still present a high probability of breaking the system even when the stored templates are not the one from which they were recovered (average SR of SR_{1b} and SR_{2b} around 45% for the appearance- and silhouette-based systems).

Furthermore, for the case of using several real samples of the user for verification (SR_3), the reconstructed samples are still able to access the system for:

- Around 92% of the attempts in the usual operating points, and for almost 80% in the extremely high operating point tested for the geometry-based validation system.
- Around 60% of the attempts in the usual operating points, and for almost 50% in the extremely high operating point tested for the remaining two validation systems.

The results presented in Tables 2–7 confirm the first and second objectives set in the present work: hand shape images may be recovered from their templates, and the reconstructed images represent a real threat to the integrity of automatic recognition systems. Recall that the third goal of the work is to determine the feasibility of generating multiple synthetic hand images that yield templates very similar to a real one. In order to address this point, results from experiment 2.a (i.e., all 3 synthetic images are compared to the original from which they were reconstructed) are presented in Tables 8–10 from a different perspective. In this case we present in each column the percentage of attacks in which only n out of the three reconstructed images (with $n = 1,2,3$) were positively matched to their original real image. For all cases the total attacks performed is $A_{Tn} = 144$ for the GPDS DB and $A_{Tn} = 564$ for the UST DB, and the success rate will be noted as SR_n.

As it can be observed, for all the operating points tested, either all the synthetic samples ($n = 3$) or none of them were able to access the system: the columns $n = 1$ and $n = 2$ show a SR of 0% in all cases. This means that for all the users, it never occurred that only 1 or 2 of the reconstructions were positively matched to the user model. However, averaging the four at-

Please cite this article in press as: M. Gomez-Barrero et al., A novel hand reconstruction approach and its application to vulnerability assessment, Inform. Sci. (2013), http://dx.doi.org/10.1016/j.ins.2013.06.015

Table 8
Percentage of successful attacks where n out of the total three reconstructions were positively matched against the original hand image from which they were reconstructed. Results are given for the four operating points tested on the *geometry-based recognition system*.

FAR	GPDS DB			UST DB		
	$n = 1$	$n = 2$	$n = 3$	$n = 1$	$n = 2$	$n = 3$
0.1%	0	0	90.26	0	0	93.29
0.01%	0	0	88.96	0	0	92.58
0.05%	0	0	85.41	0	0	90.15
$\ll$0.01%	0	0	78.97	0	0	80.27
Average	0	0	85.9	0	0	89.1

Table 9
Percentage of successful attacks where n out of the total three reconstructions were positively matched against the original hand image from which they were reconstructed. Results are given for the four operating points tested on the *appearance-based recognition system*.

FAR	GPDS DB			UST DB		
	$n = 1$	$n = 2$	$n = 3$	$n = 1$	$n = 2$	$n = 3$
0.1%	0	0	58.82	0	0	63.58
0.01%	0	0	52.94	0	0	57.25
0.05%	0	0	50.98	0	0	54.69
$\ll$0.01%	0	0	31.37	0	0	38.25
Average	0	0	48.6	0	0	53.4

Table 10
Percentage of successful attacks where n out of the total three reconstructions were positively matched against the original hand image from which they were reconstructed. Results are given for the four operating points tested on the *silhouette-based recognition system*.

FAR	GPDS DB			UST DB		
	$n = 1$	$n = 2$	$n = 3$	$n = 1$	$n = 2$	$n = 3$
0.1%	0	0	62.52	0	0	52.36
0.01%	0	0	60.26	0	0	50.53
0.05%	0	0	58.92	0	0	48.27
$\ll$0.01%	0	0	45.25	0	0	35.67
Average	0	0	56.7	0	0	46.7

tacked operating points, all three reconstructions ($n = 3$) were positively matched to the original image for around 55% of the cases. These results confirm the third objective of the work: the ability of the proposed probabilistic reconstruction algorithm to generate multiple hand shapes that match one specific template.

But, why is this the case? Why do either all or none of the reconstructed images of one user are able to access the system? A probable explanation to this fact is that, as previously explained in Section 6.1, the initialization parameters for both the Uphill Simplex (G distribution) and the hand shape generator (average hand $\bar{x}$ and PCA matrix P) remain constant across executions of the global algorithm: even though the G distribution is randomly sampled, the distribution does not change; and the same data is used to compute $\bar{x}$ and P. Therefore, the proposed method is able to reconstruct a hand sample as long as it lies within the variability range found in the development database: GPDS2 DB. This way, the reconstructed hand shapes deceive the system for a given user either always ($n = 3$) or never ($n = 0$): in the first case, the user samples fall within the development data variability range, while in the second case the user discriminative characteristics are not modelled by the development dataset. Thus, in order to achieve a higher overall SR, the development database should be as big and statistically significant as possible.

It should also be noted that the experiments have also proven that the reconstruction method is robust to:

- Databases acquired under totally different conditions: in the GPDS DB a scanner where the hands were placed flat on the surface (thus leading to a certain degree of distortion in the images) was used, while the images of the UST DB were acquired with a CCD camera (no contact plastic distortion).
- Systems based on different sets of features: even though a geometry-based system was used in the development step, while in the validation stage experiments were carried out on systems based on geometric, general appearance- and silhouette-related features, the SR of the attacks was over 50% for the three realistic operating points tested.

Please cite this article in press as: M. Gomez-Barrero et al., A novel hand reconstruction approach and its application to vulnerability assessment, Inform. Sci. (2013), http://dx.doi.org/10.1016/j.ins.2013.06.015

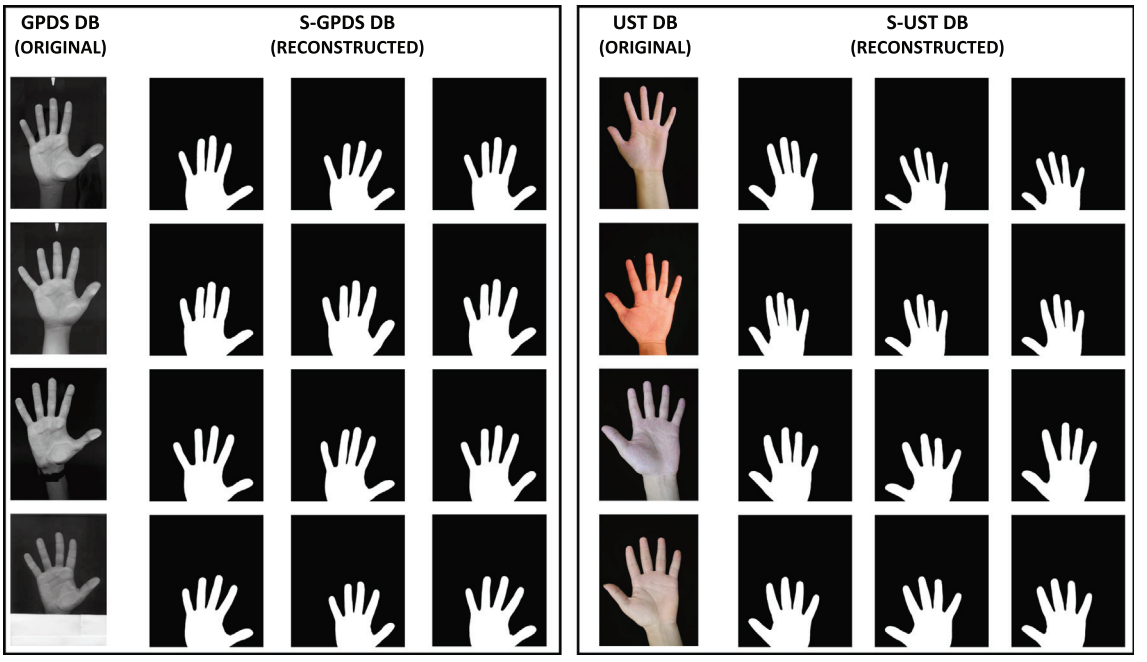

Fig. 7. Typical hand images that can be found in the real database (first column) with the three corresponding reconstructions (second to fourth columns) for the GPDS DB (left) and the UST DB (right).

Finally, in Fig. 7 some samples of both real and reconstructed hand images coming from the GPDS DB, S-GPDS DB, UST DB and S-UST DB are depicted. As can be observed, the reconstructed hand shapes capture all the details of the original user hands, such as the thick and short fingers of the fourth hand in the UST DB or the different curvatures of the outer part of the hand. Furthermore, we can also see that the three reconstructions of the same image vary among themselves as could be expected from different real samples of the same user (i.e., intra-user variability): the position of the fingers is not the same in the three images and even the shape of the fingers is slightly different.

6.3. Quality assessment

Even though quality assessment is a key research topic in biometric recognition [24,3], not many quality-related studies have been carried out on geometry hand recognition and, to the best of our knowledge, all of them classify samples as either valid or non valid (no quality measure is given) [10]. Furthermore, low-quality samples are usually quantified by means of the Failure To Enrol (FTE, for training) and Failure To Acquire (FTA, for recognition) rates [42].

Although experimental results presented in Sections 6.1 and 6.2 have proven the ability of the proposed reconstruction approach to generate realistic synthetic samples that are positively matched to the original one by a set of different recognition algorithms, in this section the appearance of the reconstructed samples is further analysed from a quality-based perspective.

The main objective of the experimental setup is to determine whether the synthetic images present a similar quality level (in terms of anatomical appearance) to that of the real samples, according to some automatic assessment tool. For this purpose, the algorithm proposed in [10] is used. Several steps are followed before reaching a valid/non-valid decision:

- Segment the hand from the background.
- Extract hand contour and measure finger widths.
- Compute ratios between finger lengths in order to assess whether the measurements are anatomically correct. If each of the quality ratios computed lies within a previously estimated (according to pre-annotated good quality images) valid range, the hand is accepted as valid; otherwise, it is discarded as non-valid. Further details about the different steps performed by this automatic quality assessment application are given in [10].

With this approach, low-quality images presenting damp on the scanner surface or other kinds of artefacts, are automatically detected and discarded: hand contours are not correctly extracted and therefore measurements are inaccurate. Similarly, if a synthetic hand image presents deformities such as irregular fingers or extremely deep valleys, this quality module will detect them.

In Table 11, the percentage of valid images of each of the databases used in the experiments is shown. The real databases do not present invalid images, as it was expected: the acquisition scenarios were controlled and lead to high-quality samples.

Please cite this article in press as: M. Gomez-Barrero et al., A novel hand reconstruction approach and its application to vulnerability assessment, Inform. Sci. (2013), http://dx.doi.org/10.1016/j.ins.2013.06.015

Table 11
Percentage of valid samples for the real (GPDS and UST DB) and synthetic (S-GPDS and S-UST DB) databases.

GPDS DB	S-GPDS DB	UST DB	S-UST DB
100%	75.30%	100%	68.60%

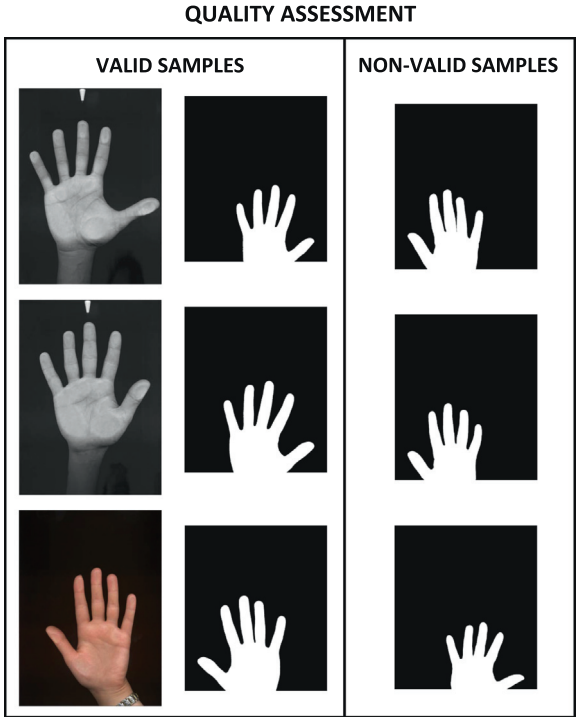

Fig. 8. Valid (on the left) and non-valid (on the right) images that may be found in the validation databases used in the experiments. Right hands belong to the UST DB while left hands belong to the GPDS DB.

For the synthetic databases generated in the previous experiments, the percentage of valid samples is also high: around 70%. Therefore, these quality-related results confirm those obtained in Sections 6.1 and 6.2 about the efficiency of the proposed reconstruction method to generate realistic and anatomically feasible hand shape samples.

Some examples of valid and non-valid reconstructed images together with the genuine samples from which they were generated are shown in Fig. 8. We can observe how non-valid synthetic images show fingers with bizarre contours (first sample), curved fingers (second sample) or protuberances on the hand shape (third sample). On the contrary, valid samples present the characteristics of actual hand images, as expected.

7. Conclusions

The experiments carried out in the present work show that the information stored on hand shape templates is enough to retrieve the original hand image, regardless of the data format and the features used for recognition. This poses serious security and privacy issues that should be taken into account by the biometric community in order to prevent that user templates are compromised or, in case they are, to detect fraudulent access attempts using reconstructed samples. This way, we may consider two different approaches to prevent this vulnerability, namely:

- Prevention, that is, try to avoid the users' templates being compromised. We could, for example, securely store biometric data or protect the communication channels through encryption [66].
- Protection, that is, try to minimize the probabilities of the attack of breaking into the system should a template be compromised. This would be the case of biometric-based countermeasures to detect synthetic from real hand images such as the liveness-detection techniques [60,78].

It may be argued that, for attacks such as the one considered in this work to be successful, the original templates must firstly fall in the wrong hands. In classic biometric systems where the enrolled templates are kept in a centralized database

Please cite this article in press as: M. Gomez-Barrero et al., A novel hand reconstruction approach and its application to vulnerability assessment, Inform. Sci. (2013), http://dx.doi.org/10.1016/j.ins.2013.06.015

this may be difficult, yet possible: the attacker would have to extract the information from the database or intercept the communication channel when the stored template is released for matching.

However, Match-on-Card (MoC) applications are rapidly growing due to several appealing characteristics such as their privacy (you carry the only copy of your biometric data) and scalability [6]. In these systems the matching is performed inside a smartcard where the enrolled template of the user is also stored. This smartcard could be easily lost or stolen. Furthermore, biometric data is being stored in many official documents such as the new biometric passport [33], some national ID cards [29], or the US FIPS-201 Personal Identity Verification initiatives (PIV) [54] and the ILO Seafarers Identity Card Program [34]. With this kind of systems, templates are more likely to be compromised as it is easier for the attacker to have physical access to the storage device and fraudulently obtain the information contained inside as has already been proven [5]. This makes MoC systems potentially more vulnerable to the type of threat described in this article.

In either case, centralized or MoC systems, the present work has proven that attacks using reconstructed hand images constitute a real threat, stressing out the importance of equipping automatic recognition systems with all the necessary countermeasures against it.

Research works such as the one presented in this article pretend to increase the existing knowledge on the hand trait and to shed some light into the difficult problem of biometric security evaluation. Performing systematic studies of biometric systems vulnerabilities is essential before effective countermeasures that minimize the effects of the detected threats can be developed, in order to increase the confidence of the final users in this thriving technology.

Other possible applications of the proposed reconstruction method that may be studied as part of future work include:

- The use of different reconstructed samples of one same user to enlarge existing databases for research purposes such as improving the performance of recognition systems: the more training samples we have, the better the system learns the intraclass variability of each user.
- The possibility of using this approach to reconstruct different biometric traits. The reconstruction algorithm could be generalized to reconstruct potentially any trait by using the Uphill Simplex algorithm to optimize the input of the appropriate generator (e.g., iris, fingerprint or face generator).

Acknowledgements

This work has been partially supported by projects Contexts (S2009/TIC-1485) from CAM, Bio-Challenge (TEC2009-11186), BIOSINT (TEC2012-38630-C04-02) and Bio-Shield (TEC2012-34881) from Spanish MINECO, TABULA RASA (FP7-ICT-257289) and BEAT (FP7-SEC-284989) from EU, and *Cátedra UAM-Telefónica*. Marta Gomez-Barrero is supported by a FPU Fellowship from Spanish MECD.

References

[1] A. Adler, Sample images can be independently restored from face recognition templates, in: Proc. Canadian Conference on Electrical and Computer Engineering (CCECE), vol. 2, 2003, pp. 1163–1166.
[2] A. Adler, Images can be regenerated from quantized biometric match score data, in: Proc. Canadian Conference on Electrical and Computer Engineering (CCECE), 2004, pp. 469–472.
[3] F. Alonso-Fernandez, J. Fierrez, J. Ortega-Garcia, Quality measures in biometric systems, IEEE Security and Privacy 99 (2011) 1.
[4] ANSI/NIST, NIST ITL American National Standards for Biometrics, 2009. <http://fingerprint.nist.gov/standard/>.
[5] J. van Beek, ePassports Reloaded, in: Black Hat USA Briefings, 2008.
[6] C. Bergman, Advances in biometrics: sensors, algorithms and systems, in: Advances in Biometrics: Sensors, Algorithms and Systems, Springer, 2008, pp. 407–422.
[7] M. Bober, Mpeg-7 visual shape descriptors, IEEE Transactions on Circuits and Systems for Video Technology 11 (2001) 716–719.
[8] Y. Bulatov, S. Jambawalikar, P. Kumar, S. Sethia, Hand recognition using geometric classifiers, in: Proc. DIMACS Workshop on Computational Geometry, 2002, pp. 14–16.
[9] J. Burgues, J. Fierrez, D. Ramos, J. Ortega-Garcia, Feature selection in a hand geometry recognition system, in: Proc. of BioID-Multicomm, Springer LNCS-5707, 2009, pp. 325–332.
[10] J. Burgues, J. Fierrez, D. Ramos, M. Puertas, J. Ortega-Garcia, Detecting invalid samples in hand geometry verification through geometric measurements, in: Proc. Int. Conf. on Pattern Recognition, 2010.
[11] R. Cappelli, Handbook of Fingerprint Recognition, Handbook of Fingerprint Recognition, Springer, 2003.
[12] R. Cappelli, D. Maio, A. Lumini, D. Maltoni, Fingerprint image reconstruction from standard templates, IEEE Transactions on Pattern Analysis and Machine Intelligence 29 (2007) 1489–1503.
[13] T.F. Cootes, G.J. Edwards, C.J. Taylor, Active appearance models, IEEE Transactions on Pattern Analysis and Machine Intelligence 23 (2001) 681–685.
[14] T.F. Cootes, C.J. Taylor, D.H. Cooper, J. Graham, Active shape models – their training and application, Computer Vision and Image Understanding 61 (1995) 38–59.
[15] J. Cui, Y. Wang, J. Huang, T. Tan, Z. Sun, An iris image synthesis method based on PCA and super-resolution, in: Proc. IAPR Int. Conf. on Pattern Recognition (ICPR), 2004, pp. 471–474.
[16] N. Duta, A survey of biometric technology based on hand shape, Pattern Recognition 42 (2009) 2797–2806.
[17] H. Dutagaci, B. Sankur, E. Yrk, Comparative analysis of global hand appearance-based person recognition, Journal of Electronic Imaging 17 (2008).
[18] T. Dutoit, An Introduction to Text-to-Speech Synthesis, Kluwer Academic Publishers, 2001.
[19] M.A. Ferrer, A. Morales, Hand-shape biometrics combining the visible and short-wave infrared bands, IEEE Transactions on Information Forensics and Security 6 (2011) 1305–1314.

Please cite this article in press as: M. Gomez-Barrero et al., A novel hand reconstruction approach and its application to vulnerability assessment, Inform. Sci. (2013), http://dx.doi.org/10.1016/j.ins.2013.06.015

[20] M.A. Ferrer, A. Morales, C.M. Travieso, J.B. Alonso, Low cost multimodal biometric identification system based on hand geometry, palm and finger print texture, in: Proc. IEEE Int. Carnahan Conf. on Security Technology, 2007, pp. 55–58.
[21] M.A. Ferrer, A. Morales, C.M. Travieso, J.B. Alonso, Wide band spectroscopic skin detection for contactless hand biometrics, IET Computer Vision 6 (2012) 415–424.
[22] J. Fierrez, J. Ortega-Garcia, On-line signature verification, in: On-line Signature Verification, Springer, 2008, pp. 189–209.
[23] T. Funkhouser, P. Min, M. Kazhdan, J. Chen, A. Halderman, D. Dobkin, A search engine for 3d models, ACM Transactions on Graphics 22 (2003) 83–105.
[24] J. Galbally, F. Alonso-Fernandez, J. Fierrez, J. Ortega-Garcia, A high performance fingerprint liveness detection method based on quality related features, Future Generation Computer Systems 28 (2012) 311–321.
[25] J. Galbally, R. Cappelli, A. Lumini, G.G. de Rivera, D. Maltoni, J. Fierrez, J. Ortega-Garcia, D. Maio, An evaluation of direct and indirect attacks using fake fingers generated from ISO templates, Pattern Recognition Letters 31 (2010) 725–732.
[26] J. Galbally, C. McCool, J. Fierrez, S. Marcel, On the vulnerability of face verification systems to hill-climbing attacks, Pattern Recognition 43 (2010) 1027–1038.
[27] M. Gomez-Barrero, J. Galbally, J. Fierrez, J. Ortega-Garcia, 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), LNCS-6583, 2011, pp. 83–94.
[28] M. Gomez-Barrero, J. Galbally, A. Morales, M.A. Ferrer, J. Fierrez, J. Ortega-Garcia, Inverse biometrics: a case study in hand geometry authentication, in: Proc. Int. Conf. on Patter Recognition (ICPR), 2012.
[29] Government of Spain, 2006. <http://www.dnielectronico.es/>.
[30] Z. Guo, D. Zhang, L. Zhang, W. Zuo, Palmprint verification using binary orientation co-occurrence vector, Pattern Recognition Letters 30 (2009) 1219–1227.
[31] C.J. Hill, Risk of Masquerade Arising from the Storage of Biometrics, Master's Thesis, Australian National University, 2001.
[32] H. Holmes, L. Wright, R. Maxwell, A Performance Evaluation of Biometric Identification Devices, Technical Report, Sandia National Laboratories, 1991.
[33] ICAO, ICAO Document 9303, Part 1, Volume 2: Machine Readable Passports – Specifications for Electronically Enabled Passports with Biometric Identification Capability, 2006.
[34] ILO, ILO SID-0002, Finger Minutiae-Based Biometric Profile for Seafarers Identity Documents, Intl Labour Organization, 2006.
[35] International Biometric Group, Generating Images from Templates, White Paper, 2002.
[36] A.K. Jain, N. Duta, Deformable matching of hand shapes for verification, in: Proc. Int. Conf. on Image Processing (ICIP), 1999.
[37] A.K. Jain, A. Ross, S. Pankanti, A prototype hand geometry-based verification system, in: Proc. Int. Conf. on Audio and Video-Based Biometric Person Authentication (AVBPA), 1999.
[38] A.K. Jain, A. Ross, S. Pankanti, Biometrics: a tool for information security, IEEE Transactions on Information Forensics and Security 1 (2006) 125–143.
[39] A.K. Jain, A.A. Ross, K. Nandakumar, Introduction to biometrics, in: Introduction to Biometrics, Springer, 2011, pp. 186–190.
[40] D.H. Klatt, Software for a cascade/parallel formant synthesizer, Journal Acoustic Society of America 67 (1980) 971–995.
[41] E. Konukoglu, E. Yrk, J. Darbon, B. Sankur, Shape-based hand recognition, IEEE Transactions on Image Processing 15 (2006) 1803–1815.
[42] E. Kukula, S. Elliott, Implementation of hand geometry: an analysis of user perspectives and system performance, IEEE Transactions on Aerospace and Electronic Systems 21 (2006) 3–9.
[43] A. Kumar, D. Zhang, Combining fingerprint, palmprint and hand-shape for user authentication, in: Proc. International Conference on Pattern Recognition (ICPR), 2006, pp. 549–552.
[44] A. Kumar, D. Zhang, Integrating shape and texture for hand verification, International Journal of Image & Graphics 6 (2006) 101–114.
[45] A. Kumar, D. Zhang, Personal recognition using hand shape and texture, IEEE Transactions on Image Processing 15 (2006) 2454–2461.
[46] A. Kumar, D. Zhang, Hand geometry recognition using entropy-based discretization, IEEE Transactions on Information Forensics and Security 2 (2007) 181–187.
[47] A. Lin, L. Wang, Style-preserving english handwriting synthesis, Pattern Recognition 40 (2007) 2097–2109.
[48] J.H. Mathews, K.K. Fink, Numerical methods using Matlab, in: Numerical Methods Using Matlab, Prentice-Hall Inc., 2004, pp. 430–436.
[49] B. Miller, Vital signs of identity, IEEE Spectrum 32 (1994) 22–30.
[50] A. Morales, E. Gonzlez, M.A. Ferrer, On the feasibility of interoperable schemes in hand biometrics, Sensors 12 (2012) 1352–1382.
[51] M. Mori, A. Suzuki, A. Shio, S. Ohtsuka, Generating new samples from handwritten numerals based on point correspondence, in: Proc. IAPR Int. Workshop on Frontiers in Handwriting Recognition (IWFHR), 2000, pp. 281–290.
[52] M.E. Munich, P. Perona, Visual identification by signature tracking, IEEE Transactions on Pattern Analysis and Machine Intelligence 25 (2003) 200–217.
[53] J.A. Nelder, R. Mead, A simplex method for function minimization, Computer Journal 7 (1965) 313–368.
[54] NIST, NIST Special Publication 800-76, Biometric Data Specification for Personal Identity Verification, 2005.
[55] C. Oliveira, C.A. Kaestner, F. Bortolozzi, R. Sabourin, Generation of signatures by deformations, in: Proc. IAPR Int. Conf. on Advances in Document Image Analysis (ICADIA), vol. 1339, Springer LNCS, 1997, pp. 283–298.
[56] N.B. Pinto, D.G. Childers, A.L. Lalwani, Formant speech synthesis: improving production quality, IEEE Transactions on Acoustics, Speech and Signal Processing 37 (1989) 1870–1887.
[57] N. Poh, S. Marcel, S. Bengio, Improving face authentication using virtual samples, in: Proc. IEEE Int. Conf. on Acoustics, Speech and Signal Processing (ICASSP), 2003.
[58] D.V. Popel, Synthesis and analysis in biometrics, in: Synthesis and Analysis in Biometrics, World Scientific, 2007, pp. 31–63.
[59] A. Ross, J. Shah, A.K. Jain, From template to image: reconstructing fingerprints from minutiae points, IEEE Transactions on Pattern Analysis and Machine Intelligence 29 (2007) 544–560.
[60] R. Rowe, U. Uludag, M. Demirkus, S. Parthasaradhi, A. Jain, A multispectral whole-hand biometric authentication system, in: Proc. Biometric Symposium Biometric Consortium Conference, 2007.
[61] R. Sanchez-Reillo, C. Sanchez-Avila, A. Gonzalez, Biometric identification through hand geometry measurements, IEEE Transactions on Pattern Analysis and Machine Intelligence 22 (2000) 1168–1171.
[62] B. Schneier, The uses and abuses of biometrics, Communications of the ACM 48 (1999) 136.
[63] D. of Computer Science The Hong Kong University of Science, Technology, UST Hand Image Database, 2008 (Provided by Dr. Helen Shen).
[64] S. Shah, A. Ross, Generating synthetic irises by feature agglomeration, in: Proc. IEEE Int. Conf. on Image Processing (ICIP), 2006, pp. 317–320.
[65] J. Suykens, T.V. Gestel, J.D. Brabanter, B.D. Moor, J. Vandewalle, L east Squares Support Vector Machines, World Scientific, Singapor, 2002.
[66] U. Uludag, S. Pankanti, S. Prabhakar, A.K. Jain, Biometric cryptosystems: issues and challenges, Proceedings of the IEEE 92 (2004) 948–960.
[67] S. Venugopalan, M. Savvides, How to generate spoofed irises from an iris code template, IEEE Transactions on Information Forensics and Security 6 (2011) 385–394.
[68] H. Wang, L. Zhang, Linear generalization probe samples for face recognition, Pattern Recognition Letters 25 (2004) 829–840.
[69] J. Wang, C. Wu, Y.Q. Xu, H.Y. Shum, L. Ji, Learning-based cursive handwriting synthesis, in: Proc. IAPR Int. Workshop on Frontiers of Handwriting Recognition (IWFHR), 2002, pp. 157–162.
[70] H.R. Wilson, G. Loffler, F. Wilkinson, Synthetic faces, face cubes, and the geometry of face space, Vision Research 42 (2002) 2909–2923.
[71] A.L.N. Wong, P. Shi, Peg-free han geometry recognition using hierarchical geometry and shape matching, in: Proc. IAPR Workshop on Machine Vision Applications (WMVA), 2002.
[72] M. Wong, D. Zhang, W. Kong, G. Lu, Real-time palmprint acquisition system design, in: IEEE Proc. Vision, Image and Signal Processing, vol. 152, 2005, pp. 527–534.
[73] E. Yrk, H. Dutagaci, B. Sankur, Hand biometrics, Image and Vision Computing 24 (2006) 483–497.
[74] E. Yrk, E. Konkoglu, B. Sankur, J. Darbon, Shape-based hand recognition, IEEE Transactions on Image Processing 15 (2006) 1803–1815.

Please cite this article in press as: M. Gomez-Barrero et al., A novel hand reconstruction approach and its application to vulnerability assessment, Inform. Sci. (2013), http://dx.doi.org/10.1016/j.ins.2013.06.015

[75] D. Zhang, Automated Biometrics – Technologies and Systems, Kluwer Academic Publishers, 2000.
[76] D. Zhang, V. Kanhangad, Encyclopedia on cryptography and security, in: Encyclopedia on Cryptography and Security, second ed., Springer, 2011, pp. 529–531.
[77] L. Zhang, D. Zhang, Characterization of palmprints by wavelet signatures via directional context modeling, IEEE Transactions on Systems, Man and Cybernetics – Part B 34 (2004) 1335–1347.
[78] Y. Zhang, Q. Li, J. You, P. Bhattacharya, Palm vein extraction and matching for personal authentication, in: Palm Vein Extraction and Matching for Personal Authentication, Springer, Berlin/Heidelberg, 2007, pp. 154–164.
[79] R.L. Zunkel, Hand geometry based verification, in: A.K. Jain, R. Bolle, S. Pankanti (Eds.), Biometrics, Springer, US, 2002, pp. 87–101.
[80] J. Zuo, N.A. Schmid, X. Chen, On generation and analysis of synthetic iris images, IEEE Transactions on Information Forensics and Security 2 (2007) 77–90.

Please cite this article in press as: M. Gomez-Barrero et al., A novel hand reconstruction approach and its application to vulnerability assessment, Inform. Sci. (2013), http://dx.doi.org/10.1016/j.ins.2013.06.015