SECURE FINGERPRINT VERIFICATION BASED ON IMAGE PROCESSING SEGMENTATION USING COMPUTATIONAL GEOMETRY ALGORITHMS

M .Poulos
marios.p@usa.net

E.Magkos
emagos@unipi.gr

Department of Informatics
University of Piraeus
80 Karaoli & Dimitriou str.,
Piraeus 18534, Greece

V. Chrissikopoulos
vchris@ionio.gr

Department of Archives and
Library Sciences, University
of Ionian, Palea Anaktora,
Corfu 49100, Greece

N. Alexandris
alexandr@unipi.gr

Department of Informatics
University of Piraeus
80 Karaoli & Dimitriou str.,
Piraeus 18534, Greece

ABSTRACT

In this paper, fingerprint segmentation for secure Internet verification purposes is investigated. The novel application of computational geometry algorithms in the fingerprint segmentation stage showed that the extracted feature (characteristic polygon) may be used as a secure and accurate method for fingerprint-based verification over the Internet. On the other hand the proposed method promisingly allows very small false acceptance and false rejection rates, as it is based on specific segmentation.

KEY WORDS

Computational Geometry, Security, Fingerprint, Verification, Image Segmentation

1. INTRODUCTION

Biometry, as the science of studying mathematical or statistical properties in physiological and behavioural human characteristics, is widely used in forensic and non-forensic applications in security field such as remote computer access, access control to physical sites, transaction authorization etc. In this paper the problem of fingerprint verification via the Internet is investigated. Specifically, the method that is used for the above purpose is based on a traditional finger scanning technique, involving the analysis of small unique marks of the finger image known as minutiae. Minutiae points are the ridge endings or bifurcations branches of the finger image. The relative position of these minutiae is used for comparison, and according to empirical studies, two individuals will not have eight or more common minutiae[1,2]. A typical live-scan fingerprint will contain 30-40 minutiae. Other systems analyse tiny sweat pores on the finger that, in the same way as minutiae, are uniquely positioned. Finger scanning is not immune to environmental disturbance. As the image is captured when the finger is touching the scanner device it is possible that dirt, condition of the skin, pressure and alignment or rotation of the finger all affect the quality of the fingerprint. Furthermore, such methods may be subject to attacks by hackers when biometric features are transferred via Internet [3].

For this reasons we developed a method, which addresses the problem of the rotation and alignment of the finger position. The proposed method is based on computational geometry algorithms. The advantages of this method are based on a novel processing method using specific extracted features, which may be characterized as unique to each person. These features depend exclusively on the pixels brightness degree for the fingerprint image, in contrast to traditional methods where features are extracted using techniques such as edge, minutiae points and ridges detection.

What makes biometrics useful for many applications is that they can be stored in a database. From a security point of view, fingerprints and biological data in general constitute sensitive information that has to be protected. Towards this direction, our method isolates a very small fraction of the user's biological data, and only this fraction is stored for future reference. This can also improve the overall efficiency and bandwidth effectiveness of the system.

2. METHOD

In brief, the proposed method is described in the following steps:

1. ***Pre-processing stage***. The input image is made suitable for further processing by image enhancement techniques using Matlab [4].
2. ***Processing stage.*** The data, which comes from step 1, is submitted to specific segmentation (data sets) using computational geometry algorithms implemented via

Matlab. Thus, onion layers (convex polygons) are created from these data sets, see figure 1.

3. ***Meta-processing stage*** (during registration only). The smallest layer (convex polygon) of the constructed onion layers is isolated from the fingerprint in vector form, see figure 2. For the rest of this paper, this will be referred to as the *referenced polygon*. This is supposed to be stored in a reference database, for subsequent verification.

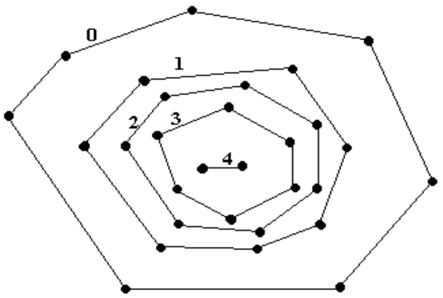

Figure 1: Onion Layers of a set of points (coordinate vector).

4. ***Verification stage.*** This stage consists of the following steps:

a) An unknown fingerprint is submitted to the proposed processing method (Steps 1 and 2), and a new set of onion layers is constructed.

b) The referenced polygon that has been extracted during registration stage is intersected with the onion layers and the system decides whether the tested vector identifies the onion layers correctly or not.

2.1 Pre-processing stage

In this stage a fingerprint image, which is available from any of the known image formats (*tif, bmp, jpg*, etc), is transformed into a matrix (a two-dimensional array) of pixels [6]. Consider, for example, the matrix of pixel values of the aforementioned array. Then the brightness of each point is proportional to the value of its pixel. This gives the synthesized image of a bright square on a dark background.This value is often derived from the output of an *A/D* converter. The matrix of pixels, i.e. the fingerprint image, is usually square and an image will be described as *N x N m-bit* pixels [6], where N is the number of points along the axes and m controls the number of brightness values. Using m bits gives a range of 2^m values, ranging from 0 to $2^m - 1$. Thus, the digital image may be denoted as the following compact matrix form:

$$f(x,y) = \begin{bmatrix} f(0,0) & f(0,1) & \dots & f(0,N-1) \\ f(1,0) & f(1,1) & \dots & f(1,N-1) \\ \vdots & \vdots & \vdots & \vdots \\ f(N-1,0) & f(N-1,1) & \dots & f(N-1,N-1) \end{bmatrix}$$

The coordinate vector of the above matrix is:

$$\mathbf{S} = [f(x,y)] \tag{2}$$

Thus, a vector $\mathbf{S}$ of $1 \times N^2$ dimension is constructed, which is then used in the next stage [7].

2.2 Processing stage

Proposition:

We considered that the *set of brightness values* for each fingerprint image contains a *convex subset*, which has a *specific position* in relation to the original set. This position may be determined by using a combination of computational geometry algorithms, which is known as *Onion Peeling Algorithms* [8].

Implementation:

We consider the *set of brightness values* of a fingerprint image to be the vector $\mathbf{S}$ (eq.2). The algorithm starts with a finite set of points $\mathbf{S} = \mathbf{S_0}$ in the plane, and the following iterative process is considered. Let $\mathbf{S}_1$ be the set $S_0 - \partial H \quad (S_0): S$ minus all the points on the boundary of the hull of $\mathbf{S}$. Similarly, define $S_{i+1} = S_i - \partial H \quad (S_i)$. The process continues until the set is ≥ 3 (see figure 1). The hulls $H_i = \partial H \quad (S_i)$ are called the layers of the set, and the process of peeling away the layers is called onion peeling for obvious reasons (see figure 1). Any point on H_i is said to have onion depth, or just depth, i. Thus, the points on the hull of the original set have depth 0 (see figure 1).

2.3 Meta-processing

In our case we consider that the smallest convex layer that has depth 3 (see figure 1) carries specific information, because this position gives a geometrical interpretation of the average of the fingerprint brightness [9]. In other words, the smallest convex polygon (layer) depicts a *particular geometrical area* in which this average ranges.

Definition: This feature may be characterized as unique to each fingerprint because the two (2) following conditions are ensured:

1. The selected area layer is non-intersected with another layer.
2. The particular depth of the smallest layer is variable in each case.

Thus, from the proposed fingerprint processing method two (2) variables are extracted: the area of the smallest onion layer $\mathbf{S_{xy}}$ and the depth of this layer.

Taking into account the specific features of the aforementioned variables it is easy to ascertain that these may be used for accurate fingerprint verification**.**

2.3 Verification stage

In this stage we tested the subset $\mathbf{S_{xy}}$ against a new subset set $\mathbf{N_{xy}}$, which came from the processing of another set $\mathbf{N}$. This testing takes place at the following 3 levels.

1. Subset $\mathbf{S_{xy}}$ is cross-correlated with subset $\mathbf{N_{xy}}$.
2. The depths of the iterative procedure, from which the subsets were extracted, are compared.
3. The intersection between subset $\mathbf{N_{xy}}$ convex layer and one of set $\mathbf{S}$ onion layers is checked.

Furthermore, it is considered that subset $\mathbf{N_{xy}}$ identifies set $\mathbf{S}$ as the parent onion layers when:

1. The cross-correlation number of subset $\mathbf{S_{xy}}$ and subset $\mathbf{N_{xy}}$ is *approximately 1*.
2. The intersection [10] between the convex layer of subset $\mathbf{N_{xy}}$ and one of the onion layers of set $\mathbf{S}$ is *0.*

Otherwise, subset $\mathbf{N_{xy}}$ does not identify set $\mathbf{S}$ as the parent onion layers.

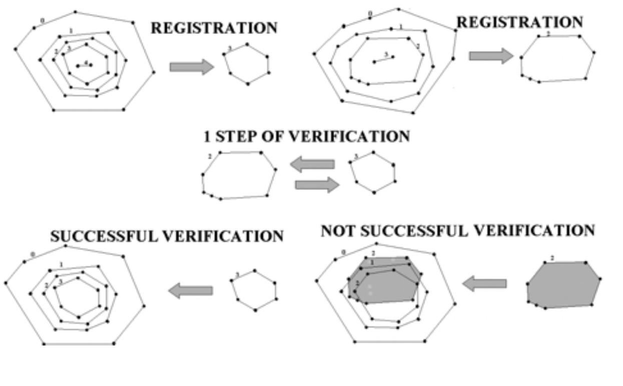

Figure 2**:** Theoretical presentation of the registration and verification stages of two (2) onions layers

3. EXPERIMENTAL PART

During registration we registered two coordinate vectors on a server, which belonged to two (2) individuals, A and B respectively. For this reason we used the method described in Section 2. In the following attack scenario, we will assume that during verification B submits his fingerprint and tries to identify himself as A.

3. 1. Pre-processing stage

In our experiment, each of the recorded fingerprints in TIFF format is represented by a complete 255×255 image matrix (equation 1), which came from a converting quantization sampling process implemented via the *imread.m* Matlab function.

1. Each pixel of the used fingerprint consists of 8 bits, therefore *m=8* and the gray levels of brightness range between *0* and *255*.
2. The dimension of the created compact matrix $f(x, y)$ of equation 1 is 255×255 and the coordinate vector $\mathbf{S}$ is 1×65025 respectively**.**

3. 2. Processing stage

The coordinate vector, which was extracted in the pre-processing stage, is submitted to further processing. In particular, the onion layers of vector *S* are created according to the computational geometry algorithm (figure 3a), which was described in the Section 2.2. Thus, a variable number of layers (convex polygons) were extracted for each fingerprint case. For better comprehension, an example of the aforementioned method is presented in figure 2. In this case, the created onion consisted of *944 layers* (convex polygons), and the number of vertexes of the smallest internal layer was six (6). Furthermore, the average of vector value $\mathbf{S}$ in this example was *140,67*.

3.3. Meta-Processing stage

As can be seen in figure 3d the area that encloses the smallest internal layer contains the aforementioned average value. In other words, *the area of this layer may be characterized as a specific area in which the dominant brightness value of the fingerprint ranges.*

3.4. Verification stage

In this stage, it is assumed that the referenced polygon A, must lead to a rejection decision. Then we applied the aforementioned VERIFICATION conditions in order for the system to decide whether polygon B is correctly identified or not. For better comprehension this procedure is described in figure 4. The final decision of this system is that the tested fingerprint is not identified correctly for the following reasons:

1. The depth of the smallest referenced layer (polygon) was *944* in contrast to that of the tested vector that was *677* respectively.
2. The layer of the tested polygon intersected the other layers.

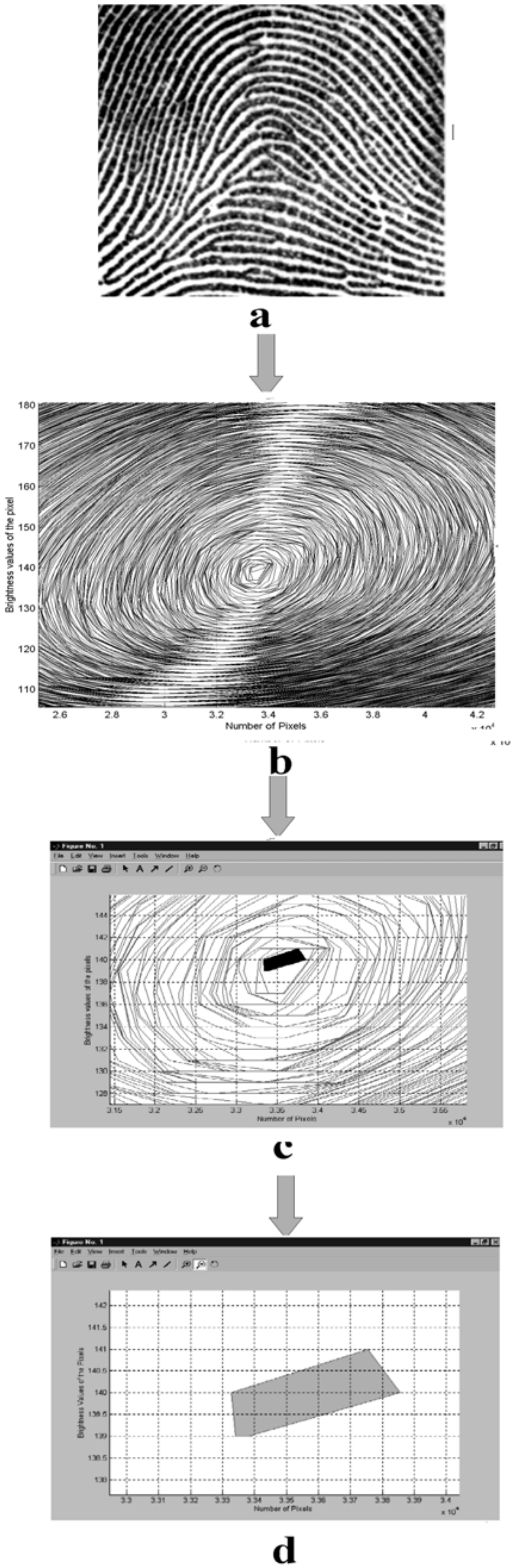

Figure 3: The analytical procedure of the feature extraction of a fingerprint in 4 frames. In the frame d the smaller onion layer is distinguished, which is used in the registration and the verification stages.

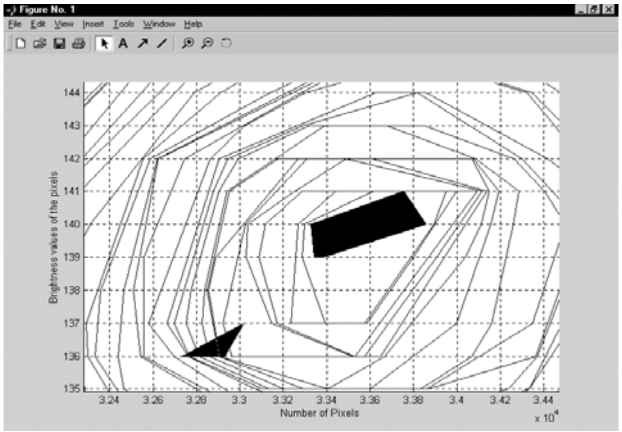

Figure 4: The verification procedure between two smaller layers which come from different individuals.

4. SECURE INTERNET VERIFICATION

Based on the feature extraction method and verification procedures proposed in Section 2, we describe, from a security point of view [10,12], a model for a fingerprint verification system that takes place over the Internet. There are two discrete stages for such a system: a *Registration Stage* and a *Verification Stage*. Moreover, the following components are employed:

Biometric Reader: it accepts a user's analog fingerprint and transforms it into digital information (e.g. TIFF format).
Processing Unit: takes as input the raw information provided by the reader, and extracts the onion layers from the data. These are sent to the Meta-processing Unit (during registration) or to the Comparison Unit (during verification).
Meta-Processing Unit: it isolates the smallest convex polygon from any set of onion layers it gets from the Processing Unit and submits the referenced polygon to the Reference Database.
Comparison Unit: it intersects and compares the onion layers provided by the Processing Unit with the referenced polygon provided by the Reference Database.
Reference Database: it stores the users' reference polygons, provided by the Meta-Processing Unit during registration, or provides the Comparison Unit, during verification, with a user's reference polygon**.**
All components must be tamper-resistant to avoid attacks by hackers who wish to undermine the verification mechanism. Furthermore, in the sequel we propose the use of some very basic cryptographic primitives as well as several precautions in respect of securing communication links between the units of the system.
All messages originated by all components of the system should be digitally signed [13] to avoid attacks such as man-in-the-middle attacks [11] that impersonate an entity to a component or vice versa. Such impersonation (or spoofing) attacks are usually met in false acceptance scenarios [12].

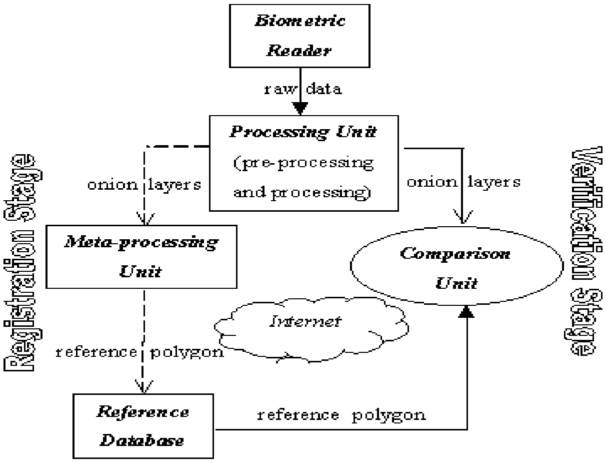

Figure 5. Communication Paths for a Biometric Verification System

Even the biometric reader should authenticate itself to the user, to deal with ATM spoofing-like attacks, where a fake reader is used to steal the user's biological data. Furthermore, the digital signing of data in conjunction with sufficient freshness information (timestamps, serial numbers - nonces) can prevent various replay attacks [11]. In such an attack for example, the attacker feeds the component with digitally signed data that he eavesdropped during a previous genuine verification. Reasonably, encryption must also be used to protect the links between units from eavesdropping or data injection.

Data stored in the Reference Database should also be encrypted and protected against writing, to prevent a hacker from replacing a user's referenced polygon by his own in order to get false acceptance.

5. CONCLUSION

Taking into account the results of the experiment of Section 3 it is ascertained that the method proposed in Section 2, having also in mind the security considerations made in Section 4, can be used for accurate and secure fingerprint verification purposes, because the proposed feature extraction is based in a specific area in which the dominant brightness value of the fingerprint ranges. On the other hand the proposed method promisingly allows very small false acceptance and false rejection rates, as it is based on specific segmentation. It has to be noted that biometric applications will gain universal acceptance in digital technologies only when the number of false rejections / acceptances approach zero.

It has been pointed out that biometrics are not a security solution on their own [11,12]. For example, a well determined criminal could fake a fingerprint using silicon imprints made from wax molds. However there is an increasing trend to use biometrics in conjunction with other technologies for security (pass codes or in attended environments). The most promising application involves tamper-resistant smart-cards, where the overall security is increased by unlocking a secret cryptographic key only after a successful biometric verification.

6. ACKNOWLEDGEMENT

This research was supported by the Dept. of Informatics, University of Piraeus and the Dept. of Archives and Library Sciences, University of Ionian, Greece.

References

1. A. K. Jain, A. Ross, & S. Pankanti, Fingerprint matching using minutiae and texture features, *Proc. International Conference on Image Processing (ICIP)*, Thessalonica, GR, 2001, 282-285.
2. D. Maio & Maltoni, Direct gray-scale minutiae detection in fingerprints*, IEEE Transactions on PAMI, 19*(1), 1997, 27-40.
3. L. O'Gorman, *Fingerprint verification, in Biometrics* (Jain, A, K. Bolle, R. & Pantanti, S.: Kluwer Academic Publishers, 1999).
4. T. Poon & P. Banerjee, *Contemporary Optical Image Processing With Matlab,* (Hardcover: Elsevier Science Ltd, 2001).
5. R. Bracewell, *Two-Dimensional Imaging*, (Horton M., NJ: Prentice – Hall, Upper Sandle River, 1995).
6. R. Gonzales, R. Woods, *Digital Image Processing*, (Horton M., NJ: Prentice – Hall, Upper Sandle River , 2002).
7. M. Spiegel, *Theory and Problems of Vector Analysis*, (Schaum S., London: McGraw-Hill, 1974).
8. J. O'Rourke, *Computational Geometry in C*, (Spencer T., NY: Cambridge University Press, 1993).
9. M. Nixon, A. Aguado, *Feature Extraction and Image Processing*, (Butterworth Heineman, GB: Newnes-Oxford, 2002).
10. J. O'Rourke, J. Chien, C. Olson, & T. Naddor, A new linear algorithm for intersecting convex polygons*, Comput. Graph. Image Proces. 19* (4), 1982, 384-391.
11. C. Calabrese, The Trouble with Biometrics, *Login*, 24(4), 1999, 56-61.
12. G. Hachez, F. Koeune, J.J. Quisquater, Biometrics, Access Control, Smart Cards: a Not So Simple Combination", *Proc. of the 4th Working Conference on Smart Card Research and Advanced Applications (CARDIS 2000),* Bristol, GB, 2000, 273-288.
13. B. Schneier, *Applied Cryptography, Protocols, Algorithms and Source Code in C*, (2nd Edition, 1996).