International Journal of Scientific Research Engineering & Technology (IJSRET)
Volume 1 Issue 5 pp 091-095 August 2012 www.ijsret.org ISSN 2278 - 0882

SECURE INTERNET VERIFICATION BASED ON IMAGE PROCESSING SEGMENTATION

[1]Shiv Kumar Tripathi, [2]Anshul Maheshwari
Computer Science & Engineering
Babu Banarasi Das Institute of Engineering Technology & Research Centre, Bulandshahr
shiv_tripathi0102@yahoo.com
er.anshul786@gmail.com

ABSTRACT
From security point of view, fingerprints and biological data in general constitute sensitive information that has to be protected. Towards this direction, the method discussed in this paper 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. 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.

Biometrics technology allows determination and verification of ones identity through physical characteristics. To put it simply, it turns the human body in to his or her password. In this paper two algorithms have been proposed by taking biometric techniques to authenticate an ATM account holder, enabling a secure ATM by image processing.

1. INTRODUCTION
Biometry, as the science of studying mathematical or statistical properties in physiological and behavioral human characteristics, is widely used in forensic and no 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. A typical live-scan fingerprint will contain 30-40 minutiae. Other systems analyze 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.

In this paper a method is developed, 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. Specifically, these features express a specific geometric area (convex layer) in which the dominant brightness value of the fingerprint ranges. What makes biometrics useful for many applications is that they can be stored in a database.

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.

2. ***Processing stag:.*** 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.

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

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

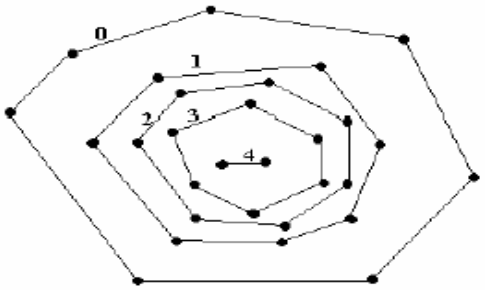

Figure 1: Onion Layers of a set of points (coordinate vector).

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. 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, 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:

1.

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

The coordinate vector of the above matrix is:

$$S = f(x,y) \quad (2)$$

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

2.2 Processing stage

*Proposition***:**

It is 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.

*Implementation***:**

Consider the *set of brightness values* of a fingerprint image to be the vector **S** (eq.2). The algorithm starts with a finite set of points $S = S_0$ in the plane, and the following iterative process is considered. Let S_1 be the set $S_0 - \partial H(S_0) : S$ minus all the points on the boundary of the hull of S. Similarly, define $S_{i+1} = S_i - \partial H(S_i)$.

The process continues until the set is $\geq$ 3 (see figure 1). The hulls $H_i = \partial H(S_i)$ 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 this case it is considered 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. In other words, the smallest convex polygon (layer) depicts a *particular geometrical area* in which this average ranges. This feature may be characterized as unique to each fingerprint because the two (2) following conditions are ensured:

i. The selected area layer is non-intersected with another layer.
ii. 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 S_{xy} and the depth of this layer, which is a subset of the original fingerprint set **S** values. Taking into account the specific features of the aforementioned variables it is easy to ascertain that these may be used for accurate fingerprint verification**.**

2.4 Verification stage

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

i. Subset S_{xy} is cross-correlated with subset N_{xy}.
ii. The depths of the iterative procedure, from which the subsets were extracted, are compared.

The intersection between subset N_{xy} convex layer and one of set **S** onion layers is controlled.

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

i. The cross-correlation number of subset S_{xy} and subset N_{xy} is *approximately 1*
ii. The intersection between the convex layer of subset N_{xy} and one of the onion layers of set **S** is *0.*

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

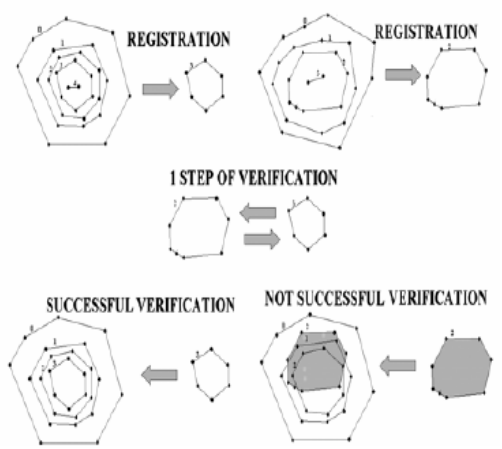

Figure 2**:** Theoretical presentation of the registration and verification stages of two (2) onion layers.

3. SECURE INTERNET VERIFICATION

Based on the feature extraction method and verification procedures proposed in Section 2, it is described from a security point of view, a model for a fingerprint verification system that takes place over the Internet (see figure 3). 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 to avoid attacks such as man-in-the-middle attacks that impersonate an entity to a component or vice versa. Such impersonation (or spoofing) attacks are usually met in false acceptance scenarios.

International Journal of Scientific Research Engineering & Technology (IJSRET)
Volume 1 Issue 5 pp 091-095 August 2012 www.ijsret.org ISSN 2278 - 0882

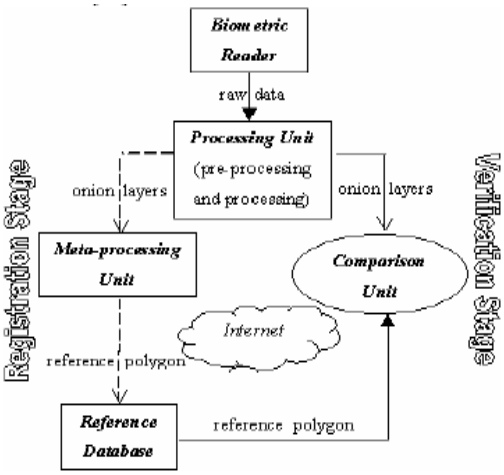

Figure3. Communication Paths for a Biometric Verification System

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) can prevent various replay attacks. 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.

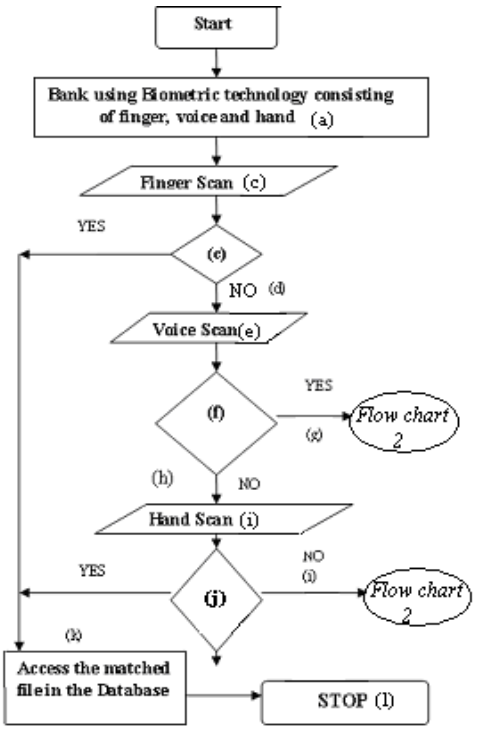

Figure 4: Flowchart for Algorithm 1

4. WORK ON IMAGE PROCESSING

Every system has its limitations. Therefore, identification based on multiple biometrics is an emerging trend as Multimodel biometrics can provide a more balanced solution to the security Multimodel systems involve the use of more than one biometric system. For the contribution to the above subject an algorithm is developed on banking security. For this consider a bank using biometric technology for its security purpose. The security is assured by using finger scan, voice scan, hand geometry scan and by requesting the password given by the bank for a particular user when necessary. The following are the flowcharts and the algorithms.

4. Algorithm:

4.1 Algorithm 1:

a) STEP 1: A person enters the bank that uses biometric technology (finger scan, voice scan & hand scan) for greater degree of security (Figure 4).

b) STEP 2: The person is requested to give his or her fingerprint (as input) on the finger scan pad.

c) STEP 3: The fingerprint from above step is compared with all the fingerprints in the database.

If fingerprint is matched with any one of the fingerprints available in the database (condition)

THEN …

GOTO STEP 8

d) **ELSE** (i.e., if finger print does not find a match)

GOTO STEP 4

e) STEP 4: The person is requested to speak few words, which is converted into digitalized code by the voice scanner.

f) STEP 5: The code in the above step is compared with all the voice codes in the database

g) **IF** the code is matched (condition)

THEN,

GOTO ALGORITHM 2

h) **ELSE** (i.e., if the code does not find a match)

GOTO STEP 6

i) STEP 6: The person is requested to place his hand above the hand scanner so that the structure of the hand is recorded.

j) STEP 7: The data in the above step is compared with all the data available in the database.

IF the data is matched

THEN,..... GOTO STEP 8

ELSE (i.e., the data does not find a match)…….GOTO Algorithm 2.

k) STEP 8: access the matched file in the database

l) STEP 9: Exit.

4.2 Algorithm 2:

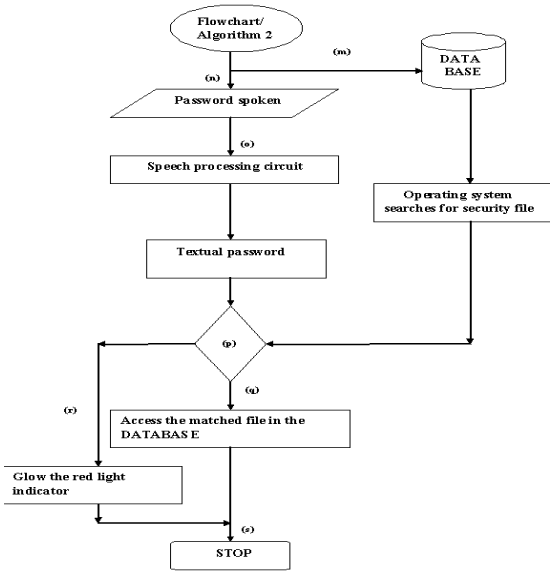

Figure 5: Flowchart for Algorithm 2

m) STEP 1: A request is sent to the database querying it to send the password file from the OS security files (Figure 5).

The passwords are received in an encrypted form (DES-Data Encryption Standards).

n) STEP 2: The person is requested to speak his password.

o) STEP 3: The vocal password spoken in the above step is converted into textual password by the speech processing circuit

p) STEP 4: This password is compared with the password file from STEP 1;

q) IF match is found

THEN, …….. Access the database.

r) ELSE**,** ……..Glow the danger light (indicating theft)

s) STEP 5: Exit.

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 features described in 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. 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.

Finally, more extensive experimentation is necessary, in order to obtain statistically significant results and thus verify the conjecture of this proposed method.

6. 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 Acadenic 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] M. Nixon, A. Aguado, *Feature Extraction and Image Processing*, (Butterworth Heineman, GB: Newnes-Oxford, 2002).

[7] R. Gonzales, R. Woods, *Digital Image Processing*,

[8] Anil K. Jain (Editor). Ruud Bolle, Sharath Pankanti. "Biometrics, Personal identification in Networked Society:" Vol.479,