Development of an Algorithm for Biometric System Using Finger Vein with Liveness Detection

Tashida Yeasmin, Mehnaz Tarannum, Tamanna Shaown, Akila Khatun

Abstract— The biometric system we are offering is an advanced system with less searching. The system would be very efficient as it can also detect the presence of authorized person. In our system we used finger vein as feature instead of finger printing. In this context the finger vein images are obtained from near infrared based or thermal infrared based optical imaging. As previous experiments showed us that finger vein pattern of different individuals are unique, so our objective was to give this technique more efficiency and less searching cost. For that we tried a new technique in recognizing individual's finger vein pattern. From Ajay Kumar and Yingbu Zhou's Human Identification Using Finger Images- we find the finger vein pattern of individual. From that image we will produce a new algorithm for determining authorized individual or fake. In our searching technique we used optimal technique instead of block by block searching.

Index Terms— Biometric, Liveness Detection, Authorized, Fingerprint, Finger Vein Pattern, Efficiency and Optimal Technique.

1 Introduction

Biometrics is becoming an exciting topic now in regards to computer and network security, however the ideas of biometrics have been developed for many years. Possibly the first known example of biometrics in practice was a form of finger printing which being used in China in the 14th century, which was reported by explorer Joao de Barros. He wrote that the Chinese were pressing children's palm and footprints on paper with ink to differentiate the children from one another. This is the earliest known case of biometrics in use and is still being used today also [1].

Biometrics is an automated method of identifying a person based on a physiological or behavioral characteristic. Biometric recognition technology depends on the physical characteristics of an individual, such as fingerprints, pattern of the iris of the eye, voiceprint, and facial pattern, in identifying an individual. Examples of physiological biometric features include height, weight, the shape of the hand, body odor, the pattern of veins, retina or iris, the face and the patterns on the skin of thumbs or fingerprints. Examples of behavioral biometrics are voice patterns, keystroke sequences, signature and gait (the body movement while walking) [2].

Several biometric technologies are successful in determining spoof attacks. In case of aliveness detection some sensor level spoof attacks have been suggested such as- finger response to electrical impulse, finger temperature and electrocardiographic signals, percentage of oxygen saturated hemoglobin in the blood, time varying perspiration patterns from fingertips etc. Regardless of the variety of these suggestions only a few have been found appropriate for biometric systems [3].

In spite of the variety of these suggestions, only a few have been found appropriate for online fingerprint identification, and these techniques need close contact of respective sensors with the fingers, which makes them unsuitable for unconstrained finger images. In this context, the finger-vein images obtained from the near-infrared-based or thermal-infrared-based optical imaging offer promising alternatives. The application of some other techniques such as ultrasonic scanning using a high-frequency transducer, computerized tomography and magnetic resonance imaging could also deliver valuable finger image data for the personal identification system [4].

To prohibit identity theft, biometric data is usually encrypted when it's collected. Here is the description of how biometric verification works on the back end: At first to convert the biometric input, we need to use a software application to determine specific points of data as match points. After getting the match points in the database, those data are processed by using an algorithm that converts the given information into a numeric value. The database value is then compared with the biometric input the end user has submitted into the scanner and authentication is either approved or denied.

Some biometric systems allow more than one attempt to detect or verify an individual.

Some biometric features are constant over time while others may change. All biometric features are considered 'unique' but some are less 'distinct' than others and less convenient for automated identification purposes. The distinguishability of any biometric feature depends also on the effectiveness of the sampling technique which is used to measure it and the efficiency of the matching process used to declare a 'match' between two samples. Biometric identification is a method that uses biometric attributes to identify or verify human beings. Because a person's biometric features are a part of his or her

- *Tashida Yeasmin is currently pursuing masters degree program in computer science & engineering (CSE) in Military Institute of Science & Technology (MIST), Bangladesh. E-mail: tashida.tithi58@gmail.com*
- *Mehnaz Tarannum is currently pursuing masters degree program in electrical & electronic engineering(EEE) in Dhaka University, Bangladesh. E-mail:tarannumtushty@gmail.com*
- *Tamanna Shaown is currently pursuing masters degree program in electrical & electronic engineering in Brac University, Bangladesh. E-mail:tamannashaown@gmail.com*
- *Akila Khatun is currently pursuing masters degree program in electrical & electronic engineering (EEE) in Dhaka University, Bangladesh. E-mail:akila.shahina37@gmail.com*

body, they will always be with that person where ever he/she goes and available to prove his or her identity. Biometric technologies are used in three ways: (i) to verify that people are who they claim to be, (ii) to discover the identity of unknown people, and (iii) to screen people against a watch-list.

2 Related Work

Biometric technologies are becoming the infrastructure of an extensive array of highly secure identification and personal verification solutions. As the security level and transaction fraud increases, the need for highly secure personal verification and identification technologies is becoming apparent.

In order to identify a person by a security system it has to compare their characteristics with a database, this will draw a biometric point and calculate the distances between them in order to recognize the biometric features person to identify. For the science Biometrics is the science of measuring physical properties of living beings and for the engineer is the automated recognition of individuals based on their behavioral and physiological characteristics.

By measuring a person's suitable behavioral and physiological characteristics in a recognition inquiry and comparing these data with the biometric reference data, which had been saved during a learning procedure, the identity of a specific person is determined [5].

The blood vessels, which are part of the circulatory system, transport blood throughout the body to sustain the metabolism, using a network of arteries, capillaries and veins[6]. The use of such vascular structures in the palm, palm–dorsal, and fingers has been analyzed in the biometrics literature with high success [8]. E.C. Lee, K. R. Park, D.Mulyono & H.S. Jinns said that-the finger-vein patterns are believed to be quite unique, even in the case of identical twins and even between the different fingers of an individual person[9]. There are two key factors that are cited for the preference of finger-vein biometrics [10]. First, the finger vein patterns are hidden structures; it is extremely difficult to steal the finger-vein patterns of an individual person without their knowledge, therefore offering a high degree of privacy. Second, the use of finger-vein in biometrics offers strong antispoofing capabilities as it can also ensure liveness in the presented fingers during the imaging.

Personal identification and verification using finger-vein patterns has invited lot of research interest, and currently, several business products have been available for civilian applications. The biometric identification from finger-vein patterns uses normalized cross correlation of finger-vein images which is detailed in . Miura *et al.* have further enhanced the performance for the vein identification using a repeated line tracking algorithm[11]. The robustness in the extraction of finger-vein patterns can be significantly improved with the use of local maximum curvature across the vein images and is detailed in with promising results [12]. Wu and Ye have successfully investigated finger-vein identification with the use of Radon transform based statistical features and a probabilistic neural network classifier [13]. Although, the database employed in this paper is too small to create a reliable conclusion on the stability of such features in the noisy vein patterns [14]. The curvelet-based extraction of finger-vein patterns and its classification using a back-propagation neural network are described in "Multiscale feature extraction of fingervein patterns based on curvelets and local interconnection structure neural network"[15]. The performance from this approach is shown to be very high, but the key details of their implementation are missing in this paper. Lee and Park have recently investigated the restoration of finger-vein images using a point spread function [10]. The authors suggest remarkable improvement in the performance for the vein identification using such restored finger images. The finger-vein imaging setup explained in "Restoration method of skin scattering blurred vein image for finger vein recognition," and "A study of finger vein biometric for personal identification," is rather constrained the motion of fingers during the imaging[8]. A survey of prior work on finger-vein identification suggests that, although analysts have demonstrated highly promising results, this area lacks a systematic study, i.e., a comparative assessment of performance from previously proposed approaches, and most importantly, there is no publicly available finger-vein database that analysts can utilize for comparing the performance [17].

3 Methodology

3.1 Block Diagram and Finger Imaging

The block diagram of the suggested system is described in fig. 1. The fingers which is presented for the identification of subjects are concurrently exposed to webcam and infrared camera as illustrated from the device of our imaging device in

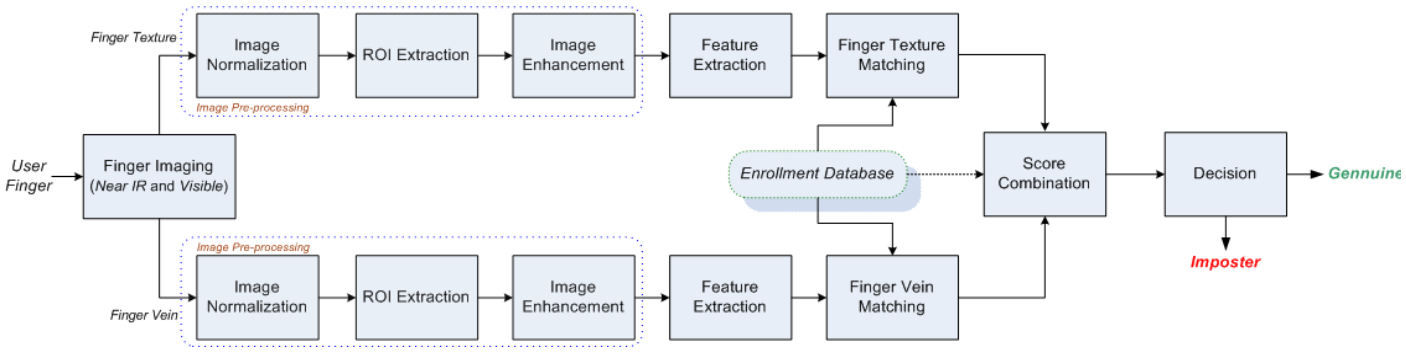

Fig. 1: Block diagram for personal identification using simultaneous finger vein and finger texture imaging.[7]

figure 2(a). The dorsal side of finger is exposed to the near infrared frontal surface illuminators, using light emitting diodes whose radiation peaks are at a wavelength of 850 nm, whereas the frontal surface entirely remains in the contactless place with both of the imaging cameras. Even though our imaging system is unconstrained, i.e., it does not use any finger docking frame, it may not be specified as completely touchless. This is only because the user often partially or fully touches the finger dorsal surface with the white diffusion surroundings which holds the infrared illuminators beneath. The finger vein and finger texture images are unanimously acquired using the switching device/hardware that can switch the infrared illumination at a fast pace.

Figure 2(b) shows a typical image samples obtained from our device from a left index finger [7]. The near infrared illumination incident on the finger dorsal surface which is absorbed by the braches of arteries and veins in the blood. However, the absorption coefficients of bio-tissue are remarkably different to that of blood for the infrared illumination or radiation. The higher scattering coefficient results in more path changes of inferred illumination from the blood than those resulting from the surrounding tissues. As a result, it is scattering from infrared illumination, rather than absorption, that results in darker appearance of finger vein patterns [7].

The collected finger vein and finger texture images are firstly subjected to pre-processing steps which automatically remove the region of interest (ROI) images while minimizing the translational and rotational variations. These steps are described in section 3 and 5 for the finger vein and finger texture images respectively. The enhanced and normalized ROI images are occupied to extract features and then generate matching scores like conventional biometrics system. The combined matching results are employed to authenticate the user.

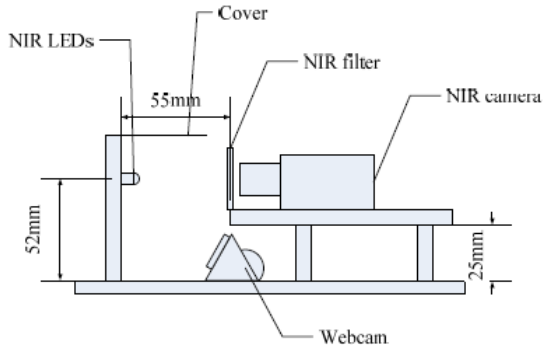

Fig. 2(a). Unconstrained finger identification using near infrared camera and webcam imaging;

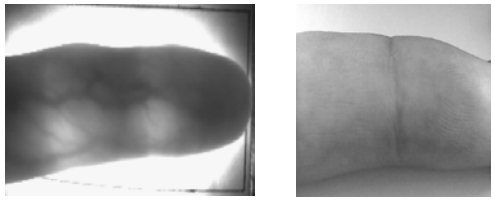

Fig.2(b). simultaneously acquired image samples from the imaging device. [7]

3.2 Finger Vein Image Pre-processing

The collected finger images are noisy with rotational and translational variations that resulting from unconstrained imaging. Hence the acquired images are firstly subjected to preprocessing steps (see figure 3) that include (1) segmentation of ROI, (2) translation and alignment and (3) image enhancement to extract stable/reliable vascular patterns.

Each of the obtained finger vein images is firstly subjected to binarization, using a fixed threshold value as 230, to coarsely place the finger shape in the images. Some portions of background still appear as connected to the bright finger regions, predominantly due to uneven illumination. The isolated and loosely connected areas in the binarized images are eliminated in two steps: firstly, the Sobel edge detector is applied to the whole image and the resulting edge map is subtracted from the binarized image. Subsequently, the isolated blobs in the final resulting images are removed from the area thresholding, i.e., eliminating number of attached white pixels being less than a threshold. The resulting binary mask is used to segment region of interest from the original finger vein image [17].

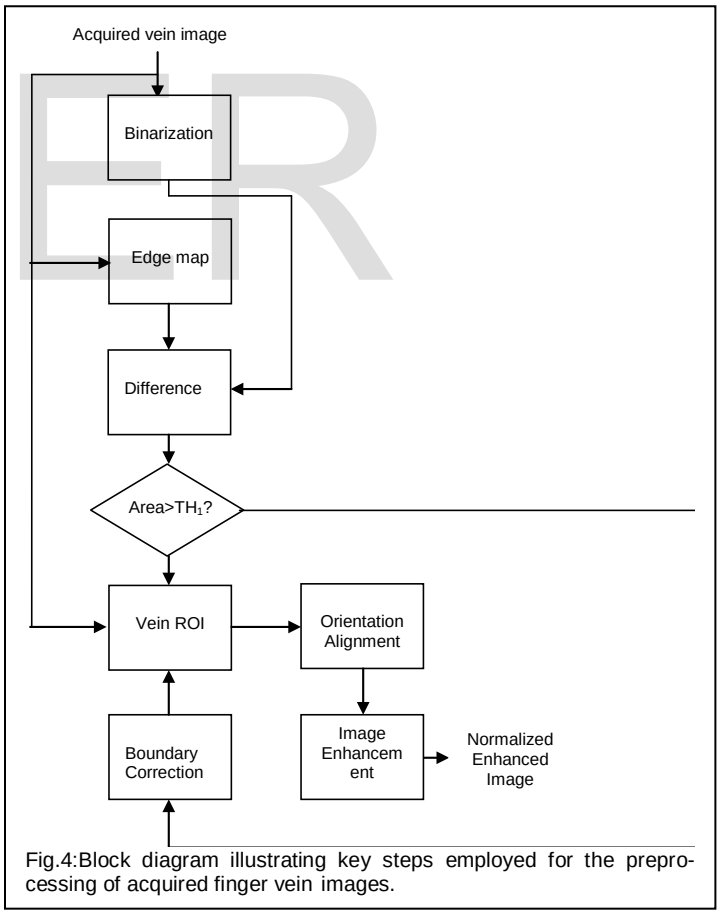

Fig.4:Block diagram illustrating key steps employed for the preprocessing of acquired finger vein images.

Figure 4 shows the step step process of finger vein extraction from a captured image of a finger. The picture in (f) shows the final picture of finger vein. From this picture machine will find the cross points of veins in a co-ordinate system. This vein crosses are different from man to man. So this will be an effec-

tive process for fulfilling our motto.

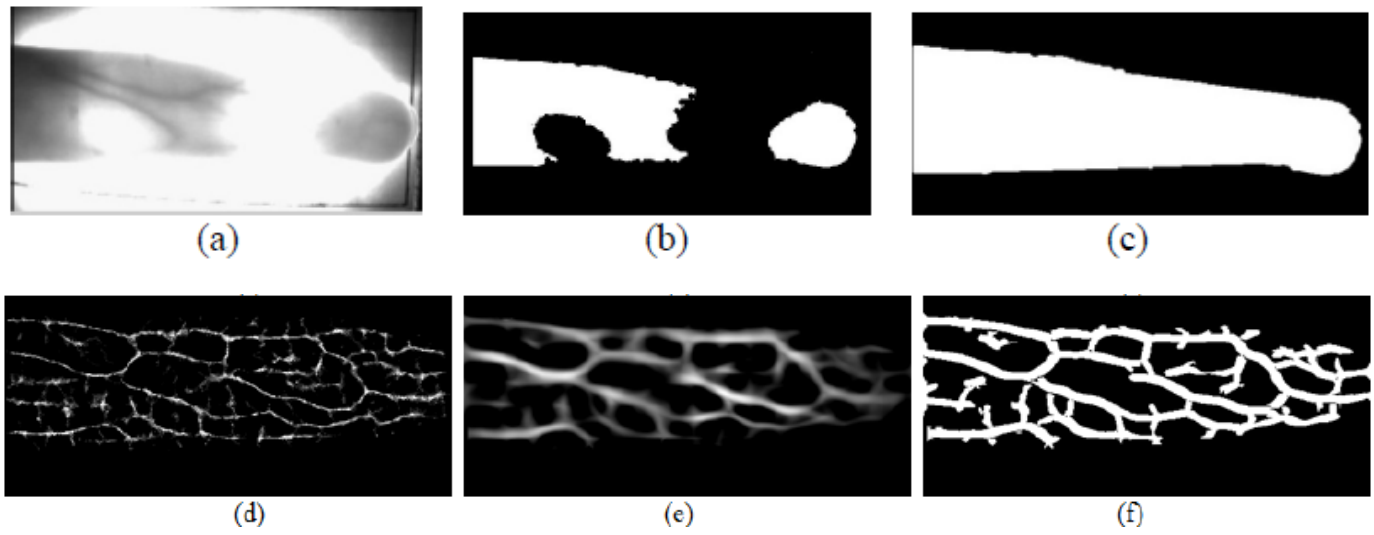

Fig. 4: (a) Acquired finger vein image. (b) ROI mask from (a). (c) ROI mask after refinement.
(d) Output from the maximum curvature. (e) Output from Gabor filters. (f) Output from morphological operations on (e). [7]

At the first step of our algorithm, the finger vein information of authorized person is saved. By Ajay Kumar and Yingbo Zhou's work we find the finger vein image [7]. The whole image will be a coordinate system. In that image, the vein image will be plot [16].

From the above picture we can define our searching technique, each point in the coordinate system will store the horizontal distance of the passing vein and the database will contain the authorized person's vein information. The Euclidean distance of a respective point is measured y this algorithm. From the above figure the two boundaries represent the internal part of a vein where internal part is recognized by bit 1 and external part which is the black part is recognized as bit 0.

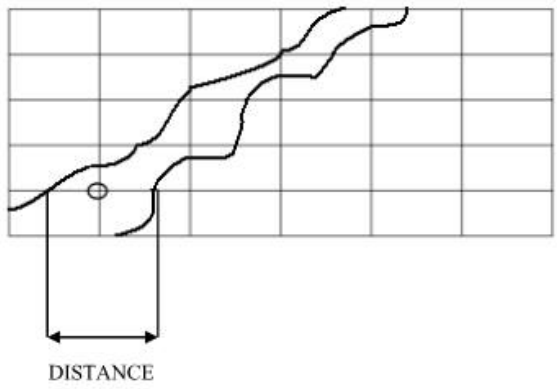

Figure 6: Euclidean distance (Internal distance) of a passing vein at a definite point.

Here the authorized person's Euclidean distance is calculated. At first the right boundary distance is determined. Then the left boundary distance is calculated. Then their subtraction value is kept in an array and the loop will continue until all

3.3.2 Producing boundary

As each point needs a distance of passing vein's boundary, an algorithm is required to measure the boundary. There are two boundary allocation algorithms- one is for determining right boundary and another one is for left boundary.

3.3.3 Sorting

As the Euclidean distances for each point are found they will be sorted from maximum to minimum value.

3.3.4 User check algorithm

In case of user check same procedure will be applied for finding user's Euclidean distance and then those distances will be sorted from maximum to minimum. Then there will be a checking among the sorted distances. Whenever there one mismatch occurs, the machine will go to its denial state.

3.3.5 Extra feature

Our feature adds an extra feature which includes a block state for 3 same fake or imposter inputs.

4 Liveness Detection

4.1 Preface

Liveness detection in a biometric system means the ability for the system to detect, during enrollment and identification/verification, whether the biometric sample which is represented is alive or not, Furthermore, if the system is designed to protect against attacks with artificial fingerprints, it must also check that the presented biometric sample belongs to the live human being who was originally registered in the system and not just any live human being. Many people believe that biometric systems can detect liveness in biometric samples [18]. Some manufacturers of biometric system also claim that they have liveness detection in their system, It has however been shown that fingerprint systems can be fooled with artifi-

cial fingerprints, the static facial images can be used to fool face recognition systems, and that static iris images can be utilized to fool iris recognition systems[19].

4.2 Liveness Detection in Biometric Systems

Liveness detection can be conducted either at the acquisition stage, or at the processing stage. For example, an optical fingerprint scanner would create an image of an eraser, but not extract any features; the liveness detection takes place at the processing stage [20]. A capacitive fingerprint sensor on the other hand, would not even create an image of the eraser; the liveness detection takes place at the acquisition stage. There are two approaches in determining if a finger is alive or not; liveness detection and non-liveness detection [13].

The data used to spoof a system often have a number of different non-liveness characteristics that could be used to inspect non-liveness. An example of a non-liveness detection process would be to detect air bubbles in gelatin artificial fingerprints. Most biometric systems today have a decision process which first checks liveness [21]:

if data = live then perform acquisition and extraction else if data = not live do not perform acquisition and extraction.

This means that an attacker has the simpler task of imitating a live finger that circumventing a non-liveness detection mechanism. In fact, any detection mechanism can and will be defeated according to "International Biometric Group. Liveness detection in biometric systems, 2003".

There are essentially three different ways to introduce liveness detection into a biometric system [23].

1. Using extra hardware to acquire life signs. 2. Using the information already captured by the system to detect life signs. 3. Using liveness information inherent to the biometric.

The first of these methods introduces a few other problems; (1) it is costly, (2) it is bulky, and (3) it could still be possible to present the artificial fingerprint to the fingerprint sensor and the real fingerprint of the intruder to the hardware that detects liveness [15]. Also, in some instances it is still feasible to fool the additional hardware with a wafer-thin artificial fingerprint. The second method does not have these drawbacks, except maybe that it could be possible to still fool with an artificial fingerprint. It is on the other hand a bit more complicated to extract the life signs using no additional hardware. The third method of using inherent liveness information to the biometric is not applicable to fingerprint recognition [24]. Other biometric systems including facial thermograms, gait, body odor, keystroke dynamics, etc. use this however. These technologies are not widely executed and still need to be validated as reliable biometric identifier [25]. The main problem of distinguishable between an artificial fingerprint and a real fingerprint is that the epidermis (outer skin) of the finger is in fact not alive either [25]. Many different techniques have been suggested to detect liveness, and some of them will be presented in the following sections. For each of these techniques, a method to fool the system with an artificial fingerprint will also be suggested.

5 Conclusion

In our paper, we worked on finger vein instead of finger prints which is unique for individuals. On the other hand, human finger is very much reachable for others, so it can hamper privacy. But in that sense, finger vein is not very much reachable so it can store privacy and using some useful sensors the system can identify the aliveness of individual.

So according to the previous works we tried to develop the searching algorithm which is really optimized than previous works. These algorithms can find a quick searching. As an extra feature if three same inputs from a fake are given, the system will go to a denial state. So it can be said that further work on this algorithm and implementation can bring high degree of security and optimization.

References

[1] http://biometrics.pbworks.com/w/page/14811351/authentication

[2] http://grandgroovedjs,wordpress.com/2010/01/08/first-touch-its-yours/.

[3]http://terrorism.about.com/od/issuestrends/tp/history-of-biometrics.htm.

[4] http://www.all-about-forensic-science.com/fingerprints-brush.html.

[5] D. Zhang A. Kumar. Personal recognition using hand-shape and texture. 2006.

[6] K. V. Prathyusha A. Kumar. Personal authentication using hand vein triangulation and knuckle shape. 2009.

[7] Y. Zhou A. Kumar. Human identification using knucklecodes. 2009.

[8] H. S. Jinn D. Mulyono. A study of finger vein biometric for personal identification.2008.

[9] M. R. Arneson D. Osten, H. M. Carin. Biometric personal authentication system. 1998.

[10] K. R. ParkE. C. Lee. Restoration method of skin scattering blurred vein image for finger vein recognition. 2009.

[11] J. Hashimoto. Finger vein authentication technology and its future. 2006

[12] S.-H. Ye J.-D.Wu. Driver identification using finger-vein patterns with radon transform and neural network. *Systems,Man and Cybernetics,*2009.

[13] T. Vo-Dinh J. Mobley. Biomedical photonics handbook. 2003.

[14] A. Suwandy E. Sung J.G.Wang, W.Y.Yau. Person recognition by palmprint and palm vein images based on 'laplacianpalm' representation. 2008.

[15] X. Han Z. Zhang, S. Ma, Multiscale feature extraction of fingervein pattens based on curvelets and local interconnection structure neural network. 2006.

[16] S. O.Koh J.W. Severinghaus. Effect of anemia on pulse oximeter accuracy at low saturation. 1990.

[17] Ajay Kumar and Yingbo Zhou. Human identification using finger images. 2008.

[18] S.Y. Cho L. Wang, G. Leedham. Minutiae feature analysis for infrared hand vein pattern biometrics. 2008.

[19] S. Umermura M. Kon, H.Ueki. Near-infrared finger vein patterns for personal identification. 2002

[20] T. Miyatake N. Miura, A. Nagasaka. Feature extraction of finger vein patterns based on repeated line tracking and its application to personal identification. 2004.

[21] T. Miyatake N. Miura, A. Nagasaka. Extraction of finger-vein patterns using maximum curvature points in image profiles. 2005.

[22] J.W. Severinghaus P. E. Philip, J. R. Feiner. Effects of skin pigmentation on pulse oximeter accuracy at low saturation. 2005.

[23] S. M. K. Rahman T.S. Mundra P. V. Reddy, A. Kumar. A new anti-

spoofing approach for biometric devices. 2008.
[24] L. A. Hornak S. A. C. Schuckers S. T. V. Parthasaradhi, R. Derakhshani. Time-series detection of perspiration as a liveness test in fingerprint devices. 2005.
[25] D. Zhang W. Jia, D.-S. Huang. Palmprint verification based on robust line orientation code. 2008.

APPENDIX

```
ProduceDistance(D[])
{
        L=0
        For I=-1 to n
            X[I]=I+1
            I++
        End for
        For J=-1 to n
            Y[J]=J+1
            J++
        End for
        For I=1 to n
            For J=1 to n
                Distance[I][J]=detrb(I,J)-detlb(I,J)
                D[L]=Distance[I][J]
                I++
                J++
                L++
            End for
        End for
}

For right boundary,
detrb(A,B)
{
        For A=A to A+1
            If(point[A][B]==bit 1)
                A=A+0.05
            Else M=A-0.03
        End for
        Return M
}

For left boundary
Detlb(A,B)
{
        For A=A to A-1
            If( point[A][B]==bit 1)
                A=A-0.05
            Else M=A+0.03
        End for
        Return M
}


SortDistance(S[])
{
        Sort distances
        For i=1 to n
            S[i]=ith D[ ]
        End for
}
Match()
{
        ProductDistance(p[ ])
        Check(P[ ])
        SortDistance(B[ ])
        For i=1 to n
            If (S[i]==B[i])
                Flag=1
            Else flag=0
                Break
        End for
        If (flag==1) matched
        Else imposter
}


Check(A[ ])
{
    cq[ ]=A[ ]
    If (wq[ ]==cq[ ])
            f++
    else
            wq[ ]=cq[ ]
    if (f==3) system blocked and f is initialized to 0 again
}
```