FINGERPRINTS IDENTIFICATION USING NEUROFUZZY SYSTEM

Emad S. Jabber **Maytham A. Shahed**

Department of Computer Science, College of Science, University of Basrah Basrah, Iraq

Abstract

This paper deals with NeuroFuzzy System (NFS), which is used for fingerprint identification to determine a person's identity. Each fingerprint is represented by 8 bits/pixel grayscale image acquired by a scanner device.

Many operations are performed on input image to present it on NFS, this operations are: image enhancement from noisy or distorted fingerprint image input and scaling the image to a suitable size presenting the maximum value for the pixel in grayscale image which represent the inputs for the NFS.

For the NFS, it is trained on a set of fingerprints and tested on another set of fingerprints to illustrate its efficiency in identifying new fingerprints. The results proved that the NFS is an effective and simple method, but there are many factors that affect the efficiency of NFS learning and it has been noticed that the changing one of this factors affects the NFS results. These affecting factors are: number of training samples for each person, type and number of membership functions, and the type of fingerprint image that used.

تعريف بصمات الإصابع باستخدام الشبكات العصبية المضببة

عماد شعلان جبر هيثم ابو الخيل شهيد
قسم علوم الحاسبات / كلية العلوم / جامعة البصرة

الخلاصة:

يتناول هذا البحث الشبكات العصبية المضببة و التي استخدمت لتعريف بصمة الأصبع لتحديد هوية الشخص. مثلت كل بصمة بشكل صورة ذات تدرج رمادي (كل نقطة فيها تمثل بثمان ثنائيات) وتم التقاط هذه الصورة باستخدام جهاز الماسح الضوئي.

لغرض عرض هذه الصورة على الشبكة العصبية المضببة تم أجراء مجموعة من العمليات عليها، وهذه العمليات هي: تحسين الصورة من الوضوح أو التشويه الذي قد يحدث على الصورة المدخلة و تقييس الصورة إلى حجم معين يمثل أقصى قيمة للنقطة في الصورة والذي بدوره يمثل عدد خلايا الإدخال للشبكة.

بالنسبة للشبكة فقد تم تعليمها على مجموعة من البصمات، ثم اختبرت باستخدام مجموعة أخرى لتوضيح كفاءتها في التعرف على البصمات الجديدة.

أثبتت نتائج الاختبارات ان الشبكة العصبية المضببة هي طريقة كفوءه وبسيطة لكن هنالك عدة عوامل تؤثر على كفاءة تعلمها، ولوحظ تغير النتائج عند تغير عامل واحد من هذه العوامل، وهذه العوامل هي: عدد نماذج التعليم لكل شخص ونوع وعدد دوال الانتماء ونوع الصورة المستخدمة للبصمة.

1. Introduction

A fingerprint is the pattern of ridges and furrows on the surface of the fingertip. Fingerprints have been used as a means to identify individuals uniquely for a very long time, having many various purposes such as criminal identification, high security access control, credit card usage verification and employee identification. The main reason for the popularity of fingerprints as a method of identification results forms the fact that each fingerprint of a person is unique as well as easy to access. The uniqueness of a fingerprint is exclusively determined by the local ridge characteristics and their relationships. Two most important ridge characteristics, called minutiae, are ridge ending and ridge bifurcation. Ridge ending is defined as a point where a ridge ends abruptly [1].

A part from minutiae identification and extraction high-level features can also characterize a given class of the fingerprint. The important high-level features are the core and the delta points.

Automatic fingerprint matching depends on the comparisons of either local ridge characteristics or the high-level characteristics to make a personal identification. A critical step in fingerprint matching in both cases is to reliably extract features form the input fingerprint images. The performance of fingerprint identification mechanism relies heavily on the quality of the input fingerprint images. However, in practice due to variations in impression conditions, ridge configurations, skin conditions, acquisition devices and non-cooperative attitude of the subjects, a significant percentage of acquired fingerprint images are of poor quality. The use of computers in the fingerprint matching process is highly desirable in many applications, such as building security systems, police work, ...etc. In the latter, computers can be used to simplify the task of searching large files of fingerprints [1].

2. Fingerprint Recognition Systems

The major issues in designing a fingerprint recognition system include: defining the system working mode *verification* or *identification* see figure(1), choose hardware and software computers and making them work together, dealing with exceptions and poor quality fingerprint images, and defining effective administration and optimization policy.

In fact, it is significantly more difficult to design an identification system than a verification system. For an identification

system, both speed and accuracy are critical [1].

Fingerprint identification is one of the more certain methods [2]. It has been applied since antique civilization of Orient, where Emperor's fingerprint was a usual sign for certifying state documents. The use of fingerprint was increasing up to resulting in an important technique for personal identification [1].

However, manual identification is too tedious, too much time is needed, and today is nearly impossible of being applied because of the great number of fingerprints involved in a comparison [1]. Because of this, in the 60th it became obvious the necessity of developing and applying an Automated Fingerprint Identification System (A.F.I.S.) [2, 3, 4, 5].

Automated Fingerprint Identification is one of the most important biometric (*it is the science of identifying or verifying the identity of a person based on physiological or behavioral characteristics*) technologies at present. It has extended the use of fingerprint identification not only to forensic applications but to other civil ones like access control, Internet transaction validation, and Automatic Teller Machine (A.T.M.), among others [2, 3, 5, 6].

In the last years, several techniques have been developed, like those based on iris patterns, fingerprint and voice recognition to verify someone's identity. Fingerprint recognition has been used for a long time and it has been imposed like a robust person-identification method for two main reasons. First, in spite of the fact that the fingerprints may suffer little alteration, e.g. scars or burnt, they remain inalterable for life-time from the point of view of identification, and second, for *fingerprints uniqueness property* – as mentioned by Lee and Gaensslen [3] – determined by the characteristics of the ridges and valleys and their relationships.

Automated Fingerprint Identification System involves several processes, being a critical one the proper minutiae detection. This process becomes more difficult because of the presence of image noise or filth that might generate undesired spikes and breaks, resulting in a great number of false minutiae detected. Some authors [7] argued that the application of a pruning process might resolve this problem of false minutiae. However, spurious minutiae still might remain and confused with true minutiae.

There are many problems associated with the use of computer aids in

identifying and matching fingerprint images. Some of these problem stem directly from the physical nature of marks (dirt, scars, bad inking, ...etc), usually causes loss of information or creation of false information. Other problems faced by digital matching techniques arise mostly from image digitization and sampling or the use of X-Y grid. Examples of these problems are the Displacement, Rotation, Stretching or Compression during fingerprinting.

Various fingerprint recognition techniques have been proposed in literature. Leung et al. [8] presented a neural network approach for fingerprint recognition.

Fingerprint verification algorithm has been presented by Jain et al. [2]. Ammar et al. [9] used an approach for fingerprint image alignment.

Recently, Khan et al. [10] have presented a fingerprint image enhancement method, using decimation-free Directional Filter Bank.

In this study, we introduce an approach using NeuroFuzzy system for fingerprint image identification, because it's simple and effective method.

3.NeuroFuzzy System (NFS)

Existing fuzzy reasoning techniques suffer from the lack of a definite method to determine membership functions and a learning capability which can be overcome by neural networks driven fuzzy reasoning. Neural networks are used to tune the membership functions of fuzzy systems that are employed for controlling equipment. Although fuzzy logic has the ability to convert expert knowledge directly into fuzzy rules, it usually takes a lot of time to design and adjust the linguistic labels (fuzzy sets) of the problem. In addition, the tuning of membership functions is a tricky procedure as it sometimes embodies a number of free parameters that must be assigned by an expert [11]. Neural network techniques can automate this design procedure improving the performance and reducing the computational time. Neural network approach is used to tune the membership functions parameters was proposed in 1989 [12]. The parameters of membership functions (centers and widths) are modified to reduce error between the output of fuzzy system and desired output [13].

The resultant combined system for the Fuzzy System and the Neural Network is called NeuroFuzzy System, which possess

the advantage of both, and overcomes some of the drawbacks of individual approaches, such as black-box of neural networks and the limited learning capability of fuzzy systems [11].

A general layout of NFS, which based on Mamdani fuzzy model combined with neural network learning algorithms, with multi-inputs and one output is shown in figure (2). The architecture of this network is analogous to that of artificial neural network with four-layers [11, 12]. In this system, the most widely used as error is Least Mean Square *E(t)* which characterizes the learning performance of the network at time *t* in terms of the sum of squared errors. It has the formulas [12]:

$$E(t)^p = \frac{1}{2}\left(Yd^p(t) - Y^p(t)\right)^2 \qquad (1)$$

$$E(t) = \sum_{p=1}^{P} E(t)^p \qquad (2)$$

Where:

E is the total error for the NFS.

E^p is the error in the pattern p.

Yd^p is the desired output in the pattern p.

Y^p is the actual output in the pattern p.

P is the patterns number.

The adaptation of membership functions parameters (centers *aij* and widths *bij* for the input membership functions, and centers *ci* for the output membership functions) could be calculated by the formulas[12] :

$$a_{ij}(t+1) = a_{ij}(t) + k_a\left[\left(Yd(t) - Y(t)\right) * \left(c_i(t) - Y(t)\right) * \frac{u_i}{\sum_{L=1}^{n} u_L} * \frac{\left(x_j - a_{ij}(t)\right)}{\left(b_{ij}(t)\right)^2}\right] \qquad (3)$$

$$b_{ij}(t+1) = b_{ij}(t) + k_b\left[\left(Yd(t) - Y(t)\right) * \left(c_i(t) - Y(t)\right) * \frac{u_i}{\sum_{L=1}^{n} u_L} * \frac{\left(x_j - a_{ij}(t)\right)^2}{\left(b_{ij}(t)\right)^3}\right] \qquad (4)$$

$$c_i(t+1) = c_i(t) + k_c\left[\left(Yd(t) - Y(t)\right) * \frac{u_i}{\sum_{L=1}^{n} u_L}\right] \qquad (5)$$

where:

$i = 1, \ldots, m$; {m is no. of input variables}

$j = 1, \ldots, n$; {n is no. of rules in NFS}

ka, *kb*, and *kc* are the learning rates.

4. The Proposed Approach

The purpose of the proposed approach is to design a fingerprint identification system to determine a person's identity. The sequence stages are depicted in figure (3), which are described in the next sections.

4.1. Image Acquisition

This stage has taken a picture for the person fingerprint and transmitted it to a Bitmap (BMP) image file as 8-bits grayscale image using a scanner device. Therefore, each pixel have 256 intensity values in the range (0 – 255) and it has the

advantage of giving high accuracy in the identification of fingerprint larger than when using the binary image which take only two values to represent each pixel 0 or 1 see figure (4a). The size of image that used in this work is (128 x 128) pixels.

4.2. Image Enhancement

The identification of fingerprint images mainly requires matching the features of the fingerprint in question with those stored in the database. Since fingerprint identification system may receive noisy and distorted fingerprint image inputs, an efficient and robust enhancement of fingerprint images is essential for reliable fingerprint identification see figure (4b).

In this work, the Directional Filter Bank (DFB) is used because it is an effective filter fingerprinting image [14].

4.3. Image Standardization

This stage is responsible for standardization of the enhancement BMP image by changing the size of image to a suitable size for a later identification. In the current work the size of image after standardization is (16 x 16) pixels, it is a reasonable size, because it represent the number of intensity values for grayscale image (256 level) which is represent the inputs for the NFS (in the next stage). This size provides several advantages such as, high speed, minimize the storage requirement, and also minimize the inputs of NFS see Figure (4c).

4.4. Recognition using NFS

In this paper the use of NFS for fingerprint identification to determine a person's identity will be applied, and NFS has given encouragement results in identification. The NFS that shown in figure (2) is used with input variables (m=256) and each input has (n=9) membership functions.

To training NFS, we used 100 patterns (20 persons, 5 samples for each person take). Five samples are taken because these samples didn't matching 100% for one to another from many problems such as, noisy, displacement, rotation, stretch or compression, ...,etc during image acquisition. Each person has a code number represent the ID person as an output for the NFS. The training process was stopped when the net error become less than or equal (0.0003).

4.5. Search Database Files

To identify the information about the persons, an information(such as: *code number, name, address , birthday,* ... etc) about all training persons are stored in database file.

In this stage, the Identity Error (IE) is calculated by the following equation:

$$IE = person's\ code - NFS\ output \quad (6)$$

The person is enrolled in the system database which gives IE value less than or equal (0.001), represent the result and we can get all his information. Otherwise the person is *unknown*.

5. Experimental Results

To test our system , a new fingerprint for each person is enrolled in the system database in addition to a fingerprint for the new persons that are not enrolled in the system database. For the sake of brevity we will only present the results for 15 persons (10 from them are defined in the system database and the others are undefined). Table (1) illustrates the results of these tests.

6. Conclusion

In this work a scanner device has been used as an image acquisition which is more beneficial in pattern recognition system, and an off-line fingerprint identification system has been designed include several stages, digitized the image in a suitable form for processing later.

Based on the presented results we conclude the following:

a. NFS is a good and efficient method for fingerprint image identification. Where the test phase is taken very small time.

b. The structure of NFS is a simple in comparison with other method for the fingerprint image identification. It is giving high accuracy and good generalization performance for the tested fingerprints, this make the NFS an effective tool for fingerprint identification.

c. The results of any testing fingerprint when using 5 samples for each person are better than these that are obtained when using one or three samples for each person, but required more storage. This problem can be processed by using an effective compression technique such as JPEG methods.

d. From experiments, we found that the suitable number of membership functions is 9 and the best type is a Gaussian membership function, this architectural finding a NFS with a good generalization performance.

e. In this work, the grayscale fingerprint image gives high accuracy as compared with other Black/White fingerprint image.

7. References

1. D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, "Handbook of Fingerprint Recognition", Springer Verlag, New York, 2003.
2. A. K. Jain and L. Hong, " On-Line Fingerprint Verification", Technical Report MSU-CPS-99-19, Department of Computer Science, Michigan State University, East Lansing, Michigan, 1999.
3. H. C. Lee and R. E. Gaensslen, editors, "Advances in Fingerprint Technology", New York: Elsevier, 1991.
4. Federal Bureau of Investigation (F.B.I.), (www.fbi.gov/hq/cjisd/iafis.com).
5. N. K. Ratha, A. Senior and R. M. Bolle, "Automated Biometrics", Lecture Notes in Computer Science, 2013:445-455, 2001.
6. Federal Bureau of Investigation. "The Science of Fingerprints: Classification and Uses", U. S. Government Printing Office. Washington D. C., 1984.
7. N. K. Ratha, S. Chen and A. K. Jain, "Adaptive Flow Orientation Based Feature Extraction in Fingerprint Images", Technical Report MSU-CPS-99-17, Department of Computer Science, Michigan State University, East Lansing, Michigan, 1999.
8. W.F. Leung, S. H. Leung, W. H. Lau and A. Luk, "Fingerprint Recognition Using Neural Network", In IEEE workshop Neural Network for Signal Processing, pages 226-235, 1991.
9. H. H. Ammar, S. Zeng, and Z. Miao, "Parallel processing and fingerprint image comparison", Int. J. modeling and simulation, vol. 18, no. 2, pp 85-99, 1998.
10. M. A. U. Khan, M. K. Khan, and M. A. Khan, "Fingerprint image enhancement using decimation-free directional filter bank", Information Technology Journal, vol. 7, no. 1, pp 16-20, 2005.
11. S . G. Tzafestas and K. D. Blekas, "Hybrid Soft Computing Systems: A Critical Survey with Engineering Applications", (www.isda2001.softcomputing.net), 2001.
12. J. Jantzen, "NeuroFuzzy Modelling", (www.iau.dtu.dk/~jj/pubs), 1998.
13. S. Mitaim and B. Kosko, "The Shape of Fuzzy Sets in Adaptive Function Approximation", IEEE Trans. On Fuzzy Systems, vol.9, no.4, (www.sipi.usc.edu/~kosko/IEEETFS2001), 2001.

14. S. K. Oh, J. J. Lee, C. H. Park and B. S. Kim, " New fingerprint image enhancement using directional filter bank, WSCG. 11, 2003.

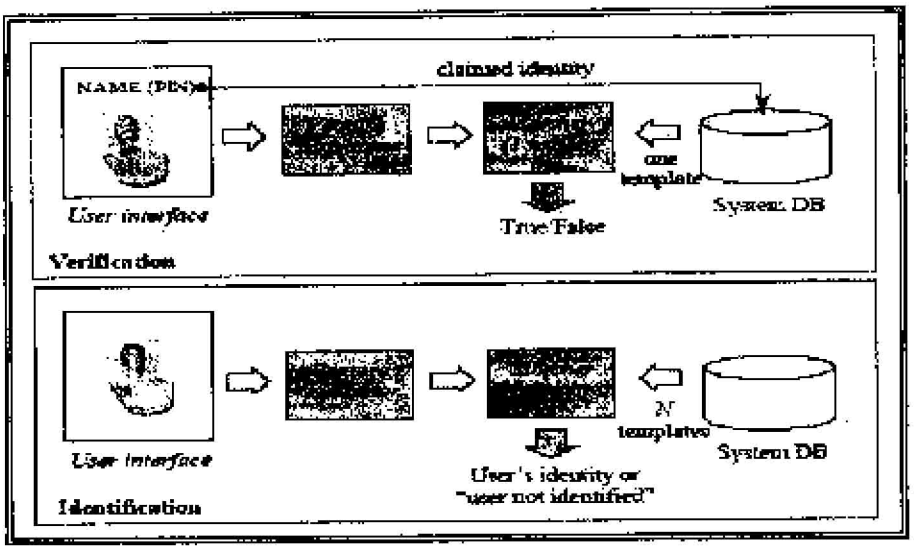

Figure (1) Block diagrams of verification and identification takes, where DB (database) and PIN (personal identification number) [1]

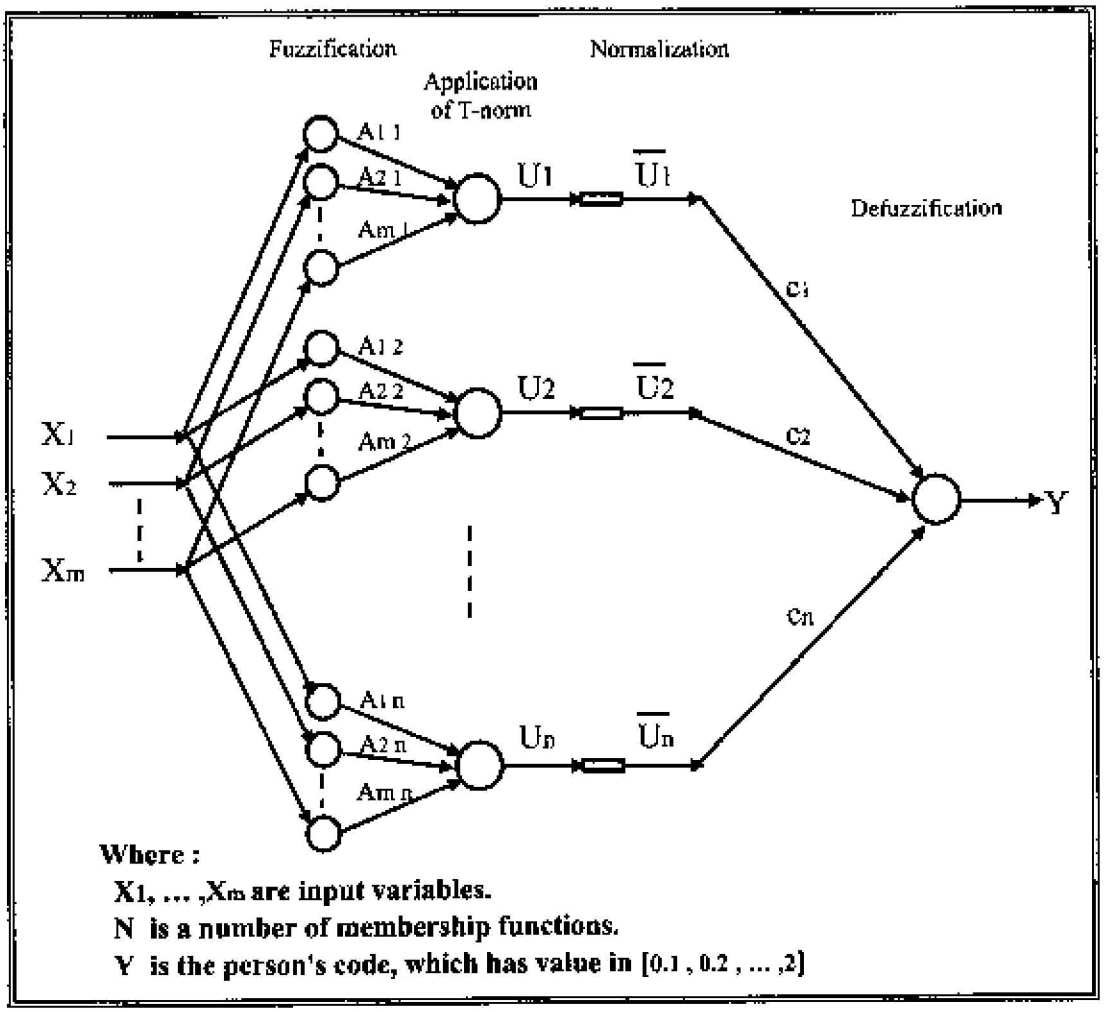

Figure (2) NeuroFuzzy System (NFS) Structure

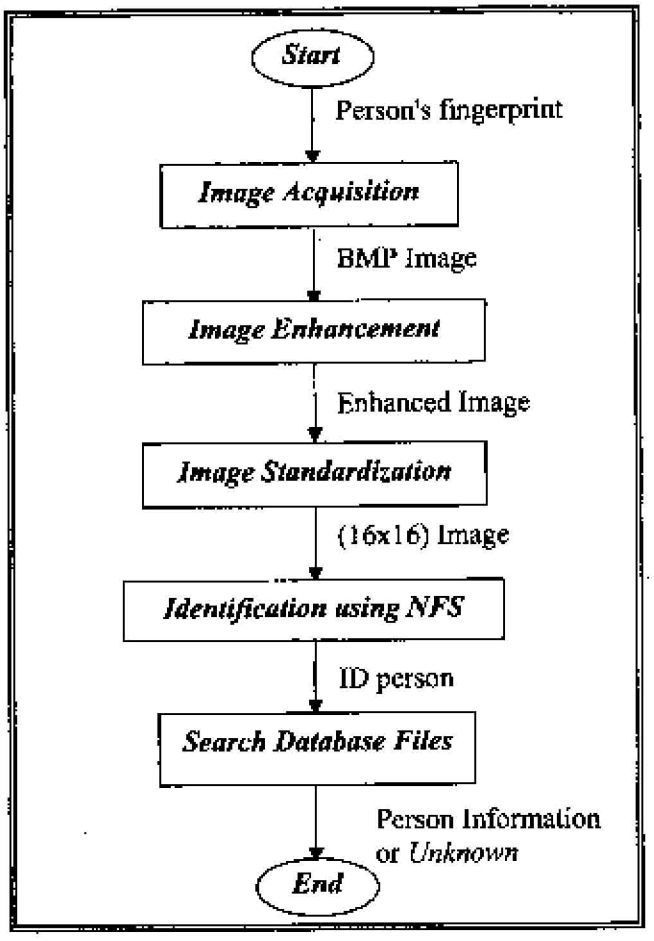

Figure (3) Stages sequence of the proposed approach

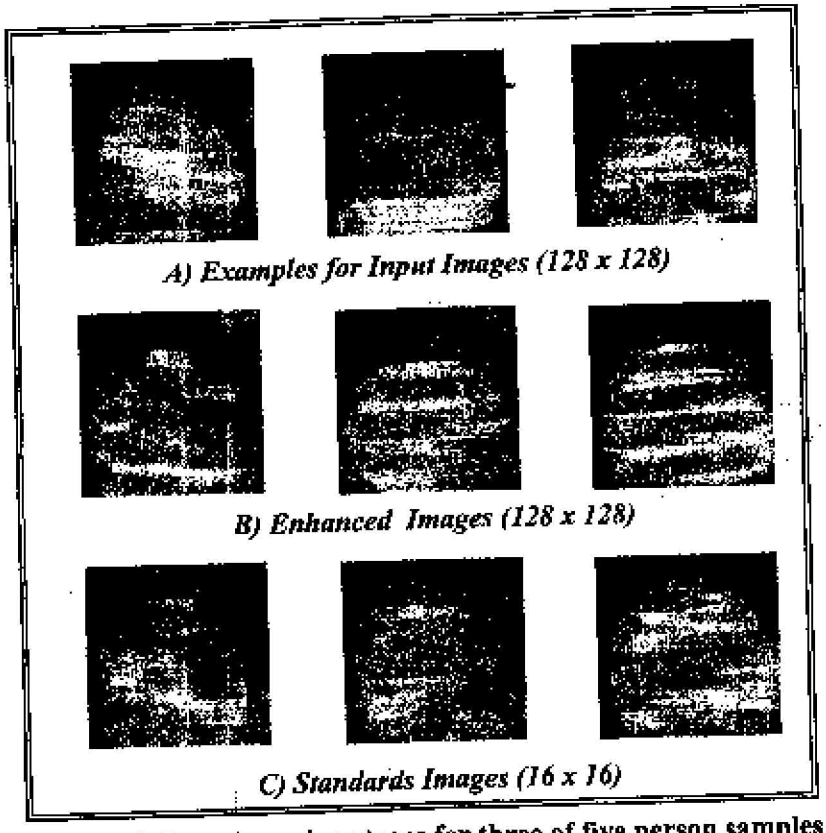

Figure (4) Pre-processing stages for three of five person samples

	Fingerprint for	NFS output	Nearest person's code in database	EE	Result
Training Persons	Ahmmed Sallam	0.09975	0.1	0.00025	***Known***
	Mhaned	0.3009	0.3	0.0009	***Known***
	Marwan Hassan	0.500908	0.5	0.000908	***Known***
	Zainab Ali	0.7992	0.8	0.0008	***Known***
	Jamal Ahmmed	0.9999	1	0.0001	***Known***
	Emad Shallan	1.20094	1.2	0.00094	***Known***
	Hameed	1.40014	1.4	0.00014	***Known***
	Mohmmed Sameer	1.59936	1.6	0.00064	***Known***
	Raid Abdulih	1.70045	1.7	0.00045	***Known***
	Soha Mohmmed	1.90032	1.9	0.00032	***Known***
New Persons	Saher Ali	0.15002	0.2	0.04998	Unknown
	Samir	0.94014	0.9	0.04014	Unknown
	Saad	0.55038	0.6	0.04962	Unknown
	Ali	0.2231	0.2	0.0231	Unknown
	Muha	0.78132	0.8	0.01868	Unknown

Table (1) The results of the proposed approach for the tested fingerprints