ISSN:0975-9646
Chaitanya Kommini et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (4) , 2011, 1764-1773

SCALE AND ROTATION INDEPENDENT FINGERPRINT RECOGNITION

Chaitanya Kommini
Dept of IT,
SVEC, Tirupati
J.N.T.Univeristy, Anantapur
A.P – 517 102, India

Srinivasulu Asadi
Dept of IT,
SVEC, Tirupati
J.N.T.Univeristy, Anantapur
A.P – 517 102, India

Kamalesh Ellanti
Dept of IT,
SVEC, Tirupati
J.N.T.Univeristy, Anantapur
A.P – 517 102, India

ABSTRACT
This paper focuses on the various phases and challenges in Fingerprint Recognition systems, and how these systems can be used in various spheres of life. A new method of fingerprint recognition based on features extracted from the fractal transform of the discrete image is proposed. The fractal features are extracted directly from the gray-scale fingerprint images without applying any pre-processing operations (e.g. image enhancement, directional filtering, ridge segmentation, ridge thinning and minutiae extraction). This helps to achieve lower computational complexity than conventional methods based on minutiae features. It is found that, this method facilitates in obtaining different depth information for the same image, and thus is more informative than the conventional feature parameters currently being used. A comparative study of the feature parameters obtained from fractals and another method (wavelets) revealed that fractal features shows lesser variation when scale or orientation are changed, than wavelet features. The high recognition rates as well as its low computational complexity and independence from variation of scale and rotation, achieved shows that the proposed method may constitute an efficient solution for a small fingerprint recognition system.

GENERAL TERMS
Biometrics, Fingerprint recognition, Feature Extraction.

INDEX TERMS
Fractal transform, wavelet transform, minutiae features.

1. INTRODUCTION
Human recognition and identity verification systems are an important part of our everyday life. A typical example is the *Automated Teller Machine* (ATM) which employs a simple identity verification scheme: the user is asked to enter their secret password after inserting their ATM card into the slot provided for the purpose. If the password matches with the one prescribed to the card, the user is allowed access to their bank account. This scheme suffers from a major drawback: only the validity of the combination of certain possession (the ATM card) and certain knowledge (the password) is verified. The ATM card can be lost or stolen, and the password can be compromised. Thus new verification methods have emerged, where the password has either been replaced by, or used in addition to, biometrics such as person's fingerprints, face image or speech.

Other than the ATM example described above, biometrics can be applied to other areas, such as telephone & internet based banking, airline reservations and check ins, and also in forensic work and law enforcement applications.

Biometric systems based on fingerprints have shown to be quite effective. However their performance easily degrades in the presence of a mismatch between training and testing conditions. For fingerprint based systems this is usually in the form of a change in the illumination direction or orientation of the fingerprints during its acquisition.

A system which uses more than one biometric at the same time is known as a multi-modal verification system. But using more than one biometrics can have a great ask on the systems performance as a large amount of computations might be involved. So fingerprints can be a better alternative to multi-modal verification system, because the probability of two fingerprints patterns of different persons being same is 1 in 1.9 x 1015. So fingerprint alone is sufficient to differentiate two persons.

The robustness of a fingerprint based system to scale, rotation or translation can be increased by using fractals for feature extraction since fractal features are known to be scale and rotation independent.

This paper presents a discussion of the prevailing trends in the field of Biometrics, concentrating more on Fingerprint recognition systems. Research activity in the domain of Biometrics and specially fingerprints has increased significantly over the past decade. The aim of this work here is to improve understanding of biometrics as a technology and to explore its possible use in Fingerprint recognition. An introduction on the topics like *Biometrics (*specially *Fingerprints)* and *Fractals* have been included, as these are central in this work. Finally, a method based on fractals, is proposed to automatically recognize an individual from the fingerprint image.

The study of fingerprints over the years have resulted in enlisting of some essential facts about fingerprints, which are as follows

- Fingerprints are imprints formed by friction ridges of the skins in fingers and thumbs.
- Their formations depend on the initial conditions of the embryonic mesoderm from which they develop.
- Fingerprints exhibits Individuality, which refers to the uniqueness of ridge details across individuals, the probability that two fingerprints are alike is about 1 in 1.9 x 1015.
- Fingerprints exhibit immutability, which refers to the permanent and unchanging character of the pattern on each finger, from before birth until decomposition after death.

Unauthorized access to mission critical or risk involving applications like entry into restricted places or monetary transactions have caused a great deal of problems and financial loss for the affected ones. Moreover the increase in the number of crimes in the society and the increase in number of cases where a

culprit or the convicted is acquitted for the lack of evidence has brought about a matter of concern for the society. So a means of identification of an individual need to be installed at every such institution where operations can be critical if an unauthorized person access the system in it or those (courts) which are responsible for nailing down a culprit accused of committing a crime and giving appropriate punishment. This gave motivation to make some efforts in coming up with an individual recognition system based on biometrics. And then search for an appropriate biometric revealed that fingerprints can be a good choice. The survey of past research in the area of Fingerprint Recognition revealed that there has been one or the other problem in the methodologies adopted. For e.g. the minutiae-based methods have to go through a preprocessing stage in which operations like image enhancement, directional filtering, ridge segmentation, ridge thinning and minutiae extraction are to be done on the fingerprint image. Moreover the fingerprint images with low quality (low resolution or low illumination) cannot render them for reliable minutiae extraction. Among the image-based methods, the one that uses wavelet features for fingerprint recognition has the disadvantage of exhibiting limited ability to track the variations in position, scale and orientation angle. To remove these disabilities additional operations need to be done, such as, canceling the effect of the variation in position between two fingerprints by choosing a reference point in each fingerprint, which may be the singular points or the core points, and can be detected using methods like those proposed in [11], [12]. The search for a methodology that can tackle both the problems of minutiae based methods and also the wavelet based approach of the image based methods led to the domain of fractals, which are known to be scale and rotation independent. Moreover the fractal approach for feature extraction is applied directly to the gray-scale fingerprint image without preprocessing, and hence they may achieve higher computational efficiency than the minutiae based methods. Thus this finding became the motivation to tread on the road to develop a fingerprint recognition system based on fractals.

In *Section 2*, a detailed analysis of past research is presented, in which the information such as, about the history of fingerprints and the background of biometrics, the analysis of some existing fingerprint recognition methods have been dealt with. In *Section 3*, the details of the various phases of the proposed methodology are brought forward. *Section 4* gives the results obtained after the proposed method was applied on the test images. It also shows the comparative analysis of Fuzzy membership of closeness function and Euclidean classifier, a comparative analysis of fractal and wavelet features and also makes a discussion on the results. Finally conclusions of the work done in this paper are drawn in *Section 6,* and the future directions for the method proposed are also indicated.

2. PRIOR WORK

Fingerprint recognition has a very good balance of all the desirable properties like universality, Distinctiveness, Permanence, Collectability, Performance, Acceptability and Circumvention. Every human being possesses fingerprints with the exception of any hand-related disabilities. Fingerprints are very distinctive; fingerprint details are permanent, even if they may temporarily change slightly due to cuts and bruises on the skin or weather conditions. Live-scan fingerprint sensors can easily capture high quality images and they do not suffer from the problem of segmentation of the fingerprint from the background (e.g., unlike face recognition). However, they are not suitable for covert applications (e.g., surveillance) as live-scan fingerprint scanners cannot capture a fingerprint image from a distance without the knowledge of the person. The deployed fingerprint based biometric systems offer good performance and fingerprint sensors have become quite small and affordable. Although each of these techniques, to a certain extent, satisfies the requirement of establishing the identity of an individual and has been used in practical systems or has the potential to become a valid biometric technique, not many of them are acceptable (in a court of law) as indisputable evidence of identity. For example, despite the fact that extensive studies have been conducted on automatic face recognition and that a number of face-recognition systems are available [22], [23], [24], it has not yet been proven that

- Face can be used reliably to establish/verify identity and
- A biometric system that uses only face can achieve acceptable identification accuracy in a practical environment.

Without any other information about the people, it will be extremely difficult for both a human and a face-recognition system to conclude that the different faces are disguised versions of the same person. So far, the only legally acceptable, readily automated, and mature biometric technique is the automatic fingerprint identification technique, which has been used and accepted in forensics since the early 1970's [25]. Although signatures also are legally acceptable biometrics, they rank a distant second to fingerprints due to issues involved with accuracy, forgery, and behavioral variability.

A. Design of a Fingerprint Recognition System

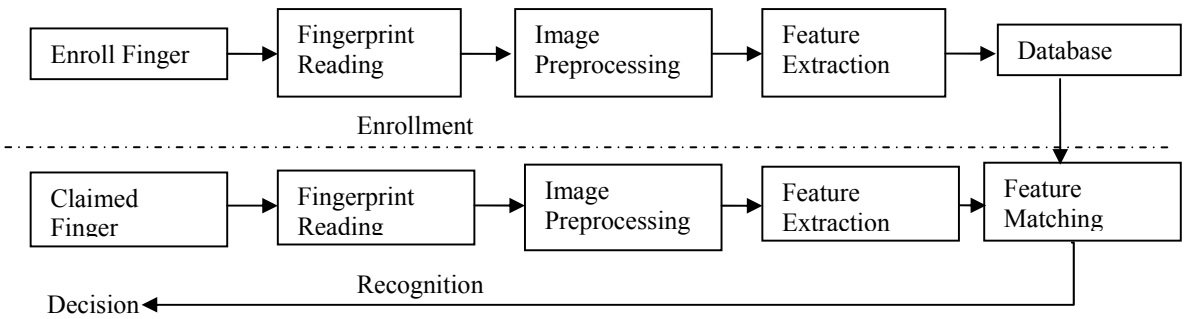


Figure 2.1 Block Diagram of a typical fingerprint recognition system.

As shown in *Figure 2.1*, a typical fingerprint recognition system works in two distinct modes: enrollment and recognition. The purpose of the enrollment mode is to create a database. During this mode, an enrollee fingerprint is captured and processed in three stages: Fingerprint Reading, Image Preprocessing and Feature Extraction. After the Feature Extraction stage, a set of representative features of the enrollee fingerprint is saved in the database. During the recognition mode, a fingerprint to be recognized undergoes the same three preprocessing steps as in the enrollment mode. The result, a test template is compared with the stored templates from the database in the Feature Matching stage. A matching score which measure the degree of similarity between the two templates is calculated. Higher values indicate higher confidence in a match. An automatic fingerprint identity authentication system has four main design components: *acquisition*, *representation* (template), f*eature extraction*, and *matching*. The third phase i.e. feature extraction involves representing the image by a set of numerical features to remove redundancy from the data and reduce its dimension. The last stage performs matching, where a class label is assigned to the unknown image by examining its extracted features and comparing them with class representations that the classifier has learned during its training stage.

i) Acquisition:

The first step is image acquisition, i.e. converting a scene into an array of numbers that can be manipulated by the computer. There are two primary methods of capturing a fingerprint image: inked (off-line) and live scan (ink-less). An inked fingerprint image is typically acquired in the following way: a trained professional obtains an impression of an inked finger on a paper, and the impression is then scanned using a flatbed document scanner. The live scan fingerprint is a collective term for a fingerprint image directly obtained from the finger without the intermediate step of getting an impression on a paper. Acquisition of inked fingerprints is cumbersome; in the context of an identity authentication system, it is both infeasible and socially unacceptable for identity verification. The most popular technology to obtain a live-scan fingerprint image is based on the optical frustrated total internal reflection (FTIR) concept [19]. When a finger is placed on one side of a glass platen (prism), ridges of the finger are in contact with the platen while the valleys of the finger are not. The rest of the imaging system essentially consists of an assembly of a light emitting diode (LED) light source and a charge-couple device (CCD) placed on the other side of the glass platen. The laser light source illuminates the glass at a certain angle, and the camera is placed such that it can capture the laser light reflected from the glass. The light that is incident on the plate at the glass surface touched by the ridges is randomly scattered, while the light incident at the glass surface corresponding to valleys suffers total internal reflection, resulting in a corresponding fingerprint image on the imaging plane of the CCD. A number of other live-scan imaging methods are now available, based on ultrasound total internal reflection [19], optical total internal reflection of edge-lit holograms [21], thermal sensing of the temperature differential (across the ridges and valleys) [19], sensing of differential capacitance [25], and noncontact three-dimensional scanning [25]. These alternate methods are primarily concerned with either reducing the size/price of the optical scanning system or improving the quality/resolution/consistency of the image capture.

ii) Representation (Template):

The second phase is representation, which may involve preprocessing operations like removing noise, enhancing the picture, and if necessary, segmenting the image into meaningful regions to be analyzed separately. The main representation issue – "Which machine readable representation completely captures the invariant and discriminatory information in a fingerprint image?" constitutes the essence of fingerprint verification design and has far-reaching implications on the design of the rest of the system. The unprocessed grayscale values of the fingerprint images are not invariant over the time of capture.

Representations based on the entire gray-scale profile of a fingerprint image are prevalent among the verification systems using optical matching [21]. The utility of the systems using such representation schemes, however, may be limited due to factors like brightness variations, image-quality variations, scars, and large global distortions present in the fingerprint image because these systems are essentially resorting to template-matching strategies for verification. Further, in many verification applications, terser representations are desirable, which preclude representations that involve the entire grayscale profile fingerprint images. Some system designers attempt to circumvent this problem by restricting that the representation is derived from a *small* (but consistent) part of the finger [21]. If this same representation is also being used for identification applications, however, then the resulting systems might stand a risk of restricting the number of unique identities that could be handled simply because of the fact that the number of distinguishable templates is limited. On the other hand, an image-based representation makes fewer assumptions about the application domain (fingerprints) and therefore has the potential to be robust to wider varieties of fingerprint images. For instance, it is extremely difficult to extract a landmark-based representation from a (degenerate) finger devoid of any ridge structure. Representations that rely on the entire ridge structure (ridge based representations) are largely invariant to the brightness variations but are significantly more sensitive to the quality of the fingerprint image than the landmark-based representations described below. This is because the presence of the landmarks is, in principle, easier to verify [25]. An alternative to gray-scale-based representation is to extract landmark features from a binarized fingerprint image. Landmark-based representations are also used for privacy reasons—one cannot reconstruct the entire fingerprint image from the fingerprint landmark information alone. The common hypothesis underlying such representations is the belief that the individuality of fingerprints is captured by the local ridge structures (minute details) and their spatial distributions [21], [25]. Therefore, automatic fingerprint verification is usually achieved with minute-detail matching instead of a pixel-wise matching or a ridge-pattern matching of fingerprint images. In total, there are approximately 150 different types of local ridge structures that have been identified [25]. It would be extremely difficult to automatically, quickly, and reliably extract these different representations from the fingerprint images because

1) Some of them are so similar to each other, and

2) Their characterization depends upon the fine details of the ridge structure, which are very difficult to obtain from fingerprint images of a variety of quality.

Typically, automatic fingerprint identification and authentication systems rely on representing the two most prominent structures: *ridge endings* and *ridge bifurcations*, shown in *Figure 2.2*.

These two structures are background-foreground duals of each other, and pressure variations could convert one type of structure into the other. Therefore, many common representation schemes do not distinguish between ridge endings and bifurcations. Both the structures are treated equivalently and are collectively called *minutiae*. The simplest of the minutiae based representations constitute a list of points defined by their spatial coordinates with respect to a fixed image centric coordinate system. Typically, though, these minimal minutiae-based representations are further enhanced by tagging each minutia (or each combination of minutiae subset, e.g., pairs, triplets) with additional features. For instance, each minutia could be associated with the orientation of the ridge at that minutia; or each pair of the minutiae could be associated with the ridge count: the number of ridges visited during the linear traversal between the two minutiae. The minutiae-based representation might also include one or more global attributes like orientation of the finger, locations of core or delta, and fingerprint class.

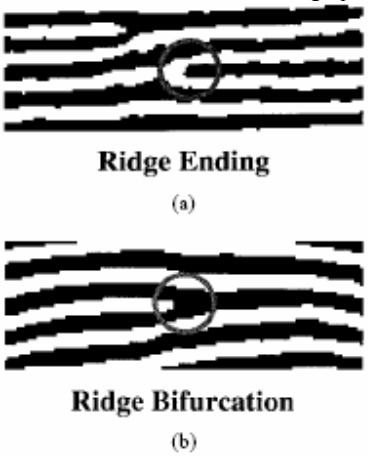


Figure 2.2: Ridge ending and ridge bifurcation.

iii) Feature Extraction:

A feature extractor finds the ridge endings and ridge bifurcations from the input fingerprint images. If ridges can be perfectly located in an input fingerprint image, then minutiae extraction is just a trivial task of extracting singular points in a thinned ridge map. In practice, however, it is not always possible to obtain a perfect ridge map. The performance of currently available minutiae-extraction algorithms depends heavily on the quality of input fingerprint images. Due to a number of factors (aberrant formations of epidermal ridges of fingerprints, postnatal marks, occupational marks, problems with acquisition devices, etc.), fingerprint images may not always have well-defined ridge structures. Reliable minutiae-extraction algorithms should not assume perfect ridge structures and should degrade gracefully with the quality of fingerprint images.

iv) Matching:

Given two (test and reference) representations, the matching module determines whether the prints are impressions of the same finger. The matching phase typically defines a metric of the similarity between two fingerprint representations. The matching stage also defines a threshold to decide whether a given pair of representations is of the same finger (mated pair) or not. In the case of the minutiae-based representations, the fingerprint verification problem may be reduced to a point pattern matching (minutiae pattern matching) problem. In the ideal case, if

1) The correspondence between the template minutiae pattern and input minutiae pattern is known,
2) There are no deformations such as translation, rotation, and deformations between them, and
3) Each minutia present in a fingerprint image is exactly localized,

Then fingerprint verification is only a trivial task of counting the number of spatially matching pairs between the two images. Determining whether two representations of a finger extracted from its two impressions, possibly separated by a long duration of time, are indeed representing the same finger is an extremely difficult problem. Difficulty is often encountered in the matching of the images of the same finger. The difficulty can be attributed to two primary reasons. First, if the test and reference representations are indeed mated pairs, the correspondence between the test and reference minutiae in the two representations is not known. Second, the imaging system presents a number of peculiar and challenging situations, some of which are unique to a fingerprint image capture scenario.

3. PROPOSED SYSTEM

In this current work, the methodology proposed is based on fractals. Fractal characteristics have recently gained popularity in image analysis. They have been applied to different areas, especially to image compression and texture image segmentation. The main reason for it is their insensitivity to a wide range of distortions of a scene and good descriptive qualities. Fractal dimensions (more precisely, different *estimates of fractal dimensions* (EFDs) calculated from images) is the primary characteristics, used in image recognition tasks. Mathematically fractal dimension is invariant to scaling, rotation and smooth deformations. When fractal features are used for texture discrimination, it is supposed that the area of patches of homogeneous texture is rather large.

As discussed in *Section 2*, a typical fingerprint recognition system has four phases. The four phases during the development of the current fingerprint recognition system are shown in *Figure 3.1* and discussed hereunder.

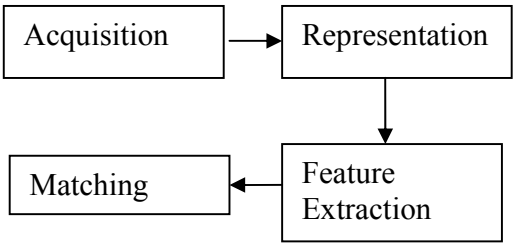


Figure 3.1: Various Phases of the proposed Fingerprint Recognition System.

a) **Acquisition**: The fingerprint image databases were acquired from a website which conducts Fingerprint Verification Competition. The URL for the website is http://bias.csr.unibo.it/fvc2000/. They had collected the four

different databases (DB1, DB2, DB3 and DB4) by using the following sensors/technologies:

DB1: low-cost optical sensor "Secure Desktop Scanner" by KeyTronic.

DB2: low-cost capacitive sensor "Touch Chip" by ST Microelectronics.

DB3: optical sensor "DF-90" by Identicator Technology.

DB4: synthetic fingerprint generation. Each of these databases has 80 images, 8 each from 10 individuals. The *Figure 3.2* shows a sample image from each database.

Figure 3.2: A sample image from each database.

b) **Representation**: All the fingerprint images contained in databases, obtained from the above mentioned URL are 8-bit gray-scale images with their intensity values in the range (0-255). The images of DB1 are of size 300 x 300. Since the methodology adopted here is an image-based approach, rather than a minutiae-based approach, the preprocessing operations like image enhancement, orientation flow estimation, ridge segmentation, ridge thinning, and minutiae detection are not required to be performed before the feature extraction phase.

c) **Feature Extraction**: Fractal dimension is used to calculate the feature vectors from the training fingerprint images. The feature extraction phase comprises of several stages. Firstly, from the original gray-scale image, *n* numbers of binary images are obtained by splitting the image at different intensity levels. Thus those pixels of the original image which had intensity values in a particular interval are marked as occupied in the binary image for that intensity interval of the original image. Box-counting algorithm is then used on several (*m*) low scale version of each binary image to get the number of occupied cells in the sub block of size (Scale x Scale) of the binary image. If the sub blocks contain at least one occupied cell then the corresponding cell in reduced scale is marked as occupied. Then the number of occupied cells in the reduced scale image is counted. In this way, for each binary image, *m* different counts for *m* different scales of the binary image are obtained.

$$\log M = D \log L + C \quad (3.3)$$

Then using the *equation 3.3* where the *m* different values of M and L are known the fractal parameters D and C are obtained. This is generally done by a line-fitting algorithm, in which a line which best fits the *m* pairs of X and Y is obtained. Then the slope and Y-intercept of the line thus obtained are taken to be the feature parameters.

The quality of the feature parameters obtained can be analyzed using a clustering algorithm. In this algorithm, fingerprints taken as training samples are grouped into clusters. Each cluster consists of the fingerprints belonging to a particular individual. The clustering algorithm [6] used for the purpose, involves the following steps:

Step 1) the centre of gravity (*c.g*) of the multi-fractal parameter vector (MFPV) of a particular fingerprint is calculated in a multidimensional space.

Step 2) the distances of the (MFPV) from the c.g and the respective standard deviation are calculated.

Step 3) if the c.g.s along with the sphere drawn with a radius as their respective standard deviation for all the fingerprints are found to be well separated so that there occurs no overlapping of the spheres, then this parameter may be fixed as a good clustering tool or classifying tool for the fingerprints.

d) **Matching**: Two criteria are used for the purpose of matching, which are Fuzzy Closeness of Membership Function [6] and Euclidean distance classifier [2]. The feature vector of the test fingerprint image is compared with the training set feature vectors to obtain the Euclidean distance between them. And then the minimum value of the Euclidean distance gives the closest match for the test fingerprint.

A 2nd criterion i.e. Fuzzy Closeness of Membership function, used for the above purpose, is given by:

The Membership of closeness function is defined for any two images X & Y of image database as $\boldsymbol{\mu}^{\mathbf{c}}_{\mathbf{x,\ y}} \leq 1\text{-}|\ (D^jX - D^jY)/\ \max\_of(D^jX,\ D^jY)|$ where j indicates jth component of multifractal that varies from 1 to m. For an image database of N number of images, a closeness membership vector (CMV) is defined for an unknown image U as $\{\mu^{\mathbf{c}}\mathbf{U},\ i\}$ i, where i varies from 1 to N which could be used to sort the images of the database.

4. RESULTS

A database of 80 images of size 300 x 300 including 8 images per finger from 10 individuals have been used for experiments. The recognition performances achieved by using the proposed fractal features have been evaluated using both Fuzzy Membership of Closeness Function and Euclidean distance classifier, with no rejection option.

A number of k images from each individual (for a total of 10k images) have been used as the training set, whereas the remaining 8-k images from each individual (for a total of 10 x (8-k) images) have been used for testing.

Figure 4.1 shows one sample fingerprint of each person. The results shown hereunder in the *Figures 4.2(a) – 4.2(d)* have been obtained by taking k = 7, i.e. 7 images from each person has been taken for the training image set and 1 each for the test image set.

Table 4.1 and *Table 4.2* shows the percentage success of identifying an exact match within first 1,2 and 3 images, sorted in order of closest matches, using Fuzzy Membership of Closeness Function and Euclidean Distance Classifier respectively.

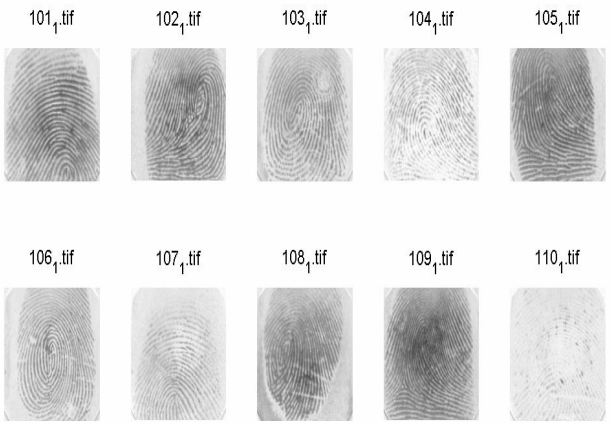


Figure 4.1: Training Set fingerprint images. (One Each from 10 Persons)

Table 4.1: Representation of the result of query submission for fingerprint-image database using Fuzzy Membership of Closeness Function.

Number of queries	Percentage of success to identify exact match within first image sorted	Percentage of success to identify exact match within first 2 images sorted	Percentage of success to identify exact match within first 3 images sorted
10	70	90	100

Table 4.2 Representation of the result of query submission for fingerprint-image database using Euclidean Distance Classifier.

Number of queries	Percentage of success to identify exact match within first image sorted	Percentage of success to identify exact match within first 2 images sorted	Percentage of success to identify exact match within first 3 images sorted
10	70	90	90

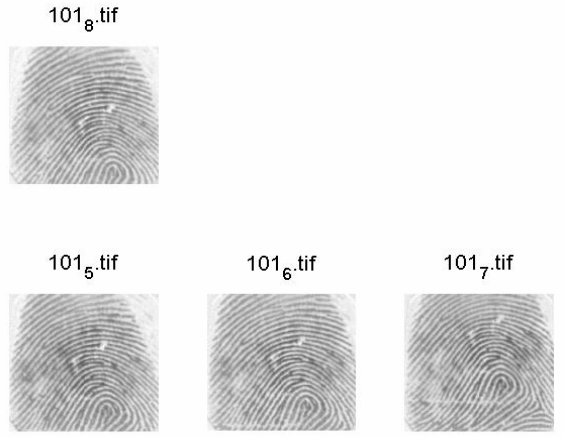
5. DISCUSSIONS

Table 4.1 and *Table 4.2* shows that the Fuzzy Membership of Closeness function as a matching criterion is better than the Euclidean Distance Classifier, as the exact match is found in 100% of the queries within first 3 images sorted for Fuzzy Membership of Closeness criterion while for Euclidean Distance Classifier it is found in 90% of the queries.

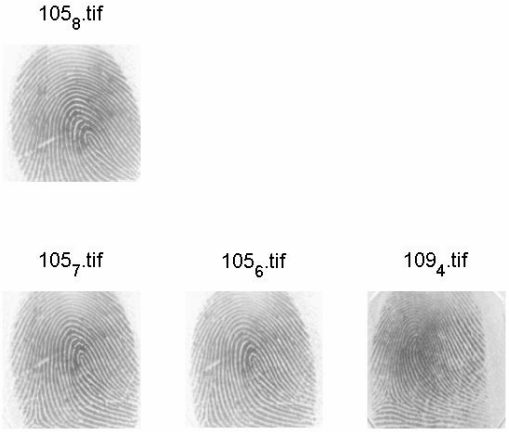
Figures 4.2 (a) - (d) shows that the exact match for a test image is found within first 3 images sorted in order of closeness.

Figures 4.3 (a) – (d) shows the results obtained during the intermediate steps of the recognition process, and the accuracy of the results.

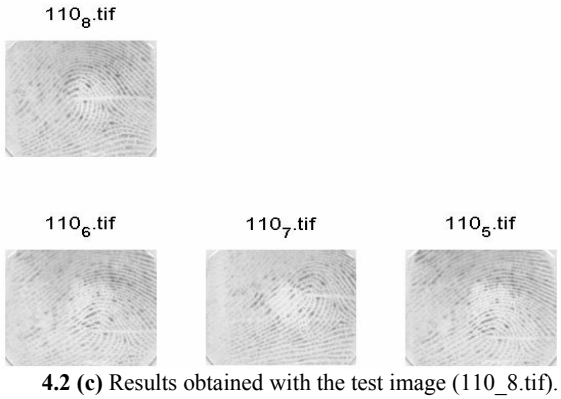
Figure 4.4 and the associated result values reiterate that the fractal feature parameters exhibit more scale and rotation independence than the wavelet feature parameters.



4.2 (a) Results obtained with the test image (101_8.tif).



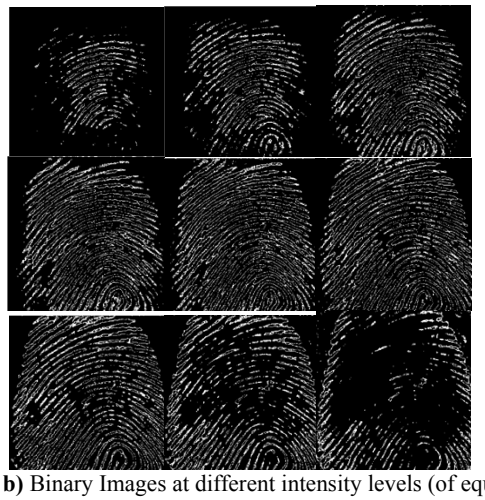
4.2 (b) Results obtained with the test image (105_8.tif).



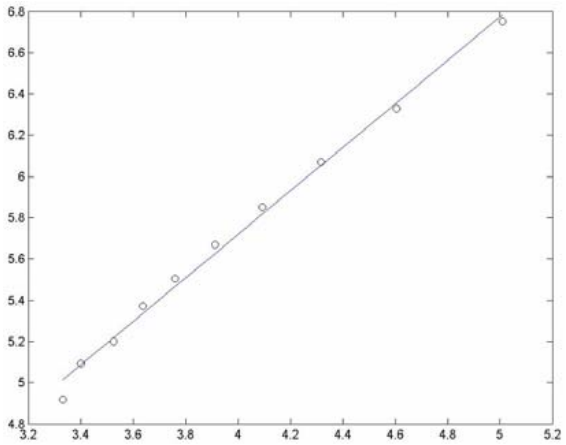
4.2 (c) Results obtained with the test image (110_8.tif).

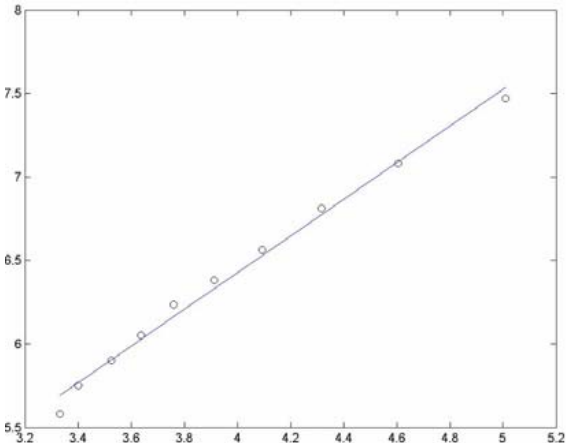
Figure 4.2 (a) – (c): Some representative output (showing 3 closest matches) based on multi-fractal approach.

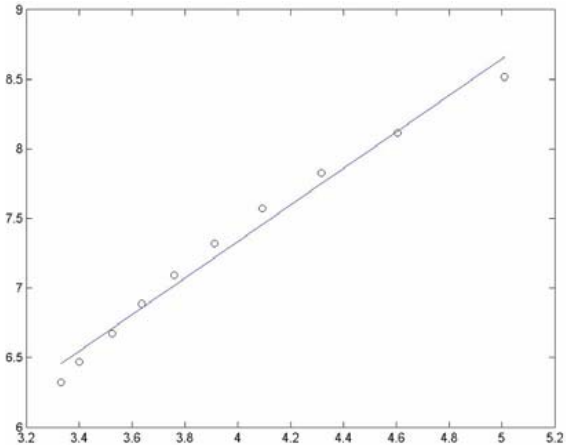
4.3 a) Original Test Image. (101_8.tif)

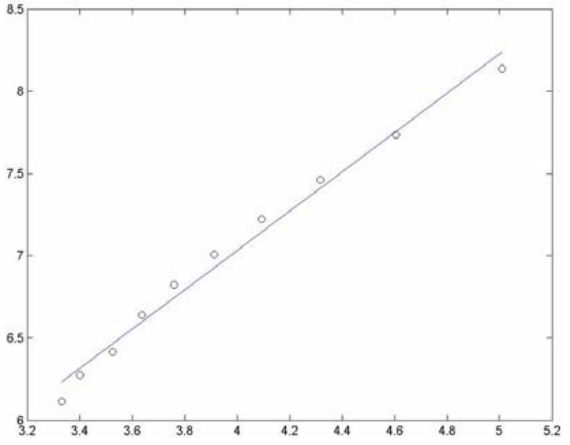


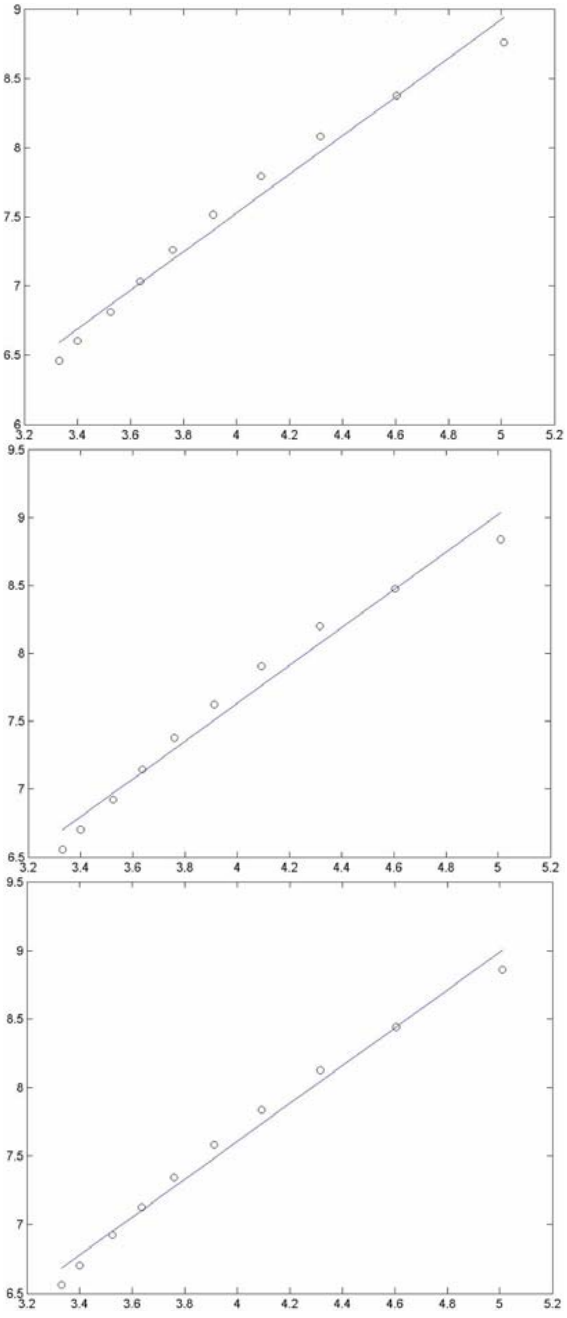
4.3 b) Binary Images at different intensity levels (of equal interval) for the image in (a)

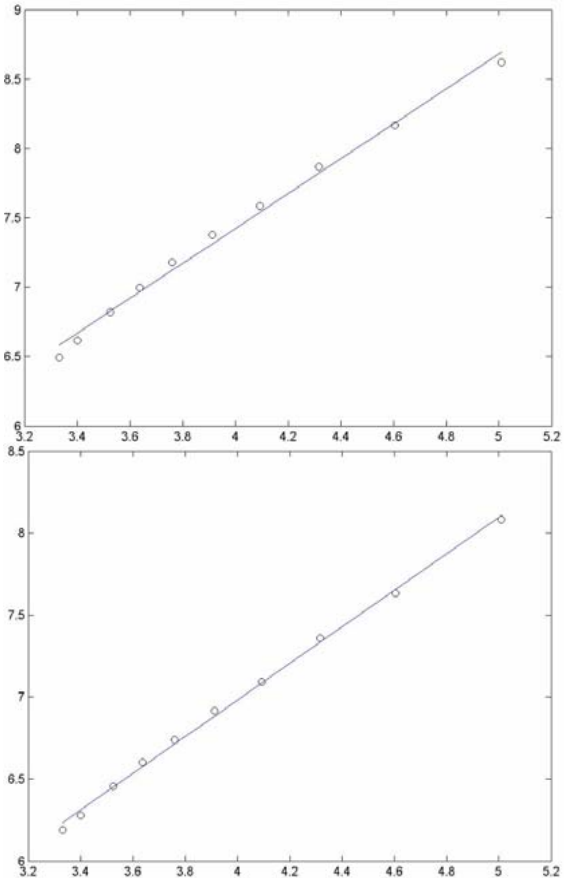




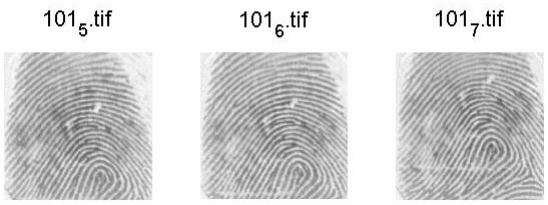








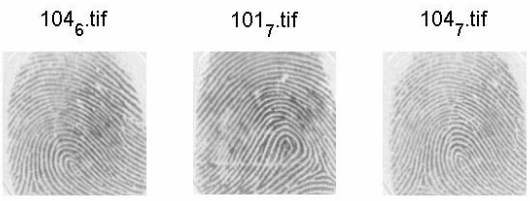
4.3 c) Fractal Line-fit curves for the image in (a)



4.3 d) Results obtained for the image in (a).

a) Original Image.

b) *Scale Reduced by 3.*



c) 3 Closest matches for the reduced scale test image (101_8.tif) in (b).

Figure 4.3 (a) - (d): Various images obtained at intermediate steps during the entire process.

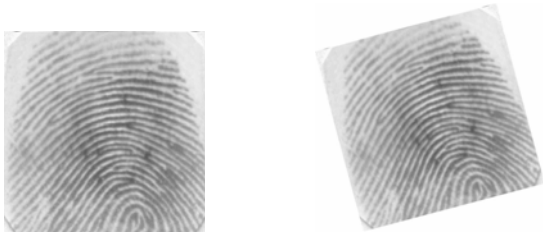


Figure 4.4 Shows portrait and rotated version of same image. (101_8.tif)

6. CONCLUSIONS

A new method of fingerprint recognition using fractal features has been proposed. The features are extracted directly from the gray scale fingerprint image without preprocessing, and hence the proposed method achieves lower computational complexity than conventional methods based on minutiae features. The Fuzzy Membership of Closeness Function proved a better matching criterion than Euclidean Distance Classifier. The method has been successfully compared against one of the methods (wavelets) recently proposed in the literature. This revealed that the fractal feature vectors are independent of variation in scale and rotation, as the variation in fractal feature parameters is less after a change in scale and orientation while it is very high for wavelet feature parameters. And it is also found that the clusters obtained from the fractal features have lesser overlap region than that obtained from wavelet features, thus increasing the ability to separate out the clusters during the matching stage of the recognition process. the high recognition rates achieved by this method as well as its low computational complexity and independence from variation of scale and rotation reveal that this method can be used to effectively solve a security problem involving a small number of fingerprint images.

There is great scope of using the multifractal parameter approach proposed here in other domains where scale and rotation independence are desired such as:

- Face Recognition Systems.
- Natural Texture Identification.
- Analysis of Biological Images, e.g. histo-pathological images, for disease diagnosis.

7. REFERENCES

[1]. Barnsley**,** Michael F., **"**Fractals Everywhere**",** *2nd Edition***.** *AP Professional*, 1993.

[2]. Gonzales, R. and Woods, R., "Digital Image Processing". *2nd edition, Prentice-Hall, Englewood Cliffs, NJ*, 2002 Mandelbrot, B.B., "The Fractal Geometry of Nature*"*, *Freeman*, *USA*, 1988

[3]. Feder, "Fractals", *Plenum Press*, *New York*, 1988.

[4]. Maltoni, D.; Maio, D.; Jain, A.K.; Prabhakar, S., "Handbook of Fingerprint Recognition." *Springer*, *New York*, 2003.

[5]. Lahiri, T. and Dutta Majumder, D., "Fuzzy multi fractal approach in the study of texture complexity in an image database", *Proceedings of the Conference on Fuzzy Set Theory and Its Mathematical Aspects and Application* held on December 26-28, 2002 at Department of Mathematics, Banaras

[6]. Hindu University, Allied Publishers Pvt. Ltd., India.

[7]. Tico, M.; Immonen, E.; Ramo, P.; Kuosmanen, P.; Saarinen, J., "Fingerprint recognition using wavelet features.", *The 2001 IEEE International Symposium on Circuits and Systems, 2001*. ISCAS 2001, Volume: 2, 6-9 May 2001 Pages: 21 - 24

[8]. Leung, W.F.; Leung, S.H.; Lau, W.H.; Luk, A., "Fingerprint recognition using neural network.", *Proceedings of the 1991 IEEE workshop on Neural Networks for Signal Processing [1991]*., 30 Sept.-1 Oct. 1991, Pages: 226 – 235

[9]. Xuejun, Tan; Bhanu, B., "Fingerprint verification using genetic algorithms.", in *Proceedings of Sixth IEEE Workshop on Applications of Computer Vision, 2002. (WACV 2002)*, 3-4 Dec. 2002 Pages: 79 – 83

[10]. Senior, A., "A hidden Markov model fingerprint classifier.", in *Conference Record of the Thirty-First Asilomar Conference on Signals, Systems & Computers, 1997.* Volume: 1, 2-5 Nov. 1997, Pages: 306 – 310

[11]. Wei Shen; Xia Chen; Jun Shen, "Robust detection of singular points for fingerprint recognition.", in *Proceedings of Seventh International Symposium on Signal Processing and Its Applications, 2003*, volume: 2, July 1-4, 2003 Pages: 439 – 442

[12]. Ching-Tang Hsieh; Zhuang Yuan Lu; Tan Chi Li; Kung Chen Mei, "An effective method to extract fingerprint singular point.", in *Proceedings of The Fourth International Conference/Exhibition on High Performance Computing in the Asia-Pacific Region, 2000*, Volume: 2, 14-17 May 2000, Pages: 696 - 699 vol.2

[13]. Clarke, R., "Human identification in information systems: Management challenges and public policy issues," *Info. Technol. People,* vol. 7, no. 4, pp. 6–37, 1994.

[14]. Coetzee, L. and Botha, E. C., "Fingerprint recognition in low quality images," *Pattern Recognition,* vol. 26, no. 10, pp. 1441–1460, 1993.

[15]. Mimoso, Michael S. - News Editor*," Current economic, political climate opening doors for biometrics"*, 24 Oct 2001 Campbell, J. P., Jr.; Alyea, L. A. and Dunn, J. S. (1996)., "Biometric security: Government applications and operations." [Online]. Available: *http://www.vitro.bloomington.in.us:8080/BC/.*

[16]. Candela, G. T.; Grother, P. J.; Watson, C. I.; Wilkinson, R. A. and Wilson, C. L., "PCASYS: A pattern-level classification automation system for fingerprints," *National Institute of Standards and Technology, Gaithersburg*, MD, NIST Tech. Rep. NISTIR 5647, Aug. 1995.

[17]. Daugman, J. G., "High confidence visual recognition of persons by a test of statistical independence," *IEEE Trans. Pattern Analysis & Machine Intelligence.,* vol. 15, no. 11, pp. 1148–1161, 1993.

[18]. Jain, A. and Pankanti, S., "Automated Fingerprint Identification and Imaging Systems."

[19]. Davies, S. G., "Touching Big Brother: How biometric technology will fuse flesh and machine," *Info. Technol. People*, vol. 7, no. 4, pp. 60–69, 1994.

[20]. Jain, A.K.; Lin Hong; Pankanti, S.; Bolle, R., "An identity-authentication system using fingerprints." Proceedings of the IEEE, Volume: 85, Issue: 9, Sept. 1997

[21]. Anagnostopoulos, C.; Anagnostopoulos, I.; Vergados, D.; Papaleonidopoulos, I.; Kayafas, E.; Loumos, V.; Stasinopoulos, G., "A probabilistic neural network for face detection on segmented skin areas based on fuzzy rules", *Electrotechnical Conference, 2002. MELECON 2002. 11th Mediterranean*, 7-9 May 2002, Pages: 493 - 497

[22]. Rowley, H.A.; Baluja, S.; Kanade, T., "Neural network-based face detection.", *Proceedings CVPR '96, 1996 IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, 1996., 18-20 June 1996 Pages:203 - 208

[23]. Turk, M.A.; Pentland, A.P., "Face recognition using eigenfaces." *Proceedings CVPR '91, IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 1991.*, 3-6 June 1991, Pages:586 - 591

[24]. Jain, A.K.; Pankanti, S.; Prabhakar, S.; Ross, A., "Recent advances in Fingerprint Verification." Newham, E., "*The Biometric Report*." New York: *SJB Services*, 1995. (Available:http://www.sjb.co.uk/.)