Fingerprint Identification Using Fractal Geometry

Mahmoud H. Farhan
College of Computer
AL Anbar University, Iraq

Loay E. George
College of Science
Baghdad University

Azmi T. Hussein
College of Pure Education
AL Anbar University

Abstract: Fingerprints have been used for personal identification for long time. The fingerprints of any individual are unique and do not change throughout his/her life. The proposal research is using Fractal Geometry as a tool for fingerprint identification. The system has two main phases: Training phase and Test phase. For each phase, the system is applied to two main stages on each fingerprint: preprocessing and features extraction. The preprocessing sub stages consist of some image processing techniques as: Enhancement, Binarization, and Thinning. The extracted attributes are the ridges density, minutiae concentration and the directional intersection count with ridges. From these ridge attributes, the fractal dimension is computed to produce fractal arrays. The test results showed that fractal geometry is a powerful tool in fingerprint recognition, where the attained identification rate is (95%) for training set, while this rate is (92%) for the test set, where the database contains samples for 51 person, 8 samples for each person.

Keywords: Biometrics, Fingerprint, Minutia, Fractal Dimension, Box Counting.

I. INTRODUCTION

Fingerprint is the representation of the epidermis of a finger; it consists of a pattern of interleaved ridges and valleys[1]. In the early twentieth century, fingerprint recognition was formally accepted as a valid personal identification method and became a standard routine in forensics. Fingerprint identification agencies were set up worldwide and criminal fingerprint databases were established. Various fingerprint recognition techniques, including latent fingerprint acquisition, fingerprint classification, and fingerprint matching were developed [2]. Nowadays, automatic fingerprint recognition is one of the most common applications of machine pattern recognition (it dates back to more than fifty years ago). Because of this, there is a popular misconception that fingerprint recognition is a fully solved problem. On the contrary, fingerprint recognition is still a complex and very challenging pattern recognition task [1].

II. FRACTAL GEOMETRY AND FRACTAL DIMENSION

Fractal geometry is the formal study of self-similar structures and is at the conceptual core of understanding nature's complexity. The fractal dimension provides a measure of the complexity of a structure. It is a measure of the mixture of order and surprise in a structure [3]. The fractal dimension is a geometrical quantity which gives the indication of how completely the fractal appears as it is zoomed down to finer and finer scales. Fractal dimension measures the degree of fractal boundary fragmentation or irregularity over multiple scales. Fractal dimension is an effective measure for complex objects. It is widely applied in the fields of image segmentation and shape recognition [4].

Fractal codes have this ability to reproduce an image (or at least a good approximation of it) by a set of contractive transformations. These transformations can be shown in simple affine form and can be recorded by several simple parameters. This compact presentation of images shows its usefulness in image compression. The fractal parameters used in the recognition technique are affine fractal transformations similar to those used for fractal image compression [5]. Fractal image compression suffers from the drawback that the compression algorithm takes an extremely long time to implement [6].

III. PATTERN RECOGNITION AND FRACTAL GEOMETRY

Using fractals for object or shape recognition is a relatively new application of fractal image encoding [5]. It utilizes the powerful mathematics of fractal geometry to extract parameters from an object using fractal image encoding algorithms. Then, those fractal parameters are used for comparing objects to classify an unknown object. The fractal parameters used in the recognition technique are affine fractal transformations similar to those used for fractal image compression. The main difference is that all objects are considered to be compact subsets of the unit square. It is this assumption which allows the development of a scale invariant recognition technique. The problem of "long encoding time requirement" is removed from the recognition technique by the use of binary images supplied by thresholding algorithms. If a pixel is part of an object in the binary image it has the value 1 otherwise it has the value 0 for each binary image the fractal dimension is computed as function of threshold, and the set of determination is considered as the fractal spectral vector [6].

IV. TEST MATERIALS

The database used for training and testing consists of different fingerprint samples which belong to fifty one persons; and for each person eight fingerprint samples were used. Those samples were downloaded from the standard reference database [7]. The Fingerprint images are a BMP 24 bit/pixels (bit depth), the size of each test image is 504×480 pixels

and 500 dpi as resolution. The use of large amount of data in training phase will improve the probability of getting more precise knowledge about the behaviors of the necessary representation features. This will make the training result more stable. Therefore, the data of each person has been divided into two sets: 6 fingerprints are used as samples which belong to the first set (i.e., training set), and the remaining 2 fingerprints are used as a test set.

V. THE SYSTEM MODEL

The general structure of the proposed fingerprint identification system is shown in Figure (1). It consists of three main stages: preprocessing, Features extraction and (Matching or enrollment). The preprocessing stage consists of the main modules: enhancement, binarization and thinning. The input to the system is a bitmap (BMP) image file; the image data is loaded using Read Fingerprint module, and then it passed into the Enhancement step to produce a processed image that is suitable for recognition task. The enhanced gray is converted to binary image in the binarization step. The binary image subjected to thinning process using Skelton methods. Then, a set of fingerprint attributes are calculated, and finally, the fingerprint features are extracted by calculating the Fractal dimension for those attributes. At matching stage, the calculated moments (including the mean values) of each fractal dimension array either matched with those previously extracted or stored in fingerprint database during the enrollment phase (Fig. 1).
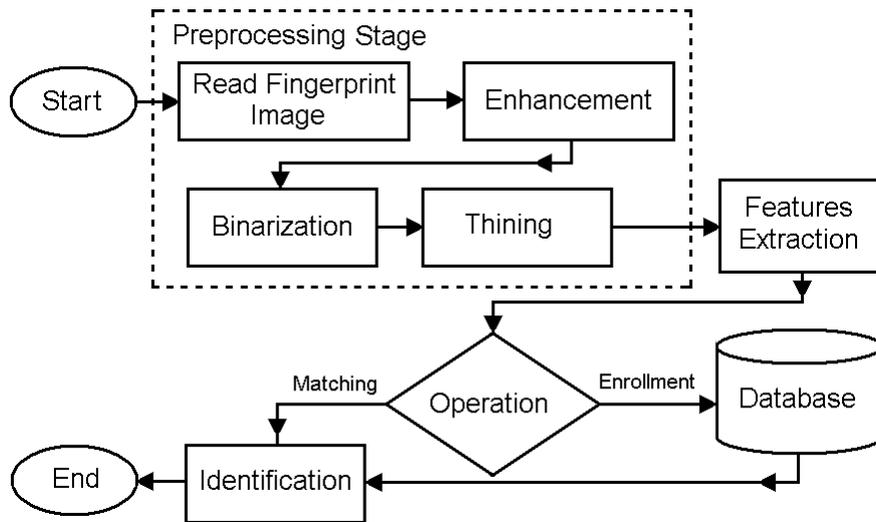

Fig. 1 The System Model

A. Read Fingerprint Image

The fingerprint image input to the established identification is a BMP images file; the color resolution of the image is taken 8 or 24 bit/pixel. The image data (i.e., Red, Green and Blue components) is loaded, and then used to compute the Gray array from the Red (), Green () and Blue () arrays. The Gray image is the output of this stage.

B. Fingerprint Image Enhancement

In this stage, the fingerprint gray image is enhanced using contextual filtering in the Fourier domain [8]. This adopted enhancement method is able to simultaneously yield the local ridge orientation using Fourier analysis. Figure (2) illustrates the main steps of the enhancement method. The enhancement process can be outlined as follows: it consists of two stages. The first stage consists of Fourier analysis and the second stage performs the contextual filtering. The Fourier stage yields the ridge orientation image and the block energy image, the latter which is then used to compute the region mask. The analysis phase simultaneously yields all the intrinsic images that are needed to perform full contextual filtering.
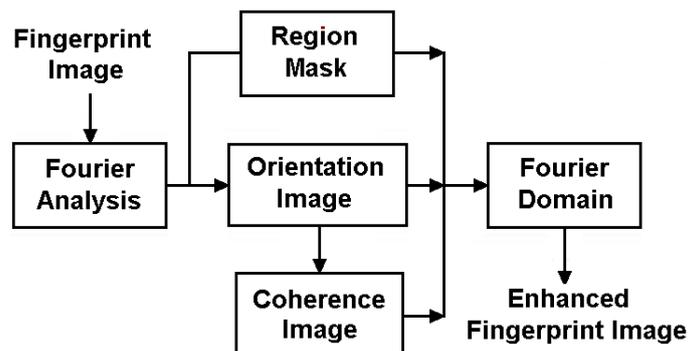

Fig. 2 Overview of the enhancement approach

C. Binarization

The selection of threshold value is either done manually by the user, or it is assessed automatically. In our developed system the proper value of threshold is estimated automatically. In this work, an ad hoc threshold assessment method is developed; it is based on the local characteristic of fingerprint image. It is assumed that the ridges in image usually cover areas which are nearly around (10%) of the whole image area, so the accumulated histogram of image pixel values can be utilized to describe the statistical distribution of image pixels , then a scan from upper bound value (i.e., 255) is started down to lower values, to find out at which gray value "the number of pixel" whose gray values are equal or more than the tested gray value become more than 10%, then this tested gray value is considered as the threshold. Any pixel value is higher than this threshold value is considered as white pixel, while for other pixel value cases another threshold value is used to decide to fill out the black pixels. For the pixels whose gray level is between two threshold values are decided to be either black or white depending on its value relative to the local average value, it is higher than the average decided as white pixels, otherwise it is considered black.

D. Thinning

For thinning purpose, the algorithm called Perfectly Parallel Thinning Algorithm (PPTA) is adopted, it was proposed by Zhang and Wang. It can generate perfect skeletons, which consist of end points, break points, and hole points only. The experimental results showed that PPTA can also preserve image connectivity, produce thinner skeletons, and it is faster than many existing thinning algorithms [9].

E. Features Extraction

In this stage, a set of features based on average of fractal dimension array is extracted. As a first step, the fingerprint attributes arrays for the thin image are computed. In this research, the taken fingerprint attributes are: Density of ridges, Minutia density, and the ridges intersection count along the four directions (all at the same time) and along specific direction. Then, fractal dimensions are computed for these fingerprint attributes. The total determined arrays are seven fractal arrays (named as FDR, FDM, FDI, FDP, FDS, FDV and FDH) as shown in Table I.

TABLE I
DESCRIPTION OF EACH FRACTAL ARRAY

No.	Fractal Array	Description
1	FDR	Fractal Dimension of ridges density
2	FDM	Fractal Dimension of Minutiae Density
3	FDI	Fractal Dimension of ridges Intersection count Density (all directions)
4	FDP	Fractal Dimension of ridges Intersection count along the Primary Diagonal Density
5	FDS	Fractal Dimension of ridges Intersection count along the Secondary Diagonal Density
6	FDV	Fractal Dimension of ridges Intersection count along the middle Vertical Line Density
7	FDH	Fractal Dimension of ridges Intersection count along the middle Horizontal Line Density

At the next step, the fractal dimension of each fingerprint attribute array is partitioned into: (i) 4 equal regions (four quarters), (ii) 2 equal regions partitioned vertically and (iii) 2 equal regions partitioned horizontally. After the partitioning step, the average value of the determined fractal array for each of fifty six blocks (8 blocks × 7 arrays) are determined, they represent the discriminating Features for fingerprint. This set of features is used to make matching with the set of features which had been pre-extracted during the enrollment stage and stored in the database. Figure (3) illustrates the involved features extraction stage starting from the calculation of fingerprint attributes for the input image using different criteria, then passing through the stage of separating each attributes array into 8 arrays and finally determining the features of the fingerprint.
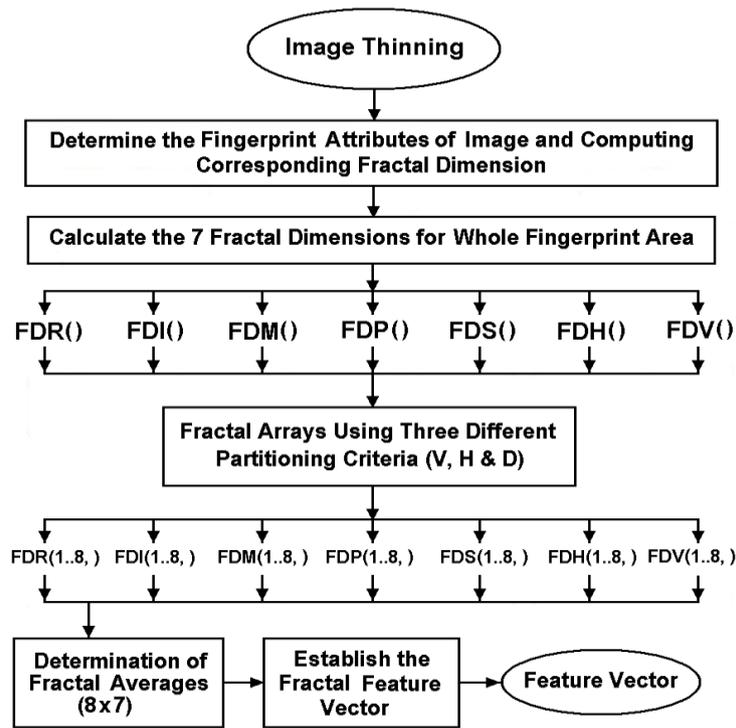
```
                    ╭─────────────────╮
                    │  Image Thinning │
                    ╰─────────────────╯
                             │
        ┌────────────────────────────────────────────┐
        │ Determine the Fingerprint Attributes of     │
        │ Image and Computing Corresponding Fractal    │
        │               Dimension                      │
        └────────────────────────────────────────────┘
                             │
        ┌────────────────────────────────────────────┐
        │ Calculate the 7 Fractal Dimensions for       │
        │         Whole Fingerprint Area               │
        └────────────────────────────────────────────┘
                             │
   FDR()  FDI()  FDM()  FDP()  FDS()  FDH()  FDV()
                             │
        ┌────────────────────────────────────────────┐
        │ Fractal Arrays Using Three Different         │
        │        Partitioning Criteria (V, H & D)      │
        └────────────────────────────────────────────┘
                             │
FDR(1..8, ) FDI(1..8, ) FDM(1..8, ) FDP(1..8, ) FDS(1..8, ) FDH(1..8, ) FDV(1..8, )
                             │
  ┌──────────────────┐   ┌────────────────┐    ╭────────────────╮
  │ Determination of │ → │ Establish the   │ → │ Feature Vector │
  │ Fractal Averages │   │ Fractal Feature │   ╰────────────────╯
  │      (8x7)       │   │     Vector      │
  └──────────────────┘   └────────────────┘
```

Fig. 3 Features Extraction Based on Fractal Dimension

1) Finding Fractal Dimensions: The fractal dimension of the fingerprint attributes are calculated by applying seven different ridges criterion. Each fractal array is constructed using one specific criterion, but the determination procedure for the seven arrays is same. Firstly, an image of size M×N pixels is partitioned to h×w sub regions, where h and w represents the size of extracted fractal array FD. The image is partitioned using overlapping window (LMax×LMax) moves with overlapping distance (Ovrlp) (see Fig. 4). After the partitioning step, there will be h×w boxes each has (LMax×LMax) pixel size, where h=(M×Ovrlp)/LMax and w= (N×Ovrlp)/LMax.
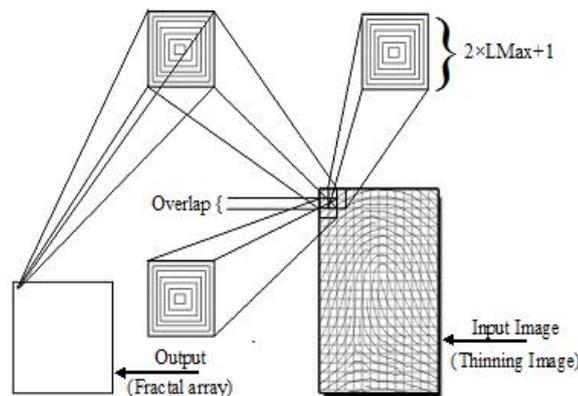
Fig. 4 Image Partitioned into overlapping boxes to compute fractal value

For each box (or sub region), the fractal dimension of its points is determined using Box Counting Method (BCM). According to this method the number (NL) of point q which belongs to a window (2L+1)×(2L+1) centered around the tested pixel (p) and satisfy the condition ($|q-p|\leq L$) are determined. The number of points (NL) satisfy the condition is determined for different values of (L) (i.e., L=1, 2,…, Lmax). Finally, the fractal dimension at pixel (p) is determined using the following equation:

$$FD = \frac{\sum_{L=1}^{L_{max}} log(N(L))\, log(2L+1)^2}{\sum_{L=1}^{L_{max}} log(2L+1)^4} \qquad ,\dots\dots\dots(1)$$

Where FD represents the fractal dimension value at (x, y) pixel of the tested box, where x = 1, 2, … , w and y = 1, 2, …, h . The determined value of FD for all pixels belong to the box are registered in array, to be processes, in the next stage to get the fractal based discriminating attributes.

2) Separation and Averaging: After computing the Fractal dimension arrays for different boxes of fingerprint attributes arrays then each fractal array is partitioned into 8 sub-arrays using three partitioning mechanisms (see figure 5):

- Partition the image horizontally into two halves (i.e., 2 sub-arrays).
- Partition the image vertically into two halves (i.e., 2 sub-arrays).
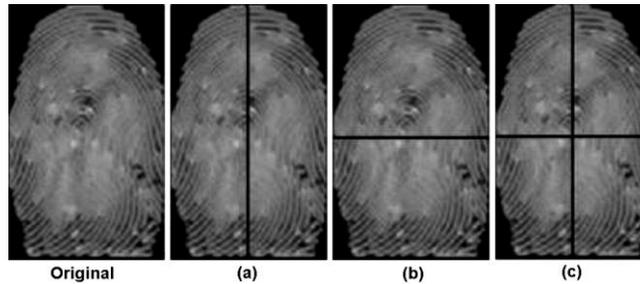- Partition the image into four quarters (i.e., 4 sub-arrays).

Fig. 5 (Original) Fractal array , (a) two equal vertical regions, (b) two equal horizontal regions, and (c) four equal regions (quarters)

Then, the average of each sub-array (region) is computed using the following equation:

$$Feat(N)=\frac{\sum_{y=0}^{H}\sum_{x=0}^{W}FD(x,y,n)}{H_R \times W_R} \quad ,..............(2)$$

Where N =1, 2, …, 56 is the features number, (H_R and W_R are height and width of each region). The set of fifty six feature is consist of:

- From the two horizontal partitions there will be 14 (i.e., 2x7) extracted feature.
- From the two vertical partitions there will be 14 (i.e., 2x7) extracted feature.
- From the four quadrants there will be 28 (i.e., 4x7) extracted feature.

Then, the fifty six determined FD feature will be analyzed to find out the best discriminating features for the tested fingerprint.

F. Features Analysis

A training set of fingerprint samples is used to train the classifier and to address the feature list. While, the test set is used to assess the recognition accuracy of the system (after the training phase). To get a robust recognition performance, there is a need to find out the list of features which shows little intra-class variability. In this work, a set of features which can represent the spatial distribution of minutia density, ridges density and their intersection along different directions is adopted. The selection of those attributes is due to their inter-class stability. Through the training phase, a subset consists of 36 features were selected from the overall set of features (i.e., 56 Features) and this selection was due to the comprehensive tests which were conducted on the training set of samples to find out the best set of features that can be used to yield best matching score.

G. Matching

A fingerprint matching module computes the match score (or in other words, the similarity degree) between the features vectors extracted from two different fingerprints. The similarity score should be high for fingerprints which belong to the same finger and low for those belong to different fingers. Fingerprint matching is a difficult pattern recognition task due to large intra-class variations (i.e., variations in fingerprint images for the same finger) and large inter-class similarity (i.e., similarity between fingerprint images from different fingers). In our project, the fifty six features which have been extracted in previous stage, have been used either to match the tested fingerprints data previously stored in database or stored in database (during the enrollment phase).

To perform matching, the features of the fingerprint samples belong to training set are used to yield the template mean feature vector for each person. The determined mean feature vector ($\overline{F}$) of each person, and the corresponding standard division vector (σ^2) are saved in a database in enrollment phase. While in matching (or identification) phase they loaded from the database, and then their similarity degrees are computed with the feature vector extracted from the tested fingerprint. using the following criteria:

$$\overline{F}(p,f)=\frac{1}{S}\sum_{i=1}^{S}Feat(p,f,i) \quad ,............................(3)$$

$$\sigma^2(p,f)=\sqrt{\frac{1}{S}\sum_{i=1}^{S}\left(Feat(p,f,i)-\overline{F}(p,f)\right)^2} \quad ,......(4)$$

$$A_\sigma(f) = \frac{1}{P}\sum_{p=1}^{P}\sigma^2(p,f) \quad ,.................................(5)$$

$$\sigma^2_{A\sigma}(f) = \sqrt{\frac{1}{P}\sum_{p=1}^{P}\left(\sigma^2(p,f) - A_\sigma(f)\right)^2} \quad ,...........(6)$$

Where p, f, s are the person number, feature number and sample number, respectively; and P,F,S are the total numbers of person, features, taken samples, respectively.

The difference, Dif(f), value for the tested feature (f) is computed as the absolutes difference of the feature value (determined from the tested fingerprint) and the corresponding feature mean value (determined for each person) divided by overall standard division:

$$Dif(f) = \left|Feat_{test}(f) - \overline{F}(p,f)\right| / \sigma^2_{A\sigma}(f) \quad ,.....(7)$$

The conducted tests for evaluating the discriminating capability of the proposed feature have led to select only 36 of these features (as will illustrated in the next section). Then, the sum (sDif) of all Dif(f), for the selected 36 features, will be considered as the distance between the feature vector of the tested fingerprint and the template feature vector of each person.

$$sDif = \sum_{f=1}^{36}Dif(f) \quad ,..(8)$$

The tested fingerprint will assigned the identification number of the person whose template feature vector led to smallest sum (sDif).

VI. THE EFFECTIVENESS OF FINGERPRINT ATTRIBUTES

Different sets of tests have been conducted to find out the proper values for proposed system parameters which lead to best recognition rate. The window size was taken 15 (i.e., *Lmax=7*) and the *overlap* depth is taken *8*. Figure (6) shows the identification rate when one feature is used for identification decision. Figure (6a)) is the results when the training set is used, while figure (6(b)) is for the test set.

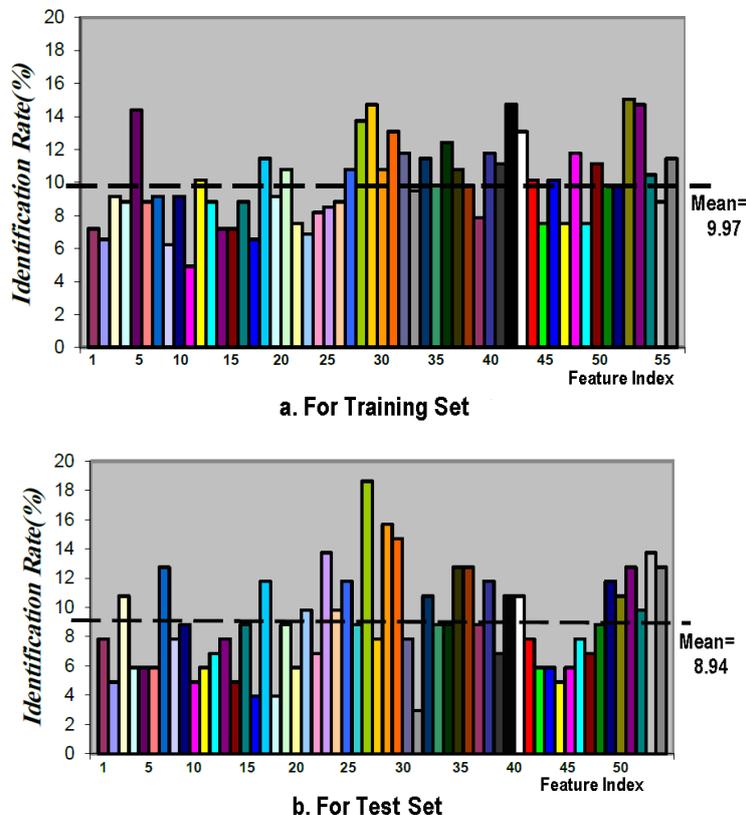a. For Training Set

b. For Test Set

Fig. 6 The attained identification rate for the case of using one feature for identification decision

Figure (7) shows the identification rate for the best 20 combinations of the two features used in the distance criteria. The upper bar chart is for training set, while the lower chart is for the test set.
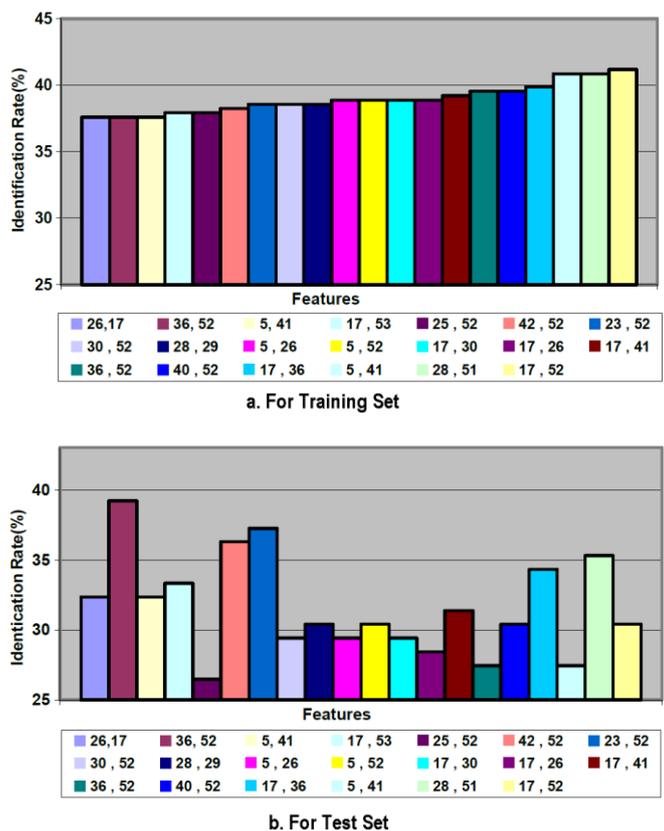
a. For Training Set

b. For Test Set

Fig. 7 The highest 20 attained identification when combination of two features is used for identification

Figure (8) shows the identification rate for the best combinations of three features. The result in those figures show that the combination of features (41, 47, 53) leads to the highest identification value (65.359%). Therefore, those features will be always adopted when other features are added to the combination in order to get better identification rate.
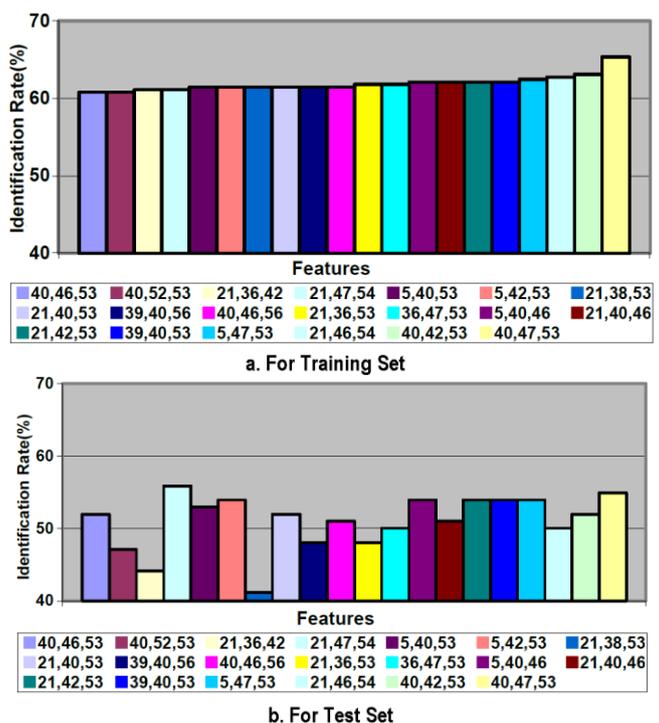

a. For Training Set

b. For Test Set

Fig. 8 The highest attained identification rate when combination of three features are used

Figure (9) shows the best attained identification rate for the best 20 combinations of six features. This figure shows that the features (5, 13, 54), beside to the set of features (41, 47, 53), led to the highest identification value (85.95). The addition of a set of triple features is repeated till no improvement is occurred in the identification rate.
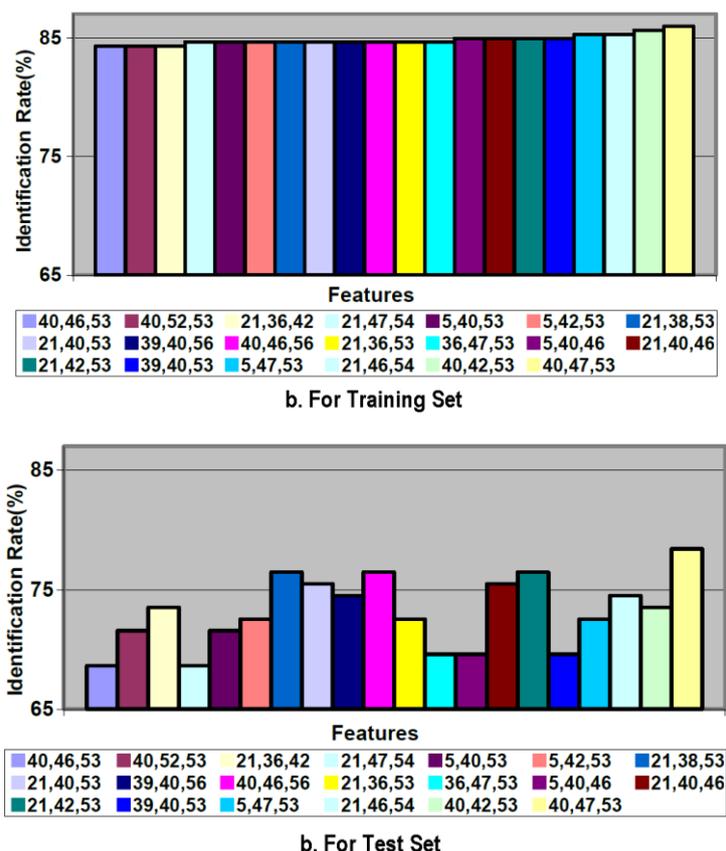
b. For Training Set

b. For Test Set

Fig. 9 The highest 20 attained identification rates due to the use of combinations of six features,
three new features added to previous features (41, 47, 53)

Table II describes the selected features which provide the highest recognition rate, at each features addition round, and the identification rate. At each round a set of three features is increased. Finally, after 19 rounds the highest identification rate was attained, no improvement was occurred in the next rounds. During the repeated additions some of the features were repeated many times. The final highest identification rate is (95%) for the training set, and the corresponding identification rate for the test set, using same set of features, was (92%).

TABLE II
THE FEATURES SET ADDED DURING EACH ROUND DURING TRAINING PHASE

Round	Selected Features	Recognition Rate (%)
3	39, 46, 49	87.908
4	1, 10, 43	90.196
5	14, 21, 42	91.176
6	9, 32, 51	91.83
7	36, 37, 54	92.484
8	9, 13, 56	92.81
9	1, 10, 47	92.127
10	17, 52, 53	92.81
11	5, 16, 34	93.137
12	23, 41, 42	92.484
13	5, 35, 36	93.137
14	12, 15, 50	93.137
15	9, 11, 48	93.791
16	4, 8, 39	93.791
17	11,15,26	94.118
18	1, 5, 40	94.771
19	5, 13, 42	95.098

Table III shows the number of repetition of the 36 features added to the matching criteria during the 19 rounds.

TABLE III
THE NUMBER OF REPETITION OF EACH FEATURE SELECTED THROUGH THE 19 ROUND

No.	Feature Name	Repeated Times	No.	Feature Name	Repeated Times
1	F1	3	19	F35	1
2	F4	1	20	F36	2
3	F5	5	21	F37	1
4	F8	1	22	F39	2
5	F9	3	23	F40	2
6	F10	2	24	F41	1
7	F11	2	25	F42	3
8	F12	1	26	F43	1
9	F13	3	27	F46	1
10	F14	1	28	F47	2
11	F15	2	29	F48	1
12	F16	1	30	F49	1
13	F17	1	31	F50	1
14	F21	1	32	F51	1
15	F23	1	33	F52	1
16	F26	1	34	F53	2
17	F32	1	35	F54	2
18	F34	1	36	F56	1

Table IV describes the time consumed at each stage of the developed identification system. The table shows that the enhancement stage spends the longest time with respect to other stages. The required time to identify each fingerprint stores in the database is very small (i.e., 0.016 second).

TABLE IV
SHOWS THE MEAN OF TIME CONSUMING AT EACH STAGE

No.	Stages	Consumed Time (in second)
1	Read image	0.058
2	Enhancement	12.92
3	Binarization	0.486
4	Thinning	0.364
5	Computing Fractal arrays and finding Averages of them	0.678
6	Identify Fingerprint	0.0156
Total Time		14.515

VII. CONCLUSIONS

A novel approach based on fractal dimension as a feature for recognizing the fingerprint is presented in this paper. The fingerprint area is partitioned into an array of overlapped blocks; then the average values of fractal dimension for seven different types of ridges attributes are computed and used as fingerprint discriminating features. The test results indicated that the proposed method is promising and can be further developed to be more accurate and robust. Also, the results indicated there is need to find out a faster method for the enhancement stage. The developed system has been established using Visual Basic programming language, and the tests have been conducted under the environment: Microsoft Window XP Professional operating system, Laptop computer (Processor: mobile Intel Celeron processor 540, 1.86 GHz, 533 MHz, 1 MB L2 cache, and Memory: 1GB).

REFERENCES
[1] K. Jain, P. Flynn, and A. A. Ross, Handbook of Biometrics, Springer-Verlag, 2008.
[2] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar (Eds.), Handbook of Fingerprint Recognition, second edition, Springer-Verlag, 2009.
[3] Bovill, Fractal Geometry as Design Aid, Journal for Geometry and Graphics , vol. 4, no. 1, pp. 71-78, 2000.
[4] S. Sukumaran, and M. Punithavalli, Retina Recognition Based on Fractal Dimension, IJCSNS International Journal of Computer Science and Network Security, vol.9 no.10, October 2009.

[5]   H. E. Komleh, Fractal Techniques for Face Recognition, PhD Thesis, Queensland University of Technology, August 2004.

[6]   G. Neil and K. M. Curtis, Scale and rotationally invariant object recognition using fractal transformations, Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP96, vol. 6, pp. 3458-3461, 1996.

[7]   NEURO technology, Biometric and Artificial Intelligence Technologies www.neurotechnology.com/download/CrossMatch_Sample_DB.zip.

[8]   S. S. Chikkerur, Online Fingerprint Verification System, Msc. Thesis, State University of New York at Buffalo, June 2005.

[9]   Y. Y. Zhang and P. S. P. Wang, A new parallel thinning methodology. Internat. J. Pattern Recognition Artif. Intell., vol. 8, no. 4, pp. 999-1010, 1994.