Asian Journal of Computer and Information Systems (ISSN: 2321 – 5658)
Volume 01– Issue 03, October 2013

Effectiveness of Extended Invariant Moments in Fingerprint Analysis

Hussein Attya Lafta[1], Safa Saad Abbas[2]

[1]Assistant Prof. Phd in Computer Science
Babel, Iraq

[2] Assist. Lec
Babel,Iraq

ABSTRACT— ***Automatic fingerprint identification system includes person identification process based on fingerprint which is in digital form. Fingerprint identification system consists of acquiring fingerprint module, classification module, and the matching module, which it performs a comparison between the unknown input fingerprint and the others stored in the fingerprint database and related to the class labeled by the classification module. In this paper, extended are used in fingerprint analyzing process for extracting local features. In extraction local features, extended moments gave best results than when using centralized invariant moments with order 3. for decision making in identification, K_NN classifier used in this work.***

Keywords— Biometrics, Pattern Recognition, invariant moments, Fingerprint, Authentication, Identification, K_NN.

1. INTRODUCTION

One major application of pattern recognition systems is the person identification. With the exponential growth in technology and business carried worldwide, it is becoming crucial to build automated systems that identify people. Personal identification, which refers to identifying an individual based on his or her physiological or behavioral characteristics, has the capability to reliably distinguish between an authorized person and an impostor. The person identification which based on fingerprint is the technology that uses image processing and pattern recognition. The need for personal authentication increases in the current world in all fields of technology where many people are turning to biometric authentication as an alternative to traditional identification techniques [16][10]**.** Traditional knowledge-based identification, (Password or Personal Identification Number (PIN)), and token-based, (identity smart card), are exposed to imposture because PINs may be forgotten or guessed and the tokens may be lost or stolen. The process of automatically associating an identity with an individual by means of some personal characteristic is called biometric recognition. Among all the biometrics (face, fingerprint hand geometry, iris, signature, voice, etc.) [7][24], fingerprint based authentication is one of the most proven techniques. Fingerprint is used in the identification of individuals because of the well-known fact that each person has a unique fingerprint, and it is not changed during the people's life [9][19].

A fingerprint is the pattern of ridges and valleys on the surface of the finger. The uniqueness of fingerprints can be determined by the overall patterns of ridges and valleys, as well as the local ridge anomalies (ridge bifurcation or ridge ending) [10]. There are two main features in the fingerprint image. The first type is the overall ridge flow information which is defined by the pattern of the ridges and valleys in the fingerprint. This type of information describes the global pattern of the fingerprint and can be utilized for the classification of the fingerprint database into classes at the global pattern level. The second type of information is represented by many local points of discontinuities in the ridges and valleys, which are usually referred to as minutiae. Fingerprints are unique in their information content in that the combination of the local and global information forms a topological minutiae map represented by the minutiae, their relative relationships, and their relationship to points of global singularities of the pattern classes [8][4].

2. RELATED WORKS

In June 1998, Wahab, Chin, and Tan used minutiae extraction method for extracting ridge ending and bifurcation based on computing crossing number value. In matching stage, the structural model of the local features was used, for each extracted feature; a neighborhood of some specified radius about the centre feature was defined. NeXT, five nearest features to the central feature within the radius were selected as the neighborhood features for matching. The concept of matching by correlation was used in two stages; local features used in first stage and global features used in second stage [25]. In 2001, Simon, Garcia, Llanas, and Rodriguez proposed a method for minutiae extraction which used improving alternatives for the image enhancement process in order to introduce a complete minutiae extraction for automatic fingerprint recognition systems. At first, image normalization and orientation field were calculated. A spatial low-pass filter was applied to the estimated oriented field to correctly realign all the segments, this filter mask was 5x5 pixels. Then converting an image to a binary and applying thinning process in order to reduce the width of the ridges to a single pixel to simplify the subsequent structural analysis of the image for the minutiae extraction. For evaluating reliability, Goodness Index (GI) of the extracted minutiae was used; a high value of GI indicates a high reliability degree of the extraction process [22]. In 2004, Afsar, Arif, and Hussain introduced research that was presented the implementation of a minutiae based approach to fingerprint identification and verification. This technique was based on the extraction of true minutiae (location coordinates and orientation) by using three level-filtering processes in order to filter false minutiae. The minutiae type was not used during the matching process. A minutia matching was carried out firstly by registering the minutiae sets followed by spatial and orientation-based distance computation. IN order to enhance the performance of matching algorithm, fingerprint classification for indexing during fingerprint matching was used, it is based on extraction of the singular points, and then, performing a rule-based classification [2]. In 2005, Al-Kharaz presented a method for fingerprints recognition by using quantitative measures associated with oriented texture, as features. This schema combines both global and local information of a fingerprint. It yields a relatively short, fixed length code (called Finger Code) which is suitable for matching as well as storage on a smart card). Gabor filter banks with eight directions, (0, 22.5, 45, 67.5, 90, 112.5, 135, 157.5), were used for this purpose, to capture useful information. In matching phase, the Euclidean distance between the Finger Codes, was used [3]. In May 2010, Thai and Tam proposed a fingerprint-matching approach, which was based on standardized fingerprint model to synthesize fingerprint from original templates in order to improve matching score. From these templates of finger in the database, choosing one as mean image and use Genetic Algorithms to find the transformation among them. Then, these transformations are used to synthesize fingerprint (add ridge lines and minutiae from original template to mean fingerprint). Finally, performing matching between mean fingerprint and other templates in database [23]. In this paper, extended moment invariant technique used for recognition process, and K_NN classifier used for making the decision of fingerprint identification.

3. BIOMAETRICS

Biometric, which refers to identification based on physical or behavioral characteristics, is more reliable and more capable than traditional knowledge-based and token-based techniques. It is the most secure and convenient identification tool because it can't be borrowed, stolen, or forgotten. Common physical biometrics include: fingerprint, hand or palm geometry, retina, iris, and facial characteristics. Behavioral characters include: signature, voice, and gait [20][18]. Figure (1) shows biometrics types.

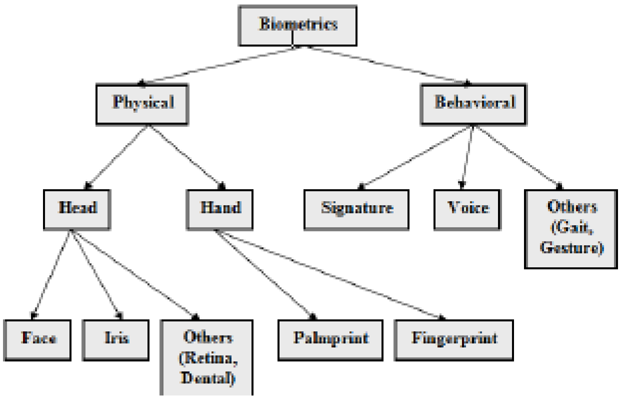


Figure 1: Types of Biometrics.

Fingerprint is one of the biometrics which can be systematically used to make personal identifications. A fingerprint pattern is described by the epidermis ridges and valleys, that it does not change and is relatively easy to capture. In this paper, such biometric (i.e. fingerprint) is dependent. Fingerprints are considered unique for each person, i.e., there are no two persons with identical fingerprints, even if the two persons are twins. Another advantage is that fingerprints are unalterable since the fetus is formed until the death [19]. A behavioral or physiological characteristic is a biometric if it holds the following properties [16][19]:

- *Universality*: It can be found in all people except hand cut people.
- *Uniqueness*: It is unique from person to person.
- *Permanence*: It does not change over the time, during the live unless the hand cut.

• *Collectability*: It is possible to capture it quantitatively.
• *Performance*: The biometric allows distinguishing the persons with high degree of accuracy.
• *Acceptability*: The biometric must be accepted by the users.

• *Circumvention*: The violability degree of the system must be very low.

3.1. Identification and Verification

A biometric system is essentially a pattern recognition system that acquires biometric data from an individual, extracts a salient feature set from the data, compares this feature set against the feature set(s) stored in the database, and executes an action based on the result of the comparison. Therefore, a generic biometric system can be viewed as having four main modules: a sensor module, a feature extraction module, a matching module, and a database module [9]. One of the most important and often overlooked processes of any biometric system is the enrollment or registration process. This is where the biometric feature is captured and coupled with other personal information. It is crucial to make sure that the person who is going to be enrolled/registered, is the person he claims to be. Once the biometric feature is coupled with other personal information, the identity is now accessed via this biometric feature [17][10].

A biometric system can be operated in one of two modes: verification mode or identification mode. In the ***verification mode,*** a biometric system either accepts or rejects a user's claimed identity. The biometric comparison will attempt to match the individual's biometric data to that of the stored information being claimed against. This is referred to as a *one-to-one matching*. The result from this matching is a simply yes or no: Yes, which means that the individual's claim is verified, or no, which means that the claim cannot be verified. If the claim cannot be verified, no more results are provided to further narrow down the claim. A biometric system operating in the ***identification mode*** establishes the identity of the user without a claimed identity. A biometric comparison attempts to match an individual's biometric data against all the biometric data on file. This is what is referred to as *one-to-many matching* [17], as shown in Figure 2.

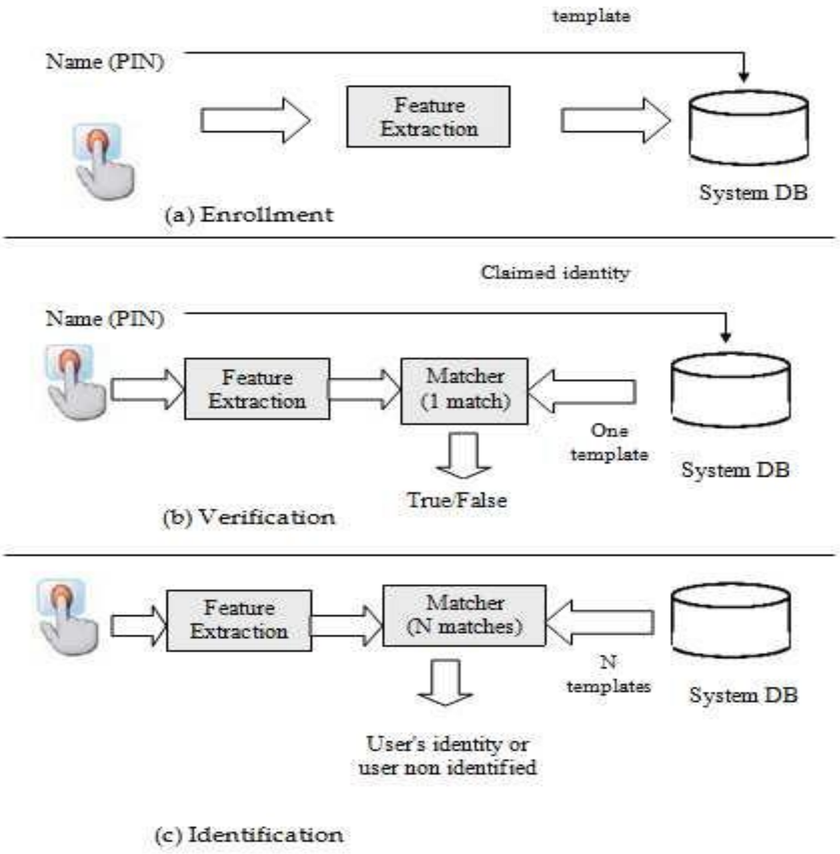


Figure (2): Block Diagrams of (a) Enrollment, (b) Verification and (c) Identification tasks.

3.2. Fingerprint Analysis

Fingerprint is the pattern of ridges and valleys on the surface of a fingertip used for personal identification, as shown in Figure 3. There are two main types of features in fingerprints [11][12]:
- global ridge and furrow structures which form a special pattern in the central region of the fingerprints.
- minutiae details associated with local ridges and furrows.

A fingerprint is typically classified, based on the first type of features only, and identified, based on the second type of features. The minutiae-based representation is the most popular representation of fingerprints.

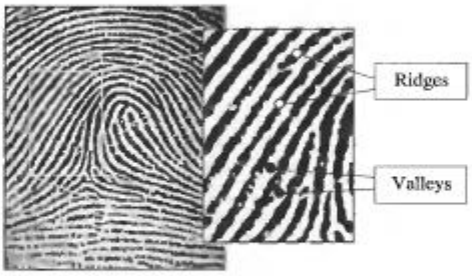


Figure 3: Ridges and Valleys on a Fingerprint Image.

The fingerprint minutiae ridge ending and ridge bifurcation are shown in more detail in Figure 4, a *ridge ending* occurs when a ridgeline comes to an end, and no ridge ending with the same orientation is adjacent to it. A *ridge bifurcation* occurs when a ridgeline comes to a branch point, that is, where it splits into two ridgelines. A ridge bifurcation can be viewed as a valley ending. Similarly, a ridge ending can be viewed as a valley bifurcation. These minutiae have a pattern that is unique for each fingerprint [12][14].

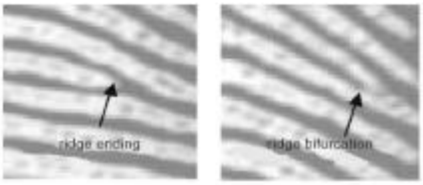


Figure 4: Ridge Ending and Ridge Bifurcation.

Minutiae Feature Extraction (consists mainly of three stages: orientation field estimation, ridge extraction, and minutiae extraction) finds the ridge endings and ridge bifurcations from the input fingerprint images. It is imperfect and introduces measurement errors, and the automatic extraction of representations based on an explicit detection of complete ridge structures in the fingerprint is difficult [6]. The smooth flow pattern of ridges and valleys in a fingerprint can be viewed as an oriented texture field, whereas the image intensity surface in fingerprint images is comprised of ridges whose directions vary continuously, and it constitutes an oriented texture [17]. Therefore, fingerprints can be represented/matched by using quantitative measures associated with the flow pattern (oriented texture) as features.

4. MOMENT INVARIANT

One of the most important object recognition methods is the moment method which was introduced by Hu. Moments are actually often associated more with statistical pattern recognition, and they are examples of derived features. This method is used to identify object from 2D image, these moments are descriptors. The operations such as rotation, translation, scaling, and reflection may exist in images; these are also called transformations, that cause changes for each order of image moments. The solutions were introduced to keep the moments constant or invariants, which are called *moment invariants* [5][15]. The idea behind moment invariants is to use region-based geometric moments. Moment invariants are image statistics that are independent of transformation. They are uniquely determined by an image and, conversely, uniquely determine the image (modulus rotation, translation, and scale). These properties of moment invariants facilitate pattern recognition in the visual field that is independent of size, position, and orientation. The two-dimensional moment is actually associated with an order that starts from low (where the lowest is zero) up to higher orders. The moments invariants are derived from the definitions of moments, centralized moments, and normalized central moments. These statistics are defined as follows [13][21]:

Let *f* be a two dimensional continuous function, The moment of order (*p*,*q*) of *f* is defined as:

$$m_{pq} = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} x^p y^q f(x,y)dxdy \qquad \text{for } p,\ q{=}0,\ 1,\ 2,\ \ldots. \qquad \ldots\ldots\ldots\ldots(1)$$

For discrete image with size *N***M*, equation 3.20 is usually approximated by:

$$m_{pq} = \sum_{x=0}^{N-1}\sum_{y=0}^{M-1} x^p y^q f(x,y) \qquad ....\ (2)$$

The zero-order moment, *m*00 , represents the total mass of a function *f*. The central moments [1] are expressed as:

$$\mu_{pq} = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} (x - x_c)^p (y - y_c)^q f(x,y)dxdy \quad \text{for } p,\ q=0,\ 1,\ 2,\ .... \qquad ....\ (3)$$

$$\text{Where} \qquad x_c = \frac{m_{10}}{m_{00}} \quad \text{and} \quad y_c = \frac{m_{01}}{m_{00}} \qquad ....\ (4)$$

If *f*(x, y) is a digital image, then equation 3 becomes:

$$\mu_{pq} = \sum_{x=0}^{N-1}\sum_{y=0}^{M-1} (x - x_c)^p (y - y_c)^q f(x,y) \qquad ....\ (5)$$

The point (*x*$_c$, *yc*) is the center of the region or object, which is called the image centroid. The centralized moments of order up to 3 are:

$$\mu_{00} = m_{00} \qquad \mu_{02} = m_{02} - y_c m_{01}$$
$$\mu_{10} = 0 \qquad \mu_{30} = m_{30} - 3x_c m_{20} + 2m_{10}x_c^2$$
$$\mu_{01} = 0 \qquad \mu_{03} = m_{03} - 3y_c m_{02} + 2m_{01}y_c^2$$

$$\mu_{11} = m_{11} - y_c m_{10} \qquad \mu_{12} = m_{12} - 2y_c m_{11} - x_c m_{02} + 2y_c^2 m_{10} \quad \mu_{20} = m_{20} - x_c m_{10}$$
$$\mu_{21} = m_{21} - 2x_c m_{11} - y_c m_{20} + 2x_c^2 m_{01}$$

However, centralized moments are only *translation* invariant. In order to accrue invariance to scale [15], we require *normalized central moments*, hpq , which defined as:

$$\eta_{pq} = \frac{\mu_{pq}}{\mu_{00}^{\alpha}} \qquad ....(6)$$

$$\text{Where} \qquad \alpha = \frac{p+q}{2} + 1 \qquad \text{For } p+q \geq 2. \qquad ....(7)$$

From the second-order and third-order moments, a set of seven transformation invariant moments can be derived [1], as follows:

$$\phi_1 = \eta_{20} + \eta_{02} \qquad ....(8.1)$$

$$\phi_2 = (\eta_{20} - \eta_{02})^2 + 4\eta_{11}^2 \qquad ....(8.2)$$

$$\phi_3 = (\eta_{30} - 3\eta_{12})^2 + (3\eta_{21} - \eta_{03})^2 \qquad ......(8.3)$$

$$\phi_4 = (\eta_{30} - \eta_{12})^2 + (\eta_{21} - \eta_{03})^2 \qquad ....(8.4)$$

$$\phi_5 = (\eta_{30} - 3\eta_{12})(\eta_{30} + \eta_{12})[(\eta_{30} + \eta_{12})^2 - 3(\eta_{21} + \eta_{03})^2]$$
$$+ (3\eta_{21} - \eta_{03})(\eta_{21} + \eta_{03})[3(\eta_{30} + \eta_{12})^2 - (\eta_{21} + \eta_{03})^2] \qquad ....(8.5)$$

$$\phi_6 = (\eta_{20} - \eta_{02})[(\eta_{30} + \eta_{12})^2 - (\eta_{21} + \eta_{03})^2]$$
$$+ 4\eta_{11}(\eta_{30} + \eta_{12})(\eta_{21} + \eta_{03}) \qquad ....(8.6)$$

$$\phi_7 = (3\eta_{21} - \eta_{30})(\eta_{30} + \eta_{12})[(\eta_{30} + \eta_{12})^2 - 3(\eta_{21} + \eta_{03})^2]$$
$$+ (3\eta_{12} - \eta_{30})(\eta_{21} + \eta_{03})[3(\eta_{30} + \eta_{12})^2 - (\eta_{21} + \eta_{03})^2] \qquad ....(8.7)$$

This set of normalized central moments is independent of translation, rotation, and scale changes in an image. The first of these, f1 and f2 , are second-order moments, those for which *p* + *q* = 2. Those remaining are third-order moments, since *p* + *q* = 3.

5. PROPOSED SYSTEM

The block diagram of the proposed system of fingerprint classification and identification is shown in figure 5.

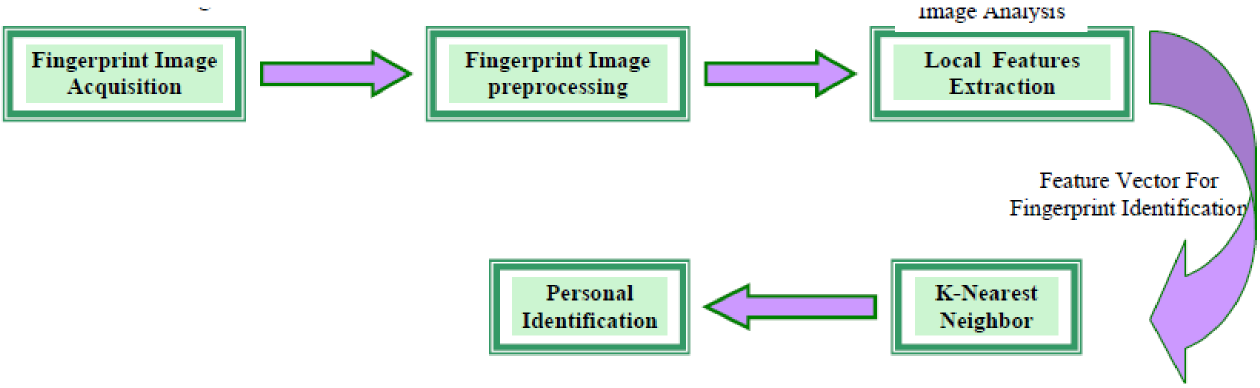


Image Analysis
Fingerprint Image Acquisition
Fingerprint Image preprocessing
Local Features Extraction
Feature Vector For Fingerprint Identification
K-Nearest Neighbor
Personal Identification

Figure 5: The Block Diagram of the Proposed System.

This block diagram states all the steps of the practical stages that are required for designing the proposed system. Its essential parts are:
1- Personal fingerprint images database.
2- Fingerprint characteristics files.
3- Enrollment module.
4- Identification module.

5.1 Fingerprint Image Acquisition

Obtained fingerprint can either be inked or live scan, if it is inked, a scanned image is obtained by blotting ink on the fingertip and making an inked print on a paper, and then scanning this paper to become in digital form. This scheme usually produces images with very poor quality because of the non-uniform ink distribution. In live scan fingerprint image acquisition, optical fingerprint scanners such as URU4000, Cross Match Verifire300, etc. are used. In this paper, a database of fingerprint images which were obtained using Cross Match Verifier300 optical scanner with resolution 500 dpi, which is suitable to extract necessary information.

5.2 Fingerprint Image Preprocessing

Fingerprint images which are captured by the scanner, contain two regions, the ROI (region of interest) and the background. The ROI is the contacted area of scanner side with a fingerprint skin while the remaining area is called background. The ROI involves necessary information for fingerprint recognition, while the background does not have any benefit data. Therefore, in order to study the fingerprint image, ROI (foreground) will be separated from the image background. This preprocessing stage can be defined as cropping, which will be happened by performing required steps to specify the fingerprint area from the scanned image. To perform cropping correctly, the reference point (core point) might be detected, and then a region centered in detected reference point is cropped. The cropped region contains sufficient information to represent the fingerprint. The algorithm of cropping is:

Algorithm (1) : Image Preprocessing.

```
-----------------------------------------------
Input: Fingerprint Image (foreground and background).
Output: Region of Interest (ROI).
Begin
Step1: Select required size of ROI, said w.
Step2: Determine the position of reference point.
Step3: Crop ROI with w x w square shape from the entire fingerprint image.
Step4: Store the cropped ROI, and use it as input to the proposed system.
End
```

Figure 6 shows the cropping process, where the scanned fingerprint image in (a), and the cropped image that has been studied in (b).

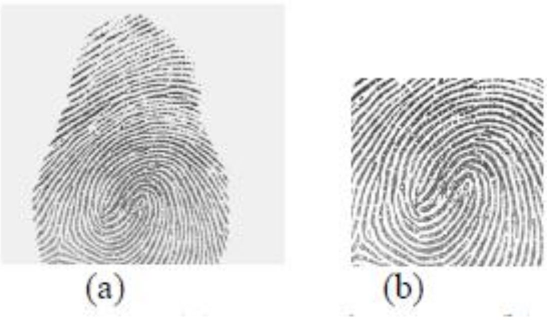
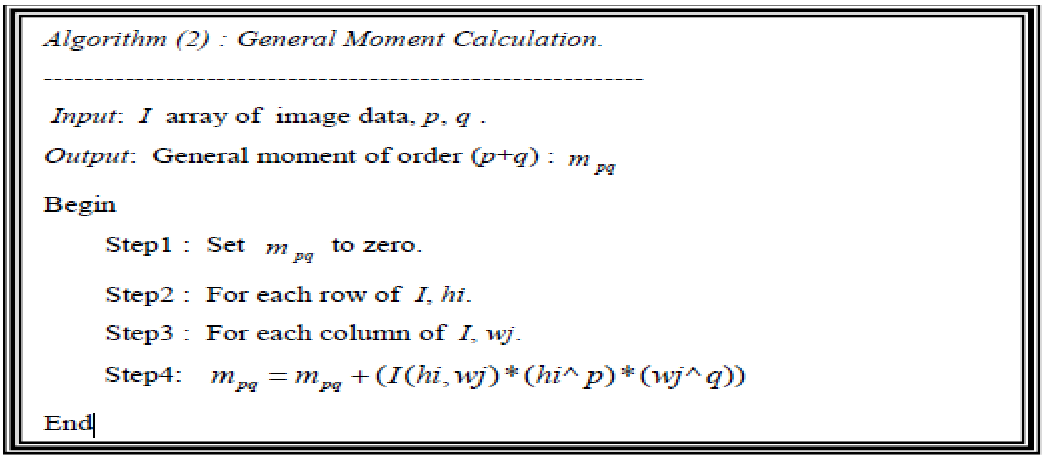


Figure 6: Cropping Process. (a) Scanned Image. (b) ROI of Fingerprint.

5.3 Local Features Extraction

Local features are extracted using central moments invariant that are invariant to transformations. In this paper, central invariant moments up to order 4, where 12 central moments are used in features extraction to recognize the fingerprint image (7 features and 5 extended features). The following algorithm indicates computation of each general moment.



```
Algorithm (2) : General Moment Calculation.
-----------------------------------------------------------
Input: $I$ array of image data, $p$, $q$ .
Output: General moment of order $(p+q)$ : $m_{pq}$
Begin
    Step1 : Set $m_{pq}$ to zero.
    Step2 : For each row of $I$, $hi$.
    Step3 : For each column of $I$, $wj$.
    Step4: $m_{pq} = m_{pq} + (I(hi, wj) * (hi \wedge p) * (wj \wedge q))$
End
```

Using this algorithm, the general moments that are computed are

$m_{00}, m_{01}, m_{10}, m_{11}, m_{02}, m_{20}, m_{03}, m_{30}, m_{12}, m_{21}, m_{04}, m_{40}, m_{13}, m_{31}, m_{22}$.

The normalized geometrical central moments up to the order 4, seven moment invariants (ϕ1- ϕ7) and five extended moments (ϕ8 - ϕ12). After computing extended central moments, they are normalized and a set of five extended transformation invariant moments can be derived, as follows:

$$\phi_8 = \eta_{40} + \eta_{22} + \eta_{02} \qquad \text{.........(9.1)}$$

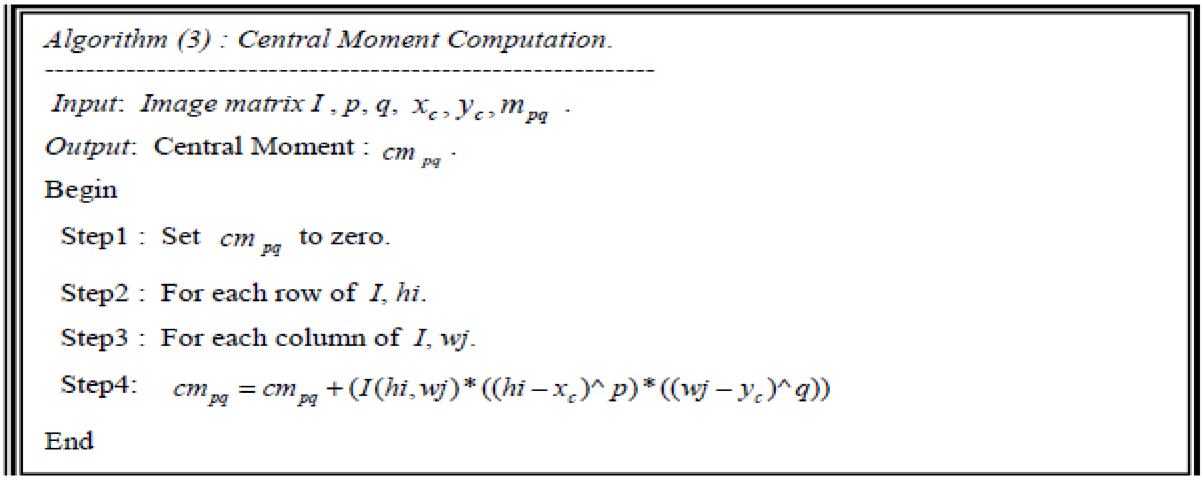
$$\phi_9 = (\eta_{40} - \eta_{04})^2 + 4(\eta_{31} - \eta_{13})^2 \qquad \text{............(9.2)}$$

$$\phi_{10} = (\eta_{40} - 6\eta_{22} + \eta_{04})^2 + 16(\eta_{31} - \eta_{13})^2 \qquad \text{............(9.3)}$$

$$\phi_{11} = (\eta_{40} - 6\eta_{22} + \eta_{04})^2[(\eta_{40} - \eta_{04})^2 + 4(\eta_{31} - \eta_{13})^2] + 16(\eta_{40} - \eta_{04}) + (\eta_{31} + \eta_{13})(\eta_{31} - \eta_{13}) \qquad \text{...........(9.4)}$$

$$\phi_{12} = (\eta_{40} - 6\eta_{22} + \eta_{04})^2[(\eta_{40} - \eta_{04})^2 + 4(\eta_{31} - \eta_{13})^2] - 16(\eta_{40} - \eta_{04}) + (\eta_{31} + \eta_{13})(\eta_{31} - \eta_{13}) \qquad \text{.........(9.5)}$$

The following algorithm presents how each central moment will be computed.



```
Algorithm (3) : Central Moment Computation.
-----------------------------------------------------------
Input: Image matrix $I$ , $p$, $q$, $x_c$ , $y_c$ , $m_{pq}$ .
Output: Central Moment : $cm_{pq}$ .
Begin
  Step1 : Set $cm_{pq}$ to zero.
  Step2 : For each row of $I$, $hi$.
  Step3 : For each column of $I$, $wj$.
  Step4: $cm_{pq} = cm_{pq} + (I(hi,wj)*((hi - x_c)\hat{}\,p)*((wj - y_c)\hat{}\,q))$
End
```

5.4 K-NN Classifier

K-Nearest Neighbor is a nonparametric supervised recognition method which examines the *k* nearest samples from the training set and classifies the test sample by using a voting scheme. Where the distance between features vector of test image and every record in moments database is calculated, then *k* value will be selected, and according to this, chosen *k* of the nearest prototypes to a test vector, and making voting to determine to which person a test image belongs.

5.5 Personal Identification

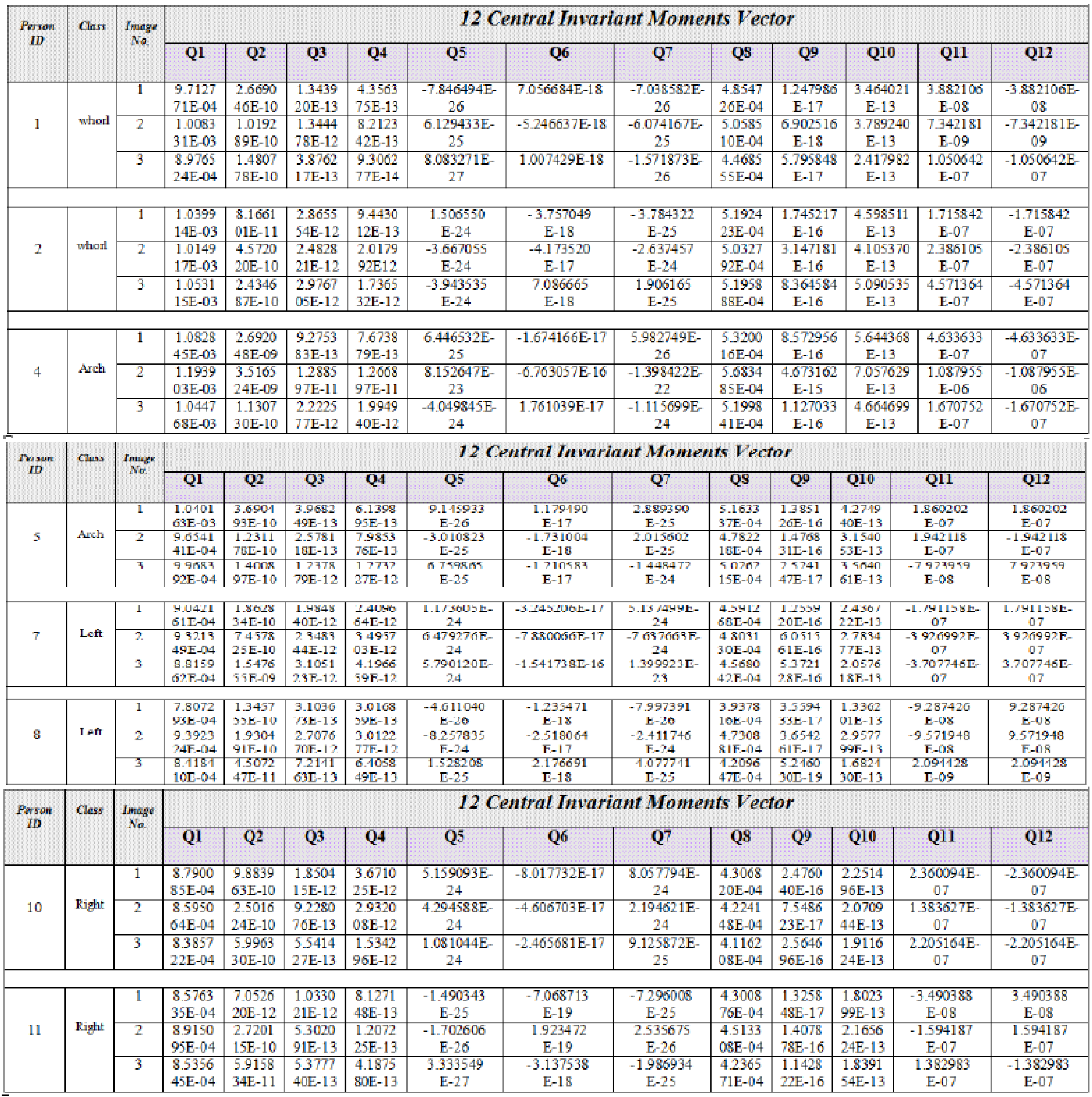
The final stage of the identification process requires decision making whether a test fingerprint image should be recognized successfully or not. If it is recognized, this means that it belongs to one person of enrollment phase (the individual who has this test image is identified).

6. EXPERMENTAL RESULTS

Enrollment Module In enrollment module, the samples' images are enrolled by the system, the 12 central invariant moments are extracted and stored in moment file. Table (1) tabulates the results of central moments of some individuals.

```
Algorithm (3) : K-NN Classifier.
------------------------------------------
Input: Moments database file, Vector of test image features.
Output: Person ID that is regarded to a test image.
Begin
Step1: Open moment's database.
Step2: For each record in moments file
Step2-1: Compute the distance between that features record and features vector of a test image.
Step2-2: Store computed distance in a data structure, let's call it Distances File.
Step3: Sort the Distances File according to the distance value.
Step4: Input the value of k parameter.
Step5: Select first k samples (they are with minimum distance to a test image) from distances file.
Step6: Count the number of occurrence each person in selected k samples.
Step7: Choose the person who has the larger occurrence number.
Step8: Return ID of the person who is selected in step7, this ID will be considered as the ID of his/her person of a test image.
End
```

Table 1: Centralized moment invariant



Person ID	*Class*	*Image No.*	***12 Central Invariant Moments Vector***											
			Q1	**Q2**	**Q3**	**Q4**	**Q5**	**Q6**	**Q7**	**Q8**	**Q9**	**Q10**	**Q11**	**Q12**
1	whorl	1	9.712771E-04	2.669046E-10	1.343920E-13	4.356375E-13	-7.846494E-26	7.056684E-18	-7.038582E-26	4.854726E-04	1.247986E-17	3.464021E-13	3.882106E-08	-3.882106E-08
		2	1.008331E-03	1.019289E-10	1.344478E-12	8.212342E-13	6.129433E-25	-5.246637E-18	-6.074167E-25	5.058510E-04	6.902516E-18	3.789240E-13	7.342181E-09	-7.342181E-09
		3	8.976524E-04	1.480778E-10	3.876217E-13	9.300277E-14	8.083271E-27	1.007429E-18	-1.571873E-26	4.468555E-04	5.795848E-17	2.417982E-13	1.050642E-07	-1.050642E-07
2	whorl	1	1.039914E-03	8.166101E-11	2.865554E-12	9.443012E-13	1.506550E-24	- 3.757049E-18	- 3.784322E-25	5.192423E-04	1.745217E-16	4.598511E-13	1.715842E-07	-1.715842E-07
		2	1.014917E-03	4.572020E-10	2.482821E-12	2.017992E12	-3.667055E-24	-4.173520E-17	-2.637457E-24	5.032792E-04	3.147181E-16	4.105370E-13	2.386105E-07	-2.386105E-07
		3	1.053115E-03	2.434687E-10	2.976705E-12	1.736532E-12	-3.943535E-24	7.086665E-18	1.906165E-25	5.195888E-04	8.364584E-16	5.090535E-13	4.571364E-07	-4.571364E-07
4	Arch	1	1.082845E-03	2.692048E-09	9.275383E-13	7.673879E-13	6.446532E-25	-1.674166E-17	5.982749E-26	5.320016E-04	8.572956E-16	5.644368E-13	4.633633E-07	-4.633633E-07
		2	1.193903E-03	3.516524E-09	1.288597E-11	1.266897E-11	8.152647E-23	-6.763057E-16	-1.398422E-22	5.683485E-04	4.673162E-15	7.057629E-13	1.087955E-06	-1.087955E-06
		3	1.044768E-03	1.130730E-10	2.222577E-12	1.994940E-12	-4.049845E-24	1.761039E-17	-1.115699E-24	5.199841E-04	1.127033E-16	4.664699E-13	1.670752E-07	-1.670752E-07
5	Arch	1	1.040163E-03	3.690493E-10	3.968249E-13	6.139895E-13	9.145933E-26	1.179490E-17	2.889390E-25	5.163337E-04	1.385126E-16	4.274940E-13	1.860202E-07	1.860202E-07
		2	9.654141E-04	1.231178E-10	2.578118E-13	7.985376E-13	-3.010823E-25	-1.731004E-18	2.015602E-25	4.782218E-04	1.476831E-16	3.154053E-13	1.942118E-07	-1.942118E-07
		3	9.968392E-04	1.400897E-10	1.237879E-12	1.273227E-12	6.759865E-25	-1.210583E-17	-1.448472E-24	5.076715E-04	7.574147E-17	3.564061E-13	-7.923959E-08	7.923959E-08
7	Left	1	9.042161E-04	1.862834E-10	1.984840E-12	2.409664E-12	1.173605E-24	-3.245206E-17	5.137499E-24	4.591268E-04	1.255920E-16	2.436722E-13	-1.791158E-07	1.791158E-07
		2	9.321349E-04	7.437825E-10	2.348344E-12	3.493703E-12	6.479276E-24	-7.880066E-17	-7.637663E-24	4.803130E-04	6.031561E-16	2.783477E-13	-3.926992E-07	3.926992E-07
		3	8.815962E-04	1.547655E-09	3.105123E-12	4.196659E-12	5.790120E-24	-1.541738E-16	1.399923E-23	4.568042E-04	5.372128E-16	2.057618E-13	-3.707746E-07	3.707746E-07
8	Left	1	7.807293E-04	1.345755E-10	3.103673E-13	3.016859E-13	-4.611040E-26	-1.235471E-18	-7.997391E-26	3.937816E-04	3.539433E-17	1.336201E-13	-9.287420E-08	9.287420E-08
		2	9.392324E-04	1.930491E-10	2.707670E-12	3.012277E-12	-8.257835E-24	-2.518064E-17	-2.411746E-24	4.730881E-04	3.654261E-17	2.957799E-13	-9.571948E-08	9.571948E-08
		3	8.418110E-04	4.507247E-11	7.214163E-13	6.405849E-13	1.528208E-25	2.176691E-18	4.077741E-25	4.209647E-04	5.246030E-19	1.682430E-13	2.094128E-09	2.094128E-09
10	Right	1	8.790085E-04	9.883963E-10	1.850415E-12	3.671025E-12	5.159093E-24	-8.017732E-17	8.057794E-24	4.306820E-04	2.476040E-16	2.251496E-13	2.360094E-07	-2.360094E-07
		2	8.595064E-04	2.501624E-10	9.228076E-13	2.932008E-12	4.294588E-24	-4.606703E-17	2.194621E-24	4.224148E-04	7.548623E-17	2.070944E-13	1.383627E-07	-1.383627E-07
		3	8.385722E-04	5.996330E-10	5.541427E-13	1.534296E-12	1.081044E-24	-2.465681E-17	9.125872E-25	4.116208E-04	2.564696E-16	1.911624E-13	2.205164E-07	-2.205164E-07
11	Right	1	8.576335E-04	7.052620E-12	1.033021E-12	8.127148E-13	-1.490343E-25	-7.068713E-19	-7.296008E-25	4.300876E-04	1.325848E-17	1.802399E-13	-3.490388E-08	3.490388E-08
		2	8.915095E-04	2.720115E-10	5.302091E-13	1.207225E-13	-1.702606E-26	1.923472E-19	2.535675E-26	4.513308E-04	1.407878E-16	2.165624E-13	-1.594187E-07	1.594187E-07
		3	8.535645E-04	5.915834E-11	5.377740E-13	4.187580E-13	3.333549E-27	-3.137538E-18	-1.986934E-25	4.236571E-04	1.142822E-16	1.839154E-13	1.382983E-07	-1.382983E-07

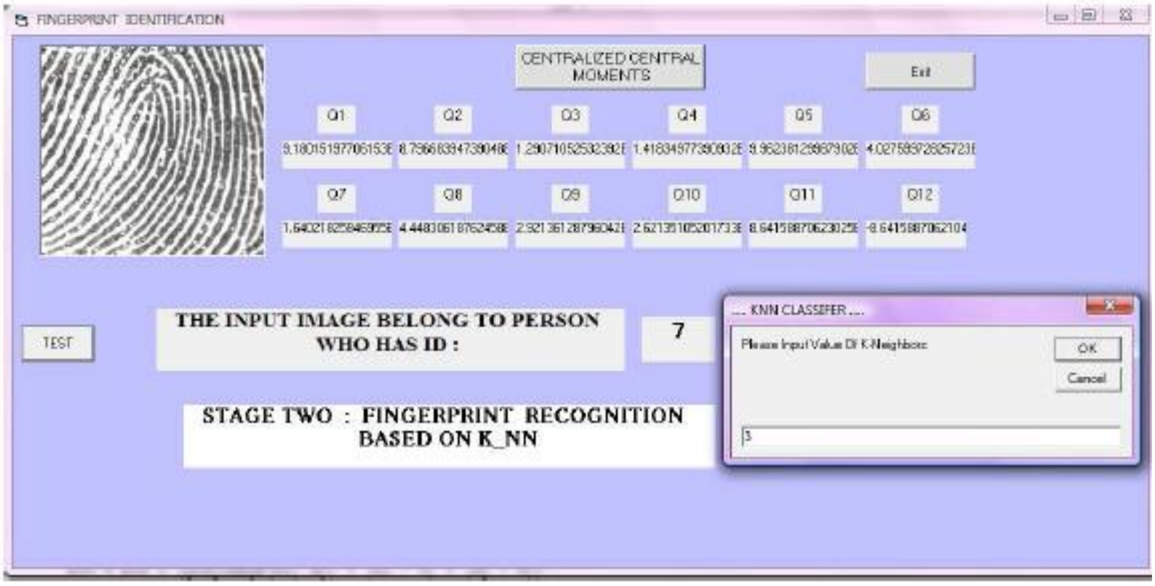
Identification Module

In the identification phase, each new image will be recognized to whom person it is, in fingerprint recognition operation, the major step, which impacts on system accuracy, is matching between enrolled images and test image, for this purpose, the *K-NN* algorithm is used. From the classified test images central moments are derived and taken as input to the *K-NN* algorithm, the values of *k* which are used in testing phase are 3, 5, 7, the best results of identification system performance is obtained when *k*=3. Figure (7) shows results of central moments and decision making of identification process of certain image.

Table (2) shows the results of identification process of testing images with *k*=3, where the following terms that are used in the Table referred to:

MDM: Matching Decision Making.

1. **ID-Voting: Resulted person ID that has larger majority among k-nearest persons to the test image.**



Q1	Q2	Q3	Q4	Q5	Q6
9.18015197706153E	8.79668394739048E	1.29071052532392E	1.41834977390803E	9.96238129867902E	4.02759972825723E

Q7	Q8	Q9	Q10	Q11	Q12
1.64021625846955E	4.44830618762458E	2.92136128796042E	2.62135105201733E	8.64158870623025E	-8.6415887062104

THE INPUT IMAGE BELONG TO PERSON WHO HAS ID : 7

STAGE TWO : FINGERPRINT RECOGNITION BASED ON K_NN

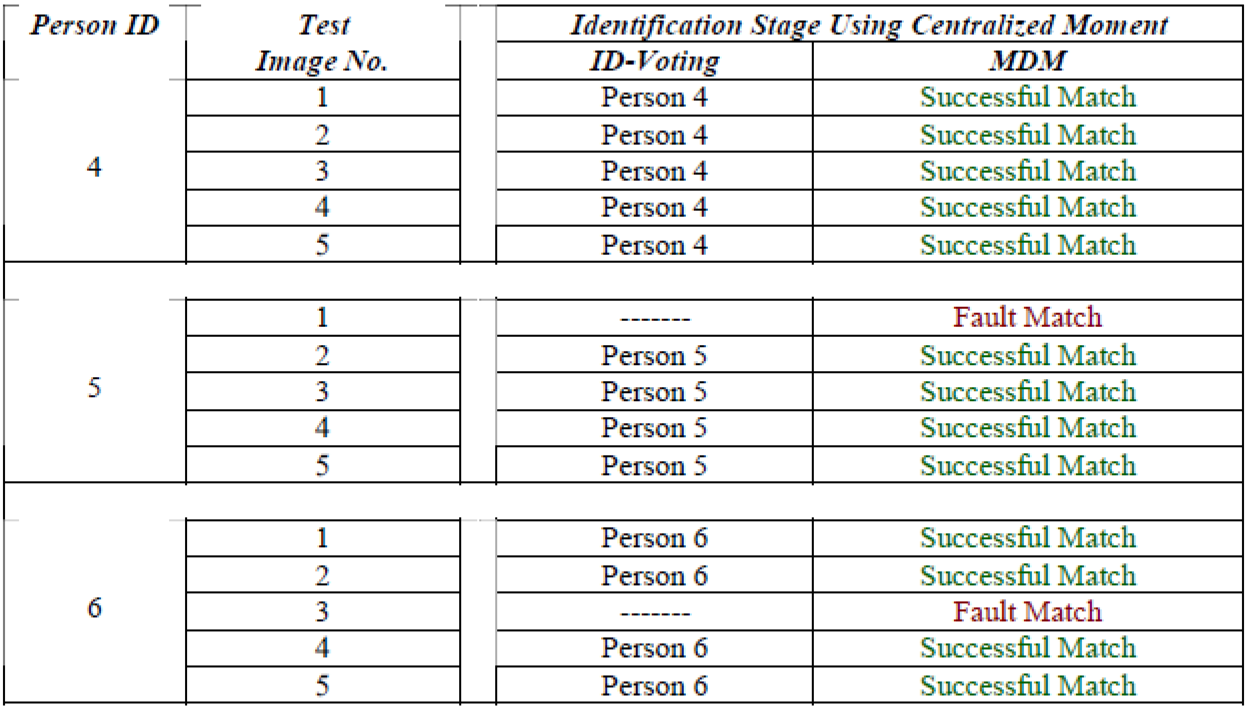
Please Input Value Of K-Neighbors

3

Figure7: Example of Identification Process.

Table 2: Some of matching results of identification of the system

Person ID	*Test Image No.*		*Identification Stage Using Centralized Moment*	
			ID-Voting	*MDM*
1	1		Person 1	Successful Match
	2		Person 1	Successful Match
	3		Person 1	Successful Match
	4		Person 1	Successful Match
	5		Person 1	Successful Match
2	1		Person 2	Successful Match
	2		Person 2	Successful Match
	3		Person 2	Successful Match
	4		Person 2	Successful Match
	5		Person 2	Successful Match
3	1		Person 3	Successful Match
	2		-------	Fault Match
	3		Person 3	Successful Match
	4		-------	Fault Match
	5		Person 3	Successful Match



Person ID	Test Image No.	Identification Stage Using Centralized Moment	
		ID-Voting	MDM
4	1	Person 4	Successful Match
	2	Person 4	Successful Match
	3	Person 4	Successful Match
	4	Person 4	Successful Match
	5	Person 4	Successful Match
5	1	-------	Fault Match
	2	Person 5	Successful Match
	3	Person 5	Successful Match
	4	Person 5	Successful Match
	5	Person 5	Successful Match
6	1	Person 6	Successful Match
	2	Person 6	Successful Match
	3	-------	Fault Match
	4	Person 6	Successful Match
	5	Person 6	Successful Match

To evaluate classification and identification system, accuracy is defined as:
Accuracy =Number of both successful classification and identification* 100% / Total number of test images

7. CONCLUSIONS

From this work for fingerprint identification system, the following conclusions are deduced according to the test results.
1- Centralized invariant moments is good method for local features extraction, specially extended five moments Q8-Q12 (in addition to first seven moments), whereas the accuracy of fingerprint identification (recognition) system when extending invariant moments is better than with no extension, it is 87.6%.
2- Using K-Nearest Neighbor algorithm in recognition phase gave good results in spite of its simplicity, but there is no scheme to determine appropriate value of k, it works depending on experiment concept for k value selecting, in spite of this, it achieves good accuracy of identification.
3- The selected value of k affects the system accuracy. In this paper, the best results of the identification were obtained when k=3.

8. FERENCES

[1] Acharya T., and Ray A. K., "Image Processing: Principles And Applications", Wiley-Interscience, USA, 2005.
[2] Afsar F. A., Arif M., and Hussain M., "Fingerprint Identification and Verification System Using Minutiae Matching", National Conference or Emerging Technologies, 2004.
[3] Al-Kharaz A. A. M., "Fingerprints Recognition Using Gabor Filters", MSC. Thesis, Baghdad University, 2005.
[4] Bhuyan M. H., and Bhattacharyya D. K., "An Effective Fingerprint Classification And Search Method", International Journal Of Computer Science And Network Security, Vol.9, No.11, November 2009.
[5] Bow S., "Pattern Recognition And Image Processing", Marcel Dekker, New York, USA, 2002.
[6] Cappelli R., Maltoni D., and Turroni F., "Benchmarking Local Orientation Extraction in Fingerprint Recognition", IEEE International Conference on Pattern Recognition, 2010.
[7] Dass S. C., Zhu Y., and Jain A. K., "Validating a Biometric Authentication System: Sample Size Requirements", IEEE Transaction on Pattern Analysis and Machine Intelligence, Vol.28, No.12, Dec. 2006.
[8] Espinosa V., "Minutiae Detection Algorithm For Fingerprint Recognition", IEEE, 2002.
[9] He M., and Zhao H., "An Identity Authentication Based on Fingerprint Identification", Proceeding of the 2009 International Symposium on Web Information Systems And Applications, pp.261-263, May 2009.
[10] Jain A. K., Flynn P., and Ross A. A., "Handbook of Biometrics", Springer, 2008.
[11] Konar A., "Artificial Intelligence And Soft Computing", USA, 2000.
[12] Lee H. C., and Gaensslen R. E., "Advances In Fingerprint Technology", Second Edition, CRC, USA, 2001.

[13] Li Y., "Reforming The Theory Of Invariant Moments For Pattern Recognition", Pattern Recognition Lett., Vol.25, pp.723-730, July 1992.
[14] Mostafa M., "A Novel Line Pattern Algorithm for Embedded Fingerprint Authentication System", GVIP Special issue on Fingerprint Recognition, 2007.
[15] Nixon M. S., and Aguado A. S., "Feature Extraction And Image Processing", Newnes, Great Britain, 2002.
[16] Pankanti S., Bolle R. M., and Jain A., "Biometrics: The Future Of Identification", Computer, Vol.33, No.2, pp.46-49, Feb.9, 2000.
[17] Ratha N., and Bolle R., "Automatic Fingerprint Recognition Systems", Springer, New York, 2004.
[18] Ratha N., and Govindaraju V., "Advances In Biometrics", Springer, 2008.
[19] Ravi J., Raja K. B., and Venugopal K. R., "Fingerprint Recognition Using Minutiae Score Matching", International Journal Of Engineering Science And Technology, Vol.1(2), pp.35-42, 2009.
[20] Reid P., "Biometrics For Network Security", Prentice Hall, Dec.30, 2003.
[21] Ritter G. X., and Wilson J. N., "Handbook Of Computer Vision Algorithms In Image Algebra",IT Knowledge, 1996.
[22] Simon D., Ortega J., Cruz S., and Etal, "Minutiae Extraction Scheme for Fingerprint Recognition System", IEEE, pp.254-257, 2001.
[23] Thai L. H., and Tam H. N., "Fingerprint Recognition Using Standardized Fingerprint Model", International Journal Of Computer Science Issues, Vol.7, Issue 3, No.7, May 2010.
[24] Uludag U., and Jain A., "Securing Fingerprint Template: Fuzzy Vault with Helper Data", Proceedings of the 2006 Conference on Computer Vision and Pattern Recognition Workshop, IEEE, 2006.
[25] Wahab A., Chin S. H., and Tan E. C., "Novel Approach To Automated Fingerprint Recognition", IEE Proceeding-Vis. Image Signal Process, Vol.145, No.3, June 1998.