Extract Unique Personal ID Using Fingerprint

Abdul Monem S. Rahma[1] and Esraa Q. Naamha[2]

[1,2]Computer Science Department - University of Technology- Baghdad-Iraq
[1]monem.rahma@yahoo.com
[2]esraakasim2005@yahoo.com

Received: 10 December 2016 **Accepted: 19 February 2017**

Abstract

Security documents like certificates, land revenue documents, etc., have only the individual's name, address, and in some cases a photo as means of personal identification. This makes criminal impersonation an easy task. Therefore, many of these limitations can be eliminated by incorporation of better methods that can be used to verify identity by measuring and analyzing human characteristics instead of things the individual may have (smart card) or know (password). The main goal of this paper is using the fingerprint technology to generate the unique ID based on the core point of the fingerprint of an individual that can be used for identifying person identity. The finger-print's minutia features are extracted with the core point as the reference based on the seven moment invariants, Then the extracted features are converted into numerical value, This numerical value is used as the unique ID for printing in the security documents for the personal identification. If the fingerprint image does not contain the core point such as the plain arch and tented arch patterns then we must create the center point in this fingerprint image and this is considered as the core point. The minutia features will be computed with this point as the reference point and this is used to generate a unique ID.

Keywords: Fingerprint, Fingerprint Recognition, seven Moment Invariants, Feature extraction, unique ID.

DIYALA JOURNAL FOR PURE SCIENCES

Extract Unique Personal ID Using Fingerprint

Abdul Monem S. Rahma and Esraa Q. Naamha

استخلاص رقم فريد لتحديد الهوية الشخصية باستخدام بصمة الاصبع

عبدالمنعم صالح ابو طبيخ [1] و **اســـراء قاســـم نعمـــة**[2]
[1,2]قسم علوم الحاسوب - الجامعة التكنولوجية – بغداد – العراق

الخلاصة

الوثائق الامنية مثل الشهادات ووثائق عائدات الاراضي وغيرها تحتوي فقط اسم الشخص ومكان الاقامة وفي بعض الحالات تحتوي صورة كوسيلة لتحديد الهوية الشخصية وهذا يجعل التمثيل الجنائي مهمة سهلة . لذا الكثير من هذه المحددات يمكن تلافيها من خلال دمج طرق افضل يمكن ان تستخدم للتحقق من الهوية وذلك من خلال قياس وتحليل الخصائص الانسانية بدلاً من اشياء يمتلكها (البطاقة الذكية) او يعرفها (كلمة المرور) الفرد. الهدف الرئيسي لهذا البحث هو استخدام تقنية بصمة الاصبع لتوليد معرف فريد بالاعتماد على نقطة المركز لبصمة الاصبع والذي يمكن استخدامه لتحديد هوية الشخص . ان الصفات الثانوية لبصمة الاصبع يتم استخلاصها مع نقطة المركز كنقطة مرجع باستخدام تقنية العزوم السبعة ، ومن ثم هذه الصفات المستخلصة يتم تحويلها الى قيمة رقمية ، وهذه القيمة الرقمية تستخدم كمعرف فريد يتم طبعه في الوثائق الامنية لتحديد الهوية الشخصية . اما اذا كانت صورة بصمة الاصبع لا تحتوي على نقطة مركز ففي هذه الحالة يجب علينا انشاء نقطة في صورة بصمة الاصبع واعتبارها كنقطة مركز. وان الصفات الثانوية المستخلصة بالاعتماد على هذه النقطة كنقطة مرجع يتم استخدامها لتوليد المعرف الفريد.

الكلمات المفتاحية: بصمة الاصبع ، تمييز بصمة الاصبع ، العزوم السبعة ، استخلاص الخصائص ، رقم فريد

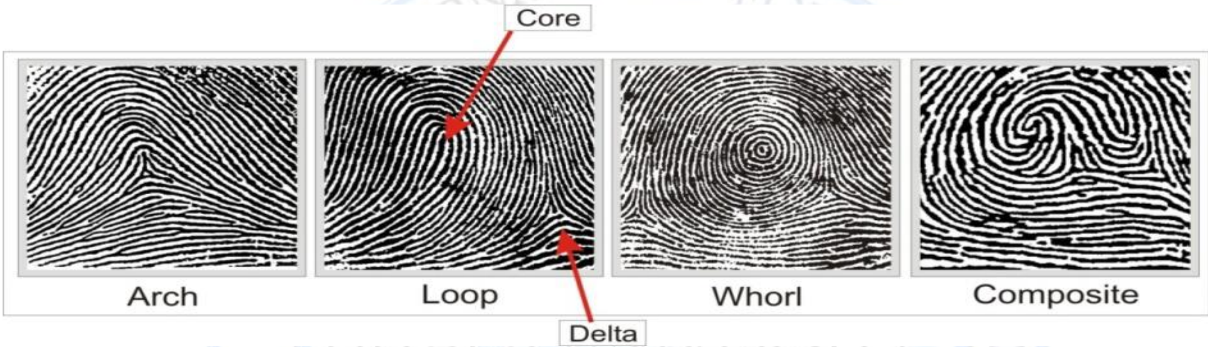
Introduction

Highly important documents such as certifications, passports, driving licenses, and land revenue documents have a degree of security that makes forging rather a difficult task. However, once a malicious person who has good technical experience gets the possession of such a document, they can simply perform a criminal impersonation. This is very simple due to the fact that documents like these have only name, place of residence, and a picture of the owner for the ID. Every single one of these details is under the risk of duplication. The usage of biometric characteristics will be helpful in reducing the risk of duplication. Nowadays, the usage of biometrical features in these documents is quite uncommon. However, in order to stop impersonation and avoid the forgery of this kind of documents, the correct solution will be the usage of biometric techniques. The usage of substantial physical and behavioral features of an individual being to individually recognize a person is called as biometrics. Biometrical techniques in general, take a specific portion of the human's body to distinguish an individual and those techniques are very precise. The person's biometrical features that are deduced have to be somehow transferred to the documents [1].

Biometrics means measuring of individual physiological or behavioral features of an individual for the sake of identifying that individual. Biometrics is an individual feature which is a part of the human being. Therefore, there's no necessity to worry about remembering any passwords, or carrying any form of document for identification. Biometric features can be divided in two basic kinds. Physiological character: Which is concerned with the shape of the body and therefore it is different from one person to another. Examples of that are fingerprints, face recognitions, hand geometry and iris recognitions. Behavioral character: This is concerned with the individual's behavior such as signatures, key stroke dynamics and voice. Behavioral features might change as the person ages [2].

Personal identification is mainly split into three kinds depending on what the person possesses (such as a credit card or keys), by something they know (such as a password or a PIN code) or by physiological or behavioral features. The third method is called biometrics and the six most widely known characteristics consist of face, voice, iris, signature, hand geometry and fingerprint. It has been proven and is widely known, the fact that everybody has an individual fingerprint that doesn't vary with the change of time. Every individual's finger is of its own unrepeated pattern; therefore, any finger might be used in identifying an individual successfully [3].

Fingerprints are of the most predominant biometrical features. Fingerprint is the representation of the friction ridges on finger. A friction ridge is an elevated part of the epidermis on the surface of the finger and they are permanent along the life. Two fingerprints, even in the case where they're taken from identical twins, could never be identically similar. Some of the most common biometrical characteristics such as Fingerprints, Iris and face recognition and fingerprint are the most popular feature. It's used in individual distinguishing in many personal and civilian implementations due to its characteristics such as uniqueness and un-changeability. Fingerprints may be divided into several kinds depending on the general ridge formation like the arches, loops, whorls, and composites as depicted in Figure (1). In the pattern of arch ridges are drawn from one side to the other one in a continuous manner. The ridges in arch manner drawn with no backward turn or re-curve. The patterns of loops are the ones where the ridges make a backward turn with not wits. Therefore, the center of the print seems to look like a hairpin in loop pattern. The ridges in whorl pattern form a highly complicated pattern that has two or more deltas. The composite pattern includes a mix of two or more arches, whorl and loop patterns [1].



.

Figure (1): Basic patterns of finger-print ridges

In the pattern of a fingerprint there are specific individual points, such as core and delta that are mainly marked as the singular points. Singular points are the ones where there is a sudden variation in the ridge patterns. In finger-prints, Minutiae, the breakings in the patterns of ridges that interrupt the usually smooth flow of ridges, are important characteristics that are utilized in order to contrast one print from others. There are a number of kinds of Minutiae such as ridge endings, ridge bifurcations, short ridges, islands, spurs, bridges, and so on[1].

This research reports a simpler mechanism for developing a unique ID through the extraction of the minutia features depending on the fingerprint's core point of a person for printing in the documents for the individual identification.

The paper is arranged in the following order: Section 2 explains concepts of moment invariants. Section 3 illustration of the proposed system presented. Section 4 gives the results acquired from the evaluation of simulation and performance seen in section 3. Lastly, section 5 concludes the analysis.

2. Concepts of Moment Invariants

Moment invariants are common characteristics used in the processing of images, remote sensing, recognizing shapes and classifying. Moments are capable of providing object properties which uniquely identify its form. Invariant recognizing of shape is done by classifying in the multi-dimensional moment invariant feature space. A number of methods for the derivation of invariant characteristics from moments for recognizing objects and for representation were developed. These methods are identified by their definition of moment, like the kind of the data that is implemented and the technique for the derivation of invariant values from the image moments. Hu was the first one to determine the algebraic base for the 2D moment invariants and implemented their applications in recognizing shapes. They have been initially implemented in Aircraft shape recognition and have proved to be fast and dependable (Dudani, Breeding and McGhee, 1977). These values of moment invariants don't change with respect to translating, scaling and rotating of the object [5].

Representation of region moment interprets a normalized grey level image function as a probability density of a two dimensional random variable. Characteristics of this random variable may be represented with the use of statistical characteristic-moments [Papoulis, 1991]. Supposing that a pixel with values greater than zero represents areas, moments can be used in black and white or grey level area description. A moment that has the order (p + q) depends on scaling, translating, rotating, and even on grey level transformations and is depicted by [6]:

$$\mu_{pq} = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} x^p y^q f(x,y)\,dx\,dy \qquad \textbf{(1)}$$

In digitized images we evaluate sums

$$\mu_{pq} = \sum_{i=-\infty}^{\infty}\sum_{i=-\infty}^{\infty} i^p j^q f(i,j) \qquad \textbf{(2)}$$

Where x, y, i, j are the region point co-ordinates (pixel co-ordinates in digitized images). Translation invariance can be achieved if we use the central moments

$$\mu_{pq} = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty}(x - x_c)^p\,(y - y_c)^q\,f(x,y)\,dxdy \tag{3}$$

Or in digitized images

$$\mu_{pq} = \sum_{i=-\infty}^{\infty}\sum_{i=-\infty}^{\infty}(i - x_c)^p(j - y_c)^q\,f(i,j) \tag{4}$$

Wherex_c, y_c are the co-ordinates of the region's center of gravity (centroid), which can beobtained using the following relationships:

$$x_c = \frac{m_{10}}{m_{00}} \quad , \qquad y_c = \frac{m_{01}}{m_{00}} \tag{5}$$

In the case of the binary,m_{00} means the region area (see equations (1) and (2)).Scale-invariant features can also be found in scaled central moments η_{pq}(scale change$\acute{x} = \alpha x, \acute{y} = \alpha\, y$)

$$\eta_{pq} = \frac{\acute{\mu}_{pq}}{(\acute{\mu}_{00})^{\gamma}}\,, \quad \gamma = \frac{p+q}{2} + 1\,, \quad \acute{\mu}_{pq} = \frac{\mu_{pq}}{\alpha^{p+q+2}} \tag{6}$$

and normalized un-scaled central moments

$$\vartheta_{pq} = \frac{\mu_{pq}}{(\mu_{00})^{\gamma}} \tag{7}$$

A group of 7 invariant moments are possible to be deduced from the second moment and the third moment which were introduced by Hu. As the formulas that are listed below, Hu deduced the expressions from algebraic invariants applied to the moment producing function under a rotating operation [7].

$$\left.\begin{aligned}
\varphi_1 &= \vartheta_{20} + \vartheta_{02}, \\
\varphi_2 &= (\vartheta_{20} - \vartheta_{02})^2 + 4\vartheta_{11}^2, \\
\varphi_3 &= (\vartheta_{30} - 3\vartheta_{12})^2 + (3\vartheta_{21} - \vartheta_{03})^2, \\
\varphi_4 &= (\vartheta_{30} + \vartheta_{12})^2 + (\vartheta_{21} + \vartheta_{03})^2, \\
\varphi_5 &= (\vartheta_{30} - 3\vartheta_{12})(\vartheta_{30} + \vartheta_{12})((\vartheta_{30} + \vartheta_{12})^2 - 3(\vartheta_{21} + \vartheta_{03})^2) \\
&\quad + (3\vartheta_{21} - \vartheta_{03})(\vartheta_{21} + \vartheta_{03})(3(\vartheta_{30} + \vartheta_{12})^2 - (\vartheta_{21} + \vartheta_{03})^2), \\
\varphi_6 &= (\vartheta_{20} - \vartheta_{02})((\vartheta_{30} + \vartheta_{12})^2 - (\vartheta_{21} + \vartheta_{03})^2) \\
&\quad + 4\vartheta_{11}(\vartheta_{30} + \vartheta_{12})(\vartheta_{21} - \vartheta_{03}), \\
\varphi_7 &= (3\vartheta_{21} - \vartheta_{12})(\vartheta_{30} + \vartheta_{12})((\vartheta_{30} + \vartheta_{12})^2 - 3(\vartheta_{21} + \vartheta_{03})^2) \\
&\quad - (\vartheta_{30} - 3\vartheta_{12})(\vartheta_{21} + \vartheta_{03})(3(\vartheta_{30} + \vartheta_{12})^2 - (\vartheta_{21} + \vartheta_{03})^2)
\end{aligned}\right\} \quad (8)$$

where the $\boldsymbol{\vartheta_{pq}}$values can be calculated from equation (7) .

3. The Proposed System stages

The proposed system contains two stages: feature extraction and unique ID generation. They are described in the following sections.

3.1 Feature Extraction

Feature extraction is defined as the process of converting a captured biometric sample, i.e. fingerprint, in to a unique, distinctive and compact form so that it can be compared to a reference template. Feature extraction is a significant step to improve the efficiency of personal identification. This stage consists of two phases training phase and testing phase. Each phase has specific steps.

3.1.1Training Phase: The training phase contains three steps.

a. Sample Image Binarazation: Ten samples for each fingerprint's feature (core, delta, ridge bifurcation and ridge ending) that act as training database are converted in to binary form as pre-processing step in order to be used in the seven invariant moments in subsequent steps**.**

b. Computing seven invariant moments of fingerprint's features samples: compute the seven invariant moments of the binarized sample images of each fingerprint's feature which were produced by the binarazation process in the previous step.

c. Computing variance of fingerprint's features samples: The variance of each sample can be achieved by finding the maximum and minimum values of each moment of the samples and compute the mean of each moment of the samples by applying this equation:

Mean = (max + min)/2. **(9)**

Then compute the variance of each sample by applying this equation

$$Variance_S = \sum_{i=1}^{7}(moment\ invariants(i) - mean(i)\ )^2 \quad (10)$$

3.1.2 Testing Phase: The testing phase contains seven steps.

a. Fingerprint Image Binarazation: compute the binarazation of the original fingerprint image which is obtained from testing database as pre-processing step.

b. Region of Interest (ROI) Extraction: Crop the binarized of the fingerprint image into an ROI in order to separate foreground region and background region.

c. Computing Total Ridge Width: The total ridge width of the fingerprint image can be computed by applying this equation: **$Total_{RW} = (max_W + max_B)*K$.** **(11)**

Where total $_{RW}$ is the total ridge width of the fingerprint image, max $_W$ is the maximum value of the frequency of occurrence of the white ridge width, max $_B$ is the maximum value of the frequency of occurrence of the black ridge width and K is the integer value identifies how many lines that the fingerprint's feature has. Depending on trial-and-error, best integer value for K is 6. If K is more or less than 6 then the result is incorrect.

d. Fingerprint Image Partition: After computing the total ridge width, we will divide the fingerprint image (ROI) into blocks with equal size of w x w and detect blocks size based on the total ridge width that is computed in the previous step. The fingerprint image partition can be performed pixel by pixel**.**

e. Computing seven moment invariants of blocks: compute the seven invariant moments of the blocks of the fingerprint image that are obtained from applying the fingerprint image partition process.

f. Computing variances of blocks: The variance of each block can be calculated from applying this equation:

$$Variance_B = \sum_{i=1}^{7}(moment\ invariants(i) - mean_{DB}(i))^2 \quad (12)$$

where $Variance_B$ is the variance of each block and $mean_{DB}$ is the seven means of the fingerprint features stored in database

g. Variance Matching: After calculating the variances of each fingerprint's feature stored in database and the variances of each block which were produced previously. The variance matching process first compares and matches the variances of each block with the variances of each fingerprint's feature stored in database. Next find the largest matches, these largest matches are considered as the fingerprint feature points and mark them on the fingerprint image.

Algorithm (1): Fingerprint Image Features Extraction
Input: a number of samples of each fingerprint feature, Fingerprint image**.** **Output:** the largest matches as the fingerprint feature points and mark it in the image. **Begin** **Step1:** Initialize fingerprint feature samples in a binary form. **Step2:** Compute the seven invariant moments as mentioned in equation (8) of each fingerprint feature sample. **Step3:** Find the maximum (Max) and minimum (Min) of each moment of the fingerprint feature samples and compute the mean of each moment of the fingerprint feature samples by applying equation (9) **Step4:** Compute the variance$_s$ of each fingerprint feature sample by applying the equation (10). **Step5:** store the mean and variance$_s$ of each fingerprint feature sample in the database for later use in the testing phase. **Step6:** Initialize fingerprint image in a binary form. **Step7:** Crop the binarized of the fingerprint image into an ROI in order to separate foreground region and background region. **Step8:** Compute the white ridge width and the black ridge width of the fingerprint image and find the histogram of the white ridge width and the black ridge width and then compute the total ridge width by applying the equation (11) **Step9:** Divide the ROIs into blocks with equal size of w x w and detect blocks size based on the total ridge width which computed in step 8. **Step10:** Compute the seven moments as mentioned in equation (8) of each block and compute the variance $_B$ of

each block by applying the equation (12).

Step11: Compare and match of the $Variance_{B}$ of each block with the $variance_{S}$of samples stored in database.

Step12: Find the largest match and mark it as the fingerprint feature point on fingerprint image.

End

3.2 Unique ID Generation

After finding the core point and the minutia points there will be a big number of minutiae. However, just a little number of minutiae that is completely individual for that specific fingerprint is necessary in generating the unique ID. Therefore only the minutiae that lie within a Region of Interest (ROI) distributed in the area that surrounds the core point are taken. Here, the ROI is a square with an appropriate pixel area that is centered on the core point. There are two cases in the fingerprint image; in the first case the fingerprint image contains the core point such as loop and whorl, while in the second case the fingerprint image does not contain the core point like arch.

a. The fingerprint image contains the core point: In this case the unique ID generation algorithm must apply the Region Of Interest (ROI) centered around the core point so that only the minutia points (ridge bifurcation and ridge ending points) which are inside ROI are taken, The size of the ROI can be determined by finding the distance between the core point and the rest of the other minutia points (ridge bifurcation and ridge ending points) by using the Euclidean distance equation and selecting the required number of the minutia points that have the less distance between them and the core point so that only these minutia points are inside ROI. The required number of the minutia points can be determined by the system user. By applying parametric equation of a circle, a circle can be defined as the locus of all points that satisfy the equations[8]:

$$\mathbf{x = x_c + r \cos \Theta} \qquad \mathbf{For\ 0 < \Theta > 2\Pi} \qquad \mathbf{(13)}$$
$$\mathbf{y = y_c + r\ sine\ \Theta}$$

If we find minutia points located within the boundaries of these circles then we find their own angles. This process continues until the end of all the minutia points contained within the Region Of Interest (ROI). Each angle of the minutia points is converted to fixed length which consists of three digits. Depending on the priority of the finding the minutia points on the circles, all the angles are connected with each other to generate the numerical values. These numerical values are considered as a unique ID

b. The fingerprint image does not contain the core point: In this case the unique ID generation algorithm must calculate the distance between each point and the rest of the other minutia points which are marked in the fingerprint image by using the Euclidean distance equation.

In the Euclidean distance, if $\mathbf{P_1\ (x_1,y_1)}$ and $\mathbf{P_2(x_2,y_2)}$ then the distance is given by [9]:

$$\mathbf{D\ (P_1, P_2)} = \sqrt{(\mathbf{x_2} - \mathbf{x_1})^2 + (\mathbf{y_2} - \mathbf{y_1})^2} \tag{14}$$

Choose the less distance between two minutia points and find the midpoint between them by using the midpoint equation, if $\mathbf{P_1\ (x_1,y_1)}$ and $\mathbf{P_2(x_2,y_2)}$ then the midpoint is given by [10]:

$$\mathbf{x} = (\mathbf{x_1} + \mathbf{x_2})/2$$
$$\mathbf{y} = (\mathbf{y_1} + \mathbf{y_2})/2 \tag{15}$$

The Midpoint is $\mathbf{P(x, y) = (\ (x_1 + x_2)/2, (y_1 + y_2)/2)}$

This midpoint is considered as the core point of the fingerprint image. Then repeat the same steps that have been applied in the case of the fingerprint image contain the core point in order to generate a unique ID.

Algorithm (2): Unique ID generation
Input: A number of feature points that marked in the fingerprint image, **Output:** A unique ID. **Begin** **Step1:** If the fingerprint image contains the core point **Step2:** Apply Region Of Interest (ROI) that resides around the core-point so that only the minutia points which are inside ROI are taken. **Step3:** Draw circles in clockwise direction by applying the equation (13) **Step4:** If find minutia point lie within the boundaries of the circle then find the angle of this minutia point. **Step5:** All angles which found in step 4 is converted to fixed length consist of three digits. **Step6:** Depending on the priority of the finding of the minutia points on the circles, all the angles are connected with each other to generate the numerical values. These numerical values are considered as a unique ID. **Step7:** If the fingerprint image does not contain the core point. **Step8:** Calculate the distance between each point and the rest of the other feature points which marked in the fingerprint image by using the Euclidean distance equation (14). **Step9:** Choose the less distance between two minutia points and find the midpoint between them by using the midpoint equation (15) and this is considered as the core point. **Step10:** Repeat steps 2 to 6 in order to generate a unique ID. **End**

4. Experimental Results of the proposed system:

This section illustrates the phases of implementing the proposed system:

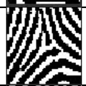
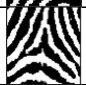
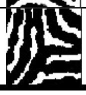
4.1. Feature Extraction

In the training phase, samples of fingerprint's features were chosen. These samples consist of 40 sample images, 10 sample images for each fingerprint's features (core, delta, ridge bifurcation and ridge ending). The system will train all the samples images and store the values in the database. This phase runs only one time at the beginning of running the program. After these sample images of each fingerprint's feature are converted in to binarized images, now the seven invariant moment processes are applied to these binarized images as described in section (3.1.1.b). After computing the seven invariant moment values for each sample of the fingerprint's features, now we will compute the maximum value, minimum value and mean value for each moment of the samples and compute the variance of each sample as previously explained in section (3. 1.1.c). Tables (1), (2), (3) and (4) show the results of applying the seven invariant moments, max, min , mean and variance processes to the binarized sample images of each fingerprint's feature (core, delta, ridge bifurcation and ridge ending).

Table (1): seven moment, max, min, mean and variance of core samples

feature	samples	Moment1	Moment2	Moment3	Moment4	Moment5	Moment6	Moment7	variance
core		0.367762323	0.000714789	0.175638161	0.725816942	-1.918946153	0.014110304	0.501909748	2.811271395
		0.309771329	2.56547E-05	0.014512146	0.055314476	0.000745919	0.000278269	-0.000906803	9.221962369
		0.580427746	0.001769553	1.706835688	1.767221261	-0.618864922	-0.060357975	0.239818112	5.821359907
		0.556888429	0.000877853	0.823600113	2.398501391	-5.089908191	0.065463794	-2.101493351	9.565227831
		0.405781532	0.00033202	0.723355259	0.4836853	-1.235365909	0.002361229	0.285443772	3.464051882
		0.429146916	0.000760343	1.299642739	0.152185502	-0.198682694	-0.003893395	-0.015555868	7.466106408
		0.295461614	0.000133857	0.158098028	0.23718008	-0.66518317	-0.00247542	0.04163621	5.733639206
		0.394401412	0.000304832	0.301284502	0.163270822	-0.443334358	-0.000919352	0.030240055	6.55033975
		0.396413655	0.000447024	0.120041595	0.159973504	-0.390423125	-0.002062225	-0.00863987	6.954949756
		0.327947458	2.35765E-05	0.245495361	0.117376241	-0.089073409	-0.000383326	-0.010626527	8.273914034
max		0.580427746	0.001769553	1.706835688	2.398501391	0.000745919	0.065463794	0.501909748	
min		0.295461614	2.35765E-05	0.014512146	0.055314476	-5.089908191	-0.060357975	-2.101493351	
mean		0.43794468	0.000896519	0.860673917	1.226907934	-2.544581136	0.00255291	-0.799791802	

Table (2): seven moments, max, min, mean and variance of delta samples

feature	samples	Moment1	Moment2	Moment3	Moment4	Moment5	Moment6	Moment7	variance
delta		0.398021912	0.000358359	0.228402446	0.011944634	-0.034439928	0.00019266	-0.000266615	11.91745728
		0.307270542	0.000300198	0.258209624	0.063425711	-0.006023135	0.000495218	0.006109293	11.58675371
		0.375840517	1.60336E-05	0.556478308	0.025449866	-0.064567897	-6.13854E-05	-0.001271169	10.70379288
		0.378251223	1.86876E-05	0.211595783	0.212014751	-0.58217782	-0.000678736	0.035490289	13.36973624
		0.536997267	0.000406862	4.596825496	0.006017693	-0.001919519	8.74876E-05	-0.000588616	12.4557066

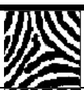
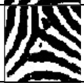
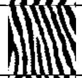
		0.412386454	0.000615736	0.427103054	0.30780312	-0.701869925	0.006863814	-0.036616508	13.12508875
		0.405235015	0.000998863	2.392517104	0.596002269	-1.25687297	-0.004821653	-0.340355651	13.11313138
		0.333507254	0.000521079	1.244606272	0.051057856	0.001534662	-0.000120223	-0.011149183	8.514886205
		0.478957997	0.000334098	1.906419225	2.192144554	4.141442694	0.023489162	4.380522371	14.24612555
		0.387120856	1.48567E-05	0.089587624	0.075851011	-0.023122066	0.000234092	-0.001611861	12.36177616
max		0.536997267	0.000998863	4.596825496	2.192144554	4.141442694	0.023489162	4.380522371	
min		0.307270542	1.48567E-05	0.089587624	0.006017693	-1.25687297	-0.004821653	-0.340355651	
mean		0.422133904	0.000506818	2.34320656	1.099081123	1.442284862	0.009333755	2.02008336	

Table (3): seven moments, max, min, mean and variance of ridge bifurcation samples

feature	samples	Moment1	Moment2	Moment3	Moment4	Moment5	Moment6	Moment7	variance
Bifurca-tion		0.54762365	5.62921E-05	0.072674651	1.433013344	-0.370900492	0.008426563	0.363588885	17.587481
		0.600068034	0.001859057	0.383473321	0.907239113	-1.850206763	0.032937322	-1.046518234	16.06416884
		0.521030117	0.002921895	8.26076871	0.811497341	0.097011912	0.041956038	0.83930616	18.76413524
		0.369862809	4.73742E-05	0.335685451	0.165898083	-0.460433761	8.45921E-05	-0.00785301	15.04078375
		0.333251954	0.000274358	0.340239079	0.150924275	-0.19039099	-0.001434758	-0.009894182	15.32752976
		0.33309385	1.72983E-05	0.345220064	0.045058252	-0.090387999	0.000162705	0.003516336	15.57330648
		0.336228047	0.000253873	0.649569429	0.148894624	0.029794735	0.001095928	-0.036005702	13.41551271
		0.327358925	6.17876E-06	0.224260408	0.239708176	-0.002146589	0.000394319	-0.034232376	16.42043417
		0.293429086	3.05983E-05	0.035326925	0.244870348	-0.714598843	0.001352768	0.034288927	17.21876369
		0.30883988	0.000228635	0.824650732	0.026604785	-0.06435607	0.000396924	-0.002843009	12.22876855
max		0.600068034	0.002921895	8.26076871	1.433013344	0.097011912	0.041956038	0.83930616	
min		0.293429086	6.17876E-06	0.035326925	0.026604785	-1.850206763	-0.001434758	-1.046518234	
mean		0.44674856	0.001464032	4.148047818	0.729809064	-0.876597425	0.02026064	-0.103606037	

Table (4): seven moments, max, min, mean and variance of ridge ending samples

feature	samples	Moment1	Moment2	Moment3	Moment4	Moment5	Moment6	Moment7	variance
ending		0.37875198	9.49985E-05	0.20315345	0.435533805	0.128983086	0.002436308	0.017220067	0.08469289
		0.331590032	3.37321E-05	0.572676125	0.060875837	-0.072654295	-0.000316533	-0.001383538	0.10833972
		0.359157615	0.000109981	0.573490845	0.036373215	-0.105165919	0.000307322	-0.000703257	0.121718016
		0.30928586	0.000116632	0.060874434	0.238347394	-0.200541385	-0.002065959	-0.068766901	0.081613613
		0.284982105	4.69043E-06	0.188015711	0.031494706	-0.059358278	-6.78732E-05	0.000497865	0.049402838
		0.359546512	1.54543E-05	0.082316203	0.057202802	-0.067630218	-0.000157262	0.002939939	0.072503359
		0.356305043	5.71319E-05	0.138533532	0.21987027	0.012877215	0.001148169	-0.028180914	0.025770375
		0.280827359	1.01541E-05	0.380309639	0.007598341	-0.002028789	1.37113E-05	0.000349491	0.05820209
		0.277462565	0.00042095	0.35117337	0.037042907	-0.110693593	-0.000314897	0.00324446	0.046951084
		0.281276413	1.48943E-05	0.004230146	0.009330249	-0.014822329	-3.31854E-05	-0.000120517	0.129348957
max		0.37875198	0.00042095	0.573490845	0.435533805	0.128983086	0.002436308	0.017220067	
min		0.277462565	4.69043E-06	0.004230146	0.007598341	-0.200541385	-0.002065959	-0.068766901	
mean		0.328107273	0.00021282	0.288860495	0.221566073	-0.035779149	0.000185175	-0.025773417	

In the testing phase, the system will identify an individual person by testing his fingerprint image. This phase is done every time we want to identify a fingerprint image. In this phase the binarization process will be applied to the original fingerprint image that was described in section (3.1.2.a). Figure (2) shows examples of binarized fingerprint images obtained after applying the binarization process to the original fingerprint image.

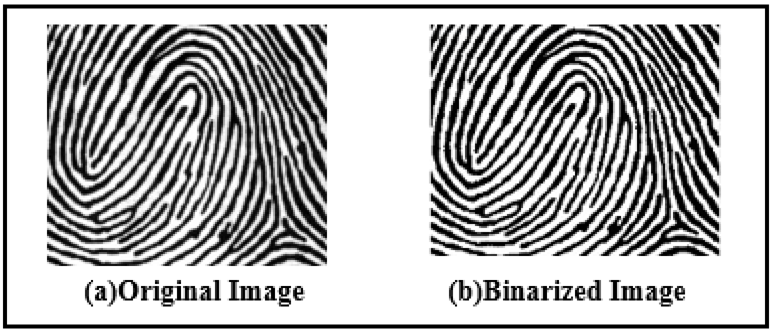
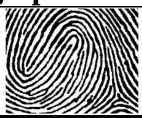


Figure (2): Sample of fingerprint image binarazation

After applying the binarization process on the original fingerprint image, now crop the binarized fingerprint image into an ROI in order to separate foreground region and background region and speedup the overall process. To extract fingerprint features from fingerprint image **(**ROI), first must compute the total ridge width of the fingerprint image **(**ROI**)** as described in section (3.1.2.c). Table (5) shows the results of applying the total ridge width process to the fingerprint image **(**ROI).

Table (5): Total ridge width

fingerprint Image	white ridge width	black ridge width	total ridge width
	6	6	72

Next divide the fingerprint image (ROI) into blocks with equal size of w x w and detect blocks size based on the total ridge width which were produced in the previously step. The fingerprint image partition can be performed pixel by pixel as shown in Figure (3).

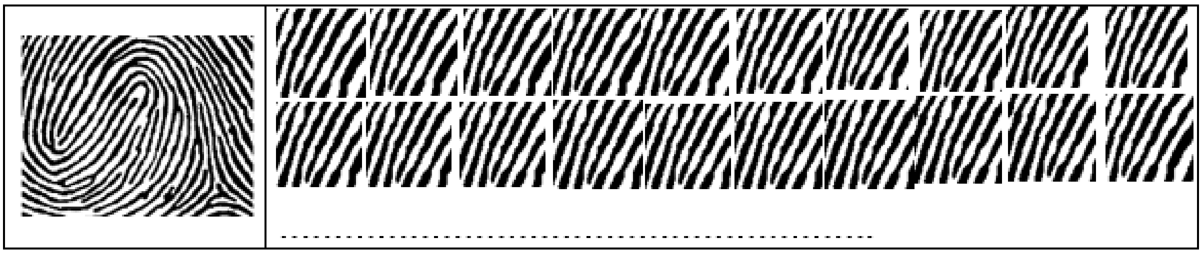


Figure (3): Fingerprint image partition pixel by pixel

After producing the blocks by applying the fingerprint image partition process to the fingerprint image (ROI) in the previously step, now compute the seven invariant moment values and the variance values of each block as shown in table (6).

Table (6): seven moments and variance of each block

image	blocks	Moment1	Moment2	Moment3	Moment4	Moment5	Moment6	Moment7	variance
		0.342898521	0.000257502	0.035279937	0.020369413	-0.005767374	5.40765E-05	-0.000271723	0.1065530385
		0.34120435	0.000180458	0.010421897	0.022297226	-0.007215288	3.61221E-05	0.000124527	0.1188942802
		0.340184748	0.0001096144	0.038803371	0.030785787	-0.008644951	-1.69997E-05	0.0013424805	0.1005431358
		0.339804342	8.60723E-05	0.154585078	0.042455501	-0.006724813	-9.79553E-05	0.004226543	0.0519915541
		0.340324912	8.40054E-05	0.1818390503	0.044248926	-0.0028877302	-0.000157016	0.003929101	0.0450084496
		0.340483725	8.64543E-05	0.184155566	0.040046169	-0.0023529377	-0.000160334	0.002514773	0.0459834426
		0.340288361	9.71221E-05	0.140554647	0.026993725	-0.001366158	-0.000119102	0.001088231	0.0619073097
		0.340036587	0.000118826	0.094754891	0.013147241	-0.000623654	-6.70065E-05	0.000318978	0.0831744976
		0.339478558	0.0001785261	0.092825812	0.002400637	-0.000237476	-1.79995E-05	2.59543E-05	0.0885212539
		0.339116163	0.000231118	0.147619763	0.0004374961	-0.0001959501	3.82321E-06	-1.02221E-07	0.0708984484
	...	...	...	...	...	...	...	...	...
	in this example the image is divided in to 40198 blocks								

After calculating the variances of each fingerprint's feature stored in database and the variances of each block which were produced in the previously step, now will Perform variance matching as described in section (3.1.2.g). Figure (4) illustrates the results of extracting features from fingerprint image. Table (7) shows largest match for feature points in this table, feature type is the last column where 1 for core point, 2 for delta point, 3 for bifurcation and 4 for endpoint.

Table (7): largest match for feature points

Feature position		Core match	Delta match	Bifurcation match	Ending match	Feature type
x	y					
74	136	99.9999999999997	95.6934969418086	93.4240741951056	0	1
237	234	93.2921975754341	99.9999999999994	95.0902790402499	0	2
38	99	92.5082698218601	93.7376985781088	99.9999741951056	0	3
41	138	92.9056018617444	95.4632328264831	99.9992790402499	0	3
106	180	99.1858451512205	94.9692564959883	99.9988781951056	0	3
154	204	94.7812098809957	93.4373409552182	99.9999999999992	92.4822913703269	3
166	36	94.7756831210265	95.0573769081595	99.9999999999993	0	3
214	80	98.8548312110211	94.1355260006473	99.9999999999996	0	3
215	47	95.1020288823191	91.849037851303	99.9999999999998	0	3
50	205	93.1512553742612	96.1716782812274	92.6660558199812	99.9999941951033	4
60	38	95.0792425729754	95.2777957563352	94.4647595954505	99.9999930402477	4
101	213	95.0344705341812	96.1763434399121	94.4692505349539	99.9999911951023	4
108	157	92.6687129483537	93.722836767945	95.4371121362432	99.9999790402488	4
140	134	92.605356157641	91.8896860417537	91.1315312674244	99.9996541951056	4
150	230	92.7372750981964	93.8318201262524	95.0419976784059	99.9954990402477	4
202	214	94.7224844673222	95.7535006853598	90.99648441643	99.9999999999991	4
207	116	93.0425396805441	94.5332582856652	97.2930452807276	99.9999999999993	4
207	152	95.1159352584475	95.2872306951873	97.2957803662206	99.9999999999995	4
215	127	98.1963736660011	92.4644054564638	94.6679995810491	99.9999999999996	4

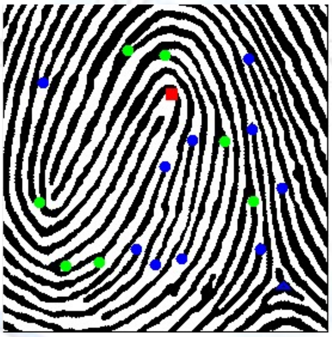


Figure (4): Features extraction results in fingerprint image. Red box denotes the core point, blue triangle denotes the delta point, blue circle denotes the end point and green circle denotes the bifurcation point

4.2 Unique ID Generation

In the case of the fingerprint image contains the core point as described in section (3.2.a), the unique ID generation process must apply the Region of Interest (ROI) centered around the core point so that only the minutia points (ridge bifurcation and ridge ending points) which are inside ROI are taken and draw circles in clockwise direction in region of interest by applying parametric equation of a circle as shown in Figure (5). Table (8) shows the results of applying the unique ID generation process.

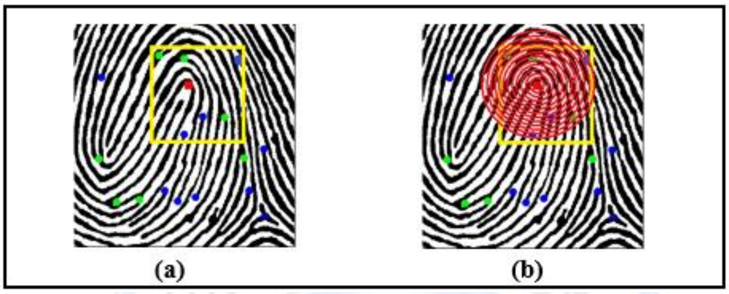


Figure (5): (a) Image after applying ROI, (b) Illustration of circles in ROI

Table (8): calculate the angles and a unique ID

core position		Minutiae position		angle	integer angle	priority
x	y	x	y			
74	136	41	138	273.499999999994	273	P1
		108	157	58.3000000000006	058	P2
		38	99	223.499999999992	223	P3
		106	180	35.6000000000002	035	P4
		140	134	90.8999999999991	090	P5
		50	205	341.000000000009	341	P6
Unique ID			273058223035090341			

While in the case of the fingerprint image does not contain the core point as described in section (3. 2. b), the unique ID generation process must calculate the distance between each point and the rest of the other minutia points which are marked in the fingerprint image by using the Euclidean distance equation. After finding the less distance between any two minutia points and computing the midpoint which is considered as the core point of the fingerprint image, now the region of interest in fingerprint image and draw circles in clockwise direction in region of interest by applying parametric equation of a circle will be applied as shown in Figure (6). Table (9) shows the results of applying the unique ID generation process.

.

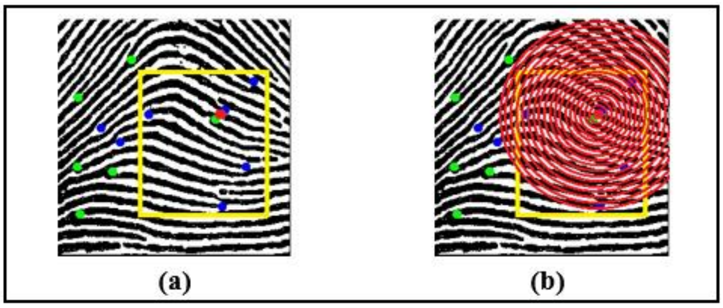


Figure (6): (a) Image after applying ROI, (b) Illustration of circles in ROI

Table (9): calculate the angles and a unique ID

core position		Minutiae position		angle	integer angle	priority
x	y	x	y			
170	99.5	174	96	323.200000000005	323	P1
		166	103	123.599999999997	123	P2
		204	64	314.500000000003	314	P3
		195	153	64.4000000000006	064	P4
		96	97	180.799999999994	180	P5
		167	194	91.1999999999991	091	P6
Unique ID				323123314064180091		

Conclusions

1. Fingerprint is useable in biometric identification systems because of its uniqueness, stability for a long time, and is rich in information such as local features (end and bifurcation points) and global features (core and delta points).

2. This paper suggests an easy and inexpensive counterfeit-resistant system for generating a unique ID for confidential documents depending on the core-point of the finger-print.

3. If the fingerprint image does not contain the core point such as the plain arch and tented arch patterns then we must create the center point in this fingerprint image and this is considered as the core point. The minutia features will be computed with this point as the reference point and this is used to generate a unique ID.

4. The analyzing of the suggested approach shows the fact that the system has quite good parameters of performance.

5. Ease of use and power performance are the basic properties of the proposed method.

References

1. Ambadiyil S., Soorej K. S. and Pillai V.P.M.,*" Fingerprint's Core Point based Unique ID generation for Security Document"* International Conference on Electrical, Electronics, Signals, Communication and Optimization (EESCO) , 2015.
2. Kodgire S. and Mohan G.," Automatic Fingerprint Recognition Systems: A Review", International Journal of Electronics, Communication & Soft Computing Science and Engineering, SSN: 2277-9477, Volume 3, Issue 3, 2012.
3. Ponnarasi S. S. and Rajaram M.," Impact of Algorithms for the Extraction
4. of Minutiae Points in Fingerprint Biometrics" Department of EEE, Information and Communication Engineering, Government College of Engineering, Tirunelveli, India, Journal of Computer Science 8 (9): 1467-1472, 2012, ISSN 1549-3636.
5. Dr. Chandra E. and Kanagalakshmi K.," Noise Elimination in Fingerprint Image Using Median Filter" International Journal Advanced Networking and Applications, Volume: 02, Issue: 06, Pages: 950-955 (2011).
6. Keyes L. and Winstanley A.," Using Moment Invariants for Classifying Shapes On Large-scale maps" Department of Computer Science, National University of Ireland Maynooth Co. Kildare Ireland, Enterprise Ireland's Strategic Research Grants scheme
7. 1998.
8. Sonka M., Hlavac V. and Boyle R.," Image a Processing, Analysis, and Machine Vision" AMATLAB Companion. Thomson Engineering, 2008.
9. Yang J. C. and Park D. S. ," Fingerprint Verification Based on Invariant Moment Features and Nonlinear BPNN" International Journal of Control, Automation, and Systems, vol. 6, no. 6, pp. 800-808, December 2008.
10. http://www.mathopenref.com/coordcirclealgorithm.html.
11. https://en.wikipedia.org/wiki/Euclidean_distance.
12. https://en.wikipedia.org/wiki/Midpoint.