ISSN 2047-3338

Design of a Fingerprint Biometric Authentication Technique for Electronic Examination

Mohammed Babatunde Ibrahim[1], Abubakar Usman Othman[2], Olumide Sunday Adewale[3] and Bukola Fatimah Balogun[4]
[1,2]Department of Computer Science, Federal University of Technology Minna, Nigeria
[3]Federal University of Technology Akure, Nigeria
[4]Department of Computer Science, Kwara State University, Nigeria
[1]othmannyya2016s@gmail.com, [2]imbamok@gmail.com, [3]adewale@futa.edu.ng, [4]arinolafula87@yahoo.com

***Abstract*– The rapid growth of online examination using internet based tools in lieu with increasing reliance on technology and other shared resources has revolutionized the way authentication is being initiated and carried out in this information age. The unprecedented growth in electronic examination (e-exams) has underlined the need for more secure, faster and more suitable method of user's verification than passwords can provide. Despite, the numerous advantages of biometric systems and its impact on various sectors across the globe, most users still face the issue of defining the right and accurate biometrics technology system in solving particular problems. This paper addresses the issue of accuracy by proposing an image enhancement approach that incorporates SecuGen fingerprint in conjunction with electronic learning environments to curb unethical conducts associated with electronic examination in a university environment. Minutiae points which are one of the unique features of fingerprints were extracted using the Crossing Number (CN) Concept by extracting the ridge endings and ridge bifurcations using the local neighborhoods of a ridge pixel from a 3 x 3 window. At authentication stage, the fingerprint is captured again with the extracted features compared with the templates stored in the database to determine a match before a student can login to write an examination.**

***Index Terms*– Fingerprint, Biometric, Electronic Examination, Learning and Authentication**

I. INTRODUCTION

INFORMATION Technology (IT) has improved our lives and provided us with a new dimension of thinking and doing things. IT has had effects in all aspects of human endeavour. The World Wide Web (www), an aspect of IT is one of the inventions of computer technology which has wide spread in all aspect of life. In many institutions and academic organizations, examination is a very important criterion which is used for students or employee's grading, assessing, and promotion. Today, many industries as well as schools are experiencing technological innovation and changes in the mode in which they carry out their operations. Learning through the web is a new idea from the internet which is known as electronic learning (e-learning) [1].

One application of e-learning is Electronic-examination which is made in assessing student's knowledge through recent computer machinery which has no effect on the conventional institution of higher education course examination comprising of invigilators, Pens and Papers. Electronic-examination can improve the standards of student's examination whereas the conventional examination system using the pen and paper requires more effort on the part of students and invigilators. Online (electronic) examinations are considered an important source for university examinations, and the development of network technology polices has given the possibility to conduct the examinations online [2]. Questions used in e-exams include set of multiple choice objective tests and quiz that can be evaluated online.

Since the inception of e-learning, there has been a security breach as it poses various threats especially when exams are held electronically (online). Security is one of the challenges of both traditional and online-based examination system. One way to mitigate security breach during online examination is to identify, authenticate and monitor candidates during online examination. Double submission of work was also done as students can re-take that same examination by simply re-clicking on the course code [3].

One important issue in institutions and business is the need for security and authentication with biometric authentication being one of the exciting technological improvements looks set to provide and also change the way majority of individual lives.

Due to its distinctiveness and compactness, fingerprint plays an important role in many aspects where an individual needs to be identified/verified. Fingerprint consists of oriented texture of interleaving ridges and valleys, which is one of the uniqueness of a fingerprint. It also consists of a pattern of minutiae which are the endpoint and merging points of ridges. Template extracted by minutiae represents a compact fingerprint which leads us to believe that duplicating a fingerprint is not possible from a minutiae template. A biometric system is designed to solve a problem of matching an individual, through the behavioural and physiological body features of individuals. It works in two ways; an individual must have registered in a system where the templates are saved in a database. The system then processes the output with an algorithm used in processing the templates during registration which is compared with what is in the database. Verification is considered successful, if a given threshold in the algorithm has been met, otherwise it is considered unsuccessful [4].

The innovation and presence of information technology has led to the present day means of examining students using electronic systems which is bound to replace the paper or manual method characterized by impersonation, excessive examination leakages, bribing of lecturers, invigilators and supervisors of examinations. In Federal University of Technology, Minna, students' examinations can either be taking in two ways; pen-on-paper or electronic examination.

II. RELATED WORK

A number of related works exist on the application of different methods and principles to effectively apply biometrics to electronic-examinations. The use of biometrics in electronic learning has been projected by researchers.

The authors in [5] presented a technique that merged numerous biometric traits in the field of e-learning. They made use of Fingerprint with mouse dynamics (FP-MD) and fingerprints with hand geometry dynamics (FP-HGD) using intelligent security agents. [6], put forward a model integrating random fingerprint biometrics user verification during exam taking in e-learning courses. In their approach, a webcam was required to monitor student's activities while taking exams and another requirement was the use of high speed internet connection, proctor devices were also used as alerts were sent to it, if it was someone else other than the real person that was writing the exams. Problems encountered included; inconvenience on the part of the user as well as user interference. The authors suggested that fingerprints matched should be in an implanted device rather than a server and that the server should only receive signal from the device as it will guide the system against security compromise.

In [7], the use of face images captured online by a webcam in Internet environment was presented to verify the attendance of individuals offering courses in online education. The problem encountered here was that during the cause of taking the examination, if the server goes down or interrupted different activities might take place before it is restored, users were also afraid of the system laser that scans the face during identification process.

Authors [8], presented a model using fingerprints for electronic examinations. In his work, challenges encountered were the authentication of students so that unauthorized individual(s) are not permitted to upload submissions or access information from another location. Secondly, double submission by the same students was allowed in the previous system and the electronic examinations were not held at a supervised location. He proposed the use of liveness detection to detect fake input and the use of intelligent security agents (fingerprint mouse and keyboard application).

[9], proposed a replica for Electronic Examination in Nigeria where every candidate is to take their examination through the web or intranet so as to reduce the malpractices as projected by the Joint Admissions Matriculation Board (JAMB), the institution given mandated to conduct examinations for candidates in higher institutions in Nigeria. Covenant University, Ota was where the model was designed and implemented. Their result shows the model having the capability to reduce unethical conducts linked with conventional methods of examination such as impersonation.

[10], employed software that performs examination for students and get their score immediately they are through with the examination. The system conducts examinations, answers collection, automatic marking, submissions and reports generation for the test and also supports varieties of questions. It is suitable for both the remote and local examination since it is used over the internet. The system assists tutors in creating examination questions or make modifications for students partaking in the examination. AJAX, PHP, HTML and MySQL are all open source technologies used in building the system. Auto-grading unit was generalized to allow examination and question types. Mansoura university quality assurance centre was used to test the system. The test proved the validity of using this kind of web based systems for evaluating students in the institutions.

[11], opined that all computers need to be audited if they are to be used for examinations. But it becomes difficult to secure computers connected to the internet and examinations that require longer time also require safety measures. To implement the proposed system, new security features have been put in place during the process of development and design. Validation of users and identification using fingerprint have been integrated with the proposed system to improve examination security. Hence, to increase the security of online examination the current research proposes the development of a fingerprint biometric authentication technique for electronic examination.

Authors in [12], proposed an efficient authentication system on biometrics. In their research Image enhancement based on Gabor filter and Crossing Number technique for extraction of minutiae was used. They had an accuracy rate of 99.75%, as well as (FAR = 0.085% and a FRR = 1.4%).

In [13], the authors proposed Fingerprint authentication System using Minutiae Extraction Technique with an accuracy rate of 75%. Their model integrated methods in building a minutia extractor and a minutia matcher was introduced. Segmentation in addition to operations using morphology to improve the thinning, false minutiae removal, minutia marking. They made use of Histogram Equalization and Fast Fourier Transform (FFT) for their image enhancement on fingerprint and for minutiae extraction crossing number concept was used.

[14] proposed phase correlation using a new minutiae-based fingerprint matching algorithm, which defined a new representation called Minutiae Direction Map (MDM) which is done by first converting the sets of minutiae into two-dimensional (2D) image spaces with transformation parameters calculated using their proposed phase correlation between the two MDMs to align the fingerprints so that they can be matched. The distance between the two minutiae sets determines the fingerprints similarity scores. The accuracy of their system was not available but they had an equal error rate of 2.44%.

A technique was presented in [15] and was used implement a minutiae based fingerprint using crossing number concept. In their research, they proposed a three phase method for their algorithm consisting of image pre-processing, use of crossing number to extract minutiae and comparing the pre-processing with the extracted munitiae with the templates in the database. Their implemented system had an accuracy of 99.77% with a (FAR = 0% and FRR = 0.23%).

The thrust of the related works only performed image enhancement on fingerprints authentication system without integrating it with an electronic examination platform, while other authors who incorporated fingerprint biometrics within an electronic examination platform did that without performing image enhancement on the templates. This study therefore, intends to incorporate an image enhancement process based fingerprint technique within an electronic examination platform with a view of carrying out an accuracy evaluation on the system.

In designing a biometric (fingerprint) system, the following must be taking into considerations: selecting the designated hardware and software components is important and both must be integrated to work together, managing poor quality templates (image enhancement), defining the right system working mode (identification or verification), programming language exceptions as well as the optimization and administration policy.

A) The Biometric Fingerprint System

Fingerprint Technology

A fingerprint is an impression of the friction ridges of all or part of the finger. This friction ridge consists of a raised segment of the fingers, toes, skin or palm which consists of one or more ridge units of the ridge skin. Dermal is also called ridges. The use of ink in getting the fingerprint on a piece of a paper was the conventional way which is then scanned using a scanner. But of recent, modern fingerprint scanner which captures live images are now being used and they include (optical, thermal, silicon or ultrasonic) [16]. The optical fingerprint scanner is the most popular among them and is based on reflection changes at the spot where the papillary lines of the fingers touch the surface of the scanner. The light sensor, source of light and a special reflection is what the optical reader consists of, and changes reflection based on the pressure. Most of the readers consist of memory and processing chips. The fingerprint obtained from an Optical Fingerprint Reader is shown in Fig. 1.

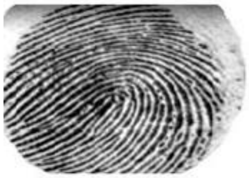

Fig. 1. Fingerprint obtained from reader (Debnath *et al*, 2009)

There are two techniques used for fingerprint matching. One is Minutiae based technique and Correlation based technique. A minutiae point is found when the finger is placed on the scanner and their relation is mapped, while the exact position of a registration point affected by image rotation and translation is known as Correlation based technique.

B) Fingerprint Sensors

The uniqueness and permanency of a fingerprint makes it the world most accepted form of biometric identifiers. In fingerprints, the area of high sensitivity is called ridges while the area of low sensitivity is called valleys. The discriminating features in the pattern of ridge flow is used for minutiae, which makes a fingerprint sensor read the surface of the scanner and converts the analog interpretation into a digital form by using the analog-to-digital converter (ADC).An *RF* sensor is used for acquiring fingerprint from the skin's moist and conductive boundary electrically and the live cells begin to turn to keratinised skin. The live part of the subsurface layer is the origin of the fingerprint pattern, and rarely affected by damage or wear to the finger surface [17].

The main parameter that characterizes fingerprint sensors includes number of pixels, resolution, area, and dynamic range. Dots per inch (pixel) is used in measuring resolutions, and higher resolutions allows for better definition between ridges and valleys and minutiae points of finer isolation which plays the role of matching fingerprint as most algorithms rely most on the coincidence of minutiae to determine if two templates are the same. Resolution and area is used to derive fingerprint image from the number of pixels, and the dynamic depth or range is used to denote the number of bits used to encode the intensity of each pixel.

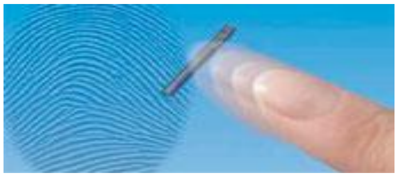

Fig. 2: Typical fingerprint and finger being swept over a sensor (Sharat, Alexander and Venu, 2006)

III. DESIGN

A) Fingerprint-based system for e-examination

After a study of the security challenges of electronic examination, a new fingerprint biometrics solution for electronic examination identification and verification was proposed. The architecture of the proposed system is

B) Biometric system

Fingerprint Image Acquisition

In this research, SecuGen fingerprint optical scanner was used for fingerprint image acquisition. This is because the pattern of the ridges and valleys of a person's fingerprint surface fingerprint is unique. A single curve segment on a fingerprint is known as ridge while a region between two adjacent ridges is known as valleys. Ridge endings and ridge bifurcations are the two major types of minutiae points which are used for uniqueness determination of an individual's fingerprint. Research has proposed several methods for enhancement of fingerprint images Binarisation Method as well as other methods.

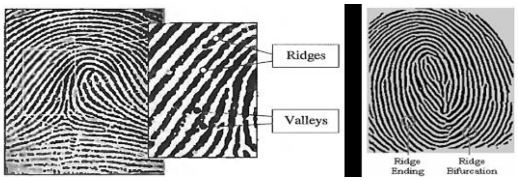

Fig. 3: Ridges and valleys of a finger (Hatim, 2009)

Therefore, the proposed system uses the features of minutia fingerprint for extraction for students writing electronic examination. The algorithm considered for matching minutiae is a triplet m = {x, y, θ} which indicate x, y location coordinate of the minutiae (distance from the origin) and angle θ of the minutiae (destination between x and y). Minutia is gotten by the extraction of samples from same set of fingerprints and storedas a set of points in two-dimensional (2D) plane. For feature extraction, the description of its location (indicating x, y coordinates) and orientation $(\theta)$is found based on the ridge endings and bifurcation of the input from the fingerprint images as shown in Fig. 4.

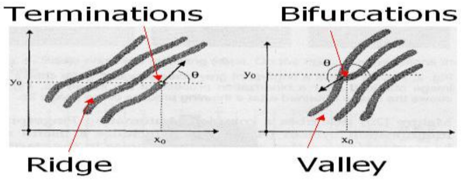

Fig. 4: Ridge ending and bifurcations minutiae coordinate (x, y) and minutiae orientation (θ) (Hatim, 2009)

C) Fingerprint Image Enhancement

One important characteristic is the ridge structures of a fingerprint image as this is what carries the information of the feature characteristics required for minutia extraction. The quality input of the fingerprint image for the performance of extracting the minutiae algorithms. Therefore, improving the clarity of the ridge structure is the purpose of the algorithm enhancement in the regions recoverable while the region unrecoverable is marked as too noisy for processing further. Therefore, enhancement of fingerprint print image is often deployed for noise reduction and improves the definition of ridges against valleys (Raymond, 2003). Below are the stages of enhancement performed on the fingerprint image.

Segmentation in image enhancement algorithm is the first step. It involves removing foreground regions from background region from the fingerprint image. An area of interest is the foreground regions which correspond to the fingerprint area that is clean which contain the valleys and ridges. The background corresponds to the region outside the borders of the fingerprint area (Raymond, 2003). Variance Thresholding (VT) is employed to separate the foreground from the background, in VT, the grey-scale variance is calculated when the image is divided into blocks. If the global threshold is lesser than the variance, the block is assigned to a foreground region. Otherwise, it is assigned the background region, the grey-level variance for a block of size. WxW image is defined as:

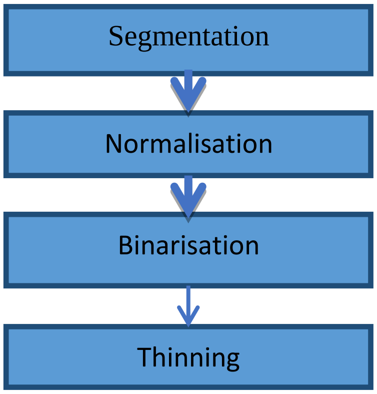

Fig. 5: Image Enhancement Process

$$\text{Var (k)} = \frac{1}{D2}\sum_{i=0}^{D-1}\sum_{j=0}^{D-1}(B(i,j) - M\ (k))^{2} \qquad (1)$$

Where Var(k) is the variance for block k, B(i,j) is the grey-level at pixel (i,j) and M(k) is the mean grey-level value for block k.

Normalization is the next step after image segmentation, where the intensity values are normalized using the image modified by the values of the grey-level range lying within a designed range values. Let I(i,j) represent the grey-level value at pixel (i,j) and the normalized grey-level value be represented by N(i,j) at pixel (i,j). The normalized range is defined as:

$$N(\mathrm{I,j}) = \begin{cases} \mathrm{M}_0 + \sqrt{\dfrac{V0\ (I(i,j)-M)2}{v}} & \text{If } \mathrm{I(i,j)} > \mathrm{M}, \\ \mathrm{M}_0 - \sqrt{\dfrac{V0\ (I(i,j)-M)2}{v}} & \text{Otherwise} \end{cases} \qquad (2)$$

Where M and V are the estimated mean and variance of (i, j).

Thinning is the last image pre-processing/enhancement step, which is a morphological operation that mops up the pixels in the foreground from the binary image until they are one pixel wide. Applying an algorithm used for thinning for a fingerprint image presents the connectivity of the ridge structures which forms a skeletonised version of the binary image required which are required for the extraction of minutia.

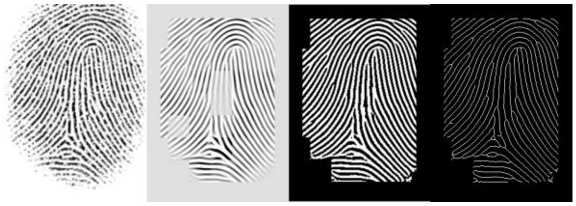

Fig. 6: (a) Original Image, (b) Enhanced Image, (c) Binarized Image, (d) Thinned

Crossing Number (CN) Concept

This concept involves the use of the skeleton image where the ridge flow pattern is eight-connected and scanned in an anti-clockwise direction and is the most commonly employed concept for minutiae extraction (Raymond, 2003) and (Roli, Priti and Punam, 2011).

P_4	P_3	P_2
P_5	P	P_1
P_6	P_7	P_8

Fig. 7: 3x3 Neighborhood

This concept is highly preferred over others because of its computational efficiency, improved localization, higher sensitivity and inherent simplicity. Extracting the minutiae is done by scanning the local neighborhood of the image pixel based on the ridges from top to down, left to right in order to detect ridges using a 3 x 3 window. This concept is computed using equation (3) defined as half the sum of the differences between pairs of adjacent pixels in the eight-neighborhood.

Table I: Crossing Number property

CN	Property
0	Isolated Point
I	Ridge ending point
2	Continuing ridge point
3	Bifurcation point
4	Crossing point

The ridge pixel which has been detected as a 3x3 window is then classified as a ridge ending (1), bifurcation (3) or non-minutiae point (0,2,4). The formula is given in equation (3):

Table II: Description and Specification

S/N	Description	Specification
I	Image size/ resolution	260 x 300 pixels/ 500DPI
ii	Fingerprint capture time	0.2~0.5 seconds (smart capture
iii	Sensing area	inclusive)
iv	Typical lifeline / Light	13.2 x 15.2
v	Source	60,000 hours / LED
vi	CPU/ Flash Memory	400MHz ARM/ 32MB
vii	Storage Capacity	3,000 users (1:1 0r 1:N)
viii	Minutiae Extraction time	<0.4 second
ix	Matching Time (1:1)	<0.1 second
x	Matching Time (1:N)	<0.2 second
xi	Fingerprint Template	SecuGen, INCITS 378, ISO
xii	Communication speed	19794-2
xiii	(maximum)	460,800bps (RS 232, CMOS
xiv	External Interface	Serial)
xv	Dimensions /Weight	RS232 Serial, Wiegand, GPIO
xvi	Supply Voltage	59 x 43 x 8 mm / 16g
xvii	Current Consumption	3.3V DC
	Operation Temperature	120mA (idle), 320mA
	Operation Humidity	(operation)
		$-20^{o} \sim 65^{o}$C
		90% or less RH, non-
		condensing

$$CN = 0.5 \sum_{i=1}^{8} |P_i - P_{i+1}| P_9 = P_1 \qquad (3)$$

Where Pi is the pixel value in the neighborhood of P with Pi = (0 or 1).

For a pixel p, the eight pixels are scanned in an anti-clockwise direction from top to down, left to right in order to detect ridges. The pixel can be classified after obtaining its pixel value. The orientation, coordinates and minutiae types of the ridge segment and type of minutiae of each minutiae point is recorded for each minutiae. After the minutiae has been successfully extracted, the template is stored, which then contains the minutia position (x, y), minutia direction (angle), minutia type (bifurcation or termination) and these parameters are later used for minutia-based matching algorithm in this thesis.

D) Template Generation for Fingerprint

At this stage, the minutiae feature of the fingerprint image is extracted and a template is generated after the student must have enrolled. This involves defining a 3 x 3 window size pixels centred at the black pixel. The algorithm then finds the number of pixels N, within the size which determines the minutia features which is shown in the algorithm section. The extracted template is stored along with the students other bio-information in the database.
Source: SecuGen (2015)

E) Electronic Examination System

The proposed electronic examination system consists of primarily two parts:

i. The Frontend Webpage
ii. The Backend Database

The Frontend Webpage

This application consists of an initial Login screen which asks the students to present his/her enrolled fingerprint for verification before proceeding to write the examination, if a defined threshold has been met. For new students, there is an option for Signing Up by giving their details.

After Sign-Up, the details are stored in the database managed by MySQL. The Fingerprint is stored in “SHA1” Encryption Format, thereby adding to the security. Each time the student tries to Login using the biometric scanner, the scanned fingerprint is matched with the stored template in the Database, which if successful is allowed to continue to the Welcome Screen.

The Welcome Screen has Provisions for Log out as well as taking the Examination/ Test. If the option for the Examination/ Test is selected, the user is directed to the questionnaire which is connected to the Question Generator Database, from where random Questions are generated using random function. This page also has an embedded JavaScript code which maintains a timer, and redirects to the results page as soon as the time gets expired. The results are calculated comparing the input from user to the answer stored in the database. The Score is stored by a Server-side Counter which displays the results. The result is then stored in the Results Database, where the track of attempted and correct questions are kept. Then the User logs out from the session once he/she is done writing the examination.

The Backend Database

This is where the enrolled student's information is saved as well as the generated templates. Questions being uploaded, displayed, policy settings (time, date, number of questions, and mark per question) editing is done the administrator at the backend. This is developed using PHP and MySQL.

F) Development Life Cycle of the fingerprint biometric authentication System for electronic examination

The development of the electronic examination system is based on the waterfall model. Five stages in software development model are viewed, where the activities of one stage will be completed before the next stage is implemented. Phases involved in the Waterfall Model are:

i. Requirement Analysis and Definition
ii. System and Software Design
iii. Implementation and testing
iv. System testing
v. Maintenance

Requirement Analysis and Definition: This phase defines the scope and peculiarity of the problems involved. In other for the proposed system not to suffer the same setback as the existing system, the researcher design an electronic examination system based on fingerprint biometric system for authenticating students about to write examination.

System and Software Design: The specification required for the system design of the first phase was studied which also helped in specifying hardware and software components and to help in defining the overall system architecture. This includes the use of Unified Modeling Language (UML) and its use cases.

Implementation and Testing: The actual development of the system takes place in this phase by the designing the graphical user interface, implementing the model using HTML, PHP, JavaScript and creating the database using SQL server.

System Testing: This is the stage after coding where every unit of the program was tested and integrated as a complete system in order to ensure the system works according to required specification.

Maintenance: This is the final stage of development in which all necessary maintenance activities were carried out in order to see that the software continues to work even when there is a new development in the future.

After the students must have filled the necessary information needed and fingerprints been enrolled, the algorithm attempts to find a match between the previously stored (S) templates and a new live (L) templates, before the students can proceed to write an examination. Therefore, in matching the sets of minutia, S is taken from the database and L is the test / live fingerprint. S and L are said to be paired if their minutia type are close in direction, and position and their minutia are the same.

Here, (M^1, M^2) are set of minutia features that are matched. Their displacement (in x and y = D_m) and rotation (θ = A_m) are recovered respectively. According to Ghazali (2005), let S_m be a set of matched pairs of each element in S_m has the form $(M^1_{1,}M^2_1\ )$ whereM^1_1, is from S and M^2_1 is from L. There are two constrains to S_m.

All M^1_1, M^2_1should be different which implies that each minutia in S and L should not be matched more than once. Therefore, the following condition must also be satisfied if(M^1_1, M^2_1) and(M^1_2, M^2_2) are two element in S_m

DIST $(M^1_1, M^2_1) - \ DIST\ (M^1_2, M^2_2)$ / <b, where b is a small value.

The next process involved therefore is to perform a similarity score Q as shown Fig. 7 by simply normalizing the matched minutiae element (representing k) with half the sum (m + n) / 2 of minutiae set in S and L.

$$\text{Score } (Q) = \frac{2k}{m+n} 3.7$$

where m = number of minutia in S
n = number of minutia in L

G) Pseudo-codes

Algorithm for Crossing Number Concept Algorithm

```
Step 1:   Scan the local neighborhood of each ridge pixel in the image derived from thinning from top to down, left to right in order to detect ridges using a 3 x 3 window and set J =1.
Step 2:   At point P, centre the J^th 3 x 3 window
Step 3:   Compute crossing number $CN_J$ for window J using
          $CN = 0.5 \sum_{i=1}^{8} |P_i - P_{i+1}|, P_9 = P_1$
Step 4:   If ($CN_J$=1) then
              Centre point P in window J is said to be ridge ending
          else if ($CN_J$=3) then
              Centre point P in window J is said to be ridge bifurcation
          End it
Step 5:   Increase J by 1 and repeat step 2 and 3 until all 3 x 3 windows have been checked.
Step 6:   Store the output in step 4 as a template which will later be used for matching
Step 7:   Stop
```

Pseudo-code for Fingerprint template Generation

```
Step 1:   Start
Step 2:   Scan the fingerprint thinned image t and generate a new template $t_p$ from the thinned image
              For i = 0 to N -1 where N depicts number of rows
                  For j = 0 to M-1 where M depicts number of columns
```

```
            -   Scan the thinned image T from the
                origin point and find any black pixel
            -   A 3 x 3 window size in centered at the
                point
            -   Count the total number of black pixels
                within the 3 x 3 window as N
                If (N=2) point is ridge endings
                If (N=3) point is ridge continuity
                If (N>3) point is ridge bifurcations
                end j
                endi
step 3:   Output the template $t_p$
step 4:   Stop
```

Pseudo-code for template matching

```
Step 1:   Set K=1, $S_{count} = 0$
Step 2:       Get the minutia sets S and L for each
              fingerprint template $t_1$ and $t_p^k$ respectively
              where $t_1$ is the test/live template and $t_p^k$ is
              the enrolled template of position k in the
              database.
Step 3:       For each of the sets S and L, the minutia
              type is obtained e1 and e2, coordinates c1
              and c2 of the corresponding minutia type,
              $\theta 1$ and $\theta 2$ for the orientation angles of the
              minutia points for sets S and L $\epsilon$ $t_1$and $t_p^k$
              respectively.
Step 4:       Compare if S and L are paired such that:
              If (type (e1) type (e2)) and
              Dist (c1,c2) $\leq D_T$) and
              (ANGLE ($\theta 1$, $\theta 2$) < $A_T$) then
              Increase $S_{count}$ by 1
              Go to step 2 until no more sets to pair
              else
              Go to step 3 until no more sets to pair end if
Step 5:       Get the total number of sets in $t_1$ call it m
Step 6:       Get the total number of set in $tp^k$, call it n
Step 7:       Compute the similarity score Q between $t_1$
              and $tp^k$ using
              $Q = 2 * k / (m+n)$
Step 8:       Compare the origin of the two fingerprint
image
              If (Q > = T) then        (where $T = Q - (c/(n+m) * 0.5)$
           Set match = True
              Else
                  Set match = false
                  Increase N by 1
                  Go back to step 2
     End if
Step 9:   Stop
```

H) Unified Modelling Language

Although, this system is developed using Object Oriented Design (OOD) techniques, it may be useful to identify the overall requirements in functional terms. According to Dale (2005) "built functional models is one of the weaknesses of OOD methods within the objects" from the above, this can lead to requirements being dismissed because "the requirement needed to build the system must be understood" Dale (2005).Therefore, this thesis, uses a process of requirements engineering (RE) to complement OOD modelling using the Unified Modelling Language (UML). UML is used to specify, visualize, modify, construct and document the artifacts. So also the building block of UML is diagram.

The above diagram provides an outline of the required components of a fingerprint system. The use case diagram is a behavioural unified modelling language (UML) diagram that presents system functionality. In this system, the actors' depicted represent Users (students), finger prints scanner, client, server and database. When the students decide to write an e-exam, the first step he/she does is to present required finger (thumb) in the fingerprint scanner. The scanner then performs a number of roles; it has to authenticate the fingerprint presented by the user and confirm the user details with other components in the system.

The student presents the finger (thumb) for verification when he/she wants to write the examination using the proposed system, the system extracts the presented fingerprint and then tries to match the fingerprint with the template generated during the time of enrolment and compares with the database, if successful the student proceeds to write the examination, otherwise it rejects the student.

V. CONCLUSION

Traditionally, students' authentication during electronic examination is done in the conventional way (username and password). Therefore, the implementation of an electronic biometric method of authentication will greatly assist institutions and organizations thereby prevent time consuming process. Employing a more simplified, reliable and efficient model for authenticating students writing electronic examinations based on biometric is formulated and implemented. This system provides both the students and administrators with ease of access to information needed as well as monitoring of the students by the administrators. This will increase the productivity of institutions and organizations.

Experiments were conducted using SecuGen fingerprint reader to capture live image of students and image enhancement was performed using crossing number concept to extract the enhanced images so as to improve the image quality. It was coded using Java (NetBeans IDE 7.4) to implement algorithms for enhancement, minutiae extraction and matching processing, where the resulting minutiae information was used as a method for identifying and matching fingerprints. The naturalness in the use of fingerprint makes it a better method for access control as this will dissuade students from carrying identity cards or other known documents for identification and authentication during electronic examinations explains the ease of use.

REFERENCES

[1] Y. Takahashi, T. Abiko,, and E. Negishi, “An Ontology-based System for Network Security’, IEEE. Using Biometrics Authentication via Fingerprint Recognition, *the 4th Saudi International Conference*, 1(1), 2010, 1-2

[2] S. Mohammed, and M. Ilyas “Challenges of Online Exam, Performances and problems for Online University Examination. *International Journal of Computer Science Issues*, 10(1-1), 2013, pp. 439-443.

[3] K. M. Apampa, G. B. Wills, D. Argles, and E. Marais, “Electronic Integrity Issues in E-assessment Security”. *Proceedings of 8th IEEE International Conference on Advanced Learning,* Spain, 2013. Available at: http://eprints.soton.ac.uk/id/eprint/265892. Retrieved on March 6th, 2016.

[4] Qinghai, G. “Online teaching: Do you know who is taking the final exam? *Fall 2010 Mid-Atlantic ASEE Conference, Villanova University, United State of America (USA)* (2010).

[5] K. Rabuzin, M. Baca, and M. Sajko, “E-learning: Biometrics as a Security Factor”. *International Multi-Conference on Computing in the Global Information Technology* (ICCGI'06), 2006, 64.

[6] Y. Levy, and M. M. Ramin, “A Theoretical Approach for Biometrics Authentication of e-Exams, 2007. Available at: http://telem-pub.openu.ac.il/users/chais/2007/morning_1/M1_6.pdf, Retrieved on March 8th, 2016

[7] B. E. Penteado, and A. N. Marana, “Video-Based Biometric Authentication for e-Learning Web Applications. *Enterprise Information Systems. Lecture Notes in Business Information Processing*, 24(4), 2009, pp. 770-779.

[8] S. Alotaibi, “Using Biometrics Authentication via Fingerprint Recognition in E-exams in E-Learning Environment”. *The 4th Saudi International Conference*, University of Manchester, United Kingdom, 2010.

[9] C. K. Ayo, I. O. Akinyemi, A. A. Adebiyi, and U. O. Ekong, “The Prospects of E-Examination Implementation in Nigeria”. *Turkish Online Journal of Distance Education,* 8 (4), 2007, pp. 125-135.

[10] M. Z. Rashad, S. K. Mahmoud E. H. Ahmed, and A. Z. Mahmoud, “An Arabic Web-Based Exam Management System”. *International Journal of Electrical & Computer Sciences*, 10(1), 2010, pp. 48-55.

[11] M. R. Michelle, and L. Yair “*Towards a Framework of Biometric Exam Authentication in E-Learning Environments”*. Nova Southeastern University, Florida, USA. Idea Group Inc, 2007.

[12] L. Liu, and T. Cao, “The Research and Design of an Efficient Verification System Based on Biometrics”. *International Conference on Computer Science and Electrical Engineering.*

[13] M. Kaur, M. Singh, and P. S. Sindhu, “Fingerprint Verification System using Minutiae Extraction Technique”. *Proceedings of World Academy of Science, Engineering and Technology,* 46, 2008, pp. 497-502.

[14] W. Chen, and Y. Gao, “A Minutiae-based Fingerprint Matching Algorithm Using Phase Correlation”. Digital Image Computing Techniques and Applications, IEEE, 2007, 233-238. Retrieved 23rd July, 2015.

[15] A. S. Chaudhari, G. K. Patnaik, and S. S. Patil, “Implementation of Minutiae Based Fingerprint Identification System Using Crossing Number Concept”. *Informatica Economică*, 18(1), 2014, pp. 17-26.

[16] A. Ross, S. Dass, and A. K. Jain, “A Deformable Model for Fingerprint Matching, *Journal of Pattern Recognition*, 38(1), 2005, pp. 95–103.

[17] B. Debnath, R. Rahul, A. Farkhod, and C. Minkyu, “Biometric Authentication: A Review”. *International Journal of u- and e-Service, Science and Technology*, 2(3), 2009. Pp. 13 – 28.

[18] S. C. Sharat, N. C. Alexander, and G. Venu, G. “Fingerprint Image Enhancement using STFT Analysis”. *Journal of the Pattern Recognition Society*,4(2), 2006, pp. 198-211.

[19] A. A. Hatim, “Vein and Fingerprint Biometrics Authentication- Future Trends, *International Journal of Computers and Communications*, 4(3), 2009, pp. 67 – 75.