An Enhanced ATM Security System Using Multimodal Biometric Strategy

Mohamed A. Kassem  
Faculty of Computers& Information Sciences, Mansoura University, Egypt,  
Cs.engineer.moha.1987@gmail.com

Ngham E. Mekky  
Lecturer, Dept. of IT, Faculty of Computers& Information Sciences, Mansoura University, Egypt, nona762005@hotmail.com

Rasheed M. EL-Awady  
Professor, Dept. of Electronics and Communications Engineering, Faculty of Engineering, Mansoura University, Egypt  
Actt_egypt@yahoo.com

Abstract-- This paper presents a new biometric identification and authentication schema in relation to payment systems and ATMs. The financial sector has used ATMs as a means to make payment and offer financial services for its clients. But, security is a major issue in accessing these machines. Improving the performance of individual matchers in the aforementioned situation may not be effective. Multi-biometric systems are used to overcome this problem by providing multiple pieces of evidence of the same identity. In this paper, we have proposed the development of a fingerprint and iris fusion system which utilizes a Minutiae Matcher for fingerprint and Hamming Distance Matcher for iris with matching score level. It has been found that the proposed multimodal technique using threshold of 0.6 gave the best results. It has an accuracy of 96.67%, FAR of 0%, FRR of 5%, and run time of 32 seconds.

Index Term-- Multi-model System, Biometric, Fingerprint, Iris, Identification, Recognition, ATM, Biometric Computing, Fingerprint Recognition, IRIS Recognition, Minutiae Extraction, FAR, FRR.

I. INTRODUCTION

Automated teller machines (ATM) were first used in 1939. Nowadays, about 1.5 million are installed worldwide. There are different aspects that should be considered. One of the paramount consideration issue is security because all over the world is an increasing use of ATMs and it mean that risks of hacking turn to be a reality more than before. Nowadays there are many persons use technological progress in circumvention of humans to steal their money, like Skimming Attack, Card trapping, PIN Cracking, Phishing/Wishing Attack, ATM Malware and ATM hacking (see Figure 1)[1].

So we need to make framework with more secure and make unenlightened people able to use ATMS with quick secure way, it lead us to use biometrics which use human traits.

Biometrics refers to the identification of individuals by their characteristics or traits. Biometric identifiers are the unique, measurable characteristics used to describe individuals. Biometric identifiers are classified as physiological and behavioral characteristics. Physiological characteristics are related to the shape of the body. Examples fingerprint, face recognition, DNA, Palm print, hand geometry, recognition and retina. Behavioral characteristics are related to the behavior of a person like typing rhythm, gait, and voice. Many different aspects of human physiology, chemistry or behavior can be used for biometric authentication. The selection of a particular biometric for use in a specific application involves a weighting of several factors.

- **Universality** means that every person using a system should possess the trait.
- **Uniqueness** means the trait should be sufficiently different for individuals such that they can be distinguished from one another.
- **Permanence** relates to the manner in which a trait varies over time. A trait with 'good' permanence will be reasonably invariant over time.
- **Measurability** (collectability) relates to the ease of acquisition or measurement of the trait. And, acquired data should be in a form that permits subsequent processing and extraction of the relevant feature sets.
- **Performance** relates to the accuracy, speed, and robustness of technology used.
- **Acceptability** relates to how well individuals in the relevant population accept the technology such that they are willing to have their biometric trait captured and assessed.
- **Circumvention** relates to the ease with which a trait might be imitated using an artifact or substitute.

Fig. 1. ATM attack example
Biometrics systems were mostly used in forensic sciences, but nowadays it is mainly due to civilian applications such as controlling physical access to facilities, controlling logical access to software, and controlling voters during elections. A key component in fingerprint recognition systems is the fingerprint matching algorithm [2]. No single biometric will meet all the requirements of every possible application. But, the most widely pattern used in the identification method is fingerprint [3]. Fingerprint is based on minutiae extractor for recognition that is based on three basic steps:

A. Pre-processing
In this phase Segmentation of the fingerprint area is done to extract the region of interest and avoid extraction of noisy and background areas and increasing the performance evaluation of feature extraction. After identification of the foreground and background regions now locating ridges step. Smoothing now take place, it is performed by using one dimensional average mask in the direction orthogonal to the orientation field. Applying threshold to the image by assigning the ridge pixels to “1” and all the remaining pixels to “0” so the resulting binary image is suitable for feature extraction.

B. Processing [Minutiae Extraction]
Extraction is done by thinning the ridges so that they are single pixel wide. Then locating minutia points in the thinned image is easy by counting ‘on’ neighbors at point of interest in (3*3) window.

C. Post processing
It eliminates spurious feature points based on the structural and spatial relationships of the minutiae. Then validate the minutiae points. So a large number of spurious minutiae get deleted. This method does seem to identify most of true feature points. And the post-processing stage filters out the undesired feature points based on their structural characteristics.

Among the most amazing strengths of fingerprint recognition, we can observe that: it has a high level accuracy, low cost because of small size acquisition devices which make it widely used and also the easier way of identification [4]. But there weaknesses which may affect the recognition of the fingerprint:

- Its association with forensic or criminal applications.
- Factors such as finger injuries or manual working can result in positive users being unable to use a fingerprint based recognition system, either temporarily or permanently.
- Small area sensors may result in less information available from a fingerprint and/or little overlap between different acquisitions.

The iris is unique pattern which remains stable throughout adult life which makes it very as a biometric for identifying individuals. The unique iris pattern can be extracted from a template image of the eye. This biometric template contains a representation of the unique information stored in the iris which could be compared with other templates [5].

Image processing techniques used to convert iris pattern to unique code which can be stored in a database and allows comparisons between templates.

The overall process for acquiring and storing iris features with iris images can be listed as follow [6]:

1. Image acquisition: take photo of iris with good resolution
   and quality.
2. Segmentation: process the acquiring image for separation of iris from eye image.
4. Feature extraction and feature encoding,
5. Storing extracted codes in database and comparing acquiring iris images with codes in database.

Multiple sensors could be used as a Multimodal biometric system to overcome the limitations of uni-model biometric systems. Because of uni-model system limited to one identifier which may have some limitations as if we use iris recognition systems the features can be changed by aging iris and finger scanning systems by worn-out, wet or cut fingerprints. Multimodal system can get more information rather than a single biometric or information from different biometrics.

Organization: This paper is organized into the following sections. Section II is an overview of the related work, in section III the tools that we have used. Section IV describes the proposed model. In section V performance analysis and results are discussed and finally in section VI give the conclusions.

II. RELATED WORK
Due to gently importance and impact of biometrics techniques in security field, there is many, today, researchers attempt to build robust and stable technique that are compatible and applicable in recognition restricted environment.

Miguel Angel Medina-Perez et. al. proposed improving fingerprint verification using minutiae triplets this algorithm contains three components: a new feature representation containing clockwise-arranged minutiae without a central minutia, a new similarity measure that shifts the triplets to find the best minutiae correspondence, and a global matching procedure that selects the alignment by maximizing the amount of global matching minutiae[7].

Ghazvini, Met. Al. proposed a fingerprint matching method based on genetic algorithm. Then use the local properties of minutiae. Also there is a new kind of triangle descriptors are proposed, which uses these descriptors properties, the approximated value of transfer parameters for alignment and similarity between two fingerprints can be attained [8].
Hoyle et al. proposed methodologies use minutiae triplet-based features in a hierarchical fashion, where not only minutia points are used, but ridge information is used to help establish relations between minutiae[9].

Prabhakar, S et al. discussed the signal acquisition aspects of fingerprint and iris biometrics-two of the most widely used biometric traits. Personal recognition of people is necessary to conduct many social and economic activities. Besides visual recognition of acquaintances, checking a person's government issued photo ID is the most common procedure[10].

Anil K. Jain et al. proposed a system for matching latent images with full fingerprints that uses minutiae as well as ridge information as the discriminative features. Also, developed a minutiae-based fingerprint matcher is considered besides the specific characteristics of the latent matching problem[11].

Himanshi Budhiraja et al. proposes a biometric personal authentication system using a novel combination of iris and fingerprint. For system deployment the combination is found to be useful as one needs a close up system and other needs contact. One modality is used to overcome the limitations posed by the other [12].

III. UNI-MODAL STRUCTURE

A. Fingerprint Recognition

Fingerprint verification is a quick and appropriate method of establishing an individual’s identity among all the biometric techniques. Owing to the high complexity of matching fingerprints and the enormous amount of existing fingerprints historically, fingerprint recognition systems were mostly used in forensic sciences, but nowadays the popularity of fingerprint recognition systems is mainly due to civilian applications such as controlling physical access to facilities, controlling logical access to software, and controlling voters during elections. A key component in fingerprint recognition systems is the fingerprint matching algorithm[6]. The biological properties of fingerprint formation are well understood and fingerprints have been used for identification purposes for centuries.

The most important step in matching fingerprints is to automatically extract minutiae from the input fingerprint images. However, the performance of a minutiae extraction algorithm relies deeply on the quality of the input images. In order to ensure that the performance of an automatic fingerprint identification/verification system would be robust with respect to the quality of the fingerprint images we have to include a fingerprint enhancement algorithm in the minutiae extraction module.

- **Histogram Equalization**

Histogram equalization expands the pixel value distribution of an image to increase the perceptual information (see Figure 2). The original histogram of a fingerprint image has more number of pixels having particular intensity and lower number of pixels of other intensity to occupy all the range.

Fig. 2. Histogram Equalized Image

- **Fast Fourier Transform**

FFT is able to perform a sort of contextual filtering without explicitly computing local ridge orientation and frequency (see Figure 3).

Fig. 3. FFT Enhancement Image

- **Adaptive Binarization**

Fingerprint Image Binarization transforms the 8-bit Gray fingerprint image to a 1-bit image with 0-value for ridges and 1-value for furrows. A locally adaptive binarization method is performed to binarize the fingerprint image (see Figure 4). This method is done by transforming a pixel value to 1 if the value is larger than the mean intensity value of the pixel and transforming a pixel value to 0 if the value is smaller than the mean intensity value.

Fig. 4. Binarized Image

- **Local Ridge Orientation Image**

The local ridge orientation at a pixel \([x,y]\) is the angle \(\theta(x,y)\) that the fingerprint ridges. The simplest approach for extracting local ridge orientation is based on computation of gradients in the fingerprint image (see Figure 5). The gradient \(g(x,y)\) at point \([x,y]\) of image, is a two dimensional vector \([g_x(x, y), g_y(x, y)]\), where \(g_x\) and \(g_y\) components are the...
derivatives of image at \([x, y]\) with respect to the \(x\) and \(y\) directions.

Fig. 5. Local Ridge Orientation Image

- Segmentation and extraction the region of interest

Extracting the Region of Interest (ROI) is useful to be recognized for each fingerprint image. First discard the image area without effective ridges and furrows as it only holds background information (see Figure 6). Then in the bound region are confusing with those spurious minutiae that are generated when the ridges are out of the sensor. The method of block direction estimation is used here.

Fig. 6. ROI Extracted Image

- Minutia Extraction

Minutiae are the endings and bifurcations of the fingerprint images. The Crossing Number (CN) concept is the most common method for minutiae extraction which involves the use of the skeleton image where the ridge flow pattern is eight-connected. By scanning the local neighborhood of each ridge pixel in the image using a \(3 \times 3\) window the minutiae are extracted (see Figure 7). Then compute CN value, which is defined as half the sum of the differences between pairs of neighboring pixels in the eight-neighborhood. The ridge pixel can then be classified as a ridge ending, bifurcation or non-minutiae point by the properties of the CN. For example, a ridge pixel with a CN of one corresponds to a ridge ending, and a CN of three corresponds to a bifurcation, and if the value of the CN is two then it corresponds to normal ridge pixel.

Fig. 7. Minutia Extraction

- Thinning

Thinning is the process of reducing the thickness of each line of patterns to be a single pixel width. Thinning is a morphological operation that successively erodes away the foreground pixels until they are one pixel wide. A standard thinning algorithm, which performs the thinning operation using two sub iterations. The thinning algorithm to a fingerprint image preserves the connectivity of the ridge structures while forming a skeleton version of the binary image (see Figure 8). This skeleton image is used in the subsequent extraction of minutiae.

Fig. 8. Thinned Image

- Termination and Bifurcation

We need to remove false minutia after the preprocessing stage. For example, false ridge breaks due to insufficient amount of ink and ridge cross-connections due to over inking are not totally eliminated. Actually all the earlier stages themselves rarely introduce some artifacts which later lead to false minutia which will affect the accuracy of matching if they are simply regarded as genuine minutia (see Figure 9). So removing false minutia is essential to keep the fingerprint verification system effective.

Fig. 9. Remove H breaks and Remove spike

- Steps to Remove False Minutia

1. If the distance between one bifurcation and one termination is less than \(D\) and the two minutiae are in the same ridge. Remove both of them. (Where \(D\) is the average inter-ridge width representing the average distance between two parallel neighboring ridges).

2. If the distance between two bifurcations is less than \(D\) and they are in the same ridge, remove the two bifurcations.
3. If two terminations are within a distance D and their directions are coincident with a small angle variation. And they suffice the condition that no any other termination is located between the two terminations. Then the two terminations are regarded as false minutia derived from a broken ridge and are removed.

4. If two terminations are located in a short ridge with length less than D, remove the two terminations (see Figure 10).

- **Matching**

The matching stage takes a feature set and enrollment template as input and computes the similarity between them in terms of a matching score. If the matching score is higher than the threshold, then the decision is matched and the person is recognized as genuine. The matching process is done by minutiae matcher.

**B. IRIS Recognition**

The iris formation happens in the third month of early life and unique patterns are formed during the first year of life. These patterns are random and don’t depend on genetic factor and the only characteristic that is dependent on genetics is the pigmentation. Iris systems have a very low False Accept Rate (FAR) compared to other biometric traits; the False Reject Rate (FRR) of these systems can be rather high. Iris recognition analyzes features like rings, furrows, and freckles existing in the colored tissue surrounding the pupil. Image processing techniques can be employed to convert iris pattern to unique code which can be stored in a database and allows comparisons between templates.

- **Iris Localization**

Circle detection algorithm is used to increase the overall speed of the system (see Figure 11). Circle detection is used because of the following:

1. It has good recognition performance and speed.
2. The algorithm is able to very accurately detect even partially occluded circles.
3. The algorithm needs a very small amount of memory.
4. The algorithm creates low processing burden than other methods.
5. It is simple and efficient method.

- **Iris Segmentation**

This involves first employing Canny Edge Detection to generate an edge map (see Figure 12). Process the image for separation of iris from eye image.

- **Iris Normalization**

After successfully extracting the iris part from the eye image, in order to allow comparisons between different irises, transform the extracted iris region so that it has a fixed dimension, and hence removing the dimensional inconsistencies between eye images due to the stretching of the iris caused by the pupil dilation from varying levels of illumination (see Figure 13). Therefore, this normalization process will produce irises with same fixed dimensions so that two photographs for the same iris under different lighting conditions will have the same characteristic features.

- **Iris Feature Extraction and matching**

This is the most key component of an iris recognition system and determines the system’s performance to a large extent. Iris recognition produces the correct result by extracting features of the input images and matching these features with known patterns in the feature database. Features are the attributes or values extracted to get the unique characteristics from the image. Features from the iris image are extracted using hamming distance algorithm.

**IV. PROPOSED MULTI-MODEL STRATEGY**

The purpose of the proposed model is to achieve higher performance that may not be possible using a single biometric indicator alone. Here we must know why fingerprint and iris recognition must be used with ATM there are many reasons like the acceptance for people to use their own traits by other
mean which biometrics I can accept to use it on this place if we tell him/her to use face for recognition they will be afraid to use like this biometric may be used in the acts of bad or scandalous, another thing is ATMs devices is small to integrate a palm device with it and also who can accept to put his palm on to get his secure line so it mean usability for people to use them.
biometric so the more usability are finger and iris for human to use them in general identification and authentication and the availability to integrate devices with ATM. The proposed model is a fusion of iris and fingerprint biometrics (see Figure 14). Feature vectors are created independently for each sensor and are then compared to the enrollment templates which are stored separately for each biometric trait. Based on the proximity of feature vector and template each subsystem computes its own matching score. These individual scores are finally combined into a total score which is passed to the decision module.

In the fingerprint module a matching score has been computed using the minutiae matcher algorithm and in the iris module a matching score has been computed using the hamming distance algorithm.

When talking about ATM, one of the important requirement is timeless to get the money so we make two matching framework using the same algorithm minutiae for fingerprint and hamming distance for iris but the first technique get the max for fingerprint and iris then pass the score to the fusion equation and We know that iris processing and matching take long time cause of hard processing so the other technique is to get all fingers matching score that pass Specified threshold and compare the enrollment iris with the stored iris relate to the finger values pass the threshold and compute the fusion for iris and passed fingers then the max fusion equation that pass whole system threshold will get the access.

The integrated system also provide anti spoofing measures by making it difficult for an intruder to spoof multiple biometric traits simultaneously. Scores generated from individual traits are combined at matching score level using weighted sum of score technique.

V. EXPERIMENTAL DISCUSSION

The experiments reported in this paper has been conducted on the fingerprint images , DB1_B in FVC2004 and DB3_B in FVC2004 each containing fingerprint images of size (640 *480) pixels [13] and the iris database images is CASIA iris image database version 1.0 [14]. The database consists of 20 person each person has 7 images for finger and 7 images for iris. For each person 4 images have been used in the training phase and 3 images for test phase. Two levels of experiments have been performed. The first level tested using iris and fingerprint individually. The second level combined iris and fingerprint using proposed model.

Three performance criteria have been computed: false acceptance rate (FAR), false rejection rate (FRR), and accuracy. FAR is the probability of invalid inputs which are incorrectly accepted. While, FRR is the probability of valid inputs which are incorrectly rejected [15]. Accuracy is the proportion of true results [16].

\[
FAR = \frac{\text{Number of falsely accepted images}}{\text{Total number of persons in the database}}
\]

\[
FRR = \frac{\text{Number of falsely rejected images}}{\text{Total number of persons in the database}}
\]

\[
\text{Accuracy} = \frac{\text{No of true positive} + \text{No of true negative}}{\text{No of true positive} + \text{false positive} + \text{false negative} + \text{true negative}}
\]

Which true positive is correctly identified, false positive is incorrectly identified, true negative is correctly rejected and false negative is incorrectly rejected.

After a set of experiments have been conducted we found these results as shown in table (I) and plotted (see Figure 15). It has been found that the maximum accuracy happened when using threshold of 0.6.

We have done our experiments on windows 7, processor core i5 and RAM 4 GB to obtain accuracy and run time. Table (II) illustrated the results of using fingerprint and iris models individually. The results of the two proposed model when using threshold and without using threshold are the same. They gave FAR of 0%, FRR of 5%, and accuracy of 96.67%.

When we compute the time for the two proposed matching technique for the first technique that get the max match score for the whole system without threshold on finger the time was 44 seconds, for the second matching technique which get fusion for finger that pass threshold with its corresponding iris the time was 32 seconds. So we will use the second proposed matching technique as it take less time and it is very good with ATM.

<table>
<thead>
<tr>
<th>Threshold</th>
<th>FAR (%)</th>
<th>FRR (%)</th>
<th>Accuracy (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>100</td>
<td>0</td>
<td>66</td>
</tr>
<tr>
<td>0.1</td>
<td>100</td>
<td>0</td>
<td>66</td>
</tr>
<tr>
<td>0.2</td>
<td>100</td>
<td>0</td>
<td>66</td>
</tr>
<tr>
<td>0.3</td>
<td>100</td>
<td>0</td>
<td>66</td>
</tr>
<tr>
<td>0.4</td>
<td>100</td>
<td>0</td>
<td>66</td>
</tr>
<tr>
<td>0.5</td>
<td>80</td>
<td>0</td>
<td>73</td>
</tr>
<tr>
<td>0.6</td>
<td>0</td>
<td>5</td>
<td>96.67</td>
</tr>
<tr>
<td>0.7</td>
<td>0</td>
<td>30</td>
<td>80</td>
</tr>
<tr>
<td>0.8</td>
<td>0</td>
<td>100</td>
<td>33</td>
</tr>
<tr>
<td>0.9</td>
<td>0</td>
<td>100</td>
<td>33</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>100</td>
<td>33</td>
</tr>
</tbody>
</table>
VI. CONCLUSION AND FUTURE WORK

Biometrics is a very promising technology, challenges are slowing its development and deployment. Fingerprint images and Iris images are chosen due to their unique physiological traits. In identification and authentication replacing the combination of possession (cards) and knowledge (pins) to have full access in ATMs with only biometrics. In the proposed system, it divided into two stage feature extraction and matching stage in matching stage we develop two technique on get the max match score for fingerprint then use the enrollment iris to get the match score for the iris related to this finger then pass to the fusion equation get the max fusion and it will be the person get access. The two proposed multimodal biometric systems with and without using threshold gave an accuracy of 96.67%, FAR of 0%, and FRR of 5%, and the run time reached 32 and 44 seconds, respectively. By these steps an efficient and secured authentication system which has all these factor of identification and authentication in ATMs is brought out.

<table>
<thead>
<tr>
<th></th>
<th>FAR</th>
<th>FRR</th>
<th>accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fingerprint</td>
<td>4.23</td>
<td>12.66</td>
<td>90.30</td>
</tr>
<tr>
<td>Iris</td>
<td>5.42</td>
<td>6.45</td>
<td>93.21</td>
</tr>
<tr>
<td>Proposed model</td>
<td>0%</td>
<td>5%</td>
<td>96.67</td>
</tr>
</tbody>
</table>

Table II

FINAL RESULT

Fig. 15. Results Histogram

REFERENCES