International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 9 (2018) pp. 6608-6612

Development of an Improved Fingerprint Feature Extraction Algorithm for Personal Verification

Charity Atuegwu, Daramola S.A., Kennedy Okokpujie, Etinosa Noma-Osaghae

Engr. Okokpujie Kennedy (B.Eng, M.Sc, MBA, M.Eng.)
Lecturer / Researcher,
Department of Electrical and Information Engineering,
Covenant University, Ota, OgunState, Nigeria.

Abstract

New and sophisticated technologies are regularly developed to counter every new wave of breaches in data security. At the heart of some of these technologies is the personal verification system that rests on the oars of biometrics. Biometric systems use unique physical and behavioral traits for identification or verification. In this paper, an improved fingerprint feature extraction algorithm for personal verification is proposed. The improved fingerprint feature extraction algorithm is capable of recognizing authorized individuals and differentiating them from fraudulent imposters. The input images were pre-processed before extracting robust features for matching. Euclidean distance was used for classification. The proposed system was tested using the fingerprint images of fifty registered individuals and thirty imposters. The results obtained were a False Acceptance Rate and False Rejection Rate of 16% and 24% respectively. It is also faster than other feature extraction algorithms by forty (40) seconds

Keywords: Fingerprint, biometrics, robust features, division into blocks, ridge pattern, euclidean distance, personal verification, feature extraction, classification.

INTRODUCTION

From the perspective of personal verification, so many questions arise when dealing with the identity of an individual. Questions like; "should this person be given the permission to carry out this transaction or have access to this electronic device?", "has this person been seen here before?", "is this individual who he or she claims to be?" Health centers, telecommunication firms, financial services, e-commerce and so on, are connected electronically due to rapid adoption of information technology. This has made the need for a highly reliable, efficient and robust personal verification system, vital and important. Biometric system uses unique physiological and behavioural traits for identification or verification. Examples of these traits include fingerprint, face, iris, retinal pattern, hand geometry, hand writing, signature, palm printing and voices [1].

The development of an improved fingerprint feature extraction algorithm for personal verification will aid the authentication and identification of individuals in such a way that unauthorized accesses are minimal to nonexistent [2] [3]. Personal verification can be conventional or automated. Conventional method uses among others, attendance book and the clock. Automated method uses bar code, biometric, radio frequency signal and magnetic stripe [4].

In biometric systems, an individual's trait is enrolled. The trait can be retrieved for verification purposes after being stored in a database [5]. In this paper, an improved fingerprint feature extraction algorithm for personal verification was developed.

FOUNDATIONAL CONCEPTS

Review Stage

The identity of an individual can be established using the following approaches:

1. *What you possess*: this has to do with the custody of physical objects like keys, smart card, identity card etc.
2. *What you know*: acquiring a secret knowledge that is not known to other people unless you reveal it. Examples include passwords and pin numbers.
3. *What you are*: this has to do with measurable biological traits that can distinguish one person form others.

Biometrics involve the measurement of some biological traits [6] [7]. Physiological features are entailed in the physical structure of the human body and can be extracted using different methods[8]. Behavioural features depend on individual behaviour and typical examples used for personal verification are gait and signature [9].

All physiological and behavioural traits classified as biometrics must possess the following properties:

1. *Universality*: every user must have a specific biometric characteristic.
2. *Uniqueness*: each user must possess characteristics that will be totally different from other individuals enrolled in the database.
3. *Robustness*: biometric system must be invariant over a period of time.
4. *Collectability*: it must be easy to acquire the characteristics without much difficulty from a practical point of view.
5. *Performance*: the required recognition accuracy and speed in an application should be achievable using the available resources.

6. *Acceptability*: the person should be free and willing to make use of the biometric identification without any inhibition.
7. *Spoof Resistance*: the system must be resistant to any form of manipulation with fake identity.

Personal verification addresses the following problems:

1. Personal data security and privacy issues [10].
2. Trust in financial and business transaction [11].
3. Personal Identification Number (PIN) theft for fraudulent use [12].
4. Unauthorized access [13].

METHOD AND MATERIALS

This paper focuses on the development of an improved fingerprint feature extraction algorithm for personal verification. As shown in Figure 1, it is a MATLAB® based solution that covers all the steps involved in fingerprint recognition. The methods adopted for this work include:

i. Fingerprint images from fifty individuals were captured with a fingerprint scanner. Four fingerprint samples were taken from each individual. The dataset contains 200 sample images.

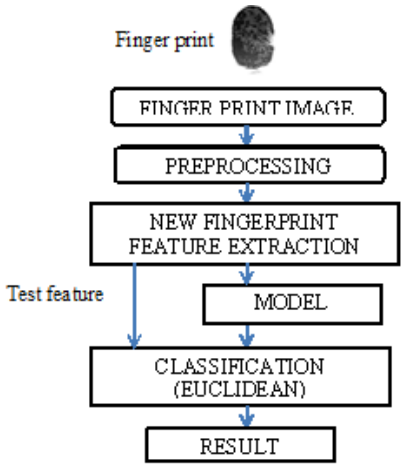

Figure 1. An improved fingerprint feature extraction algorithm for personal verification.

The images were pre-processed by binarization using OTSU method and thinned using morphological method.

i. The feature extraction was done by dividing the fingerprint image into sixteen (16) small blocks and extracting the number of connected pixels (minutiae) in each block.

ii. Euclidean distance was used for classification.

The tools used for developing the biometric verification system are:

i. MATLAB®

ii. Items will be numbered, followed by a period.

Graphical User Interface

A graphical user interface called "welcome.fig" was created using Matlab; it carries all the core call functions that starts the registration and verification process [14] [15]. This is clearly shown in Figure 2.

The Fingerprint Algorithm

The Fingerprint images were pre-processed using different types of pre-processing and enhancement algorithms to increase the recognition performance of the biometric system. The algorithms relating to the finger verification processes are explained as follows.

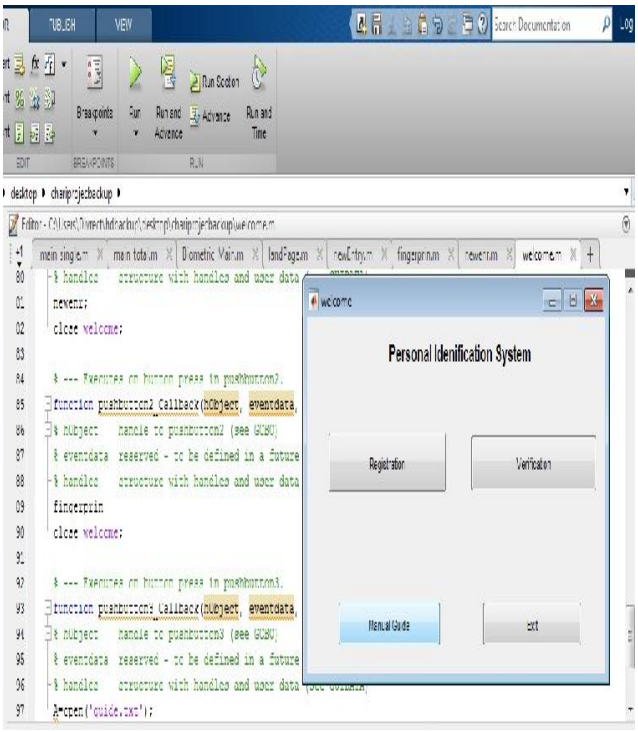

Figure 2. The MATLAB® Graphical User Interface

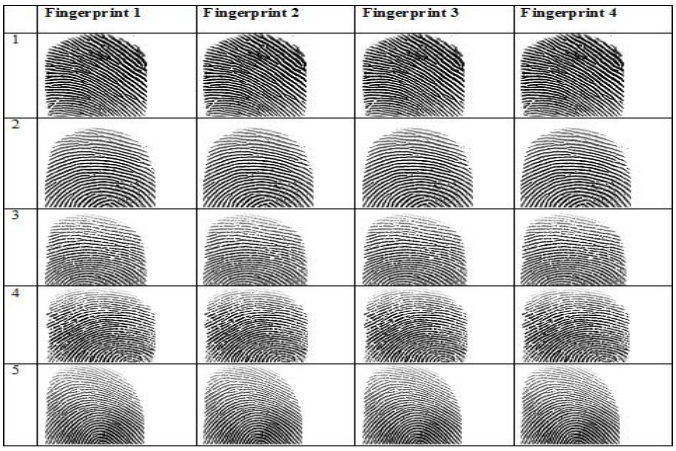

Figure 3. Sample Fingerprint Input Images Improved Fingerprint Feature Extraction Algorithm for Personal Verification.

1. *Binarization:* Binarization is the process of converting a gray scale image into a binary image. Binary images are simple to manipulate, store and generate because its pixels are only a single bit. For fingerprint images, the binary consists of 0 for black (ridge) and 1 for white (furrow). The gray scale image has 256 gray levels (0-255). Thresholding was used to convert the gray scale input image to binary image. The thresholding employed was based on the OTSU method where pixel values of the component with the background are consistent with their respective values in the whole image. It stores the intensities of the pixels in an array. The background and foreground pixels were set to be either 0 or 1. The image changes from greyscale to binary once the threshold value T is set as shown in Equation1.

$$S_{i,j}^{m} = \begin{Bmatrix} 1 & if\ S_{i,j}^{m} > T \\ 0' & Otherwise \end{Bmatrix} i = 1,2\ldots, M; j = 1,2..N..$$

(1)

2. *Thinning*: The process of eroding away the foreground pixels till they are one pixel wide is a morphological operation known as thinning. This is done during the preprocessing stage and before extracting features from the fingerprint. The skeletonized image is formed after applying thinning algorithms to the binary image. The connectivity of the ridge structure is preserved when thinning. Features can be extracted from the outcome of the thinning process (skeletonized image). The thinning operation behaves like a structuring element that has been described as a hit and miss transform containing both ones and zeros. This is expressed in Equation 2.

$$x - y = x \cap NOT\ Y \tag{2}$$

Feature Extraction from Fingerprint

The blocks on the fingerprint image guide the feature extraction process as shown in Figure 3. The technique involves partitioning the entire fingerprint image into rectangular cells with normal resolution. The orientation, ridge direction and foreground pixel positions are then acquired [11]. The feature extraction algorithm is as follows:

1. Partition the image into sixteen *(16)* equal blocks by dividing the entire length *(x)* and breadth *(y)* of the image by four *(4).*
2. Extract the following set of features from all the blocks; The number of connected pixels *(M)*, The city-block distance of the pixels *(N)* which is given as the city block distance between points (x_1, y_1) and (x_2, y_2) as shown in Equation 3, the area of each of the sixteen fingerprint block images *(A)*, given by Equation 4.

$$N = |X_1 \quad X_2|\,|Y_1 \quad Y_2| \tag{3}$$

$$A = \sum_{i=1}^{n} = 1 \sum_{j=1}^{m} = 1(i,j) \tag{4}$$

3. Fuse the three set of features to get a 16-dimensional feature vector F_{finger}.

$$F_{finger} = \left[[F_{area}]\,[F_{c,b}]\,[F_{c,c}] \right]$$

$$F_{finger} = [F_1, F_2, \ldots \ldots F_{16}]$$

(5)

4. The 16-dimensional feature vector (F_{finger}) is obtained from each of the three fingerprint image samples F_1, F2, and F_3. These are used to calculate the threshold value.

$$F_1 = [f_{1,1}, f_{1,2}, \quad f_{1,3} \ldots\ldots f_{1,16}]$$

$$F_2 = [f_{2,1}, f_{2,2}, \quad f_{2,3} \ldots\ldots f_{2,16}]$$

$$F_3 = [f_{3,1}, f_{3,2}, \quad f_{3,3} \ldots\ldots f_{3,16}] \tag{6}$$

5. Then the mean value of the 16-dimensional feature vector is calculated to get the feature vector of the fingerprint template that will be stored in the database. This is done for the three samples of each of the fifty individual fingerprint images. The fingerprint feature vector template is obtained by finding the mean values (F_{mean}) for each corresponding feature components. The fingerprint mean model for each of the subject is represented by Equation 7. The threshold of each of the subjects is obtained using Equation 7. Where (σf) is the standard deviations of the training feature vector components.

$$F_{mean} = [f_{mean,1}, f_{mean,2}, f_{mean,3}, \ldots\ldots\ldots f_{mean,16}]$$

(7)

$$Threshold = \sqrt{\sum_{f=1}^{48} \sigma f} \tag{8}$$

Classfication of Fingerprint Images

Euclidean distance was used to classify the fingerprint images. The Euclidean distance measure is one of the most suitable classifier used to obtain distance measurement between two vectors of equal sizes on a two-dimensional plane. In this work, *Tf* is the template's feature vector of size *f* = 16 for each subject. The Euclidean distance *(d)* between the query fingerprint feature vector and each of the template feature vector of the subjects in the database was calculated by using Equation 9.

$$d = \sqrt{\sum_{f=1}^{48} (Tf - If)} \tag{9}$$

Registration

When registering a new person into the verification system, click on the "registration" button on the welcome.fig GUI, this will call the "newenry.fig" GUI using the functions on newen ry.m MATLAB file that carries the code. On the newenry GUI follow the step:

1. Enter personal details (Name and Unique ID)
2. Take fingerprint data (select the fingerprint file from file browser)
3. Click on Enter button to save data into the database
4. For adding another person, go to step 1

RESULT AND DISCUSSION

False (Imposter) Acceptance Rate (FAR)

This is the recognition of an imposter as a genuine user. It can happen when the template falls within the intra user variation of the genuine user. The formula in percentage is:

$$FAR = NFA/TN * 100 \quad (10)$$

NFA: Number of fingerprint accepted

TN: Total number of fingerprint.

Thirty (30) imposter fingerprints were collected and tested. During the testing, five fingerprints were accepted and twenty-five were rejected. The result obtained was 16% as shown in Table 1.

$$FAR = 5/30 * 100 = 16\%$$

False (Genuinue Individual) Rejection Rate

This occurs when genuine users are rejected during verification. It is usually the result matching failure. The formula in percentage is given as:

$$FRR = NFR/TN * 100 \quad (11)$$

NFR: Number of fingerprints rejected

TN: Total number of fingerprints

Fifty genuine users' fingerprints were collected and trained. During testing, twelve fingerprints were rejected and thirty-eight were accepted. The result obtained was 24% as shown in Table 2.

$$FRR = 12/50 * 100 = 24\%$$

CONCLUSION

The development of an improved fingerprint feature extraction algorithm for personal verification is the major contribution of this paper. A total of fifty (50) individuals were used in this project, but the database is large enough to accommodate hundreds of thousands of people. For each individual, a total of four (4) fingerprint images were taken and tested. MATLAB® was used to develop the improved feature extraction algorithm. It was also used to develop the user interface for fingerprint image capturing. The results obtained were efficient and convenience for personal verification.

REFERENCES

[1] K. Okokpujie, E. Noma-Osaghae, S. John, and A. Ajulibe, "An Improved Iris Segmentation Technique Using Circular Hough Transform," in International Conference on Information Theoretic Security, 2017, pp. 203-211.

[2] L. Introna and H. Nissenbaum, "Facial recognition technology a survey of policy and implementation issues," 2010.

[3] K. Okokpujie, F. Olajide, S. John, and C. G. Kennedy, "Implementation of the Enhanced Fingerprint Authentication in the ATM System Using ATmega128," in Proceedings of the International Conference on Security and Management (SAM), 2016, p. 258.

[4] L. Shen, L. Bai, and Z. Ji, "FPCODE: An efficient approach for multi-modal biometrics," International Journal of Pattern Recognition and Artificial Intelligence, vol. 25, pp. 273-286, 2011.

[5] K. Okokpujie, N.-O. Etinosa, S. John, and E. Joy, "Comparative Analysis of Fingerprint Preprocessing Algorithms for Electronic Voting Processes," in International Conference on Information Theoretic Security, 2017, pp. 212-219.

[6] S. Daramola and C. Nwankwo, "Algorithm for fingerprint verification system," Journal of Emerging Trends in Engineering and Applied Sciences, vol. 2, pp. 355-359, 2011.

[7] S. Daramola and T. Ibiyemi, "Person Identification System using Static-dyamic Signatures Fusion," (IJCSIS) International Journal of Computer Science and Information Security, vol. 8, pp. 88-92, 2010.

[8] S. A. Daramola and T. S. Ibiyemi, "Offline signature recognition using hidden markov model (HMM)," International journal of computer applications, vol. 10, pp. 17-22, 2010.

[9] S. A. Daramola, T. Sokunbi, and A. Adoghe, "Fingerprint Verification System Using Support Vector Machine," International Journal on Computer Science and Engineering (IJCSE) ISSN:, vol. 5, pp. 678-683, 2013.

[10] K. O. Okokpujie, E. Noma-Osaghae, G. Kalu-Anyah, and I. P. Okokpujie, "A Face Recognition Attendance System with GSM Notification," 2017.

[11] K.O. Okokpujie, O.O. Uduehi, and F. O. Edeko, "An Innovative Technique in ATM Security: An Enhanced Biometric ATM with GSM Feedback Mechanism," Journal of Electrical and Electronics Engineering (JEEE), vol. 12, pp.

Pages 68-81, 2016.

[12] K. Okokpujie, E. Noma-Osaghae, S. John, and R. Oputa, "Development of a facial recognition system with email identification message relay mechanism," in Computing Networking and Informatics (ICCNI), 2017 International Conference on, 2017, pp. 1-6.

[13] C. Atuegwu, K. O. Okokpujie, and E. Noma-Osaghae, "A Bimodal Biometric Student Attendance System," 2017.

[14] K. O. Okokpujie, N.-O. Etinosa, O. J. Okesola, J. N. Samuel, and O. Robert, "Design and Implementation of a Student Attendance System Using Iris Biometric Recognition," in *Computational Science and Computational Intelligence (CSCI), 2017*, Las Vegas, USA, 2017.

[15] N.-O. Etinosa, C. Okereke, O. Robert, O. J. Okesola, and K. O. Okokpujie, "Design and Implementation of an Iris Biometric Door Access Control System," in *Computational Science and Computational Intelligence (CSCI), 2017*, Las Vegas, USA, 2017.