American Scientific Research Journal for Engineering, Technology, and Sciences (ASRJETS)
ISSN (Print) 2313-4410, ISSN (Online) 2313-4402

http://asrjetsjournal.org/

Development and Performance Evaluation of Hausdorff Distance Algorithm Based Facial Recognition System

Olumayowa A. Idowu[a]*,Waliu O. Mufutau[b], Abolaji O. Ilori[c], Olufemi P. Alao[d]

[a,b]*Electrical &Electronic Department, Moshood Abiola Polytechnic Abeokuta, Nigeria*
[b]*Department of Computer Science, Oyo State College of Agriculture, Igboora, Oyo State, Nigeria*
[d]*Department of Electrical and Electronic Engineering, OOU, Ibogun Campus, Nigeria*
[a]*Email: olumayor2@gmail.com*

Abstract

Securing access to information is of primary concern in many frame of reference including personal, commercial, governmental and military purpose. Computer verifiable biometric such as face provide an attractive means of securing access to information. Earlier algorithms for facial recognition system which includes Linear Discriminant Analysis (LDA), Principle Component Analysis (PCA) andIndependent Component Analysis (ICA) have yielded unsatisfactory result especially when confronted with unconstrained scenarios such as varying illumination, varying poses, expression and aging. This work presents a facial recognition authentication system using hausdorff distance algorithm in combating the highlighted problems. A system camera was employed for capturing images, information was stored using MYSQL database and biometric templates were stored as binary large object (BLOB). The developed system performance was evaluated using False Reject Rate (FRR), False Accept Rate (FAR), and Receiver Operating Characteristic Curve (ROC graph) as performance metrics. Tests were conducted at various threshold values. FRR errors obtained are 20%, 7%, and 2% at 500 threshold value for one-try, two-try and three-try configuration respectively. The system also presented FAR error of 0% at 500 threshold value for all configurations. As threshold value increases, FAR reduces while FRR increases.

Keywords: Hausdorff; Cryptography; Biometric; Authentication; Information; Subject; Database.

---

* Corresponding author.

1. Introduction

The information age is quickly revolutionizing the way humans carry out daily activities. Everyday actions are increasingly being handled electronically and transferred across complex network. This growth in electronic transactions has resulted in a greater demand for fast and accurate user identification and authentication. Access codes for buildings, banks accounts and computer systems often use PIN's for identification and security clearances. The use of proper PIN will undoubtedly grant access to user, but the user of the PIN is not verified. When credit and ATM cards are lost or stolen, an unauthorized user can often come up with the correct personal codes. Despite warning, many people continue to choose easily guessed PIN's and passwords by using birthdays, phone numbers and social security numbers. Recent cases of identity theft have heighten the need for methods to prove that someone is truly who he/she claims to be.

Recently, biometrics had been identified as a panacea to the problem of data and information security in the field of Computer and Electrical Engineering. Biometric uses unique physiological or behavioral characteristics such as fingerprints, face, voice, writing style, and gait to recognize individuals. Theoretically, any human physiological or behavioral characteristic can be used to make a personal identification as long as it satisfies features like universality, uniqueness, permanence and finally collectability [1].

Face is a biometric, as a consequence, face recognition finds wide applications in authentication, security, and so on. Among all biometrics, face is a very unique one because it is the only biometric belonging to both the physiological and behavioral categories. In addition, as reported in [2, 3], face enjoys many advantages over other biometrics because it is natural, nonintrusive, and easy-to-use biometric. Among the six biometrics of face, finger, hand, voice, eye, and signature, face biometric ranks the first in the compatibility evaluation of a machine readable travel document (MRTD) system in terms of six criteria: enrolment, renewal, machine-assisted identity verification requirements, redundancy, public perception, and storage requirements and performance. Probably the most important feature of acquiring the face biometric signature is that no cooperation is required during data acquisition.

A wide array of face recognition approaches has been proposed in the literature, this is mainly associated to its advantages over other biometrics. Early face recognition algorithms used simple geometric models, but the recognition process has now matured into a science of sophisticated mathematical representations and matching processes. Major advancements and initiatives in the past ten to fifteen years have propelled face recognition technology into the spotlight. Face recognition can be used for both verification and identification (open-set and closed-set). For face recognition system to be practical, it should be robust to variations in illumination, pose and expression as humans recognize faces irrespective of all these variations. Psychological studies have revealed that humans can categorize a human face at a glance and recognize the line drawings of objects as quickly and almost as accurately as photographs [4]. It is suggested that the edge-like retinal images of faces can provide useful information for face identification at the level of early vision. The advantage of using edges as image features is that they can provide robustness to illumination change and simplicity of presentation.

This research focuses on the use of Hausdorff distance algorithm for facial recognition. The Hausdorff distance

is a metric between two point sets. In object recognition, as shape information plays a decisive role, Hausdorff distance between edge images is a suitable measure for comparison.

2. Biometric System

The term "biometric" refers to metric related to human physiological or behavioral characteristic that can be used to establish authentication or verification. Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals [5]. The scientific literature on quantitative measurement of humans for the purpose of identification dates back to the 1870s and the measurement system of Alphonse Bertillon [6]. Bertillon's system of body measurements, including such measures as skull diameter and arm and foot length, was used in the USA to identify prisoners until the 1920s. Henry Faulds, William Herschel and Sir Francis Galton proposed quantitative identification through fingerprint and facial measurements in the 1880s [5]. The development of digital signal processing techniques in the 1960s led immediately to work in automating human identification. Speech and fingerprint recognition systems were among the first to be explored [7]. The potential for application of this technology to high-security access control, personal locks and financial transactions was recognized in the early 1960s [8]. The 1970s saw development and deployment of hand geometry systems [7], the start of large-scale testing and increasing interest in government use of these "automated personal identification" technologies. Retinal and signature verification systems came in the 1980s, followed by face systems. Iris recognition systems were developed in the 1990s.

3. Face Recognition

Face recognition is a task that humans perform routinely and effortlessly in their daily lives. Wide availability of powerful and low-cost desktop and embedded computing systems has created an enormous interest in automatic processing of digital images and videos in a number of applications, including biometric authentication, surveillance, human-computer interaction, and multimedia management. Research and development in automatic face recognition follows naturally.

Research in face recognition is motivated not only by the fundamental challenges this recognition problem poses but also by numerous practical applications where human identification is needed [9]. Face recognition, as one of the primary biometric technologies, became more and more important owing to rapid advances in technologies such as digital cameras, the Internet and mobile devices, and increased demands on security. Face recognition has several advantages over other biometric technologies: It is natural, nonintrusive, and easy to use. Among the six biometric attributes considered by [10], facial features scored the highest compatibility in a Machine Readable Travel Documents (MRTD) [11] system based on a number of evaluation factors, such as enrollment, renewal, machine requirements, and public perception, shown in Figure 1a & 1b.

A face recognition system is expected to identify faces present in images and videos automatically. It can operate in either or both of two modes: (1) face verification (or authentication), and (2) face identification (or recognition). Face verification involves a one-to-one match that compares a query face image against a template face image whose identity is being claimed. Face identification involves one-to-many matches that compares a

query face image against all the template images in the database to determine the identity of the query face. Another face recognition scenario involves a watch-list check, where a query face is matched to a list of suspects (one-to-few matches). The performance of face recognition systems has improved significantly since the first automatic face recognition system was developed by [12]. Furthermore, face detection, facial feature extraction, and recognition can now be performed in "real-time" for images captured under favourable (i.e., constrained) situations. Although progress in face recognition has been encouraging, the task has also turned out to be a difficult endeavour, especially for unconstrained tasks where viewpoint, illumination, expression, occlusion, accessories, and so on vary considerably. In the following sections, we give a brief review on technical advances and analyze technical challenges.

Figure 1a: A scenario of using biometric MRTD systems for passport control

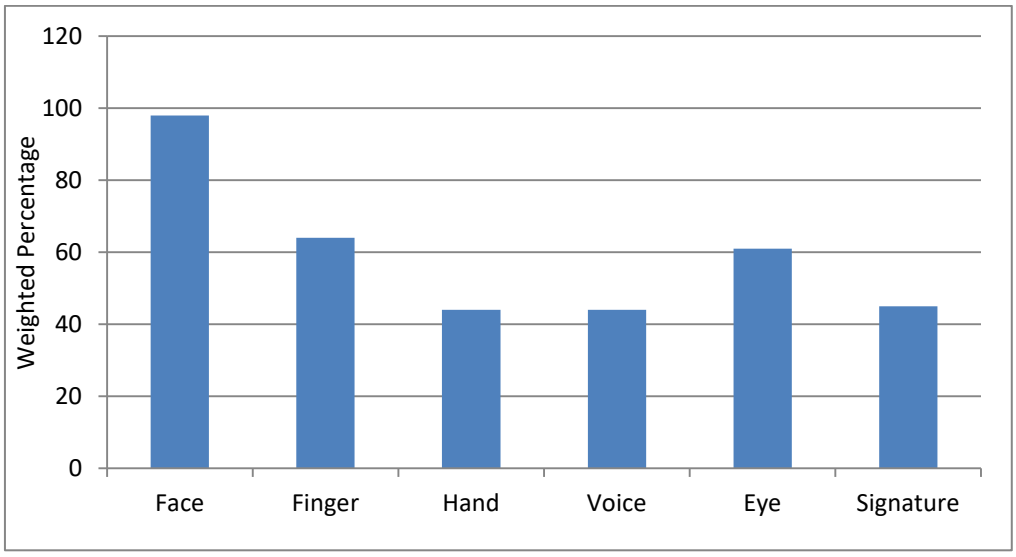

Figure 1b: comparison of various biometric features based on MRTD compatibility [10].

3.1 Available Technical Solutions

There are two strategies for dealing with the above difficulties: feature extraction and pattern classification based on the extracted features. One is to construct a "good" feature space in which the face manifolds become

simpler i.e., less nonlinear and non-convex than those in the other spaces. This includes two levels of processing: (1) normalize face images geometrically and photometrically, such as using morphing and histogram equalization; and (2) extract features in the normalized images which are stable with respect to such variations, such as based on Gabor wavelets.

The second strategy is to construct classification engines able to solve difficult nonlinear classification and regression problems in the feature space and to generalize better. Although good normalization and feature extraction reduce the nonlinearity and non-convexity, they do not solve the problems completely and classification engines able to deal with such difficulties are still necessary to achieve high performance. A successful algorithm usually combines bothstrategies.

With the geometric feature-based approach used in the early days [5, 10, 14], facial features such as eyes, nose, mouth, and chin are detected. Properties of and relations (e.g., areas, distances, angles) between the features are used as descriptors for face recognition. Advantages of this approach include economy and efficiency when achieving data reduction and insensitivity to variations in illumination and viewpoint. However, facial feature detection and measurement techniques developed to date are not reliable enough for the geometric feature based recognition [7], and such geometric properties alone are inadequate for face recognition because rich information contained in the facial texture or appearance is discarded. These are reasons why early techniques are not effective.

The statistical learning approach learns from training data (appearance images or features extracted from appearance) to extract good features and construct classification engines. During the learning, both prior knowledge about face(s) and variations seen in the training data are taken into consideration. Many successful algorithms for face detection, alignment and matching nowadays are learning-based.

The appearance-based approach, such as PCA [13] and LDA [3] based methods, has significantly advanced face recognition techniques. Such an approach generally operates directly on an image-based representation (i.e., array of pixel intensities). It extracts features in a subspace derived from training images. Using PCA, a face subspace is constructed to represent “optimally” only the face object; using LDA, a discriminant subspace is constructed to distinguish “optimally” faces of different persons. Comparative reports (e.g., [3]) show that LDA-based methods generally yield better results than PCA-based ones. Although these linear, holistic appearance-based methods avoid instability of the early geometric feature-based methods, they are not accurate enough to describe subtleties of original manifolds in the original image space. This is due to their limitations in handling nonlinearity in face recognition: there, protrusions of nonlinear manifolds may be smoothed and concavities may be filled in, causing unfavourable consequences. Such linear methods can be extended using nonlinear kernel techniques (kernel PCA [16] and kernel LDA [14]) to deal with nonlinearity in face recognition [11, 16, 17]. There, a nonlinear projection (dimension reduction) from the image space to a feature space is performed; the manifolds in the resulting feature space become simple, yet with subtleties preserved. Although the kernel methods may achieve good performance on the training data, however, it may not be so for unseen data owing to their more flexibility than the linear methods and over fitting thereof.

Another approach to handle the nonlinearity is to construct a local appearance-based feature space, using appropriate image filters, so the distributions of faces are less affected by various changes. Local features analysis (LFA) [17], Gabor wavelet-based features (such as elastic graph bunch matching, EGBM) [15, 17] and local binary pattern (LBP) [1] have been used for this purpose. Some of these algorithms may be considered as combining geometric (or structural) feature detection and local appearance feature extraction, to increase stability of recognition performance under changes in viewpoint, illumination, and expression. A taxonomy of major face recognition algorithms in Figure 2.8 provides an overview of face recognition technology based on pose dependency, face representation, and features used for matching.

A large number of local features can be produced with varying parameters in the position, scale and orientation of the filters. For example, more than 100,000 local appearance features can be produced when an image of 100×100 is filtered with Gabor filters of five scales and eight orientation for all pixel positions, causing increased dimensionality. Some of these features are effective and important for the classification task whereas the others may not be so. AdaBoost methods have been used successfully to tackle the feature selection and nonlinear classification problems [18, 19, 20]. These works lead to a framework for learning both effective features and effective classifiers.

3.2 Current Technology Maturity

As introduced earlier, a face recognition system consists of several components, including face detection, tracking, alignment, feature extraction, and matching. Where are we along the road of making automatic face recognition systems? To answer this question, we have to assume some given constraints namely what the intended situation for the application is and how strong constraints are assumed, including pose, illumination, facial expression, age, occlusion, and facial hair. Real-time face detection and tracking in the normal indoor environment is relatively well solved, whereas more work is needed for handling outdoor scenes. When faces are detected and tracked, alignment can be done as well, assuming the image resolution is good enough for localizing the facial components, face recognition works well for cooperative frontal faces without exaggerated expressions and under illumination without much shadow. Face recognition in an unconstrained daily life environment without the user's cooperation, such as for recognizing someone in an airport, is currently a challenging task. Many years' effort is required to produce practical solutions to such problems.

3.3 The Hausdorff Distance

Given two infinite point sets $A = \{a_1 \dots \dots . . a_p\}$ and B =$\{b_1 \dots \dots . . b_q\}$, the Hausdorff distance is defined as:

$$H = (A, B) = \max\big(h(A, B), h(B, A)\big) \quad (1)$$

Where

$$h(A, B) = \max_{a \in A} \min_{b \in B} \|a - b\| \quad (2)$$

and $\|.\|$ is some underlying norm between pouts A and B.

The function h *(A,B)*is called the directed Hausdorff distance from A to B. It identifies the point a ε A that is farthestfrom any point of B and measures the distance from a to this nearest neigbor in B. The Hausdorff distance measures the mismatch between two sets that are at fixed positions with respect to one another. Considering measuring the mismatch between all possible relative positions of two sets, as given by the value of the Hausdorff distance as a function of relative position, that is, for any group G, the minimum Hausdorff distance is defined to be

$$M_g(A,B) = \min_{g_1 g_2 \in G} H\ g_1 A, g_2 B \tag{3}$$

If the group G is such that for any g ε G and for any points x_1, x_2 , $\|gx_1 - gx_2\| = \|x_1 - x_2\|$, then we need only consider transforming one of the sets:

$$M_G(A,B) = \min_{g \in G} H(A, gB). \tag{4}$$

This property holds when G is the group of translations, and ‖ . ‖ is any norm, as well as when G is the group of rigid motions and ‖ . ‖ is the Euclidean norm.

4. Methodology

The facial recognition system consists of modules which work seamlessly to authenticate and verify users. The system has been divided into two main stages; enrollment and verification.

4.1 Enrolment stage

This stage involves the process of inputting the subject data (name, sex, age, marital status, occupation etc.) and biometrics information (fingerprint and facial data.). A graphical user interface (GUI) was design to provide a mechanism for collecting subject's details.

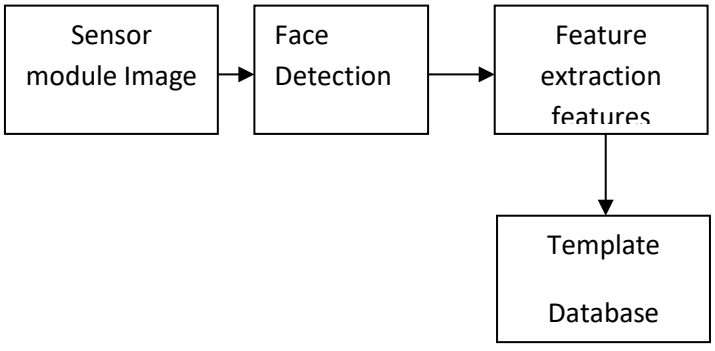

Figure 2: Block diagram of the system enrollment stage

The enrollment stage of the system includes sensor module, face detection module, feature extraction module, template database as shown in Figure 3.1. Each module is explained as follows:

4.1.1 Sensor Module

At sensor module a suitable user interface incorporating the biometric sensor or scanner was developed to measure or record the raw biometric data of the user. This raw biometric data was captured and transferred to the next module for detection. The system web camera was employed for capturing face images. This enhances capturing high quality images. Another camera could also be connected to the computer via USB interface.

4.1.2 Face Image Scanner

The face image is captured automatically whenever a face image is detected by the system through the camera. This is to control the quality of the image and to capture uniform images during enrollment and authentication. The face scanner was design using the AdaBoost object detection algorithm for detecting face. The algorithm involves training a series of increasingly discriminating simple classifiers and then blending their outputs.

4.1.3 Face Detection

The main function of this step is to determine (1) whether human faces appear in a given image, and (2) where these faces are located at. The expected outputs of this step are patches containing each face in the input image. In order to make further face recognition system more robust and easy to design, face alignment are per-formed to justify the scales and orientations of these patches. Besides serving as the pre-processing for face recognition, face detection could be used for region-of-interest detection, retargeting, video and image classification, etc.

4.1.4 Feature Extraction

After the face detection step, human-face patches are extracted from images. Directly using these patches for face recognition have some disadvantages, first, each patch usually contains over 1000 pixels, which are too large to build a robust recognition system. Second, face patches may be taken from different camera alignments, with different face expressions, illuminations, and may suffer from occlusion and clutter. To overcome these drawbacks, feature extractions are performed to do information packing, dimension reduction, salience extraction, and noise cleaning. After this step, a face patch is usually transformed into a vector with fixed dimension or a set of fiducial points and their corresponding locations. The developed system employs hausdorff distance algorithm to extract features.

4.1.5 Template Database

A database is an organized collection of related data. It is a collection of data, describing the activities of one or more related systems. In the database design, database management system was employed. This enables the adoption of database security methodology in storing data. In order to determine the logical structure of a database, data would be modeled using relational data model. A relational model is a conceptual representation of data structures that are required by a database. The information contained in relational model is used to define relational tables, primary and foreign keys, stored procedures, and triggers. Message Digest 5 (MD5) Hashing technique is used in securing access to the database.

4.2 Authentication Stage

At the authentication stage, subject presents his/her ID. Thereafter face image would be acquired from the subject. The features will again be extracted and match with the enrolled data linked with the ID. As explained previously, the authentication stage includes the sensor and face detection module, feature extraction module, matching module, and decision module.

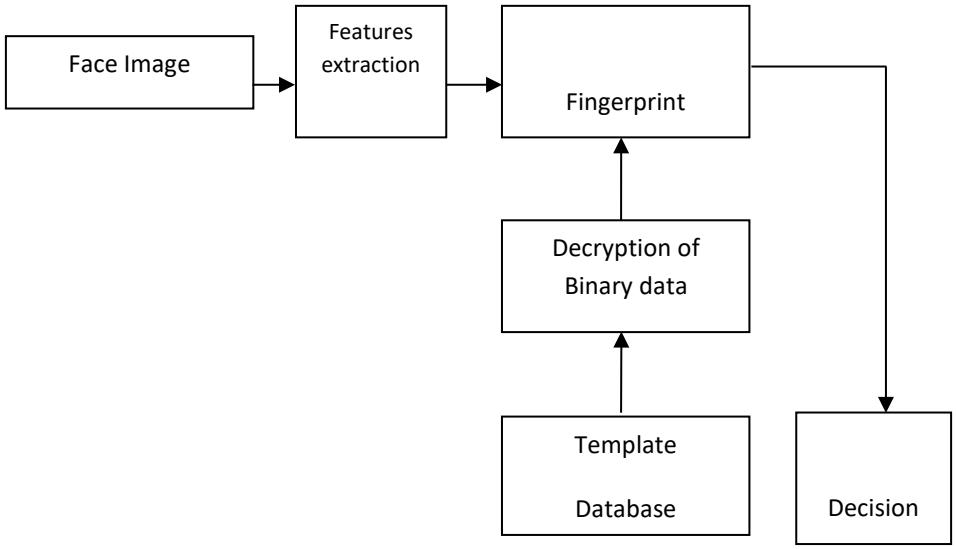

Figure 3: Block diagram of the system verification stage

4.2.1 Matching Module

The extracted features when compared with the templates in the database will generate a match score. This match score may be controlled by the quality of the given biometric data. The matcher uses hausdorff distance metric to compare images. For a subject to be granted access, face image must match the enrolled templates.

4.2.2 Decision Module

Decision making module identifies whether the user is a genuine user or an impostor based on the match scores. If scores from the matcher are closed access would be granted to the user else access would be denied.

5. Software Implementation

Object Oriented Analysis and Design (OOAD) approach was followed in the design of the system. OOAD provides a natural and intuitive way to view the software design process—namely, modeling objects by their attributes and behaviors just as human describe real-world objects. The developed system model was implemented using Java technology because of the support Java has for database connectivity. Sun created a standardized interface to databases from Java called Java Database Connectivity (JDBC), which makes it possible to connect a Java application with MySQL database. Using the Connector/J JDBC driver, the system queries the database for data.

5.1 System Testing and Documentation

Data Input

Upon approaching the recognition system for the first time (assuming no one is currently using it), the user should experience the following sequence of event:

1. A graphical user interface (GUI) design to provide a mechanism for collecting data is displayed as shown in Figure 4. On the menu tab, the user can choose to input biometric details to generate a template or input face for recognition.

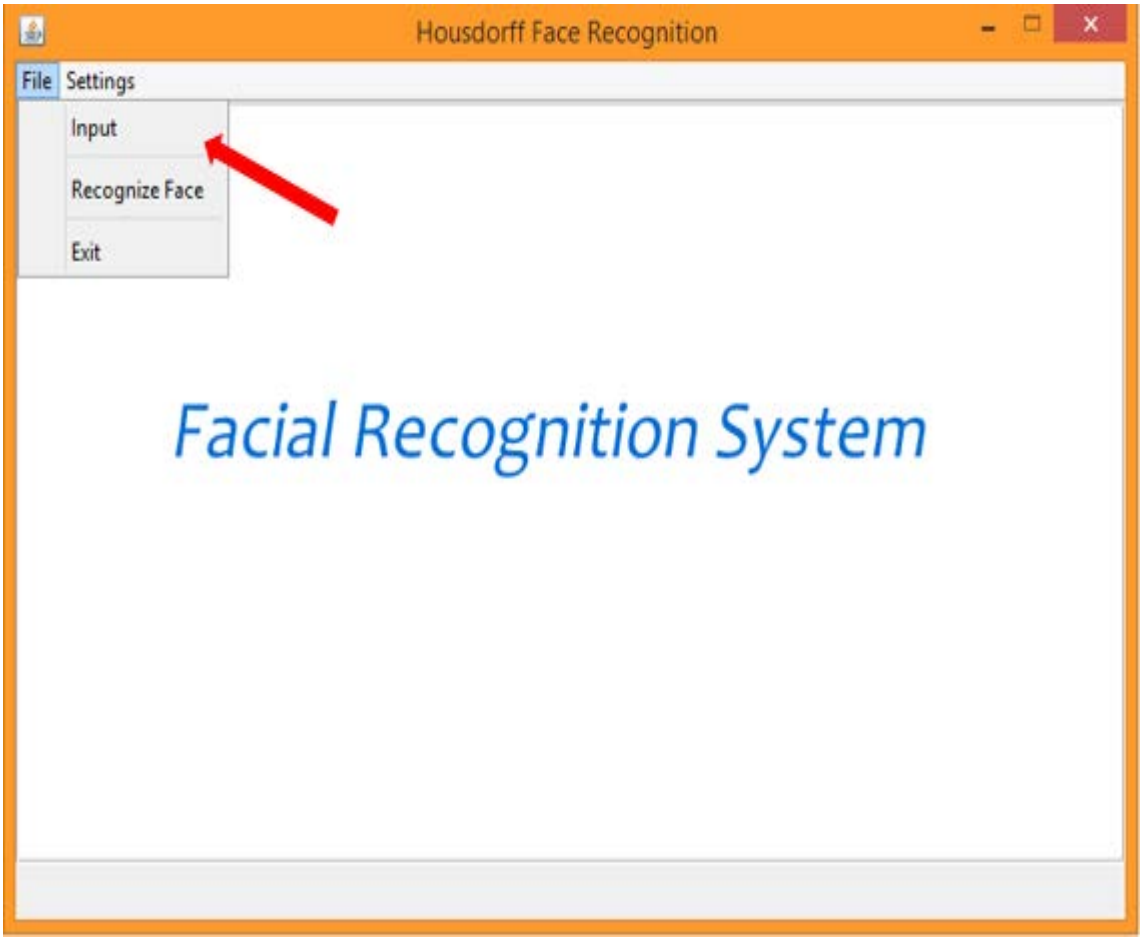

Figure 4: Interface for Input Selection

2. If input is selected as shown in Figure 4, an interface to collect subjects details would be displayed as shown in Figure 5. On the input interface all field are disabled until snap passport button is click and a passport is taken using the Passport Snapper as shown in Figure 6. The Passport Snapper is a module that reads image data from a camera hardware on the computer or hardware attached to the computer. If the passport is successfully taken, all the fields on the input interface will be enabled and the passport taken would be displayed as shown in Figure 7

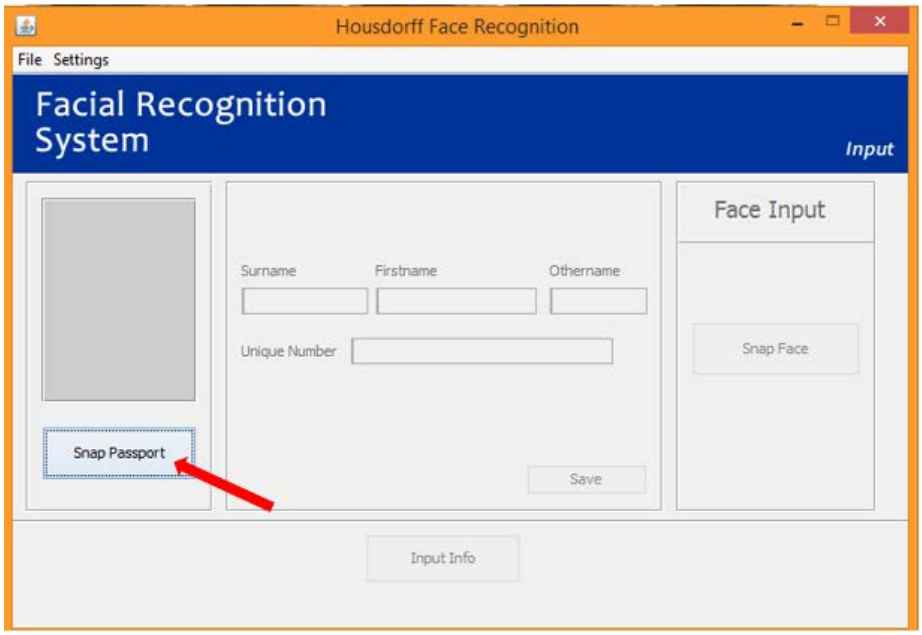

Figure 5: Interface for Subject details

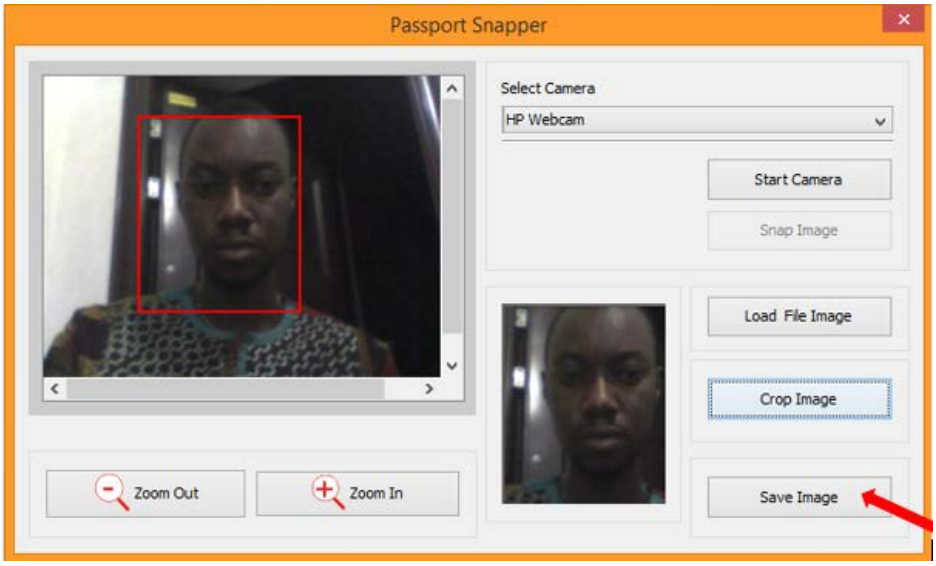

Figure 6: Interface for Passport Snapper

3. On the input interface all the fields such as Surname, First name, etc. must be filled and a unique number should be provided for the subject. The unique number is a means for the subject to indicate his/her identity for recognition. The unique number provided is attached to the template generated. After all the fields had been filled, the face biometric template may be generated by clicking Snap face button. This in turn popup the face-scanner module as shown in Figure 8. The Face scanner automatically captured five face images whenever a face image is detected by the system through the camera. The image is captured only when the subject is facing the camera. This is to control the quality of the image and to capture uniform images when generating template.

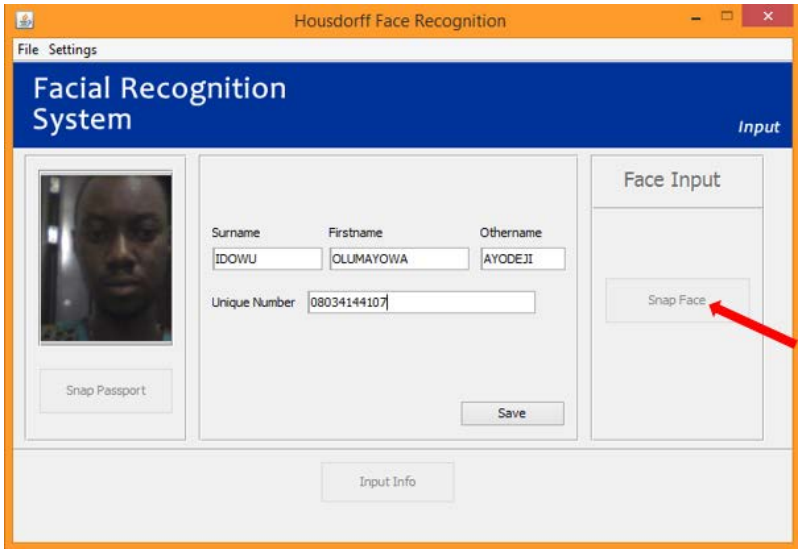

Figure 7: Interface for displaying details

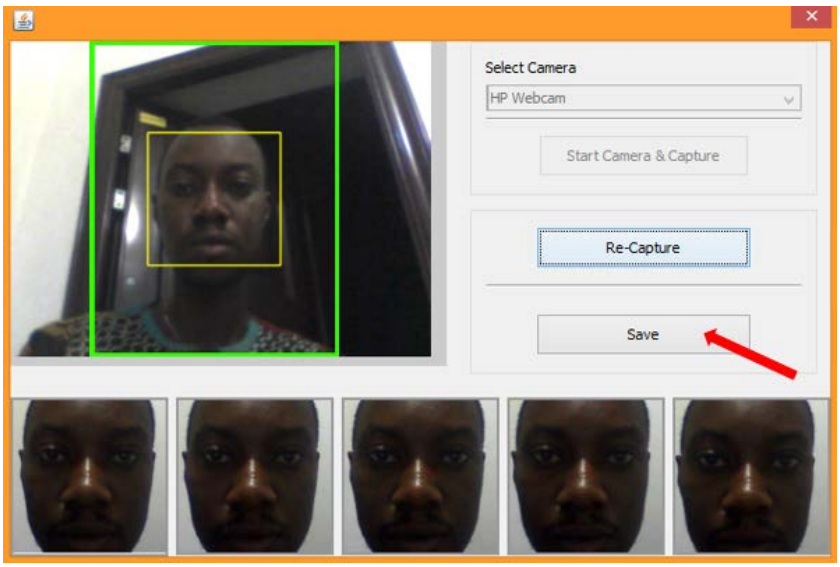

Figure 8: Interface for Face Scanner Module

Recognition

In order to recognize or verify a face the user should select Recognize face button on file menu. This makes the output interface to popup as shown in Figure 9. At this stage, subject presents his/her unique number. Thereafter, a single face image would be acquired from the subject using the face scanner as shown in Figure 10. The features will again be extracted and compare with the data linked with the unique number. If the image matches, an interface showing the details of the recognized person will be displayed as shown in Figure 11. On the other hand if face does not match the claimed identity, a notification dialog box is displayed indicating face mismatch as shown in Figure 12.

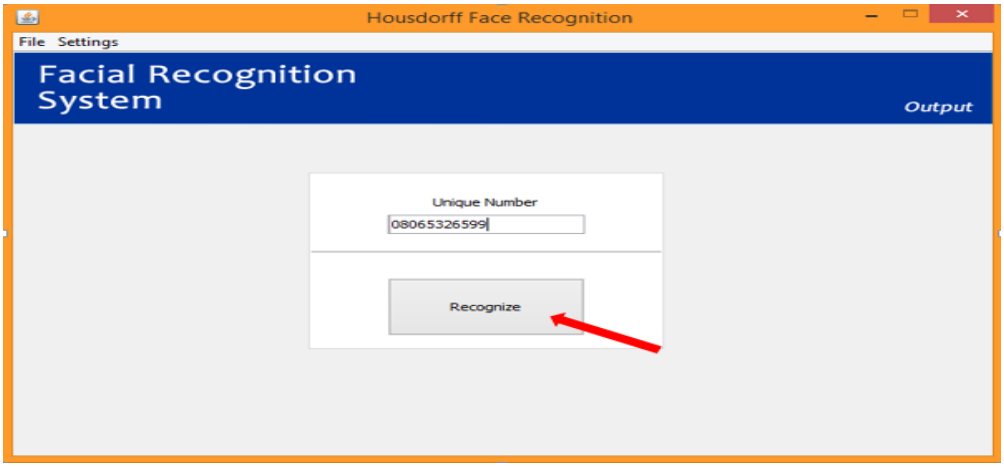

Figure 9: Output Interface 1

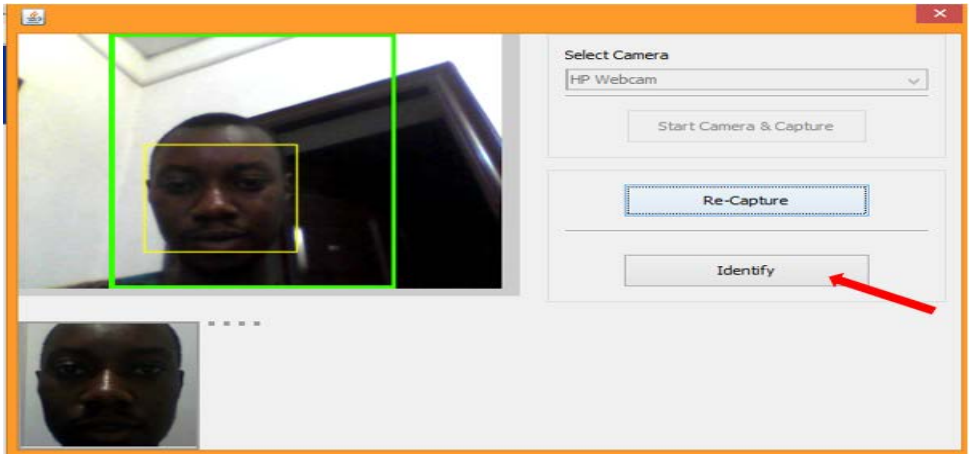

Figure 10: Output Interface 2

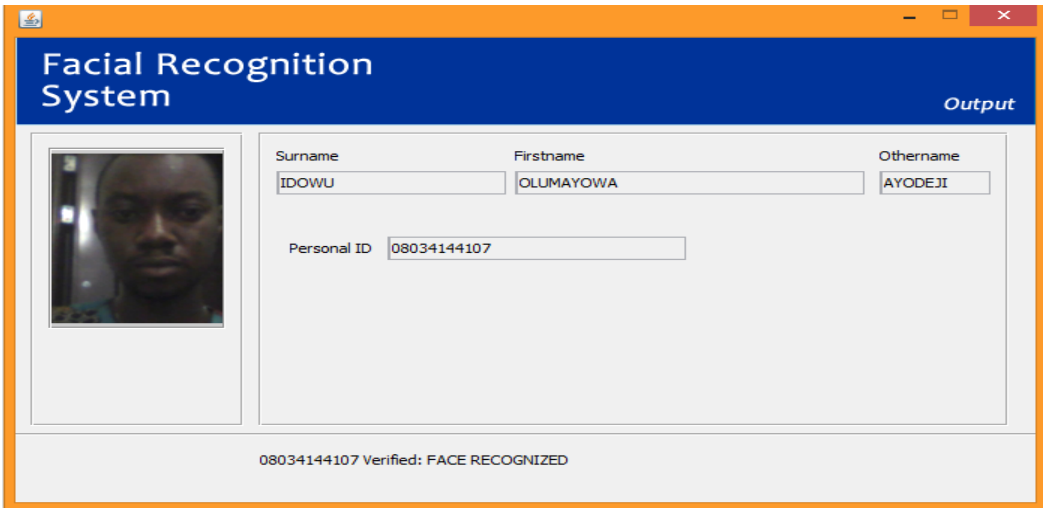

Figure 11: Output Interface 3

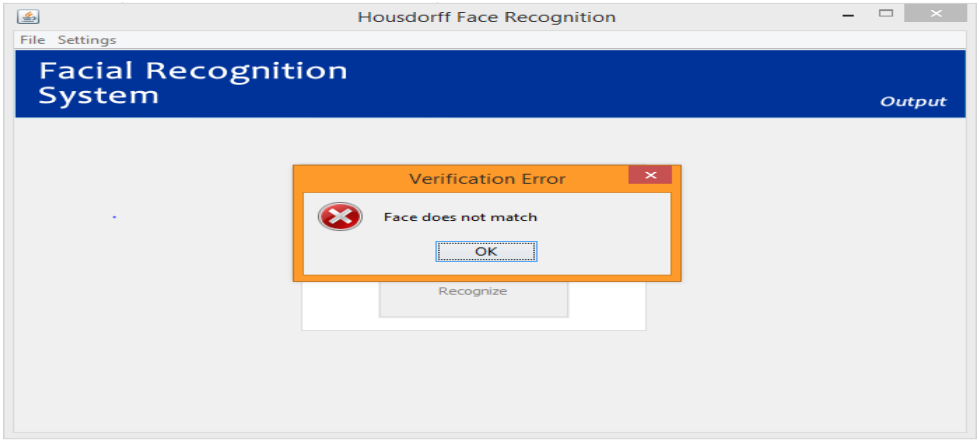

Figure 12: Another Possible Output Interface

5.2 Developed System Performance Evaluation

For the purpose of evaluating the performance of the proposed system, performance metrics peculiar to authentication systems would be employed. These metrics are described briefly as follows:

i. False rejection rate (FRR): The proportion of authentic users that are incorrectly denied. If a verification transaction consists of a single attempt, the false reject rate would be given by:

$$FFR(t) = FTA + FNMR(t) \times (1 - FTA) \quad (5)$$

Where, FTA is Failure To Acquire Rate and

FNMR is False-Non-Match rate

In order to estimate false rejection rate, the test was conducted at different threshold values. Figure 13depicts the graphs of false rejection rate at various threshold values. The graphs show that the authentication system false rejection error rate reduces as the threshold is reduced.

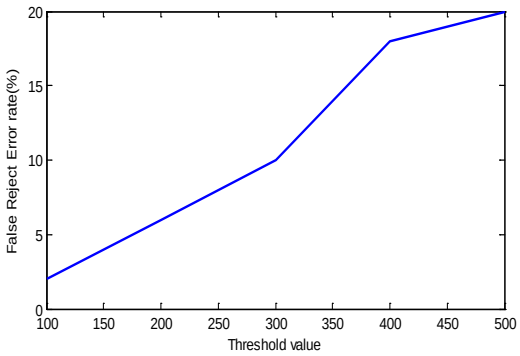

Figure 13: False Reject Error

ii. False acceptation rate (FAR): The proportion of impostors that are accepted by the biometric system. If a verification transaction consists of a single attempt, the false accept rate would be given by:

$$FAR(t) = FMR(t) \times (1 - FTA) \quad (6)$$

Where, FMR is False Match rate

The results of the test is shown in Figure 14, the system false acceptance error rate is 2% at 100 threshold value and 0% at 500 threshold value.

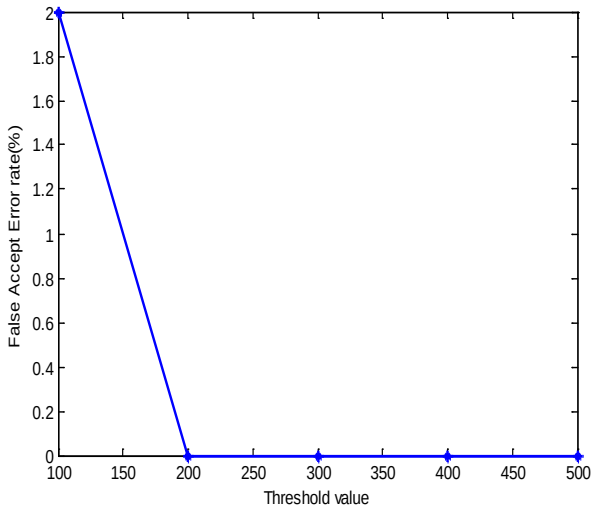

Figure 14: False Accept Error

6. Conclusion

Over the years results from facial recognition systems, have been unsatisfactory especially when confronted with unconstrained scenarios such as varying illumination, varying poses, expression, and aging. In this research, an authentication system was developed using hausdorff algorithm which combated the highlighted problems. The developed system was designed to operate at three configuration; one-, two-, three-try configuration. False Reject Rate (FRR), False Accept Rate (FAR), and Receiver Operating Characteristic Curve (ROC graph) were used as performance metrics. FRR error is 20%, 7%, and 2% at 500 threshold value for one-try, two-try and three-try configuration respectively. The system also presents FAR error of 0% at 500 threshold value for all configurations. There is always a trade-off between the false accept rate (the fraud rate) and the false reject rate (the insult rate). As the threshold values increases false accept rate reduces while false reject rate increase for all configurations.

7. Recommendation

The performance of the biometric system for distributed applications depends not only on algorithm employed but also on the efficiency of the network. The developed system was design and deployed as a client-server

application on a desktop system. It is recommended that further works should be geared towards improving the performance of biometric systems on communication and business networks.

References

[1] Shweta M., and Chander K.V. A Hybrid Approach for Securing Biometric Template International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, 2(5) 2013

[2] R. Hietmeyer. Biometric identification promises fast and secure processings of airline passengers. I.C.A.O.J., 55(9):10-11, 2000

[3] P. J. Phillips, R.M. McCabe, and R. Chellappa. Biometric image processing and recognition. Proc. European signal Process. Conf., Rhodes, Greece, 1998.

[4] Shang-Hung L. An Introduction to Face Recognition Technology Informing Science Special issues onMultimedia informing Technologies- Part 2, 3(13), 2000.

[5] Jain, A., Hong, L., & Pankanti, S. Biometric Identification. Communications of the ACM, 43(2): 91-98. 2000.

[6] Beavan C., Fingerprints: The Origins of Crime Detection and the Murder Case that Launched Forensic Science. Hyperion, New York 2001

[7] Beavan C. Fingerprints: The Origins of Crime Detection and the Murder Case that Launched Forensic Science. Hyperion, New York 2001

[8] Trauring M. On the automatic comparison of finger-ridge patterns. Hughes Laboratory Research Report No. 190. 1961

[9] M. Bichsel and A. P. Pentland. Human face recognition and the face image set's topology. CVGIP: Image Understanding, 59:254–261, 1994.

[10] R. Hietmeyer. Biometric identification promises fast and secure processing of airline passengers. The International Civil Aviation Organization Journal, 55(9):10–11, 2000.

[11] R.-L. Hsu. Face Detection and Modeling for Recognition. Ph.D. thesis, Michigan State University, 2002.

[12] T. Kanade. Picture Processing by Computer Complex and Recognition of Human Faces. Ph.D. thesis, Kyoto University, 1973.

[13] P. J. Phillips, H. Moon, S. A. Rizvi, and P. J. Rauss. The FERET evaluation methodology for face-recognition algorithms". IEEE Transactions on Pattern Analysis and Machine Intelligence,

22(10):1090–1104, 2000.

[14] D. Valentin, H. Abdi, A. J. O'Toole, and G. W. Cottrell. Connectionist models of face processing: A survey. Pattern Recognition, 27(9):1209–1230, 1994.

[15] Y. Moses, Y. Adini, and S. Ullman. Face recognition: The problem of compensating for changes in illumination direction. In Proceedings of the European Conference on Computer Vision, volume A, pages 286–296, 1994.

[16] B. Sch¨olkopf, A. Smola, and K. R. M¨uller. Nonlinear component analysis as a kernel eigenvalue problem. Neural Computation, 10:1299–1319, 1999.

[17] M.-H. Yang, N. Ahuja, and D. Kriegman. Face recognition using kernel eigenfaces. In Proceedings of the IEEE International Conference on Image Processing, volume 1, pages 37–40, 2000.

[18] P. Yang, S. Shan,W. Gao, S. Z. Li, and D. Zhang. Face recognition using ada-boosted gabor features. In Proceedings of International Conference on Automatic Face and Gesture Recognition, Vancouver, 2004.

[19] G. Zhang, X. Huang, S. Z. Li, and Y. Wang. Boosting local binary pattern (LBP)-based face recognition. In S. Z. Li, J. Lai, T. Tan, G. Feng, and Y. Wang, editors, Advances in Biometric Personal Authentication, volume 3338 of Lecture Notes in Computer Science, pages 180–187. Springer, 2004.

[20] L. Zhang, S. Z. Li, Z. Qu, and X. Huang. Boosting local feature based classifiers for face recognition. In Proceedings of First IEEE Workshop on Face Processing in Video, Washington, D.C., 2004.