Computing, Information Systems, Development Informatics & Allied Research Journal
Vol. 8 No. 1, March, 2017 - www.cisdijournal.net

An Evaluation of performance of k-NN and Mahalanobis Distance on Local Binary Pattern Feature representation for Access Control in Face Recognition System

Yusuff, S.R., Balogun, F.B., Babatunde, A.N. & Babatunde, R.S.
Department of Computer Science
Kwara State University
Malete, Nigeria.
ronsule@yahoo.com, arinolafula87@yahoo.com, akinbowale.babatunde@kwasu.edu.ng, ronkebabs711@gmail.com

ABSTRACT

A vast majority of the existing face recognition techniques encounter misclassifications when there is a large variation of the subject in terms of pose, illumination and expression as well as artefact such as occlusion. With the usage of Local Binary Pattern (LBP), local feature representation which preserves local primitives and texture information, robust against illumination, expression and occlusion was realized in the feature extraction process. Mahalanobis distance and k-NN classifier were employed for recognition as basis for comparison. An assessment of both algorithms was considered. It was observed that Mahalanobis distance measure outperformed the k-NN classifier for access control and recognition system due to its high recognition rate (98.4%), genuine acceptance rate (98.37) and its stern adherence to both FAR and FRR (0.0144, 1.568) than k-NN with 94.9% and (0.392 and 2.895) respectively. This result demonstrates the robustness of Mahalanobis distance classifier for use access control system.

Keywords - Information and Communications Technology, devices, infusion modeling, Nigeria, private transport companies.

CISDI Journal Reference Format
Yusuff, S.R., Balogun, F.B., Babatunde, A.N. & Babatunde, R.S. (2017): An Evaluation of performance of k-NN and Mahalanobis Distance on Local Binary Pattern Feature representation for Access Control in Face Recognition System. Computing, Information Systems & Development Informatics Journal. Vol 8 No 1. Pp 121-130.

1. BACKGROUND TO THE STUDY

In the transforming world of global data communications, low-priced internet connections, and rapid software development, security is becoming more and more of an issue. Global computing is inherently insecure hence security becomes a basic requirement. Many applications contain confidential information generated by their users and therefore the need arises to verify the individual as an authentic user before access is granted (Adnan et al, 2013). Access control (AC) is the selective restriction of access to a place or other resources. The act of accessing may mean consuming, entering or using. AC is a way of limiting access to a system or to a physical or virtual resources. Traditionally AC was partially accomplished through PIN and password but biometric indicators offer better candidate solution (Omidiora et al 2008). Some biometric modalities are less permanent over time than others, and some are more difficult to present and capture consistently (Ylber, Artan, Ymer and Vehbi, 2015). Some are more prone to sample quality problems. There is no perfect biometric modality; each has advantages and disadvantages for a given use case. For example, perhaps the most differentiating feature of fingerprints as a modality is that they leave behind evidence at a crime scene as "covert" (e.g. fingerprints on a glass). Irises are perhaps the most consistent, information-dense, "barcode-like" of the modalities. Facial images stand out because they are the biometric modality that humans excel at comparing, and so we can integrate complementary human-and machine-based recognition (Ojo and Adeniran, 2011).

Additionally, facial images are abundant in the digital realm, and also can be collected covertly from a distance. Voice is notable for being behavioral as well as physical, and thus the samples available from a given individual are abundant (Dmitry and Valery, 2012). The possession of access control is of prime importance when persons seek to secure important, confidential, or sensitive information and equipment. Access control is, in reality, an everyday phenomenon. A lock on a car door is essentially a form of access control. A PIN on an ATM system at a bank is another means of access control. Among the various biometric modalities, the face biometric is predominately used by considering its many advantages including contactless capture, non-intrusive and user-friendly interaction, (Aluko, Omidiora, Adetunji and Odeniyi, 2015). The need for access control in face recognition has increased due to the recent increase in impersonation related incidents (Ylber Januzaj, Artan Luma, Ymer Januzaj and Vehbi Ramaj, 2015). Babatunde et al 2015, remarked that the image variations of the same subject due to pose, expression, structural component and illumination are almost always greater than the variations between the images of two different subjects. To overcome visual variations, pre-processing step which involves cropping, normalization, grayscale conversion, filtering and segmentation to enhance facial details so as to ease further analysis is very important in the process of face recognition. One of the constant challenges in image analysis is to improve the process used to obtain distinctive characteristics. This is due to the curse of dimensionality which is a predominant characteristics of high dimensional data such as an image. Moreover, the higher the dimension of the feature representation, the more the time consumption of the recognition.

In the process of image analysis, local primitive features (descriptors) are used to represent characteristics which contain sufficient information for identification. These descriptors are used in object recognition, image matching, image retrieval, among other tasks. LBP has the capable of transforming and characterizing the facial details to obtain texture cues which are very important for personal identification. LBP can make the texture information of local neighborhood in the gray scale image to adapt to the different rotation and illumination inherent in operational face data.

Therefore, the biometric process of identification and verification involves preprocessing, feature transformation in which relevant data (such as curves, blob, edges, gradients, color or texture) are extracted to represent interest points into a feature vector, and classification using the descriptors to determine and or verify the authenticity of users and claimed identity. The superiority of the Biometric authentication process depends on the distinctiveness and invariance of the interest points, and this determines the more accuracy of the processes and application that uses it. Furthermore, the recognition time (time taken to identify and authorize an individual) will be determined by the dimension of data and size of feature descriptors.

The remaining part of this article is organized as follows - In section 2, we give a review of related works on face biometric identification. Section 3, explain the detail methodology used in preprocessing and face analysis to obtain the descriptors and subsequent recognition based on both Mahalanobis distance and K- nearest neighbor. Furthermore, in section 4, we present and discuss the results obtained for recognition and access control based on the LBP feature descriptors using the two classifiers and evaluate the performance of both on locally acquired face data. Section 5 summarizes and conclude our works and gives insight to further research focus.

2. RELATED WORKS

There have been a vast amount of research works on access control using face recognition. Omidiora et al. (2008) carried out an assessment of PCA and DCT algorithms for access control system. It was discovered that PCA proved to be a better algorithm for access control and recognition system based on the high percentage (90.43%) of correctly classified faces and its strict attendance to both FAR and FRR (0.1077, 0.0609) respectively. Dmitry and Valery, (2012) developed a Multilayer Perceptron Neural Networks (NN) for access control based on face image recognition. For this set of experiments ORL database were divided into two parts; the first part represented authorized persons and has 20 individuals, from which 5 images were randomly used for training (total 100 images) and the other 5 for testing (total 100 images). The Second part represented unauthorized persons. It has 20 persons and 10 images per person (total 200 images) only for testing purposes. Thus system has 100 images for training, and 200 for testing (100 authorized and 200 unauthorized). the introduced 'sqr' thresholding rule has better performance for rejection of an unauthorized persons than 'min' thresholding rule. The drawback of 'min' algorithm as stated in the works was that it cannot deal with situation such as when some class is similar to more than one class. The system yielded high performance when used for access control and acceptable FAR and FRR.

Aluko, Omidiora, Adetunji and Odeniyi (2015) carried out a performance evaluation of selected Principal Component Analysis-Based techniques for face image recognition. The systems were subjected to three selected eigenvectors: 75, 150 and 300 to determine the effect of the size of eigenvectors on the recognition rate of the systems. The performances of the techniques were evaluated based on recognition rate and total recognition time. The performance evaluation of the three PCA-based systems showed that PCA – ANN technique gave the best recognition rate of 94% with a trade-off in recognition time. Adnan, Mohammed, Mubashshir and Ahmed (2013) developed a face recognition supported with remote frequency identification (RFID) and communication system for access control. The approach presented in the works uses DWT and Euclidean distance method. DWT was used in data compression (JPEG2000) and the Euclidean distance measure was used for classification. RFID components and technology was explored in the research. The testing of the system involves taking a snapshot using the web-cam when a person presents his RFID card to the system. The system scans the RFID card and compares with the probe image. Once the image is matched, the system sends the information to the other station and access is either granted or denied.

Ylber, Artan, Ymer and Vehbi (2015) developed a real time access control based on face recognition. The works used haar-like features for face detection and PCA algorithm for face recognition. OpenCV libraries and python computer language was used, which resulted in a higher accuracy and effectiveness. Training and identification was done in an embedded device known as Raspberry Pi. The paper focused on accuracy increment by controlling parameters such as background, light and number of trainings. Adedeji *et al.*(2012) carried out a performance evaluation of optimized PCA (OPCA) and Projection Combined PCA $(PC)^2A$ methods in Facial Images based on recognition accuracy, total training time and average recognition time. The result obtained indicated that OPCA performed better than $(PC)^2A$.

3. METHODOLOGY

3.1. Face acquisition and normalization

Face images of 250 individuals were captured. This acquisition was done using a genx 300 digital camera of 23 mega pixels. For each individual, eight images of different pose were captured including indoor and outdoor coverage, at different times of the day, varying the lighting, facial expressions (open/closed eyes, smiling/not smiling) and facial details (glasses/no glasses).The Face images were converted to grayscale and normalized by cropping out essential facial region from the whole face image using AdaBoost, to obtain 750 x 200 cropped threshold, and were later resized to a dimension of100 x 100 pixels.

AdaBoost is a feature selector with a principled strategy that minimizes the upper bound on empirical error. The face image preprocessing using AdaBoost is a procedure for greedily minimizing the exponential loss, namely,

$$\frac{1}{m}\sum_{i=1}^{m}\exp(-y_i F(x_i)) \quad (1)$$

where F(x) is given as

$$F(x)=\sum_{t=1}^{T}\alpha_t h_t(x). \quad (2)$$

and h(x) is a weak hypothesis/feature, $\alpha_t \in R$ and F(x) is a final strong hypothesis/feature, and $y_i \in \{-1,+1\}$..The pseudocode for AdaBoost as explained in Schapire, Freund, Bartlett and Lee, (1989) is shown in Figure 1. Given m labeled training examples (x_1,y_1),..... (x_m,y_m) where the xi's are in some domain X, and the labels $y_i \in \{-1,+1\}$. On each round t = 1;.....T, a distribution $D_t$is computed as in the figure over the m training examples, and a given weak learner or weaklearning algorithm is applied to find a weak hypothesis $ht: X \rightarrow \{-1,+1\}$ where the aim of the weak learner is to find a weak hypothesis with low weighted error ε relative to D_t. The final or combined hypothesis H computes the sign of a weighted combination of weak hypotheses.

Given: $(x_1,y_1),\ldots,(x_m,y_m)$ where $x_i \in \mathcal{X}$, $y_i \in \{-1,+1\}$.
Initialize: $D_1(i)=1/m$ for $i=1,\ldots,m$.
For $t=1,\ldots,T$:

- Train weak learner using distribution D_t.
- Get weak hypothesis $h_t : \mathcal{X} \rightarrow \{-1,+1\}$.
- Aim: select h_t with low weighted error:

$$\varepsilon_t = \Pr_{i\sim D_t}[h_t(x_i)\neq y_i].$$

- Choose $\alpha_t = \frac{1}{2}\ln\left(\frac{1-\varepsilon_t}{\varepsilon_t}\right)$.
- Update, for $i=1,\ldots,m$:

$$D_{t+1}(i)=\frac{D_t(i)\exp(-\alpha_t y_i h_t(x_i))}{Z_t}$$

where Z_t is a normalization factor (chosen so that D_{t+1} will be a distribution).

Output the final hypothesis:

$$H(x)=\text{sign}\left(\sum_{t=1}^{T}\alpha_t h_t(x)\right).$$

Figure 1: The Boosting Algorithm (Schapire, et al, 1989)

3.2. Face Feature Descriptor Extraction

In this research, the face image was transformed using LBP and in the process, features are extracted. To obtain the local information which describes the faces, face images were equally subdivided into small sub-regions to extract LBP histograms. LBP code was calculated for every pixel in the sub-region and the code obtained were converted to histogram. The LBP histogram extracted from each sub-region are concatenated into a single, spatially enhanced feature histogram. The histogram of these patterns, also called labels, forms a feature vector, and thus a representation for the texture of the image. Readers are referred to related literatures such as Ojala et al 2002, Babatunde et al, 2015, Babatunde et al 2016 , Rahim et al. 2013 for details of feature extraction using LBP. Figure 2 shows the process flow of the proposed Access Control System.

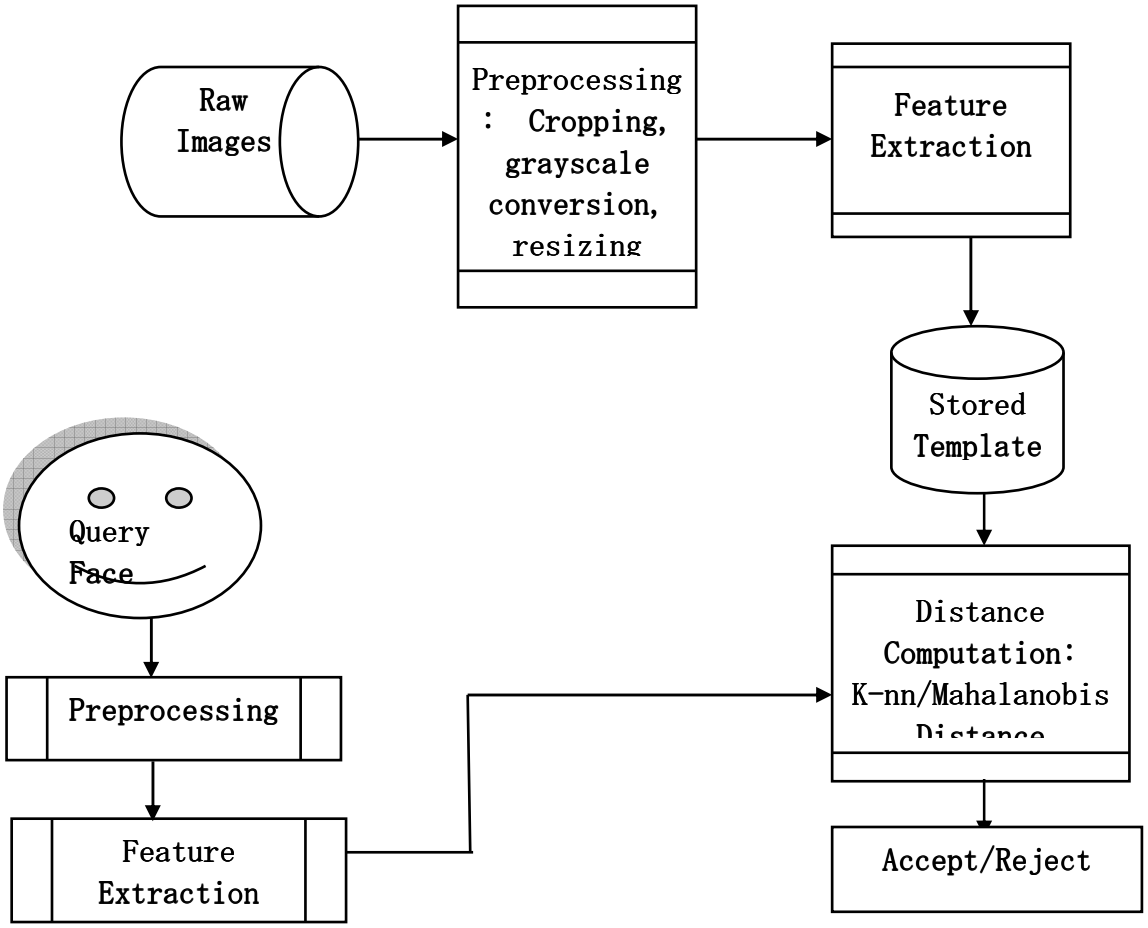

Figure 2: Process Flow of the Access Control System

3.3 Materials and Methods

The face database generated in this research which is made up of 250 Africans were grouped into training and testing sets. The training set contains five images per individual with one thousand two hundred and fifty (1250) images and testing set includes three images per individual having a total of seven hundred and fifty (750) images. Eighty extra faces composed of two different expressions of forty persons, that were not part of the training set (intended to serve as impostor) were added to the testing set to make a total of Eight hundred and thirty (830) images.

3.3.1 Recognition using k-NN

In this research, the LBP algorithm generates histograms, which are the local primitives of the face image, and these template were passed on to KNN classifier. For a probe image to be authenticated or granted access, it is first normalized and transformed using the above stated procedure. The KNN classifier compares these histogram (template) to those already generated from the training images. In order to measure the similarity between the test and trained templates, k-nearest neighbor computes the root of square difference between co-ordinates of pair of objects as with the Euclidean distance, based on closest training examples in the feature space. In this research, the training process for k-NN was carried out by storing feature vectors and labels of the training images. Therefore, recognition is done by assigning the unlabelled probe face (query point) to the label of its k nearest neighbors by majority rule of the nearest neighbour approach.

3.3.2 Recognition using Mahalanobis Distance

Mahalanobis distance measures the distance of a point x from a data distribution, characterized by a mean and the covariance matrix. It is used in this research as similarity measure between the pattern of the training samples (data distribution of training example of a class) and the pattern of the test sample/probe/query. The covariance matrix gives the shape of how data is distributed in the feature space, which is elliptical in nature. Essentially, Mahalanobis distance measure transforms the variables/values/pattern into uncorrelated variables with variances equal to 1, and then calculates simple Euclidean distance. The Mahalanobis distance is computed with a positive definite covariance matrix C using equation 3

$$D(x,y) = \sqrt{(x-y)C^{-1}(x-y)} \qquad (3)$$

Where C is the covariance matrix. The key feature is the use of covariance as a normalization factor. Mahalanobis distance automatically takes into account the correlation between feature descriptor axes through the covariance which makes it a unique distance classifier. In this research, recognition using Mahalanobis distance metric was done by computing the Mahalanobis distance between the feature descriptors of the test and trained images. The Mahalanobis distance between the trained feature vectors and the test image vector was determined by comparing the covariance between the vectors of the test image and each of the trained images using equation 3. Mahalanobis of a projected test image from all the trained images are calculated and the minimum value is chosen in order to find out the train image which is most similar to the test image. The test image is assumed to fall in the same class that the closest train image belongs.

3.4. Experimentations

The face database used in this research as earlier stated is made up of authorized and unauthorized faces. The former representing faces that were in the training database while the latter represent the faces that were never part of the training database. The intent was to evaluate the robustness of the algorithms employed and to determine if access is been granted to authorized users and denied to impostors. The performance of the algorithms used for recognition in this research is measured based on the following factors; False Acceptance Rate (FAR), False Rejection Rate (FRR), Equal Error Rate (EER), Genuine Acceptance Rate (GAR), Recognition Time (RT) and Recognition Rate(RR). Therefore,

$$FAR = \frac{\text{number of unauthorized persons considered as authorized}}{\text{total number of unauthorized attempts}} \qquad (4)$$

$$FRR = \frac{\text{number of authorized persons considered as unauthorized}}{\text{total number of authorized attempts}} \qquad (5)$$

$$Recognition\ rate = \frac{total\ number\ of\ recognized\ faces}{total\ number\ of\ authorized\ attempt} * 100 \qquad (6)$$

Equal error rate is the point at which the FAR and FRR are equal and have the same value
GAR is defined as the percentage of genuine users accepted by the system, given by;

$$GAR = 100 - FRR \qquad (7)$$

The Recognition Time is the time taken by the face recognition system to recognize a probe face. The FAR is defined as the percentage of impostors accepted by the Biometric system. It is essential that this percentage is as small as possible so that the persons that are not enrolled in the system will not be accepted by the system, which is the major importance of an access control system. Likewise, FRR is the percentage of genuine users rejected by the biometric system. The system must not reject an enrolled user, hence the number of false rejection must also be kept as minimal as possible.

4. RESULT AND DISCUSSION

The initial set of experiments were carried out to determine the Average training time for all trained images, Recognition time, Total number of unrecognized images and Recognition rate. The result obtained is shown in Table 1 for k-NN and Mahalanobis distance classifier respectively.

Table 1: Result showing the recognition result based on time and rate for the two algorithms

Metrics	k-NN	Mahalanobis Distance
Training time (sec)	16.07	11.03
Recognition time (sec)	0.88	0.48
Recognition rate (%)	94.9	98.4
Total Number of recognized faces	712	738
Total Number of unrecognized faces	38	12

From Table 1, it can be observed that the recognition rate recorded with recognition based on Mahalanobis distance outperforms that of k-nn. This is also shown in the graph in Figure 2. The Number of images unrecognized with Mahalanobis Distance is smaller in number from the result of this experiment as seen from the table. Additionally, the recognition time recorded with Mahalanobis distance is shorter than that recorded using k-nn.

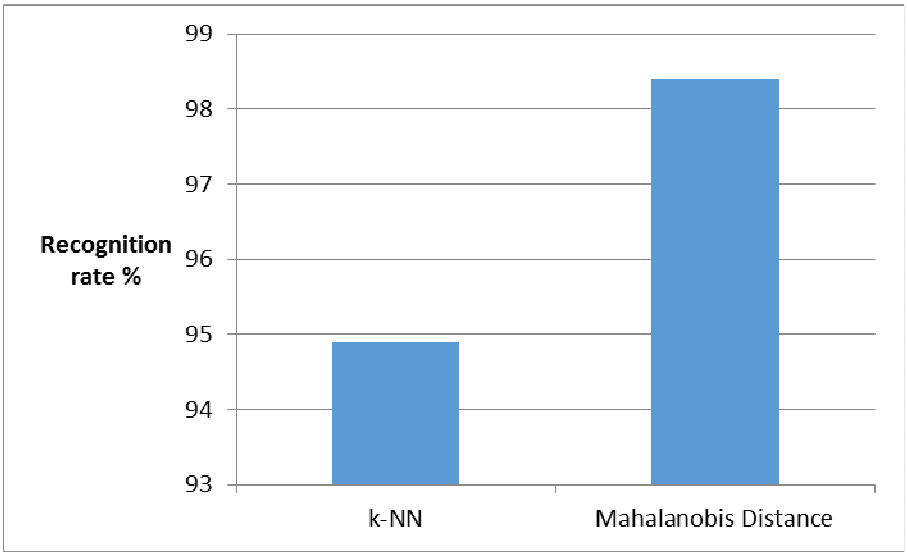

Figure 2: Result of Recognition Rate for the Two Algorithms

A well-performing biometric system is characterized by prompt results and low rates of false acceptance and false rejection. The final experiments were carried out to determine the FAR, FRR, EER and GAR using the two algorithms. In this experiment, k-nn and Mahalanobis distance classifiers were individually used for matching the LPB feature descriptors. The threshold was initially set to 0.15 and the matching score obtained was recorded. Subsequently, the threshold was increased in steps of 0.15 for ten trials, of which FAR, FRR and GAR were computed for each experiment. The result obtained is shown in Tables 2.1, Figure 3, Table 2.2 and Figure 4 for k-nn and Mahalanobis distance respectively. Figures 3 and 4 shows the graph plotted for FAR and FRR against threshold values to determine the ERR (i.e. the point of intersection of the two curves).

Table 2.1: Result of Access Control Experiment using k-nn classifier

Threshold value	FAR	FRR	GAR
0.15	0.85	0.32	99.68
0.25	0.66	0.85	99.15
0.35	0.60	1.77	98.23
0.45	0.48	2.09	97.91
0.55	0.39	2.60	97.40
0.65	0.27	2.99	97.01
0.75	0.21	3.67	96.33
0.85	0.18	4.28	95.72
0.95	0.16	4.79	95.21
1.10	0.12	5.23	94.77

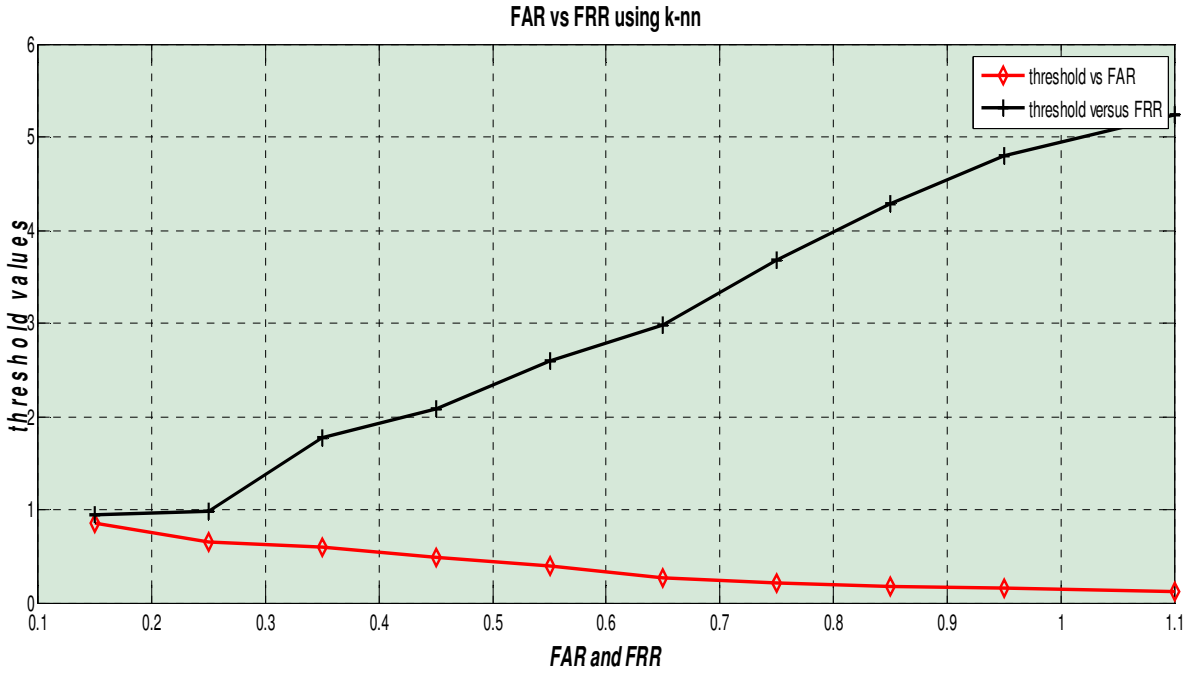

Figure 3: FAR vs FRR using k-NN

Table 2.2 : Result of Access Control Experiment using Mahalanobis Distance measure

Threshold value	FAR	FRR	GAR
0.15	0.22	0.13	99.87
0.25	0.19	0.19	98.81
0.35	0.18	0.21	99.79
0.45	0.16	0.16	99.84
0.55	0.14	1.15	98.85
0.65	0.14	1.71	98.29
0.75	0.13	2.04	97.96
0.85	0.11	2.91	97.09
0.95	0.10	3.36	96.64
1.10	0.07	3.82	96.18

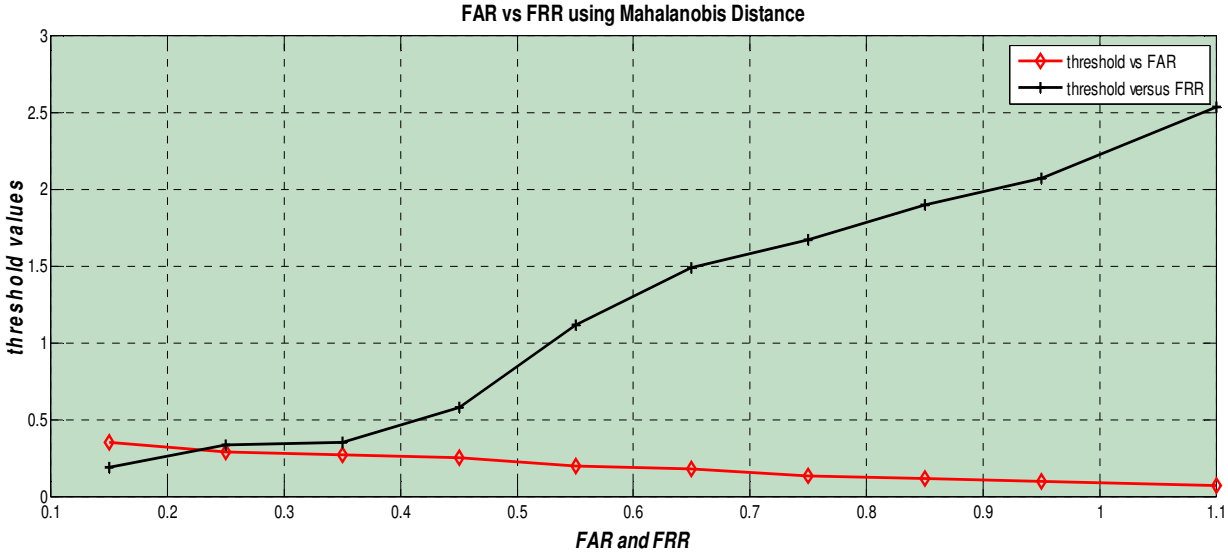

Figure 4: FAR vs FRR using Mahalanobis

From Tables 2.1 and 2.2, varying the threshold at each run of the experiment as earlier explained, it can be observed that the FAR for the two algorithms reduces as the threshold increases while the FRR tends to increase as the threshold increases. Furthermore, the EER does not exist with k-nn, while EER was observed to be 0.25 at threshold value 0.45 for Mahalanobis distance classifier. The result can further be explained for GAR obtained in the experiment for both algorithms as shown in the Figure 5.

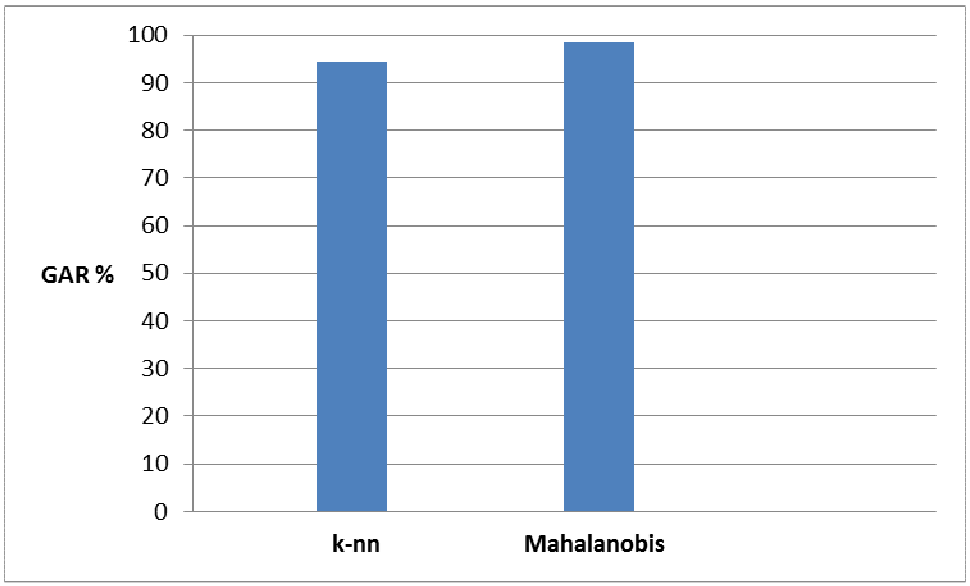

Figure 5: GAR for both Algorithms.

5. CONCLUSION

This research has examined the performance of k-nn and Mahalanobis distance metrics on LBP feature descriptor. The research was benchmarked on Locally acquired face data made up of high intra class variance which is typical of real time scenario of face data. The performance of Mahalanobis distance on the feature descriptors outperformed k-nn classifier from the numerical results obtained in the course of the experiment. In future, we are interested experimenting with huge and robust face data set such as labeled face in the wild (LFW) and Pose Illumination and Expression (PIE) database.

REFERENCES

1. T Ojala., M Pietikäinen., and T Mäenpää.. (2002) "Multi resolution gray-scale and rotation invariant texture classification with local binary patterns". IEEE Transactions on Pattern Analysis and Machine intelligence, 24: 971–987
2. Babatunde R. S, Olabiyisi S. O, Omidiora E. O, Ganiyu R. A. (2015) Local Binary Pattern and Ant Colony Optimization Based Feature Dimensionality Reduction Technique for Face Recognition Systems. British Journal of Mathematics & Computer Science. Article no. BJMCS.19490. ISSN: 2231-0851 Science Domain International. Volume 11. No.5 pp1-11
3. Babatunde R. S, Olabiyisi S. O, Omidiora E. O, Ganiyu R. A, Isiaka R. M. (2015). Assessing the performance of Random Partitioning and K-Fold Cross Validation methods of evaluation of a Face Recognition System. Society for Science and Education, Journal of Advances in Image and Video Processing..Vol 3, No 6. pp.18-26
4. Aluko J. O, Omidiora E. O, Adetunji A. B., Odeniyi O. A.(2015). "Performance Evaluation Of Selected Principal Component Analysis-Based Techniques For Face Image Recognition". International Journal Of Scientific and Technology Research. 4(1):35-41
5. Adedeji O. T, Omidiora E. O, Olabiyisi S. O and Adigun A. A. (2012)."Performance Evaluation of Optimised PCA and Projection Combined PCA methods in Facial Images". Journal of Computations and Modelling, 2(3): 17-29
6. Schapire, R.E., Freund, Y., Bartlett, P., Lee,W.S.: Boosting the margin: A new explanation for the effectiveness of voting methods. Annals of Statistics 26(5), 1651–1686 (1998)
7. Adnan Affandi, Mohammed Awedh, Mubashshir Husain & Ahmed Alghamdi: (2013) RFID and Face Recognition Based Security and Access Control System. International Journal of Innovative Research in Science, Engineering and Technology Vol. 2, Issue 11, pp. 5955-5964
8. Dmitry Bryliuk and Valery Starovoitov. (2012): Access control by face recognition using neural Networks. 11th International Conference on Neural Networks and Artificial Intelligence http://neuroface.narod.ru
9. Ylber Januzaj, Artan Luma, Ymer Januzaj and Vehbi Ramaj (2015): Real time access control based on recognition. International Conference on Networks security & Computer Science (ICNSCS-15), Antalya (Turkey). pp.7-12
10. Rahim Abdur, Azam Shafiul, Hossain Nazmul Islam Rashedul. (2013). "Face Recognition using Local Binary Patterns (LBP)" Global Journal of Computer Science and Technology. Graphics and Vision. 13(4).
11. Rose R. Reena and Suruliandi A. (2011). "Improving Performance of Texture Based Face Recognition Systems by Segmenting Face Region" International Journal of Networks Security, 2(3):23-27.
12. Ojo, J.A. and Adeniran, S.A. (2011). "One-sample Face Recognition Using HMM Model of Fiducial Areas". International Journal of Image Processing (IJIP), 5(1):733-743
13. Shan Caifeng, Gong Shaogang, and McOwan Peter W. (2009). "Facial expression recognition based on Local Binary Patterns". A comprehensive study. Image and Vision Computing 27.pp 803–816. doi.10.1016/j.imavis.2008.08.005