PROJECT REPORT
REVOCABLE BIOMETRIC SYSTEM BASED ON LOG GABOR FEATURES AND HOG FEATURES-A COMPARATIVE STUDY

Arpita Nema (202116004), Ambuj Mishra (202116003)

Dhirubhai Ambani-Institute of Information and Communication Technology, Gandhinagar, Gujarat

ABSTRACT

Biometrics are considered as the most advanced security solutions in the market. They offers greater security and convenience than traditional methods of personal recognition. Biometrics for security and security for biometrics are essential. This work devises the comparative analysis of log-gabor XOR based and HOG features based revocable biometric systems. A thorough analysis is performed to study the performance and non-invertibility of both the approaches under stolen token scenario on ORL face dataset. We received 100% accuracy for both the approaches for legitimate token scenario.

Index Terms— Histogram of Oriented Gradients (HOG), log-Gabor filter, revocable biometric, Support Vector Machine, Kernel Discriminant Analysis.

1. INTRODUCTION

Astonishingly versatile face recognition technology is used in wide variety of applications from consumer centric to law enforcing. The face recognition systems for authentication is common these days but it is extravagantly prone to as an adversary may use printed photographs or video playback attack. Concerns about the safe keeping of the biometric modalities are prevalent now. This has given rise to the revocable biometric systems.

In revocable biometric system, instead of storing the original biometric, pseudo identities are stored in the database. So, even in case of adversities the original biometric sample is not leaked. In our work, we considered only facial images but it is expected that these methods are versatile enough to be applied on other biometric modalities as well.

In our work, we tried to analyze two different revocable biometric system approaches. In first approach, we transformed the data into higher dimensional space using log-gabor filter and in the other approach dimensionality has been reduced using HOG features. The Log-Gabor filter is preferred to analyze both frequency and space components simultaneously. It is considered best alternative as it better fits the resemblance with natural appearance of images. The Histogram of Oriented Gradients (HOG) as a feature descriptor is the fastest method for face detection on general-purpose CPU.

This document is organised to have related works and proposed methodology in following section. Section II mentions about the cognate work of some revocable biometric approaches along with face recognition based desktop security applications. Section III discusses the approaches to built revocable biometric system. Section IV illustrates implementation details and results. Section V gives the analysis of the approaches. Section VI mention the future work with concluding remarks in section VII.

2. RELATED WORKS

Most of the already existing approaches focus on feature level transformation to develop revocable biometric system. These approaches are mainly classified as biometric salting and non-invertible transformations.

BioHashing is a type of biometric salting in which biometric features is combined with tokenized (pseudo) random number (TRN) to generate BioCodes [1]. This technique has been reportedly to have zero equal error rate [2, 1, 3].

[4] proposes biometric salting for creating revocable face templates using and random kernels and Minimum Average Correlation Energy (MACE) filter. [5] presented use of non-linear operations for robust hashing technique for face templates to achieve improved security.

[6] proposed Biotokens which is a cryptographically secure technique for face templates. This divides data into two parts. Encoding that approximates a match uses one segment of data and the other segment is used for compuatation of support robust distances.

Our work is based on BioPhasoring which generates cancelable fingerprints based on multichannel Gabor filter to address the invertibility issue [7].

3. PROPOSED ALGORITHM

We used two different approaches to develop a revocable biometric system. For the first approach, we have used Log-Gabor features and HOG features for the other one.

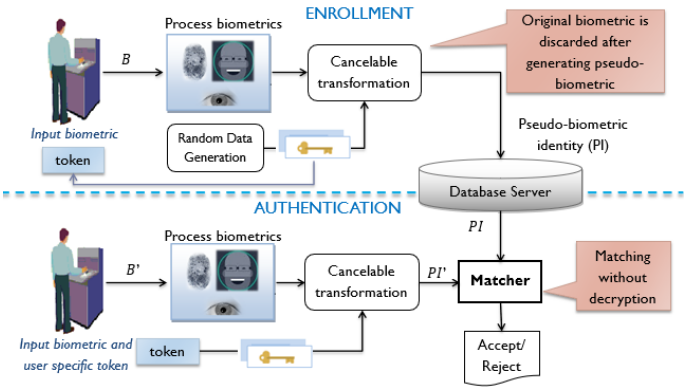

Fig. 1: Basic Architecture of Revocable Biometric System

3.1. Approach 1 - log Gabor and XOR based transformation

Facial images after pre-processing, are passed through log-Gabor filters. These filters are applied at four scales and six orientations to generate 24 images which are of same size as the original image. The magnitude and the phase spectrum for each of these 24 images are salted at feature level by applying XOR operation between them and the random grid matrix. This random grid matrix contains the key mapped with the password of the users. This is followed by application of Median Filter to induce invertibility. Further, all these transformed images are flattened and concatenated to form final feature vector and final classification is done using Kernel Discriminant Analysis.
Overall transfer function for log-gabor filter:

$$\mathrm{G}(r,\Theta) = \mathrm{G}_r(r).\mathrm{G}_\theta(\theta)$$

$$= \exp\left(\frac{\log(\mathrm{r}/\mathrm{f}_0)}{2\sigma_r^2}\right).\exp\left(\frac{-(\theta-\theta_0)^2}{2\sigma_\theta^2}\right)$$

where (r,Θ) represents polar coordinates and f_0 is the center frequency of the filter.

3.2. Approach 2 - Histogram of oriented gradients based revocable system

In this approach Histogram of Oriented Gradient (HOG) function is applied on every profile image to obtain a corresponding HOG feature array. The distributions (histograms) of directions of gradients (oriented gradients) are used as features in HOG descriptor. In this approach also user's password is mapped to key. The number of elements present in the key is equivalent to the size of HOG feature descriptor.The HOG feature array and the key is partitioned into two halves (x1, y1) and (x2, y2) respectively. Next step is the calculation of the euclidean distance between (x1, y1) and (x2, y2). Further, non linear filtering technique is applied to generate the transformed feature vector.

Support Vector Machine (SVM) Classifier in machine

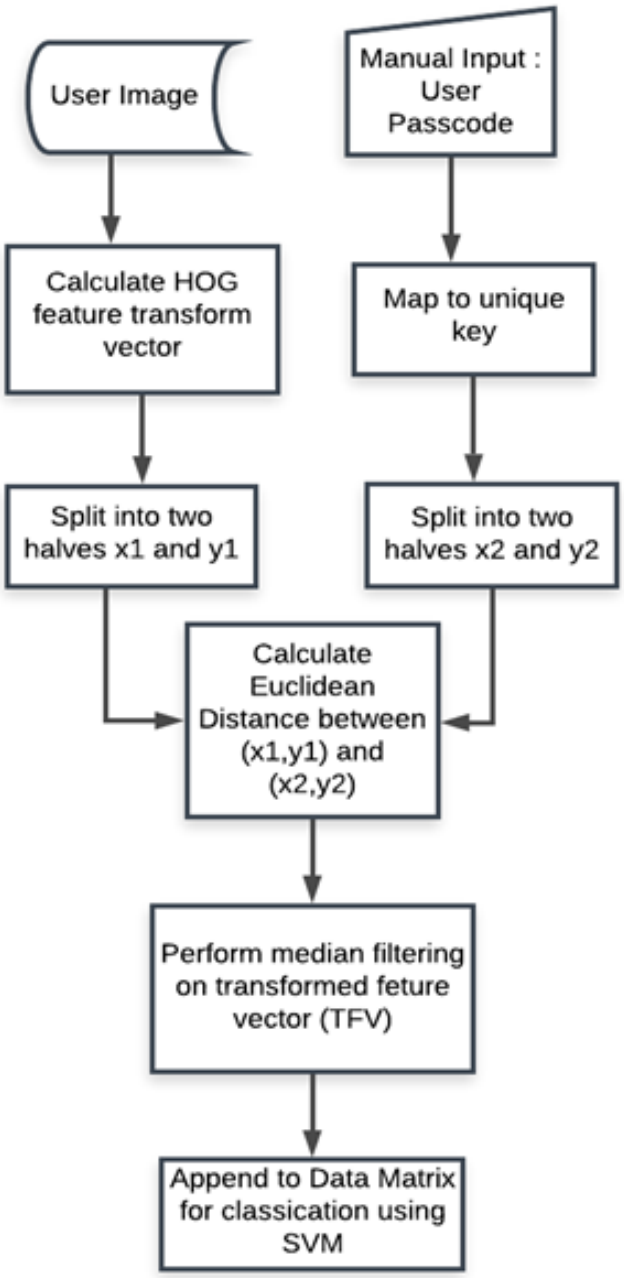

Fig. 2: Flow Chart for Approach-2

learning, SVM solves various regression and classification problems. The goal of the SVM method is to determine the best line or decision boundary for categorizing n-dimensional space in categories such that subsequent data points can be easily placed in the right category. SVM can be used for classification as well as pattern recognition applications of speech data and emotion data etc.

$$min_{w,b,D} \quad \frac{1}{2}W^T W + C\sum_{i=1}^{n} D_i \tag{1}$$

$$y_i(W^T\phi(x_i) + b) \geq 1 - D_i \tag{2}$$

where, C is regularization parameter,
D_i is the margin correction distance with $D_i \geq 0$, i=1...n,
$W^T W$ = $||W^2||$ denotes the normal vector,
$\phi(x_i)$ represents the transformed input vector space,
b represents the bias parameter,
y_i denotes the i-th target value.

For one-vs-one multi-class classification, the number of classifiers necessary can be retrieved with the following formula (with n being the number of classes and 5 for our problem):

$$n * (n-1)/2 \tag{3}$$

The objective is to find w and b such that most audios are predicted accurately. The kernel function explicitly maps every data point in the input space into a higher-dimensional space. In our solution, we used a linear kernel.

$$k(x_i, x_j) = x_i * x_j \tag{4}$$

In the proposed model, we made use of the simple SVM to cater to the given task.

4. IMPLEMENTATION AND RESULTS

Software script is implemented using python which makes it multi-platform application. We did a 10-fold stratified cross-validation of the whole data to get the generalized results and evaluate the performance of the revocable biometric system on the ORL face database.

ORL Database
Captured within April 1992 and April 1994, this database is composed of facial images. Vision, Robotics and Speech Group of the Engineering Department, Cambridge University uses this database in various face recognition projects. For each of the 40 different individuals, 10 distinct images were taken. Images were captured by varying face details and expressions and at various intervals of time. This makes it an apt choice to get incorporated into the recognition task.

Approach 1
In this approach, we first calculated log- Gabor features for 4 scales and 6 orientations and performed XOR with random grid matrix and used KDA to reduce the dimensionality and used Mahalanobis cosine distance for evaluating the similarity.

Table 1: Approach 1-Matching Performance Accuracy (%) for ORL Database

Methods and Evaluation Scores		
Evaluating Method	***Average Accuracy***	***Equal Error Rate***
Best Case	**100.0**	**0.0**
Worst Case	**97.50**	**0.59**

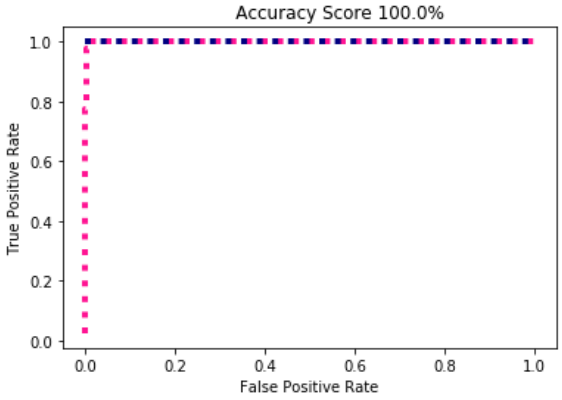

Fig. 3: Best Case Accuracy for Approach-1

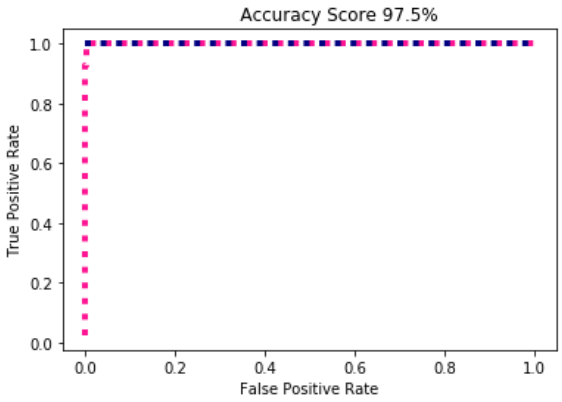

Fig. 4: Worst Case Accuracy for Approach-1

Approach 2
In this approach, we first calculated HOG features, applied transformation to make it non-invertible and trained SVM classifier to make predictions.
We evaluated the performance under three cases:
Case 1 - When each user uses a unique passcode

Case 2 - Same passcode is used by all users
Case 3 - When users' original HOG features are used for classification

Table 2: Approach 2-Matching Performance Accuracy (%) for ORL Database

Fold number and Evaluation Scores			
Fold	***Case 1***	***Case 2***	***Case 3***
1	**100.0**	**92.5**	**100.0**
2	**100.0**	**77.5**	**97.5**
3	**100.0**	**92.5**	**100.0**
4	**100.0**	**90.0**	**97.5**
5	**100.0**	**87.5**	**100.0**
6	**100.0**	**100.0**	**97.5**
7	**100.0**	**87.5**	**92.5**
8	**100.0**	**72.5**	**90.0**
9	**100.0**	**82.5**	**95.0**
10	**100.0**	**77.5**	**92.0**
Average	**100.0**	**86.0**	**96.25**

5. ANALYSIS AND DISCUSSION

In approach 1, we evaluated performance using accuracy and equal error rate. Matching performance of the proposed approach is evaluated in stolen token scenario (worst case) was poor as compared to legitimate token scenario (best case).

In approach 2, we observed that when a unique password mapped key is used, the performance is comparably high. Same password used by more than one user does not help in authentication step and degrades the performance. Original HOG feature performance metric, without use of any password mapped key is comparable to mapped ones.

6. FUTURE WORK

Prospective efforts will be aimed to get variable size feature vectors so that we can control the dimensionality. Modules could be added to detect liveness of the facial images along with the matching process of the revocable biometric system.

7. CONCLUSION

Application to enhance the privacy using revocable biometric system has been proposed. Both approaches discussed are automatic and low-cost solution that does not require any user cooperation. The system testing was conducted in adverse conditions on authentic data that demonstrate the sturdiness and efficacy of the work proposed. The performance evaluation of the log-gabor XOR based approach using KDA for dimensionality reduction and HOG feature based using SVM classifier on ORL dataset have satisfying results.

8. REFERENCES

[1] A. T. B. Jin, D. N. C. Ling, and A. Goh, "Biohashing: two factor authentication featuring fingerprint data and tokenised random number," *Pattern recognition*, vol. 37, no. 11, pp. 2245–2255, 2004.

[2] T. Connie, A. Teoh, M. Goh, and D. Ngo, "Palmhashing: a novel approach for cancelable biometrics," *Information processing letters*, vol. 93, no. 1, pp. 1–5, 2005.

[3] A. Teoh, B. Jin, T. Connie, D. Ngo, and C. Ling, "Remarks on biohash and its mathematical foundation," *Information processing letters*, vol. 100, no. 4, pp. 145–150, 2006.

[4] M. Savvides, B. V. Kumar, and P. K. Khosla, "Cancelable biometric filters for face recognition," in *Proceedings of the 17th International Conference on Pattern Recognition, 2004. ICPR 2004.*, vol. 3. IEEE, 2004, pp. 922–925.

[5] Y. Sutcu, H. T. Sencar, and N. Memon, "A secure biometric authentication scheme based on robust hashing," in *Proceedings of the 7th Workshop on Multimedia and Security*, 2005, pp. 111–116.

[6] T. E. Boult, W. J. Scheirer, and R. Woodworth, "Revocable fingerprint biotokens: Accuracy and security analysis," in *2007 IEEE Conference on Computer Vision and Pattern Recognition*. IEEE, 2007, pp. 1–8.

[7] A. B. Teoh and D. C. Ngo, "Biophasor: Token supplemented cancellable biometrics," in *2006 9th international conference on control, automation, robotics and vision*. IEEE, 2006, pp. 1–5.