Forgery Detection by Biometric Images using SVM Classifier

Anusha R, Deepak Raj K R, Deepak N V, Lakshmi E, Sumitha Manoj
Department of Electronics and Communication
RajaRajeswari College of Engineering
Bangalore, Karnataka

***Abstract*— In this work, we have developed a method for the forgery detection, by the biometric images using an SVM (Support Vector Machine) classifier. We are mainly aiming towards the detection of given query image whether it is genuine or forged. A biometric image here refers to the metrics related to human characteristics such as fingerprints and face recognition. Forgery is a crime of falsely making, this involves false document, signature or any other imitation of an object. Image texture and pixel value based features are extracted and analyzed from the input samples. The process consists of two phases they are training and the testing phase. An SVM classifier which has similar functional form to neural networks is used. SVM classifier is trained with a set of images. SVM classifiers are used to classify whether the given input images are genuine or forged. For the secure use, SVM algorithm can be applied so that only authorized person can run the application to check whether the given query image is genuine or forged**.

Keywords*— *Forgery, biometric images, query image, SVM classifier, training and testing phase, genuine

I. INTRODUCTION

In today's world authentication of a person is must in order to prevent forgery. The method of authentication is to be carried out in order to identify a person. We all know that the issue of crime is happening all over the world. Any illegal activity can be addressed as a crime. Now-a-days People choose illegal methods to earn money, one of the illegal method is a forgery. The crime of forgery is increasing day by day, this may be due to lack of job opportunities, to achieve people comfort zones, greediness and to lead a luxurious life by earning money. A person who is literate or an illiterate undergoes in forging activities due to his/her need. It has been a challenge for the cops in identifying the culprits those who commits different crimes. The detectors can make use of our proposed technique, if they get the samples of biometric images related to the human characteristics in identifying the culprits, since we are dealing with the real time images. The term biometrics is commonly used today to refer to the authentication of a person by analysing physical characteristics such as fingerprints or behavioural characteristics such as signatures. For the individuals the physical and behavioral characteristics will remain unique, when compare to ID cards, keys, passwords, or other traditional systems, biometrics provides a more reliable system of authentication. We have many photo editing tools to manipulate the image, hence we have to maintain the originality of image carefully

Reduction of image dimension, pattern recognition are related to the feature extraction. A knowledge base acts as a storage block or a register which is used to store the complicated structured and unstructured information's that are used by the computer system. SVM (support vector machines) is a learning algorithm which analyze data used for classification and regression. A model of SVM is representation of examples as points in space and are mapped and further divided by a clear gap to separate categories

II. PROPOSED METHODOLOGY

A. Sample input images

First the sample images are captured from the webcam for the training phase. These images are used for creating database. Normally training phase has to be carried with the sample input images of few number to create the database.

B. Pre-processimg

This is the step to be carried for every image that we capture. It involves resizing, gray scale conversion and filtering process.

Resizing: The 2D sample images will have different sizes which makes process difficult in order to avoid processing difficulties the image is resized to 512*512. Resizing all the images to a same dimension is necessary

Grey image: Gray scale conversion is carried out with the following equation

$$0.2989*R+0.5870*G+0.1140*B$$

Filtering: This process is carried with the image in order to remove the noise present (if any). Gaussain filter used here mainly will remove the blurness of the image captured,

The region of interest (ROI) in the image is the face, finally the face is recognized from a filtered image using bounding box and cropped.

C. Feature Extraction

This is done after preprocessing phase in the system. It aims at the extraction of the relevant information that characterizes each class. In this process relevant features are extracted from the image to form feature vectors. These feature vectors are then used by classifiers to recognize the input with the intended output unit. This becomes easier for any classifier to classify between different classes by looking at the features as it allows an easy method to distinguish. Feature extraction is the process of retrieving the important part of data from the given raw data.

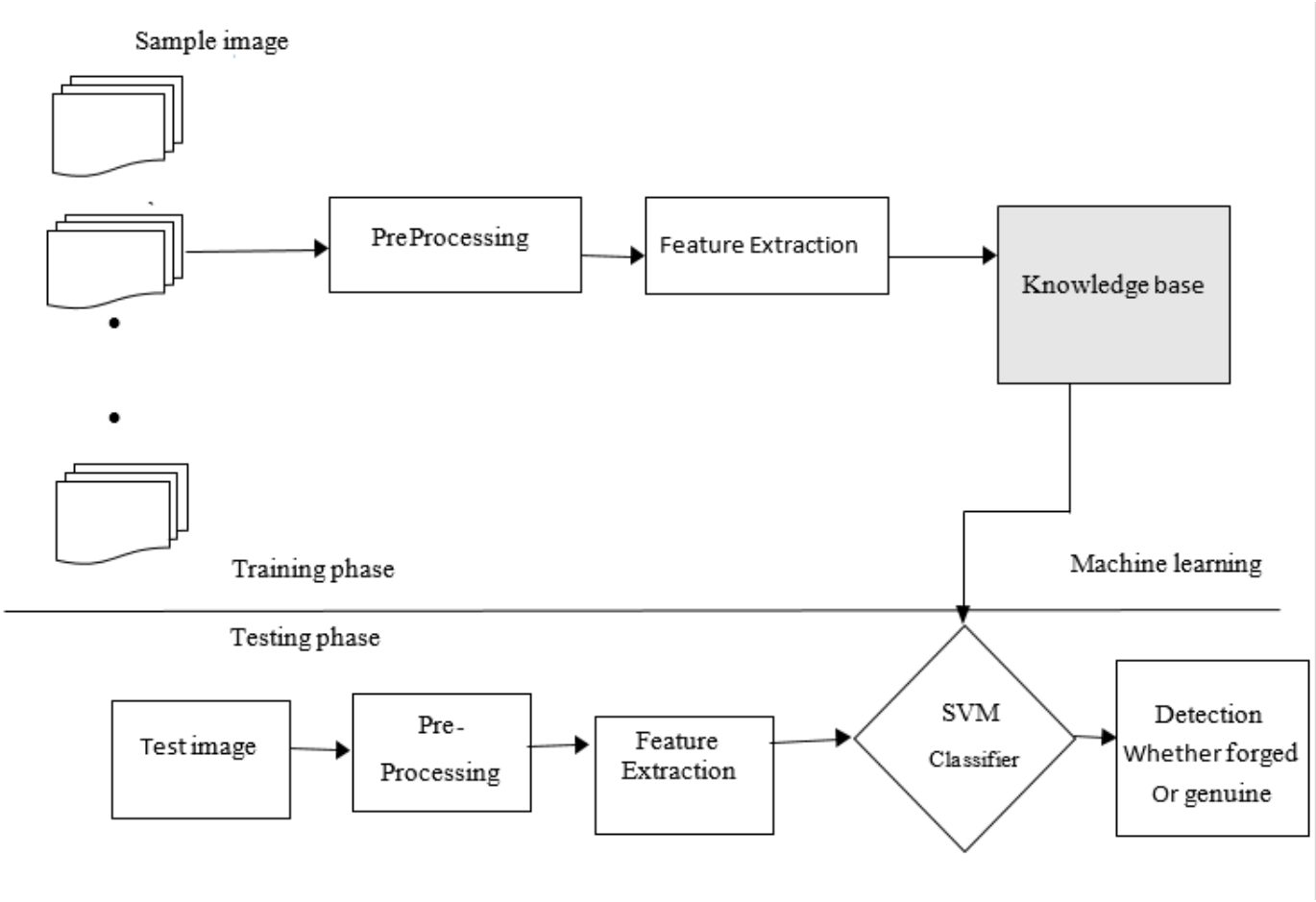

Fig. 1. Block diagram of the system

D. Knowledge base

The complete database is stored in the knowledge base after the training phase in order to compare with test or query image which is to be checked for its genuineness.

This provides the source for the classifier to distinguish as forged or genuine

E. SVM classifier

After the feature vectors are obtained and normalized SVM is employed to classify the images. A supervised learning algorithm called SVM seeks a decision boundary (which is normally called hyperplane) with the maximum margin for the training set. Support Vector Machine which can be used for both classification and regression challenges. Support Vector Machine is a one which best segregates the two classes (hyper-plane/ line).

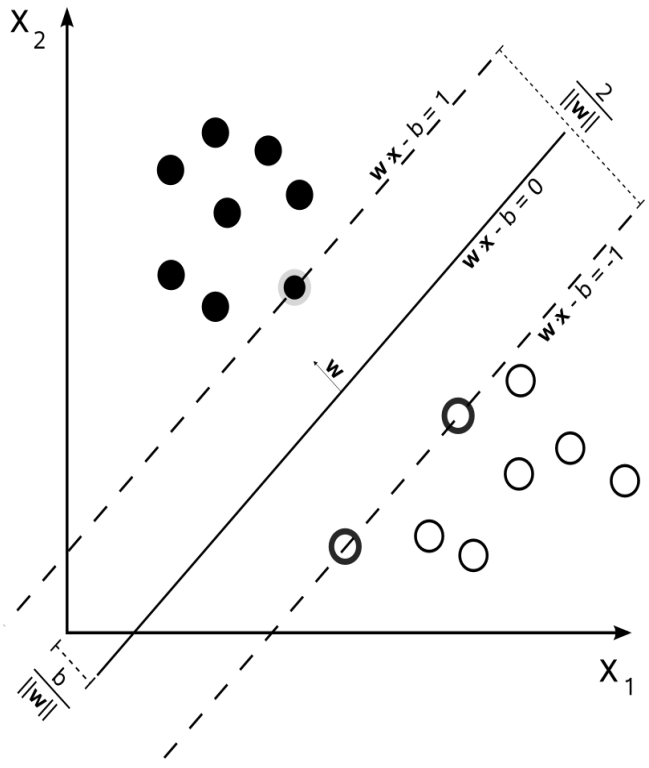

Fig.2: Maximum-margin hyperplane and margins for an SVM trained with samples from two classes. Samples on the margin are called the support vectors.

III. FEATURE EXTRACTION

Transforming of input data into set of features is referred as feature extraction. We use DWT (Discrete wavelet Transformation) transformation to the preprocessed image after cropping the detected face.

On applying DWT we get high and low frequency components such as approximated and detailed coefficients. In order to extract we take only approximated coefficient (LL) to make the extraction easier. Detailed coefficients are neglected and DWT features are extracted from calculating mean of the Approximated coefficients.

The process of DWT transformation is shown in the flow diagram

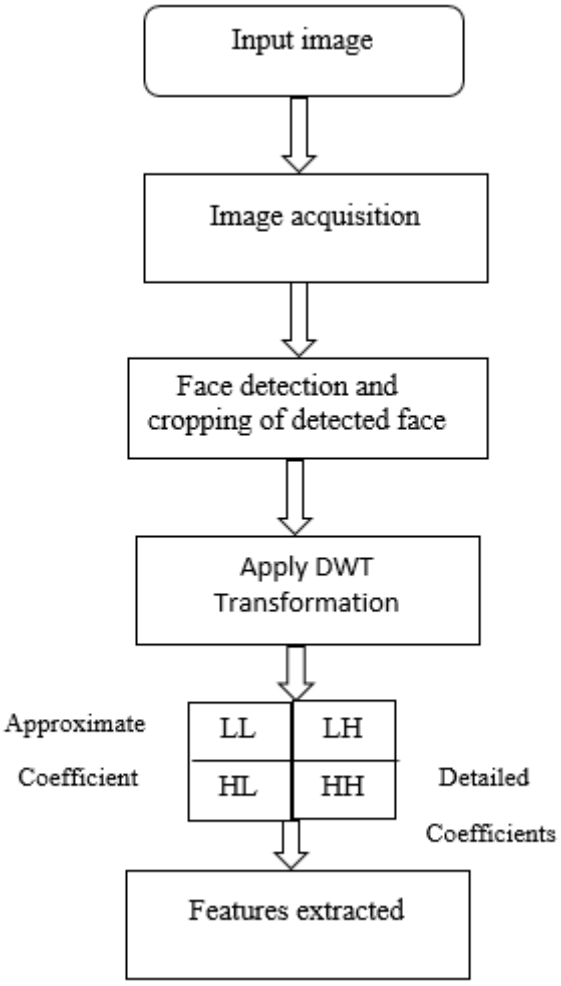

Fig.3: Flow diagram

Principle component analysis(PCA)

PCA is a technique used to emphasize variation and bring out strong patterns in a dataset. It's often used to make data easy to explore and visualize. PCA is a mathematical procedure that uses an orthogonal transformation to convert set of observations of possibly correlated variables into a set of linearly uncorrelated variables called principal components. The total principle components are less than or equal to original variables. It is sensitive to relative scaling of the original variables.

PCA is an unsupervised technique and as such does not include label information of the data. If data are normally distributed then principle components are independent. PCA reduces the number of original variables by eliminating the last principle components that do not contribute significantly to the observed variability. PCA is a linear transformation of data that minimize the redundancy (measured through covariance) and maximize information (measured through variance). Main application areas of PCA include data compression, image analysis, visualization, pattern recognition, regression, and time series prediction.

IV. MINUTIAE EXTRACTION

The most popular and widely used biometric identification method is fingerprint recognition. Fingerprints are unique and remain permanent throughout a person's life. Among all the biometrics, fingerprint recognition is the most reliable and promising person identification technology. The uniqueness of fingerprint has been studied and the probability of two fingerprints being alike is 1 in 1.9 x 1015. In biometric process of finger scanning, a point where ridge ends abruptly is called ridge ending and a point where ridge forks into branches is called ridge bifurcation. These are usually called minutiae and are prominent structures used in fingerprint identification system.

Minutiae can be defined as the points where the ridge lines end or fork. So the minutiae points are the local ridge discontinuities and can be of many types. These types are –

- **Ridge ending** is the point where the ridge ends suddenly.
- **Ridge bifurcation** is the point where a single ridge branches out into two or more ridges.
- **Ridge dots** are very small ridges.
- **Ridge islands** are slightly longer than dots and occupy a middle space between two diverging ridges.
- **Ponds or Lakes** are the empty space between two diverging ridges.
- **Spurs** is a notch protruding from a ridge.
- **Bridges** are the small ridges that join two longer adjacent ridges.
- **Crossovers** are formed when two ridges cross each other.

In case of a fingerprint identification system, the captured fingerprint image needs to be matched against the stored fingerprint templates of every user in the database.

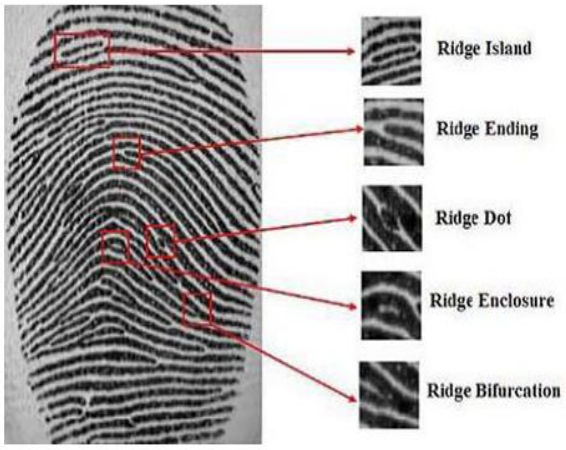

Fig.4: Common minutiae patterns

V. RESULTS

The training of a set of input images is carried out to create the database. The feature vectors are stored and they are compared with the feature vectors of the given query image to distinguish as genuine or a forged.

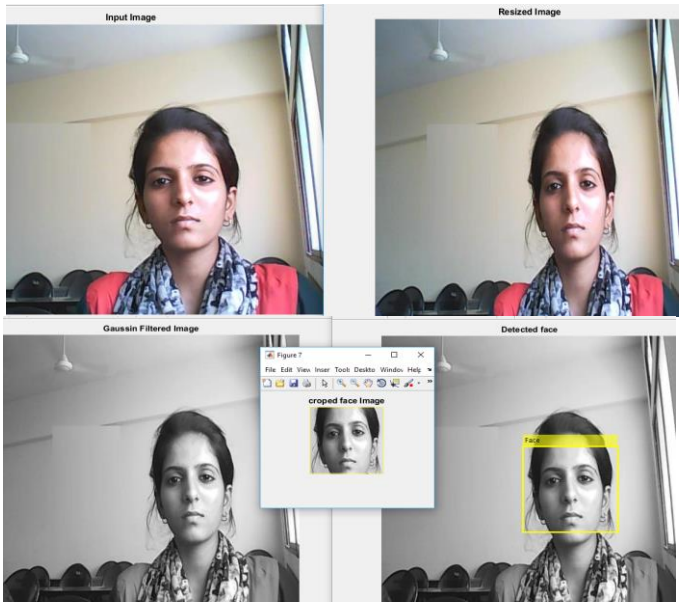

Fig.5: Image acquisition and detection of face

The feature extraction of an input image is done and feature vectors are compared with the database.

Next step is to input the fingerprint as a query image. The minutiae extraction of fingerprint is done and displays message as “person identified“if the database holds the same feature value as that of the queried feature value, or else if the feature is found different then it displays “unauthorized person”.

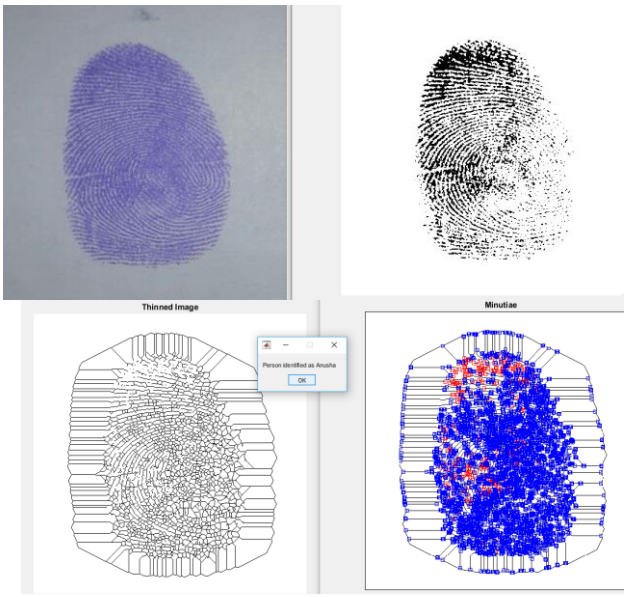

Fig.6: Minutiae extraction

If an unauthorized person image is given as query image then the following results were obtained displaying “unauthorized person”

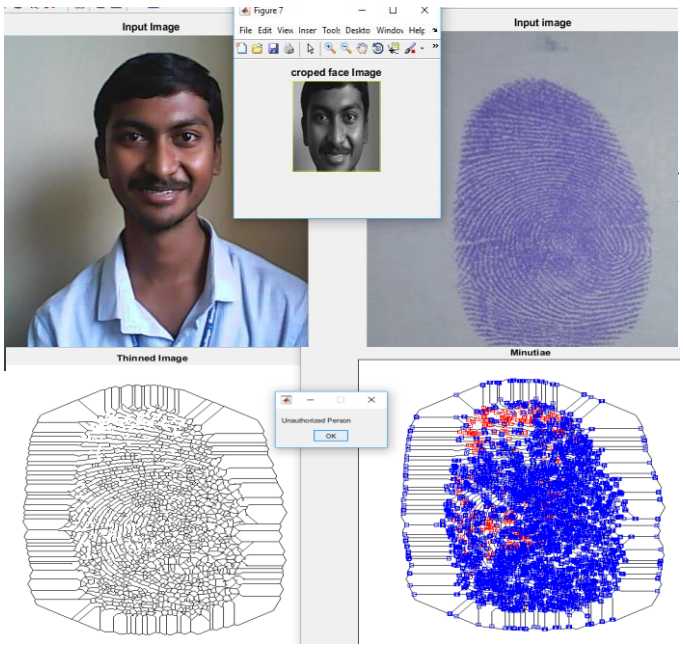

Fig.7: Results when an unauthorized person image and fingerprint is given for test

Given query image is checked whether it is as genuine or forged on comparing the feature values of query image with the database.

FUTURE SCOPE

The database is created for a few number and tested with the query image. Further the increase in number of users for database is needed. This is to be implemented further. The biometrics used here are only face recognition and fingerprint recognition, further iris recognition and other biometrics considered for verification.

REFERENCES

[1] Forgery Detection in Biometric System with Efficient Image Analysis International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 9,September 2015

[2] IMAGE FORGERY DETECTION USING SVM CLASSIFIER , IEEE Sponsored 2nd International Conference on Innovations in Information Embedded and Communication Systems ICIIECS'15

[3] SVM classification for fake biometric detection using image quality assessment: application to iris, face and palm print, INTERNATIONAL JOURNAL OF INNOVATIONS IN ENGINEERING RESEARCH AND TECHNOLOGY [IJIERT] ISSN: 2394-3696 VOLUME 2, ISSUE 2 FEB.-2015

[4] A Survey on Image Forgery Detection Techniques, Tu K.Huynh, Thuong Le-TienKhoa V.Huynh, Sy C.Nguyen, The 2015 IEEE RIVF International Conference on Computing & Communication Technologies Research, Innovation, and Vision for Future (RIVF)

[5] An Improved Method For Copy-move Forgery Detection In Digital Forensic, 2016 Online International Conference on Green Engineering and Technologies (IC-GET)

[6] Human Identification and Verification based on Signature, Fingerprint and Iris Integration, Vikramaditya Agarwal, Akshay Sahai, Akshay Gupta, Nidhi Jain, Department of Electrical and Electronics, MAIT, GGSIPU

[7] Facial marks: Soft Biometric for face recognition, A.K. Jain, U Park, ICIP'09 Proceedings of 16th IEEE, International confernce on Image Processing, 2009

[8] A Detailed Review of Feature Extraction in Image Processing Systems, Gaurav Kumar, Pradeep Kumar Bhatia, 2014 Fourth International Conference on Advanced Computing & Communication Technologies

[9] Fingerprint Feature Extraction using Ridges and Valleys,c Department of Computer Engineering,Punjabi university, Patiala, India

[10] Minutiae Based Partial Fingerprint Registration and Matching Method, Prof. Dr. Asaf VAROL, Naveed AHMED, Dept. of Software Engineering Firat University Elazig, Turkey

[11] Minutiae Extraction from Fingerprint Images - a Review, Roli Bansal, Priti Sehgal and Punam Bedi IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 3, September 2011

[12] Minutiae-based Fingerprint Extraction and Recognition, Naser Zaeri Arab Open University Kuwait

[13] Fingerprint Feature Extraction, Shaifali Dogra, Dileep Sharma Electronics and Communication Eternal University Baru Sahib, HP India, International Journal of Advanced Research in Computer Science and Software Engineering

[14] Minutiae and Corner Detection in Fingerprints without Image Enhancement for Real Time Recognition, Rabih Nachar and Elie Inaty, Patrick J. Bonnin and Yasser Alayli, Patrick J. Bonnin and Yasser Alayli

[15] Fingerprint Identification by Wave atoms Transform and SVM, Leila Boutella and Amina Serir, 2017 International Conference on Advanced Systems and Electric Technologies (IC_ASET)

.