Living Passport By Two Level Authentication Using Iris And Cryptographic In National Border

Kirthana Barathy.J.P.[1], Arokia Magdaline.S.[2]
[1] Dept of ECE
[2]HOD, Dept of ECE
[1, 2] Parisutham Institute of Technology and Science.

Abstract- *It is a security based concept in the fields where we are using our iris recognition. Problems being faced by the people living near the International Border and the Line of Control (LoC) in Jammu and Kashmir. Additionally, cultural radicalism which is targeted on India, and terrorists and mafia groups are patronized by some of India's neighbouring states. There is cross border smuggling problem of drugs, cattle, humans, artifacts, fake currency note etc. Unfortunately, in this scenario our border forces appear to be severely undermanned and under-equipped which is taking heavy toll on economic, social and political stability of our country. Border management becomes more important for the fact that India is like island of democracy between seas of anarchical or instable states. Biometric passport (e-passport) is to prevent the illegitimate entry of traveller into a particular country and border the use of counterfeit documents by more accurate identification of an individual. The electronic passport, implemented here , have two new technologies:cryptography authentication protocols and biometrics (face, fingerprints, palm prints and iris). Goal of the adoption of the electronic passport is not only to accelerate processing at border crossings, but also to increase safety measures.*

Keywords- DNA, RFID, MRZ, MRTD, PNN, SVM, Feature Selection, Feature Extraction.

I. INTRODUCTION

NATIONAL BORDER CONTROLS

The existing implementation was an effort to understand how the presence on biometric passport using cryptographic authentication towards their improved identification. The application of facial, fingerprint, palm print and iris recognition in passports requires high accuracy rates; secure data storage, secure transfer of data and reliable generation of biometric data. The passport data is not required to be encrypted, identity thief and terrorists can easily obtain the biometric information. The discrepancy in privacy laws between different countries is a barrier for global implementation and acceptance of biometric passports. The cryptographic key is used to decrypt passport data and forces thieves to physically obtain passports to steal personal information. More research into the technology, additional access and auditing policies, and further security enhancements are required before biometric recognition is considered as a viable solution to biometric security in passports. The inclusion of multiple biometric identification information into machine readable passports will improve their robustness against identity theft if additional security measures are implemented in order to compensate for the limitations of the biometric technologies. It enables countries to digitize their security at border control and provides faster and safer processing of an e-passport bearer. E-passports may provide valuable experience in how to build more secure and biometric identification platforms in the years to come.

1.1 Biometrics

Biometric is an automated methodology to uniquely identify human based on their physiological and behavioural characteristics. A lot of biometric characteristics have been proposed for authentication purpose. Traditionally, the biometric method can be categorized into two types: behavioural-based method and physiological based method. In behavioural based method perform task of authentication based on their behavioural characteristics, such as, keyboard typing, signature, gait and voice. the main problem with behavioural based method they all have large variation, can't cope with and can be difficult to measure because of influences such as illness or stress. The Implementation of behavioural based method less cost. Physiological-based method perform authentication by means of his and her physiological characteristics such as, face, fingerprint, hand geometry, iris or DNA. In general physiological based methods are more stable than methods in behavioural category because non-alterable of physiological based method.

1.2 Iris recognition system

Iris recognition technology encodes and matches iris patterns to identify enrolled users. Iris recognition systems are comprised of collection devices and encoding / matching

engines. Collection devices include advanced imaging and optics components along with one or more infrared illuminators. Images may be encoded and matched on the device, on a host PC, or on a central server. Iris recognition technology requires the acquisition of a high-resolution, infrared-illuminated image to effectively locate and encode iris data.Iris recognition technology is imbedded in peripheral cameras no larger than typical web cams, and is also build into wall-mounted and kiosk-based form factors for access control and identification applications. The latter types have been deployed successfully in air travel applications, and are generally capable of acquiring higher-quality iris images (and therefore providing higher degrees of accuracy). Once the iris is located and segmented, a grayscale image is used for feature extraction. Characteristics derived from the iris include the orientation and spatial frequency of furrows and striations. Iris recognition is recognized for (1) resistance to false matching regardless of database size and (2) rapid searches of large databases. Assuming that thresholds are properly implemented, false positive matches should be exceptionally rare. In fact, some iris systems are implemented such that all matches are assumed to be positive. The trade-off is that iris systems may be more prone to false negatives (in which an enrolled subject is falsely not identified) than, for example, fingerprint systems.

1.3 Problem :

Problems being facedby the people living near the International Border and the Line of Control (LoC) in Jammu and Kashmir.Additionally, cultural radicalismwhich is targeted on India, and terrorists and mafia groups are patronized by some of India's neighboring states. There is cross border smuggling problem of **drugs**, cattle, humans, artifacts, fake currency note etc.

1.4 Solution :

Biometric passport (e-passport) is to prevent the illegitimate entry of traveller into a particular country and border the use of counterfeit documents by more accurate identification of an individual.

1.5 MATLAB Image Processing Toolbox

Image processing toolbox provides a comprehensive set if reference- standard algorithms, functions, and apps for image processing, analysis, visualization, and algorithm development. It can perform image analysis, image segmentation, image enhancement, noise reduction, geometric transformations, and image registration. Image processing toolbox supports a diverse set of image types, including high dynamic range, giga pixel resolution, embedded ICC profile, and tomographic. Visualization functions and apps explore images and videos, examine a region of pixels, adjust color and contrast, create contours or histograms, and manipulate regions of interest. The toolbox supports workflows for processing, displaying, and navigating large images.

II. DESIGN ASPECTS

2.1 Design :

The Iris Recognition System is shown in**Fig:1**

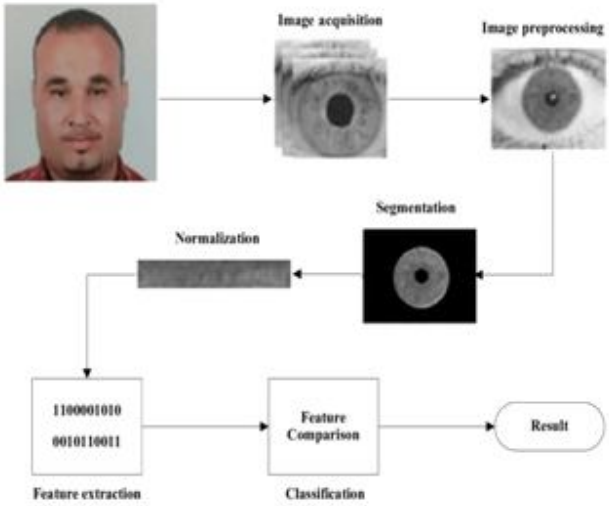

Fig1:Iris Recognition System

In this design,It is a security based concept in the fields where we are using our **Biometrics** (**Iris**). The proposed concept holds two technologies.

- SVM classification
- PNN classification

In our project we are deducting IRIS to attain the accessibility in the airport using e-passport. Our overview is to predict the smuggling problem of drugs, cattle, humans, artifacts, fake currency note etc, and some illegal aspects by providing the authentication through the IRIS. The iris-scan process begins with a photograph. A specialized camera, typically very close to the subject, not more than three feet, uses an infrared imager to illuminate the eye and capture a very high-resolution photograph. This process takes 1 to 2 seconds. The picture of eye first is processed by software that localizes the inner and outer boundaries of the iris. And it is encoded by image processing technologies. In less than few seconds, even on a database of millions of records, the iris code template generated from a live image is compared to

previously enrolled ones to see if it matches to any of them. An iris recognition camera takes a black and white picture from 5 to 24 inches away. The camera uses non-invasive, near-infrared illumination that is barely visible and very safe. And this iris recognition cannot take place without the person permission. As we discussed, the typical iris recognition system is consists of image acquisition, iris pre-processing which includes iris localization and segmentation, iris normalization, feature extraction i.e. encoding and comparison.

2.2 Flow diagram for the proposed design:

The flow diagram of proposed design is shown in **Fig: 2 and Fig: 3**

Module 1:

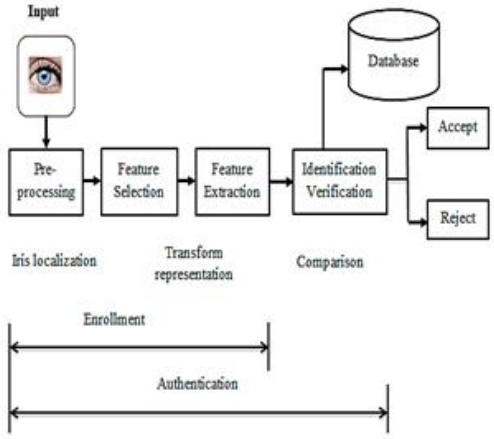

Fig 2: Flow diagram of proposed design

Module 2:

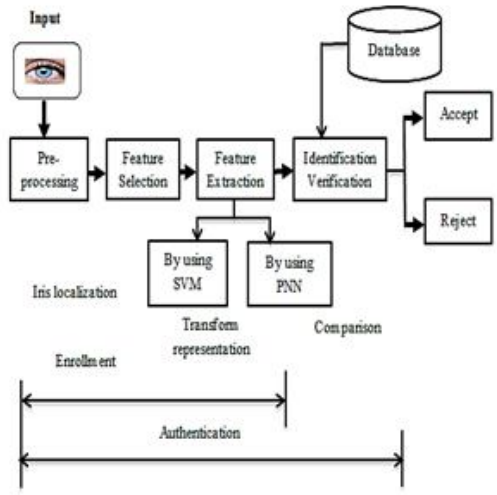

Fig 3: Flow diagram of proposed design

2.3 Design procedure:

The system is represented by seven steps:

Iris Image acquisition, challenge response test, Iris segmentation, iris normalization, iris enhancement, Iris feature encoding and iris matching.

2.3.1 IMAGE ACQUISITION

One of the major challenges of automated iris recognition is to capture a high-quality image of the iris while remaining non-invasive to the human operator. The concerns of the image acquisition are,

- Obtained images with sufficient resolution and sharpness.
- Good contrast in the interior iris pattern with proper illumination.
- Well centered without unduly constraining the operator.

2.3.2 IRIS PRE-PROCESSING

2.3.2.1 Iris Localization:

After getting the input image, the next step is to localize the circular edge in the region of interest. Canny edge detection operator uses a multi-stage algorithm to detect a wide range of edges images. It is an optimal edge detector with good detection, good localization and minimal response. In localization we used this detection, in which the inner and outer circles of the iris is approximated, in which inner circle corresponds to iris/pupil boundary and outer circle corresponds to iris/sclera boundary. But the two circles are usually not concentric. Also, comparing with other parts of the eye, the pupil is much darker. The inner boundary is detected between the pupil and the iris. At the same time, the outer boundary of the iris is more difficult to detect because of the low contrast between the two sides of the boundary. So, we detect the outer boundary by maximizing changes of the perimeter normalized along the circle.

2.3.2.2 Iris segmentation:

Iris segmentation is an essential process which localizes the correct iris region in an eye image. Circular edge detection function is used for detecting iris as the boundary is circular and darker than the surrounding.

2.3.2.3 Iris Normalization:

In normalization the obtained iris regions is transformed in order to have fixed dimensions for the purpose of comparison. The size of pupil may change due to the variation of the illumination and associated elastic deformation in iris texture mayinterface with results of pattern matching. And so, for the purpose of accurate texture analysis, it is necessary to compensate this deformation. Since we have detected both inner and outer boundaries of the iris, it is easy to map the iris ring to a rectangular block of texture of a fixed size. The original image has low contrast and may have non-uniform illumination caused by the position of the light source.These may impair the result of the texture analysis. We enhance the iris image in order to reduce the effect of non-uniform illumination.

2.3.2.4 Feature Selection:

In feature selection, we ex-tract iris features, which are ultimately used in matching. Since there is a large number of iris features and computational time increases as the number of features increases, it is therefore a challenge to develop an iris processing system with as few as possible number of features and at the same time without compromising the correctness.

2.3.2.5 Feature Extraction:

The most important step in automatic iris recognition is the ability of extracting some unique attributes from iris, which help to generate a specific code for each individual. Gabor and wavelet transforms are typically used for analysing the human iris patterns and extracting features from them.

2.3.2.6 Pattern Matching:

The purpose of pattern matching is to establish a precise correspondence between characteristic structures across the two images.

There are Four steps,

- Bringing the newly acquired iris pattern into spatial alignment with a candidate data base entry.
- Choosing a representation of the aligned iris patterns that makes their distinctive patterns apparent.
- Evaluating the goodness of match between the newly acquired and data base representations.
- Deciding if the newly acquired data and the data base entry were derived from the same iris based on the goodness of match.

Matching of two iris code is performed using the Hamming distance. The Hamming distance gives a measure of how many bits are the same between two bit patterns. Using the Hamming distance of two bit patterns, a decision can be made as to whether the two patterns were generated from different irises or from the same one.

2.4Support Vector Machines

In machine learning, support vector machines **(**SVMs**)** are supervised learning models with associated learning algorithms that analyse data used for classification and regression analysis.

So just when we talk about classification there is already four different Support Vector Machines:

1. The original one : the Maximal Margin Classifier,
2. The kernelized version using the Kernel Trick,
3. The soft-margin version,
4. The soft-margin kernelized version (which combine 1, 2 and 3

A Support Vector Machine (SVM) is a discriminative classifier formally defined by a separating hyper plane. In other words, given labelled training data (supervised learning), the algorithm outputs an optimal hyper plane which categorizes new examples. In two dimensionalspace this hyper plane is a line dividing a plane in two parts where in each class lay in either side.

2.5 Probabilistic Neural Network

Consider the problem of multi-class classification. We are given a set of data points from each class. The objective is to classify any new data sample into one of the classes. Consider the problem of multi-class classification. We are given a set of data points from each class. The objective is to classify any new data sample into one of the classes.Probabilistic Neural Network or, PNN can be useful for multi-class classifier.

Architecture

A PNN is an implementation of a statistical algorithm called kernel discriminant analysis in which the operations are organized into a multi-layeredfeed forward network with four layers.

1) Input layer

The input layer contains the nodes with set of measurements. Each neuron in the input layer represents a predictor variable. In categorical variables, N-1 neurons are used when there are N number of categories. It standardizes the range of the values by subtracting the median and dividing by the interquartile range. Then the input neurons feed the values to each of the neurons in the hidden layer.

2) Pattern layer

The pattern layer consists of the Gaussian functions formed using the given set of data points as centers. This layer contains one neuron for each case in the training data set. It stores the values of the predictor variables for the case along with the target value. A hidden neuron computes the Euclidean distance of the test case from the neuron's center point and then applies the RBF kernel function using the sigma values.

3) Summation layer

The summation layer performs a sum operation of the outputs from the second layer for each class.

4) Output layer

The output layer performs a vote, selecting the largest value. The associated class label is then determined.

III. IMPLEMENTATION OF BIOMETRIC PASSPORT SYSTEM

A successful design, deployment and operation of biometric passport systems depend highly on the results for existing biometrical technologies and components. These existing technologies as well as new solutions need to be evaluated on their passport system performance. However it is often forgotten that the biometric (iris, finger, face, palm prints.) is only one part of a fully deployed application. In this design process, to ensure that appropriate mechanisms are in place to reassure such users. This article discusses the requirements, design and application scenarios of biometrical systems in general and the introduction of a new biometrical passport in particular.

3.1 Enrollment Module Of Biometric Passport

The e-passport authentication system is divided into enrollment module and authentication module. The passport users who are included in the enrollment module are e-passport holder, Immigration administrator. It shows the enrollment module in the e-passport authentication architecture design. The e-passport holder registers to the system by providing the personal data and some important documentation to the immigration officer. After that, Immigration Administrator will make the enrollment for the e-passport holder by filling the data into the enrollment system. After enrollment process, the data of the e-passport holder will be encrypted by proposed cryptography technique and stored into immigration database and RFID tag inside the e-passport.

Besides that, Enrollment module also includes the modifying process and deleting process. Deleting process will be carried out if the previous e-passport validation date was expired or the e-passport holder lost their passport. They have to register a new e-passport in order to get an e-passport again. The passport user involve in the authentication module are e-passport holder and check point officer. When e-passport holder arrives to check point, e-passport holder will put the e-passport onto RFID reader, and a signature required key in bye-passport holder so that authentication process can be performed to verify an e-passport holder.

After authentication process authenticated the e-passport holder, RFID reader will read the encrypted data which was stored inside the RFID tag in e-passport. The encrypted data will be sent to the system to match with the encrypted data in the database system. If the encrypted data in the e-passport match with the encrypted data which is stored inside the database during enrollment process, the encrypted data in the e-passport will be decrypted by a certain key. Then the check point officer has to check and verify the identity of the e-passport holder.

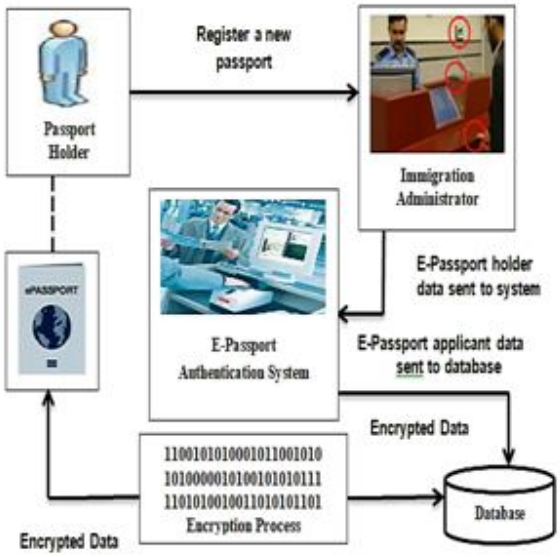

Fig 4: Enrollment Module Of Biometric Passport Authentication Architectures

3.2 Authentication Module Of Biometric Passport

The attributes inherent in the e-Passport provide a here to fore unavailable means of improving the security of the international travel system. These are described below under three general categories: preventing the use of multiple identities; linking the bearer to the document in a traditional border operations environment; and serving as a strong token to drive a biometric identification process. After these uses have been explored in some detail, the paper will examine why the e-Passport may not be universally accepted by states as the sole device used to fully automate the border clearance process for registered participants as envisioned by the process flow.

The personal data stored in the chip as defined to be the mandatory minimum for global interoperability are the MRZ and the digitally stored image of the bearer's face. Both items can also be seen (read) visually after the MRTD has been opened and offered for inspection. Beside the digitally stored image of the face as the primary biometrics for global interoperability, ICAO also has endorsed the use of digitally stored images of fingerprint, palm print and/or irises in addition to the face. To begin, the security policy must ensure that the desired functionality of the system is satisfied.

The following items of the security policy ensure proper functionality of the passport system:

1) Passports should only be usable as authentication documents if issued by correct entities. 2) Passports should only be issued to correct people.3) Passports should only be usable as authentication documents for people to whom they were issued.4) Passports should not be able to be forged.5) Passports should not be able to be copied.

The passport should be usable as an authentication document. The following items provide privacy guarantees about the data stored in the passport and about the passport itself.

1)Digital data on the passport should not be readable unless desired by the owner.2)Digital data on the passport should only be readable by an authorized entity.3) An entity authorized or otherwise, should only be able to detect the presence of a passport if the owner desires.

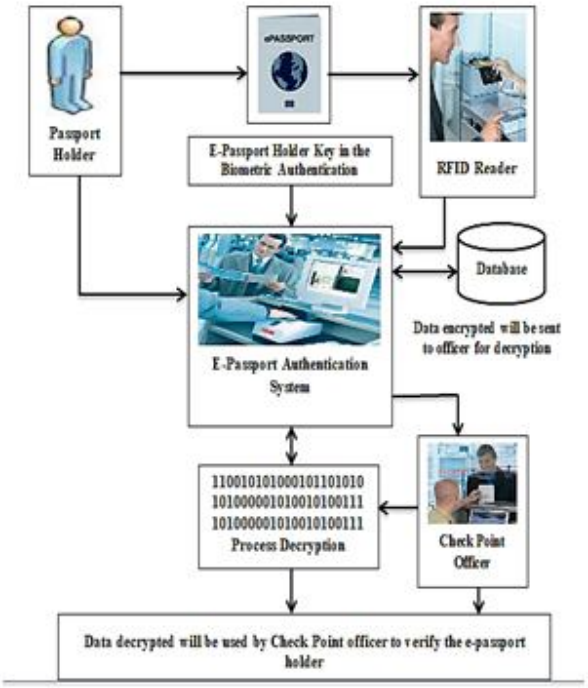

Fig 5:Authentication Module Of Biometric Passport Authentication Architecture

IV. RESULT AND DISCUSSION

In this work, Iris authentication system was developed using classification algorithms SVM and PNN through MATLAB tool to predict effective and better accurate results.We use Pre-processing, image enhancement, morphological operation, feature selection region of interest using segmentation techniques(SVM & PNN), feature extraction and finally classify the image with database whether it is Authenticated or Non-authenticated. Therefore, it reducessmuggling problem of drugs, cattle, humans, artifacts, fake currency note etc..in national borders.

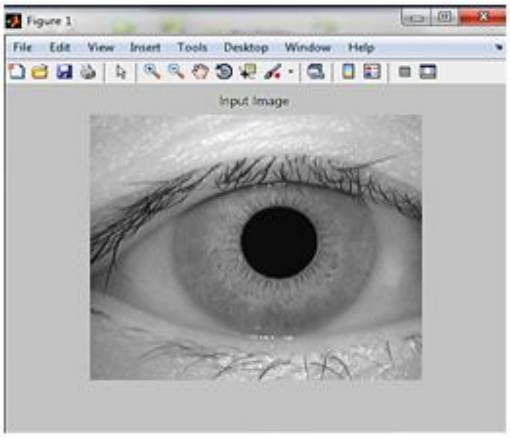

Fig 6: Input Image

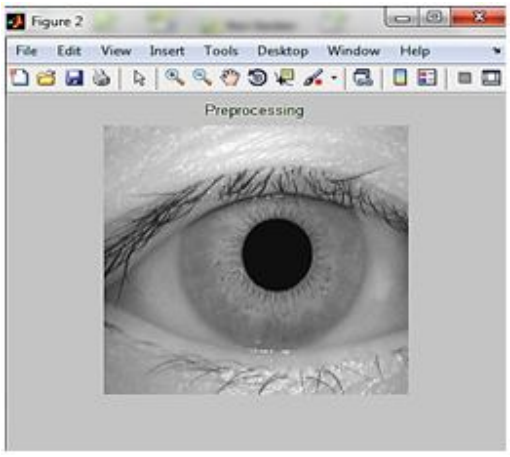

Fig 7: Pre-processing Image

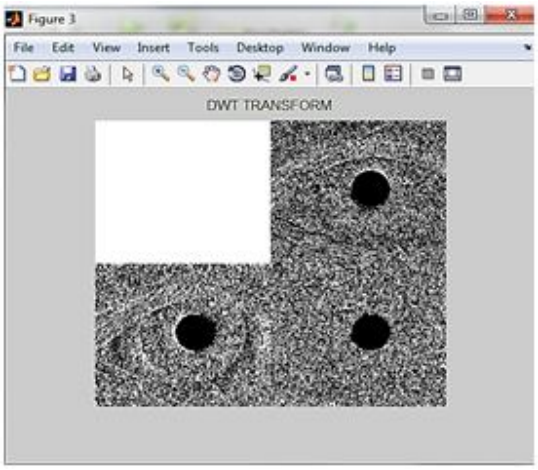

Fig 8: DWT Transform

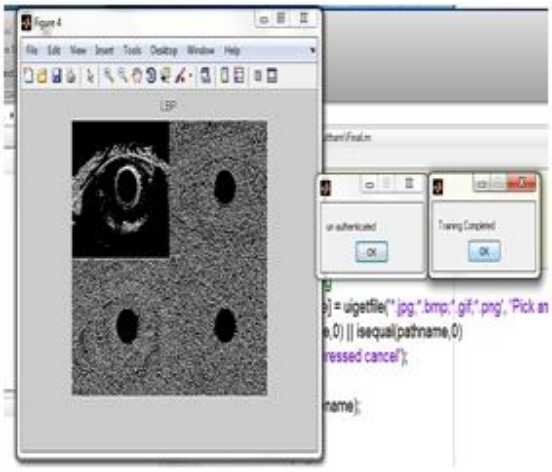

Fig 9:Non-Authenticated Image

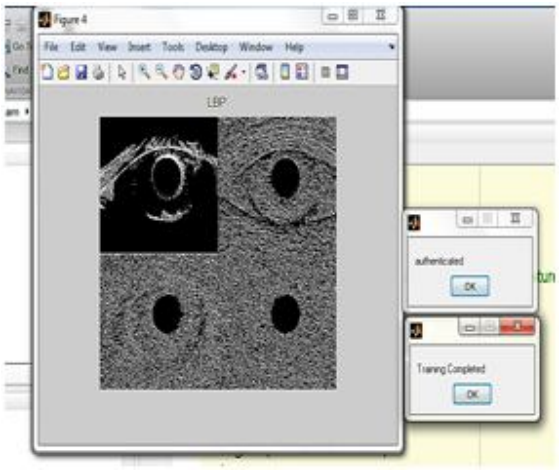

Fig 10:Authenticated Image

IV. CONCLUSION

In this paper, the Iris authentication is the most feasible because of stability throughout the life and its uniqueness. The need for secure methods of authentication is becoming increasingly important. In our project, we designed a living e- passport using Iris authentication by Feature extraction and Classification of data using SVM and PNN We evaluated these two technique and proved that these are best among existing technologies. These concerns may relate to privacy or to safety issues, which may be addressed in part through legal and regulatory measures. Being the successful design, deployment and operation of biometric passport systems depends highly on the results for existing biometrical technologies and components. In our future , our living e-passport is also enriched and fully deployed with other biometric like finger print , Aathar , and QR code for compact and efficient and have shown promising performance

REFERENCES

[1] P.Prabhusundhar, V. K.Narendira Kumar, B.Srinivasan, "Border crossingsecurity and privacy in biometric passport using cryptographic authentication protocol,"[Online].Available:https://ieeexplore.ieee.org/document/6466144/citations#citations

[2] John Daugman,(2009) **"**Iris Recognition at Airports and Border-Crossings**,"**in *Li S.Z., Jain A. (eds) Encyclopedia of Biometrics.* (*SPRINGER, BOSTON, MA*)

[3] V.K. Narendira Kumar, B. Srinivasan, "Design and implementation of e-passport Scheme using cryptographic algorithm Along with multimodal biometrics Technology," *International Journal of Advanced Information Technology (IJAIT) Vol. 1, No. 6, December 2011*

[4] JohnDaugman OBE, "Iris recognition border-crossing system in the UAE," *University of Cambridge* and ImadMalhas, *President and CEO, IrisGuard Inc.*

[5] Mr.SachinS.Bhosale, Mr.RakeshP.Kumawat ,Mr.PramodP.Gadekar, "Person Identification Technique Using Human Iris Recognition," IJRASET,*Volume 4 Issue III, March 2016, ISSN: 2321-9653*.

[6] Riscure Security Lab, *"E-passport privacy attack"*, at the Cards Asia Singapore, April 2006. Page No. 1-56.

[7] Sachin Gupta , AshishGagneja , "Proposed Iris Recognition Algorithm through Image Acquisition technique " IJARCSSE Volume 4, Issue 2, February 2014 , ISSN: 2277. 128X

[8] HOME AFFAIRS JUSTICE, "EU standard specifications for security features and biometrics in passports and travel documents", Technical report, European Union, 2006. Page No. 62-65.

[9] Kang, J.-S. Mobile iris recognition systems: An emerging biometric technology. ProcediaComput. Sci. **2012**, 1,475–484.

[10] Albadarneh, A.; Albadarneh, I.; Alqatawna, J. Iris recognition system for secure authentication based on texture and shape features. In Proceedings of the IEEE Jordan Conference on Applied Electrical Engineering and Computing Technologies, The Dead Sea, Jordan, 3–5 November 2015; pp. 1–6.

[11] Roy, D.A.; Soni, U.S. IRIS segmentation using Daughman's method. In Proceedings of the International Conference on Electrical, Electronics, and Optimization Techniques, Chennai, India, 3–5 March 2016; pp. 2668–2676.