ILivSpot: Secure Biometric System based on Iris Liveliness Detection

Sunil Kumar, Vijay Kumar Lamba, SurenderJangra

Abstract*:Liveliness detection aims to determine whether the iris presented to the sensor belongs to a live subject or it is a fake one. Liveliness detection is to classify input sample into one of the category between fake and real. This work proposes an improved biometric system which recognizes the liveliness of the iris samples in order to increase the security. In this work, the dataset of UBIRIS.v2 is used where input samples are segmented into pupil, sclera and iris and these individual segments are filtered to enhance the quality of the samples. Further, the segmentation using Fuzzy C-Mean and K-Mean clustering methods is done. Different features are extracted and fused thereafter. Fused features are then used as a training data. For testing purpose, a combined dataset of original and fake samples is used and accuracy of the system is calculated with a novel hybrid classifier AHyBrK which is a combination of ANN and KNN. Results achieve 97% accuracy in differentiating between fake and live which is 8.2% better than KNN and 5.1% better than ANN.

***Keywords*: Iris, Liveliness, Segmentation, Filters, Fuzzy C-Mean, K-Mean, Features, Fusion, ANN, KNN, AHyBrK Classifier, Hybrid Classification.**

I. INTRODUCTION

With daily happening technological advancements, the use of biometric systems for security purpose is increasing day-by-day but we can't rely fully on these systems due to their vulnerability to spoof attacks. Biometrics systems are the systems that use physiological or behaviour characteristics of the individuals and perform recognition for the same. These characteristics are extracted using biometric traits like face, fingerprint, iris, hand geometry and ear. The other characteristics are behavioural like voice, gait, handwriting and signature of the person. The main aim of these systems is to provide accuracy and to reduce forgeries by detecting fake samples. Several government and private organizations use biometric systems for different purposes to avoid unwanted access. The use of these systems is immensely increased due to number of benefits over the conventional security mechanisms. However, there are few flaws too in these systems which are: (a) Privacy (e.g. face can't be private) (b) the fact of possibility of replacement of such biometric traits (which now-a-days is possible through masks or surgery) poses some external attacks. Uludag and Jain [1] proposed a biometric systems using fingerprint and add attacks on it which uses procedure named hill climbing for the synthesis of the minutia template. After analysis it is observed that fingerprint based security system can be broken. Among all the traits used in biometric systems, iris trait is considered to be more reliable and accurate in compare to others. So, special attention has been paid to iris trait for finding its vulnerabilities and to analyse its security level. These attacks may use the samples which are synthetically generated for granting access. As Galbally et al. [2] observed that iris and fingerprint based biometric systems can be smashed with some external attacks and it can be cured with liveliness detection and for this some researchers proposed liveliness detection approaches and will discuss in the next sections. Galbally et al. [3] worked for iris liveliness detection based on the quality related measures of iris. They have tested this novel anti-spoofing mechanism by using high quality samples where 1600 real and fake samples were used. This mechanism protects the system against direct attacks and also results the decision that whether the input is real or fake. The other liveliness detection mechanism for iris is presented by Jemi et al. [4] which work on the concept of liveliness where they describes that the detection of liveliness using the symptoms of liveliness is well known technique for the authenticity of any person. In their work, they have used dynamic features of the pupil instead of static properties. The change in the size of pupil describes pupil dilation and it varies from person to person and situation to situation; also amount of light present affects the pupil dynamics e.g., the diameter of adults in bright light varies from 2mm to 4mm whereas in the dark its size increases from 4mm to 8mm. They have also described the characteristics the iris images from the available databases. They have presented all the quality factors and noise factors of the samples and identified real and fake images. The other work on the detection of Iris liveliness was done by Long and Zeng [22] based on batch normalized convolutional neural network (BNCNN). They tested their approach on three different datasets namely the CASIA Iris Lamp database, the CASIA-Iris-Syn database and ND-contact database and show the effectiveness of their approach. Biometric verification systems also come under the category where the probability of spoofing increased day-by-day. To deal with the issue, different studies have been conducted and various countermeasures have been developed to diminish risks and prevent the system from these types of attacks. Liveliness detection is one of the solutions proposed to deal with the presentation attacks by differentiating real and fake traits on the basis of different properties. So, considering this concept, Ahmad and Abdulkareem

Revised Manuscript Received on December 30, 2019.
* Correspondence Author

Sunil Kumar*, Computer Science and Engineering, I.K.G. Punjab Technical University, Jalandhar, Punjab, India. Email: chawla_sunil2011@yahoo.in

Vijay Kumar Lamba, Electronics and Communication Engineering, Global College of Engineering and Technology, Ropar, Punjab, India. Email: lamba_vj@hotmail.com

SurenderJangra, Computer Science and Applications, Guru TegBahadur College, Sangrur, Punjab, India. Email: surender.jangra@gmail.com

[5] proposed a secure biometric system which considers the iris based biometric system with liveliness detection module. Here in this work, there are two sub modules of liveliness detection namely, static and dynamic. They tested this verification system using two different databases and achieved accuracy of 97% for CASIA database on dataset of 90 samples and 99% for MMU database on dataset of 180 samples.

Thavalengal et al. [6] proposed a novel method for the detection of liveliness of Iris. This system is implemented using a hybrid visible (RGB)/near infra-red (NIR) sensor on smartphones where these sensors are capable of capturing RGB and NIR images. This work is first use classification and follows it with pupil localization. For pupil localization, a fast and multi-frame mechanism is proposed which uses 1-D processing of the region of eye and analyse whether it is live or not.

Gragnaniello et al. [25] also proposed a liveliness detection methodology for Iris based on LBP descriptors. For classification, SVM classifier was utilized by them. There are number of other methods that were proposed by different researchers like, Threshold based method were proposed by Kaneamtsu et al. [26], Hierarchical Multiclass classification by Yan et al. [29], and Texture features based detection by Wei et al. [30]. The other methodologies based on features were designed to detect liveliness by Galbally et al. [24] where the authors proposed a high performance based method for fingerprint liveliness detection.

Sequeira et al. [7] also addresses the issues related to the vulnerable attacks and proposed mechanism for the same. In this work, the main focus is on feature selection mechanism so that the best subset of features helps to achieve highest classification rate. This system is tested on Biosec and Clarkson databases and three different classifiers KNN, SVM and Discriminant analysis are used in this work for liveliness detection. The results show that there is a scope of improvement so upon analysis; we found that there is a requirement of secure system which may achieve better performance in real world application. The other challenges related to biometric templates and liveliness detection were discussed by Akhtar et al. [23], Soleimani and Asem [27].

As per literature available, various authors developed different mechanisms for the detection of liveliness and secure the biometric systems from various attacks but still efficiency in the existed mechanisms are very less. So, there is a need to develop an efficient and secure biometric system which reduces the level of risks. To achieve this, in this work a novel mechanism named as ILivSpot is proposed where biometric system uses iris as trait and performs liveliness detection. In this work, for classification purpose, a new hybrid classifier is used which is a combination of ANN and KNN as explained in the next section.

II. AHYBRK CLASSIFIER

Classification is one of the important steps in the biometric systems. Classifiers are the one which help to recognize or classify the data and find out whether it belongs to the input or not. There are number of classifiers which are used for classification purpose in various fields with good performances. These days with advancing mechanism, classifiers are also fused with each other for more enhanced performance. In this work, we also use a hybrid classifiernamed as **A**HyBr**K**which is a combination of **A**NN and **K**NN.

A. Artificial Neural Network (ANN)

ANN is based on the principle of human brain where neurons and dendrites makes a connection and makes decision on the questions asked. Similarly ANN classifier decides whether the input passed to it produces output or not. This classifier is composed of number of nodes where every node is linked with each other to produce output. These links which connect the nodes are associated with weights. In this, the input data is taken by the nodes and operation is performed on it then further this output will be passed to other neurons /nodes and form some output. This classifier work in the same way that human brain works and the output generated at each node is known as its activation value. ANN follows the procedure of learning and is capable to change the behaviour of processing on the basis of its knowledge.

B. K-Nearest Neighbours (KNN)

The other best classification method is KNN which uses a supervised mechanism for classification. In this firstly, all the input cases are stored and on the basis of these inputs it checks the majority votes to find out the k neighbours and classifies the new cases. These new cases are further assigned to the class which is common among its neighbours and this can calculated by calculating the distance function. This distance function may be Hamming, Manhattan, Euclidean and Minkowski Distance. The hamming distance function is used for categorical variables where as others are used for continuous functions. KNN need pre-processing and is computationally expensive but its results are good in most cases.

C. Hybrid Classifier

Here, we have used a hybrid classifier which is a combination of Artificial Neural Network and K-Nearest Neighbour and named it as AHyBrK Classifier. For this work, firstly; inputs will be passed to the ANN and after processing, the output of ANN is further passed to KNN and after this, generated output is a final result. The pseudo code given below describes the process of AHyBrK Classifier.

```
Algorithm 1: Hybrid Classifier (AHyBrK)
Input:Extracted Features of the Modalities ($\mathcal{F}$)
Output:Error Rate (ER), Accuracy (A)
Start
For each set of Features
Start ANN
    Distinguish Training and Test Dataset
        Set Input, Output and Hidden Layers
        Initialize Weight Feature ($W_i$)
        For each layer in Output Layer Calculate Output
            Update Parameters
            IF matched with the Criterion required
            Then Start KNN
            End of IF
        End of For
```

```
Start KNN
    Set Values of 'K' Parameters
    For each Input and Test Data Set
        Calculate Distance (D)between all the Points
        Sort distance in Ascending Order
        For all K-Neighbours
            Select best K-Neighbour
            Final Matched
        End of For
    End of For
End of For
Calculate ER and A on the basis of percentage of matched samples

Stop
```

III. ILIVSPOT: SECURE BIOMETRIC SYSTEM

In this work, a new enhanced biometric system is proposed which recognize the liveliness of the iris samples and find the correctness of the recognition system. The step-by-step details of this proposed system are as follows:

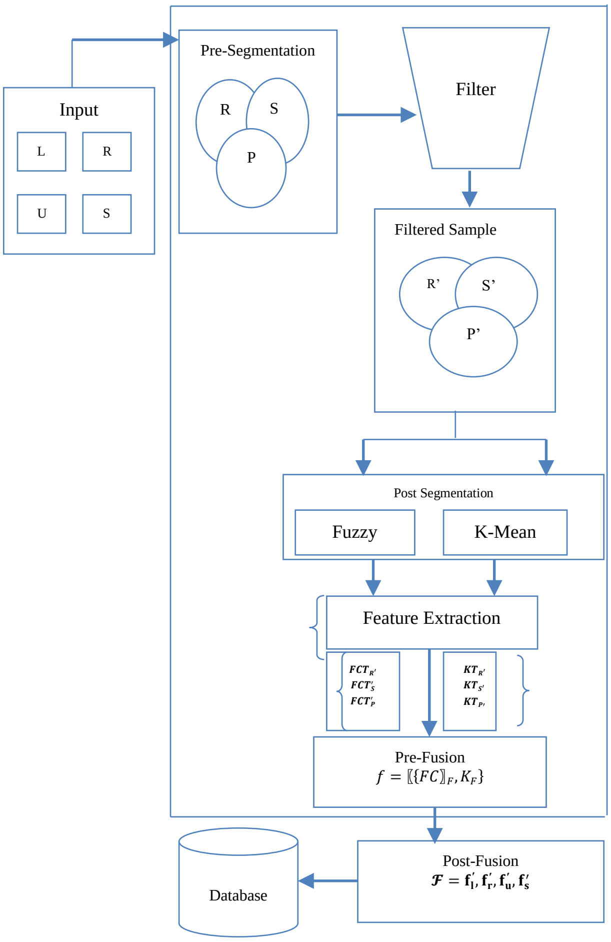

Figure 1: Training Phase

Step 1: Data Acquisition

The first main step of this recognition system is to collect the samples. For this work, the dataset of UBIRIS.v2 is used [20] which is a collection of iris images captured in non-constrained conditions i.e. at-a-distance, on-the-move, in the visible wavelength andhaving more realistic noise factors. This dataset was generated using Canon EOS 5D Camera with shutter speed of 1/197seconds, focal length of 400mm, exposure time 1/200seconds and in Pattern Metering Mode. These images were then cropped with the width of 400 pixels and 300 pixels height with 72 dpi resolutions, and saved in .tiff format. The dataset was collected from total 261 subjects. Total 11102 images were acquired by them where 54.4% images are of male gender and 45.6% are of female gender. For the purpose of testing the performance of this proposed classifier, we have used those images in which eyeball is moved, where samples of 100 subjectsare collected and each sample contains four images of moved eyeball in Left (l), Right (r), Up (u), and Straight (s) direction. This dataset is used for training purpose. Testing in this work is done with 100 images which contains 30% of forged samples.In this wok, four samples are collected from each person so total 400 samples were used and these samples were treated as input for the system while we trained the data. The details of this proposed work before classification are shown in figure 1.

Step 2: Pre-Segmentation

To enhance the image quality of the input sample, unlike general practice, we have segmented the iris (ROI), sclera and pupil from the input image before actually applying any filters.

$$Iris_i = R_i \cup S_i \cup P_i \qquad \text{(i)}$$

Where R_i is ROI, $S_i$is Sclera and P_i is Pupil region for an iris.

This will indirectly increase the quality of image taken for the recognition purpose. In this work, firstly we have used circle drawing algorithm which scans the whole Iris image and find the center point of it. Then as according to radius the region of the circular pixels are selected and lines are drawn on the same region and find the outer circle region and inner circle region. From the center, this algorithm starts detecting circular pixels and inner circle is drawn where the intensity of the pixels are changed from the centre and same in case of outer circle. Because the outer region of the pupil having different intensity pixels and similarly iris and sclera has different intensity pixel, this will help to detect outer and inner circle in this algorithm. ROI is specifically that area where user's interest is more. Iris is the annular part between pupil boundary and iris boundary i.e. inner and outer circles respectively. In this work, these pixel values are detected and stored in an array. For this, we have used filling algorithm in which inner circle boundary pixels are selected first and then filling algorithm select the pixels by using eight connected regions up to outer circle boundaries and form an array of pixels. The pupil is a gap situated in the focal point of the iris of the eye that enables light to strike the retina. It seems dark since light entering the pupil is either consumed by the tissues inside the eye specifically, or assimilated after diffuse reflections inside the eye that mostly miss exiting the narrow pupil. In this work, to extract pupil from the full eye image, we subtracted the extracted ROI region from the original image and these pixels are further stored in the array.

Step 3: Quality Enhancement

Quality Enhancement plays a major role to improve the effectiveness of any system therefore; this step is the key ingredient of a biometric system. A number of filters are there which can be used to enhance the quality of an image. In this work, Gaussian filter is used for the purpose of filtering the noise and result in image enhancement. This filter is selected because quality of the segmented iris is better using this as analysed in [21]. Filter is applied on the ROI, Pupil and Scleraindividually and this will improve the quality of the sample with higher rate as compare to the other mechanism where filter is directly applied on the whole image. The resultant factor is represented as:

$$R' = Gauss(R) \qquad \text{(ii)}$$

$$S' = Gauss(S) \qquad \text{(iii)}$$

$$P' = Gauss(P) \qquad \text{(iv)}$$

Step 4: Post-Segmentation

Segmentation is an important step for recognition purpose and here after filtration of the ROI, Pupil and Sclera, each part is segmented using two different mechanisms- Fuzzy C-Mean Clustering and K-mean Clustering. The output of both mechanisms is further used in feature extraction. K-Mean and Fuzzy C-Mean, both the methods are very popular and used for segmentation purposes.

Fuzzy C-Mean

In this mechanism, firstly distance between the clusters are calculated and on their basis membership function is assigned to each data members of the cluster. If the quantity of the data is more, then it is near to the center of the cluster and its membership is also toward the center of the cluster. It means that the sum of all the membership of the data points is equal to one. In this, the cluster centers and membership are updated at the end ofeach iterationby using following equations:

$$P_{ij} = {}^{1}\Big/_{\sum_{k=1}^{n}\left(d_{ij}/d_{ik}\right)^{(2/r-1)}} \qquad \text{(v)}$$

$$K_j = \left[\sum_{i=1}^{m}\left(P_{ij}\right)^{r} x_i\right] / \left[\sum_{i=1}^{m}\left(P_{ij}\right)^{r}\right], \forall\, j = 1, 2, \ldots \ldots n \text{(vi)}$$

Where*m* is the number of data points, K_j represents the j^{th}cluster centre,*r* is the fuzziness index $r \epsilon [1, \infty]$, *n* represents the number of cluster centre, P_{ij} represents the membership of i^{th} data to j^{th} cluster centre and d_{ij} represents the Euclidean distance between i^{th} data and j^{th} cluster centre.

K-Mean Clustering

This type of clustering method is used when data is unlabelled because this mechanism is based on unsupervised learning. The aim of K-mean clustering is to discover K-groups of data based on some features. This algorithm assign data point to the clusters based on the similarity in their features. The output of this method is:

- Centroids: which are used to label data
- Labels for the training data (different segmented parts)

Step 5: Feature Extraction

Features are very important constituent in image processing systemswhich contain detailed and relevant information of the input data and this information affects the performance of the recognition systems. A number of techniques were used for the extraction of features from image samples. Some of these are: Color Features, Spatial Features, Edge and Boundary Features, Shape Features, Transform Features and Texture Features. In this work, texture features are extracted after segmentation.

The surface characteristics of an object and its appearance are referred to as texture which depends on the shape, size, arrangement, density and proportion of the elementary parts of the object. Texture features can be calculated by using GLCM points which is Gray Level Co-occurrence matrix. These features are comes under the category of 2nd order statistic features means information in this is based on the pixel values. Some of the texture features are entropy, energy, contrast, correlation etc. which are calculated at the different angles.The set of texture features which are extracted are represented as:

$$T = \{Con, Corr, E, H\} \qquad \text{(vii)}$$

Where *T* is set of texture features, *Con* is Contrast, *Corr* is correlation, *E* is Energy and *H* is Homogeneity.

(a) ***Contrast:***Contrast refers to the 'Sum of Square Variance' and is defined as the calculation of the intensity contrast linking pixel and its neighbour over the whole image. At constant image, contrast value is 0 i.e. (i-j) =0. Contrast increases with the increase in (i-j).

$$Con = \sum_{i,j=0}^{N-1} P_{i,j}(i-j)^2 \qquad \text{(viii)}$$

(b) ***Correlation***:Correlation finds the linear dependency of the gray levels on a pixel and its neighbour pixels. Correlation value of an image lies between [-1, 1]. If value of correlation is NaN that means image is constant.

$$Corr = \sum_{i,j=0}^{N-1} P_{i,j}\left[\frac{(i-\mu i)(j-\mu j)}{\sqrt{(\sigma i^2)(\sigma j^2)}}\right] \qquad \text{(ix)}$$

(c) ***Energy***:Energy is also one of the parameters for texture features and it defines the orderliness of an image. It can be calculated by the sum of the square of the elements in the GLCM. The energy value of an image is high when window is proficient orderly. The range of this parameter is [0, 1]. Its value is 1 when image is constant.

$$E = \sum_{i,j=0} P(i,j)^2 \qquad \text{(x)}$$

(d) ***Homogeneity***:Homogeneity is defined as the factor of tightness and it is calculated by calculating the tightness of the distribution in GLCM to its diagonal. The range of homogeneity is [0, 1] and is 1 for diagonal GLCM.

$$H = \sum_{i,j=0}^{N-1} P(i,j)/R \qquad \text{(xi)}$$

In this work, two sets of texture features are extracted where one set is after Fuzzy C-mean Clustering and other is after K-Mean clustering, and these features are represented by:

$$FC_F = \{FCT_{R'}\} \cup \{FCT_{S'}\} \cup \{FCT_{P'}\} \qquad \text{(xii)}$$

Step 6: Pre-Fusion

Fusion is basically the combination of two or more things. Here in this step fusion of the features extracted from ROI, Sclera and Pupil of a sample is fused together and treated as single entity. This step is known as pre-fusion because here we combine the features of an individual Iris sample. This can be written as following equation:

$$f = \{FC_F\} \cup \{K_F\} \qquad \text{(xiii)}$$

Where f is fused feature vector; FC_F is the set of texture features extracted after fuzzy C-mean clustering; K_F is the set of texture features extracted after K-mean clustering.

Step 7: Post-Fusion

Here, two-step Fusion is done named as pre-fusion and post-fusion. As discussed earlier, pre-fusion is a fusion where we fuse a set of feature for one iris sample but here in post-fusion, fusion of the set of feature vector which is generates in the last step is done for the iris samples provided by each person means with the four image samples provided by one person which contains L, R, U and S movement of the eyeball. This post fusion is basically characterize the concept of liveliness because live eyeball contains movement of eyeball is any angle or direction and this fused factor provide optimal solution for the detection of the same.This fused vector is represented in the following form and then it will be stored in the database and use for training purpose.

$$\mathcal{F} = \{f_l, f_r, f_u, f_s\} \qquad \text{(xiv)}$$

Where $\mathcal{F}$ is the fused feature vector which contains set of fused texture features for *left (f_l)*, *right (f_r)*, *up (f_u)* and *straight (f_s)* iris samples provided by one person.

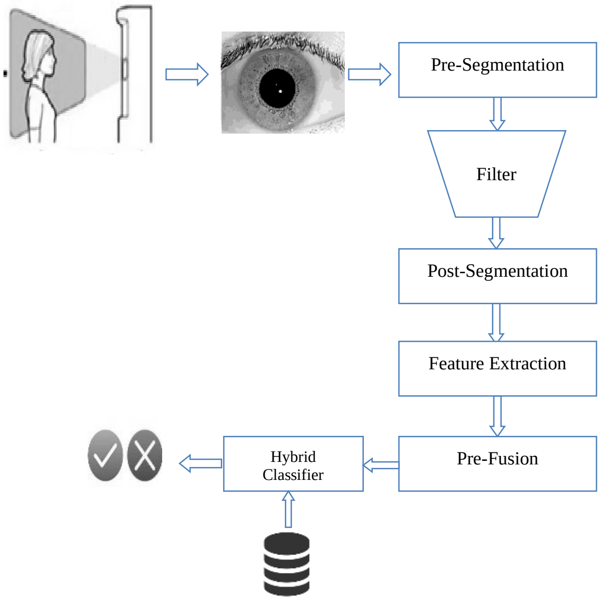

Figure 2: Testing Phase

Step 8: Classification

This step is an important step of the biometric system. This step performs classification which helps to recognize or classify the data as shown in Figure 2 and find out whether it belongs to the input or not. In this secured biometric system, a new hybrid classifier '**A**Hy**B**r**K**' is used. This is the final step of the biometric recognition system which identifies the samples if they are matched with the database or not. As a result of which, we can find out the fake samples or forgeries.

IV. EXPERIMENT & RESULT ANALYSIS

For experimentation of this proposed work, simulation is done using MATLAB and dataset of UBIRIS is used. This dataset contains several images and this system is trained using 400 samples and for testing purpose 100 samples are used where 30% samples are forged samples.The measurement of the effectiveness of biometric system cannot be achieved with single value, but some parameters are there which defines the accuracy under the same data with same set of rules. Some of these parameters are False Acceptance Rate (FAR), False Rejection Rate (FRR), Error rate, Accuracy etc.

FAR:It is probability of the fake users that are accepted accidently and this can be calculated as the ratio of number of imposters who were able to enter in the system to the total no. of imposters.

FRR: It is the probability of the valid users that are denied accidently and this can be calculated as the ratio of the falsely rejected and the truly accepted(TA) samples.

The performance of the classification system determines the liveliness of the system and it can be measured in terms of Error Rate and Accuracy. The ratio of number of misclassified samples and the total no. of images in the test set is defined as Error Rate whereas accuracy is the percentage of the correctly classified samples and is opposite to error rate.

Table 1summarizes the results achieved by the simulation of ILivSpot.

Table 1: Experimentation Results (ILivSpot)

Parameter	Formula	Results
FAR	$\frac{FA}{FA+TR} = \frac{2}{2+28} = \frac{2}{30}$	0.06
FRR	$\frac{FR}{FR+TA} = \frac{1}{1+59} = \frac{1}{60}$	0.01
Error Rate	$\frac{misclassifiedsamples}{TotalSamples} * 100 = \frac{3}{100} * 100$	3%
Accuracy	$100 - ErrorRate = 100 - 3$	97%

In this work, a hybrid classifier (AHyBrK) which is a combination of ANN and KNN is used. Results shows that the performance of AhyBrK is better while used in ILivSpot as compare to ANN and KNN. The comparative results for all three classifier in the novel framework in terms of FAR and FRR are as shown in figure 4 and in terms of Error Rate and Accuracy is shown in figure 5.

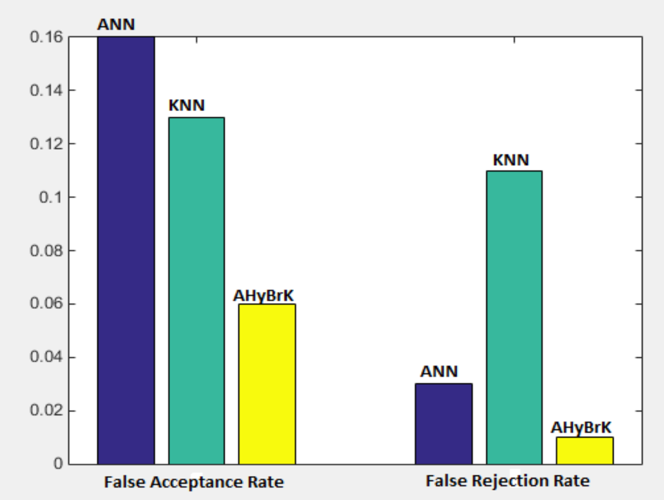

Figure 4: FAR and FRR of Different Classifiers

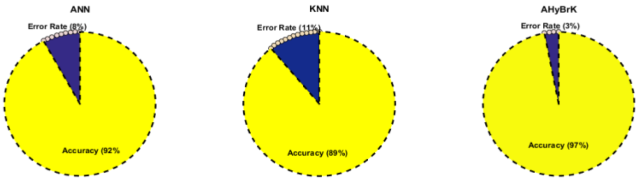

Figure 5: Accuracy and Error Rate of Different Classifiers

V. CONCLUSION

In this era of technology, digitalization becomes very common part of the day-to-day life and has both positive and negative outcomes. So, for the protection of any activity different mechanisms are used. Biometrics is also one of the systems which are used for security purpose now-a-days. This advancement also affects the biometric systems in the form of spoofing. Various Biometric Recognition systems are infected because of spoofing and its performance decreases. To prevent biometric systems, liveliness detection mechanism is introduces. In this work, a novel biometric system is proposed and named as ‘ILivSpot: Secure Biometric System based on Iris Liveliness Detection’ where liveliness detection mechanism is used to prevent systems from unauthorized access. This mechanism tested on three different classifiers ANN,KNN and **AHyBrK** (Hybrid ANN-KNN) and results shows that the performance of hybrid classifier is better than other classifier in terms of different accuracy measurements. The accuracy percentage of ILivSpot with ANN, KNN and **AHyBrK** is 92%, 89% and 97% respectively.

ACKNOWLEDGMENT

Authors are thankful to IKG Punjab Technical University for providing platform for experimenting for this work. Also, sincere thanks are due to anonymous reviewers of the manuscript.

Conflict of Interest

The authors declare no conflict of interest.

REFERENCES

1. U. Uludag and A. K. Jain, “Attacks on biometric systems: a case study in fingerprints,” Security, Steganography, and Watermarking of Multimedia Contents VI, vol. 2, no. 2, pp. 1–12, 2004.
2. J. Galbally, J. Fierrez, and J. O. Garcia, “Vulnerabilities in Biometric Systems: Attacks and Recent Advances in Liveness Detection,” Spanish Workshop on Biometrics SWB, pp. 1–8, Jun. 2007.
3. J. Galbally, J. Ortiz-Lopez, J. Fierrez, and J. Ortega-Garcia, “Iris liveness detection based on quality related features,” 2012 5th IAPR International Conference on Biometrics (ICB), pp. 1–7, 2012.
4. J. Jemi P, R. K, and D. C. J. Winnie Wise, “Fake Iris Liveness Detection Using Pupil Dynamics,” ITSI Transactions on Electrical and Electronics Engineering (ITSI-TEEE), vol. 3, no. 5, pp. 6–9, 2015.
5. H. M. Ahmad and B. J. Abdulkareem, “Integrate Liveness Detection with Iris Verification to Construct Support Biometric System,” Journal of Computer and Communications, vol. 04, no. 01, pp. 23–32, 2016.
6. S. Thavalengal, T. Nedelcu, P. Bigioi, and P. Corcoran, “Iris liveness detection for next generation smartphones,” IEEE Transactions on Consumer Electronics, vol. 62, no. 2, pp. 95–102, 2016.
7. A. F. Sequeira, J. Murari, and J. S. Cardoso, “Iris Liveness Detection Methods in Mobile Applications,” Proceedings of the 9th International Conference on Computer Vision Theory and Applications, pp. 22–33, 2014.
8. R. Jain and C. Kant, “Attacks on Biometric Systems: An Overview,” International Journal of Advances in Scientific Research, vol. 1, no. 7, pp. 283–288, 2015.
9. S. Kaur and A. Ada, “A New Hybrid Technique for Iris Recognition,” International Journal of Computer Applications, vol. 122, no. 13, pp. 11–18, 2015.
10. A. G. Gale and S. S. Salankar, “Evolution of performance analysis of Iris recognition system by using hybrid methods of feature extraction and matching by hybrid classifier for iris recognition system,” 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), pp. 3259–3263, 2016.
11. J. Malik, S. Belongie, J. Shi, and T. Leung, “Textons, contours and regions: cue integration in image segmentation,” Proceedings of the Seventh IEEE International Conference on Computer Vision, pp. 1–8, 1999.
12. A. Das, U. Pal, M. A. F. Ballester, and M. Blumenstein, “Multi-angle based lively sclera biometrics at a distance,” 2014 IEEE Symposium on Computational Intelligence in Biometrics and Identity Management (CIBIM), pp. 200–208, 2014.
13. M. Kumar and N. B. Puhan, “Iris liveness detection using texture segmentation,” 2015 Fifth National Conference on Computer Vision, Pattern Recognition, Image Processing and Graphics (NCVPRIPG), pp. 5–8, 2015.
14. H. Kabir, T. Jabid, and O. Chae, “Local Directional Pattern Variance (LDPv): A Robust Feature Descriptor for Facial Expression Recognition,” The International Arab Journal of Information Technology, vol. 9, no. 4, pp. 382–391, 2012.
15. S. Thavalengal, T. Nedelcu, P. Bigioi, and P. Corcoran, “Iris liveness detection for next generation smartphones,” IEEE Transactions on Consumer Electronics, vol. 62, no. 2, pp. 95–102, 2016.
16. A. F. Sequeira, J. Murari, and J. S. Cardoso, “Iris liveness detection methods in the mobile biometrics scenario,” 2014 International Joint Conference on Neural Networks (IJCNN), pp. 3002–3008, 2014.
17. R. Chen, X. Lin, and T. Ding, “Liveness detection for iris recognition using multispectral images,” Pattern Recognition Letters, vol. 33, no. 12, pp. 1513–1519, 2012.
18. A. Czajka, “Pupil Dynamics for Iris Liveness Detection,” IEEE Transactions on Information Forensics and Security, vol. 10, no. 4, pp. 726–735, 2015.
19. J. Galbally, J. Ortiz-Lopez, J. Fierrez, and J. Ortega-Garcia, “Iris liveness detection based on quality related features,” 2012 5th IAPR International Conference on Biometrics (ICB), pp. 271–276, 2012.
20. H. Proença, S. Filipe, R. Santos, J. Oliveira, and L. A. Alexandre, “The UBIRIS.v2: A Database of Visible Wavelength Iris Images Captured On-The-Move and At-A-Distance,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 32, no. 8, pp. 970–977, 2005.
21. S. Kumar, V.K. Lamba, S. Jangra, “Image quality analysis of segmented iris using filters”, Int. Journal of Recent Technology Engineering, vol. 7, no. 5, pp. 279-296, 2019.
22. M. Long and Y. Zeng, “Detecting Iris Liveness with Batch Normalized Convolutional Neural Network,” Computers, Materials & Continua, vol. 58, no. 2, pp. 493–504, 2019.

23. Z. Akhtar, C. Micheloni, and G. L. Foresti, “Biometric Liveness Detection: Challenges and Research Opportunities,” IEEE Security & Privacy, vol. 13, no. 5, pp. 63–72, 2015.
24. J. Galbally, F. Alonso-Fernandez, J. Fierrez, and J. Ortega-Garcia, “A high performance fingerprint liveness detection method based on quality related features,” Future Generation Computer Systems, vol. 28, no. 1, pp. 311–321, 2012.
25. D. Gragnaniello, C. Sansone, and L. Verdoliva, “Iris liveness detection for mobile devices based on local descriptors,” Pattern Recognition Letters, vol. 57, pp. 81–87, 2015.
26. M. Kanematsu, H. Takano, and K. Nakamura, “Highly reliable liveness detection method for iris recognition,” SICE Annual Conference 2007, 2007.
27. S. A. Soleimani and M. M. Asem, “Iris Live Detection Assessment; A Structural Survey,” 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), pp. 974–980, 2019.
28. K. A. Nixon, V. Aimale, and R. K. Rowe, “Spoof Detection Schemes,” Handbook of Biometrics, pp. 403–423, 2007.
29. Z. Yan, L. He, M. Zhang, Z. Sun, and T. Tan, “Hierarchical Multi-class Iris Classification for Liveness Detection,” 2018 International Conference on Biometrics (ICB), pp. 47–53, 2018.
30. Z. Wei, X. Qiu, Z. Sun, and T. Tan, “Counterfeit iris detection based on texture analysis,” 2008 19th International Conference on Pattern Recognition, pp. 47–50, 2008.

AUTHORS PROFILE

Sunil Kumar is pursuing Ph.D. in Computer Engineering from IKG Punjab Technical University, Jalandhar. His research interests lie in Digital Image Processing, Biometrics, Image Segmentation, Machine Learning, and Computer Vision. He has over 10 publications in different International Journals and Conferences.

Dr. Vijay Kumar Lambahas done his Ph.D. from Guru Nanak Dev University, Amritsar in 2009. His research interests lie in VLSI design, Nano Technology, and Digital Image Processing.He has more than 100 publications in various National and International journals of repute out of which 15+ are in SCI journals. He has been involved in many funded projects from several government agencies of repute. He is having more than 18 years of experience.

Dr. SurenderJangrahas completed his Ph.D. inComputer Science andApplication fromKurukshetraUniversity, Kurukshetra in 2011. His research interests lies in Fault Tolerance in Mobile Distributed Systems, Adhoc Networks, Data Mining, Cloud Computing, Biometrics, System Security and Cryptography. He has over 50 publications in different International Journals and Conferences of repute