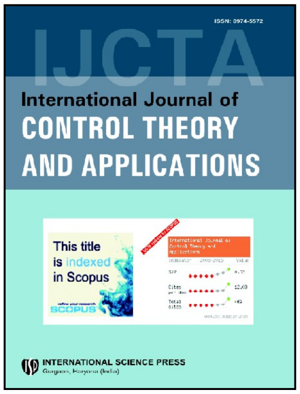


International Journal of Control Theory and Applications

ISSN : 0974-5572

© International Science Press

Volume 10 • Number 29 • 2017

Efficient Support Vector Machine with Radial Basis Function for Biometric Authentication System

K. Juliana (Gnana Selvi)[1*] and M. Hemalatha[2]

[1]Head, Dept of ICT, Rathinam College of Arts and Science, Coimbatore-21.*
[2]Head, Department of Software Systems, Karpagam University, E-mail:
[1]Corresponding author E-mail:sunil.juliana@gmail.com*
[2]E-mail:hema.bioinf@gmail.com

Abstract: Improvement in communication technology and computer applications in our day-to-day life highlights the strong requisite for user-friendly schemes to secure our assets and guard our confidentiality without losing our distinctiveness. Usually, use a password to access a computer, Personal Identification Number (PIN) to access ATM, cryptographic methods to access and outlook files and dozen others to admittance the internet and so on. These conventional approaches of identification can be effortlessly guessed, perceived or forgotten. Henceforth the alternative selection a like biometric-based recognition for consistent and robust human identification has specified more significance in the varied assortment of commercial sectors. In prevailing scheme, face recognition is made through hybrid swarm intelligence method which uses both PSO and ABC. Hybrid ABC optimization procedure was cast-off to train a weighting mask for supplementary the face recognition procedure. In this scheme training process can be completed offline, since of this it accomplishes less computation time. Nevertheless it does not fashioned satisfactory recognition precision. So as to progress the recognition precision the anticipated scheme familiarized a Radial Basis Function-Support Vector Machine (RBF-SVM) grounded biometric authentication system. In this anticipated scheme preprocessing is achieved by means of median filter. Then the skin areas are noticed from pre processed images. And face detection is achieved by means of boosted classifiers with Haar-like features. The similar boosted classifiers are also used for eye detection. In this eye detection the left eye and right eye features haul out. To trace multi faces in the outcome. To guarantee the high security eye pupil is noticed by means of circle Hough transforms. The extracted features are specified to RBF-SVM. It categorizes the input images as matched or non matched. The investigational outcomes display that the anticipated scheme attains improved recital associated with prevailing scheme in terms of exactness, precision and recall.

Keywords: Human identification, boosted classifiers, RBF, SVM and authentication.

I. INTRODUCTION

In the current era of e-commerce more and more services are being obtainable over the electronic devices and internet. These comprise banking, credit card facility, e-shopping, etc. To guarantee appropriate use of these facilities only by the authorized or genuine users and evade any misuse by the unauthorized or imposter users, certain person authentication system is entrenched into these services. Precise automatic personal identification is becoming more and more significant to the process of our progressively electronically interconnected data society [1]. Presently, person authentication is done typically by means of one or more of the subsequent means: text passwords, personal identification numbers, barcodes and identity cards. Person authentication comprises verification of a person's identity grounded on his/her physiological or behavioral features. The worth of these systems is that they do not change their value with respect to time and also unpretentious by the situation in which they are used. The chief demerit of them is that they can be effortlessly misused or forgotten. Also, with time more and more facilities are being obtainable over the electronic devices and internet.

To overwhelm the above stated difficulties Biometric-based authentication scheme has been familiarized. Biometric-based methods have arisen as the most promising choice for distinguishing individuals in recent years since, as a substitute of authenticating people grounded on passwords, PINs, smart cards, plastic cards, tokens, keys and so forth. Passwords and PINs are durable to remember and can be stolen or guessed; cards, tokens, keys and the like can be inappropriate, forgotten, purloined or duplicated; magnetic cards can become tainted and unreadable. Though, an individual's biological traits cannot be inappropriate, elapsed, stolen or forged.

So as to progress the security in ATM machines idea of fingerprint and Iris identification is familiarized [2]. The designed scheme associations a sum of authentication mechanisms (id card, RFID, passwords, fingerprint and iris recognition) composed with a series of authentication phases for ATM access. While this scheme seems to have the high level of security, the 5 levels of authentication for the user can be burdensome. For attain continuous user authentication soft biometric traits (e.g., color of user's clothing and facial skin)is cast-off. The intended structure automatically registers (enrolls) soft biometric traits each time the user logs in and fuses soft biometric matching with the conventional authentication systems, specifically password and face biometric. It has high acceptance to the user's posture in front of the computer system.

Similar to Sim and Zhang [6, 7], Azzini and Marrara [8, 9] also projected a continuous authentication method by means of face and fingerprint biometrics. Their system patterned the uniqueness of the user only on the basis of face recognition. If the authentication certainty of face recognition falls underneath a threshold, then a novel fingerprint acquisition is essential. Again, the authentication certainty in this method must go down quickly with time in order to guarantee the security, irrespective of whether the user is in front of the console or not. Kang and Ju [10] anticipated a continuous authentication method by means of face and behavioral biometrics. They cast-offf ace trajectory and its pose as behavioral features. Since behavioral biometrics was cast-off only for supporting face authentication, the authentication certainty must go down quickly over time in the nonexistence of face biometric information.

2. LITERATURE REVIEW

Christopher Garcia *et al.* (1999) anticipated a human face detection system for color images. The skin regions are attained by color clustering and filtering using the YCbCr and HSI skin color subspaces on the original image. Potential face regions are then attained by amalgamation alike skin color regions in the color quantized image. Constraints associated to shape and size of face is functional, and face intensity texture is examined by execution wavelet packet decomposition on every candidate face area in order to notice human faces. A set of modest statistical deviations form the feature vectors. The Bhattacharya distance is cast-off to categorize the extracted feature vectors into face or non face areas [8]. Alajel *et al.* (2011) anticipated a face detection procedure by means of skin color modeling and the improved Hausdorff distance. The probability of a pixel as being a skin color is resolute grounded on the mean and the 35 covariance matrix of learned skin colors. A predetermined threshold is cast-off to added resolve skin color pixels. A series of morphological operations is achieved to eliminate the noise and distinct potential face candidates. Lastly, a template-based object classifier is cast-off to categorize the skin color candidates as a face or a non-face by means of the modified Hausdorff distance [9] .

Altinok and Turk [10] anticipated continuous authentication methods by means of face, voice, and fingerprint. They demanded that a continuous biometric authentication scheme should be capable to offer eloquent estimate of authentication conviction at any specified time, even in the absence of any biometric information. They obtainable a novel temporal integration method that fulfilled this requirement. Every match score is demonstrated as a Gaussian random variable and, as predictable, the authentication uncertainty upsurges over time. Amazingly, even in the nonexistence of any biometric information, Altinok and Turk were able to offer an estimation of the authentication certainty. Nevertheless, in such a situation, the authentication certainty must go down quickly with time in order to sustain the system security, irrespective of whether the user is in front of the console or not. This indicates to a reduction in the scheme usability.

Xiao *et al.* [11] grants a prototype scheme that uses facial recognition technology to observe the authenticated user. The objective is to guarantee that the user who is spending the computer is the similar person that logged onto the system. A neural network-based algorithm is executed to carry out face detection, and an eigen face technique is engaged to achieve facial recognition. A graphical user interface (GUI) has been established which allows the recital of face detection and facial recognition to be observed at run time. It achieves near-real-time face detection and facial recognition after user logon. The system will log the user off the computer when the user's face vanishes after a preset and adaptable time interval, or when the detected face is diverse than that of the user who initially logged on.

Liu and Chen [12] applied adaptive Hidden Markov Models (HMM) for pose-varying video-based face recognition. All face images were abridged to low-dimensional feature vectors by means of PCA. In the training procedure, an HMM was produced to learn both the statistics of the video sequences and the temporal dynamics of every subject. Throughout the recognition stage, the temporal features of the investigation face sequence were examined over time by the HMM consistent to every subject. The possibility scores delivered by the HMMs were associated. Grounded on maximum possibility scores, the uniqueness of a face in the video sequence was renowned. A sum of studies on continuous user authentication has been familiarized. These system characteristically use one or more primary (hard) biometric traits (e.g., fingerprint or face). Sim et al. [13] and Kwang et al. [14] apprehended the user's face and fingerprint with a camera and a mouse with anintegral fingerprint sensor, correspondingly. Although they exhibited promising authentication outcomes, their scheme agonized from low obtain ability of the biometric traits.

Janakiramanet., alp resented a continuous face verification system to progress desktop security. Continually confirms the occurrence of a logged-in user at a computer console. It upholds a sliding window of about ten seconds of confirmation data points and uses them as contribution to a Bayesian structure to calculate a probability that the logged-in user is tranquil extant at the console. If the probability drops below a threshold, the scheme can delay or freeze operating system practices fitting to the logged-in user. These aids avert misuse of computer possessions when an unauthorized user cruelly takes the place of an authorized user.

The rest of the paper is prearranged as trails: a short-term assessment of some of the literature works in biometric grounded authentication is obtainable in Section 2. The anticipated methodology for face recognition grounded biometric authentication **is**comprehensive in Section 3. The experimental outcomes and recital analysis discussion is provided in Section 4. Lastly, the conclusions are summed up in Section 5.

3. PROPOSED METHODOLOGY

The anticipated system presented an initiative passive continuous authentication (CA) system grounded on both hard and soft biometrics is offered. Human facial features are cast-off as hard biometric data for the authentication procedure, and the skin color of a user is engaged as the soft biometric information. At first hard biometrics grounded scheme is achieved. Then soft biometric authentication unswervingly when there is nonhuman face detected in the input frame; else, the perceived faces will be directed to the eye detection segment. Henceforth, the entire system is grounded on software. In this design, the system comprises the subsequent components: Preprocessing, the skin color detection module, the face detection module, the eye detection module, rotation and normalization module, eye pupil detection and the face recognition module. Flow diagram of anticipated scheme is revealed in fig. 1.

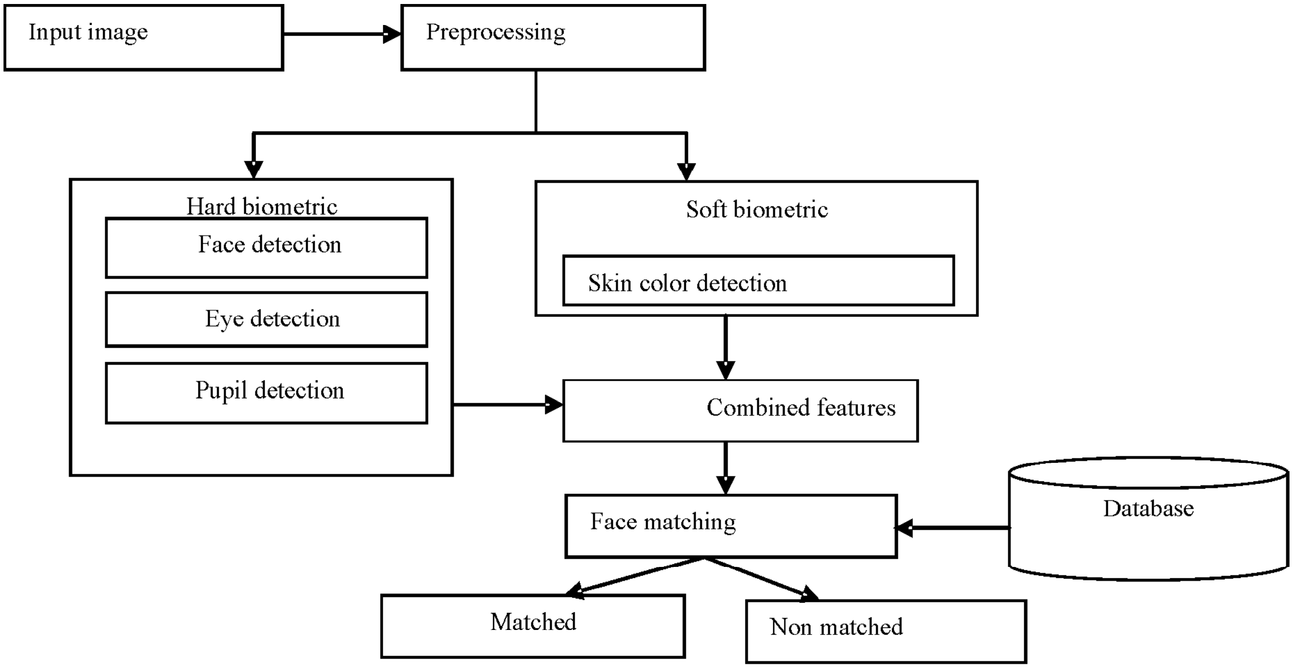


Figure 1: Flow diagram of proposed system

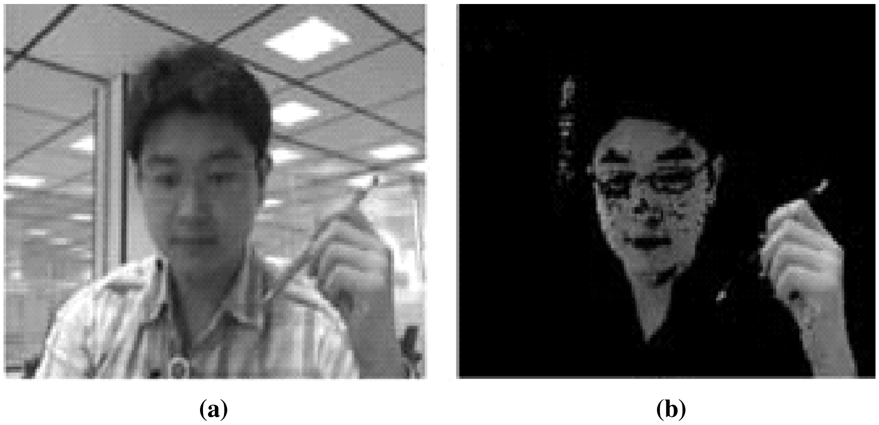
(A) Preprocessing

The noise in the input image is preprocessed by means of Adaptive Median Filter. It achieves spatial processing to regulate which pixels in an image have been pretentious by impulse noise. The Adaptive Median Filter classifies pixels as noise by associating every pixel in the image to its adjacent neighbor pixels. The size of the neighborhood is adjustable, as well as the threshold for the assessment. A pixel that is diverse from a majority of its neighbors, as well as being not structurally associated with those pixels to which it is comparable, is considered as impulse noise. These noise pixels are then substituted by the median pixel value of the pixels in the neighborhood.

(B) Skin Color Detection

After the preprocessing the skin colour is noticed. Henceforth, color model transmute is desirable since numerous lighting circumstances have a higher outcome on the pixel value in the RGB color model than the others. Color model transformation from the RGB model to YC_bC_r or HSV has been deliberate to trace the likely skin areas. The scheme operates RGB to color model transformation to filter out the non skin area ssince it is tranquil to implement and has been established that the YC_bC_r color model offers decentattention of diverse ethnicities. By proper assortment of the thresholds, the potential skin pixels are removed. In the experimentation, the thresholds for the skin color recognition are set by

$$\begin{matrix} Y \\ C_b \\ C_r \end{matrix} \in \begin{bmatrix} 65, & 253 \\ 105, & 125 \\ 138, & 168 \end{bmatrix}. \tag{1}$$



(a) **(b)**

Figure 2: Instance of skin color extraction outcome (a) Original frame (b) Extracted skin color pixels

The RGB to color transformation is specified by

$$\begin{bmatrix} Y \\ C_b \\ C_r \end{bmatrix} = \frac{1}{256}\begin{bmatrix} 77 & 150 & 29 \\ -44 & -87 & 131 \\ 131 & -110 & -21 \end{bmatrix}\begin{bmatrix} R \\ G \\ B \end{bmatrix} + \begin{bmatrix} 2 \\ 128 \\ 128 \end{bmatrix} \tag{2}$$

Where *R*, *G*, *B*, *Y*, *Cb*, and *Cr* signify the color channels from the unique image and the transformed image, correspondingly. An instance of skin color extraction is specified in Fig. 2.

(C) Face Detection

The face detection algorithm constructed in the Open CV library is constructed grounded on a cascade of boosted classifiers, which effort with Haar-like features. It was initially projected by Viola *et al.* in 2001. The input frame is transformed into gray-scale for face detection. Since the face detection is grounded on the boosted classifiers with Haar-like features, occasionally a shape similar to a human face wills also be noticed even if that shape is not tranquil of human skin color pixels. Consequently, the data attained from the skin color detection component is exploited to support in examination whether the noticed face region is a potential human face by the standard registered in

$$f_i \in \begin{cases} \textit{face region} & \textit{if } \Sigma_{j \in skin} x_j / \Sigma x_j \geq 0.5 \\ \textit{nonface region,} & \textit{otherwise} \end{cases} \tag{3}$$

where f_i signifies the potential face region situated by the classifier and x_j specifies the pixels in the Cr channel consistent to the similar location of f_i. Please note that *xj* has been transformed into a binary image by means of "1" to designate a human skin pixel and "0" to present a non-skin pixel. If the result of the face detection segment does not trace any possible face region from the input, the subsequentelement will be substituted to the soft biometric corresponding; else, the potential face regions will be directed to the eye detection segment. The result of the face detection module is exposed in Fig. 3.

(D) Eye Detection Module

The eye detection segment is also constructed by the similar boosted classifiers, excluding that the Haar-like features are substituted by the left eye and right eye features, correspondingly. It is likely to trace multi faces in

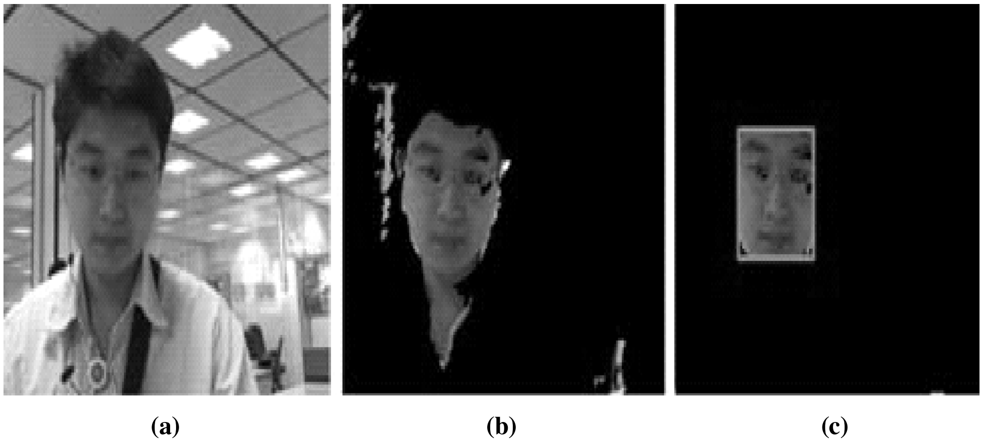


Figure 3: Example of face detection result (a) Frame captured by the webcam (b) Detected skin color region (c) Detected face region

the outcome, and henceforth the eye detection outcome may have added than one left or right eye noticed. A modestinstance of the eye detection outcome is specified in Fig. 5.

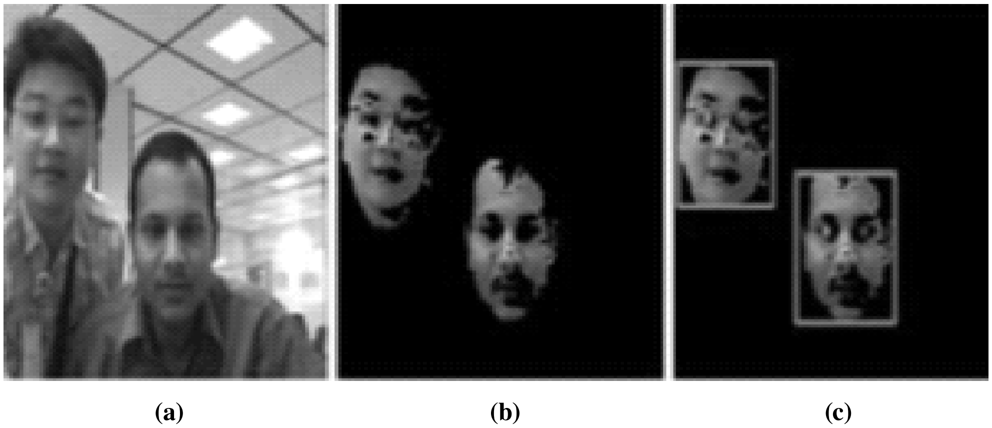


Figure 4: Example of the detection result (a) Frame captured by the webcam (b) Detected skin color pixels (c) Face and eye detection results

(E) Rotation and Normalization

When a face image is directed into this segment, the left eye and right eye coordinates, which are noticed inside the area of this image, are also attached to be the reference data for rotating the face image to be horizontal. Take up that the input eye coordinates of an image are (x_1, y_1) and (x_2, y_2). Let $x_1 \leq x_2$. Theforecast rotation angle θ can be originate by

$$\theta = \cos^{-1}\left[\frac{(x_2 - x_1)}{\sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}}\right] \tag{4}$$

Where, θ → rotation angle in radian. In this scheme, the face images are normalized to be 64×64 images. An instance of the face rotation and normalization is specified in Fig. 6

(F) Pupil Detection

Circle Hough transforms could be cast-off to regulate a circle when the similar amount of points situated on the unknown factors. A circle with radius R and Center (a,b) can be defined by Equation 2 and Equation

$$x = a + r\cos \tag{5}$$

$$y = b + r\sin \tag{6}$$

Where r → radius of the circle and a and b → center coordinates. From the equation, when the angle θ rotated to 360° then it will practice a circle. If an image comprises a lot of points, and specific can practice a circle, then the circle can be found by defining the first value of R, a and b. The transform is calculated by drawing circles of a specified radius at each point in the edge image. For each point where the perimeter of a drawn circle passes, the coordinate was incremented by 1. This was completed for each circle drawn to generate an accumulation array. A circle is designated by peaks in the accumulation array (Hough space) . Detection of circles by means of this transformation necessitates knowledge of the radius. If the scheme doesn't know the certain radius of the pupil or iris, the transform must be calculated for a range of radii. For every radius verified, the location and value of the extreme is stored. The radius with the uppermost peak specifies the utmost likely radius and center coordinate for the boundary.

(G) Support Vector Machines with Radial Basis Function

SVM fits to kernel methods. Kernel algorithms map information from an original space into a higher dimensional feature space by means of non-linear mapping. This algorithm is functional to feature space. The high dimensional feature space upsurges the exertion for calculating the scalar products in the feature space happens. Kernel functions cast-off to calculate these scalar products. By means of kernel functions there is not essential to calculate the feature space obviously. The SVM technique was initially established as a linear classifier. By exploiting kernel method, it also efficient for non-linear mapping of data. The technique of data separation by SVM is confirmed on a simplified example in Fig. 5.

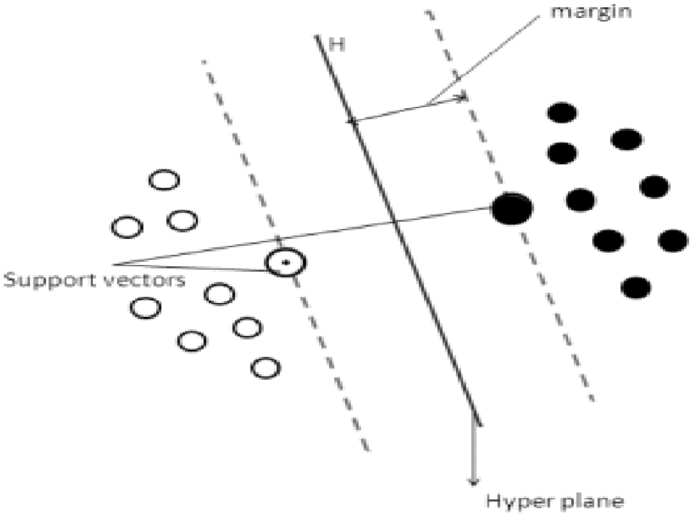


Figure 5: SVM hyperplane separation

SVM splits p-dimensional data by means of p-1 dimensional decision surface (hyper plane) in such a way that it exploits the margin of the information sets. The margin is distinct as the minimal distance of a model to the decision surface. The distance of the decision surface from the nearest presence of the individual information sets should be as huge as probable. In, the dashed lines that are similar with the hyper plane comprise support vectors. In our examinations we practice SVM with the RBF (radial basis function) kernel

$$K(X_i, X_j) = \exp(-\gamma \| X_i - X_j \|^2, \gamma > 0 \qquad (7)$$

Where xi, xj are data points from the original space. It is significant to discovery optimal factors γ (gamma) and C because diverse factor setups are appropriate for resolving diverse problems. With C >0 factor of for determination of a separating hyperplane with the maximal margin in advanced dimensional space by SVM.

A classification task typically comprises with training and testing phase which entail face images. In this work, separate the face images into two classes: face fits to the train database and face doesn't fit to the train database. Input information X that fall one region of the hyper-plane, (XT•W– b) > 0, are categorized as +1 and those that fall on the further area, (XT•W– b) < 0, are labeled as -1. The anticipated RBF grounded SVM categorizes the input images as matched or non matched.

4. EXPERIMENTAL RESULTS

In this segment, the recital of the anticipated RBF -SVM based biometric authentication is assessed and associated with prevailing Hybrid Artificial Bee Colony (ABC) based biometric authentication system. The investigates are directed by means of Matlab. The prevailing and anticipated detection methods are associated in terms of exactness, precision and recall.

Accuracy

It is distinct as the sum of the true positives and the true negatives, divided by the entireamount of classification parameters ($T_p + T_n + F_p + F_n$).

$$Accuracy = \frac{Tp + Tn}{Tp + Tn + Fp + Fn} \qquad (8)$$

Where,

Tp – True positive

Tn – Ture negative

Fp – False positive

Fn – False negative

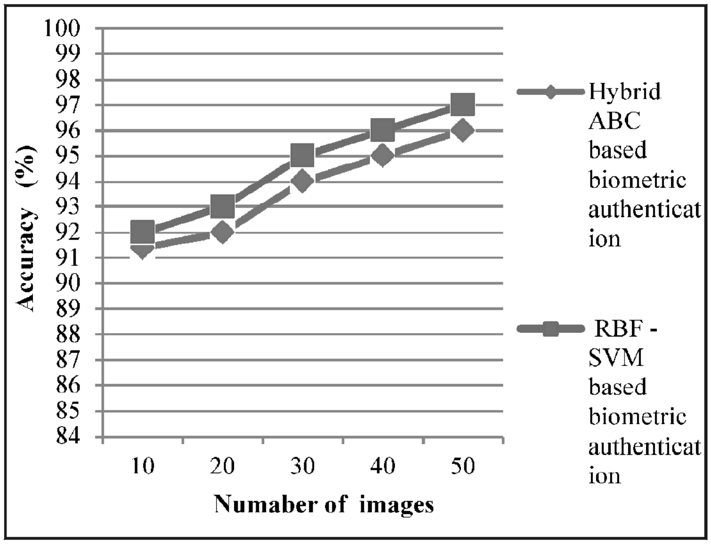


Figure 6: Accuracy Comparison

Figure 6 demonstrates that the assessment of projected RBF -SVM based biometric authentication and prevailing Hybrid ABC based biometric authentication system in terms of accuracy. The amount of images is taken as X axis and in y axis accuracy is taken. It accomplishes that the RBF -SVM based biometric authentication has shown the high precision outcomes for amount of image upsurges.

Precision

Precision is defined as the proportion of the true positives against both true positives and false positives results for intrusion and real features. It is defined as follows

$$Precision = \frac{T_p}{T_p + F_p} \tag{9}$$

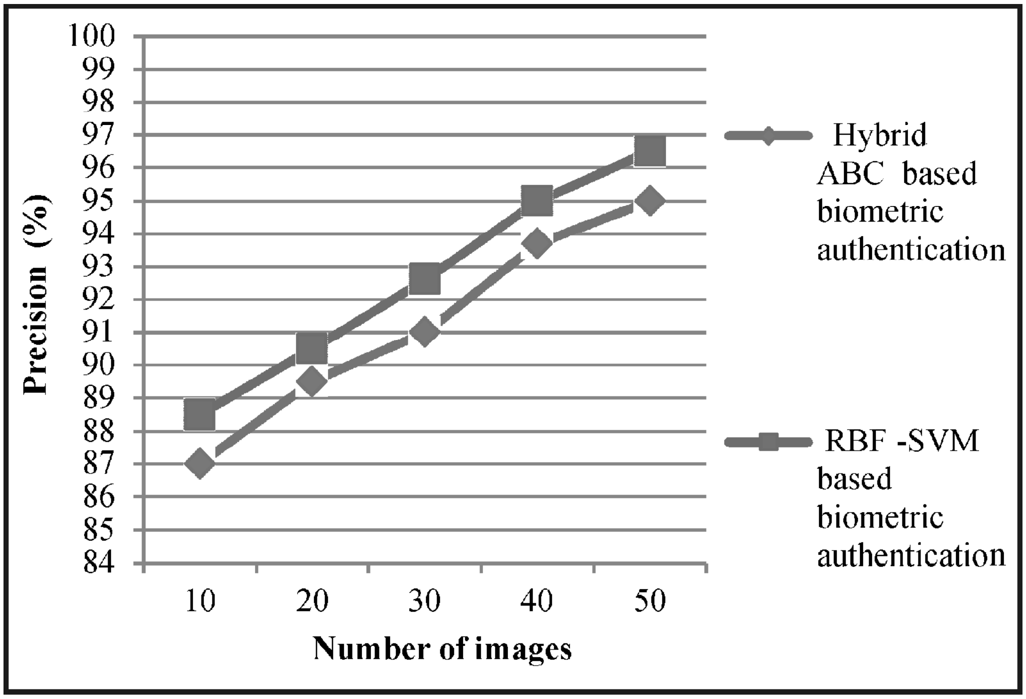


Figure 7: Precision comparison

Figure 7 displays the comparison outcome of projected RBF -SVM based biometric authentication, and prevailing Hybrid ABC based biometric authentication system in terms of precision. The number of images is taken as X axis and in y axis precision is taken. The anticipated system presented a pupil detection mechanism to progress the recital of the authentication scheme. The anticipated RBF -SVM based biometric authentication system attains improved precision result associated with the prevailing system.

Recall

It measures the ratio of positives that are correctly recognized

$$Recall = \frac{T_p}{T_p + F_n} \tag{10}$$

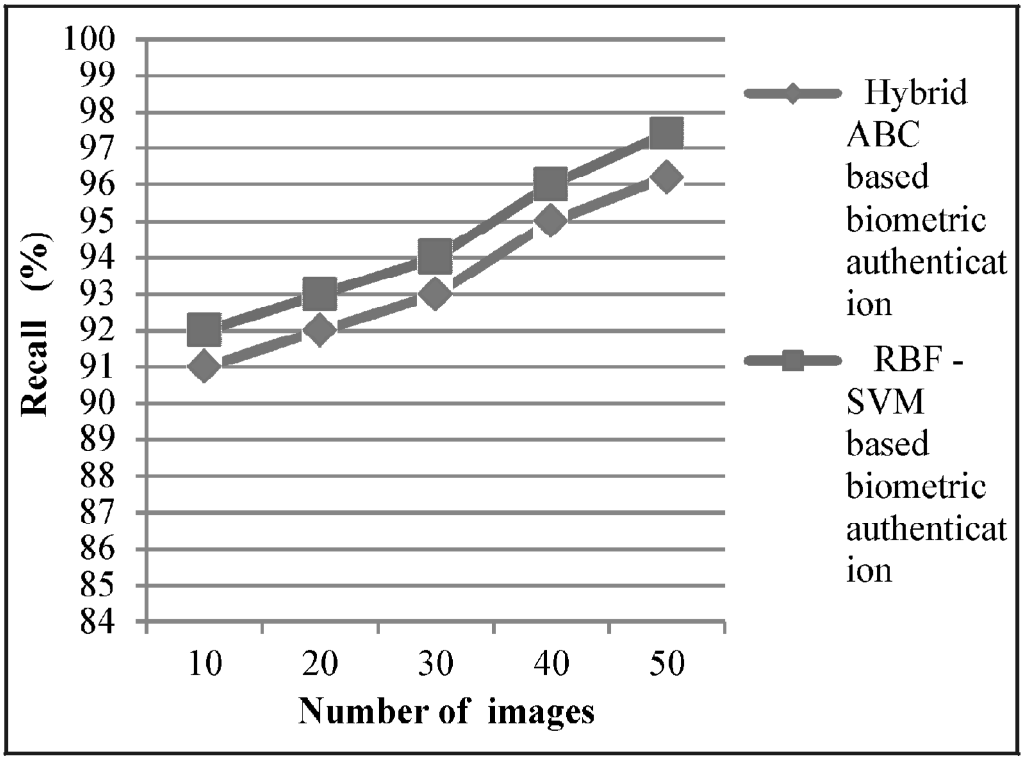


Figure 8: Recall comparison

Figure 8 displays the comparison outcome of anticipated RBF -SVM based biometric authentication, and prevailing Hybrid ABC grounded biometric authentication system in terms of recall. The number of images is taken as X axis and in y axis recall is taken. The anticipated system familiarized a pupil detection mechanism to progress the recital of the authentication system. The projected RBF -SVM based biometric authentication scheme attains better recall outcome associated with the prevailing system

5. CONCLUSION

The anticipated system presented an efficient Support Vector Machine with Radial Basis Function for biometric authentication scheme.At first the preprocessing is achieved by means of adaptive median filter. After the accomplishment of preprocessing the skin colour detection, face detection, eye detection and eye pupil detection is achieved and features area haul out. The extracted features are directingfor classification. Here SVMwith RBF is classifies the input images as matched or non matched. The face recognition was deliberate to be the chief elementmonitoring the authentication outcome, and the soft biometricmatching was engaged as the supporting system.The investigationaloutcomes show that the anticipated system accomplishes better recitalassociated with prevailing system in terms of accuracy, precision and recall.

REFERENCES

[1] K. Niinuma, U. Park, and A.K. Jain, "Soft biometric traits for continuous user authentication", *IEEE Transactions on information forensics and security*, Vol.5. No.4, pp.771-780, 2010.

[2] T. Rajyalakshmi, and K. Koteswararao, K. Anuradha, "The Design and Implementation of ID Authentication System Based on Fingerprint and Iris Identification", *International Journal of Professional Engineering Studies,* Vol.I, No. 2, 2013.

[3] S. Zhang, R. Janakiraman, T. Sim, and S. Kumar, "Continuous Verification Using Multimodal Biometrics," *Proc.Second Int'l Conf. Biometrics*, pp. 562-570, 2006.

[4] T. Sim, S. Zhang, R. Janakiraman and S. Kumar, "Continuous Verification UsingMultimodal Biometrics," *IEEE Trans. Pattern Analysis and Machine Intelligence*, Vol.29, No.4, 2007.

[5] A. Azzini, S. Marrara, R. Sassi and F. Scotti, "A fuzzy approach to multimodal biometric continuous authentication", *Fuzzy Optimal Decision Making*, Vol.7, pp.243-256, 2008.

[6] A. Azzini and S. Marrara, "Impostor Users Discovery Using a Multimodal Biometric Continuous Authentication Fuzzy System", *Lecture Notes In Artificial Intelligence, vol. 5178, Proceedings of the 12thInternational Conference on Knowledge-Based Intelligent Information and Engineering Systems, Part II, Section II,* pp.371-378, 2008.

[7] H. Bong Kang, and M. Ho Ju, "Multi-modal Feature Integration for Secure Authentication", *International Conference on Intelligent Computing*, pp1191-1200, 2006.

[8] C. Gracia, and G. Tziritas, "Face detection using quantized skin color regions merging and wavelet packet analysis", *IEEE Transactions on Multimedia*, Vol.1, No.3, pp. 264-277, 1999.

[9] Alajel, KM, Xiang, W & Leis, 2011, 'Face detection based on skin color modeling & modified Hausdorff distance', In Proceeding of IEEE International Conference on Consumer Communications and Networking, pp. 399-404.

[10] A. Altinok and M. Turk, "Temporal Integration for Continuous Multimodal Biometrics", *Proc. Workshop on Multimodal User Authentication,* pp.131-137, 2003.

[11] Q. Xiao, and X.D. Yang, "A facial presence monitoring system for information security", *Computational Intelligence in Biometrics: Theory, Algorithms, and Applications, 2009. CIB 2009.IEEE Workshop on IEEE,* 2009.

[12] X. Liu and T. Chen, "Video-based face recognition using adaptive hidden Markov models", *In Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, Vol.1, pp. 340–345, 2003.

[13] T. Sim, S. Zhang, R. Janakiraman, and S. Kumar, "Continuous verifi- cation using multimodal biometrics", *IEEE Trans. Pattern Anal. Mach. Intell.*, Vol.29, No.4, pp. 687–700, 2007.

[14] G. Kwang, R.H. Yap, T. Sim, and R. Ramnath, "A usability study of continuous biometrics authentication," *LNCS*, Vol.5558, pp. 828–837, 2009.

[15] R. Janakiraman, S. Kumar, S. Zhang and T. Sim, "Using continuous face verification to improve desktop security", *In Application of Computer Vision, 2005.WACV/MOTIONS'05* Vol. 1, pp. 501-507, 2005.