Received: July 12, 2019

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Multimodal Biometric Authentication System Using Modified ReliefF Feature Selection and Multi Support Vector Machine

Gavisiddappa[1]* Shivakumar Mahadevappa[2] Chandrashekar Mohan Patil[3]

[1]Department of Electronics and Communication Engineering,
Channabasaveshwara Institute of Technology, India
[2]Department of Electronics & Instrumentation Engineering,
GSSS Institute of Engineering and Technology for Women, India
[3]Department of Electronics and Communication Engineering,
Vidyavardhaka college of Engineering, Electronics and Communication Engineering, India
* Corresponding author's Email: gavi.hugar@gmail.com

Abstract: In the present scenario, multimodal biometric authentication is one of the emerging fields, which is applied in different applications like prison security, criminal identification, banking security, etc. The objective of this research work is to develop an effective feature selection algorithm to determine the optimal feature values for further improving the performance of multimodal biometric authentication. Initially, the input images were collected from Chinese Academy of Science Institute for Automation (CASIA) dataset. Then, feature extraction was carried-out by using Local Binary Pattern (LBP), minutiae feature extraction, Histogram of Oriented Gradient (HOG), and Gray-Level Co-Occurrence Matrix (GLCM) features like cluster prominence, Inverse Difference Moment Normalized (IDMN), and autocorrelation. After feature extraction, modified reliefF feature selection algorithm was used for rejecting the irrelevant features or for choosing the optimal features. In modified algorithm, Chebyshev distance measure was utilized instead of Manhattan distance in order to find the nearest miss and nearest hit instances. At last, the optimal feature values were given as the input for Multi-Support Vector Machine (MSVM) classifier for classifying an individual as an authorized or unauthorized person. The experimental result showed that the proposed system improved the classification accuracy up to 7% as related to the existing systems in terms of accuracy.

Keywords: Gray-level co-occurrence matrix, Histogram of oriented gradient, Local binary pattern, Multimodal biometric authentication, Multi-support vector machine.

1. Introduction

Biometric system is an automatic system, which recognizes an individual on the basis of behavioural or physiological traits that shows significant advances in a range of applications like surveillance, authentication, access control, security, etc. [1, 2]. Biometric system offers several benefits over possession and knowledge-based identity management systems [3]. The biometric system which uses only a single modality (either; iris, ear, face, fingerprint, etc.) for authentication is named as unimodal biometric authentication system [4, 5]. The unimodal biometric systems are more reliable, but it limitedly addresses the issues like robustness against spoofing attack, and high security [6]. The recognition accuracy of unimodal biometric system highly depends on physical and environmental challenges such as small sample size, and noisy sensor data. In order to address these problems, multimodal biometric systems are recently developed [7, 8]. The multimodal biometric systems utilize complementary traits that are extracted from dissimilar modalities (more than two modalities). In contrast to unimodal biometric authentication systems, the multimodal systems achieve good

performance against spoofing attacks and also delivers high system reliability. Though, most of the existing multimodal biometric systems performance is diminished by conflicting classifier scores under a dynamic environment [9-11]. To overcome this problem, a new multimodal biometric system is proposed on the basis of machine learning network.

In this research paper, a new automated system has been developed for improving the performance of multimodal biometric authentication. Initially, the input data were collected from CASIA dataset that contains three modalities; iris, face and fingerprint. After collecting the input data, feature extraction was carried out on individual modalities. At first, HOG, LBP, and GLCM features; cluster prominence, IDMN, and autocorrelation were used for extracting the feature values from the iris, and facial images. Correspondingly, minutiae feature was used to extract the feature vectors from the fingerprint images. The extracted hybrid feature values were fused by using feature level fusion technique. After obtaining the hybrid feature values, modified reliefF feature selection algorithm was used to reduce the dimensions of the extracted features. In modified reliefF feature selection algorithm, Chebyshev distance was used instead of Manhattan distance to identify the nearest miss and nearest hit instances. Here, Chebyshev distance uses only a limited number of features for representing the data that effectively reduces the "curse of dimensionality" problem. Then, the output of feature selection was given as the input for MSVM classifier for classifying an individual as an authorized or unauthorized person. At last, the proposed system performance was compared with the existing systems in light of accuracy, specificity, sensitivity, false rejection rate, and false acceptance rate.

This research paper is pre-arranged as follows. In section 2, numerous research papers on multimodal biometric authentication are reviewed. Detailed explanation about the proposed system is given in section 3. In addition, section 4 illustrates the quantitative analysis and comparative analysis of the proposed system. The conclusion is made in section 5.

2. Literature review

Many methods are developed by the researchers in multimodal biometric authentication topic. In this literature section, a brief review of some important contributions to the existing literature is presented.

J. Peng, A.A.A. El-Latif, Q. Li, and X. Niu, [12] developed an effective finger based multimodal biometric authentication system that combines fingerprint, finger knuckle, finger vein, and finger shape features of an individual human finger. In addition, the developed system utilized score level fusion approach on the basis of the triangular norm with forefinger biometric traits. The experimental analysis was performed on a virtual multimodal biometric data. The experimental outcome shows that the developed score level fusion approach using triangular norm achieves lower error rate compared to the existing systems. In this research paper, the computational complexity was high, while considering more modalities in a united framework.

H.M. Sim, H. Asmuni, R. Hassan, and R.M. Othman, [13] presented a new biometric system, which combines iris and facial biometric traits. In this research work, weighted score level fusion approach was used to fuse these modalities on the basis of weight availability. In order to validate the effectiveness of the developed system, three online available datasets were undertaken such as ORL dataset, UBIRIS version 2 dataset, and Universiti Teknologi Malaysia Iris and Face Multimodal Datasets (UTMIFM). In experimental phase, the developed system achieved high decidability index and accuracy that effectively distinct the distance between inter and intra distance. In this research study, the developed biometric system attains high false acceptance rate. So, the developed system was mostly applicable for individual modalities (iris, face, fingerprint, etc,) not for combined modalities.

H. Benaliouche, and M. Touahria, [14] developed a multimodal recognition system on the basis of iris and fingerprint traits. At first, the scores from the iris and fingerprint traits were fused at the decision levels. Then, the fuzzy logic methodology was utilized to match the scores combinations at the decision levels on the basis of classical sum rule and weighted rule. In this research study, CASIA iris dataset, and FVC 2004 fingerprint dataset were used for evaluating the efficiency of developed system in light of accuracy, error rate and matching time. The fusion of fuzzy logic decision involves human intervention, which was considered as one of the major drawbacks in the developed system.

S. Yuan, T. Zhang, X. Zhou, X. Liu, and M. Liu, [15] presented a multimodal biometric authentication system on the basis of multi-dimensional properties in optical technique. In this research study, the developed system combines optical encryption with multimodal biometric. Here, 200 pairs of biometric images were taken from polyU dataset for experimental investigation. The experimental phase confirmed that the developed system outperformed the existing systems on polyU database. The developed system considered only a

few traits, which need to be increased for further improving the performance of multimodal biometric.

B.S. Vidya, and E. Chandra, [16] developed a new automated multimodal biometric authentication system to improve the identification performance. At first, the input data were collected from CASIA iris, facial and fingerprint datasets. Besides, feature extraction was performed on the collected data by using Entropy based Local Binary Pattern (ELBP). At last, the extracted feature vectors were given as the input for MSVM classifier for classifying an individual as an authorized or unauthorized person. Still, the developed system requires a new feature selection approach to further improve the performance of multimodal biometric.

In order to overcome the above-mentioned problems, a new supervised system is developed for improving the performance of multimodal biometric authentication.

3. Proposed system

Biometric is one of the emerging technologies, which is extensively used in all type of secured transaction based forensics, prison security, criminal identification, etc. The biometric system recognizes an individual by detecting the authenticity of the behavioural trait possessed by an individual. Presently, fingerprint, face, and iris are some of the commonly utilized traits for recognizing an individual. The usage of single biometric trait systems is a lack of reliability and also susceptible to attacks. To address this problem, multi-modal biometric authentication systems are coming into existence. In this research study, the proposed multimodal biometric authentication system contains four stages; data collection, feature extraction, feature selection and classification. Fig. 1 represents the block diagram of the proposed system and the detailed explanation about the proposed system is described below.

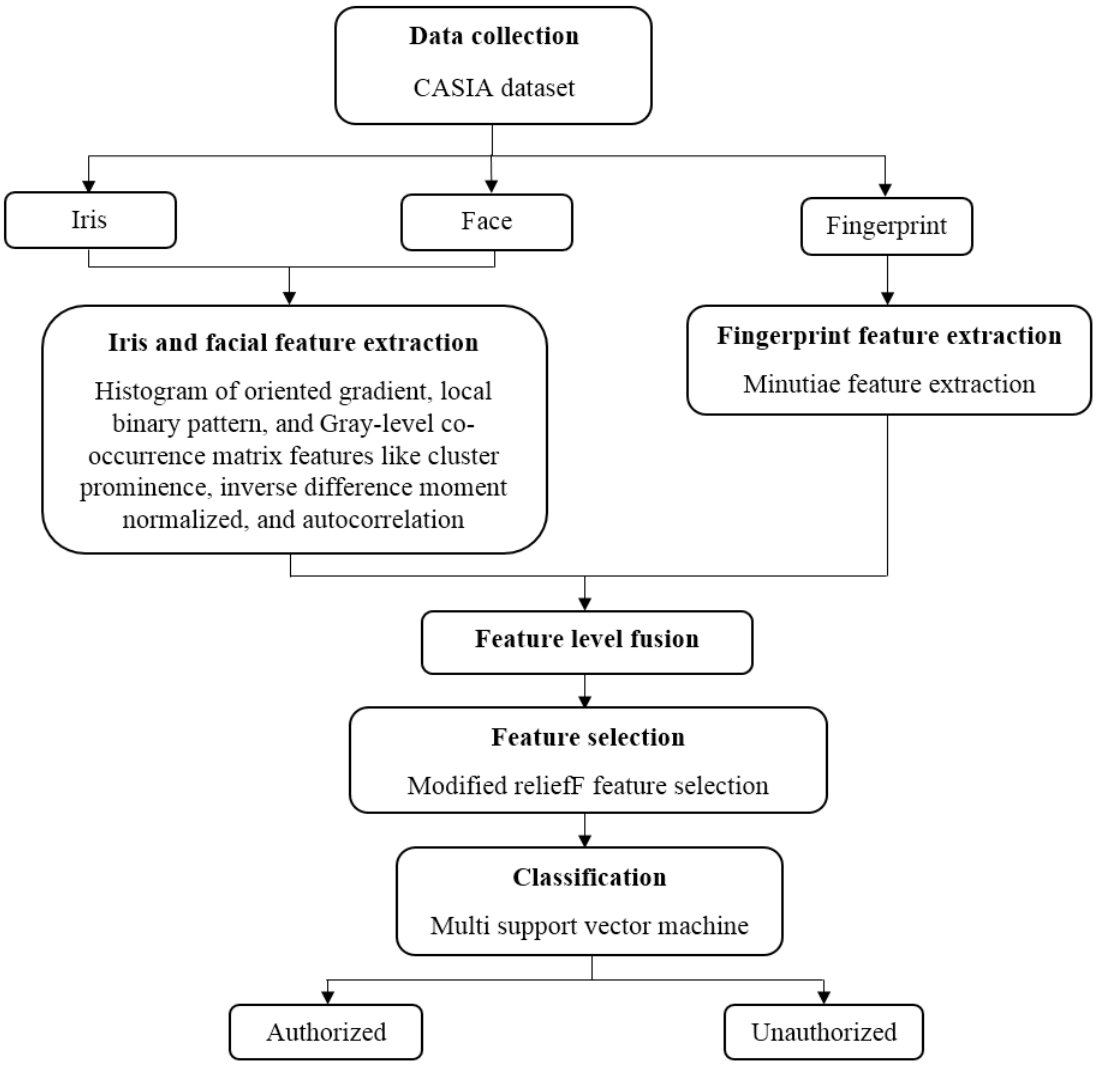


Figure.1 Work flow of proposed system

3.1 Image collection

Initially, the input data are collected from an online available dataset: CASIA dataset. In this research, the proposed system has experimented on three datasets: CASIA iris, CASIA face, and CASIA fingerprint. The CASIA iris dataset contains 22,035 iris images from 700 subjects. Each iris image is eight-bit gray level JPEG file, which is collected under infrared illumination. The CASIA fingerprint dataset comprises of 500 classes with 400 samples in each of the class. Similarly, the CASIA face dataset comprises of 2,500 facial images of 500 subjects with different factors like expression, illumination, eye-glasses, pose, etc. The sample images of CASIA dataset is represented in Fig. 2.

3.2 Feature extraction

After collecting the images, feature extraction is carried-out for extracting the feature values from the collected data. Feature extraction is defined as the action of mapping the image from image space to feature space and also it transforms the large redundant data into a reduced data representation. Feature extraction process helps to decrease the computational complexity of the system. In this research, feature extraction is performed by using HOG, LBP, GLCM, and minutiae feature extraction for extracting the feature values from the collected images (iris, face and fingerprint). The detailed explanation about the feature descriptors is given below.

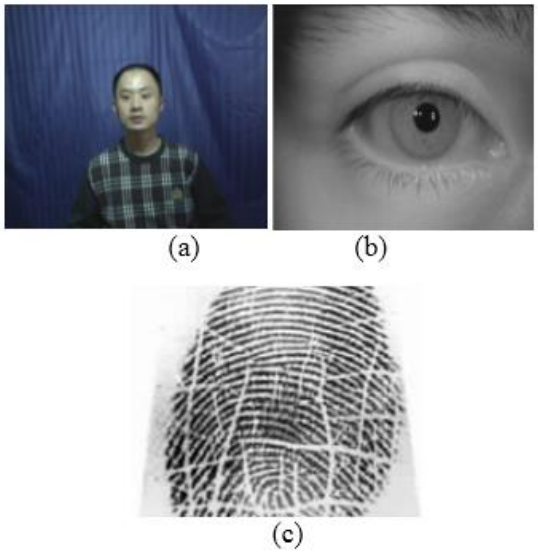


Figure.2 (a) CASIA face image, (b) CASIA iris image, and (c) CASIA fingerprint image

3.2.1. Iris and facial feature extraction

In iris and facial feature extraction, hybrid feature descriptors are applied to extract the feature information from the iris and facial data. The hybrid feature descriptors include HOG, LBP, and GLCM features; cluster prominence, IDMN, and autocorrelation. A brief description of hybrid feature extraction is detailed below.

3.2.1.1. Histogram of oriented gradients

The HOG feature descriptor effectively captures the local appearance of the objects in order to account the invariance in illumination conditions and object transformations. Initially, the information about the gradient is evaluated by applying a gradient operator N. Gradient point of the image I is indicated as(x, y)that is mathematically expressed in Eq. (1).

$$G_x = N \times I(x,y) \text{and } G_y = N^T \times I(x,y) \quad (1)$$

Where, G_x is denoted as horizontal direction of the gradient, and G_y is stated as vertical direction of the gradient. Usually, the image detection windows are partitioned into many spatial regions that are named as cells. Hence, the gradient magnitude of the image pixels is determined along with the edge orientation. Refer the Eq. (2) and (3) in order to calculate the gradient magnitude $G(x, y)$ and edge orientation $\theta(x, y)$ of the image.

$$G(x,y) = \sqrt{G_x(x,y)^2} + \sqrt{G_y(x,y)^2} \quad (2)$$

$$\theta(x,y) = tan^{-1} \frac{G_y(x,y)}{G_x(x,y)} \quad (3)$$

Where, $\theta(x, y)$ is indicated as edge orientation of the image, I is specified as input image, N is denoted as gradient operator, and N^T is indicated as transformation of gradient point.

After calculating the histogram values, the normalization process is carried-out to eliminate the illumination condition and noise from the collected images. Normalization is an essential phase in HOG feature descriptor that helps to maintain discriminative characteristics and also to perform consistently even against the factors like background-foreground contrast and local illumination variations in the collected images. Normalization is done by using “block” as a fundamental region of operation. Each block region

24	155	243
78	**112**	12
11	45	122

0	1	1
0		0
0	0	1

32	64	128
16		1
8	4	2

Input image 3×3 neighbourhood pixel Threshold Weighted matrix

Local binary pattern code is 2+64+128=194

Figure.3 Basic binary pattern operator

comprises of a square array of four cells. Each new block is defined with a 50% overlap with the previous block.

Normalization effectively maintains the cell-based local gradient information, which is invariant to local illumination conditions. In HOG feature descriptor, four dissimilar patterns of normalizations are available such as, L1-Sqrt, L2-norm, L1-norm, and L2-Hys. Among these normalizations, L2-norm delivers better performance, because it encodes the similar image features across the different coloured squares that are mathematically given in the Eq. (4).

$$L_{2-norm} : f = \frac{x}{\sqrt{||x||_2^2 + e^2}} \tag{4}$$

Where, e is represented as small positive value or small constant value (hopefully the exact value is unimportant) in HOG feature descriptor, f is stated as feature extracted value, x is represented as non-normalized vector in histogram blocks and $||x||_2^2$ is denoted as L2-norm of HOG normalization.

3.2.1.2. Local binary pattern

LBP is a texture analysis descriptor that transforms the collected image into labels based on the luminance value. In LBP feature descriptor, gray-scale invariance is an essential factor that depends on the texture and local patterns. In an image I , the pixel positions are mentioned as x and y, which is derived by using the central pixel value x_c of x as the threshold to signify the neighbourhood pixel m value. The binary value of the pixel is weighted by using the power of two and then summed to create a decimal number for storing in the location of central pixel x_c that is mathematically given in the Eq. (5).

$$LBP\ (x,y) = \sum_{i=0}^{m-1} I(x_i - x_c)^{2i}, I(x) = \begin{Bmatrix} 1, x \geq 0 \\ 0, x \leq 0 \end{Bmatrix} \tag{5}$$

Where, x_i indicated as gray level value of the central pixel of a local neighbourhood. For instance, the basic binary pattern operator is denoted in Fig. 3.

The basic neighbourhood model of LBP is p-neighbourhood model that gives 2^p output, which leads to a large number of possible patterns. If the texture analysis area is small, the LBP histogram is not attractive. The uniform model of LBP attains only when the jumping time u maximizes. It is measured by using the Eq. (6).

$$U\big(LBP(x,y)\big) = |I(x_{c-1} - x_i) - I(x_0 - x_i)| + \sum_{i=1}^{m-1} |I(x_c - x_i) - I(x_{c-1} - x_i)| \tag{6}$$

Where, x_c is represented as central pixel value, u is stated as jumping time, and I is indicated as input image.

3.2.1.3. Gray level co-occurrence matrix

GLCM is a high-level feature descriptor, which evaluates image properties on the basis of second order statistics. In each entry (x, y) , GLCM calculates the number of gray level pairs of x and y with a distance d. Hence, GLCM calculates gray level pixel intensity value x in a particular pixel with the value y. Every element (x, y) is the sum of pixel x that occurred in the input facial and iris images. The gray level numbers help to determine the GLCM size. In addition, GLCM feature descriptor reveals certain characteristics about gray-level spatial distribution. Co-occurrence metric is defined as relative separation vector, which utilizes each image pixels for separating the vector from matrix indices and then the matrix elements are incremented. The image texture is characterized by the object shapes, which are extracted from the collected images. The co-occurrence is stated in a matrix of relative frequencies with two neighbouring elements(x, y), which are distinct by a distance d at orientation θ. Here, three GLCM features are used to

extract the features from collected images such as, autocorrelation, cluster prominence, and IDMN.

- **Cluster prominence**

Cluster prominence calculates asymmetry in the collected images. If prominence of the clusters indicates maximum value, then the digital image has minimum symmetric. Further, if the prominence of the clusters represents maximum value, then the GLCM matrix includes peaks around the mean values. But in the collected facial and iris image, minimum cluster prominence value represents the bit fluctuations in grayscale. The formula to calculate cluster prominence is represented in Eq. (7).

$$Cluster\ prominence = \sum_{x=0}^{n-1}\sum_{y=0}^{n-1}(x + y - \mu_x - \mu_y)^4 \times p_{xy} \quad (7)$$

Where, μ is denoted as mean and p_{xy} is stated as normalized co-occurrence matrix, and n is indicated as number of images.

- **Inverse difference moment normalized**

IDMN is one of the effective image texture measures that is mathematically defined in Eq. (8). It is also named as homogeneity that is used to calculate the local homogeneity of the collected images. In addition, IDMN identifies the GLCM feature distributions in order to determine whether the given image is non-textured or textured.

$$IDMN = \sum_{x=0}^{n-1}\sum_{y=0}^{n-1}\frac{1}{1+(x+y)^2}M(x,y) \quad (8)$$

Where, n is denoted as number of images, and $M\ (x, y)$ is stated as normalized image.

- **Autocorrelation**

Autocorrelation feature is used to analysis the roughness or fitness of the image texture. Initially, the extracted features are related to the size of texture primitive, for instance, texture fitness. If the image texture is unsmooth, the autocorrelation function works inefficiently. Usually, the autocorrelation function shows valleys and peaks in the normal textures. In addition, it has a link with power spectrum of Fourier transform (u, v), so it is reactive to noise intrusion. The autocorrelation function is mathematically represented in Eq. (9).

$$Autocorrelation = \frac{\sum_{x=0}^{n}\sum_{y=0}^{n} I(x,y).I(x+u,y+v)}{\sum_{x=0}^{n}\sum_{y=0}^{n} I^2(x,y)} \quad (9)$$

Where, power spectrum of Fourier transform is denoted as (u, v), n is indicated as number of images, and $I(x, y)$ is stated as normalized image.

3.2.2. Fingerprint feature extraction using minutiae feature

In this section, minutiae feature extraction is undertaken for extracting the features from fingerprint data. The commonly utilized concept in minutiae extraction is crossing number that includes skeleton picture, where the edge stream design is eight-connected. The minutiae are separated by checking the nearby neighbourhood of each edge pixels in the fingerprint image by utilizing a 3×3 window. Then, register the crossing number esteems, which are characterized as a half of the sum of difference between the sets of nearby pixels in the eight-neighbourhood. By using the properties of crossing number, the edge pixels are classified as non-minutiae point or bifurcation, and edge ending, which is graphically denoted in Table 1.

After minutiae extraction, it is crucial to use a post processing stage for authenticating the minutiae. In this research study, crossing number method is slightly modified for a pixel *P* in order to increase the extraction speed. The general equation of crossing number for an edge pixel *P* is given in the Eq. (10).

$$Crossing\ number = 0.5\sum_{i=1}^{8}|P_i - P_{i+1}|, \quad P_9 = P_1 \quad (10)$$

Where, P_i is stated as a pixel intensity value in the neighbourhood of P. For a pixel P, eight neighbouring pixels are scanned in an anti-clockwise direction as given in Table 2.

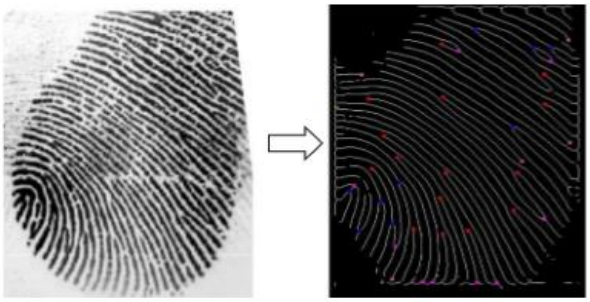
The minutiae based unique fingerprint matching is intended to solve the problems of correspondence and similarity calculation. Also, it enhances the minutiae matching for locating an admissible arrangement between the two fingerprints and then solidify the nearby matching outcomes at a global level. Fig. 4 represents the fingerprint and minutiae detected image.

Table 1. Properties of crossing number

Crossing number	Properties
0	Isolated point
1	Ridge ending point
2	Continuing ridge point
3	Bifurcation point
4	Crossing point

Table 2. Pixel in anti-clockwise direction

P_4	P_3	P_2
P_5	P	P_1
P_6	P_7	P_8



(a) (b)

Figure.4 (a) Fingerprint image and (b) minutiae detected image

3.3 Feature level fusion

After extracting the features from iris, fingerprint and face images, feature level fusion is applied to combine all the extracted feature vectors. Presently, feature level fusion is more successful than other alternate combination levels, because it contains richer data about the input biometric information than the coordinating score or the output decision of a classifier. In this research, Feature level fusion combines the biometric information of iris, fingerprint and face images. The response time of feature level fusion is less compared to score level fusion. The feature level fusion contains two major phases such as, normalization of features and fusing the features. Normalization of features: Features extracted from the face, iris and fingerprint are high dimensional, due to the variation in distribution and range. The high dimensional issue is overcome by normalizing the features. Fusing the features: After normalizing the features, use the extracted features of face, iris and fingerprint images. After performing feature level fusion, feature selection is carried-out for selecting the optimal features from the extracted features.

3.4 Feature selection using modified reliefF feature selection

Feature selection is a high-level process that identifies the relevant subsets of data based on a particular criterion. In biometric authentication application, numerous feature selection methodologies are available such as, genetic algorithm, infinite feature selection, regularized discriminant feature selection, etc. In this research study, modified reliefF feature selection is utilized for selecting the optimal features to perform better classification. It is very robust while dealing with noisy and real time data. Initially, the reliefF feature selection algorithm randomly chooses the instances r_i and then searches for k nearest neighbor in the same class is named as nearest hit H_j and in the dissimilar classes is named as nearest miss M_j . Usually, Manhattan distance measure is utilized to identify the nearest miss M_j and nearest hit H_j instances. Here, Chebyshev distance measure is used instead of Manhattan distance measure for identifying the nearest miss M_j and nearest hit H_j instances. The major benefit of Chebyshev distance measure is that it needs only limited time for deciding the distances between the instances r_i. Although, Chebyshev distance measure utilizes only limited number of features for representing the data, which is enough to attain accurate neighbourhood selection and better prediction and also it completely reduces the "curse of dimensionality" problem.

Then, reliefF feature selection algorithm updates the quality estimation $W[A]$ for all the attributes A that mainly depends on the values of $r_i, H_j,$ and M_j. If the instances H_j and r_i have similar values of the attribute A, then the attribute A is separated into two instances with the similar classes, which is essential to minimize the quality estimation $W[A]$.In contrast, if the instances H_j and r_i have dissimilar values of the attribute A, then the attribute A separate into two instances with the dissimilar classes, which is essential to maximize the quality estimation $W[A]$. The whole mechanism repeat for m times, where m is represented as a user-defined parameter. In this research work, the user-defined parameter is fixed as twenty. In reliefF feature selection algorithm, the quality estimation $W[A]$ is updated by utilizing the Eq. (11), (12), and (13).

$$W[A] = W[A] + (\bar{H} + \bar{M})/20 \tag{11}$$

Where,

$$\bar{H} = -\sum_{j=1}^{k} D\ (A, r_i\ , H_j)/k \tag{12}$$

$$\bar{M} = \sum_{C \neq cl(r_i)} [(\frac{P(C)}{1 - P\big(cl(r_i)\big)}) \sum_{j=1}^{k} D\ (A, r_i\ , M_j(C))] \Big/ k \tag{13}$$

Where, $W[A]$ is denoted as quality estimation, r_i is represented as instances, A is indicated attributes, H_j and M_j are denoted as nearest hit and

nearest miss values, $P(C)$ is represented as prior class, D is indicated as distance between the selected instances r_i , C is represented as total number of classes, and $cl(r_i)$ is denoted as class of the i^{th} sample. The pseudo code of modified reliefF feature selection is described below.

3.4.1. Pseudo code of modified reliefF feature selection

Input: Vector of class values and attribute values are assigned to each training instances.

Output: Quality estimation W of the attributes.

1. Assign all weights $W[A] := 0.0$;
2. **For** $i := 1$**to** m **do begin**
3. Randomly choose the instances r_i
4. Identify k nearest hits H_j using Chebyshev distance measure
5. For every class $C \neq class\ (r_i)$**do**
6. From class C identify the k nearest misses $M_j(C)$;using Chebyshev distance measure
7. **For**$A := 1$
8. $W[A] = W[A] + (= -\sum_{j=1}^{k} D\ (A, r_i\ , H_j)/k + \sum_{C \neq cl(r_i)}[(\frac{P(C)}{1-P(cl(r_i))}) \sum_{j=1}^{k} D\ (A, r_i\ , M_j(C))]k)/20$
9. **End**

3.5 Classification using multi support vector machine

After obtaining the optimal feature vectors, classification is carried-out using MSVM classifier. Usually, regular SVM is a two-class classification methodology. Hence, it is essential to concentrate on the multi binary classification issues for extending the normal SVM classifier to multi-class SVM classifier. In the conventional SVM classification approach, the multi-class classification is rehabilitated into n^{th} two class and i^{th} two-class issues, where class i is distinct from the remaining classes. The two important methodologies in SVM classifier are One-Against-All (1-a-a) and One-Against-One (1-a-1). In this scenario, 1-a-a approach gives solution to create a binary classifier for every class that helps to separate the objects in the same class. In n^{th} class, 1-a-a approach generates n^{th}binary classifiers, and the i^{th}classifier is trained with the data samples in i^{th}class with the positive labels and the residual data samples are trained with the negative labels. The result of n^{th}class in 1-a-a approach relates with the 1-a-1 approach for obtaining the highest output value. In addition, the 1-a-1 approach is the resultant of previous researches on two class classifiers.

The MSVM classifier generates all possible two-class classifiers from the training sets of n^{th} classes, and it trains only two out of n^{th} classes that results in $n \times (n-1)/2$ classifiers. In MSVM, decision function is an active way to moderate the multi-class problems that is constructed by assuming all the $n-th$ classes. The M-SVM classification technique is an extension of SVM, which is mathematically represented in the Eq. (14), (15), and (16).

$$min\Phi(w, \xi) = 1/2 \sum_{m=1}^{k} (w_m . w_m) + c \sum_{i=1}^{l} \sum_{m \neq yi} \xi_i^m \quad (14)$$

Subjected to,

$$(w_{yi} . x_i) + b_{yi} \geq (w_{yi} . x_i) + b_m + 2 - \xi_i^m \quad (15)$$

$$\xi_i^m \geq 0, i = 1,2,3 \ldots l, m, yi \in \{1,2,3 \ldots k\}, m \neq yi \quad (16)$$

At last, the decision function is represented in Eq. (17).

$$f(x) = arg\ max[(w_i . x) + b_i]\ , i = 1,2,3,..k \quad (17)$$

Where, ξ_i^m is stated as slack variables, l is considered as training data point, c is represented as user's positive constant, yi is denoted as class of training data vectors x_i, and k is stated as number of classes.

4. Experimental result and discussion

In this research, MATLAB (version 2018a) was utilized for experimental simulation with Intel ® core™ i3-7100U, 4GB RAM, 64-bit OS, and x-64 based processor. In order to estimate the effectiveness of proposed system, the performance of the proposed system was compared with an existing system: ELBP-MSVM [16] on a reputed CASIA dataset. The proposed system performance was evaluated by means of accuracy, specificity, sensitivity, false rejection rate, and false acceptance rate.

4.1 Performance measure

Performance measure is defined as the regular measurement of experimental outcome that develops reliable information about the effectiveness of the proposed system. The relationship between the input values and output values of the proposed system is

understand by utilizing the performance measures such as accuracy, specificity, sensitivity, false rejection rate, and false acceptance rate. The formula to evaluate specificity, sensitivity, false rejection rate, and false acceptance rate are given in the Eq. (18), (19), (20), and (21).

$$Specificity = \frac{TN}{TN+FP} \times 100 \quad (18)$$

$$Sensitivity = \frac{TP}{TP+FN} \times 100 \quad (19)$$

$$False\ rejection\ rate = \frac{FP}{TP+FN} \times 100 \quad (20)$$

$$False\ acceptance\ rate = \frac{FP}{FP+TN} \quad (21)$$

Additionally, accuracy is another effective performance measure that is used to find the effectiveness of the proposed system for multimodal biometric authentication. In particular, accuracy is the most instinctive measure and it is simply a ratio of total observations to the correctly predicted observations. The general formula of accuracy is represented in Eq. (22).

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \times 100 \quad (22)$$

Where, FP is specified as false positive, TN is indicated as true negative, TP is stated as true positive, and FN is represented as false negative.

4.2 Quantitative analysis

In this section, CASIA dataset is used for evaluating the performance of the proposed and existing systems. In Table 3, the performance of proposed system is validated by means of specificity, sensitivity and accuracy. In this scenario, the performance evaluation is validated for 89 subjects with 80% training of data and 20% testing of data. The validation result shows that the MSVM classifier out-performed the existing classification methodologies. The sensitivity of MSVM classifier is 94.32% and the comparative classification methodologies; random forest, Adaptive Network based Fuzzy Inference System (ANFIS) and Long Short-Term Memory (LSTM) delivers 67.8%, 76.90% and 88.87% of sensitivity. Correspondingly, the specificity of MSVM classifier is 96.67% and the comparative classification methods deliver 53%, 78.43% and 84% of specificity. Additionally, the accuracy of MSVM classifier is 97.09% and the comparative classification methods; random forest, ANFIS and LSTM achieves 79%, 75.78% and89.90% of accuracy. The graphical representation of sensitivity, specificity, and accuracy is indicated in Fig. 5.

In Table 4, the performance of the proposed system was validated with dissimilar classifiers in terms of false rejection rate, and false acceptance rate. The false rejection rate of MSVM classifier is 11.89% and the comparative classification methodologies; random forest, ANFIS and LSTM delivers 32.90%, 24.67% and 14.67% of false rejection rate. Correspondingly, the false acceptance rate of MSVM classifier is 9.87% and the comparative classification methods delivers 25.78%, 20% and 9.87% of false acceptance rate. Tables 3 and 4 clearly shows that the MSVM classifier performs effectively compared to other existing classification methods on CASIA database. The graphical representation of false rejection rate, and false acceptance rate is represented in Fig. 6.

Table 3. Performance evaluation of proposed system by means of sensitivity, specificity, and accuracy

Classifiers	Sensitivity (%)	Specificity (%)	Accuracy (%)
Random forest	67.8	53	79
ANFIS	76.90	78.43	75.78
LSTM	88.87	84	89.90
MSVM	**94.32**	**96.67**	**97.09**

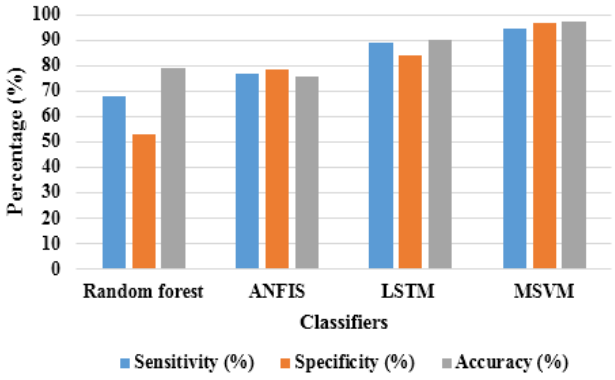


Figure.5 Graphical representation of proposed system in light of sensitivity, specificity, and accuracy

Table 4. Performance evaluation of proposed system by means of false rejection rate, and false acceptance rate

Classifiers	False rejection rate (%)	False acceptance rate (%)
Random forest	32.90	25.78
ANFIS	24.67	20
LSTM	14.67	11.87
MSVM	**11.89**	**9.87**

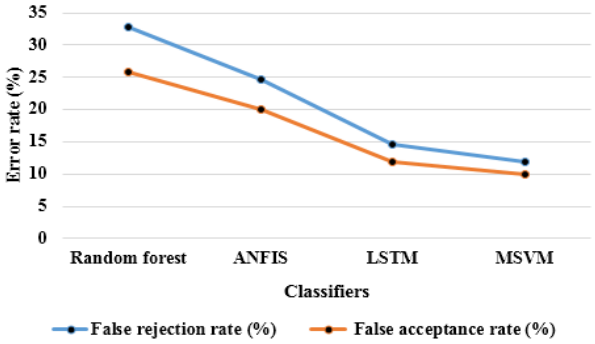


Figure.6 Graphical representation of proposed system in light of false rejection rate, and false acceptance rate

Table 5. Accuracy valuation of proposed system using feature selection

Accuracy (%)		
Modality	**Modified reliefF**	**Conventional reliefF**
Iris modality	90.56	76.5
Facial modality	93.8	60.70
Fingerprint modality	91.12	89
Iris and facial based features	93.34	84.78
Facial and fingerprint based features	92	90.87
Iris and fingerprint based features	94.53	90.12
Fusing all three modalities	**97.09**	92.89

Table 5 and Fig. 7 represents the performance of the proposed system with modified reliefF feature selection and conventional reliefF feature selection. In addition, the efficiency of feature selection is analyzed with dissimilar modalities such as iris modality, facial modality, fingerprint modality, iris and facial based features, facial and fingerprint-based features, iris and fingerprint-based features, and fusion of all three modalities (iris, face, and fingerprint). In modified reliefF feature selection, the MSVM classifier averagely improved the accuracy in multimodal biometric authentication upto 4.2% compared to conventional algorithm. In this research study, the undertaken feature extraction methods determine the non-linear and linear features of iris, face, and fingerprint data, and also preserves the quantitative relationships between the low level and high level features. The undertaken performance measures confirm that the proposed system performs well in multimodal biometric authentication compared to the existing systems.

4.3 Comparative analysis

Table 6 indicates the comparative study of proposed and existing system performance. B.S. Vidya, and E. Chandra, [16] developed a new texture based feature extraction technique (ELBP) for converting LBP histogram into one dimensional space. Biometric images (iris, face and fingerprint) gives higher uniqueness by incorporating the entropy values into local regions of biometric images. This paper was investigated on an online available database (CASIA dataset) for validating the experimental outcome. In the experimental outcome, the developed system achieved 90% of accuracy and specificity in face modality, 91% of accuracy and 90% of specificity in iris modality, and 89% of accuracy and 88% of specificity in fingerprint modality. Compared to the existing work, the proposed work attained 97.09% of accuracy, and 96.67% of specificity by combining face, iris and fingerprint modalities, which was superior compared to the existing works. In this research work, feature selection is a fundamental part of multimodal biometric authentication system. Each biometric image comprises of numerous features and high data-space volume that leads to "curse of dimensionality" problem. So, feature selection is essential to optimize the features that are appropriate for better classification.

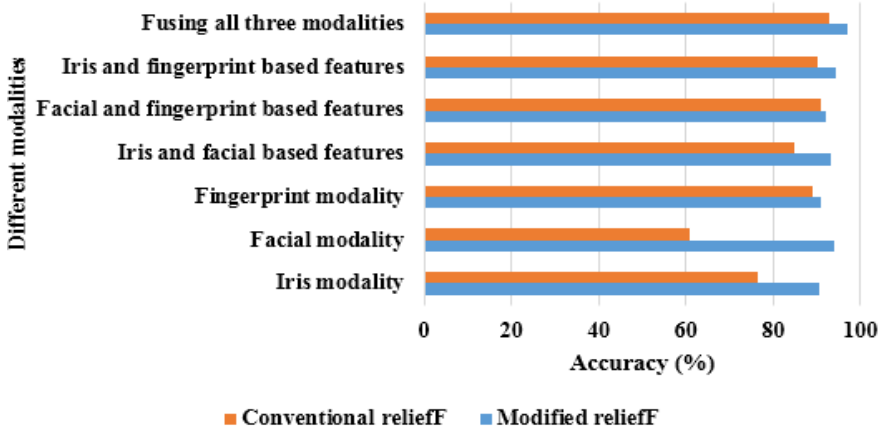


Figure.7 Graphical comparison of accuracy valuation with modified and conventional reliefF feature selection

Table 6. Comparative analysis of proposed and existing system

References	Data set	Modalities	Specificity (%)	Accuracy (%)
B.S. Vidya, and E. Chandra, [16]	CASIA dataset	Face	90	90
		Iris	90	91
		Finger print	88	89
Proposed work		Face	92	93.8
		Iris	90.28	90.56
		Finger print	93.27	91.12
		Face + iris + fingerprint	**96.67**	**97.09**

5. Conclusion

In this research, a new supervised automated system is developed for multimodal biometric authentication. The main objective of this experimental study is to develop a proper feature extraction and feature selection methods for classifying an individual as an authorized or unauthorized person. In this research, modified reliefF feature selection algorithm is used to select the optimal features. By selecting the optimal features from the extracted features, a set of most dominant discriminative features are obtained. These optimal features are classified by using a supervised classifier: MSVM. Compared to the existing system (ELBP-MSVM [16]), the proposed system delivered an effective performance by means of quantitative analysis and comparative analysis. From the experimental analysis, the proposed system achieved 97.09% of accuracy, but the existing system obtained a limited accuracy of 90% on CASIA dataset. In future work, a new unsupervised system can be developed on the basis of deep learning concept for further improving the performance of multimodal biometric authentication.

References

[1] D. Jagadiswary and D. Saraswady, "Biometric authentication using fused multimodal biometric", *Procedia Computer Science*, Vol.85, pp.109-116, 2016.

[2] P. Bedi, R. Bansal, and P. Sehgal, "Multimodal biometric authentication using PSO based watermarking", *Procedia Technology*, Vol.4, pp.612-618, 2012.

[3] G.S. Walia, T. Singh, K. Singh, and N. Verma, "Robust multimodal biometric system based on optimal score level fusion model", *Expert Systems with Applications*, Vol.116, pp.364-376, 2019.

[4] M. Hammad, Y. Liu, and K. Wang, "Multimodal Biometric Authentication Systems Using Convolution Neural Network Based on Different Level Fusion of ECG and Fingerprint", *IEEE Access*, Vol.7, pp.26527-26542, 2019.

[5] K.O. Bailey, J.S. Okolica, and G.L. Peterson, "User identification and authentication using multi-modal behavioral biometrics", *Computers & Security*, Vol.43, pp.77-89, 2014.

[6] M.J. Sudhamani, M.K. Venkatesha, and K.R. Radhika, "Fusion at decision level in multimodal biometric authentication system using Iris and Finger Vein with novel feature extraction", In: *Proc. of Annual IEEE India Conference (INDICON)*, pp.1-6, 2014.

[7] Q.D. Tran and P. Liatsis, "RABOC: An approach to handle class imbalance in multimodal biometric authentication", *Neurocomputing*, Vol.188, pp.167-177, 2016.

[8] M. Haghighat, M. Abdel-Mottaleb, and W. Alhalabi, "Discriminant correlation analysis: Real-time feature level fusion for multimodal biometric recognition", *IEEE Transactions on Information Forensics and Security*, Vol.11, No.9, pp.1984-1996, 2016.

[9] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, "A fingerprint and finger-vein based cancelable multi-biometric system", *Pattern Recognition*, Vol.78, pp.242-251, 2018.

[10] M. Xin and J. Xiaojun, "Correlation-based identification approach for multimodal biometric fusion", *The Journal of China Universities of Posts and Telecommunications*, Vol.24, No.4, pp.34-50, 2017.

[11] W. Yang, S. Wang, G. Zheng, and C. Valli, "Impact of feature proportion on matching performance of multi-biometric systems", *ICT Express*, Vol.5, No.1, pp.37-40, 2019.

[12] J. Peng, A.A.A. El-Latif, Q. Li, and X. Niu, "Multimodal biometric authentication based on score level fusion of finger biometrics", *Optik-International Journal for Light and Electron Optics*, Vol.125, No.23, pp.6891-6897, 2014.

[13] H.M. Sim, H. Asmuni, R. Hassan, and R.M. Othman, "Multimodal biometrics: weighted score level fusion based on non-ideal iris and face images", *Expert Systems with Applications*, Vol.41, No.11, pp.5390-5404, 2014.

[14] H. Benaliouche and M. Touahria, "Comparative study of multimodal biometric recognition by fusion of iris and fingerprint", *The Scientific World Journal*, 2014.

[15] S. Yuan, T. Zhang, X. Zhou, X. Liu, and M. Liu, "An optical authentication system based on encryption technique and multimodal biometrics", *Optics & Laser Technology*, Vol.54, pp.120-127, 2013.
[16] B.S. Vidya, and E. Chandra, "Entropy based Local Binary Pattern (ELBP) feature extraction technique of multimodal biometrics as defence mechanism for cloud storage", *Alexandria Engineering Journal*, Vol.58, No.1, pp.103-114, 2019.