Face Biometric Cloud Authentication Access Using Extreme Learning Class Specific Linear Discriminant Regression Classification Method

Author(s): Vishwanath P.[1], Dr. Parveen Kumar[2]
[1]Research Scholar, Department of Electronics and Communication Engineering
[2]Professor, Department of Computer Science and Engineering
NIMS University, Jaipur (Rajasthan), India

Abstract—**The Extreme Learning Class Specific Linear Discriminant Regression Classification used in this proposed system aims at improving the accuracy and recognition rate of the face biometric identification for secured cloud access. The accuracy is improved by maximizing and minimizing the reconstruction error. The between class reconstruction error (BCRE) and within-class reconstruction error (WCRE) are the two values simultaneously increased and decreased for every sample to provide improved accuracy. By selecting the suitable value of WCRE, the learned projection matrix for the discriminant subspace is identified. The class specific representation is implemented for the label created in feature vector to further improve the efficiency of identifying a face. Based on the classification results given by the proposed EL-CSLDRC method, an efficient access of secured data from the big data cloud system is promoted.**

Keywords—**Between Class Reconstruction Error (BCRE); Extreme Learning, Face Recognition System (FRS); Linear Discriminant Regression Classification (LDRC); Within Class Reconstruction Error (WCRE);**

I. INTRODUCTION

Information technology is innovating new ideas day by day to satisfy many technological requirements of the consumers across the globe. Cloud computing is one of the fastest developing technologies in IT during the past decades [1]. This technology allows for much more efficient computing by centralizing data storage, processing and bandwidth. Data protection is an important process in cloud computing as it provides a secured access and transaction of trusted information [2]. One way to protect data from theft is establishing an Authentication system, which is a security measure that helps in protecting application against adoption of any illegal access by creating a separate identity for the user. Biometrics is the most powerful authentication method used for the purpose of scanning and analysis of the biological input that are highly secure than any other modes of security method developed in clouds [3], [4] . The features like finger print, face, iris, voice, and ear are the commonly used biological inputs, in which face feature is considered as the versatile and successful trait in bringing people's identity because of its non-contact process. Face Recognition System (FRS) is a technology that uses the spatial geometry of distinguishing characteristics in a face for providing access control security[5]. However, it experiences many challenges due to the variations such as expression, head movements, ageing, and wrinkles, which are tend to happen in human beings. Thus, it is necessary to improve the efficiency of FRS in biometric authentication [6], [7], which becomes an active research among the researchers.

In FRS, the face images are captured and it is compared with authenticated images stored in the cloud databases for further processing it. Eigen face approach, Neural networks, Fisher face, Support vector machine (SVM) [8], Fuzzy method, Decision trees are the commonly used classification algorithms in face recognition based cloud access[9], [10]. A suitable algorithm is selected from this and classification of face features is provided in our system. In most of the detection methods, the classification process experiences the problem of very limited training samples, which leads to loss of efficient detection. To satisfy this problem, the proposed system is designed in such a way that an Extreme Learning Linear Regression Class Specific Discrimination (EL-LRCSD) access method is introduced in cloud biometric authentication system. The training samples stored in the databases are well analyzed and the incoming input images are learned continuously by Extreme learning machine (ELM) so as to keep track of the users accessing the cloud. Identity management is another major problem found in the design of cloud biometric system, which is also enhanced by establishing a dual cloud based access. The cloud containing big data information is protected by another cloud found inside, which helps in maintaining the authentication level. Thus, the efficiency and performance of secured access is promoted in this system with the help of EL-LRCSD face biometric cloud authentication.

II. LITERATURE REVIEW

C. Zhu et al. [1] proposed a new authenticated trust & reputation calculation & management (ATRCM) system for CC-WSN integration. The proposed ATRCM system succeeded the following three functions: 1) authenticating CSP & SNP to avoid malicious impersonation attacks; 2) calculating & managing trust & reputation regarding the service of CSP & SNP; & 3) helping CSU choose desirable CSP & assisting CSP in selecting appropriate SNP. Additionally, they demonstrated the efficiency of ATRCM, followed with system security analysis.

J. R. Troncoso- Pastoriza et al. [2] presented a private face verification system that can be performed in the server without interaction, working with encrypted feature vectors for both the templates & the probe face. Then they merge two important things: 1) a novel feature model for Gabor coefficient magnitude driving a Lloyd-Max quantizer, used to reduce plain text cardinality with no effect on performance; 2) an addition of a quasi-fully homomorphic encryption able to compute, without interaction, the soft scores of an SVM operating on quantized & encrypted parameters, features & templates. Finally, they assessed the private verification system with regards to time & communication complexity & in verification accuracy in widely known face databases (XM2VTS, FERET, & LFW).

M. Haghighat et al. [3] proposed a k-d tree structure in the core of the searchable encryption. The proposed method was the first cloud-based biometric identification system with a proven zero data disclosure possibility. It permitted various enterprises to execute biometric identification on a single database without revealing any sensitive information. Their test outcomes demonstrated that CloudID performed the identification of clients with high precision & negligible overhead & proven zero data disclosure.

K. S. Wong &M. H. Kim [4] proposed a large-scale cloud architecture to serve for biometric system that enrolls large population. In identification mode of biometric system, a query

template was matched with all stored templates in the database & a match was said to occur with the one with which match-value becomes higher. Additionally, the proposed architecture took care of threat to compromise secured data as they are passed to various nodes. This architecture passed inputs to cloud nodes hiding the identity-holder's information so that stealing the identity data of an individual will not compromise the security of the system.

III. PROPOSED SYSTEM

The secured access to the cloud using biometric face architecture consist of a series of steps like Biometric face acquisition, application of pre-processing, extraction of features, template generation, classification, and biometric cloud engine. In this section, we will discuss the process of biometric face recognition under which a kernel subspace class specific method is used for the classification of face images, followed by the access of cloud methods.

A. Biometric face acquisition:

The face biometric sample is taken from any recognized databases such as Labelled Faces in the Wild (LFC), FERET PolyU face datasets, Olivetti Research lab, Casia nir-vis 2.0, which are considered as the universal library of face databases.

B. Face Recognition using Extreme Learning-Linear Regression Class-Specific Discrimination Method

A class specific discrimination with the help of feature subspace is proposed in this paper, which exploits an extreme learned reference vector with linear data projection. This method aims at the determination of error formed due to data projection as well as the extreme learned class representation that will be subsequently used for the classification.

Let us consider a class i containing N training face images, which is represented as $X_i \in \Re^{M\times N}$, where $\Re^{i}$ is the facial database matrix containing rows and columns in which each column of X_i represents the dimensions of the face image and $1 \le i \ge c$ in which c is the total number of classes.

The input face image from the user is denoted as y, which can be formed according to X_i as

$$y = X_i \alpha_i, \text{ where } 1 \le i \ge c \qquad (1)$$

From eq (1), the α_i is said to be the regression parameter, which can be either represented as $\alpha_i \in \Re^{N\times 1}$. The α_i can be calculated by founding the least square estimation as $\hat{\alpha}_i$ shown in eq (2),

$$\hat{\alpha}_i = \left(X_i^T X_i\right)^{-1} X_i^T y,\ 1 \le i \ge c \qquad (2)$$

The input image y can be reconstructed by applying the least square value in each class as,

$$\hat{y}_i = X_i \hat{\alpha}_i = X_i \left(X_i^T X_i\right)^{-1} X_i^T y = H_i y, 1 \le i \ge c \quad (3)$$

The reconstruction error or variations occurred in each class is given by finding the difference value of $\hat{y}_i$ from y, shown in the eq (4)

$$e_i = \left\| y - \hat{y}_i \right\|_2^2, \ldots. 1 \le i \ge c \qquad (4)$$

Where, e_i is the reconstruction error.

Let us consider a single image j from the training face image sets $X_i \in \Re^{M\times N}$. The presence and absence of each features class i in each sample j can be stored in S binary label vectors, which is given as $s_i \in \Re^{M\times N}$, $1 \le i \ge c$.

Where, $\Re^{M\times N}$ is considered as the feature subspace. The elements are set equal to $s_{ij} = 1$ in the case, where sample j belongs to class i and to $s_{ij} = 0$, otherwise. Let N_{i0} and N_{i1} denote the number of zero and non- zero elements in s_i, respectively. Thus the binary label vector is created in the class i that is shown in eq (5).

Let $X = [X_1, X_2, \ldots, X_c] \in \Re^{M\times N}$ represents the total training image matrix, where m is the dimension of each training face image, N is the number of training face image from class i, where $N = \sum_{i=1}^{c} N_i$.

In addition, Data projection matrix $U \in \Re^{M\times D}$, $D < M$ is calculated by mapping each x_{ij} into the learned subspace as,

$$y_{ij} = U^T x_{ij}, \text{ where } 1 \le j \le N \qquad (5)$$

Then the mapping of the entire training face image matrix for each class is done to derive the Linear Discrimination Function Y_i equation that is shown in eq (6), where U^T is called as the projection matrix for entire set and T denotes the transformation of classes.

$$Y_i = U^T X_i \in \Re^{D\times N} \qquad (6)$$

1) Class-Specific Reference Discriminant Analysis

Let us consider a reference vector μ_i that will be used in order to represent class i, which is obtained by determining the class mean vector for the face images X_i that can be denoted as,

$$\mu_i = \frac{1}{N_{i1}} \sum_{j, s_{ij}=1} X_i \qquad (7)$$

Here s_{ij} denotes the label vector for the image j taken from the class i and N_{i1} is the non- zero element present in the image set.

The Extreme Learning Machine (ELM) algorithm is introduced to create a learning based classification of face biometrics, which can be applied in X_i of eq (7). The ELM is generally implemented by using the Single-Layer Feed forward Neural Networks (SLFN) method, which provides a weight factor to the input sample so as to learn each and every nodes of the input. Let us represent the input sample as that is mapped into the L-dimensional ELM random feature space by adding weights to get the learned output from the sample, which is shown in the eq (8)

$$X_i' = \sum_{j=1}^{N} \beta_j h_j(X_i) = h(X_i)\beta \qquad (8)$$

Where, X_i' is the learned output used to represent the N-dimensional ELM feature space, $\beta = (\beta_1 \ldots . \beta_N)^T$ is the output weight matrix between the hidden nodes and the output nodes, $h(X_i) = [g_1(X_i) \ldots\ldots g_L(X_i)]$ are the learned

hidden node outputs for input X_i and $g_j(X_i)$ is the output of the i th hidden node.

Given N training samples $\{(X_{ij}, t_j)\}_{j=1}^{N}$, the ELM can resolve the learning problem

$$H\beta = T \quad (9)$$

Where, $T = [t_1, ...t_N]^T$ are target labels, and $H = \left[h^T(x_1).....h^T(x_N)\right]^T$.

Then the output weight β is generated by using the Moore-Penrose generalized inverse matrix 3function,

$$\beta = H^{-1}T \quad (10)$$

Where, H^{-1} is the Moore-Penrose inverse of matrix H. The value of β can be detected with the help of above eq (10).

Thus the training images X_i from the class i are learned using the ELM algorithm and the ELM activation function from eq (8) is substituted in eq (7) as,

$$\boldsymbol{\mu_i} = \frac{1}{N_{i1}} \sum_{j, s_{ij}=1} X_i' \quad (11)$$

Where, $X_i = X_i'$, from the ELM method i.e., X_i - training samples and X_i' - is the extreme learned face images. The learned reference vector eq (11) is added in the eq (6) to derive a discrimination function for reference vector,

$$Y_i = U^T \boldsymbol{\mu_i} \in \Re^{D \times N} \quad (12)$$

The samples belonging to class i are as close as possible to the image of μ_i in $\Re^{D \times N}$ and Y_i is the discrimination function. The equation (8) shows the Extreme learned Class-specific Linear Discriminant (EL-CSLDRC) function respectively.

To find an optimal solution for the designed EL-CSLDRC algorithm, it is necessary to maximize the ratio of the Between-Class Reconstruction Error (BCRE) over the Within-Class Reconstruction Error (WCRE), which helps in motivating the EL-CSLDRC for classification. The reconstruction error equation is considered again from eq. (4) $e_i = \|y - \hat{y}_i\|_2^2$.

Then the BCRE and WCRE of the proposed algorithm is given by representing the inter-class and intra-class variances of the training samples with respect to μ_i in $\Re^{M \times N}$, which represents the Linear regressive EL-CSLDRC analysis as well that is shown in eq (13) and (14).

$$BCRE = \frac{1}{N} \sum_{i=1}^{c} \sum_{j=1}^{N} \left\| y_i - \hat{y}_{ij}^{inter} \right\|_2^2 \quad (13)$$

$$WCRE = \frac{1}{N} \sum_{j=1}^{N} \left\| y_i - \hat{y}_{ij}^{intra} \right\|_2^2 \quad (14)$$

Where,the inter and intra- classes are formed by

$$\hat{y}_{ij}^{inter} = Y_{ij}^{inter} \alpha_{ij}^{inter} \quad (15)$$

and

$$\hat{y}_{ij}^{intra} = Y_{ij}^{inter} \alpha_{ij}^{inter} \quad (16)$$

The value Y_{ij}^{inter} represents the Y with Y_i eliminated and the value Y_{ij}^{intra} represents the Y_i with y_{ij} eliminated. The value of α_{ij}^{inter} and α_{ij}^{intra} can be obtained from $\hat{\alpha}_i = \left(X_i^T X_i\right)^{-1} X_i^T y$, $1 \le i \ge c$ which is represented in the least square estimation equation (2). The value of α in the learned subspace is unknown to us until projection matrix is obtained. However, we can calculate $\hat{\alpha}$ in the original space and use $\hat{\alpha}$ as an approximation of α.

Then the projection matrix $U \in \Re^{M \times D}$ can be learned from the minimized equation of inter and intra class variances. According to the relationships between X & Y, CBCRE & WCRE can be rewriter as follows.

$$BCRE = \sum_{i=1}^{c} \sum_{j=1}^{N} \left(x_i - X_{ij}^{inter} \alpha_{ij}^{inter}\right)^T UU^T \left(x_i - X_{ij}^{inter} \alpha_{ij}^{inter}\right) \quad (17)$$

$$WCRE = \sum_{j=1}^{N} \left(x_i - X_{ij}^{intra} \alpha_{ij}^{intra}\right)^T UU^T \left(x_i - X_{ij}^{intra} \alpha_{ij}^{intra}\right) \quad (18)$$

The factor $1/n$ in both the eq of BCRE and WCRE should be eliminated and compressed as it may affect the ratio of the equation, which can be done by adding a trace operator $tr(\cdot)$ and the variables E_b and E_w with an algebraic deduction as,

$$BCRE = tr\left(U^T E_b U\right) \quad (19)$$

$$WCRE = tr\left(U^T E_w U\right) \quad (20)$$

Where

$$E_b = \sum_{i=1}^{c} \sum_{j=1}^{N} \left(x_i - X_{ij}^{inter} \alpha_{ij}^{inter}\right)^T \left(x_i - X_{ij}^{inter} \alpha_{ij}^{inter}\right),$$

$$E_w = \sum_{j=1}^{N} \left(x_i - X_{ij}^{intra} \alpha_{ij}^{intra}\right)^T \left(x_i - X_{ij}^{intra} \alpha_{ij}^{intra}\right)$$

The eq. (19) and (20) shows the simplified form of Linear regression equation in (17) & (18) for the proposed EL-CSLDRC algorithm.

The BCRE and WCRE are further maximized simultaneously by adopting the Maximum Margin Criterion (MMC), which can be denoted as $J(U)$.

$$\max_U J(U) = \max_U (BCRE - WCRE) = \max_U \left(tr\left(U^T (E_b - E_w) U\right)\right) \quad (21)$$

The equation (21) can be solved by finding the largest d eigenvalues and the according eigenvectors as the following

$$(E_b - E_W) u_k = \lambda_k u_k, \; 1 \le k \ge d \quad (22)$$

From eq (22), $\lambda_1 \ge ....\lambda_k .... \ge \lambda_d$ and $U = [u_1 ... u_k ... u_d]$. MMC can solve the small sample size problem (SSSP) where the dimension of the face image is larger than the number of training face images.

The Lagrange multipliers λ_k is optimized by the EL-CSLDRC algorithm as,

$$\lambda_k = \eta_F \lambda_k \; 1 \le k \ge d \quad (23)$$

Where, η_F is considered as the final rate of extreme learning class specific method in eq. (23). Thus the

reconstruction error value e_i is detected (4) with the help of EL-CSLDRC eq. (12) function and it is used for further user accessing purpose of cloud system.

2) Biometric cloud engine

The access of user is enabled based on the determination of minimized error value detection, which is given by e_i. The biometric cloud engine employed in this system consists of a big data cloud protected by another cloud found inside in a hierarchical manner, i.e., the permission to access control is given on a ranking base that only the person having permission id can be allowed into the big data cloud to visit particular data.In addition, it keeps the track of access history as the number of accesses made by a single user and also the reputation created.

The extreme learning method X_i' from eq. (8), involve in managing the track of user history and increases the accuracy of identifying a user on the next access. It iteratively checks the face input using the learned reference vector μ_i shown in eq. (11) and improves the efficiency as well. In addition, the value e_i identifies the fraudulent use of the cloud. Thus, the proposed EL-CSLDRC algorithm helps in improving the authenticated access of any user into the cloud with its extreme learning capability.

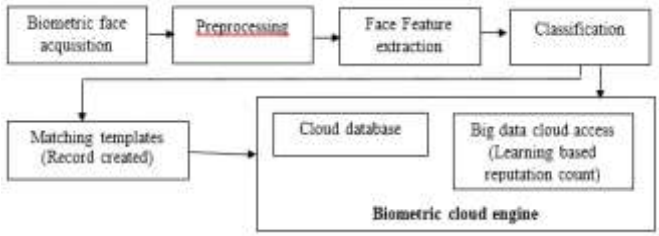

Fig. 1. Architecture of EL-CSLDRC algorithm

The above Fig.1 denotes the entire working procedure or architecture of the proposed EL-CSLDRC algorithm. It represents the module used by the system to provide security for the closed cloud data access. In addition, many experiments and analysis are undertaken to describe the efficiency of this research, which are given below.

IV.

V. Experimental Result and Discussion

The proposed EL-CSLDRC method produce better identification and differentiation of biometric facial images than the other algorithms developed earlier. In addition, it promotes a strong layer to the security of cloud data access with its extreme learning idea.

A. General discussion

The working performance of the proposed EL-CSLDRC is compared with the existing systems, which is necessary to provide conclusion that the proposed system is better than all the other systems.

Linear Regression Classification (LRC) is the early method developed to perform classification of images based on their existence of feature vectors, which calculates the distance between the pixels and reduce the error variations in it. The variation value of the error between pixels is 0.578 and their average recognition rate of this method 0.45 is shown in table.1

To reduce the occurrence of error and variations caused in the pixel, Discriminant factor is introduced in the LRC algorithm. It works by determining the highest and the lowest difference with a consideration of a decision boundary. Thereby it increases the recognition rate as with an average value of 0.63.

TABLE I. Error and Recognition Rate of Classification Methods

Algorithm	Error/ Variation value	Recognition rate	Accuracy
LRC	0.578	0.45	68.4%
LDRC	0.410	0.63	74.9%
WH-LDRC	0.329	0.75	78%
CSRDA	0.210	0.79	80.8%

Learning methods are introduced in the LDRC method to increase the recognition rate and decrease the time consumption. Widrow-Hoff Learning is one among the learning methods developed earlier. It produces the learned output from the input sample and increases the accuracy to 78%, shown in table 1. However, once if the boundary value is reached it stops learning and the value becomes constant.

Class specific classification is the other method used in face recognition process, which provides a class representation of the features in the images. It includes a reference vector and label vector for matching the images.

The proposed system is designed in such a way to improve the accuracy and the recognition rate of the classification process. The Extreme learning method is used to make the output from the projection matrix learned, which creates a new data reference from the input sample if it does not match with the database images. Each and every rows, columns of the projection matrix is checked and matches are taken from it to produce a new matrix data.

Extreme learning in this method is more efficient than the Widrow-Hoff Learning as it continues the learning process even after the boundary level is reached. It changes according to the number of arrival of the new input sample and provides more security to the cloud system. Its accuracy and recognition is rate is comparatively higher than the other systems, which can be proved by considering an example mentioned below.

An experimental verification is done to reveal the performance of EL-CSLDRC, in which it is compared with the other two algorithms Linear Collaborative Discriminant Regression Classification (LCDRC) and Widrow-Hoff Learning Parallel Linear Collaborative Discriminant Regression (WH-PLCDRC) respectively.

B. Experiments on ORL, YALE, Extended YALE B

The suitable facial image samples are taken form the ORL, YALE, Extended YALE B databases and analysis are made. Each image from the database is randomly selected and further proceeded with training and testing to provide conclusion. Using Principal component analysis (PCA), the significant features from the images of above mentioned databases is extracted and the experiment is iterated repeatedly for 10 times for each set of images.

1) ORL Analysis

The ORL Database contains 400 face images of 40 individuals with 10 face images for each subject, from which some face samples are taken for our experiment purpose shown in Fig. 2. The face images were taken under different light conditions & with different facial expressions. All the face images are cropped to be 32x32 in our experiment and

were taken in frontal position with a tolerance for face rotation a tilting up to 20◦.

Fig. 2. ORL Face Data

MMC is used both in LDRC & LCDRC such that the performance difference comes from BCRE & CBCRE. PCA is implemented before evaluating the proposed and the two existing algorithms.

The accuracy of EL-CSLDRC is comparatively shown with respect to LCDRC and WH-PLCDRC in a graphical representation. Fig. 3,and 4 shows the performance variation of the proposed with the other two methods given two, & four for each class. A comparative analysis of all the graphs represents that EL-CSLDRC curve is rising slowly to produce more performance accuracy in Fig. 3,and 4.

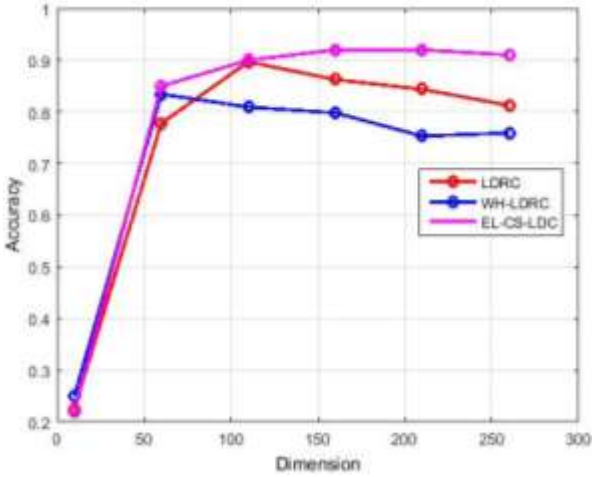

Fig. 3. Two Train ORL Database Accuracy

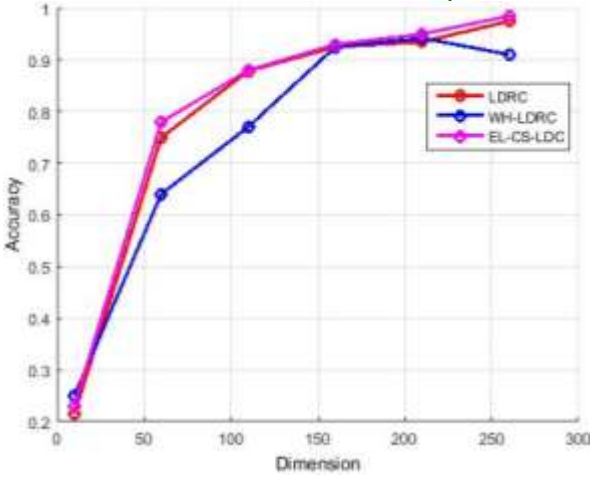

Fig. 4. Four Train ORL Database Accuracy

Each images are tested with the help of BCRE and WCRE evaluation results and the calculation made from learned output. It is noted that the performance of Extreme learned algorithm accounts for 82% in ORL face datasets, which is comparatively higher than the LCDRC and WH-PLCDRC. The calculation and deduction time is also reduced due to the addition of learned face data inputs.

2) YALE Analysis

The second experiment is made in the YALE face datasets Fig. 5. The YALE face database is another widely used database for face recognition contains 165 faces of 15 individuals. For each individual, there are 11 images under different facial expressions or configurations. There are 11 images per subject, one per different facial expression or configuration: center-light, w/glasses, happy, left-light, w/no glasses, normal, right-light, sad, and sleepy, surprised, and wink. All of the face images are cropped into a size of 32x32.

The performance comparison of the methods EL-CSLDRC, LCDRC, WH-PLCDRC in YALE face datasets are mentioned in Fig. 6,and 7. By analyzing the graphical notation, EL-CSLDRC has a much higher classification accuracy than the other method.

Fig. 5. ORL Face Data

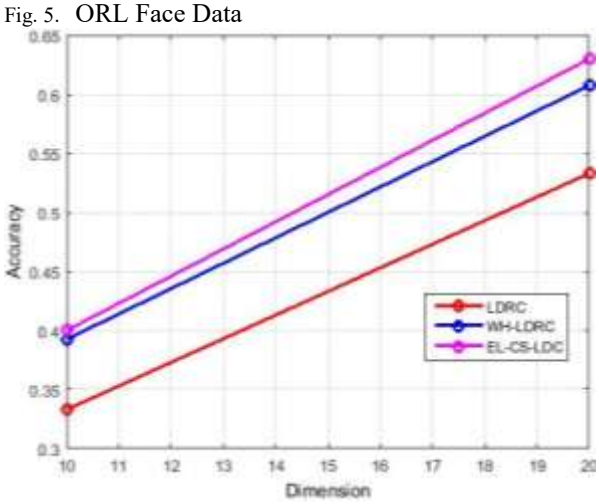

Fig. 6. Two Train YALE Database Accuracy

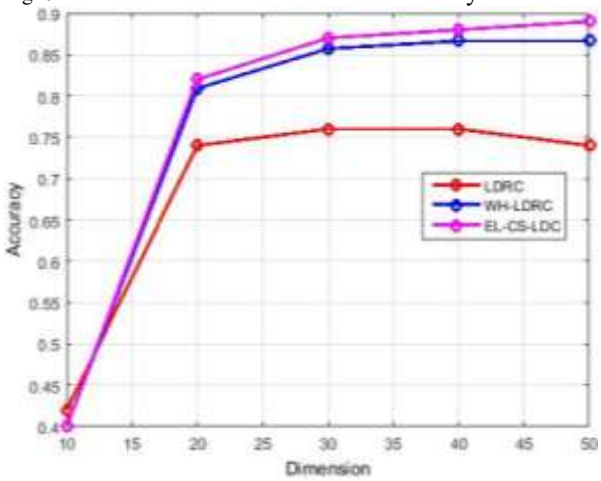

Fig. 7. Four Train YALE Database Accuracy

The above Figures 6,and 7 shows that proposed EL-CSLDRC performs well in the YALE B face database also.

The best recognition rates & the corresponding feature dimensions of CRC, SRC, LRC, LDRC, LCDRC, WH-PLCDRC and EL-CSLDRC given four training face images for each class are 70.86%, 69.24%, 61.62%, 66.48%, 77:05%, 86.6%, & 89.8%. Thus, it is seen that 89.8% accuracy is achieved on YALE B face datasets by using the proposed algorithm.

3) Extended YALE-B Analysis

The Extended YALE_B face database contains 16128 faces of 11 individuals. For each individual, there are 10 images under different facial expressions or configurations. It consists of facial images depicting 38 persons in nine poses under 64 illumination conditions. In our experiments, we have used the frontal cropped images provided by the database, in which all of the face images are cropped into a size of 32x32.

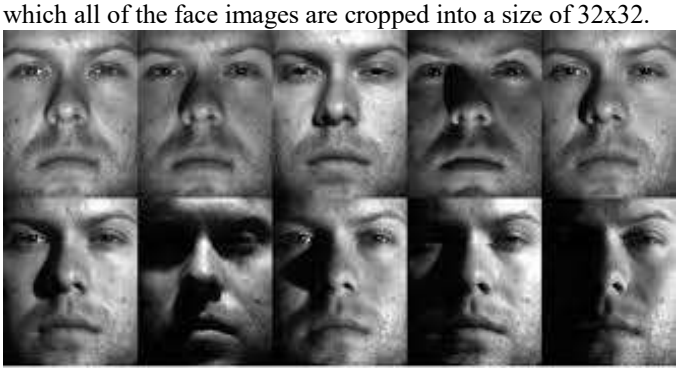

Fig. 8. Extended YALE-B Face Data

The Figures 9, and10 shows the graphical notation of variations between the compared algorithms mentioned earlier. Number of iterations are performed and results are analyzed to identify the accuracy strategy.

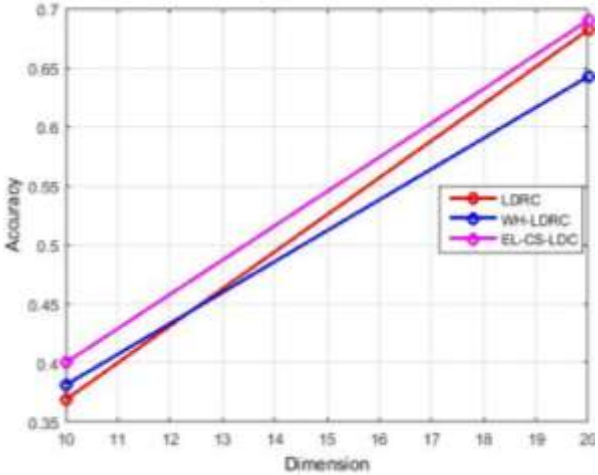

Fig. 9. Two Train Extended Yale-B Database Accuracy

The performance comparison of different methods is shown in Fig.9, and10. Comparatively EL-LRCSD has a much higher classification accuracy than the other method. For example, the best recognition rates & the corresponding feature dimensions of LCDRC, WH-PLCDRC, and EL-CSLDRC given four training face images for each class are 85.45%, 88.70%, 90.3% respectively.

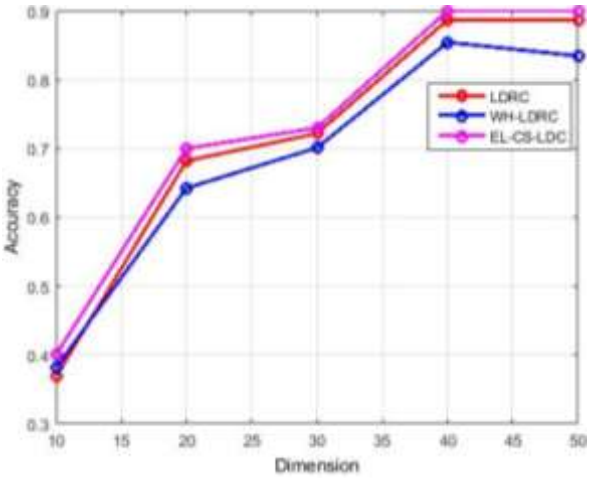

Fig. 10. Four Train Extended Yale-B Database Accuracy

The average accuracy gained in all the experiments with two and three training image data is compared and accuracy of performance in each the algorithm is listed in the table. 2 as listed below.

TABLE II. PERFORMANCE EVOLUTION TABLE

Algorithm	Database	Two training	Four training
		Accuracy	*Accuracy*
Proposed EL-CSLDRC	ORL	0.9011	0.9901
	YALE	0.6954	0.9881
	YALE-B	0.7196	0.9005
WH-PLCDRC	ORL	0.8968	0.9650
	YALE	0.5333	0.8666
	YALE-B	0.6820	0.8870
LCDRC	ORL	0.8343	0.9421
	YALE	0.3925	0.7603
	YALE-B	0.6425	0.8545

From Ttable. 2, it is clearly visible that compared to the other two methods, the value of accuracy gained in EL-CSLDRC is more. The two trained average accuracy of ORL, YALE B, and Extended YALE B are 0.9011, 0.6954 and 0.7196, where the four trained average accuracy are 0.9901, 0.9881, and 0.9005 respectively. In every experiment, the value remains increased than the LCDRC and WH-PLCDRC. The extreme learned input makes the identification and matching process of face images to increase and provides better results than the earlier algorithms

VI. CONCLUSION

The main focus of the proposed Extreme learning linear regression class specific discriminant analysis work is on motivation of the accuracy and performance for authenticating a big data cloud access with biometric face recognition. The experimental results on three types of databases discussed above reveals that EL-CSLDRC performs well in all the conditions by its extreme learning capability. It also minimizes WCRE and maximizes BCRE automatically to a great extent and provides an optimal extreme learned projection matrix. Thus, the proposed EL-CSLDRC face biometric algorithm secures the cloud from unauthorized entry in a hierarchical manner and protects the data found in it.

REFERENCES

[1] C. Zhu, H. Nicanfar, V.C. Leung, and L.T. Yang, "An authenticated trust and reputation calculation and management system for cloud and sensor networks integration," IEEE Transactions on Information Forensics and Security, vol. 10, pp. 118-131, 2015.

[2] J.R. Troncoso-Pastoriza, D. González-Jiménez, and F. Pérez-González, "Fully private noninteractive face verification," IEEE Transactions on Information Forensics and Security, vol. 8, pp.1101-1114, 2013.
[3] M. Haghighat, S. Zonouz, and M. Abdel-Mottaleb, "CloudID: trustworthy cloud-based and cross-enterprise biometric identification," Expert Systems with Applications, vol. 42, pp.7905-7916, 2015.
[4] K.S. Wong, and M.H. Kim, "Secure Biometric-Based Authentication for Cloud Computing," In International Conference on Cloud Computing and Services Science, vol. 28, pp. 86-101, 2012.
[5] M. Ahmed, and M.A. Hossain, "Cloud computing and security issues in the cloud," International Journal of Network Security & Its Applications, vol. 6, pp.25, 2014.
[6] M.A. Sharkh, A. Kanso, A. Shami, and P. Öhlén, "Building a Cloud on Earth: A Study of Cloud Computing Data Center Simulators," Computer Network, July 2016.
[7] E. Sasi, R.S.Priyadharshini, "Secured biometric authentication in cloud sharing system," International Journal of Computer Science and Mobile Computing, vol.4,pp. 572-577, March 2015.
[8] D.Pugazhenthi, B.Sree Vidya, "Multiple Biometric Security in Cloud Computing," International Journal of Advanced Research in Computer Science and Software Engineering, vol.3, April 2013.
[9] A.A. Pawle, and V.P. Pawar, "Face recognition system (FRS) on cloud computing for user authentication," International Journal of Soft Computing and Engineering (IJSCE), vol. 3, 2013.
[10] S. Deepak and S. Goutham N, "Face Recognition using Cloud Based Security in MobileDevices," International Journal of Innovative Research in Computer and CommunicationEngineering, vol. 3, June 2015.
[11] S.M.Huang, and J.F. Yang, "Linear discriminant regression classification for face recognition," IEEE Signal Processing Letters, vol. 20, pp.91-94, 2013.
[12] L. Kumar, and S. Bharti, "Analysis of Classification Techniques based on SVM forFace Recognition," Journal of Advanced Computing and Communication Technologies,vol. 1, August 2013.
[13] Hemalatha, G., and C. P. Sumathi, "A study oftechniques for facial detection and expression classification," International Journal ofComputer Science and Engineering Survey,vol. 5, April 2014.
[14] M.A. Rabbani, and C. Chellappan, "A Different Approach to Appearance–based Statistical Method for Face Recognition Using Median," International Journal of Computer Science and Network Security, vol. 7, pp.262-267, 2007.