

# Privacy preserving security using biometrics in cloud computing

Santosh Kumar<sup>1</sup> · Sanjay Kumar Singh<sup>2</sup> ·  
Amit Kumar Singh<sup>3</sup> · Shrikant Tiwari<sup>4</sup> ·  
Ravi Shankar Singh<sup>2</sup>

Received: 26 February 2017 / Revised: 23 April 2017 / Accepted: 19 June 2017 /

Published online: 22 July 2017

© Springer Science+Business Media, LLC 2017

**Abstract** Cloud computing and the efficient storage provide new paradigms and approaches designed at efficiently utilization of resources through computation and many alternatives to guarantee the privacy preservation of individual user. It also ensures the integrity of stored cloud data, and processing of stored data in the various data centers. However, to provide better protection and management of sensitive information (data) are big challenge to maintain the confidentiality and integrity of data in the cloud computation. Thus, there is an urgent need for storing and processing the data in the cloud environment without any information leakage. The sensitive data require the storing and processing mechanism and techniques to assurance the privacy preservation of individual user, to maintain the data integrity, and preserve confidentiality. Face recognition has recently

---

✉ Amit Kumar Singh  
amit\_245singh@yahoo.com

Santosh Kumar  
santosh@iitnr.edu.in

Sanjay Kumar Singh  
sks.cse@iitbhu.ac.in

Shrikant Tiwari  
shrikanttiwari15@gmail.com

Ravi Shankar Singh  
ravi.cse@iitbhu.ac.in

<sup>1</sup> Computer Science & Engineering (CSE), IIIT Naya Raipur, Chhattisgarh, India

<sup>2</sup> Department of Computer Science and Engineering, Indian Institute of Technology (B.H.U), Varanasi, India

<sup>3</sup> Department of Computer Science and Engineering, Jaypee University of Information Technology, Wagnaghat, Solan, Himachal Pradesh, India

<sup>4</sup> Department of Computer Science and Engineering, Shri Shankaracharya Group of Institutions (SSGI), Durg, Chattisgrah, India

achieved advancements in the unobtrusive recognition of individuals to maintain the privacy-preservation in the cloud computing. This paper emphasizes on cloud security and privacy issues and provides the solution using biometric face recognition. We propose a biometrics face recognition approach for security and privacy preservation of cloud users during their access to cloud resources. The proposed approach has three steps: (1) acquisition of face images (2) preprocessing and extraction of facial feature (3) recognition of individual using encrypted biometric feature. The experimental results establish that our proposed recognition approach can ensure the privacy and security of biometrics data.

**Keywords** Cloud computing · Security · Privacy Preservation · Face recognition · Biometrics identification · Encrypted Biometrics · Elliptical encryption

## 1 Introduction

Recently, biometrics-based recognition systems have gained proliferation and more attention due to its inherent advantages. It efficiently provides the privacy preservation of cloud user and security of stored more sensitive data in the cloud servers [24]. Thus, the recent research trend is emphasized towards addressing the issues of preservation of user's privacy, data integrity and management of growth of cloud data. Along with the privacy preservation of users, processing and maintain the data integrity, biometrics based recognition system retrieval has played an vital role to maintain the data in the cloud computing. The advanced and efficient algorithms for privacy-preservation and the security of biometric information, biometrics-based recognition systems have been studied and applied for the past few decades [23, 24]. These recognition systems cater the user authentication by verifying individual. In verification process, biometric features of individual user is matched with stored biometric template database using similarity matching techniques. Biometric characteristics are mainly categorized into two groups (1) physiological biometric characteristics and (2) Behavioral biometrics characteristics. The physiological biometrics based characteristics are the face, fingerprint, hand geometry, DNA, and iris. The human gait, signature, and voice are known as behavioral biometric characteristics. These biometrics characteristics are immutable, distinctive and measurable for the verification and identification of individuals [22]. The major advantages of biometrics over traditional authentication systems (e.g., passwords, and token based systems) are (1) higher level of security of stored data (2) privacy preservation of users (3) diminutive chances of forgery and (4) cost-effective based solutions and (5) user friendliness [22, 23].

According to the paper [49], smart device users (e.g., smart phones) prefer only biometrics-based authentication mechanism as an alternative solution for the passwords and token based systems. The reason behind that the biometrics-based authentication solutions are more reliable. Therefore, biometrics-based recognition systems provide a high level of security. Biometric data are unique and irrevocable, unlike passwords. The recognition process in the biometric system performed by comparison between the tests (query) biometric features with enrolled biometric templates of individual from the stored database. Therefore, biometrics-based recognition systems are more suitable for storing the biometric features of all the cloud users (subjects). The stored cloud biometrics data were utilized at the time of recognition and verification (e.g., query biometrics features) of an individual in the cloud [17].

As the number of subjects increases, the biometrics-based recognition systems need more storage capacity and processing power to advance the user privacy by face recognition efficiently [15]. Also, for the authentication of cloud users, all the stored biometrics databases are also accessible and

monitored and observed by all private enterprises or organizations. Who can access the sensitive data? The needs of were high processing capacities which are motivated the use of a cloud-based biometric recognition system. The system maintains the confidentiality and integrity of stored biometrics database and processes the data. The protection of sensitive data (biometric data, and other data) and to maintain the privacy-preservation of users are the biggest problems for authentication of users in the cloud computing [6]. These challenging issues need to be considered at every phase of system design and development. The swelling popularity of cloud computing technologies has heightened the necessity of solving these significant problems [6, 15, 39].

In the case of user authentication, the stored biometric data is pre-processed and matched with a stored biometric template database in the cloud servers. In the cloud computing, the risks of identity theft, forgery, and duplication of sensitive data, and to breach the integrity and authentication of users are involved, because stored data can be stolen, and misused during user enrollment [39]. The major advantage of biometric data is that users cannot duplicate or forge the biometric data of enrolled users.

Consequently, biometrics-based recognition systems can guarantee the privacy-preservation and security of individual users by encryption of biometric data [38, 39, 44]. Therefore, the stored biometric database needs to be encrypted for better privacy preservation and security of an individual's biometrics information in the cloud. Biometrics-based recognition of cloud users is a reliable and convenient approach [38]. Comprehensive propagation of biometrics-based recognition presents a robust privacy protection and security of sensitive information (data) beside possible misuse, information loss and leakage or theft of stored biometric data of individuals in the cloud computing. The security in the cloud using biometrics plays a vital role to solve the important, challenging problems of privacy-preservation and safety of biometrics data [38, 44].

In this paper, a novel privacy-preservation biometrics-based recognition system is proposed for cloud computing. In the proposed recognition system, the captured biometric features of cloud user are initially encrypted and outsourced. The encrypted biometric data is applied for authentication of cloud users during identification and verification for accessing the cloud resources and system resources. Here, the database administrators or managers of cloud generate a credential for the candidate biometric characteristics and present it to the cloud for identification.

In this paper, biometric facial feature of individuals is used as key attributes to access the resources of cloud by matching and recognizing the users in the cloud database. The identification is performed on the encrypted data by the cloud servers and returns the matching scores as a result for authentication of owners. The stored data consists of individual records. The storage of personal record as database provides the adequate foundation to build the encrypted biometric database. During preparation of personal records like higher academic details, complete name, date of birth (DOB), address, bank detail, insurance records and their unique identification numbers (e.g., employee id or family number and Aadhar ID), are consolidated in the cloud biometric database. These personal details are required during verification of the individual to keep the preservation of user privacy in the cloud database.

In order to prevent eavesdroppers and unauthorized access of resources, the query (test) data of users are matched with stored biometric templates database without any decryption of the biometric data. Variations in the captured biometric data due to illumination and poor image quality play a major problem during the encryption process. Therefore, small modifications in the plaintext (e.g., biometric data) may affect the experimental results during the matching process. Therefore, these differences in the cipher text (encrypted biometric data) of cloud user produces the false rejection rate during authentication [7]. These recognition systems can suffer due to a massive number of false matches with the stored biometrics template database during similarity matching in the recognition

process. The immense rate of false acceptance and false rejection mislead the attention [44, 50]. On the ground that, the addition of biometric encryption paradigms is inadvisable to the recognition system and anticipate bringing the more accurate performance measurement based results on the secure data that are accomplished without the encryption [17] [16] [28].

Encryption algorithm achieves the computation of biometric features for individual authentication. The biometric-based recognition system initially transfers the captured face image of individual to the servers in the cloud computing. The authentication of the individual user is done under the encrypted conditions and obtained the matching scores (value) results from captured encrypted biometric data [7, 50]. In this research work, biometric templates are generated and encrypted using Paillier encryption algorithm and Eigen-face encoding algorithm. Therefore, cloud computing systems have not granted to access to the biometric information of individuals because cloud systems have no intelligence to know about the encrypted stored real biometrics data (face image data). Moreover, cloud systems do not retrieve information from the stored face templates, ensuring no leakage of user privacy data.

The remaining paper is organized as follows. Section 2 illustrates the related work. Section 3 presents the proposed biometrics-based recognition system. Section 4 illustrates the privacy-preservation, encoding mechanism of biometric features and security of individual cloud user using the Eigen faces recognition and encryption algorithms which operate on encrypted face images. Section 5 demonstrates the encryption process of extracted biometric features and key generation. Section 6 illustrates the experimental results and detail analysis, and finally, Section 7 illustrates conclusions and future directions.

## 2 Related work

A cloud computing based solutions are effective to provide the computation of data and storage solutions to cloud users. In the available literature, the study of user privacy using biometric based techniques is reviewed in the two parts [50]. In the first part, it performs the privacy-preservation of users by executing the various queries in the system during execution time.

Based on the results of accomplishing several queries, the systems employ the security mechanism for maintaining the confidentiality of stored sensitive data and security of clients [7, 50]. The achieved biometric data of users are stored at the cloud server side. The stored biometric data are considered to be very trustworthy, and confidential data from stored biometric data which is not needed to be encrypted [31, 34, 56]. Hence, cloud users are authenticated and access the cloud resources by using their biometrics-based identity and authorized to store biometric data by fascinating advantages of critical vulnerabilities. These vulnerabilities accommodate the lack of access control, information leakage, data loss, and security breaches [31, 34] [3, 29, 53, 54].

Furthermore, the authenticated cloud, enterprises have the full privilege to store and process by accessing the original contents of the stored biometric database. For storing data, all cloud computing based solutions and methods are incompetent to process the stored information on the cloud servers. Privacy-preserving based biometric systems are proposed for maintaining the data integrity and confidentiality of stored biometric data using public key encryption techniques [31].

In works as mentioned earlier [8, 11, 42], the cloud servers are inadequate in the learning of either the stored biometric information of clients or the stored query result in the cloud servers. The cloud users were always unable to retrieve the discriminatory or different contents of

biometric face images without using traditional identification approaches (such as token-based identification, password based identification and other manual based authentication mechanism). Algorithms, as mentioned above [42], are not applicable for trusted servers. In this research work, the proposed methods considered the assumptions which are pretty same, but different from above mentioned standard protocols and algorithms.

In a case of other studies, the cloud servers have not the full privilege to access the stored biometric face image database. The stored database is encrypted using different encryption techniques [8, 11]. However, the second set of studies based algorithms have significant issues and suffer from the leakage of biometric information, unauthorized access to data, and security holes [2, 9, 10]. In [14], the author studied the major privacy preservation problems and introduced a biometric authentication based framework for guaranteeing the privacy-preserving of cloud users. Similarly, in [45, 46], the authors proposed a framework to advance the privacy-preservation of several cloud users using biometric characteristics in the cloud computing. The proposed system achieved the recognition of various face images based on the well-known Eigen faces algorithms [55].

In [33], Paillier intended an authentication system for the authentication of cloud users using cryptosystem public-key-encryption scheme. The encryption techniques complete the encoding of stored biometric features of individuals. In the proposed system, they consolidated the Paillier encryption methodology for the encryption process of biometric face features. The Euclidean distance method is used to compute the similarity matching scores (values) between test (query) face template and stored face template database. The similarity matching based algorithms are executed to compute the similarity scores between the query face images and stored face template database. Later, in [5], author Barney advanced biometric-based recognition system for the matching of minutiae points of human fingerprint recognition, known as Finger-Codes for protecting the privacy-preservation of cloud users in the cloud computing. In both protocols, the homomorphic encryption, the public encryption scheme is involved [5, 57]. But the major shortcoming is that authentication system consumes more time to encode the extracted features and transferring the encrypted templates to the cloud server during verification and identification steps in the cloud computing.

Sadeghi et al. [37] proposed the recognition framework for the authentication of cloud user. They have improved the efficiency of proposed systems using biometric authentication techniques and encryption methodologies for the encryption of generated templates. In the similar direction, Huang et al. [56, 58] suggested the cloud authentication system by incorporating the previous algorithms proposed in [19, 51]. The authors have provided the better paradigm to compute the resources and improved the efficacy of proposed cloud biometric systems by reducing the computation and processing of large stored data in the cloud database. The proposed cloud authenticated system in [40, 41, 58] [18, 27, 54] performs the individual identification by determining the closest match of selected biometric features.

In [21, 25], the authors recommended a cloud framework for the authentication of cloud users. The proposed cloud systems obtain the required information for the identification of cloud users by extracting the biometric and personal information. This information is saved in a designed circuit for receiving and retrieving the data quickly. The proposed system performs the computation to measure the similarity match scores. In [30], the authors proposed a biometrics-based recognition for the preservation of user information. The proposed system extracts the features from the iris codes of cloud users. During authentication, the proposed system performs the verification of individuals for preserving privacy-preservation of stored biometrics template database in the clouds [30]. In [1], the authors proposed an algorithm for protecting the privacy-preservation of users and security of biometric data using the

mathematical simulation based algorithms. The likelihood measure of the occurrence of biometric information in the multiple forms of the same information and analyzed the information leakage to maintain the privacy preservation of cloud users [35].

Recently, the biggest problem of privacy-preservation of user and security of cloud is proposed and deployed by different multidisciplinary researchers [13]. To solve these problems, researchers have utilized the efficient data searching, retrieving the information and processing techniques using the hashing function. The main advantage of the hashing function is to alleviate the redundancy of information in the extensive database by exploring few candidates [12, 30, 32] [52].

### 3 Proposed system

The proposed biometrics-based recognition system is illustrated in detail for cloud security and user privacy preservation of user by using face recognition of the individual user, shown in Fig. 1. The recognition system consists of two phases: (1) training phase, and (2) testing phase. During the training phase of the system, the recognition system creates the database by the acquisition of individual face images. The face images are stored in the cloud biometric database. In the testing phase, it recognizes the individual based on the test (query) facial images by matching the similarity scores of facial features of the test images, stored in the biometric template database.

In the proposed system, following steps are illustrated as follows:

#### 3.1 Acquisition of biometrics data

The first stage of the proposed recognition system is data acquisition. In the data acquisition, the face images of the individual user are achieved by sensors (e.g., camera). Before image capturing, the face images are detected and localized the face area as the region of interest using a face detection algorithm. The proposed system uses the Viola-Jones algorithms for the face detection [43, 48] (shown in Fig. 2).

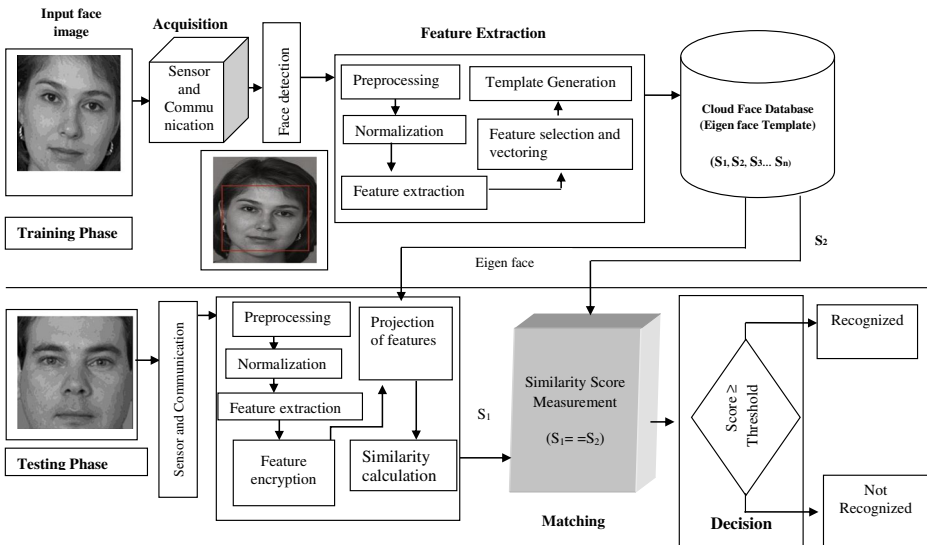


Fig. 1 Illustrates the proposed recognition system



**Fig. 2** Illustrates the detection of individual face

### 3.2 Pre-processing and normalization

The pre-processing and normalization is necessary steps for feature extraction and matching of face images. The proposed biometric recognition system originally detects the important regions in the captured face images for discriminatory features [24, 37, 45]. The corresponding regions are taken into consideration for noise reduction and conversion into grayscale images after enhancement of face images by using Contrast Limited Adaptive Histogram Equalization (CLAHE) image processing technique. The original face image is cropped and resized to  $200 \times 200$  pixels for the actual representation of the facial region.

### 3.3 Feature extraction

In this subsection, proposed system is applied for the extraction of features (e.g., pixel intensity values) from the cropped and grayscale face images [23, 33, 45]. The extracted features are transformed into the feature vectors and by applying to convert into the 2-D face image to one-dimensional feature vector matrix for better representation in the feature space, denoted as ( $\Gamma$ ). The unique face templates are generated with facial feature vectors. These facial templates are chosen for the matching of the individual by commutating the similarity scores of query test face images from the stored cloud face database [46].

### 3.4 Computation and selection of biometrics features

In this subsection, the demonstration of face-subspace and the matching of the test (query) face templates with stored biometric template database are demonstrated in detail. The proposed recognition system selects face images of different for computation of biometric facial features and matching. Then the system applies the Eigenface recognition method for the feature extraction and representation of facial images in the face subspace [22, 46].

For the computations of Eigenface values (e.g., maximum variance based pixel intensity feature), we have employed the statistical feature extraction approach known as, principal component analysis [45]. The extracted facial feature matrix is denoted as ( $X$ ). The feature matrix consists of individual face vectors [46]. The Eigenvector matrix is computed from the obtained sets of feature matrix. The feature sets of Eigenvectors are illustrated as the matrix column ( $k$ ) which is denoted as ( $M_1 \dots \dots \dots M_n$ ). The computation of Eigenvector is illustrated as



follows: The matrix ( $W_i$ ) is the collection of the column ( $k$ ) feature vector of the subject ( $i$ ) which is denoted as ( $\mu_k$ ). The mean value ( $\mu$ ) is average value of all mean face images ( $\mu = [\mu_1, \mu_2, \dots \mu_n]$ ).

The projection coefficient of each facial template  $M_i$  is calculated as follows:

$$y = W^T(X - \mu).$$

The projection coefficient of feature matrix is represented as  $\Omega_i = \{w_{i1}, w_{i2} \dots \dots w_{in}\}$ . The matrix of feature vectors ( $W$ ) and the projection coefficients of each facial template ( $\Omega_i$ ) are applied for the recognition of the individual in feature space. In order to ensure the matching and recognition of the individual, the mean face is calculated from the captured face database. The mean face is denoted by ( $\mu$ ). The computation of mean face is shown as follows [43, 45–47]:

$$\mu = \frac{1}{M} \sum_{i=1}^N (M_i)$$

Where ( $i = 1, 2, 3, 4, 5, 6, \dots N$ ).  $N$  is defined as the number of face images of cloud users in the database. The user privacy is preserved based on extracted features and selection of optimal features from biometric face database. The privacy preservation based on selected features is illustrated in the Algorithm 1.

---

**Algorithm 1:** Feature Selection for Privacy-Preservation of User

---

**Begin procedure:**

**Initialize:** Initialize the input ( $X_n, Y_n, S_n$ ) $_{n=1}^K$  for the selection of features, define a threshold ( $\Lambda$ ), total number of iterations ( $T$ )

**Computed Output:** Define the classifier function  $G(x)$ . The  $G(x)$  selects the defined weights ( $W_n^* = \frac{1}{K}$ ) where  $n$  is number of subjects, ( $n = 1, 2, 3, 4, 5, 6, \dots K$ )

Classifier  $G(x) = 0, l = \phi$

Repeat for  $h = 1, 2, \dots T$

Set working index set:

$$J = l \cup \{j \mid s_j + \sum_{i=l} s_i < \Lambda\}$$

Repeat  $j \in J$

**Fit a regression stump:**

$$g_j((X_j)) \equiv a_j(X(j) > (\theta_j + b_j)) \quad g_j(X(j)) \equiv a_j(X(j) > (\theta_j + b_j)) \text{ to the } j\text{th feature, } X(j)$$

**Error computation ( $e_j$ ):**

$$e_j = \frac{\sum_{n=1}^K W_n^* (y_n - (a_j(X_n(j) > \theta_j) + b_j))}{\sum_{n=1}^K W_n^*}$$

Set  $f_j = G_i$  where  $e_i < e_j \forall j \in J$

**Update:**

$$G(x) = G(x) + f_j(X)$$

$$W_n^* \leftarrow W_n^* \times e^{-y_n f_j(X_n)} + f_j(X)$$

$$l \leftarrow l \cup \{j\}$$

**End procedure**

---

### 3.5 Matching and recognition of facial feature

The recognition of individual user is accomplished by using similarity matching of query face image with stored face stored image server in the cloud using similarity matching step [4, 20]. The cloud system (B) takes the captured face image of cloud users. After that, facial templates are generated from the selected unique features of extracted set of facial features. Then, the facial templates are encrypted in the encrypted domain using elliptical encryption and Paillier encryption techniques. The encrypted test facial templates are matched with stored template



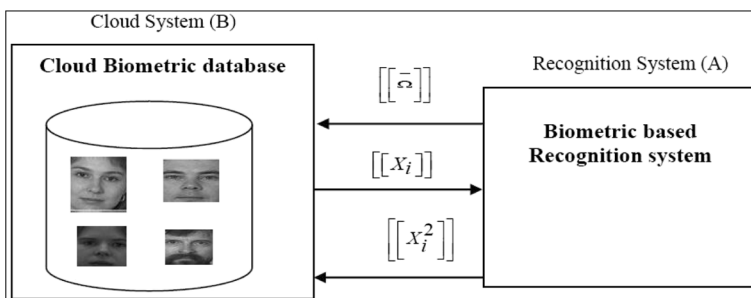
using similarity matching techniques [33]. In addition, for providing the security and integrity of biometric feature in the cloud computing, the extracted features are further encrypted using Elliptic encryption algorithms. The complete procedures are illustrated in Fig. 3. The double encryption mechanism first uses the Paillier encryption algorithm [4, 33, 47] to encrypt the extracted features (pixel intensity values) of gray face images ( $\bar{\Omega}$ ). The encrypted features of facial images are matched with a stored database using distance metric based learning technique in the cloud system (B). After that, cloud system (B) performs the encryption for encrypted face templates by using Elliptic encryption algorithm [20]. The double encrypted biometric template (features) is denoted by  $[[X]]$ . The double encrypted templates are sent to the biometrics-based recognition system (A). The biometrics-based recognition system first decodes the encrypted input feature matrix ( $X_i$ ) where  $(n = 1, 2, 3, 4, 5, 6, \dots, M)$  for the recognition of individual user in the cloud server.

#### 4 Computation and representation of facial features

In the proposed recognition system, privacy preservation of users and security of cloud data are preserved based on biometric features of different face images. The features of face images are extracted by applying the Eigen faces recognition algorithm in this research work [45, 46]. The proposed biometrics-based recognition system maintained the preservation of user's privacy by performing the identification of individuals based on encrypted biometric templates of face images.

The privacy-preservation of cloud users is performed between two parties (and) settings. The semi-attacker model is considered for the checking and verifying the user privacy. Furthermore, two parties completed the required privilege in the standard protocol and followed it properly [33, 47]. They have performed the mechanism to store the necessary information in the cloud server database and keep a record log database of received and transferred information (facial images) or message during transmission process from vice versa. Besides, efficient algorithms are applied to learning the system for the discriminatory data as possible from them.

Let us consider two parties P and Q for the model. The parties mutually perform the biometrics-based recognition of individuals in the proposed system. Firstly, Q selects the setup of proposed biometrics-based recognition system by performing the individual data acquisition process [37]. The captured face images (information) are stored in the biometric face database. The basis facial feature vectors  $[\Gamma_1, \Gamma_2, \Gamma_3, \dots, \Gamma_K]$  from the facial images are generated and stored in the metrics and test feature vectors  $[\Omega_1, \Omega_2, \Omega_3, \dots, \Omega_K]$  of the face are to be recognized



**Fig. 3** Illustrates the double encryption mechanism for encryption of biometric templates

in the feature space. The feature space is represented by Eigenfaces [45, 46]. The features are transformed into one-dimensional (1-D) features vector for better representation in the feature space. These feature vectors consist of integer values (pixel intensity values). The pixel intensity values are obtained from the transformation of multidimensional facial image data into one-dimensional (1-D) data to find the maximum variance and to mitigate the standard deviation between intra-class and inter classes of sample data [45]. The conversion of feature vectors into integers is required for getting the encrypted facial image template using public-key encryption algorithm. The complete process of matching and recognition are given in brief in the next subsections:

#### 4.1 Linear projection of extracted facial features

The extracted facial features are a high-dimensional original data using linear projection technique such as Principal Component Analysis (PCA). Therefore, proposed recognition system performs the data reduction (dimensionality reduction) from the large data sets (more than 2-D) into a small dimensional subspace (feature subspace) [33, 37, 46]. After that, the projection coefficients of original face images are calculated from the low-dimensional feature sets [45]. The PCA performs the statistical computation on the extracted set of facial features by selecting the maximum variance set of features. After that, the eigenvectors are taken from the covariance matrix of the probability distribution of facial features over the high dimensional feature space of face images. In this research work, we have selected the Eigenvectors for the construction of Eigenface of individual cloud users by appropriately decreasing the statistical complexity in face image representation. The computation coefficients and average face value are illustrated as follows:

$$\text{Averageface}(\varphi) = (\Gamma - \psi)$$

$$\begin{bmatrix} \Gamma_1 - \psi_1 \\ \Gamma_2 - \psi_2 \\ \dots \\ \dots \\ \Gamma_N - \psi_N \end{bmatrix}$$

The face image database is denoted as  $(\Gamma)$ . The projection of extracted face features into low dimensional feature subspace is illustrated as follows:

$$\bar{\Omega} = W^T \phi$$

Where,  $\bar{\Omega} = [\varpi_1, \varpi_2, \dots, \varpi_M]$  and  $\varpi = [\mu_i^T \times \varphi = \varphi_1 \cdot \mu_{i1} + \varphi_1 \cdot \mu_{i2} \dots \dots \varphi_N \cdot \mu_{iN}]$   $\varpi$  is computed as the set of coefficient in the feature space. To maintain the user-privacy, the computation of coefficients for facial projection is performed into the encrypted domain using a Paillier

encryption algorithm [33, 43]. It performs an additively homomorphic process for the better security of biometric data [33, 46]. The computation is shown in the Equations ((1) - (3)) as follows:

$$Averageface(\varphi) = (\Gamma - \psi) \begin{bmatrix} \Gamma_1 - \psi_1 \\ \Gamma_2 - \psi_2 \\ \dots \\ \dots \\ \Gamma_N - \psi_N \end{bmatrix} \tag{1}$$

The calculation of coefficient of facial images in the cloud system of (B) is as follows:

$$[\varpi i] = [\theta_1 \times k_{i1} + \theta_2 \times k_{i2}, \dots, \theta_N \times k_{iN}] \tag{2}$$

$$[\theta_1]^{k_{i1}} \dots [\theta_N]^{k_{iN}} \tag{3}$$

Where  $i = [1, 2, 3 \dots M]$ . After evaluation of projection coefficient, the encrypted coefficient  $[\bar{\Omega}]$  for feature vector of facial images is taken by the cloud system (B). Then the cloud system (B) complete the encryption process of extracted feature coefficient using encryption algorithms based on  $(\psi)$  and face mean  $(\mu_i)$  for individual user (subject) (i). It does not require the participation of the other. Therefore, privacy-preservation and security of biometrics information are guaranteed.

### 4.2 Distance calculation and measurement of similarity scores

The proposed biometric recognition system performs the calculation of Euclidean distances for the matching of individual face images with stored facial template database and encrypted face  $[\Omega']$  and stored set of feature vectors  $[\Omega = \Omega'_1, \Omega'_2, \Omega'_3, \dots, \Omega'_M]$  into the database. The computation of Euclidean distances (D) between input query (test) face images and stored feature vectors of facial templates are given in Equations ((4) - (9)) as follows:

$$\begin{aligned} Distance (D) &= D[\Omega', \bar{\Omega}] = \|\Omega' - \bar{\Omega}\| \\ D[\Omega', \bar{\Omega}] &= (B - \bar{B}_1)^2 + (B - \bar{B}_2)^2 + (B - \bar{B}_3)^2 + \dots + (B - \bar{B}_K)^2 \\ D[\Omega', \bar{\Omega}] &= \sum_{i=1}^K B_i^2 + \sum_{i=1}^k (-2B\bar{B}_i) + \sum_{i=1}^k \bar{B}_i^2 \\ D[\Omega', \bar{\Omega}] &= R_1 + R_2 + R_3 \end{aligned} \tag{4}$$

The Euclidean distances are transformed into following segments, such as  $R_1, R_2$  and  $R_3$ . Each segment is defined as follows:

$$R_1 = \sum_{i=1}^k B_i^2 \tag{5}$$

$$R_2 = \sum_{i=1}^k (-2B_i \bar{B}_i) \quad (6)$$

$$R_3 = \sum_{i=1}^k \bar{B}_i^2 \quad (7)$$

In the proposed approach, the computation of the Euclidean distances between input query face image and stored face templates in the cloud database is done in the encrypted domain. The computation of distances in the encrypted domain is given as follows:

$$D[\Omega', \bar{\Omega}] = [R_1] \cdot [R_2] \cdot [R_3] \quad (8)$$

The computation of  $[R_1]$  coefficients of facial feature templates are well known. The cloud system (B) calculates the facial coefficient first, and then encrypts the coefficient of facial template by using the homomorphic public-key based Paillier algorithm [33]. Moreover, computation of  $[R_2]$  is given in Eq. (9) as follows:

$$R_2 = \sum_{i=1}^k (-2w_i \bar{w}_i) = \prod_{i=1}^k [\bar{w}]^{-2w_i} \quad (9)$$

The computation of  $(R_3)$  is complex, because it needed the collaboration between cloud system (B) and proposed biometrics-based recognition system during transfer the information of coefficients of facial templates. First, cloud system (B) produces a random number  $(E_i)$  for each  $(\bar{w}_i)$  by using public-key Paillier algorithm [33]. After that, it computes the  $[x_i] = [x_i + E_i] = [x_i] \cdot [E_i]$  using additive homomorphic encryption technique. Then encrypted projection coefficient  $[x_i]$  has been transformed into  $[[x_i]]$  using the Elliptic encryption technique. The generated random number  $(E_i)$  has been applied to increase the ambiguity during encryption of coefficients for facial templates in the cloud system (B). Therefore, transmission of the encrypted templates (data) are sufficient for providing the privacy preservation of individual in the cloud system. The double encryption of biometric templates and transmission is shown in Fig. 3.

In this block diagram (Fig. 3), it illustrates the communication and transmission of encrypted biometrics features for user identification and protecting privacy-preservation in the cloud system (B). The cloud system (B) transfers the encrypted data  $M[[x_i]]$  to  $a[[x_i]]$  which is decrypted by encryption techniques in the proposed biometric-based recognition system using a private key and achieve the  $[x_i]$  and  $[x_i^2]$ . After that,  $[x_i^2]$  is converted into double encrypted form  $[[x_i^2]]$  and received by cloud system (B). The cloud system (B) received the  $[[x_i^2]]$  facial template information and decrypts the encrypted facial templates to  $[x_i^2]$ . The decryption of encrypted coefficients of the facial template is performed as follows (using Equation 10):

$$[x_i^2] \cdot (\bar{w}_i)^{-2E_i} \cdot E_i = [(\bar{w}_i + E)]^2 - 2\bar{w}_i E_i - E_i^2 = \bar{w}_2 \quad (10)$$

Finally, the distance vectors  $D_j = D[\Omega', \bar{\Omega}]$  are calculated in the encrypted domain, where  $j = \{1, 2, 3 \dots, M\}$ .

### 4.3 Minimum distance finding

After calculation of Euclidean distances ( $D_i$ ) for the matching of face images among ( $M$ ) encrypted biometrics templates, the  $k$ - $d$  tree structure technique has been applied for the representation of biometric template features in the hierarchical form at different levels. The selected sets of discriminatory features of facial templates is applied for representation and finding the minimum distances among feature vectors at different levels of  $k$ - $d$  tree structure. The computation of distances between the features vectors is denoted as ( $M$ ) = [ $M_1, M_2, M_3, \dots, M_n$ ] distances. The distances are categorized into two neighbor distance groups ( $G_1$ ) and ( $G_2$ ), respectively (where ( $G_1$ ) > ( $G_2$ )). The size of each neighbor is equal to  $\left(\frac{M}{2}\right)$  in the individual group.

The individual group has only the small number of neighbor elements. The individual group performs the sorting mechanism to find the bigger elements from the group list and it maintains the smaller elements in the group and removes the bigger one. This sorting technique is used to compute the minimum distances between facial templates (feature vectors). During the testing phase of query data (feature set), the query face images are matched with stored biometric templates of facial features and compute the similarity matching scores of query facial image with stored data [4, 47]. The computation of minimum distance and similarity matching between facial images using Euclidean distances are shown in Algorithm 2.

Algorithm 2: Calculation for minimum distance and similarity matching algorithm

- Step 1: For the computation of minimum distance and similarity scores,
- Step 2: The system (B) encrypts the selected generated random number ( $E_i$ ) and compute the determinant  $|E|$
- Step 3: After computation, the random number ( $E_i$ ) is selected to perform the commutative law with F [ $F + E$ ] = [ $F$ ] . [ $E$ ] and [ $H + E$ ] = [ $H$ ] . [ $E$ ] to proposed system (A), where F and H are variables. .
- Step 4: Proposed system (A) decrypts the encrypted message and obtain [ $F + E$ ] and [ $H + E$ ], subtract the two numbers, if result is negative, then  $E = 1$ , otherwise  $E = 0$ ;
- Step 5: Proposed system (A) sends [ $E$ ] to cloud (B)
- Step 6: Cloud system (B) performs the computation to achieve [ $E$ ] as follows:

$$[Z] = [E]^{\left[\frac{E}{\#}\right]}, [H] = [(F < H) \cdot (F - H) + H] \quad (11)$$

The encrypted features  $[[Z]]$  is achieved by double Elliptical encryption algorithm and it is sent back to proposed biometrics based recognition system for decryption of encrypted facial features  $[Z]$  using public -private-key Paillier scheme.

## 5 Encryption process and key generation

In this section, face encryption and key generation are discussed in detail. The Elliptic encryption algorithm [4, 43, 47] is applied for double encryption of encrypted biometric facial image features. The main advantage of the double encryption process is that encrypted messages have not exploited for the information leakage and misuse of stored biometric facial image

data in the cloud computing. In the double encryption process, individual user (P) selects the Elliptic encryption curve  $E_p(a, b)$  to encrypt the face image feature and generate the set of point (V) for the matching of encrypted images [4, 47]. The double encrypted biometric can be shown by  $[[\Gamma]]$ . The cloud user (P) selects the private-key and public-key (K) for the encryption and decryption of facial features. After that, the double encrypted biometric facial templates are passed to the cloud system (B) for the matching and recognition of the individual in the cloud computing. The Elliptic encryption algorithm is shown in Algorithm 3.

Algorithm 3: Elliptic encryption algorithm

- Step 1: Cloud user (P) selects an elliptic curve  $E_p(r, s), y^2 = x^2 + rs + s(\text{mod}P) \times n$ ,
- Step 2: Cloud user calculates set of points (V) on the Elliptic curve
- Step 3: Generation of key: For the encryption, private key (k) is chosen. The public key  $K = (kV)$  is produced.
- Step 4: Transfer of generated key: The elliptic curve  $E_p(r, s)$  is transferred along with generated public key  $K = (kV)$  and set of points (V) to server side of cloud system (B).
- Step 5: The biometric facial data is received by cloud system. The received message are encoded and passed to the point (L) on  $E_p(r, s)$  and produce the random integer (Y) (where,  $Y < n$ )
- Step 6: cloud system (B) evaluates  $(S_1)$  and  $(S_2)$ , such as  $(S_1 = L + Yk)$  and  $(S = Y)$ ,
- Step 7: Cloud system transfers the points  $(S_1)$  and  $(S_2)$  for the encryption of biometric feature during enrollment process.
- Step 8: After received the information, cloud system calculates  $(S_1kS_2)$ .
- Step 9: The result  $(S_1kS_2)$  is applied for decoding the encrypted message on point (L) because  $(S_1 - kS_2 = L + YK - k(YG) = J + rK - k(rG) = J$ , and then the point (M) can be explicitly decoded.

In the proposed system, for identification of the individual users, extracted features are projected in the feature space to find the corresponding unique feature subspace. These features are used for the computation of match scores. Similarity matching is combined to achieve the face recognition of individuals under encrypted conditions. Finally, queries (test) encrypted face images are matched with stored face template's images.

The overall communication between cloud and users is done in the encrypted domain [66]. The motivation behind to apply the Paillier encryption technique [33, 47] is that it has homomorphism additive properties, efficient and simple approach for biometric features. In an additive homomorphic, encryptions [F], and [H] are added to compute the encryption [F + H], such as  $[F + E] = [F] \cdot [E]$  using homomorphic additive properties. The Elliptic encryption algorithm has done encryption in an algebraic manner. In addition, each received the encrypted face features are multiplied with a constant. For example, received encrypted face image feature [F] can be multiplied by the constant [H], such as  $[F] \cdot [H] = [F]^H$  under the homomorphic additive property.

## 6 Experimental results and discussion

To evaluate the experimental results of a biometric recognition system, we have done implementation using C language on the Linux Programming Environment for the

privacy-preserving and security of biometric data. The performances of the proposed system are evaluated through an extensive set of experiments.

To perform the evolution of experimental results, we have used the FERET face database [48]. In the database, 600 frontal face images of 200 subjects. Each cloud user (subject) has three face images of  $200 \times 200$  pixels. The applied FERET database has various types of facial images. We have used the Viola–Jones detection algorithm [48] for the face detection of individual subjects. The detected area of the frontal face image selected as the region of interest for the facial feature extraction. Fig. 4 shows the sample face images from the FERET database [35].

## 6.1 Performance evaluation

The performance measure of the biometrics-based recognition system fully depends on the extracted features from the database. The extracted features must have the high discriminative quality. For the experimental results, tuning parameters are determined for classification and recognition of facial images. However, biometrics-based recognition system is not limited to, any biometric characteristics for high availability of algorithms. We have split the used face database into two parts: (1) system training part, and (2) system testing part of the evaluation of experimental results. In the training part, 60% face image database is chosen to train the proposed system and remaining 40% of the face images are used for testing (query) face images.

In our proposed approach, few coded letter (terms) are used to encode the facial images, such as “*Image In*”, and “*Individual In*”. The code “*Image In*” illustrates that facial image of individual subject is present in the biometric templates database (shown in Table 1). While “*Individual In*” presents the identity of the individual subjects based on their face images which are available in the biometric template database. The experimental results are evaluated on the FRRET face database as mentioned in Table 1. The encryption of biometric face features, generated encrypted facial codes along with recognition accuracy are shown in Table 2.

In the experimentation, face recognition using PCA algorithm produces recognition rates 96% recognition accuracy (shown in Table 2). To complete the likelihood testing, we have performed the testing of recognition accuracy; the proposed method is consolidated with repeated (double encryption) encryption algorithm and the cloud computing model, face recognition rate does not decrease spontaneously.





For the in-depth analysis of experimental results, we completed the identification of facial images on the different stretching factor for compressed facial pictures of the individual. For the preliminary analysis, compressed image factor (i) is defined to guarantee the recognition



**Fig. 4** Illustrates face images from the FERET database



**Table 1** Distribution of facial image database for individual recognition

Face images	Example	No. of images	Image In	Subject In (Individual In)
Cloud Biometric Database		600 frontal face images from 200 subjects	Yes	Yes
Cloud user image-1		300×3	Yes	Yes
Cloud user image-2		200×3	Yes	No
Cloud user image-3		300×3	No	No

accuracy of cloud user for the preservation of user privacy, however also alleviate the complexity of the proposed approach for authentication of cloud users. We have chosen the log function base (10) as compressed factor for evaluating the experimental results. The performance of the proposed recognition system based on the compressed factor is shown in Table 3. It can observe that performance of recognition system changes at the various levels of the compressed factor for recognizing the individual user in the cloud computing.

Based on experimental results, it is validated that when the stretching factor is continuous, it increases up to level 5. The identification accuracy 96.89% prevails same at level 5, and default factor is set to 5. The stretching factor plays an indispensable role to guarantee the recognition rate of the proposed system and also decrease the complexity of the face recognition algorithm.

The computation time is also calculated during encryption of biometric features for the analysis of recognition algorithm and its time complexity in the proposed system. The time complexity is defined as the time taken for the identification of individual subjects in the available database. The computation time is shown in Table 4.

When the front facial image of cloud user is changed due to the unconstrained environment, the recognition accuracy of proposed system consumes more time for pre-processing (e.g., noise removal and background subtraction) of captured facial images and feature extraction. Therefore, within-class and between-classes of facial images are varied in low illumination and poor images quality in the unconstrained environment. Whenever number of scattered feature matrix are overlapped in the feature space, therefore, similarity matching of facial images takes more time to find the similarity scores of test face images with stored facial template database. The dimension (pixel values) of face images and total consuming time are shown in Table 4.

**Table 2** Illustrates the recognition accuracy (%) of the individual cloud users

Face database	Encrypted facial templates	Consumed time	Performance Measure
Face images –1	368,348,074,186	14 s	92.87%
Face images –2	13,595,742,070	16 s	92.67%
Face images –3	24,679,123,585	19 s	93.75%
Face images –3	17,901,256,290	23 s	94.67%
Face images –4	12,786,953,190	26 s	96.89%

**Table 3** Recognition accuracy on different compressed factors

S. No.	Level of compressed factor ()	Recognition Rate
1	0	53.78%
2	1	58.97%
3	2	62.34%
4	3	93.58%
5	4	95.48%
6	5	96.89%

Based on that Table 1, it is demonstrated that more dimension of facial images takes the time to perform the encryption of facial images, because of encryption of facial templates, pre-processing and feature extraction of face images requires a number of iterative operations. Table 5 illustrates the total time taken for the required dimension of facial images.

## 6.2 Performance comparisons

We compared the performance of our proposed approach with existing cloud privacy-preserving methods. The comprehensive description of privacy preservation and security approaches is given in Table 6. Marina Blanton and Paolo Gasti [7] proposed a cloud biometric framework for individual authentication using their detection of fingerprint minutiae points and iris codes. The proposed system consumed the total time 3178 + 79.5/fused features for offline detection and matching of minutiae points of individual fingerprint recognition.

Mohammad Haghghat [19] proposed a biometric based cloud recognition system for individual authentication. The system extracts the Gabor feature from the facial images. The extracted features are classified by generalized local discriminant analysis (GLDA) algorithms to find the class separability and achieved the 95% recognition accuracy. Li Ping et al. [36] proposed the privacy-preservation scheme for the encryption of facial features using Scale Invariant Feature Transform (SIFT) keypoint detection technique. The proposed system applied the BCP cryptographic algorithm for double encryption of detected facial images.

In the similar direction, Jegede et al. [26] proposed a cloud biometric-based facial recognition system for preservation of user privacy. The proposed system extracts the local texture feature from the facial images using Local Binary Pattern (LBP) face recognition algorithm. The system yields the 0.47% False Acceptance Rate (FAR), and 1.56% False Rejection Rate (FRR), respectively. The proposed system extracts the local features from the captured face images

**Table 4** Computation of time for identifying individual based on their face images

Face image database	Face image Size (pixels)	Time taken (seconds)
Cloud user image-1	25 × 25	150 s
Cloud user image-2	50 × 50	184 s
Cloud user image-3	75 × 75	210 s
Cloud user image-4	100 × 100	225 s
Cloud user image-5	150 × 150	267 s
Cloud user image-6	200 × 200	278 s
Cloud user image-7	250 × 250	300 s
Cloud user image-8	500 × 500	345 s

**Table 5** Illustration of dimension of face images and total consuming time

Dimension (pixels) of face image	Total Consuming (second)
500 × 500	340 s
200 × 200	240 s
150 × 150	169 s
100 × 100	130 s
75 × 75	100 s

which are reliable for low illumination and rotation invariant face image. But the system fails to encrypt the facial templates at cloud server due to the minimal number of texture facial features.

In this research work, the biometric recognition system is proposed for privacy-preservation and security of sensitive data. The proposed system is tested on the FERET face image database. We have performed the privacy-preservation and security of sensitive data based on Eigenfaces of the facial image of the individual. We have used the Eigenface recognition approach to encoding the facial images of cloud users in the feature space. The coefficients of extracting facial images are encrypted using the Paillier encryption and elliptic curve based encryption algorithms. We have further customized the Paillier encryption algorithm for the security of personal biometric data and preservation of user privacy in the cloud.

The encryption of facial templates is tested and validated the stretching (compressed) factor. In this paper, we utilize the Leave-one-out cross-validation strategy to verify the performance of the proposed recognition system. The train and test sample-splitting-ratios (60% face image for training phase and 40% of face images for testing images) are applied to validate our proposed biometric-based recognition system. Based on experimental results, it is demonstrated that when the stretching factor is continuous on face images for dimensional reduction up to level 5, the recognition accuracy of the proposed biometric recognition system remains at 96.89%. The overall comparative study of various cloud privacy-preservation biometric system is given in Table 6.

**Table 6** Comparative study of performance of cloud privacy-preservation based biometric systems

S.No.	Author name	Biometric identifiers	Algorithms/ Approaches	Performance measures	
1	Marina Blanton and Paolo Gasti [7]	Fingerprint and iris biometric images	detection of minutiae points and iris codes	Offline detection time	3178+79.5/record
				Online detection time	89+149.2/record
2	Mohammad Haghghat [19]	Face image	Gabor feature extraction, GLDA, PCA	Recognition accuracy	95%
3	Li Ping et al. [36]	Face image	SIFT keypoint descriptor, BCP double encryption algorithm	Decryption time	55s
				Feature detection	95s
4	Jegade et al. [26]	Facial features (200 face images)	Local binary pattern feature extraction	FAR	0.47%
				FRR	1.56%
5	This research study	FERET face database	PCA+Eigen face+Paillier encryption + Elliptic curve based encryption algorithm	Recognition accuracy	96.89%
				Encryption time	345s

## 7 Conclusion and future direction

In this paper, a biometrics-based recognition system is proposed for privacy-preservation and security of sensitive biometric database or information. The proposed system recognizes the cloud users based on their encrypted face template database in encryption domain. The proposed biometric-based recognition system extracts the facial features to preserve the user privacy. It also provides Eigenfaces facial features for the privacy preservation of cloud users and stores sensitive biometric data in the encrypted form in the cloud database.

We also develop a prototype system for evaluating the recognition accuracy biometric face image database. The proposed biometric-based recognition system can be deployed for assessing the efficacy of a system and identification of the individual with no information loss in the cloud computing.

The shortcoming of the proposed recognition system is that it fails to perform the better recognition of individuals in the small database and consumes time during matching of facial encryption, image data. The authentication of cloud user in the real-time identification using large biometric databases needs more storage, processing capability and significant computing resources. Moreover, in future, we plan to design and develop the automatic biometrics-based authentication system and possibly more adaptive encryption and quantization methods to alleviate the loss of cloud data and accordingly improve the performance of proposed biometric-based recognition system.

## References

1. Ahonen T, Hadid A, Pietikainen M (2006) Face description with local binary patterns: Application to face recognition. *IEEE Trans Pattern Anal Mach Intell* 28(12):2037–2041
2. Ali M, Khan SU, Vasilakos AV (2015) Security in cloud computing: Opportunities and challenges. *Inf Sci* 305:357–383
3. Samer Atawneh, Ammar Almomani et al. (2016) Secure and imperceptible digital image steganographic algorithm based on diamond encoding in DWT domain. *Multimed Tools Appl*. Springer
4. Martínez VG, Encinas LH, Ávila CS (2010) A survey of the elliptic curve integrated encryption scheme. *Ratio* 80(1024):160–223
5. Mauro Barni, Tiziano Bianchi, Dario Catalano, Mario Di Raimondo, Ruggero Donida Labati, Pierluigi Failla, Dario Fiore, Riccardo Lazzaretto, Vincenzo Piuri, Fabio Alessandro Scotti (2010) Privacy-preserving fingerprint authentication. *Proc 12th ACM Workshop Multimed Sec*, 231–240
6. Vinayak Ashok Bharadi and Godson Michael DSilva (2015) Online Signature Recognition Using Software as a Service (SaaS) Model on Public Cloud. *Proc IEEE Int Conf Comput Commun Contrl Automation (ICCUBEA)*, 65–72
7. Marina Blanton and Paolo Gasti (2011) Secure and Efficient Protocols for Iris and Fingerprint Identification. In *Computer security—ESORICS2011*, 190–209
8. Bringer J, Chabanne H, Kindarji B (2011) Identification with encrypted Biometrics data. *Sec Commun Netw* 4:548–562
9. Julien Bringer, Herve Chabanne, Alain Patey (2013) Practical identification with encrypted Biometrics data using oblivious ram. *Proc IEEE Int Conf Biomet (ICB)*, 1–8
10. Julien Bringer, Hervé Chabanne, Alain Patey (2013) SHADE: Secure hamming distance computation from oblivious transfer. *Fin Cryptograph Data Sec*, 164–176. Springer
11. Julien Bringer, Herve Chabanne, Melanie Favre, Alain Patey, Thomas Schneider, and Michael Zohner (2014) GSHADE: Faster privacy-preserving distance computation and Biometrics identification. *Proc 2<sup>nd</sup> ACM Workshop Inform Hiding Multimed Sec*, 187–198

12. Ivan Damgård, and Mats Jurik (2001) A Generalisation, a Simplification and Some Applications of Paillier's Probabilistic Public-Key System. Proc 4th Int Workshop Pract Theory Publ Key Cryptograph: Public Key Cryptograph, 119–136
13. Daugman JG (1993) High confidence visual recognition of persons by test of statistical independence. IEEE Trans Pattern Anal Mach Intell 15:1148–1161
14. Zekeriya Erkin, Martin Franz, Jorge Guajardo, Stefan Katzenbeisser, Inald Lagendijk, Tomas Toft (2009) Privacy-preserving face recognition, In Privacy enhancing technologies, 5672 of the series Lecture Notes in Computer Science, 235–253. Springer
15. Fernandes DAB, Soares LFB, Gomes JV, Freire MM, Inácio PRM (2014) Security issues in cloud environments: a survey. Int J Inf Secur 13(2):113–170
16. B. Ferreira; J. Rodrigues; J. Leita; H. Domingos Practical privacy-preserving content-based retrieval in cloud image repositories. IEEE Trans Cloud Comput (99), 1. doi: 10.1109/TCC.2017.2669999
17. Z. Fu; F. Huang; K. Ren; J. Weng; C. Wang Privacy-preserving smart semantic search based on conceptual graphs over encrypted outsourced data. IEEE Trans Inform Forensics Sec (99), 1
18. Gupta BB, Agrawal DP et al (2016) Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security. IGI Global Publisher, USA
19. Haghighata M, Zonouzb S, Abdel-Mottaleba M (2015) CloudID: trustworthy cloud-based and cross-enterprise biometric identification. Expert Syst Appl 42(21):7905–7916
20. Hankerson D, Menezes AJ, Vanstone S (2006) Guide to elliptic curve cryptography. Springer Science & Business Media
21. A. N. Jaber and Mohamad Fadli Bin Zolkipli (2013) Use of cryptography in cloud computing, Control System, Computing and Engineering (ICCSCE). IEEE Int Conf, Mindeh, 179–184
22. Jain AK, Pankanti S, Prabhakar Karthikeyan S, Lin H, Ross A (2004) Biometrics: a grand challenge. Proc 17th IEEE Int Conf Pattern Recognitn (ICPR) 2:935–942
23. Anil K. Jain, Arun Ross and Sharath Pankanti Biometrics: A tool for information security. IEEE Trans Inform Forensics Sec, 1, 125–143, 2006
24. Anil K. Jain, Arun A. Ross, Karthik Nandakumar (2011) Introduction to Biometrics, Springer Science & Business Media
25. P. Jain, D. Rane and S. Patidar (2011) A survey and analysis of cloud model-based security for computing secure cloud bursting and aggregation in renal environment, Information and Communication Technologies (WICT), 2011 World Congress on, Mumbai, 456–461
26. Jegede A, Udzir NI, Abdullah A, Mahmud R (2015) Face Recognition and Template Protection with Shielding Function. International Journal of Security and Its Applications 9(12):149–164
27. Jianzhong Li (2017) Four-image encryption scheme based on quaternion Fresnel transform, chaos and computer generated hologram. Multimed Tools Appl. Springer
28. Li J, Liu Z et al (2015) L-EncDB: A Lightweight Framework for Privacy-Preserving Data Queries in Cloud Computing. Knowl-Based Syst 79:18–26
29. Jin Li, Hongyang Yan, et al., Location-Sharing Systems with Enhanced Privacy in Mobile Online Social Networks, IEEE Systems Journal. DOI: 10.1109/JSYST.2015.2415835
30. Ojala T, Pietikainen M, Maenpaa T (2002) Multiresolution gray-scale and rotation invariant texture classification with local binary patterns. IEEE Trans Pattern Anal Mach Intell 24(7):971–987
31. Margarita Osadchy, Binyamin Pinkas, Ayman Jarrous, Boaz Moskovich (2013) System for secure face identification (SCIFI) and methods useful in conjunction therewith. U.S. Patent No. 8,542,886
32. Elena Pagnin, Christos Dimitrakakis, Aysajan Abidin, Aikaterini Mitrokotsa (2014) On the leakage of information in Biometrics authentication. Progress Cryptol (INDOCRYPT2014), 265–280. Springer
33. Pascal Paillier (1999) Public-key cryptosystems based on composite degree residuosity classes. Adv Cryptol (EUROCRYPT99), 223–238. Springer
34. Philip J, Bharadi VA (2016) Dr., Signature Verification SaaS Implementation on Microsoft Azure Cloud. Proc Int Conf Communication, Comput Virtual (ICCCV) 2016 79:410–418
35. Phillips PJ, Moon H, Rauss PJ, Rizvi S (2000) The FERET evaluation methodology for face recognition algorithm. IEEE Trans Pattern Anal Mach Intell 22(10):1090–1104
36. Li Ping, Tong Li, Zheng-An Yao, Chun-Ming Tang, Jin Li (2016) Privacy-preserving outsourcing of image feature extraction in cloud computing. Soft Comput, 1–11
37. Ahmad-Reza Sadeghi, Thomas Schneider, Immo Wehrenberg (2009) Efficient privacy-preserving face recognition. Inform, Sec Cryptol (ICISC-2009), 229–244
38. Lorenz Schauer, Florian Dorfmeister, Florian Wirth (2016) Analyzing passive Wi-Fi fingerprinting for privacy-preserving indoor-positioning. Proc IEEE Int Conf Local GNSS (ICL-GNSS), 1–6
39. Shu T, Chen Y, Yang J (2015) Protecting Multi-Lateral Localization Privacy in Pervasive Environments. IEEE/ACM Trans Network (TON) 23(5):1688–1701

40. Sowmya R, Ezhilarasu P, Satheesh Kumar D, Manoj Prabhakar J (2015) A Survey on Data Security Using Identity Based Encryption in Cloud Computing. *Int J Appl Inform Commun Eng* 1(11):3–4
41. Subashini S, Kavitha V (2011) A survey on security issues in service delivery models of cloud computing. *J Netw Comput Appl* 34(1):1–11
42. Sun Y, Wen Q, Zhang Y, Li W (2014) Privacy-Preserving Self-Helped Medical Diagnosis Scheme Based on Secure Two-Party Computation in Wireless Sensor Networks. *Computational and Mathematical Methods in Medicine* 2014:1–9
43. Suryadevara S, Kapoor S, Dhatteval S, Naaz R, Sharma A. (2011) Tongue as a Biometric Visualizes New Prospects of Cloud Computing Security. *Int Conf Inform Network Technol* 4
44. Takabi H, Joshi JBD, Ahn G-J (2010) Security and privacy challenges in cloud computing environment. *IEEE Sec Privacy* 8(6):24–31
45. M. A. Turk, A. Pentland (1991) Face recognition using eigenfaces. *Proc IEEE Comput Soc Conf Comput Vision Pattern Recogn (CVPR)*, 586–591
46. Turk MA, Pentland A (1991) Eigenfaces for recognition. *J Cogn Neurosci* 3:71–86
47. Víctor GM, Luis HE, Carmen SÁ, Katiyar V, Dutta K, Gupta S (2010) A survey on elliptic curve cryptography for pervasive computing environment. *J Comput Sci Eng* 2(2):7–13
48. Viola P, Jones MJ (2004) Robust real-time face detection. *Int J Comput Vision*. 1 57(2):137–154
49. Wang W, Chen L, Zhang Q (2015) Outsourcing high-dimensional healthcare data to cloud with personalized privacy preservation. *Comput Netw* 88:136–148
50. Xiaoshan Wang; Yao Liu; Zhiqiang Shi; Xiang Lu; Limin Sun (2015) A Privacy-Preserving Fuzzy Localization Scheme with CSI Fingerprint. *Proc IEEE Int Conf Global Commun Conf (GLOBECOM)*, 1–6
51. Qian Wang, Shengshan Hu, Kui Ren, Meiqi He, Minxin Du, Zhibo Wang (2015) CloudBI: Practical Privacy-Preserving Outsourcing of Biometric Identification in the Cloud. *Europ Symp Res Comput Sec*, 186–205. Springer International Publishing
52. Wang Y, Wu Q, Qin B, Tang S, Susilo W (2017) Online/Offline Provable Data Possession. *IEEE Trans Inform Forensics Sec* 12:1182–1194 ISSN 1556-6013
53. Zhihua Xia, et al, A Privacy-preserving and Copy-deterrence Content-based Image Retrieval Scheme in Cloud Computing. *IEEE Trans Inform Forensics Sec*, vol. 11, no. 11, pp. 2594–2608, 2016
54. Xia Z et al (2016) Steganalysis of LSB matching using differences between nonadjacent pixels. *Multimed Tools Appl* 75(4):1947–1962
55. Yu Y et al (2017) Identity-Based Remote Data Integrity Checking With Perfect Data Privacy Preserving for Cloud Storage. *IEEE Trans Inform Forensics Sec* 12(4):767–778. doi:10.1109/TIFS.2016.2615853
56. Jiawei Yuan, and Shucheng Yu (2013) Efficient privacy-preserving biometric identification in cloud computing. *Proc IEEE Int Conf INFOCOM*, 2652–2660
57. Youwen Zhu, Zhikuan Wang, Yue Zhang (2016) Secure k-NN Query on Encrypted Cloud Data with Limited Key-Disclosure and Offline Data Owner. *Pacific-Asia Conf Knowledge Discov Data Mining*, 401–414. Springer International Publishing
58. Zhu Y, Huang Z, Takagi T (2016) Secure and controllable k-NN query over encrypted cloud data with key confidentiality. *J Parallel Distrib Comput* 89:1–12



**Dr. Santosh Kumar** is an Assistant Professor in Computer Science and Engineering discipline. Prior to joining IIIT- Naya Raipur, Dr. Kumar was a Ph.D. Research Scholar in the Department of Computer Science and

Engineering, I.I.T (Banaras Hindu University), Varanasi, India. He has completed his B. Tech. (CSE) degree in Department of Computer Science and Engineering, Uttar Pradesh Technical University (UPTU) in 2008 and M. Tech. in Computer Science & Engineering from Birla Institute of Technology, Mesra, Ranchi (Jharkhand, India) in 2012. He has authored more than 14 publications in reputed journals, book chapters, and conferences. His research interests include Animal biometrics, Computer vision, Machine Learning, Pattern recognition, Wireless sensors, and Internet of Things (IoT). He is an active member of ACM and IEEE Society.



**Dr. Sanjay Kumar Singh** is currently working as Professor at the Department of Computer Science and Engineering, IIT BHU, Varanasi. He has completed his B. Tech. in Computer Engg., M. Tech. in Computer Applications and Ph.D. in Computer Science and Engineering. He is a Certified Novell Engineer (CNE) from Novell Netware, USA and a Certified Novell Administrator (CNA) from Novell Netware, USA. He is a member of LIMSTE, IEE, International Association of Engineers and ISCE. His research areas include Biometrics, Computer Vision, Image Processing, Video Processing, Pattern Recognition and Artificial Intelligence. He has over 50 national and international journal publications, book chapters and conference papers. He is also a Guest Editorial Board Member of Multimedia Application and Tools, Springer, and the EURASIP Journal of Image and Vision Processing (Springer). He is a member of the Computer Society and the Association for Computing Machinery.



**Dr. Amit Kumar Singh** is currently working as Assistant Professor (Senior Grade) in the Department of Computer Science & Engineering at Jaypee University of Information Technology (JUIT) Wanknaghat, Solan,



Himachal Pradesh-India since April 2008. He has completed his PhD degree from the Department of Computer Engineering, NIT Kurukshetra, Haryana in 2015. Recently, Dr. Singh appointed as Associate Editor of [IEEE Access](#) and [Multimedia Tools and Applications](#) (MTAP), Springer. He has presented and published over 50 research papers in reputed journals and various national and international conferences. His important research contributions include to develop watermarking methods that offer a good trade-off between major parameters i.e. perceptual quality, robustness, embedding capacity and the security of the watermark embedding into the cover digital images. His research interests include Data Hiding, Biometrics & Cryptography.



**Dr. Shrikant Tiwari** is currently working toward as Assistant Professor in Department of Computer Science & Engineering (CSE) at Shri Shankaracharya College of Engineering and Technology (SSCET), Junwani, Bhilai, Distt. Chattisgarh (India). He received his Ph.D. in Department of Computer Science & Engineering (CSE) from the Indian Institute of Technology (Banaras Hindu University), Varanasi (India) in 2012 and M. Tech. in Computer Science and Technology from University of Mysore (India) in 2009. He has published more than 20 papers in international journal and conference. His research interests include Biometrics, Image Processing and Pattern Recognition. Dr. Tiwari is a member of IEEE, IET, IETE, CSI, ISTE, IAENG, SCIEL.



**Dr. Ravi Shankar Singh** is currently working as Associate Professor at the Department of Computer Science and Engineering, IIT BHU, Varanasi. His research interests include Data Structures, Algorithms and High Performance Computing