*Biomedical Research 2018; Special Issue: S506-S516*

*ISSN 0970-938X*
*www.biomedres.info*

# Multimodal biometric hashkey cryptography based authentication and encryption for advanced security in cloud.

**Sree Vidya B[*], Chandra E**

Department of Computer Science, Bharathiar University, Coimbatore, India

## Abstract

**Cloud Computing (CC) is a technology that is growing at a faster pace, gaining much popularity with startup companies increasing and opting for clouds' services. The growth rate of this technology is high and so is the security threat. Though there are existing authentication systems like two factor authentication, biometric based authentication and so on, hackers still pose greater challenges. Though password-based authentication system is simple, it is highly vulnerable to security breaches. Biometric based authentication has better security, but usage of single biometric traits can also be easily compromised. Thus, this research work, Multimodal Biometric Hashkey Cryptography (MBHC) brings about a novel security framework that focuses on both authentication and securing cloud data using multiple modalities. Authentication is based on multiple biometric modalities *viz.* Fingerprint, Iris and Face features. Features from these modalities are extracted using linear filters. Artificial Fish Swarm Algorithm (AFSA) is used for feature optimization, further to which Support Vector Machine (SVM) acts as classifier for identifying genuine users against imposters. Cryptographic keys are generated from these modalities that serve as input to Advanced Encryption Standard (AES) Algorithm for encrypting and decrypting the information stored in cloud. Integrity of data is also ensured using hash function for which the facial features and the encrypted message are the inputs. Thus, the experimental results show that the proposed architecture provides improved security for cloud computing environment when compared to the existing models.**

**Keywords:** Multiple biometric modalities, MBHC, security, authentication, Fingerprint, Iris, Face, AFSA, SVM, Cryptographic keys, AES.

*Accepted on February 05, 2017*

## Introduction

Biometrics system is the technology of using humans' physical as well as behavioral characters for identifying individuals. These characters remain unique and distinguishable. Biometric authentication refers to the system of authenticating a user based on their registered biometric trait which can be finger print, iris, face, voice etc. A multimodal biometric system is one which validates a user not just with one trait but more than one for personal identification.

A multiple biometric system can take any number of single biometric templates and pool them together and provide better security by overcoming the limitations of using sole biometric trait as a tool for verification. Multimodal systems are commonly much more significant to fraudulent technologies, since it is very complex to crack down the system using various biometric characteristics when compared to an individual biometric characteristic, thus providing extreme accuracy rate and complete protection from spoofing. Multimodal biometric systems make the spoofing process complex since it is hard for an intruder to spoof all traits at the same time for the various biometric traits of a user. Hence, a challenge-response kind of authentication is adopted by obtaining various biometric characteristics by using multimodal biometric systems. People have used characteristics of body namely gait, face and voice for many years to recognize others [1].

In recent times, where human identification becomes very crucial, among the various biometric traits, iris feature has received more significance. Iris recognition involves imaging of eye, segmentation of iris, verification, and so on. There are number of research works that have been presented for iris recognition [2]. An iris image is represented into a compact order of multi-scale quadrature 2-D Gabor wavelet coefficients; where the most significant bit has a 256-byte iris code. To characterize the texture of the iris, a wavelet transformation was computed. Some approaches employing iris features involve texture analysis. Multiple channel Gabor filtering was utilized to acquire both the local and global information of an iris image. In addition to this, independent component analysis (ICA) and wavelet packets [3] for iris pattern analysis have been employed.

The most reliable and significant trait for identifying a human is fingerprint. The matching of finger print has two key applications: verification phase and identification phase. Verification of fingerprint deals with confirmation that a particular fingerprint belongs to a particular person. Fingerprint identification is concerned with identifying an individual. Fingerprint identification includes matching a fingerprint provided by a user with a list of fingerprints that are kept in a datastore. Such a process consumes lot of time since the comparison has to be made against each and every entry in the database. To overcome such an issue, classification of fingerprints is incorporated. This involves segmenting the database of fingerprints into subsets so that the relevant fingerprint is compared only with the entries in that subset [4]. This results in better performance since the queried fingerprint is matched only with the subset and not the entire database [5].

Multimodal biometric system utilizes various biometric traits at the same time to authenticate a person's identity. The primary technique of multimodal biometric system involves fusing the multiple traits obtained from a user. This fusion of modalities can be done in three different ways: fusion of modalities at the phase of feature extraction; fusing during the matching phase; and fusing during the decision phase [6].

In the proposed research, security is achieved by using cryptography key generation approach from the fused biometric traits of users. Since three different biometric traits are obtained from the same user, different extraction techniques that best suit each of these are applied in this work. Fingerprint features are extracted using Gabor filter while pupil detection technique is for extraction of iris features. Following feature extraction, the extracted features are combined by feature fusion technique. The cryptographic key which is an essential component in this research is finally generated from these features and it remains unique and private to varied users. This process enhances the security architecture for cloud computing. Encryption and decryption is done using double encryption technique based on symmetric key encryption. Hashkey generation is performed for message integrity using Message Digest-5 (MD5) approach and face features are fused with encrypted message for verification. In this research, the proposed algorithm is used to obtain high data security and allows access only to authorized persons. The entire process of authentication and data security is totally based on the individual traits of the user thus providing an efficient security approach. In short, this research involves user enrolment, authentication, key generation, encryption and decryption and verification using MBHC with AFSA-SVM. Hence, the suggested system gives high-end security and message integrity based on the extracted face, fingerprint and iris features.

## Related Work

Gawande et al. [7] presented multimodal biometric system for efficient feature identification. The authors employed Haar wavelet to extract discrete textual features from the two image databases. The fusion approach is formulated to link those single modal characteristics by utilizing the technique called Mahalanobis distance. The system was trained with a machine learning algorithm for the extracted features. The simulation output clearly showed the performance significance of this approach when compared with other existing algorithms.

Nagar et al. [8] discussed about fusion of biometric traits at the feature-level for a cryptosystem with multiple biometrics. By maintaining an individual secure biometric sketch, the various modalities of users are protected. This was achieved with the help of a fuzzy vault combined with a fuzzy commitment. Research on these techniques using the images from biometric databases indicate that it is possible to protect the templates and increase the performance of matching by the usage of cryptosystems with biometric traits obtained from more than one trait of a user.

Agarwal et al. [9] suggested genetic algorithm which is utilized to generate a new encryption approach. A genetic algorithm has three basic operators: reproduction, crossover, and mutation. The names of these operators are self-explanatory in the context of genetics and operate accordingly. The genetic algorithms' effective searching features are obtained from reproduction operator and crossover operator. The research results in an effective encryption of images by using such an encryption algorithm, though on the downside, lies the exchanges of multimedia data which are highly secure.

Sasidhar et al. [10] clearly examined and showed that multimodal biometric systems provide improved performance significance than unimodal biometric systems for larger databases. Anwar et al. [11] suggested a new multiple biometric based confirmation technique by utilizing the geometries of hand and finger stripe. It has been explained that the approach is highly effective because of the greater recognition rate. Mishra [12] investigated various kinds of multiple biometric systems, various fusion techniques, suitability and merits of using multimodal biometric system as against traditional unimodal biometric systems.

Alvarez et al. [13] introduced an iris template protection approach which resulted in higher level security accomplished by the significance of fuzzy extractors. The authentication is ensured through the secret value of the biometric trait. The approach showed significant security level compared to other existing systems.

## Proposed Multi-Modal Biometric Hashkey Cryptography (MBHC) Method

Biometric cryptosystem is the hybrid technology of using cryptography and biometrics together to provide security, and is applied in cloud to enhance security in the cloud environment. Biometrics is the technology of using the physical and behavioral characteristics of humans (that remain unique among individuals) for identification, authentication and verification purposes. Such applications work by getting the essential features from the obtained characters and comparing these with those that are already stored in a database. The resultant of the comparison reveals whether the querying person is a genuine user or an imposter. The proposed work includes series of steps such as preprocessing, feature extraction, feature level fusion, key generation, fusion of encrypted data and face level features and decryption using acquired keys.

The proposed approach combines finger print and iris for generating cryptographic keys and combine face features and encrypted message for hash key generation. The steps included in the suggested approach depend on multimodal biometrics for cryptographic key generation and are as follows:

1. Pre-Processing using histogram equalization

2. Extraction of features from fingerprint

3. Extraction of features from iris

4. Fusion of fingerprint and iris features

5. Generation of Cryptographic key

6. Double encryption for cloud data security

7. Extraction of feature from face

8. Fusion level of face features and encrypted message

### *Pre-processing using histogram equalization*

Images that are obtained from sensors are not free of noise and hence some pre-processing technique should be incorporated to make it noise-free. Histogram equalization is one such method that is broadly used for the purpose of pre-processing. The equalization technique transforms the image into a histogram which remains constant for different values of brightness. This results in a distribution of brightness values where the probability of occurrence of each of these values is equal. For finger print, iris and face image, the extracted features can be combined easily using fusion technique.

$$P(i) = \frac{n_i}{N} \rightarrow (1)$$

Where $i \epsilon$ 0, 1…$k$-1 grey level, n is individual pixel and N is the pixel's count in the obtained image. Transformation to a new intensity value is determined by:

$$I_{out} = \sum_{i=0}^{k-1} \frac{n_i}{N} = \sum_{i=0}^{k-1} p(i) \rightarrow (2)$$

The intensity values of pixels of images from the rage [0-255] are mapped to the rage [0-1] by using equation (2). $I_{\mathrm{out}}$ is the output image after preprocessing step by using histogram equalization method [14,15].

### *Extraction of features from fingerprint*

For extracting the features from finger print, Gabor filter is employed. This is a linear filter where the harmonic function is multiplied by a Gaussian function, thus determining its impulse response [16]. Gabor filter is a popular tool for this task of extracting more relevant features from the fingerprint image. Each point in the image is characterized by local Gabor filter responses. At specific orientations and frequencies, a two-dimensional sine wave is modulated with a Gaussian envelop, resulting in a 2D Gabor filter. The 2-D Gabor filter kernel is determined by

$$f(x, y, \theta_k, \lambda, f) = \exp\left\{-\frac{1}{2}\left[\frac{x^2}{\delta_x^2} + \frac{y^2}{\delta_y^2}\right]\right\}\cos(2\pi f x)$$

$$.\exp\left\{\frac{2\pi(x\cos\vartheta_k + y\sin\vartheta_k}{\lambda}i\right\} + \phi \rightarrow (3)$$

Where $x$ and $y$ are two random variables, $\lambda$ is the wavelength and $\theta_{\mathrm{k}}$ the orientation, $\delta_{\mathrm{x}}$,$\delta_{\mathrm{y}}$ are the standard deviations and $\phi$ is constant value. The wavelength $\lambda$ variable is used to define the Gaussian envelope's spread. Below equation (4) defines the rotation of the plane x-y at an angle $\theta_{\mathrm{k}}$. This rotation results in a Gabor filter and at orientation $\theta_{\mathrm{k}}$. $\theta_{\mathrm{k}}$ is expressed by

$$\theta_k = \frac{\pi}{n}(k-1)k = 1, 2, ..n \rightarrow (4)$$

Where $n$ indicates the number of orientations. The feature obtained at a point ($x$,$y$) of the image is the resultant of the multiple filters placed at that point. The filter kernel (for a particular wavelength and orientation $\theta_{\mathrm{k}}$) is convolved with the image resulting in filter response [17].

### *Extraction of features from iris*

Iris is a circular and a flat membrane that is present behind the cornea of the eye. Iris remains highly unique to every human and does not change till the end. At the center of the eyeball, a circle shaped black disk, pupil is present. a black disk, which is circular in shape. The pupil is sensitive to light and expands and contracts according to the level of illumination. In the presence of light, it expands and shrinks in the absence of light. The iris is the annular ring among the sclera and pupil boundary and has the flowery form specific to every individual. The texture information of the iris is unique and these texture features are extracted for verification. The features are then transformed to feature vectors. To these, pattern matching algorithm is applied for the purpose of matching the obtained features against those that are stored in the database. Following are the significant steps added in iris recognition:

1. Detection of pupil

2. Detection of Iris

3. Normalization

4. Extraction of features

**Detection of pupil:** The level of illumination can affect the intensity of the captured image. Hence as a first step to pupil detection, the image is transformed into grayscale. In the transformed image, largest black colored region indicates the pupil region in the intensity image. Therefore, the detection of edges becomes simple and easy from the grey scale image. This is achieved by employing appropriate threshold values on the image. The primary concept of this technique is to detect the curves that can overcome issues like shadows and other noise. Convolution of the given image and sobel filters is performed which detects the gradient of the intensity image at the entire location. The gradient images of vertical and horizontal is represented as $G_v$ and $G_h$ along the direction x and y, this is acquired by kernels that identify the image's change along the horizontal and vertical directions. The kernels of sobel filter are defined by

$G_v$={-1,-2,-1; 0,0,0; 1,2,1} → (5)

$G_h$={-1,0,1; -2,0,2; -1,0,1} → (6)

The gradient image's absolute value is the sum of gradient vertical and horizontal and is given by the equation

$G_{abs}=G_v+G_h \rightarrow (7)$

Where $G_v$ is the result of vertical convolution of the image and $G_h$ is the result of horizontal convolution of image. The absolute value of the gradient image detects the edge. The obtained edge image is scanned for pixels (P) that accept true value. The center is defined using the equation given below

$$x_c^2 + y_c^2 - r^2 = 0 \rightarrow (8)$$

Where $x_c$ and $y_c$ are coordinates at the scanned pixel (P) and $r$ refers to the radius values' range.

**Detection of iris:** To demarcate the variation in the outer iris limit, intensity variation technique is employed. In this approach, with the identified center, the concentric circles with varied radii are extracted. The iris circle is chosen as the one which has the maximum variation in terms of intensity in comparison with the previously obtained circle in the group of existing circles. The approach functions well if there occurs sharp difference among the boundary of iris and sclera. The iris radius and pupil boundary contribute in converting the annular part which is termed as strip to a rectangular block.

**Iris normalization:** Iris features that are captured from multiple people may differ in sizes and, even irises from the same person, the size may vary due to the illumination difference and few other factors. These kinds of deformations in the texture of iris can majorly influence the output of iris matching. In order to accomplish more accurate recognition output, it is required to adjust for the iris deformation. Daugman [18,19] resolved this issue by designing the original iris in a Cartesian coordinate system into a twice dimensionless pseudo-polar coordinate system.

The iris annular region is converted to its equivalent polar by the following equations:

$I(x(\rho,\theta),y(\rho,\theta)) \rightarrow I(\rho,\theta)$ With

$$\begin{cases} x_p(\rho,\theta) = x_{\rho 0}(\theta) + r_p \times \cos(\theta) \\ y_p(\rho,\theta) = x_{\rho 0}(\theta) + r_p \times \sin(\theta) \\ x_i(\rho,\theta) = x_{i0}(\theta) + r_i \times \cos(\theta) \\ y_i(\rho,\theta) = x_{i0}(\theta) + r_i \times \sin(\theta) \end{cases} \rightarrow (9)$$

Where $r_p$ is the radius of the pupil and $r_i$ is the radius of the iris, while $(x_p(\theta),y_p(\theta))$ is the coordinate of pupillary boundary and $(x_i(\theta),y_i(\theta))$ is the coordinate of the limbic boundary in the direction θ. The value of θ corresponds to [0,2π], corresponds to [0, 1].

**Extraction of features:** Features are the attributes or values that are extracted from the given image and are used to get the specific characteristics from the image. Feature extraction from the iris image is done using Gabor filter. Gabor filter's functional form fits in closely to the receptive profiles of cortical cells. A 2D even Gabor filter in the spatial domain is given as follows:

$$G(x,y,\theta_k,f) = \exp\left\{-\frac{1}{2}\left[\frac{x^2}{\delta_x^2} + \frac{y^2}{\delta_y^2}\right]\right\}\cos(2\pi f x) \rightarrow (10)$$

Where $f$ is the frequency of the sinusoidal plane wave on the direction $\theta_k$ from the x-axis, $\delta_x$ and $\delta_y$ are the space constants of the Gaussian envelope on x and y axes correspondingly. Convolution with Gabor filters contributes majorly to the entire feature extraction time. The filter frequency is set to the average ridge frequency (1/$k$), and $k$ here refers to the average inter-ridge distance. The average inter-ridge distance is about 6 pixels in a 600 dpi Iris image. If $f$ is huge, spurious ridges are generated in the filtered image, on the other hand, if $f$ is less, close ridges are combined into one. Both the local and global information of the iris can be obtained using the Gabor filters. This tends to a total output images from which the iris features are obtained. It provides the optimal resolution in space and time domains and generates superior visual representation in the constituted texture images.

## *Fusion of fingerprint and iris features*

Fusion of fingerprint and iris at this level can be applied to the extracted features from similar modality or different multimodalities [7]. Fusion level represents combining the various feature vectors which are acquired from multiple sensors. When feature vectors are homogeneous, an individual feature vector can be computed with "or" operations. When the feature vectors are heterogeneous, then these can be concatenated to create an individual vector [20,21]. Thus, the final feature vector is the resultant of concatenation of all obtained features. The multimodal authentication system is illustrated in Figure 1.

**Multimodal authentication system using SVM with AFSA:** In this work, feature selection is performed in which SVM acts as the classifier using the AFSA. A classified model can be established using classifiers for assigning data to the correct categories. From input images, the features are first extracted, each of which has the correct category label. These extracted features are termed as training data and the remaining forms the test images. The training images are taken as input into the SVM classifiers wherein the classified model gets established and later test images are used to verify this model and to obtain accurate classification. In view of making the matching process more optimal, the artificial fish swarm algorithm helps to give some specific definitions of the integrated weight algorithm. Identification becomes more computational and time consuming in case of biometrics when compared to the identity verification [22]. Hence, for achieving the improvement in the performance with lesser execution time, highly specialized classification-related biometric system should be employed. The extracted feature vectors are optimized using Artificial Swarm Algorithm which serve as input to classifier for making final decision. Gaussian mixture, neural networks and K-Nearest Neighbourhood (KNN) classifiers are the most commonly used models-based classifiers for different biometrics.

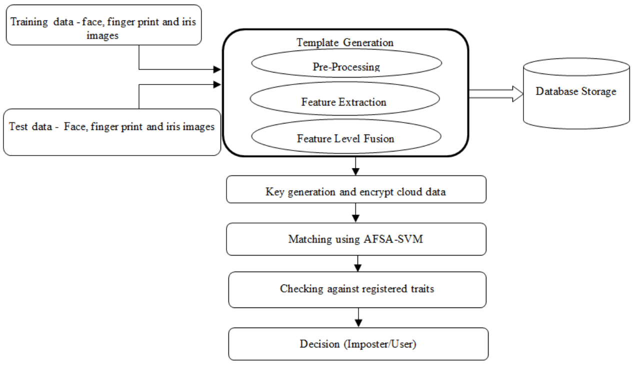
Training data - face, finger print and iris images
Test data - Face, finger print and iris images
Template Generation
Pre-Processing
Feature Extraction
Feature Level Fusion
Database Storage
Key generation and encrypt cloud data
Matching using AFSA-SVM
Checking against registered traits
Decision (Imposter/User)

*Figure 1. Multimodal authentication system.*

Statistical learning theory has the tendency to engage both the variability and the commonality among patterns. Support Vector Machine (SVM) is a powerful learning tool that works according to statistical learning theory and Machine learning. In solving different classification and pattern recognition problems, SVM has been evidenced with superior results. In case of various pattern classification applications, SVM gives good generalization performance when compared to traditional techniques specifically for huge input variables. With regard to this, evaluation of SVM for the fused feature vector is performed. Pseudo code for Biometric Authentication Process is given below.

The algorithmic process of SVM incorporated weight by utilizing the Artificial Fish Swarm Algorithm proposed in this work is as follows:

**AFSA:**

1). Initialization

2). $X_i=(x_1,x_2,\dots x_n)$ where $X_i$ is defined as an artificial fish individual

3). Calculate the food concentration FC of the current position of each artificial fish in the initial swarm

4). The individual fish with the maximum $FC_{max}>\delta FC_i$

5). Every artificial fish imitates the following and swarming behaviors, respectively. The movement with higher FC is selected to execute after each action.

6). Compute the distance $d_{i,j}=\sum_{n=1}^{N}(x_i(n)-x_j(n))^2$

7). Detectable distance of the artificial fish is denoted by VISUAL; STEP refers to the maximum step length of the artificial fish.

8). If FC is greater than the present condition, one step must be go forward, and step (11) should be proceeded; otherwise, one step should be considered randomly and step (12) must be taken;

$$x_{i+1}(p)=x_i(p)+(Random(STEP))\cdot\left(\frac{x_j(p)-x_i(p)}{d_{ij}}\right),\quad FC_i<FC_j\rightarrow(11)$$

$$x_{i+1}(p)=x_i(p)+\mathrm{Random}(STEP),\ FC_i>FC_j\rightarrow(12)$$

9). Repeat this process for every pixel

10). The movement with higher FC is selected to execute after each action.

11). Update the best pixel $p_i$

12). Compare the central pixels with other best pixels and update the current best pixel

13). Discard the error pixels

14). Integrate the features into SVM classification phase

**Pseudocode for biometric authentication process**

```
Bio-auth-process (Person P)
{
P.IDFP ← getFingerPrint(P)
P.IDIR ← getIris(P)
P.IDFA ← getFace(P)
P.IDFP ← feature_extract (P.IDFP)
P.IDIR ← feature_extract (P.IDIR)
P.IDFA ← feature_extract (P.IDFA)
for (i-0;i< dbtemplateFinger.length;i++)
{
Check(dbtemplateFinger(i))
If (dbtemplateFinger(i)) ← P.IDFP)
{
Q.feat ← feature_extract(dbtemplateFinger(i))
If (AFSASVM matcher(Q) ← P.IDFP)
P.IDFP belongs to user Q
Set P.IDFP_status←1}
else
set P.IDFP_status←0 // P has failed fingerprint authentication
}
for (j=0;j< dbtemplateIris.length;j++)
{
Check(dbtemplateIris(j))
If (dbtemplateIris(j)) ← P.IDIR)
{
Q.feat ← feature_extract(dbtemplateIris(j))
If (AFSASVM matcher(Q) ← P.IDIR)
set P.IDIR_status←1
P.IDIR belongs to user Q
}
else
set P.IDIR_status←0 // P has failed iris authentication
}
If ((P.IDFP_status←1) AND (P.IDIR_status←1))
{
P has passed multimodal authentication
return}
else If ((P.IDFP_status←0) AND (P.IDIR_status←0))
{
P has failed multimodal authentication
exit}
else
If (P.IDFP_status←1) OR (P.IDIR_status←1)
{
for (k=0;k< dbtemplateFace.length;k++)
{
Check(dbtemplateIFace(k))
If (dbtemplateFace(k)) ← P.IDFA)
{
Q.feat ← feature_extract(dbtemplateFace(k))
If (AFSASVM matcher(Q) ← P.IDFA)
set P.IDFA_status←1
P.IDFA belongs to user Q
P has passed multimodal authentication
return
}
else {
set P.IDFA_status←0
exit // P has failed face and multimodal authentication }
}
}
```

### *Generation of cryptographic key*

In this research, symmetric key approach, 128-bit Advanced Encryption Standard (AES) is used. AES as proposed by Vincent Rijmen and Joan Daemen, operates on keys of size 128-bit, 192-bit and 256-bit. The number of rounds is pre-fixed for each of these key sizes. The number of rounds is 10,12 and 14 for 128,192 and 256-bit keys respectively. For the purpose of encryption, user's bimodalities are used as cryptographic keys and the same key is used for both encryption and decryption. Here, a 128-bit block and key of 128-bit serve as inputs and produce cipher text as the output. The fused features of finger print and iris form the 128-bit key involving 10 rounds with each step having byte substitution, shifting rows, mixing columns and adding round keys. Thus, decryption again involves the bimodalities from user where the retrieval of data is completely dependent on the user's traits.

### *Double encryption for cloud data security*

Double encryption is done to ensure a higher level of security to the data that is stored in cloud. The same keys are used to perform double encryption such that the first level of encryption includes the plain text and key as the input, giving cipher text as the output. The second level again takes the same key and now the cipher text as input, thus giving a doubly encrypted cipher text as the final output. This process flow is described below (Figure 2 and 3).

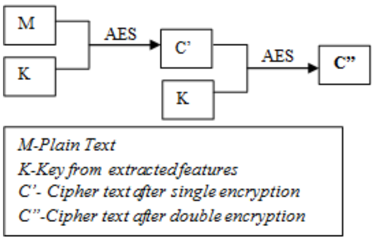
M
K
AES
C'
K
AES
C"
M-Plain Text
K-Key from extracted features
C'- Cipher text after single encryption
C"-Cipher text after double encryption

***Figure 2.** AES key generation mechanism.*

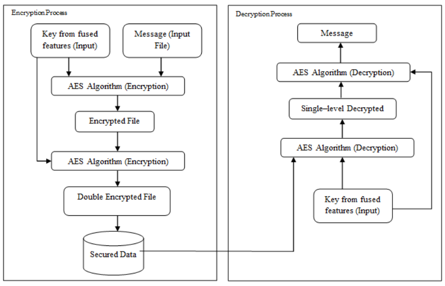
Encryption Process
Key from fused features (Input)
Message (Input File)
AES Algorithm (Encryption)
Encrypted File
AES Algorithm (Encryption)
Double Encrypted File
Secured Data
Decryption Process
Message
AES Algorithm (Decryption)
Single–level Decrypted
AES Algorithm (Decryption)
Key from fused features (Input)

***Figure 3.** Double encryption system.*

**Double encryption procedure**

```
integer count=0
```

```
Encrypt(byte input, byte output, key k)
Begin
count =count+1
byte result
result= input
AddRoundKey(result,k)
for round=1 to Nr-1 //Nr- number of rounds
subBytes(result)
ShiftRows(result)
MixColumns(result)
AddRoundKey(result,k)
end for
subBytes(result)
ShiftRows(result)
AddRoundKeY(result,k)
while count<2
Encrypt(byte result, byte output, key k)
output=result
End
integer count=0
Decrypt(byte input, byte output, key k)
Begin
count=count+1
byte result
result=input
AddRoundKey(result,k)
for round=1 to Nr-1//Nr- number of rounds
InvShiftRows(result)
InvSubBytes(result)
AddRoundKey(result,k)
InvMixColumns(result)
end for
InvShiftRows(result)
InvSubBytes(result)
AddRoundKey(result,k)
while count<2
Dencrypt(byte result, byte output, key k)
output=result
End
```

### Feature extraction from face

**Face localization and normalization:** Gabor feature extraction [23] is used for face image extraction. In this research, the local and global features of facial images are fused to achieve better accuracy with respect to facial recognition. The feature vector thus obtained is used for processing. This image is segmented into nine images that are non-overlapping. The extracted local features aid in overtaking the modification in few regions of face. A single feature vector can be obtained by combining individual features extracted from individual parts (Figure 4).

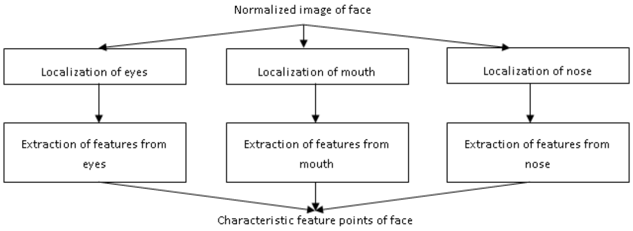
Normalized image of face
Localization of eyes
Localization of mouth
Localization of nose
Extraction of features from eyes
Extraction of features from mouth
Extraction of features from nose
Characteristic feature points of face

*Figure 4. System of features localization.*

**Facial feature localization and the face characteristic point extraction:** Chrominance components, when analyzed, indicates that, eyes have higher values of $C_b$ when compared to $C_r$ values. Here, $C_r$ and $C_b$ represents the chrominance red and blue color respectively which is used to indicate the relevant pixels. So, initially, the chrominance component $C_b$ is extracted and then its maximal value is obtained. A black and white image is obtained by setting a threshold value. The region of the eyes is segmented into two equal regions and the white stains of maximal area are observed in every region [8]. Four points are extracted that denotes the external points of every maximal area of stains in each eye. Moreover, the center of gravity of these white stains is also identified. These denote the eye's center [24,25].

The component of chrominance Cr is utilized to localize the mouth as it depends on red color. Sobel filter is employed to localize its geometrical points by identifying its contour and later extracting its extreme points. Finally, the localization of the nose becomes simple, since the nose being the mid-region, it can be easily extracted as the region lying between upper eyes and lower mouth regions. Sobel filter is employed to extract the geometrical points [25].

**Geometric distances:** The important distances among whole extracted points are denoted by the facial feature vector's elements. The distance of face metrics are taken as Deye, Dcenter_eye, Dinterior, Dnose, Deye_nose, Dmouth and Dnose_mouth.

**Mouth detection:** The redness characteristic of the lips aids in mouth identification task. Using the redness hue of the lips, the width of mouth can be detected as the distance between the corners of the lips, forming the geometric distance. After drawing-out the face-bounding box from face features, the red color lips are identified by utilizing the criterion determined in equation (13), and indicated as a mouth map.

$$Mouth\ detection = C_r^2 .(C_r^2 - \eta . C_r / C_b)^2$$

Where $C_r$ is region of red color lips and $C_b$ is boundary of lips

$$\eta = 0.95 \times \frac{(1/N)\sum Cr^2}{(1/N)\sum (Cr/Cb)} \rightarrow (13)$$

Where n denotes the spatial size of the face-bounding box, $C_b$ and $C_r$ is chrominance of blue and red color.

Regions in the division represents the identified mouth map are the first point of detection. If various regions occur, they are then linked according to their proximity, forming an individual mouth map. These are then considered as the feature position of the mouth.

**Eye detection:** Human eyes have both black and white regions. Due to the presence of this, eye images exhibit higher variation in intensities. The below given equation (14) is used to calculate such variances. The distribution of these variances of different regions for the purpose of classification is given against the 2-dimensional position in the actual image. The resultant features show higher variance in some regions.

Variance=$(1/N)\sum(Y-\bar{Y})^2$ →(14)

Where $Y$ refers to the value of the intensity of every pixel in the region. $\bar{Y}$ refers to the value of mean intensity of the region. N refers to the spatial size.

**Nose detection:** Easy and generic properties make the characterization of nose to be simple. Some of these properties are: the base of the nose has higher contrast as well as grey levels when compare to the adjacent regions; they also have set of points with higher illuminance and symmetry values. Adding to these, the tip of the nose can be easily localized by the fact that it lies above the baseline and at the profile of the nose. These permit localizing the nose tip robustly.

**Feature extraction:**

1. RGB image is transformed into gray scale image

2. Noise removal and image sharpening are done using enhanced contrast and multidimensional filtering techniques.

3. Each image is decomposed into the Contourlet by means of transformation. So the output of Contourlet Transform results in both lower and higher frequencies. These frequencies in different scales as well as directions can also be attained. These coefficients have the same size $k \times k$ as Ct1,Ct2-1,Ct2-2…..Ctn-1,….CTn-v ,where N refers to the number of directions. The column vector $I_i$ of the images can be rearranged by using these coefficients. In the current work, two level of decomposition Ct1, Ct2-1,Ct2-2,Ct2-3 coefficients are used to build the feature matrix. Each coefficient has 32 × 32 resulting in a total of 1024 points.

4. The Feature matrix of the image I=$[I_1,I_2,I_3,\ldots,I_p]$ is built from the coefficients column vector $I_i$ here i represents the number of images and $p$ is pixels.

5. The matrix I is then reduced to a subspace which of lower dimension.

6. $S^w$ consists of weights that are computed for feature belonging to every image in the database.

### *Fusion level of encryption message and face features*

A feature vector from facial texture is extracted for the purpose of hashing. This along with double encrypted cipher text serves as inputs to the hash function which is employed to ensure message integrity. A hash function is a function that takes input as key and data and computes a value of fixed-length output called a hash value. Here, the inputs are encrypted message and face features from which hash value is generated. Some general encryption algorithms use the key to encrypt the secret message. MD5 hash function is used to generate the hash value from these inputs and these hash values are recomputed to ensure that the data that is stored is not modified. The key to the hash function is from the feature vectors from face which ensure that only an authorized custodian is requesting access to the data in addition to bimodal biometric authentication. The purpose of hash function is that if the computed hash value doesn't match with the original value, it means that either there has been a modification in the message or the face vectors that are retrieved does not belong to an authorized user. In the latter case, data decryption is denied and thus securing the same from an imposter. Thus, the hash value computation here serves as a validator for message integrity (Figure 5).

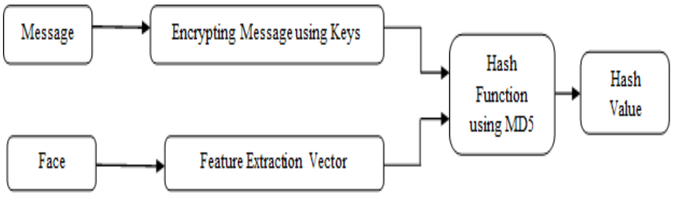

***Figure 5**. Message integrity using hash.*

The face feature vector is used to generate a cipher key for encryption and decryption. In encryption phase, the feature vector of a face is used to encrypt the input data. If the length of the face vector is N (256) and the variation of the threshold of the feature vectors from the same face is T, then the following steps are performed to encrypt the input message:

1. Consider the input message in encrypted form

2. Translate the feature vector from face into a fix length key

3. The values obtained in step 1 and 2 serve as input to the hash function

4. Hash values are computed and stored

The date that is stored in cloud becomes accessible to a custodian only if the message key and face features are matched. Otherwise, the decryption fails. Figure 6 describes the overall architecture of proposed system.

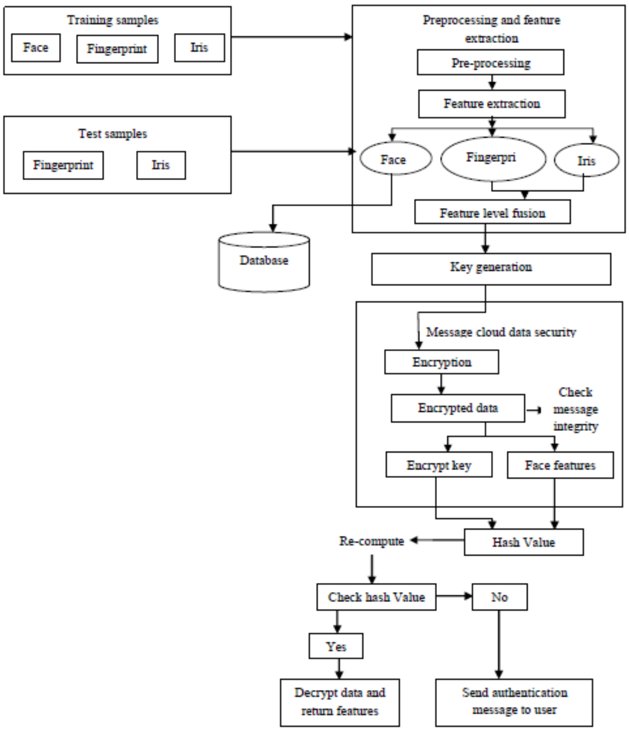

*Figure 6.* Overall block diagram of MBHC system.

## Experimental Results and Discussion

In order to perform the experiments, the fingerprint samples have been taken from databases whereas the iris images are acquired from CASIA Iris Image Database archived in Institute of Automation, Chinese Academy of Science [7]. The proposed approach has been verified for fingerprint and iris feature extraction, fusion, and segregated by proposed MBHC-AES with AFSA-SVM, and RBFSVM for unimodal also with the multimodal identification systems. The face features are estimated significantly and it is used to authenticate efficiently as an alternative means.

### *Comparison of recognition rates*

Figure 7 provides the performance metric of the proposed research work and is compared with existing system in terms of recognition accuracy. The x-axis includes feature dimensions and in y-axis recognition accuracy is plotted. From the results, it is proven that the fusion of the two modalities have higher performance significance. The result provides that the proposed MBHC-AES with AFSA-SVM approach gives higher recognition accuracy in comparison with other methods such as AFSA-SVM, RBFSVM and PolySVM.

### *Genuine acceptance rate*

It is defined as the ratio of genuine users accepted by the system. It is given by GAR=100-FRR. Figure 8 provides the performance metric of the proposed research work and is compared with existing system in terms of genuine accept rate. The feature dimensions are plotted in x-axis and recognition accuracy in y-axis is plotted.

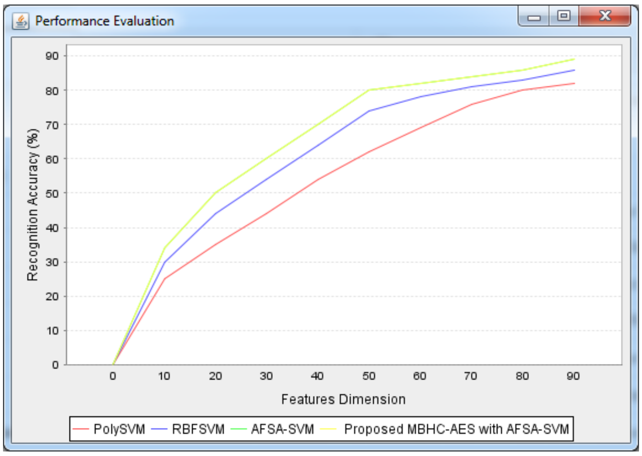

*Figure 7.* Recognition rate for different modalities.

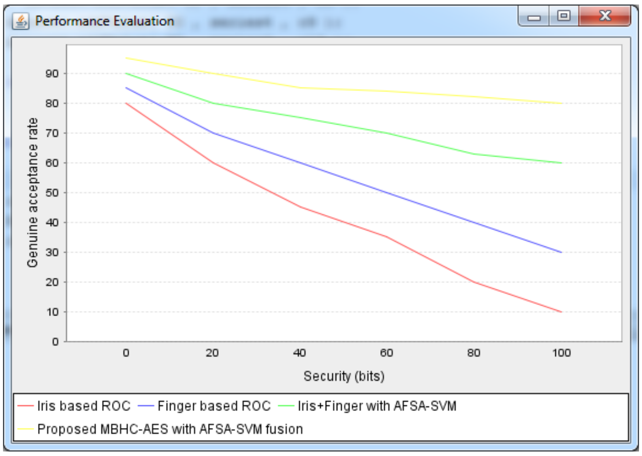

*Figure 8.* Genuine acceptance rate.

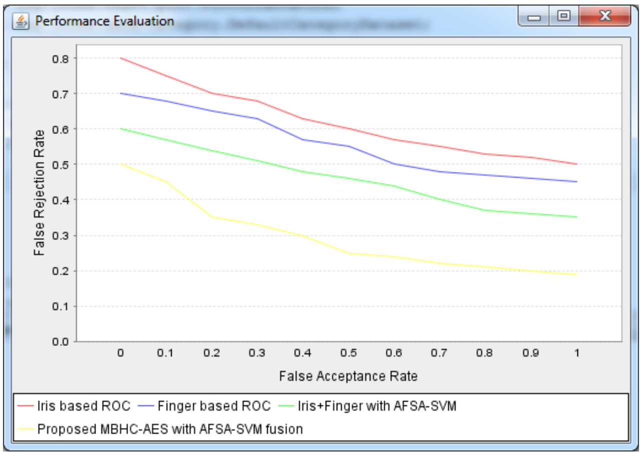

*Figure 9.* False acceptance rate vs. False rejection rate.

### *False acceptance rate*

The graphical approach for displaying the trade-off between False Acceptance Rate (FAR) and False Rejection Rate (FRR) of a classifier is referred as ROC curve.

$$FAR = \frac{The\ \ number\ \ of\ \ false\ \ acceptances}{The\ \ number\ \ of\ \ identification\ \ attempts}$$

$$FRR = \frac{The\ \ number\ \ of\ \ false\ \ rejections}{The\ \ number\ \ of\ \ identification\ \ attempts}$$

In Figure 9, the FRR is sketched along the x axis whereas FAR is sketched along the y axis. The experimental output confirms that the proposed MBHC-AES with AFSA-SVM fusion approach provides better authentication for cloud users.

### Error rate

A system is said to perform better when it exhibits lower error rates.

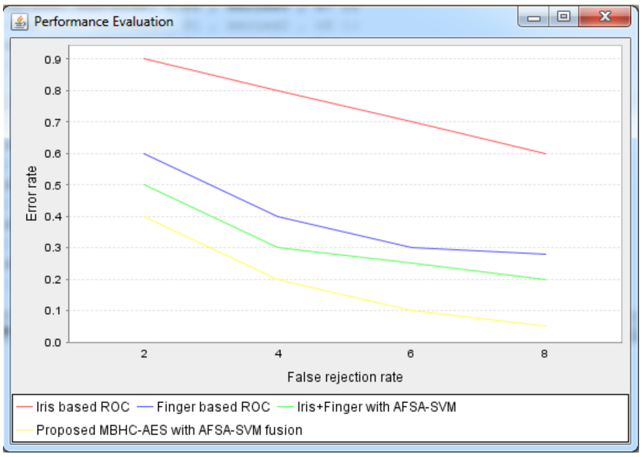

*Figure 10. Error rate.*

Figure 10 shows the error rate performance metric comparing the existing and proposed system. In x-axis, false rejection rate is considered and in y-axis error rate is plotted. The result in Figure 10 shows the performance rates of the extracted features for the iris, fingerprint and the fusion of the two modalities.

## Conclusion

In this research, Multimodal Biometric Hashkey Cryptography (MBHC) security framework with authentication and information security is proposed to ensure higher degree of security on cloud environment. The current research work employs multiple modalities for authenticating cloud users. The research work requires users to enrol for the cloud service by registering with three of their biometric traits. These templates after pre-processing are stored and used for ensuring security at various stages such as authentication, key generation, encryption, decryption and hash value computation. These templates are very specific to individual users that can neither be shared nor spoofed easily, thus not compromising security at any level. The best-suited methods of feature extraction of different modalities are applied to extract the most significant features from these modalities. This aids in better matching and recognition of users. Data security is made strong by using symmetric block-cipher AES encryption algorithm for which the users' traits serve as the keys. Thus, security is made strong in terms of authentication as well as data security. The results thus, prove that the proposed MBHC system achieves higher security when compared with the existing research work in terms of higher recognition rate and lower false acceptance and rejection rates.

## References

1. Subbarayudu VCM, Prasad MV. Multimodal biometric system. 1st International Conference on Emerging Trends in Engineering and Technology, 2008.
2. Ma L, Tan T, Wang, Y, Zhang D. Personal identification based on iris texture analysis. IEEE Transact Pattern Anal Machine Intell 2003; 25: 1519-1533.
3. Wang Y, Han JQ. Iris recognition using independent component analysis. Int Conf Machine Learn Cybernet 2005; 7: 4487-4492.
4. Jain AK, Prabhakar S, Hong L, Pankanti S. Filterbank-based fingerprint matching. IEEE Transact Image Process 2000; 9: 846-859.
5. Yang J, Xiong N, Vasilakos AV, Fang Z, Park D, Xu X, Yang Y. A fingerprint recognition scheme based on assembling invariant moments for cloud computing communications. IEEE Syst J 2011; 5: 574-583.
6. Ross A, Jain AK, Qian JZ. Information fusion in biometrics. AVBPA 2001; 1: 354-359.
7. Gawande U, Zaveri M, Kapur A. A novel algorithm for feature level fusion using SVM classifier for multi biometrics-based person identification. Appl Comput Intell Soft Comput 2013.
8. Nagar A, Nandakumar K, Jain AK. Multibiometric cryptosystems based on feature-level fusion. IEEE Transact Informat Forensics Security 2012; 7: 255-268.
9. Agarwal A. Secret key encryption algorithm using genetic algorithm. Int J Adv Res Comput Sci Software Eng 2012; 2: 216-218.
10. Sasidhar K, Kakulapati VL, Ramakrishna K, Kailasa-Rao K. Multimodal biometric systems-study to improve accuracy and performance. Int J Compute Sci Eng Survey 2010; 1: 54-61.
11. Anwar F, Rahman MA, Azad S. Multi biometric systems based verification technique. Euro J Sci Res 2009; 34: 260-270.
12. Mishra A. Multimodal biometrics it is: need for future systems. Int J Comput Appl 2010; 3: 28-33.
13. Hernández Alvarez F, Hernández Encinas L, Sánchez Ávila C. Biometric fuzzy extractor scheme for iris templates. Proceedings of World Congress in Computer Science, Computer Engineering, and Applied Computing, WORLDCOMP, 2009.
14. Garg R, Mittal B, Garg S. Histogram equalization techniques for image enhancement. Int J Electron Commun Technol 2011; 2: 107-111.
15. Chen SD, Ramli AR. Minimum mean brightness error bi-histogram equalization in contrast enhancement. IEEE Transact Consumer Electron 2003; 49: 1310-1319.
16. Zhang Z, Lyons M, Schuster M, Akamatsu S. Comparison between geometry-based and gabor-wavelets-based facial expression recognition using multi-layer perceptron. Third

IEEE International Conference on Automatic Face and Gesture Recognition, 1998.

17. Shrivas A, Tuli P. Effective analysis of iris images for iris recognition system. Int J Sci Eng Appl 2012; 1: 85-88.
18. Daugman J. Statistical richness of visual phase information: update on recognizing persons by iris patterns. Int J Comput Vision 2001; 45: 25-38.
19. Daugman J. Demodulation by complex-valued wavelets for stochastic pattern recognition. Int J Wavelets Multi Resol Informat Process 2003; 1: 1-17.
20. Ross A, Jain A. Information fusion in biometrics. Pattern Recognit Lett 2003; 24: 2115-2125.
21. Gan JY, Liang Y. A method for face and iris feature fusion in identity authentication. Int J Comp Sci Netw Secur 2006; 6: 135-138.
22. SreeVidya B, Pugazhenthi D. Multimodal Biometric cryptographic based authentication in Cloud Environment to Enhance Information Security. International Conference World Academy of Science Engineering and Technology, 2015.
23. Srinivasan M, Ravichandran N. A new technique for face recognition using 2D-gabor wavelet transform with 2D-hidden markov model approach. International Conference on Signal Processing Image Processing & Pattern Recognition (ICSIPR), 2013.
24. Hsu RL, Abdel-Mottaleb M, Jain AK. Face detection in color images. IEEE Transact Pattern Anal Machine Intell 2002; 24: 696-706.
25. Jemaa YB, Khanfir S. Automatic local Gabor features extraction for face recognition. Int J Comput Sci Informa Security 2009.

### *Correspondence to

Sree Vidya B

Research Scholar

Department of Computer Science

Bharathiyar University, Coimbatore

India