Dynamic Systems and Applications 30 (2021) No. 10, 1545 – 1559

OPTIMIZED DELBPA ALGORITHM FOR BINARY PATTERN BIOMETRIC KEY AUTHENTICATION IN CLOUD DATA PRODUCTION

KUMARI P[1*] AND THANGARAJ P[2]

[1*]Associate professor, Department of Computer Science and Engineering, Excel Engineering College, Komarapalayam, Tamilnadu, India.

[*]Email: pandikumari2020@yahoo.com

[2]Professor, Department of Computer Science and Engineering, KPR Institute of Engineering and Technology, Coimbatore, Tamilnadu, India.

Email: ctptr@yahoo.co.in

ABSTRACT. The global enterprise cloud computing services development and security need an organization to maintain and maintain critical digital data. It is the job of researchers who constantly challenge the security dimension of companies and cloud security solutions. Biometric systems provide automatic identification based on a single unique function and characteristic. Personal identities are established with the help of biometrics. Various biological features, such as irises, fingerprints, and faces, are recognized as false people identification. The uniqueness of the biometric information held by each individual is unique. Today, security is information, business, e-commerce, military, and other important factors. In the paper, to propose Deep Local Binary Pattern Recognition (DeLBPA) by analyzing the user's face shape and providing a face pattern-based key to user authentication protection. In the face, the image removed the noise and preprocessed using a bilateral filter algorithm. It uses the deep LBP algorithm to convert the user's face into a grayscale histogram image and divide it into binary value rows and columns to detect facial features. The training image set is converted to gray levels. The crossover operator is applied to multiple samples per person to produce a larger number of images. The biometric face system includes image capture, feature extraction, face pattern key generation, and verification process. In this work, a person can be certified to provide a calculated weight above a threshold. This overcomes the authentication problem when the relevant trait lacks real users or a poor-quality biometric input.

Keywords: Deep LBP, biometric key generation, encryption, bilateral filter, biometric authentication.

1. INTRODUCTION

Biometric authentication is the foundation of a secure identity and a personal authentication system. On the basis of confidentiality and biometrics technology solutions of the transaction, it will provide the security of data privacy. Biological evidence is very consistent, and it cannot be forged. Face detection (FR) is a computer-based application that detects people from digital sources, and from video sources to video verification. Images can be taken at different distances through some of the visual aids.

Features of the selected face from the image is compared to a pre-recognition process in the face database stored in the previously. This is a security system, and it has been used in the identification system and the marketing tool of companies. Compared with other biometric techniques, this method is most reliable, and it is effective. It has to analyze the features of the face image from the camera.

Pre-processing improves the quality, enhancement, and method of performing feature extraction functions in modified raw data models. Repeatable biometrics differed and were saved from the original data model. The quality of the biological samples obtained during the registration process is high.

Received DEC 17, 2020
www.dynamicpublishers.com;
www.dynamicpublishers.org;

ISSN1056-2176(Print); ISSN 2693-5295 (online)
$15.00 ©Dynamic Publishers, Inc.
https://doi.org/10.46719/dsa202130.10.01

During many re-registrations work, it is necessary to obtain the best biological model based on it. Biometrics are needed to retrieve the output of a component that is a biometric template.

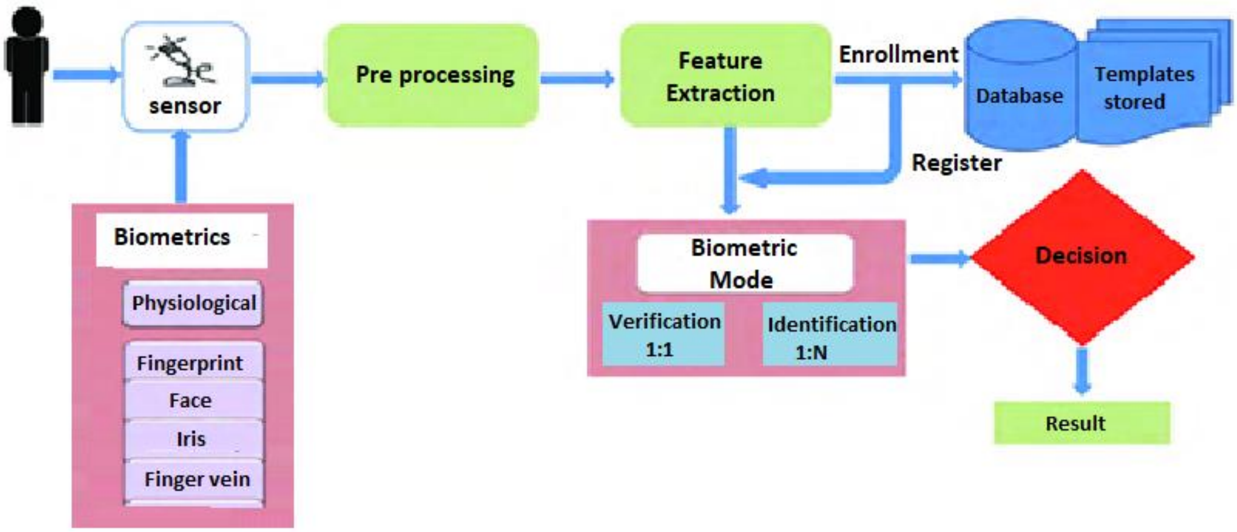


Figure 1. Biometric Identification System

In this face detection method to find and identify human faces in digital images. The biometric information extracted from the sample whose bio-operation principle is shown in Figure 1 above is compared with a reference template to generate a matching score. The biometric sensors to read the fingerprint, face, iris, and vein image. The images are removing the noise using preprocess method and to extract the features form image. Compare the templates created during the verification process with the list of candidate templates for the objection authorization process. The system-level determines the end result from the matching element. During the registration phase, some images are called user cramps and templates. The final model is based on the method used for authentication. The model for each user is stored in the database. During the authentication phase, the captured image is preprocessed. The verification process compares the claims with the mannequin input template. The feature vector is then compared to a previously stored feature in the sample database.

It allows to extract the relevant face image information and effective coding. This recognition is obtained by an internal texture in the image space spread by pixel values that are independent of the facial image data. The classical representation of a facial image is defined as the primary components of the coordinate system that is derived from it. The main part of the facial image's projects in space, to facilitate decision making, information compression, uncorrelated, and to achieve the dimensionality reduction. Mathematically, the main component of the distribution of feature vectors of the covariance matrix of a set of faces or facial images is found by the image carrier as a very high-dimensional surface treated.

Many biometric authentication systems can offer some flexibility in user authentication. It is assumed that a user with several different characteristics is involved in the system. Then, at the time of certification, only a subset of these traits can be retrieved based on application and user convenience considerations. For example, consider enrolling users into banking applications using face, voice, and fingerprint systems. During the authentication process, users can choose which features to present based on their convenience.

2. RELATED WORK

Biometrics is a great way to easily get rid of many of your product's security flaws. The captured images are processed through a procedure-filtering process to obtain the processed textures of many of these currently ubiquitous segmentation images in the expected speed. The submitted pattern can be easily compared with the processed image results.

A new method has been used and implemented, including 2-D red-black wavelet transform (RBWT), to extract novel multimodal recognition algorithm features (bi-orthogonal wavelet inverse transform). This method matches using a classification method to fuse facial, fingerprint, and iris features. The Canny Edge Detection (CED) method is applied to overcome and recover the actual ridge and valley structures of low-quality fingerprint images [1]. It is designed to fuse face, fingerprint, and iris information using a multimodal biometric system (MBS) weighting scheme. It will be enhanced by the Fourier transform of [2] the captured fingerprint images in a short time. The region of interest (ROI) is then matched by Euclidean distance matching calculated from the extracted features.

Fingerprints, iris, and facial features score levels, improve system accuracy. The captured fingerprint image is enhanced by the method of quality and histogram equalization in the Fast Fourier Transform (FFT) method. Optimal threshold segmentation for images is important [3]. Therefore, it can hide the frame multi-mode dictionary structure and create a differentiated stream. A plurality of joints can be a pre-activated sparse multimodal integration independent functional level. The algorithm is a function of multiple views, such as the performance of the multimodal biological function through the topical application, and the surface of different methods of achievement [4].

A new privacy protection ring learning with errors (RLWE) is proposed based remote biometric authentication scheme (RRBAS) in single and multi-server environments. RRBAS is the first lattice-based remote biometric system in a multi-server environment. Security RRBAS is resistant to well-known security attacks that meet the authentication key exchange (AKE) security random prediction model, which shows the analysis, and it is possible to provide quantum security [5]. And later the electrocardiogram (ECG) authentication method is introduced as a biometric security system suitable for verifying the identity of entering the building, and the RR interval-based ECG-based authentication method based on this research reconstructs the input data. Provide the limitations of learning biotechnology. In the overall performance (OP), the newly proposed performance measurement is a combination of performance measures combined with performance measures in one study [6].

The program provides strong authentication, supports legitimate user bios and passwords, and local phasing of dynamic server addition stages at any time. It uses the automation of Internet Security Protocol Validation and Application (AVISPA) tools [7] to demonstrate that the widely accepted formal security validation scheme is secure.

Gabor filter and mutual information maximization are used to extract low-dimensional features, while Bayes rule is based on a hidden Markov model (HMM) soft biological classification. Many soft biostatistical classification problems, for example, two different views, are defined as one-to-one and depending on the number of available library views [8]. The three-factor AKA method protects the anonymity and untraceable TMIS of users on multiple servers. It has established a three-factor authentication and key agreement (AKA) scheme and a telemedicine medical information system (TMIS), a security model for anonymous users on multiple servers, and provides a formal scheme for a formal security certificate [9].

The original pose remains unchanged, and the facial recognition problem is transformed into a partial frontal face recognition problem. Then, a robust tile-based surface display system was developed to represent composite surfaces. For each patch, transform the proposed method for multi-task learning in the dictionary [10]. The graph-structured database models the relationship between biological records. The label propagation method estimates missing values for two binary-valued resume attributes (for example, gender) and multi-valued resume attributes [11].

The author pays attention to EIS energy distribution information and improves the key distribution scheme based on physiological signals. First, various EI generation methods can be considered based on EDPS. It has proposed to modify the existing multi-window Fourier scheme and modify it based on generating a window that will improve the recognition performance of EIS [12].

This method has become innumerable because of this problem, making this model suitable for commercial use in some countries. They are starting from intravenous biometrics technology. This shows some of their attempts to show the most common steps in each of the major stages of these systems. What can be seen is that using the same database is not common in the literature and is a major issue in assessing the performance of new systems [13].

The ratio of the half-moon on the nail plate reflects human health. To maintain the image quality of the nail, it uses an image of the nail taken with a microscope. In addition to the arc shadow and nail plate, such a free edge, the details of the nails, such as horizontal stripes and vertical stripes, can be seen in apparent images taken with a microscope. More specifically, it means increasing the complexity of the displayed image and processing [14].

With commercial sensors and systems, key calculation methods in identifying toolchains, open data sets, open competition and open-source software, template protection schemes, demonstration attacks (S) (detection), sample quality assessment, mobile acquisitions are not only acquisition schemes, but Issue identification and template privacy are also the ultimate impacts of the disease [15].

Visual calculations like very simple concepts based on Sobel operator filters are used to find edges and simple noise reduction algorithms. These operations are very fast and produce very efficient processing and storage of binary images. In addition, this preprocessing can be regarded as a similarity measurement and evaluation task. It preprocesses one input, means that it is a dataset, all images for the fingers one after another [16].

It is an important reason for the effective fusion in an inconsistent scale of the three-peak image of the finger. Therefore, to develop a unified representation theory for the function of the finger is very important. The graphics-based feature extraction method for the finger biometric image A has been proposed. The three-finger method, based on the functional expression of the graph structure, can solve the mismatch problem of the feature space [17].

However, accurate measurement of relevant anatomy requires extensive outpatient observer variation. To resolve this issue, fetal head circumference (HC) and more than double the diameter of an automated system using a network measure recommended a complete change. An FCN (Fully Convolutional Neural) training and annotating the head with approximately 2000 2D ultrasound images provided by 45 different ultrasounds for semantic segmentation of conventional screening test heads [18].

Quality assessment methods have been used for iris recognition for adults, but none of them are considered iris recognition for children. The iris child admits that its non-cooperative nature is difficult because it may cause poor quality iris samples [19]. However, in a common framework, the evaluation results may lack a fair comparison between different methods. From one perspective, the increasing use of mobile devices has driven the development of the non-contact type organisms of two different non-contact hand database assessment [20].

3. IMPLEMENTATION OF THE PROPOSED METHOD

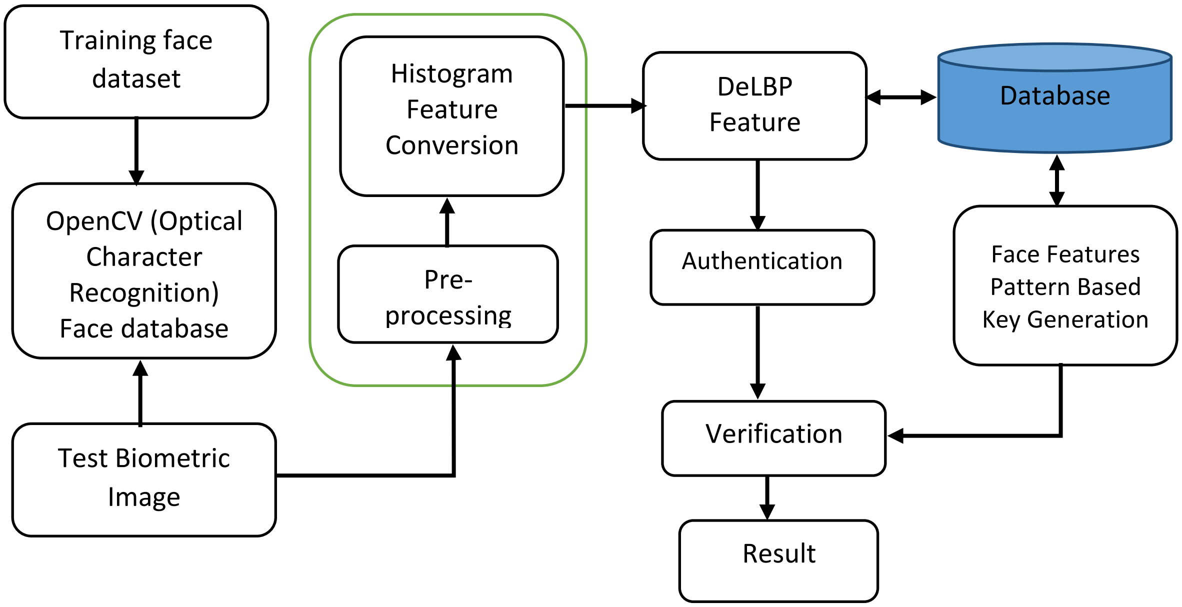

Training face dataset
OpenCV (Optical Character Recognition) Face database
Test Biometric Image
Histogram Feature Conversion
Pre-processing
DeLBP Feature
Database
Authentication
Face Features Pattern Based Key Generation
Verification
Result

Figure 2 Proposed Method Block Diagram

In the proposed DeLBPA is user face authentication system to provide security in the cloud framework. It allows us to extract the relevant face image information and effective coding. In this deep

LBP is analysis the deep pattern from face image and evaluate the binary mark to recognize the authorized user in cloud framework. This recognition is accomplished by culturing the subspace of the image space spanned by the face image data unrelated pixel value. Classic representation of the face image is obtained by highlighting in the coordinate system defined by the principal components. Projection of the face image to the main component parts on space, to facilitate decision making, information compression, uncorrelated, and to achieve the dimensionality reduction. Feature selection finds the most identifying information in the area of application. To characterize the desired pattern is to find simple extractions, noise insensitivity, and useful categories. After feature selection, the LBP value is assigned to the key generation process, the key based on facial binary pattern keys.

Figure 2 shows the proposed method DeLBPA block diagram. The input test image compares to the OpenCV face database and train face dataset. The image tested to eliminate the noise pattern image improves its image quality when the image is low using a bilateral filter. The preprocessed image extract facial features are converted to its pixels histogram values using LBP. The image pixel decimal value is converted to a binary value. The face feature binary values are using to generate the crypto keys helps to validate the authorized user in the cloud.

3.1.Preprocessing

The term "Preprocessing" the ability to filter the input image values in small neighborhoods of the same location in the broadest sense of the image values at a given location in the term. The basic idea of bilateral filtering is that traditional filters are made in the images of what to do in its domain. Two pixels may be identical to each other, occupy the space nearest to the nearest, maybe to each other, and have values that are close to the meaning of the method. This is very important for color image filtering. If the image is a three-band color filter, focus on near the edges of the image, without damaging each other. In fact, the different bands of different positions are different, and they soften. Independent tenderness can disrupt the color balance and make the color combinations appear unexpected.

Step1: Test face image *l*.

Step2: Preprocess the image using a bilateral filtration to remove the noise, blurs, or any grains in the acquired image.

Step3: By selecting the appropriate segmentation threshold converted grayscale image in binary format.

Step4: To group image pixels based on their intensities, the low-quality region.

Step 5: Initialize the all-value w, i to 0.

Step 6: compute the minimum intensity of image value

$$I_{min} = \min_{(x,y)\in S}(x, y)$$

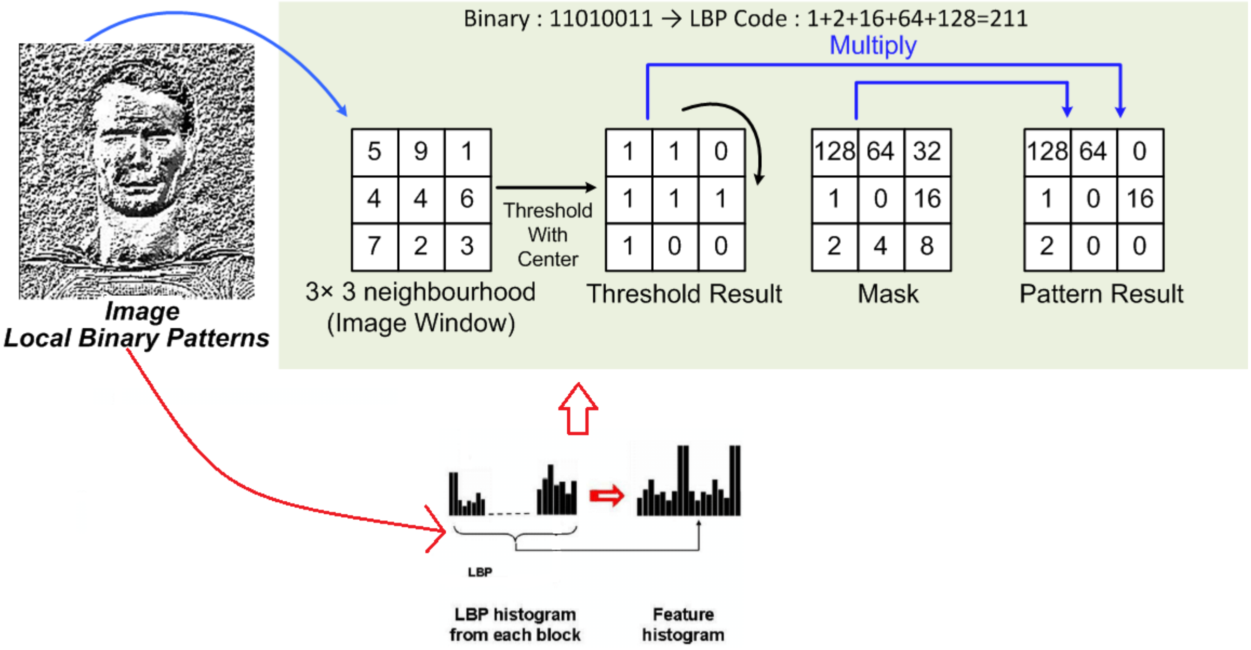
Step 7: for each $(x, y) \in S$ in the intensity of (x,y)

```
    Compute the image vector value (wi,w0) ← ((x,y)*/S)
    Compute the coordinate value (x,y) ← $\left[\frac{x}{s}\right], \left[\frac{y}{s}\right], \left[\frac{I(x,y)-I_{min}}{s_r}\right]$
Step 8: for each pixel $(x, y) \in S$ with an intensity $I(x, y) \in S$
    Interpolate function $w^b, i^b$
        $w^b, i^b(X.Y) \leftarrow \text{interpolate}\left(w^b, i^b, \left[\frac{x}{s}\right], \left[\frac{y}{s}\right], \left[\frac{I(x,y)}{s_r}\right]\right)$
Step 9: result
    $i^b(X, Y) \leftarrow \frac{w^b, i^b(X.Y)}{w^b(X,Y)}$
```

In the above algorithm, the step shows the image preprocessing step to enhance the image quality and remove the noise from the face image.

3.2.DeLBP Feature Extraction

The Deep Local Binary Pattern (DeLBP) method can also generate and process images that distinguish features that are too distinct from local. In fact, it is a real good choice for the face detection system. This DeLBP filtering technique is similar to the original image discovery, mainly for the purpose of decomposing and providing a target definition of differential images with the characteristics of indigenous people.


Binary : 11010011 → LBP Code : 1+2+16+64+128=211
Multiply
Threshold With Center
3× 3 neighbourhood (Image Window)
Threshold Result
Mask
Pattern Result
Image
Local Binary Patterns
LBP
LBP histogram from each block
Feature histogram

3× 3 neighbourhood (Image Window)

5	9	1
4	4	6
7	2	3

Threshold Result

1	1	0
1	1	1
1	0	0

Mask

128	64	32
1	0	16
2	4	8

Pattern Result

128	64	0
1	0	16
2	0	0

Figure 3. Image Binary Pattern model

In this deLBP process is shown in figure 3, the input image converts to binary histogram image and its transfer from decimal value. The main idea of DeLBP is to remove the resource sub-region of the original image to be extracted. Each field can be described as a "pattern" representing the texture of each region. These DeLBP features are extracted as a feature histogram in each region. As a follow-up, these features histograms are connected as a single feature histogram representing the face image. As shown in Figure 3, each histogram shows the method that the original DeLBP operator used to extract from each region, and the function of this area is how to form the final image feature vector. The original DeLBP operation is a 3x3 window for extracting the feature vector of each area. For each pixel, the center pixel of the window is used as the threshold. Thus, each feature list is based on the surrounding pixels and patterns. In the convolution of various groups of binary patterns of surface transformed images. The DELBA convolution expression is as follows:

$$O_{\delta,f}(F) = I(F) * \vartheta_{\delta,f} \tag{1}$$

Where $\vartheta_{\delta,f}$ is transformed by various gradation distribution images and LBP kernels described in (R, C). Then F = (R, C) * represents the convolution operator. This result reveals a typical feature of registration discrimination near spaces. All these obvious extracted feature vectors are obtained by summarizing the construction of improved DeLBP feature vectors.

3.3.Face Features Pattern Based Key Generation

Security of key management key generation based on binary facial function, distribution, and storage mode. Today, attacks that are a function of public-key schemes are often thought to focus on the important responsibility of encrypting their algorithms in computer security, rather than key management. Effective details of face patterns are stored in the database and are the only feature templates for the location of facial feature points. Let us consider a binary pattern of two faces of a single user to generate a cryptographic key. The binary pattern of these facial features, namely BPa and BPb, is retrieved from the database and as BPa = {BP1, BP2, BP3, ... BPm} and BPb = {BP1, BP2, BP3, ... BPn}. Where BP1, BP2, BP3, ... BPm and BP1, BP2, BP3, ... BPn, represent the position of each group (r, c) Details. Km, the distance between two details is defined as BPi and BPj, and its formula is

$$\text{Km}=\sqrt{BPi - BPj}\Big/(BPi - BPj)^2$$

Where, (BPi, BPj) are binary coordinate points E and F.

The Cryptographic systems are implemented using one or face feature-based cryptographic algorithms. These solutions often use feature-based symmetric and asymmetric key encryption, so that face feature-based asymmetric keys are used at both ends of the asymmetric key channel for a group, and then these symmetric keys are used to encrypt the content.

Steps:

Start: Binary pattern (BP), Pi=key pattern, XoR Operation, eL left key, fR, Right key.

```
    eL, fR are two 32-bit halves of e
    For i = 1 to 16:
        eL = Pi(BP) XOR XL
        eR = fR XOR F(XL)
        fR and XL are swapped
        fR and EL are swapped (The key will swap to end)
    end for
    fR = P17 XOR fR
    xL = P18 XOR xL
    Again combine Xr and eL
End
```

Choosing to keep the math function of these feature-based keys is believed to belong to the family's common hash function, and the performance of the encryption integrates with the confirmation of erasure of properly encoded data. It has the ability to repeat 16 times more than the network. Each round of key-dependent exchange involves the use of keys, and the exchange is data-dependent. Each operation is performed by 64-bit word addition and XOR. Only for each round, there is a lookup table for additional driving data 4 index array.

4. RESULT AND DISCUSSION

The evaluation of a complete biometric identification system is a complex and laborious task. There are currently no widely accepted methods for reporting the results of biometrics studies. The DeLBPA algorithm is designed to recognize faces by applying the databases. This will change the total number of samples retained even if check the individual settings. There are currently no widely accepted methods of reporting the results of biometrics studies. Therefore, in our study, the focus of this section gives the only matching performance of the biometric system. Security performance was measured based on algorithms that provide accurate encryption and decryption support.

Table 1. Simulation Parameters

Parameters	**value**
Language	C#
Tool	Visual studio framework
Back end	SQL Server
Face Database	OpenCV

Table 1 shows the simulation parameter used in the proposed method. In the simulation developed in dot net frame 4.0, work with SQL server and the face image compare using the OpenCV database.

4.1.Analysis of FRR and FAR

False Acceptance Rate (FAR): Also known as type I error or false positive. This demonstrates the potential of FAR for fraudulent users (i.e., scammers) to access protected resources. In this false Rejection Rate (FRR): also known as Type II error or false negative. FRR indicates that authorized users may be denied access to protected resources. Equal Error Rate (EER): The relationship between FAR and FRR has been described as mutually exclusive because it is impossible to refuse, and two accept the same authentication attempt. To analyzed the proposed method, BFTC, and fusion method to prove its efficiency.

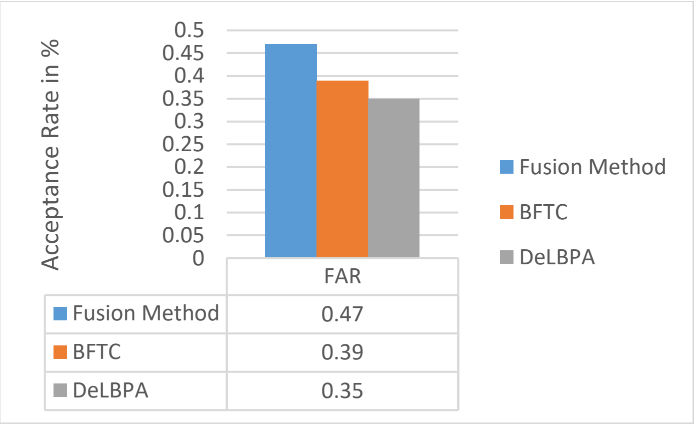


Figure 4 False Acceptance Rate

Figure 4 shows a comparative graph of the false acceptance rate in the proposed cloud security framework. The proposed method DeLBPA is 0.35 % of low FAR compare to the existing method BFTC is 0.39%,and the Fusion method is 0.47%. In this proposed method, DeLBPA is a less false rate compare to others.

In the above Figure 5 graph is shown the FRR of the existing fusion method and the BFTC proposed method comparison analysis. The proposed method BFTC is 95.7% of FRR more efficient, and the existing method fusion method has a 93.3% rate.

4.2.Time Complexity

The performance on time complexity introduced by the various algorithms in the biometric authentication process has been measured at different conditions. The measured results have been compared and presented below:

Time complexity= (N*(N-1))/ (Total processing time)

Where N=number of the image.

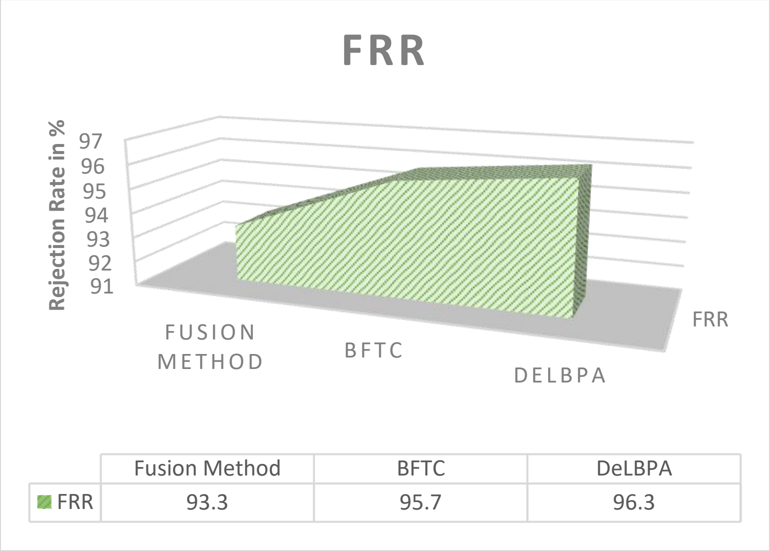


Figure 5 False Rejection Rate

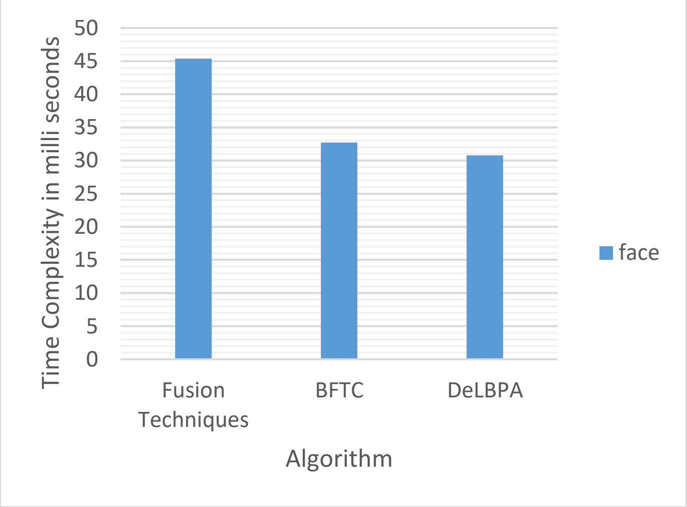


Figure 6 Time Complexity

The time complexity analysis of the proposed and existing method is shown in Figure 6. The proposed method DeLBPA is 30.8 ms less time to authentication compare to the existing method Fusion method and BFTC.

Figure 7 shows the incidence of poor performance is measured and compared with the results of the different methods. It have suggested that the BFTC algorithm is unlikely to produce false values. The proposed method DeLBPA is an 8.1% lower false ratio, compared to existing methods BFTC is 10.4% and fusion method.

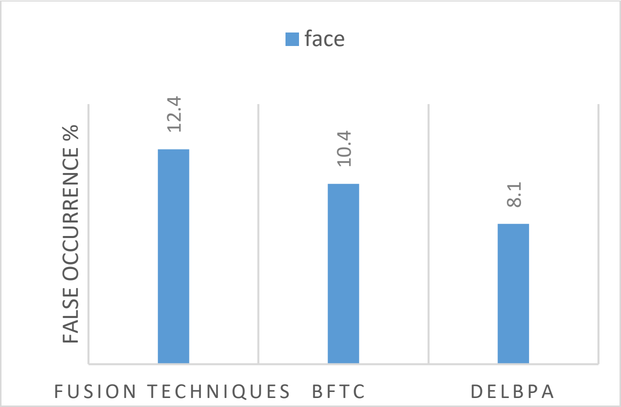


Figure 7 False Analysis

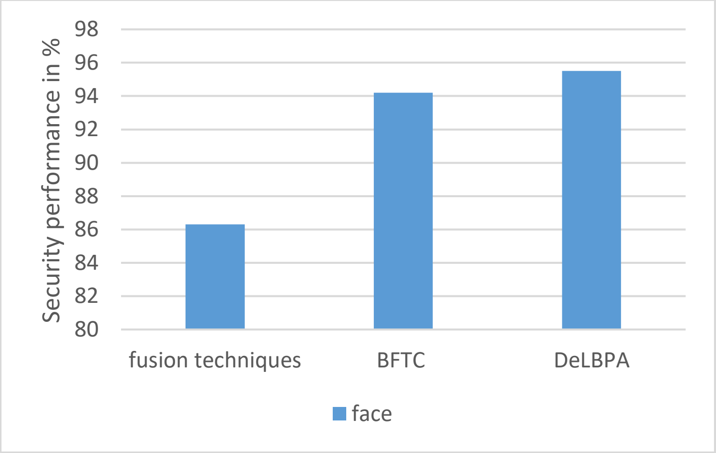


Figure 8 Security Analysis

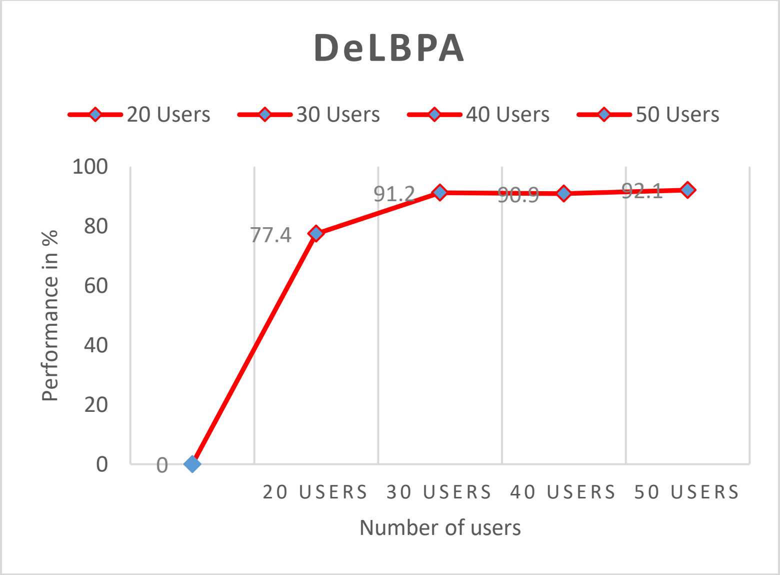


Figure 9 Authentication Performance

The performance of security enforcement was measured, and the results were compared using different methods. Both the proposed DeLBPA algorithm has achieved higher performance than other methods. Its analytical performance is shown in Figure 8.

In above Figure 9 shows the authentication performance of the multi-model biometric system. In this proposed method, the DeLBPA analysis result shows the different user authentication for 92% of efficiency for 50 number of the user. Similarly, 77.4% of authenticating performance for 20 number of users.

5. CONCLUSION

Multimodal biometric technology is popular for performance and security. This study demonstrates the problems associated with multiple biometric authentication systems. The combination of multiple biometric features improves system performance. In this work, optimal DeLBPA in a multimodal biometric system is recommended to identify authorized users using face image. In LBP, remove noise from the image by extracting the binary mode and feature in the face image and bilateral filler using advanced image quality. This proposed method is a combination of biometric and faces feature-based crypto core generation to improve user cloud security, and the proposed method of simulation results analysis is compared with other existing methods, providing high performance. Further investigation can use a large database, and the image is not preprocessed, an on-site database, so the noise includes it. The proposed technique can also be used for other biometrics to identify the effects of the face on similar images. The investigation can also be done with a discrete wavelet transform. The combination of multiple biometric features improves system performance. Future improvements in acquisition technology and the availability of algorithms and industry standards will certainly ensure a bright future biometrics technology.

REFERENCE

[1]. Saxena, J, Kaur, R, and Singh, S. "Multi-modal Biometric System for Person Identification using Wavelet Function" 2014 International Journal for Research in Applied Science & Engineering Technology (IJRASET): 2(XII) ISSN: 2321-9653.

[2]. Shalini, Verma, Dr. Singh, RK. "Multimodal Biometrics Information Fusion for Efficient Recognition using Weighted Method" 2014 International Journal of Engineering Research and General Science: 2(4): 582-88.

[3]. A Kamal, Aboshosha, EL, and Karam. EA, A, Dahshan "Score Level Fusion for Fingerprint, Iris, and Face Biometrics." 2015 International Journal of Computer Applications (0975 – 8887) 111(4): 47-55.

[4]. Nasrabadi, NM, Bahrampour, S, Jenkins. WK. Ray, A "Multimodal task-driven dictionary learning for image classification" 2016 IEEE Transactions on Image Processing 25(1): 24-38. DOI: 10.1109/TIP.2015.2496275.

[5]. Wang, C., Fu, X, Yao, H., Wu, B., & Li, F, Liu, C"A Privacy-Preserving RLWE-Based Remote Biometric Authentication Scheme for Single and Multi-server Environments" 2019 IEEE Access, 1–1.

[6]. S.-K., Kim, Yeun, Yoo, P. D C. Y "An Enhanced Machine Learning-based Biometric Authentication System Using RR-Interval Framed Electrocardiograms" 2019 IEEE Access, 1–1. doi:10.1109/access.2019.2954576.

[7]. Roy, S., Das, A. K., Chatterjee, S., S., Kumar, N., Chattopadhyay & Vasilakos, A. V "Secure Biometric-Based Authentication Scheme using Chebyshev Chaotic Map for Multi-Server Environment" 2016 IEEE Transactions on Dependable and Secure Computing, 1–1. doi:10.1109/tdsc.2016.2616876.

[8]. Wang, Y., Hu, M., & Zhang, Z "Maximization of mutual information for gait-based soft biometric classification using Gabor features" 2012 IET Biometrics, 1(1), 55. doi:10.1049/iet-bmt.2011.0004.

[9]. Yun-Hsin Chuang, Chin-Laung Lei, "Privacy Protection for Telecare Medicine Information Systems with Multiple Servers Using a Biometric-based Authenticated Key Agreement Scheme," 2019 IEEE Access, Volume: 7, Page no: 186480 - 186490.

[10]. Chang Xu, Changxing Ding, Dacheng Tao" Multi-Task Pose-Invariant Face Recognition" 2015 IEEE Transactions on Image Processing, 24(3), 980–993.

[11]. Ross, A. Swearingen, T" Label propagation approach for predicting missing biographic labels in face-based biometric records" 2018 IET Biometrics, 7(1), 71–80.

[12]. Bao, S.-D., Miao, F Li, Y. "Biometric key distribution solution with energy distribution information of physiological signals for body sensor network security" 2013 IET Information Security, 7(2), 87–96.

[13]. Blanco-Gonzalo, R., Alvarez-Nieto, A., Tirado-Martin, P & Romero-Diaz, A" Image processing techniques for improving vascular hand biometrics" 2017 International Carnahan Conference on Security Technology (ICCST), pp – (15-21).

[14]. Yang, Lee, S.-H., T.-W., & Yeh, C.-H. C.-S., Hou, "An image preprocessing method for fingernail segmentation in microscopy image" 2017 IEEE 2nd International Conference on Signal and Image Processing (ICSIP), pp – (489-493).

[15]. State-of-the-Art in Vascular Biometrics: Upcoming Modalities and Challenges in Image Processing. (2019). 2019 Ninth International Conference on Image Processing Theory, Tools, and Applications (IPTA).

[16]. E. O., Porcino, T. M, Silvah, A. C. Rodrigues, Conci, A., "A simple approach for biometrics: Finger-knuckle prints recognition based on a Sobel filter and similarity measures" 2016 International Conference on Systems, Signals and Image Processing (IWSSIP), pp – (1-4).

[17]. Li, S., Zhang, H., Yang, J, Shi, Y" Graph Fusion for Finger Multimodal Biometrics" 2019 IEEE Access, 7, pp -(28607–28615).

[18]. Matthew, J., Baumgartner, C. F., Sinclair, M., Bai, W., Martinez, J. C., Li, Y. Rueckert, D. " Human-level Performance on Automatic Head Biometrics in Fetal Ultrasound Using Fully Convolutional Neural Networks" 2018 40th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), pp – (714-717).

[19]. de Kock, Mabuza-Hocquet, G., A, Nelufule, N., Moolla, Y." Image Quality Assessment for Iris Biometrics for Minors " 2019 Conference on Information Communications Technology and Society (ICTAS), pp - (1-6).

[20]. B., Viana-Matesanz, Rios-Sanchez, M., & Sanchez-Avila, C "A comparative study of palmprint feature extraction methods for contact-less biometrics under different environmental conditions" 2017 International Carnahan Conference on Security Technology (ICCST), pp - (1-6).