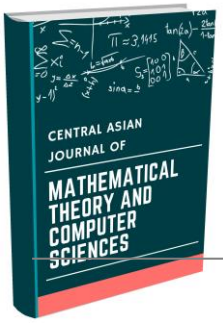


CENTRAL ASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES
https://cajmtcs.centralasianstudies.org

Volume: 04 Issue: 3 | Mar 2023 ISSN: 2660-5309

AN AUTHENTICATION MODEL FOR CLOUD STORAGE SERVICES BASED ON FINGERPRINT RECOGNITION

Mustafa A. Naser, Sadiq Obied Redywi, Saad O. Ajmi Al-Shuwaili
Ministry of Education of Iraq, Thi-Qar Education Directorate
mnstafaabd@utq.edu.iq, sadiq.o.rrdawi@utq.edu.iq, Saaed.o.alajmi2008@utq.edu.iq

Abstract

Over the past several years, cloud service becomes one of the major subjects of IT, and the major topic is cloud data storage, due to the advantages of cloud service such as flexibility, mobility, costs saving, and easy to use. Cloud services provide multiple services to users over the internet. These advantages drove individuals and organizations moved their applications, data, and services to the cloud storage server. The main concerns of these services are security and privacy when the individuals and organizations are saved private data or information (sensitive data or information) in untrusted servers because of the traditional methods that used to authenticate users such as passwords, tokens and digital certificate these credentials may be often be stolen, wrongly revealed or difficult to remember, thus companies and individuals require a secure method to authenticate their users in order to ensure the functionality of their services and data saved in the cloud storages are working in a secure environment, and prevent leakage any information for users and individuals to any untrusted party. In this paper, propose a biometric-based security and authentication paradigm to help user's authentication in the cloud storage environment,used fingerprint as a biometric to an untrusted user to login to the cloud services.

ARTICLEINFO

Article history:
Received 6 Jan 2023
Revised form 5 Feb 2023
Accepted 16 Mar 2023

Ключевые слова: *Cloud computing, cloud storage service, Biometric ,fingerprint, Ridge-End, Bifurcation Points, Encryption, Decryption.*

1-Introduction

In the past several years, the Internet has been appearing on network schema by a cloud symbol until 2008 when a diversity of new services begins to appear that allowed cloud resources to be accessed over the Internet named the cloud computing. Cloud computing includes activities such as the utilize of social networking webs and other forms of personal computing; nevertheless, most of the time cloud services are interested with accessing software applications over the Internet, data storage, and processing force. Cloud

computing is technical to increasing the capacity or add susceptibility dynamically without, wanting to invest in new infrastructure, training new users, or licensing new software. It increases Information Technology's (IT) existing susceptibility. Nowadays, cloud computing has grown from the begin of a hopeful business idea to one of the rapid-emerging technical of the IT industry [1]. It is the modern idiom for the extend-dreamed view of computing as a helpful tool. The cloud supplies suitable, on-demand network arrival to a centralized set of configurable computing resources that can be quickly deployed with senior efficiency and lower management overhead. With its wonderful benefits, cloud services enable a major model shift in how we diffuse and transfer cloud services that is, it makes sensible computing outsourcing such that both users and companies can avert committing big capital outlays when buying and managing software applications and hardware, as well as dealing with the operational overhead therein [2].

The US National Institute of Standards and Technology (NIST) has defined cloud computing [3]:**" A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction".** It is considered a very effective, suitable and centralized sharing pool through which computer resources can be deployed and accessed with minimum overhead. The most often utilized models of cloud computing sharing services are Dropbox and Google Drive [4].This cloud paradigm consists of five major characteristics, three service paradigms, and four deployment paradigms.[5].

The five main characteristics are defined as

- On-demand self-service
- Ubiquitous network access
- Resource pooling
- Rapid elasticity or expansion
- Measured service.

The service paradigms are defined as

- Cloud Software as a Service (SaaS)—Use providers applications over a network.
- Cloud Platform as a Service (PaaS)—Deploy customer-created applications to a cloud.
- Cloud Infrastructure as a Service (IaaS)—Rent processing, storage, network capacity, and other fundamental computing resources.

The deployment paradigms, which can be either internally or outlay performed, are abstractly in the NIST definition as (see figure 1)

- Private cloud—Enterprise owned or leased
- Community cloud—Shared infrastructure for specific community
- Public cloud—Sold to the public, mega-scale infrastructure
- Hybrid cloud—consist of two or more clouds.

Cloud services have benefits in the arrival of services at low cost and easy adaptability. It provides significant services efficiently, yet, small difficulties are present in it. General security attentions, synchronization, versatility, and replication are essential problems in cloud services. Data repetition involves many duplicates of the same data in different servers. In distributed computing data repetition is putting away many duplicates of the same data on different servers, locally or at distant destinations. In the case that information is available at one place (site), at this stage, it would be exceptionally fishy to deal with the prerequisites for bringing to the data. The server will face a load case and the system performance may degrade [6].

Also, the main issue before allowing a person to accesses a service of cloud is the authentication. Different techniques are used for this purpose such as fingerprint, iris, palm print, face recognition. But, still, there is no an ideal technique that provides a very high authentication accuracy. In this paper, we present a precise and sufficient method by creating an authentication system to recognize the user who has the right to access very secure and important facility using fingerprint to recognize the users. In this work, we used limited databases of a finger. FVC_2002 finger database, FVC_2004 Finger database. We took eight samples for each person for finger We used Euclidean distance in the matching and apply a threshold to match and recognize the authorized person.

2. Literature Review

The security concerns on cloud services have been currently being most discussed in the company, academia, and industry researches. Many global conferences have focused on this topic alone, for example, the ACM Workshop on Cloud Computing Security, the International Conference on Cloud Security Management, and the only European conference on the topic, Security Cloud services, which already had three layers. Thus, many scientific contributions have been deployment not only on conferences proceedings but also in international journals. As such, several surveys on this area of knowledge have also been published. [7].

Zhou et al. (2010) [8] work a survey on the security and privacy problems of several cloud services providers. Security and privacy were debated alone. However, the first was studied with a focus on availability, confidentiality, integrity, control, and auditing characteristics, the second was debated by listing out-of-date privacy acts. In addition to this, little concerns related to multi-server storage were also debated.

Vaquero et al. (2011) [9] presented a deep view of IaaS clouds security services concerns. The research focused on the security concerns that multi-tenancy gets to cloud computing services while analyzing them from the Cloud Security Alliance (CSA) point of view, that is, by classification security research according to the CSA big threats to cloud computing deployment in 2010. Their work involved showing security from the networking, virtualization, and physical sides of cloud IaaS nets.

Gonzales et. al (2011) [10], has been used cloud-based biometrics, but, focuses on how to keep the biometric data from miss-utilize by using a crypto-biometric system.

Yassin et al. (2012) [11] suggested an authentication approach utilizing three items: data owner, users, and service provider (SP). In their approach, a person does not need to register with his/her password at the SP. This approach supplies the secrecy of the session key.

Tsai et al. (2015) [12] proposed an authentication model for mobile cloud computing (MCC). Their approach supplies security to mobile users to reach multiple cloud computing services from multiple SPs by utilizing a single key. Their approach is as well able to supplying mutual authentication key exchange, and user identity.

3- User Authentication in the Cloud

When implementing authentication over the Cloud, the principal ((the user, machine, or service requesting access) will be submitted a credential [13]. In the case of the credentials match, the user is pliable to access the services it subscribed to from the service providers. There are many kinds of credentials the users can present to evidence their identity. Shared-key is typically password used protocols such as Password Authentication Protocol (PAP) [14] and Challenge Handshake Authentication Protocol (CHAP) [15]. A digital certificate is the second kind of credential that able to supply robust authentication in the cloud environment. It is an electronic document that utilized a trusted Certificate Authority (CA) to blind the encryption key with an identity [16]. Another kind of credential is usually used one-time-password (OTP) [17,18]. In this paper, the credentials of the users are a username and password, fingerprint.

4- Proposed Approach

In our proposed approach, the authentication operation is based on two credential data: (a) user's biometric (fingerprint) (b) the username and password. Both parts must be match to unsure of user's identity. We combine some parties (User, client, service provider) to collaborate together to implement the matching process between the feature vector and the biometric template that stored of the user, Figure (2) describe the players in the proposed approach.

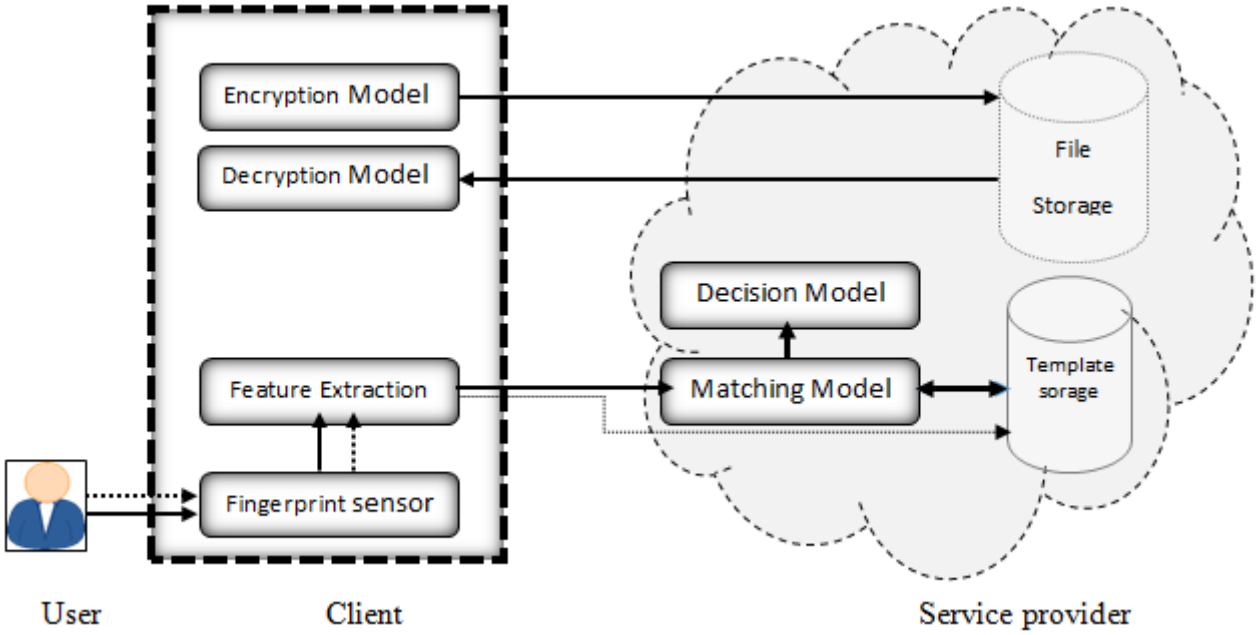


Figure (1): Illustrate of our - Proposed Approach, dashes arrows refer to the Enrolment phase.

- User: The person that sends the authentication demand.
- Client: PC or workstation with Internet arrival.
- cloud storage service: company or organization that supply cloud services (SaaS, PaaS, IaaS) to the user.

Reverse the traditional biometric authentication systems, the template is the converted feature vector and will be saved in the cloud storage. The query feature vector is a converted feature vector. similar most presenting biometric-based authentication systems, our solution composed of both the enrolment and the verification operations. In the next part, we will illustrate the components and the authentication workflows of our proposed approach.

The Client has the Following Components:

- Sensor: scans the biometric feature(fingerprint) of the user.
- Feature extractions: extracts the feature vector (Minutiae points) from the scanned biometric data.
- Encryption model: encrypts the data who the user wants to be stored in the cloud storage.
- Decryption model: decrypts the data who the user wants to be downloaded from the cloud storage.

The server in the cloud has the Following Components:

- Matching Model: compared the feature vector of the user with the template stored in the database.
- Decision Model: making the final decision by comparing the templates with the given threshold.
- Templates storage: saved the template of every user.

The proposed model includes the enrolment process and verification process as workflows as explain in the next sections:

4.1 Enrolment Operation

The aim of the enrolment operation is to treat the scanned biometric data and extract a set of a feature vector to be saved as the template for the user. The enrolment operation is required for the fresh user who desires to enter the cloud service. Fig 3 describes the overview of the enrolment operation.

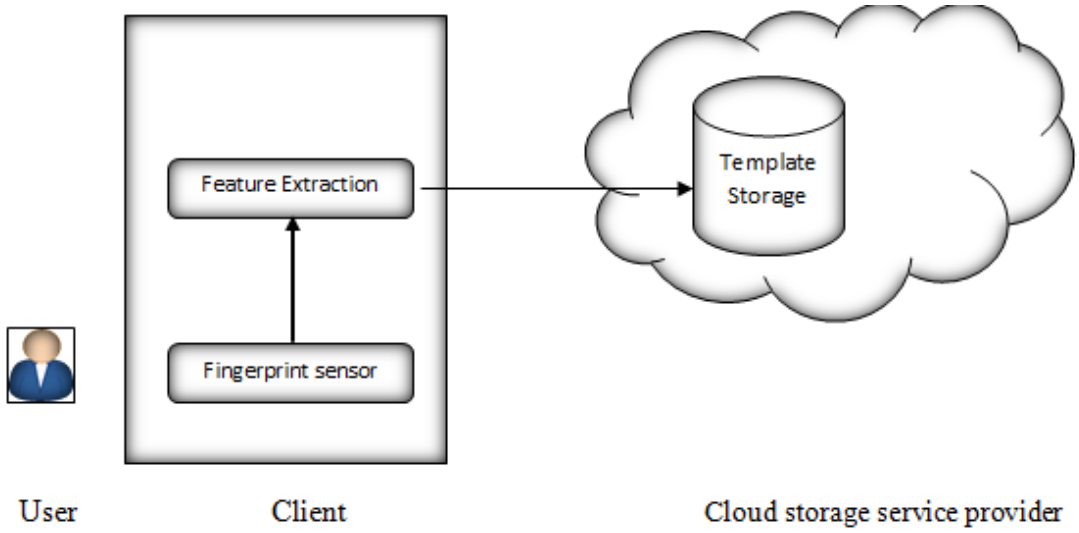


Figure (2): The overview of the enrolment operation

Steps of the Enrolment operation

1) The person enrolled in the cloud will be submitted a credential (username, password, and fingerprint), to subscribe to the service.
2) The fingerprint sensor scans the fingerprint (as an image) for the person.
3) The feature extractor processes the scanned fingerprint data to extract the feature vector of the person $X=\{x_1,x_2.....x_n\}$.
4) The feature extractor sends the X vector to the database in the service provider.
5) The service provider stored templets of all persons in the database.
6) The previous steps repeated to any user who wants to enroll the cloud service.

4.2 Verification Operation

When the person requires to arrive at data stored in the cloud storages or utilized the cloud services, the user must submit proof of their identity. The verification operation is responsible to verify the users who they claim to be. Fig 3.3 describes the overview of the Verification operation.

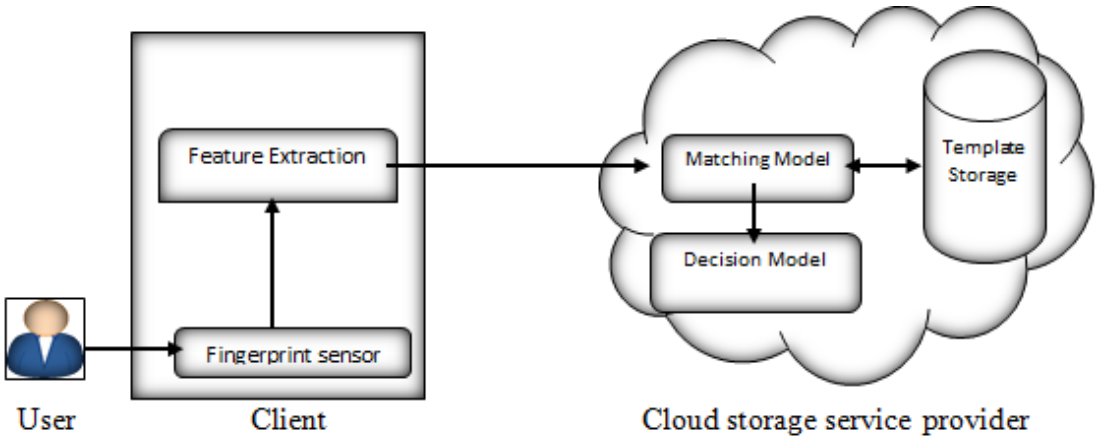


Figure (3): The overview of the Verification operation.

Steps of the Verification operation:

1) The person inputted to the service by username, password and, fingerprint.
2) The fingerprint sensor scans the fingerprint (as an image) for the person.
3) The feature extractor processes the scanned fingerprint data to extract the feature vector of the person, $Y=\{y_1,y_2.....y_n\}$.
4) The feature extractor sends the Y vector to the matching model of the service provider.
5) Next, the service provider retrieves the templates of the person based on the person's ID from the database.
6) The Matching model comparing the features vectors sent from the client with the templates stored in the database and making the decision.
7) Finally, the decision Model makes the decision as follows (S is the similarity score, t is the threshold determined by the service provider):

$$Decision= \begin{cases} Accept,\ if\ S< t \\ Reject,\ if\ S>t \end{cases}$$

Note that for several authentication demands, we might require many security levels. Therefore, our approach can assign different threshold values for different persons.

4.3 Encryption & Decryption operation.

As previously mentioned, the client has the Encryption and Decryption model, now we discuss these operations in detail. In this thesis, use the Public-Key Cryptography (RSA Algorithm). Fig 3.4 describes the overview of the Encryption and Decryption operations.

4.3.1 Public-Key Cryptography (RSA Algorithm):

The main idea of public-key cryptography is public keys. Each user's key is discrete into two parts: a public key for encryption available to everyone and a secret key for decryption, which is recorded secret by the owner. The most important examples of public-key cryptosystems are the RSA, ElGamal, and Rabin cryptosystems, in this thesis, using the RSA algorithm to Encryption and Decryption for the data who the person wants to store it in the cloud.

RSA algorithm comprises three main procedure as following:

1) Key Generation: The RSA algorithm includes a public key and a private key. The public key is utilized for encryption of the file and the private key is utilized for decryption of the file. The key generation generated as the following:

a) Randomly choose two prime numbers *p* and *q*.

b) Calculate the modulo n by using the following mode n = p * q.

c) Calculate phi (n) by using Euler's totient function phi (n) = (p – 1) * (q – 1)

d) Select the public key exponent *e* such that 1 < e < phi (n) and e and phi (n) are coprime which means that GCD (e, phi (n)) = 1.

e) Calculate the private key exponent *d* using the following formula:

d = e ^ -1 mod (phi (n)).

It means that d is the multiplicative inverse of e mod (phi (n)). So (d) can be compute as follows: e * d = 1 * mod (phi (n)).

Thus, we obtained the public key and private key as follows:

Public key: (n, e) .

Private key: (n, d) .

2) The encryption process:

For encrypting a file, we use the following equation:

Encrypted file = file ^ e mod (n). (1)

3) The Decryption process:

For encrypting a file, we use the following equation:

Decrypted file = file ^ d mod (n). (2)

Thus, find that we obtain the same file, which was uploaded in an encrypted file after decryption by utilizing the RSA algorithm**.**

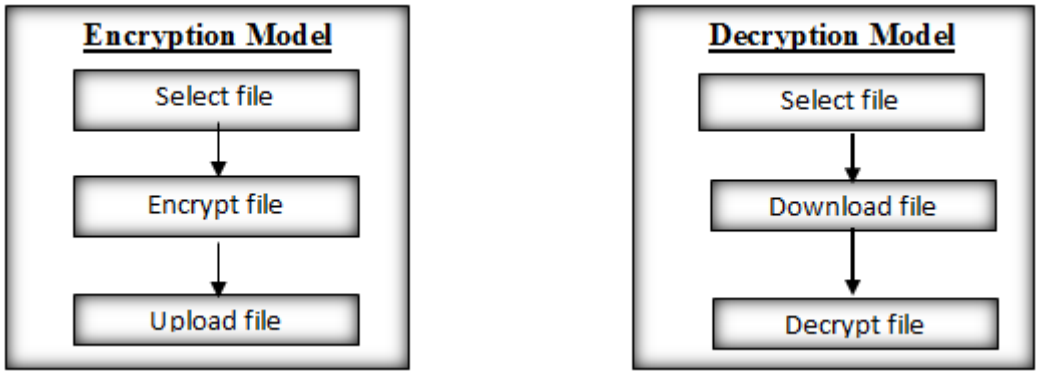


Figure (4): Illustrates the Encryption & Decryption operation.

Steps of the Encryption operation**:**

1) The person selects the file that wants to store it in the cloud and send it to the Encryption model.
2) The Encryption model encrypts the file using the RSA algorithm.
3) The person uploads the encrypted file to the cloud.

Steps of the Encryption operation**:**

1) The person selects a file that wants to download it from the cloud and send it to the decryption model.
2) The person downloads the decrypted file from the cloud.
3) The decryption model decrypts the file using the RSA algorithm.

Note these operations made after the person enter the cloud service, and the server proof a person's identity to allow him access to the data.

Algorithm1: RSA for Encryption and Decryption

Input: The parameters (p, q, e) , Output: The Encryption file or Decryption file.

1. Start.

2. Read the parameters (p, q, e).

3. If (p,q) prime numbers

n = p * q

Phi(n) = (p-1) * (q-1).

Else Go to 7

4. If (1 < e < phi(n) & GCD(e , phi(n)=1)

d = e ^ -1 mod (phi (n)).

Else Go to 7

5. Encrypted file = file ^ e mod (n).

6. Decrypted file = file ^ d mod (n).

7. Stop

4.4 Fingerprint Recognition System

The fingerprint recognition system can be utilized to match and recognize two fingerprints one is the original fingerprint and another one is the template image saved in the database. The fingerprint recognition system is fundamentally divided into two sub-parts: one is a verification model and the other is the identification model. Fingerprint verification is utilized to prove the authenticity of one person with 1: 1 matching of the database, while fingerprint identification is utilized to determine the personal identity with 1: n matching, fingerprint verification is quick execution process than fingerprint identification. fingerprint verification is quick execution process than fingerprint identification. Fingerprint identification is especially serviceable for criminal investigation cases [19].

Fingerprint matching approaches are divided into three major kinds:

- Correlation based matching,
- Minutiae based matching, and
- Pattern based matching.

Minutiae based matching is the very communal and most great utilized approach for fingerprint matching. In this thesis, we used Minutiae based matching by counting the Ridges-end point and Bifurcation point for every fingerprint by using the algorithm '**Fingerprint Matching using Ridge-End and Bifurcation Points**'. Thus, the focus will be on the major phases of the system which works on this method. The Fingerprint Recognition system comprises five parts, the fingerprint sensor, feature extractor, template storage, matching module, and the decision module. Fig 3.6 illustrates these phases.

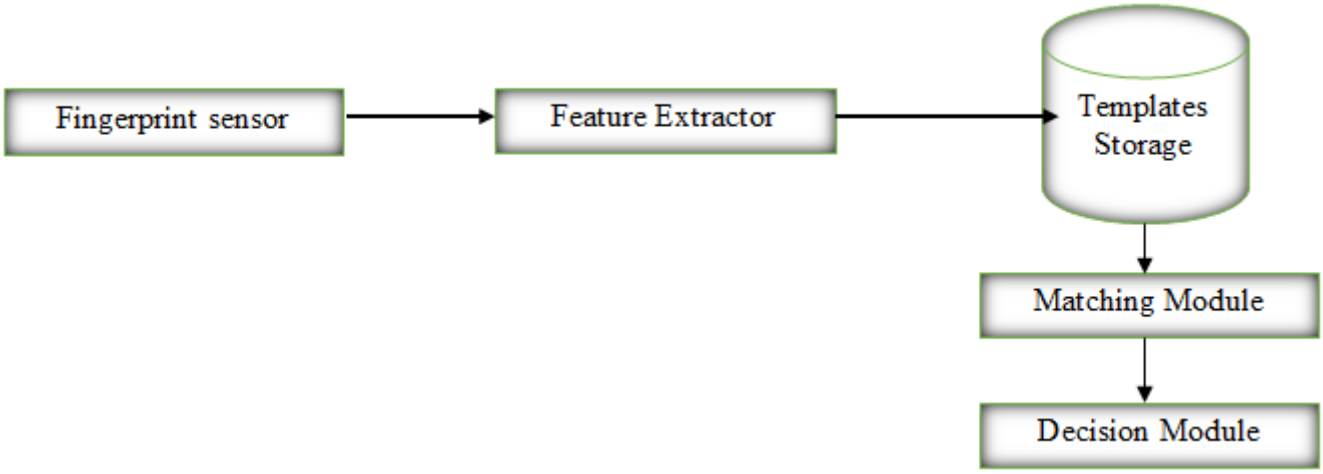


Figure (5): Main phases in fingerprint system

- **fingerprint sensor:** Is a device that the ability to acquire a fingerprint image.
- **Feature extraction (Minutiae extraction):** to extract minutiae (stage 2 that include Ridge-Ending and Bifurcation Points), this process is done by using the following Algorithm.

Algorithm 2: Minutiae Extraction

Inputs: Fingerprint image I (x, y).

Outputs: Matching result or a total number of both ridges-end and bifurcation points.

1. Start
2. Enhance I by applying the enhancement technique Histogram equalization, Fast Fourier Transform.
3. Convert I to the binary image form by using the threshold process of the entire image.
4. Apply the thinning operation on the binary image using the morphological process.
5. Apply the segmentation operations on the thinning image I to extract the Region of Interest ROI using two morphological processes; "Close", and then "Erosion".
6. Detect the minutiae points by creating matrix 3*3:

a) If the central pixel is one, has only one neighbor pixel that is the ridge-end point.

b) If the central pixel is one, has two neighbor pixel that is bifurcation point.

c) Else, it is a normal pixel.

7. Computation of the Points using two counter variables to count both ridge-end and bifurcation points.
8. Detect the location of every point in the fingerprint by pixel position, so that it can be stored separately for both ridge-end and bifurcation points.
9. Eliminate false minutiae points according to the distance between the points, and remove these points out the region of interest ROI.
10. End.

- **Matching**: During the prior steps, we are computed and stored all the required information about the points for both ridge-end and bifurcation points. Now, compares the computed values with the stored values, compares the sum of both amounts of ridge-end and bifurcation points with stored data.
- **Decision**: If the score from the matching process is true that done according to the value of the determined threshold t, then compares the location of ridge points and bifurcation points with stored location data. And finally, if all the location matches then the two fingerprints belong to the same finger, instead there is no match between the two fingers.

Now we discuss Pre-Processing operation such as the enhancement technique, binarization, thinning, segmentation and explain Minutiae Feature Extraction (Minutiae Detection).

4.4.1 Pre-Processing

The major goal of the preprocessing approach is to increase the image knowledge via removing the undesirable deformation and boosts the image options. The image enhancement technique comprises of three processes for the decrease of noises and for the better acquisition of the image. They are

- Histogram equalization
- Fast Fourier Transform

Histogram equalization is the technique that is utilized to reinforce the distinction of the image by increasing the magnitude of the image. It's a widely passable method due to it directly done on pixels or on the spatial domain, the equation used as the followed:

$$h(x,y) = floor\left((L-1)\sum_{n=0}^{x\,i,j} p_n\right) \quad (1)$$

Where h(x,y) is the given image , L is the number of bearable intensity values, often 256, and p_n is

$$p_n = \frac{number\ of\ pixels\ with\ intensity\ n}{total\ number\ of\ pixels}\ n\ =\ 0,1,\ldots,L\ -\ 1.$$

In the Discrete Fourier transform is performed Image Enhancement in the frequency domain and the enhanced image is divide into small blocks (32x 32) by applying the following formula:

$$F(u,v) = \frac{1}{M\times N}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} F(x,y)\, e^{-2j\pi(\frac{ux}{M}+\frac{vy}{N})} \quad (2)$$

Where F(x,y) is the given image ,(M,N) dimensions of the image, e is about 2.71828 , j the imaginary coordinate for a complex number, equals $\sqrt{-1}$ and u=0,1,2……31 and v=0,1,2……31.

4.4.2 Binarization and Thinning

Binarization is a prerequisite operation for minutiae extraction. It is the process of converting a grayscale image to binary format a black and white image. This process is done by applying a determined threshold value to the image as follows:

$$I(x,y) = \begin{cases} 1\ if\ I(x,y) > threshold \\ 0\ if\ I(x,y) < threshold \end{cases}$$

Here the threshold value that used is 128.

Thinning is a morphological process that is utilized to eliminate selected foreground pixels from binary images, ridge thinning is an operation of decrease the thickness of each line of patterns into one fingerprint element. It enhanced the standard of the fingerprint binary image. Also, ridge thinning eliminates unwanted pixels. One significant process, which is a controlled erosion process, is called skeletonization. To find the skeleton of a binary image we first define the thinning operation, with a given structuring element, SE:

$$Thin\,[I(x,y), SE] = I(x,y) - hit - or - miss\,[I(x,y), SE] \quad (3)$$

On the other hand, the thinning process is done by subtracting the result from the hit-or-miss process from the main image at every point. Note that this subtraction is the logical subtraction defined by:

$$A - B = (A)AND\ (NOT\ B) \quad (4)$$

The result was given by applying each of the line structuring elements to thinned the image and then performing a logical AND of the thinned results. This process is continued until the lines are one pixel wide and no changes in connectivity have occurred; that is, no change in the Euler number.

In the next step, we apply the thinning process with each of the other structuring elements, then perform a logical AND of all four results for each iteration. This process continues until the skeleton is obtained.

4.4.3 Segmentation

Fingerprint segmentation is one of the significant preprocessing steps in the fingerprint recognition system. It is used to disconnect a fingerprint area(foreground) from the image background. The correct segmentation of a fingerprint will greatly decrease the calculation time of the following processing steps and reject many false minutiae.

Here, we used morphological opening and closing operation as follows:

First, apply morphological closing operation using a disk-shaped structuring element of radius r (e.g.r=8), as follows:

" Closing is the name given to the morphological operation of dilation followed by erosion with the same structuring element. We denote the closing of A by structuring element B "

$$A \cdot B = (A \oplus B) \ominus B \quad (5)$$

Second, apply the morphological opening operation using the same disk-shaped structuring element to remove any connected spurs or noise, as follows:

"*Opening is the name given to the morphological operation of erosion followed by dilation with the same structuring element. We denote the opening of A by structuring element B"*

$$A \odot B = (A \ominus B) \oplus B \quad (6)$$

The public impact of the opening is to take out small, isolated objects from the foreground of an image and placing them in the background. It tends to smooth the contour of a binary object and breaks narrow joining regions in an object.

The general effect of closing tends to remove small holes in the foreground, changing small regions of background into the foreground. It tends to join narrow isthmuses between objects.

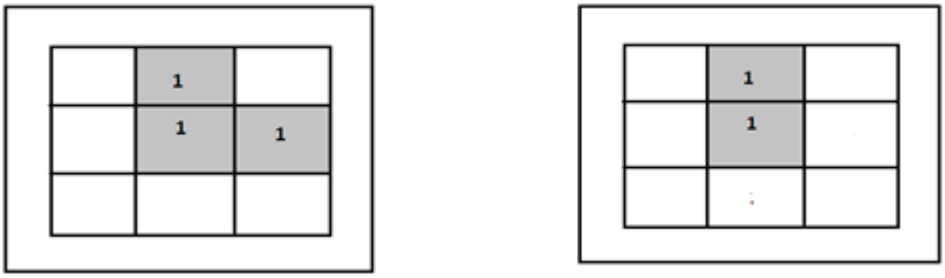
4.4.5 Minutiae Feature Extraction (Minutiae Detection).

After applying preprocessing techniques, the Minutiae Extraction is done by:

The algorithm discovered the Minutiae Points on the basis of (Ridge-end Point, and Bifurcation Point).

Matrix Creation (3×3)

To classify ridge-end or bifurcation points we create a matrix of (3*3) dimensions and pass it on the whole fingerprint image, If the central pixel is one, has only one neighbor pixel that is a ridge-end point. Else, if the central pixel is one, has two neighbor pixel that is bifurcation point, as shown in figure (3.8).



(a) (b)

Figure (6): Illustrate a) bifurcation point b) ridge-end point

The next process is the computation of a total number of available points in the fingerprint image separately, to do this step we used two variables that are used to count all ridge-end and bifurcation points and save it, due to this step is a significant part of fingerprint matching operation.

Detection location of points

All minutiae points in the fingerprint image have a given location, save the location of minutiae point of a specific point is very important for furthermore matching of fingerprints, to detect the location of every point in the fingerprint, we using the pixel position to this purpose and stored it separately for both ridge-end and bifurcation points.

Matching Amount and Locations

In the prior steps, the whole the desired information about points is counted and saved, such as locations and number of ridge and bifurcation points. Now, apply the matching step, first compares the counted values

with the saved values. Here, compares the set of both amounts of ridge-end and bifurcation points with stored data in the database. If the matching obtained, then go to the second step, which compares the location of ridge and bifurcation points with stored location data. And finally, if every location matches then the system make decision to accept the user.

5. Results

The Recognition result by implementing the matching algorithm has been executed and the outputs have been examined as shown in the table (1). The images of fingerprints that used are chosen from the FVC2002 dataset, the DB1 database [20]. This technic provides us with good performance in computation time, minimum error and increases the accuracy of the recognition system. In this paper, used commonly metrics such as “False Acceptance Rate" (FAR), “False Rejection Rate" (FRR), and," Success Match Rate"(SMR) to evaluate the fingerprint recognition system.

Table 1: Recognitions Results

Input Image /person sample	Number of images used for Recognition	Number of images recognized correctly	FRR to 8 samples for the same person	FAR to all different fingerprint in Data base	SNR%
Person1 (101_1)	8	7	1	0	87.5
Person 2 (102_1)	8	8	0	0	100
Person3 (103_1)	8	8	0	0	100
Person4 (104_1)	8	6	2	0	75
Person5 (105_1)	8	8	0	0	100
Person6 (106_1)	8	8	0	0	100
Person7 (107_1)	8	7	1	0	100
Person8 (108_1)	8	8	0	0	100
Person9 (109_1)	8	8	0	0	100
Person10 (110_1)	8	8	0	0	100
Over all	80	76	4	0	96.25

6. Discussion

From table (1) above, discussed the results of the recognition with noticing how to calculate the result of metrics, for example, person 2, person 4, and person 9:

Person 2 : FAR = $\frac{0}{72} \times 100 = 0$,FRR = $\frac{0}{8} \times 100 = 0$, SMR = $\frac{8}{8} \times 100 = 100$

Person 4: FAR = $\frac{0}{72} \times 100 = 0$,FRR = $\frac{2}{8} \times 100 = 25$, SMR = $\frac{6}{8} \times 100 = 75$

Person 9 : FAR = $\frac{0}{72} \times 100 = 0$,FRR = $\frac{0}{8} \times 100 = 0$, SMR = $\frac{8}{8} \times 100 = 100$

The total accuracy of the recognition =96% and the FRR of all persons =4 , FAR with 72 different samples =0 , concluded this technic provides us with good performance in computation time, minimum error and increases the accuracy of the recognition system.

The reason for the false Acceptance Rate" (FAR) =0 due to implementing the matching algorithm is applied to one database, when the implementation of the matching algorithm for other databases, notice the FAR has appeared, but is little and for shorting in the results, the matching algorithm is applied to one database.

References

1. Cloud Computing Security Issues and Challenges, Kuyoro S. O Department of Computer Science Babcock University Ilishan-Remo, 240001, Nigeria, Ibikunle F. Department of Computer Science Covenant University Otta, 240001, Nigeria , Awodele O Department of Computer Science Babcock University Ilishan-Remo, 240001, Nigeria .

2. Security Challenges for the Public Cloud ,Kui Ren, Cong Wang, and Qian Wang • Illinois Institute of Technology, JANUARY/FEBRUARY 2012 1089-7801/12/$31.00 © 2012 IEEE Published by the IEEE Computer Society .
3. Mell, P., Grance, T.: The NIST Definition of Cloud Computing. National Instituite of Standards and Technology (2009)
4. Mohammad Haghighat, Saman Zonouz, Mohamed Abdel-Mottaleb," CloudID: Trustworthy cloud-based and cross-enterprise biometric identification", Expert Systems with Applications 42 (2015) 7905–79
5. Kan Yang • Xiaohua Jia Department of Computer Science City University of Hong Kong Kowloon Hong Kong SAR Security for Cloud Storage Systems , ISSN 2191-5768 ISSN 2191-5776 (electronic) ISBN 978-1-4614-7872-0 ISBN 978-1-4614-7873-7 (eBook) DOI 10.1007/978-1-4614-7873-7 Springer New York Heidelberg Dordrecht London Library of Congress Control Number: 2013939832 .2014
6. Security Enhancement for Data Objects in Cloud Computing ,Sandeep Kumar Polu PG Student Department of Information Technology Acharya Nagarjuna University, India, IJIRST –International Journal for Innovative Research in Science & Technology| Volume 5 | Issue 6 | November 2018 ISSN (online): 2349-6010.
7. Diogo A. B. Fernandes · Liliana F. B. Soares · João V. Gomes ·Mário M. Freire · Pedro R. M. Inácio, Security issues in cloud environments: a survey, DOI 10.1007/s10207-013-0208-7, Springer-Verlag Berlin Heidelberg 2013.
8. Zhou, M., Zhang, R., Xie, W., Qian, W., Zhou, A.: Security and privacy in cloud computing: a survey. In: 6th International Conference on Semantics Knowledge and Grid, pp. 105–112. IEEE Computer Society, Washington, DC, USA (2010).
9. Vaquero, L.M., Rodero-Merino, L., Morán,D.: Locking the sky: a survey on IaaS cloud security. Computing 91(1), 93–118 (2011).doi:10.1007/s00607-010-0140-x.
10. D. Gonzales Martinez, F.J. Gonzels Castano, E.Argones Rua, J.L. Ala Castro, D.A. Rodriguez Silva, "Secure Crypto-Biometric System for Cloud Computing," in: International Workshop on Securing Services on the Cloud ,PP.38-45 201
11. Yassin AA, Jin H, Ibrahim A, Qiang W, Zou D. A practical privacy-preserving password authentication scheme for cloud computing. 26th International on Parallel and Distributed Processing Symposium Workshops (IPDPSW), IEEE, Shanghai, China, 2012;1210–1217.
12. Tsai JL, Lo NW. A privacy-aware authentication scheme for distributed mobile cloud computing services.IEEE Systems Journal 2015; 9(3): 805–815.
13. Convery, S.: Network Authentication, Authorization, and Accounting Part One: Concepts,Elements, and Approaches. The Internet Protocol Journal 10, 2–11 (2007).
14. Lloyd, B., Simpson, W.: PPP Authentication Protocols. RFC Editor (1992) .
15. Simpson, W.: PPP Challenge Handshake Authentication Protocol (CHAP). RFC Editor (1996).
16. Canetti, R.: Universally Composable Signature, Certification, and Authentication. In: Proceedings of the 17th IEEE Workshop on Computer Security Foundations, p. 219. IEEE Computer Society (2004).
17. Haller, N.: The S/KEY One-Time Password System. In: Internet Society Symposium on Network and Distributed Systems, pp. 151–157 (1994).
18. Rubin, A.D.: Independent one-time passwords. In: Proceedings of the 5th Conference on USENIX UNIX Security Symposium, vol. 5, p. 15. USENIX Association, Salt Lake City (1995).
19. Rohit Singh (Y6400), Utkarsh Shah (Y6510), Vinay Gupta (Y6534) , "Fingerprint Recognition", Department of Computer Science & engineering Indian Institute of technology, Kanpur. Computer Vision and Image. Processing (CS676).
20. http://bias.csr.unibo.it/fvc2002/