International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 5 (2018) pp. 2533-2540

Authentication of Biometric For Multi-Model Framework Using Fingerprint in Cloud Storage

[1]G. Preethi and [2]N.P. Gopalan

[1] Bharathiar University, Research and Development Centre, Coimbatore, India.
[2] National Institute of Technology, Department of Computer Applications, Trichy, India.
E-mail: [1] mgpreethi@gmail.com, [2] npgopalan@nitt.edu

Abstract

The rapid growths of the technologies are IoT (Internet of Things), ICT (Information and tele-Communication Technology) in a new trend of nowadays. These techniques have penetrated into our human life and it will affect in various ways in modern life. These computing devices are affecting as well as give benefits of our day to day life. All the people are having aadhar card in India. This is a mandatory personal identification card in nowadays. This is one of the ID proofs of all government and private working areas. Another most famous glorified innovation technique is called cloud computing. This has huge optimistic impacts are low cost, easy to access, portable, wide communication. The mandatory identification card detail has been stored in secure but it will access by anywhere in the world. It has some security issues are arises that deal with carefully. A fingerprint is one of the most acceptable security systems in various applications. Our contribution is the combination of a unique identification number and N2 algorithm for the secure way in cloud computing. The proposed methodology has been analyzing the biometric authentication in a cloud. The security system of a fingerprint is a unique identification for persons and it will not have a change in their lifetime. This will not be undertaken by any unauthorized person or organizations. The real-time applications of railway reservation in India have computerized with high cloud security systems. This provides a wide-ranging and complete structure of the biometric authentication in cloud security systems.

Keywords: Security Systems, biometric Authentication, Cloud Computing, Pattern Matching.

INTRODUCTION

The rapid growing technology of biometric is widely used for authenticated world. The world has been need high security for each and every activity. The modern networked world has lot of software and mobile applications in our hand. The accessing of information is very easy to gather and provide information to others. An inexpensive fingerprint scanner device are also involved and contributed a lot in biometric authentication. However, the user id and password is one of security mechanism but it may hacked by unauthorized third parties, it shows an insufficient security system in our day today life. The biometric authentication is one of the best ways to protect the documents and content in cloud storage. This is another smart way of authentication service, which is widely accepted in recent years. There are many applications has been provided this facilities to the users like banking sector, financial sector, insurance and academic sectors. The cloud computing and biometric has to acquire the next level of the security systems. This is the best way to provide security system have access the legal or authorized users no one else anywhere in the network. The biometric has a better reliable, accuracy to recognize the unique physiological or behavioral characteristics without any redundancy. Cloud computing provide multi resources includes in systems, servers and mobile application programs or many kind of administrative systems.

DIFFERENT DEPLOYMENT MODELS IN CLOUD COMPUTING

1. Public cloud is a computing services tendered by cloud service provider over the public internet. This has availability to all others who wants to use it. The public cloud may be free or pay-only-use systems are available in the internet [1]. There are lot of effective security systems available in the public cloud like Intrusion Detection Systems and Intrusion Prevention Systems
2. Community Cloud is providing one or more organizations shared the information on the community whether it may exist or not in the premise [5][6].
3. Private cloud is providing a service to any one organization. The private organizations are communicated to their people and clients.
4. Hybrid cloud has two or more private, public cloud.

Models in Cloud Computing

There are three different categories of models

1. Software as a Service (SaaS): It has ability to create software and distribute to running on a cloud [2] [3].
2. Platform as a Service (PasS): This service provides user able to generate any applications and use it by own/others. This service is more important in virtual systems.
3. Infrastructure as a Service (IaaS): It provides to the user has computing resources without permission can run the software [4].

The new service model in the proposed system is called Biometric as a Service (BaaS).

4. Biometric as a Service (BaaS): This is a new way of security system. The government and private sectors are having biometric application in mobile, laptop and desktop such as access control system, security system, students and staff attendance system and identity verification. This has unique identification of fingerprint recognition system.

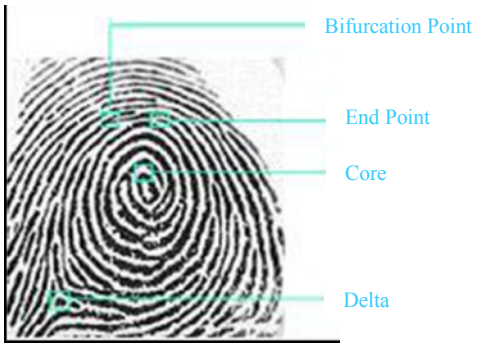


Figure 1. MSO 301 Series Optical Scanner Image

The proposed fingerprint algorithm has a mapping system of fingerprints by identifying unique spot in the human fingers. There are different pattern and location are identified in fingerprint, those have unique point in the human finger. Cloud service provider should require the biometric database without stored in local drive, network, and cloud storage, to run a query processing of identification and validating the request. The scanned image shows in the figure (1). The fingerprint features are as follows:

Bifurcation:	It's a crinkle (or ridge) flows
Core:	Largest bend or crinkle
Delta:	Precinct where the crinkle splits
	into 3 lines then immediately bends
Ending Point:	It's a endpoint in the crinkle flows
Ridge:	The Line lift-up a crinkle
Valley:	harmonize with a crinkle

The fingerprint has accepted globally as a legal process to recognize an individual person without any documentary proof. This has various impressions of the microscopic crinkle in our fingers, it is a name called dermal. Human being has unique and unchangeable ridges, valley and dermal in the finger. There are lot of applications used the biometric fingerprint such as medicine, public civil service, license registration, education, attendance service, unlock mobile access and security system in IT organizations. The biometric fingerprint machine is very easy and portable to handle with thermal, optical, silicon or ultrasonic ways of approaches are used instead of stamp pad capture. There are two matching techniques are used in biometric. Biometric identifications are based on minutiae-based matching technique of fingers in ridge ending and bifurcations. The other matching technique is correlation-based matching technique, it overcome the drawbacks of the minutiae-based techniques. This has an exact location on the registration point, the image translation and rotation will not affect the original image. This shows in the following figure (2).

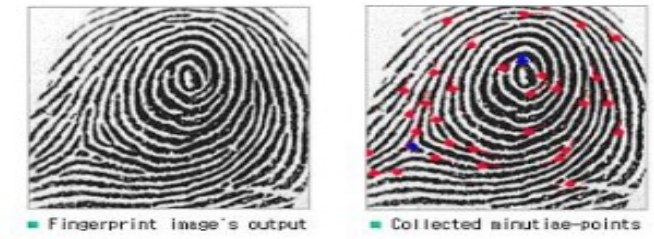


Figure 2. matching Low minutiae point

The customary finger point has many types, these types belong to any one of the minutiae-based techniques or correlation based techniques.

1. The consistency flow of ridges is called plain arch. This has a voyage all along on the finger to the other side. It is a simplest fingerprint pattern to recognize figure (a).
2. Tented Arch is a pattern similar to plain arch, the only difference is an arch line in ridges at the center point and this point has not continuous figure (b).
3. Ulnar Loop is a downward slope from thumb toward the little finger in the hand figure (c).
4. The reverse loop of Ulnar loop is called Radial Loop figure(d).
5. Plain Whorl has ridges that make one circular shape/ spiral or oval shape figure (e).
6. Central Pocket has a minimum one recurves ridge that will not intersect the inner recurves in the ridges figure (f).
7. Double loop has two set of separate as well as distinct sets of shoulder figure (g).
8. Accidental whorl is a composition pattern connects at least two distinct deltas figure (h).

The biometric fingerprint based system has very minimum false rejection rate is 3.14 to 7.43% and false acceptance rate is 0.001 to 0.01. The fingerprint is having lot of classifications. The classification are arch, tented arch, whorl and right loop. The proposed pattern matching algorithm have good performance of finger print identification, this has clarity of image resolutions in input and output. The biometric fingerprint systems are more secure because of the unique identifications of the above mention type of human beings fingerprint.

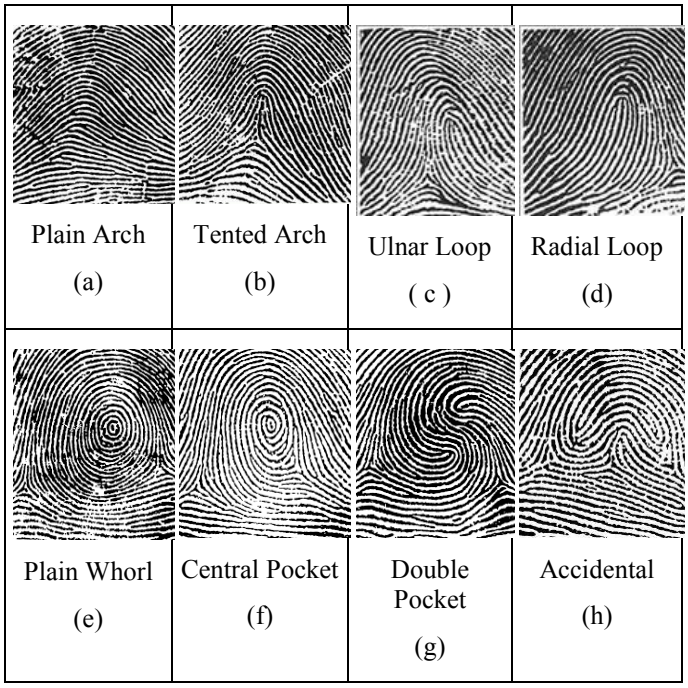


Figure 3. Types of fingerprints

POSED METHODOLOGY

Unique Key Identification with N^2 Fingerprint Matching Algorithm

A unique key of aadhar number is easy to retrieve all the information about the user. The user need not carry the hardcopy of voter id, PAN card or other identity. The user impression is registered in the fingerprint optical scanner device, the system automatically gather all the information from the cloud database. This cloud database is maintained by the Cloud Service Provider (CSP). All the information extracted within few minutes. The process is shows in the figure (4). This is secure and easy way of accessing the identity at where in the world.

Store the Fingerprints in Cloud Database

The proposed model used to scan the user's fingerprint and which is stored in the database. This fingerprint security system is more sophisticated methodology, user has a unique identification card is Aadhar card. The aadhar card number is linked with the user's bank account, family card, gas booking agencies and voter id. This is a mandatory identification for people in India. This identification number is gives an entire detail about the user. The identification is having ten finger prints and retinas of both eyes. These are mandatory details of aadhar card. The Finger print has retrieve and stored into cloud database and whenever we want to use it from the database. This finger print images has stored through double encryption techniques. These are having high security system and accessed by authorized users.

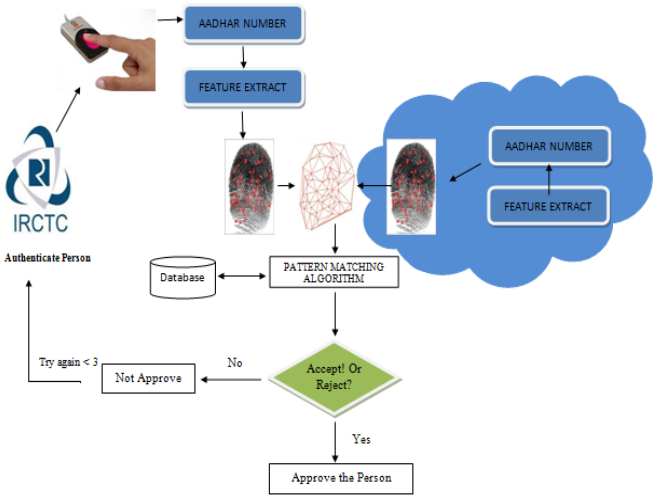


Figure 4. Matching minutiae points using unique key K with n^2

Comparing the Fingerprint with Pattern Matching Algorithm

The system has required a password to retrieve the finger print images from the cloud database. The user must have entered the password then it will be access by the authorized users. The impression is retrieving from the user to stored temporarily and compare to the cloud database. If it matches with previously stored in the cloud server database the user request will be accept and enter into the next level of authentication. Minutiae points have been identified by the proposed extraction algorithm. Here, features are characterized based on the location and direction of crinkle or ridges [7]. Features are obtained from the fingerprint and find the corresponding aadhar number then compare to the fingerprint which is stored in cloud database. These two fingerprint images are matched that should be monitored by any one of the proposed algorithm.

Algorithm 1: Ridges Matching Algorithm

Using Hough Transformation

The Hough transformation is often various lines, arch and circle recognition. The authors Agrawala and Stockman have stated the Hough Transformation and Template Matching algorithm. However, the ridges are captured and compared to a stored image in cloud database. These processes are achieved by the following steps

1. The parameters are δt_x and δt_y, δ_θ and S_x, where δt_x and δt_y are shift vectors or translation vectors along the x and y-direction, respectively θ is the rotation angle and S_x is the scaling factor.
2. Compare the minutia points in the fingerprint through the above parameter rs. In the comparison, count the matched minutia points within limited boundaries.

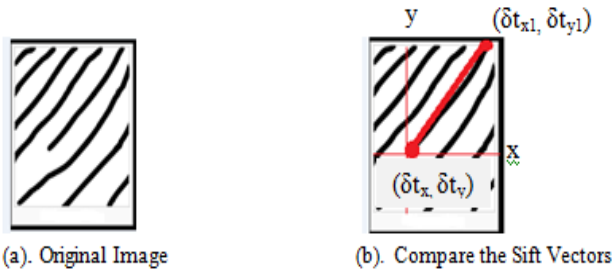


Figure 5. Translation about the origin

The translation points are added to a translation distance vectors t_x and t_y to the original co-ordinate origin vectors (x, y). The δ is a constant value for original and translated co-ordinates as we get

$$t_{x1} = x + t_x \qquad (1)$$
$$t_{x2} = y + t_y$$

and the scaling factor of S_x is the two time bigger than the original co-ordinates, the distance are compare from the original image. This distance based identification is achieved through scaling factors of proposed system. The rotation angle is to measure though minutia points in the original and its cloud database. The specified rotation angle is θ and position (x_r, y_r) instead of (t_x, t_y) of the fixed origin. The polar co-ordinates are substituted into rotation point at the position (x, y) trough an angle θ about the fixed point at the origin [19].

$$x_r' = x\cos(\theta) - y\sin(\theta) \qquad (2)\ [19]$$
$$y_r' = x\sin(\theta) + y\cos(\theta)$$

The translated rotated points have to be identified by a rigid-body transformation that moves the object without deformation of an object. The coordinate points are measure by the two angles θ and φ. the additive factors are adding to the pivot point, as well as we get the transformed co-ordinates x' and y'. The sp_org(x) and sp_org(y) is namely specified origin of x and y co-ordinates. This shows in the figure (5). In the fingerprint, minutia points get from the original image compare to the cloud which is matched or need to press

$$\left.\begin{aligned}\sin(\theta+\varphi) &= \frac{y - y_r}{r}\\ \cos(\theta+\varphi) &= \frac{x - x_r}{r}\end{aligned}\right\} \quad (3)[19]$$

$$\left.\begin{aligned}x' &= sp\_org(x) + (x - xr)\cos(\theta) - (y - yr)\sin(\theta)\\ y' &= sp\_org(y) + (x - xr)\cos(\theta) - (y - yr)\sin(\theta)\end{aligned}\right\} \quad [19]$$

again on the sensor device. The scaling factors have increased the size of ridges or reduced the size of ridges. The two sets of minutia points have a large size or small size due to the impression of the person. The scaling factor reduces the time to take again and again of the same finger print. There are two types of increased and decreased scaling factors used to identify the impression. This comparison technique is one the solution to reduce the time complexity. The scaling factors of S_x and S_y are used to identify and avoid the redundancy. The extracted minutia points are converting into polar vectors with respect to the specified origin. The string matching algorithm is used to compute the distance between δS_x, δS_y and $2\delta(S_x', S_y')$. Scaling is applied by least square fitting algorithm. The parameters in the rotation and scaling factors θ, Sx and Sy are produce the result of maximum number of matched minutia points within boundaries. The result of matched minutia points are repossess found on the least distance between the two matched scaling factors. The normalized output of matched scaling vectors are identify as follows

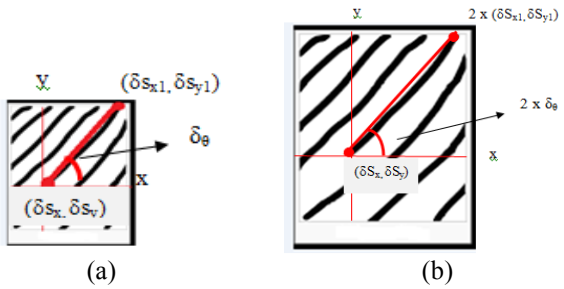


Figure 6. a) Coordinates (δS_x, δS_y) in fixed origin b) Uniform Scaling. Original image is transformed to uniform scaling and non uniform scaling

$$D = \frac{S_{X2} - S_{X1}}{X} - \frac{S_{Y2} - S_{Y1}}{Y} \qquad (4)$$

$$M_P = N^* \left\{\frac{N\text{-}0.21\,(S_X - N)}{S_X + 1}\right\} X \left\{\frac{N\text{-}0.21\,(S_Y - N)}{S_Y + 1}\right\}$$

Where D is distance between the minutias matched points and N indicate as total number of matching points respectively. The normalized matching point Mp is calculated by the above formula. The matched points should be on the boundaries rather than the complete sets of fingerprint. An unmatched minutia points are calculated for further features. The accurate matched pairs are identified by the two minutia sets respectively Sx and Sy

Algorithm for Rescaling the Image

Step 1. Rotation angle θ estimated by two minutia set features whether increased or decreased.

Step 2. The angle is estimated using the least square fit method. θ → LSF (minimal distance), parameters are θ, adj1 and adj2 points matched exactly the boundary value.

Step 3. The exact points are converting into uniform scaling factor or non uniform scaling factors coordinates at sp_origin.

Step 4. Compute the distance between two minutia sets of coordinates.

Step 5. Optimized the matching coordinates are output.

FUNDAMENTALS OF K * n^2 MINUTIAE MATCHING SCORE

Let the translation and scaling factor are Ti(xi) and Si(xi) distributions vectors of i^{th} element matching, i = 1, 2… n. In this paper, we propose a logistic distribution function of mapping matching scores of x1 and x2 into integrated of single matching score value x. The logistic distribution transformation vectors are expressed as the three parameters namely δSx, δSy, and δTx refer the figure (6). These integration parameters are used reduce the Fake Refutation Rate (FRR) for considering limits of Fake Approval Rate (FAR).

Let us assume the x1 and x2 parameters are independent, then the translation T(x1,x2) and scaling vectors S(x1, x2) can represented as follows,

$$T(x1, x2) = \iint T1(x1) \,.\, T2(x2)\, dx1.\, dx2 \quad (5)$$

and

$$S(x1, x2) = \iint S1(x1) \,.\, S2(x2)\, dx1.\, dx2 \quad (6)$$

the rewritten of logistic transformation equation as follows

$$T(x) = \iint T1(x1) \,.\, T2(x2) \quad (7)$$

$$DT(x) = \iint \delta\,(S_x + S_y + T_x - T^{-1}(x))\, dx1.\, dx2 \quad (8)$$

$$H_{far} = T(x) * D(x) \quad (9)$$

$$S(x) = \iint G1(x1) \,.\, G2(x2) \quad (10)$$

$$ST(x) = \iint \delta\,(S_x + S_y + T_x - T^{-1}(x))\, dx1.\, dx2 \quad (11)$$

$$H_{far} = S(x) * ST(x) \quad (12)$$

where the above equation has the delta function δ(x). The translation vector and scaling vector are represented along with the straight line

$S_x + S_y + T_x = T^{-1}(x)$ on the x and y- plane. However the False Rejection Rate H_{frr} for given three parameters of Sx, Sy, Tx and False Accept Rate H_{far} is calculated by

$$H_{frr}(S_x, S_y, T_x, H_{far}) = H_{frr}(t) = \int_{-\infty}^{l} T(x)\, dx \quad (13)$$

$$\text{Where } l = argument_x\, inf_x \{l_{far}(x) \geq H_{far}\}$$
$$= argument_x\, inf_x \left\{\int_x^{+\infty} S(x)\, dx \geq H_{far}\right\}$$

Here $H_{far}(t)$ *and* $H_{frr}(t)$ is the FRR and FAR's threshold value l. The integration of fingerprint matching algorithm represented as follows. The threshold values of FAR is $l_{far}^{(i)}$, where i = 1, 2, ….N, to compute the parameters (S_x, S_y, T_x, l_i) and it's gratify the following optimization decisive factor,

$$S_x\, S_y\, S_z = \text{argument}\, \min_{sx,\, sy,tx} \left\{H_{frr}\, S_x\, S_y\, T_x\, l_{far}^{(i)}\right\}$$

and

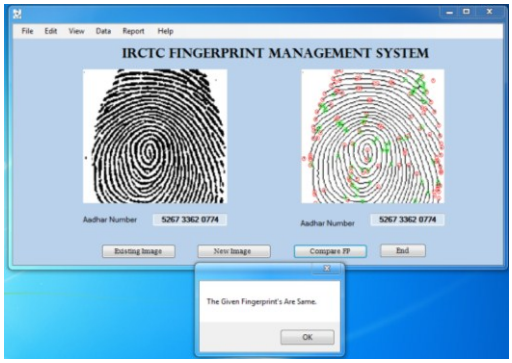
$$l_i = \text{argument}\, \min_{sx,\, sy,tx} \left\{H_{frr}\, S_x\, S_y\, T_x\, l_{far}^{(i)}\right\}$$
$$= \text{argument}\, \inf_{sx,\, sy,tx} \left\{ \int_x^{+\infty} S(x)dx \geq l_{far}^{(i)} \right\}$$

the parameters (S_x, S_y, T_x) are minimized at each specified FAR level with FRR. The analytical form is not possible to find the solution of minimization problem [9][10]. The above mentioned minimization of equation is solved by large factorization numerical algorithm.

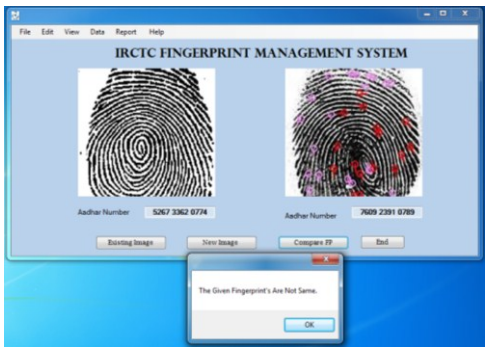
EXPERIMENTAL RESULTS:

The people fingerprints were collected while on the time of aadhar card registration. The fingerprint images were captured by MSO 301 series and stored in the cloud storage. The device has image size 23 * 23 mm and the resolution is 500 dpi with 256 gray scale levels. This has the authentication of fingerprint is < 0.7 sec and identification is < 0.9 sec in 1:1000 mode. The collected fingerprint False Acceptance Rate is less than 10^{-8}, which is based on the safety measures necessities in the database. There are two set of fingerprint impression acquired while aadhar card registration. The same finger print images were collected again from the same user on the time of travelling. The first set of fingerprint is original and second set of fingerprint for confirmation. Now there are four set of Impressions for two fingers impression are stored in cloud and compare the impressions when its necessity of identifying the user's. The sample of 1200 (150 X 4 X2) subject impression where stored in cloud. These fingerprint images are partitioned into two subsets in the cloud database. The first set contains the first 75 subjects of fingerprint and second set contains the remaining 75 subjects of fingerprints. This shows in the figure (7). However, the first set used for training dataset and second subset used for testing.

We evaluate three different algorithms 1. Minutiae- based algorithm, 2. k * n algorithm, 3. The proposed algorithm. The biometric as service based identification was weigh up by Beneficiary Operating Feature (BOF) arc examine the acceptance rate of Fake Refutation Rate against Fake Approval Rate. The approval and refutation having less Fake rate in the minutiae points. A scaling factor vector and translation vectors are having same distributions of matching score point in the minutiae. This is use to finding the matching score of minutiae point because minutia points are not matched entirely. The matching score points are obtained the accuracy level; this is called success



(a) Fingerprints are matched with minutiae



(b)

Figure 7. b) Fingerprints are not Matched with minutiae points Enhanced Fingerprint Matching through Unique Key

for fingerprint matching algorithm. We propose the new algorithm of unique key identification with n^2 matching fingerprint in large-scale database. The time complexity of n^2 algorithm and k*n matching technique is reduced to unique key identification with n^2 algorithm. There are two set of minutiae points are stored in n^2 database and combination matched points are retrieved by unique key is called aadhar card number. The training set data is stored in 'n' and testing set data is stored in 'n' the combination of these data set n^2 are used to identify matching minutiae points. The existing method of k*n is having the constant number of k [11][12][13]. This has slow process when feed the large factorization input value. Instead of this constant value, we use the unique key for compare the large number of dataset in cloud database. The integration of the above algorithm has a better matching score point. First we evaluate the False Rejection Rate for stored fingerprint image with large number of attempts. The possible matching scores combination significantly having higher performance in the proposed algorithm. The Fake Refutation Rate and Fake Approval Rate are indicating in the figure (8)**.** **T**he performance of the proposed algorithm is expressed as follows.

The efficiency of matched and unmatched minutiae points to be measured by the following formula.

$$\text{Efficiency of} = \frac{\text{Maximum No of Matched Minutiae Points}}{\text{Total No of acquire Data}}$$

The result of the equ ( ) is 1158/1200 = 96.5%. Here the H_{far} False Acceptance Rate is 96.5% which having the H_{frr} rejection rate is 3.5%. The second sets of data are retrieved on the time requirement while travelling in Train. The False Reject Rate H_{frr} is calculated through the second algorithm, E = $\frac{1169}{1200}$ = 97.42% and the H_{frr} False Rejection Rate = 2.58%. The integrate of unique key identification with n^2 algorithm efficiency is calculated by the two dataset E = $(1158) + (1169)/(1200) + (1200)$ However, the E = $\frac{2327}{2400}$ = 96.95%, The acceptance rate is 96.95% and overall H_{frr} False Rejection Rate is 3.05% . The maximum matching minutiae points are calculated through the E = $\frac{13}{2400}$ = 0.5416% . The given large datasets are processed within few minutes and have better accuracy. The existing method has not processed for given large dataset [17][18]. This is shown in figure (9). The proposed algorithm having good performance compare to the existing techniques of k * n algorithm and n^2 fingerprint matching algorithm.

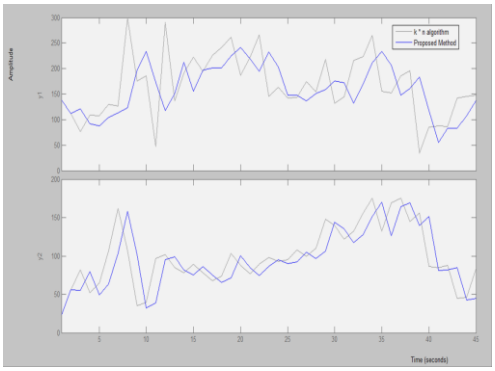


Figure 8. Time complexity of FAR H_{far} = *0.5416%* and FRR H_{frr} =0.258% 0.58%

PERFORMANCE ANALYSIS

The proposed method was implemented in MATLAB r2017a and data are retrieved from MYSQL. There were large numbers of fingerprint images stored in cloud database and compare these images to getting as new images in the above mentioned software. The given image size is 233 X 271 scanned by MSO 301 series with 500 dpi resolutions. The

Fake Approval Rate and Fake Refutation Rate were calculated very accurately is 0.051% in the proposed method and the unique identification number were exactly matched with the fingerprint images. These are used to retrieve the user information whenever we want. The hard copy of proof need not carry our self at any time. As we observed the given experiment of Unique Key * n2 is very effective identification of fingerprints.

The motivations behind in this works have growing need of identifying a unique personal security system. The fingerprint is the best way of measuring biometric technique to identifying the authorized user and unauthorized user. This proposed method provides scalable and reliable performance better than the other existing techniques. Our contribution in this paper provides fingerprint identification using Matching Minutia score method with help of MATLAB. We compare the huge number of subjects for matching process and identifying the matching minutia score [14][15][16]. The existing fingerprint images are stored in the cloud database. These images are retrieved and compared.

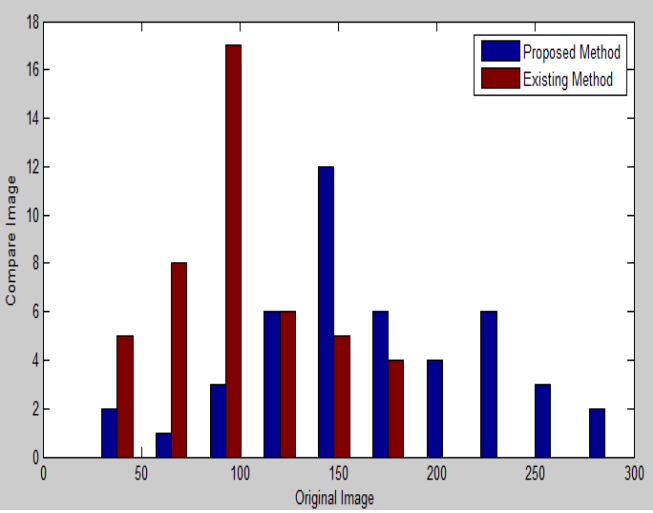


Figure 9. Overall matching minutiae points for comparison

CONCLUSION

This paper has proposed a technique to integrate the unique key and n^2 database in cloud. There are three different algorithms are integrated and give improved performance of unique key fingerprint identification system. The translation and scaling factors are used to measure the fingerprint very accurately to makes use of the conditional factors of S_x and T_x. These factors are used to observe the matching minutiae score without any redundant points. Our experimental result shows the good performance of typical matching scores. The proposed algorithm is automatically compute ridges and minutiae points with the help of Gabor filters. The future work will ensure the security system in the cloud database with the help of minutiae points and fully homomorphic encryption.

REFRENCES

[1] Farhad Farokhi, Iman Shames, 2016, " Secure and Private Cloud-Based Control Using Semi-Homomorphic Encryption", sciencedirect, IFAC-papersonLine 49-22, pp. 163-168.

[2] Ghazal Naveed and Rakhshanda Batool, 2015, "Biometric Authentication in Cloud Computing", Journal of Biomatrics & Bistatistics, ISSN 2155-6180,vol. 6, Issue. 5.

[3] Aliyu Tukur, "Fingerprint Recognition and Matching using Matlab", IJES, Vol. 4, Issue. 12, 2015, pp. 01-06.

[4] Ravi subban and Dattatreya P. Mankame, 2013, "A Study of Biometric Approach Using Fingerprint Recognition", Lecture notes on Software Engineering, Vol. 1, No.2, pp. 209-213.

[5] Hemlata Patel, Pallavi Asrodia, 2012 "Fingerprint Matching Using Two Methods", IJERA, Vol. 2, 2012, pp. 857-860.

[6] Nani Fadzlina, Ahmad Ihsan Mohd Yassin, 2011, "MySQL Databas for Storage of Fingerprint Data", IEEE, 2011, pp. 293 – 298.

[7] R. Heidn, 2008 "A world history of fingerprint,"Chinese People Public Security University Press, ISBN:978-7-81109-789-4.

[8] Abinandhan Chandrasekaran, Dr. Bhavani Thuraisingham, 2007, "Fingerprint Matching Algorithm Based on Tree Comparison using Ratios of Relational Distances", IEEE computer society, 7695-2775-2.

[9] S.Chikkerur, A. N. Cartwright and V. Govindaraju, 2006, "Kplet and CBFS: A Graph based Fingerprint Representation and Matching Algorithm," ICB.

[10] Wang, Y., X. Ao, et al. 2006, "A Fingerprint recognition algorithm based on principal component analysis", TENCON 200, IEEE Region 10 Conference.

[11] Koichi Ito, Ayumi Morita, "A Fingerprint Recognition Algorithm Using Phase- Based Image Matching for Low- Quality Fingerprints", IEEE, 2005, pp. II- 33 – 36.

[12] Sharat chikkerur, Alexander N. Cartwright and Venu govindaraju, "Fingerprint Image Enhancement Using STFT Analysis", ICAPR 2005, UK.

[13] P. Komarinski, P.T. Higgins, 2005 "Autimated Fingerprint Identification Systems (AFIS)", Elsevier Academic Press, pp. 1- 118.

[14] Kenneth Nilsson, Josef Bigun, 2003, "Localization of corresponding points in fingerprints by complex filtering", Pattern Recognitin Letters 24, 2003, pp. 2135 – 2144.

[15] K. Takita, T. Aoki, 2003, "High-accuracy subpixel image registration based on phase- only correlation," IEICE Trans. Fundamentals, vol. E86-A, no. 8, Aug. pp. 1925-1934,

[16] A. K. Jain, A.Ross, S. Prabhakar, 2001, "Fingerprint Matching using Minutiae and Texture Features", International Conference on Image, Vol. 3, 2001, pp.

282 - 285

[17] Anil K. Jain, Salil Prabhakar, 1999, "Combining multiple matchers for a high security fingerprint verification system", Pattern Recognition letters, no. 20, pp. 1371- 1379.

[18] Kalle Karu, Anil K. Jain, 1996, Fingerprint classification", Vol. 29, Issue 3, pp. 389 - 404

[19] Donald Hearn, M. Pauline Baker, 1997, "Computer Graphics C Version", Second Edition,