International Research Journal of PMC (IRJPMC)
Volume 02, Issue 01, ISSN: 2961-1717, 2023. PP. 26-39
https://doi.org/10.61916/prmn.2023.v0101.004
Research Article

Biometric Cryptosystem Based On Fingerprint Authentication And Cryptography Technique

Shivani Tyagi
shivanityagi207@gmail.com
Manish Kumar
Professor, Deptt Of Computer Science & Engineering, R D Engineering College, Ghaziabad,UP (INDIA)
manishtonk@gmail.com
Dharambeer Singh
Associate Professor, Deptt of Mechanical Engineering, R D Engineering College, Ghaziabad,UP (INDIA)
veerdharam76@gmail.com
Hariom Tyagi
Associate Professor, Deptt Of Information Technology, RKGIT, Ghaziabad, UP (INDIA)
hariom2678@gmail.com
*Corresponding Author: shivanityagi207@gmail.com

ABSTRACT

Biometric systems are one of the most reliable and popular techniques today and fingerprint authentication is one of the most reliable and robust biometric techniques due to its nature. The characteristics of fingerprints play a big and important role in the authentication of people. In this research, fingerprint authentication scheme consists of many stages: image enhancement, binarization, segmentation, spine thinning, detail extraction. In this authentication we use Gaussian filter for better result. Hybrid protection is created through a combination of biometrics and cryptography, such as fingerprint and cryptography schemes. The combination of many biometric features with a single crypto key should offer an approach to increase authenticity and reduce the fake acceptance rate (FAR) and fake rejection rate (FRR) of fingerprints. For each new user of a biometric system, the combination of a cryptobiometric system will overcome the limitations of accuracy and vulnerabilities. We want to protect our real data from unauthorized people and systems, so we use cryptographic schemes as Elliptic Curve Diffie Hellman's key exchange algorithm. Biometric techniques can be used for various applications, such as: Biometrics can help make processes, transactions and everyday life safer and more convenient. You can use biometric data anywhere. to provide a valid identity solution. Cryptographic systems and fingerprint authentication have been identified as two of the most important aspects of the security environment. In this document, two powerful techniques are combined to produce better and safer results. In this study we use Gaussian

How to Cite This Article: Tyagi, S., Kumar, M., Singh, D. & Tyagi, H. (2023). Biometric Cryptosystem Based On Fingerprint Authentication And Cryptography Technique. *International Research Journal of PMC (IRJPMC)*. 2(1), 26-39. https://doi.org/10.5281/zenodo.10258787

filters, because less FAR and less FRR, with fingerprints authorized and finally authentication being a security key or a secure message created for a particular job . If the entered fingerprint matches the authorized person, but the DBA fingerprint does not, the system says "You are an unauthorized person, please try again." If the two fingerprints match, it will send all the secure passwords or cryptographic keys or secure messages for each work. It is developed by MATLAB (Matrix Laboratory). The proposed algorithm was tested on the FVC2004 database and compared with all participants in FVC2004.

Keyword: *Biometric systems, Fingerprint authentication, Image enhancement, Cryptography, Gaussian filter, FAR, and FRR.*

Introduction

Biometrics falls under two distinct areas of research and application. Biometrics is the most widely used method to identify a person based on physical or behavioral characteristics. The properties measured include; Face, fingerprint, geometry, handwriting, iris, retina, vein and voice, etc. We want to achieve a high level of security and reduce fraud in transactions and all communications. Solutions based on biometric cryptosystems can ensure confidential and financial transactions and the confidentiality of personal data. The use of biometric cryptosystems, which combine biometric authentication and cryptography, offers a secure and reliable method for user verification. This approach leverages unique biological traits, such as fingerprints, voices, and facial features, to verify a user's identity. The use of biometric data in combination with cryptographic techniques enhances security by providing a multi-factor authentication method that is difficult to replicate. The implementation of e-Government services in developing countries, such as Nepal, can benefit from biometric cryptosystems, as they offer a high level of security and reliability. Additionally, the operation of vehicle maintenance systems and the identification of products in the context of developing countries can be enhanced through the use of biometric cryptosystems, ensuring the integrity and security of critical processes. The combination of biometric authentication and cryptography provides a robust and effective security solution for a wide range of applications, offering both convenience and protection for users' sensitive information (Bhagat, C., Mishra, A. K., & Aithal, P. S., 2022; Jha, P. B., Mishra, A. K., & Aithal, P. S., 2023; Mishra, A. K., Nepal, A., & Aithal, P. S., 2022; Pokharel, R., Mishra, A. K., & Aithal, P. S., 2021).

Cryptography is the most reliable practice and study to maintain the confidentiality of information. Cryptography almost exclusively refers to encryption, the process of changing the original message, i.e. Plain text, in cipher text. Decryption is the reverse process, changing from cipher text to plaintext. Plain text and cipher text processing is controlled by algorithms and keys. Keys are important because ciphers without variable keys are easy to crack and therefore less useful for most purposes. In this paper we will use fingerprints as security keys. The idea of cryptography and fingerprinting was introduced as part of the technology to improve confidentiality and security in relation to personal data protection, personal security communications, reliability and reliability in relation to user input and required security systems. However, it is vulnerable to attacks such as cracking and tracking of information sources, but it faces the next security channel, cryptography.

There are several methods that can be disclosed to protect keys using biometric techniques. First, it involves storing keys and matching patterns. In this method, which we use here, we first capture an image with a fingerprint with the device and compare it to a already saved template. If the user is genuine, we re-authenticate using a key exchange algorithm such as Elleptic Curve Diffie Hellman's key exchange algorithm, after which the secret message is released.

Identification and Verification Procedures

2.1 False Rejection Rate (FRR) : FRR is the frequency at which authorized persons are denied access. This is also known as the False non-match Rate (FNMR). It measures the percentage of valid input data rejected

$$\text{FRR(n)} = \frac{\text{number of all rejected verification checks up for a qualified or like authorized person n}}{\text{number of all verification checks up for a qualified or like authorized person n}}$$

2.2 False Acceptance Rate (FAR): FAR is the number of times an unauthorized person is deemed to be authorized. Since taking it incorrectly can often cause harm, FAR is usually a safety measure. This is also known as False Match Rate (FMR). It measures the percentage of invalid matches.

$$\text{FAR (n)} = \frac{\text{number of all successful independent fraud checks up against a people}}{\text{number of all independent fraud checks up against a people}}$$

2.3 Equal Error Rate (EER): The common value of FAR and FRR when FAR equals FRR. This is the value at which FAR and FRR are kept as low as possible at the same time. A low EER value indicates a high level of system accuracy.

3. BIOMETRIC TECHNIQUES

Currently, there are many different techniques available to identify/verify a person based on biometrics.

3.1 Physical characteristics: The following are examples of biometric techniques based on physical characteristics:

3.1.1 Fingerprint authentication: The fingerprint matching, either for the one-to-one verification case or one -to-many identification case, is straightforward and easy.

3.1.2 Recognition of hand 3.1.3 Face recognition 3.1.4 Face geometry

3.1.5 Vein pattern recognition 3.1.6 Retina recognition 3.1.7 Iris recognition

3.2 Behavioral characteristics: The following are examples of biometric techniques based on behavioral characteristics:

3.2.1 Voice recognition 3.2.2 Signature recognition 3.2.3 Keystrokes dynamics

Some other Physical and Behavioral Biometrics techniques , we discussed here, as follows: Nail identification, DNA patterns, Sweat pore analysis, Ear recognition, Odor detection, Walking recognition,
Gait etc.

4. COMPARISON OF VARIOUS BIOMETRIC TECHNOLOGIES

It is possible to understand if a human characteristic can be used for biometrics in terms of the following Parameters:

Table 1.1: Comparison between Biometrics Technologies

Biometrics	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	High	Low	Medium	High	Low	High	Low
Fingerprint	Medium	High	High	Medium	High	Medium	High
Hand geom.	Medium	Medium	Medium	High	Medium	Medium	Medium
Hand vein	Medium	Medium	Medium	Medium	Medium	Medium	High
Iris	High	High	High	Medium	Medium	Medium	High
Retinal	High	High	Medium	Low	High	Low	High
Signature	Low	Low	Low	High	Low	Low	Low
Voice	Medium	Low	Low	Medium	Low	High	Low
Thermo-gram	High	High	Low	High	Medium	High	High
Ear	Medium	Medium	High	Medium	Medium	High	Medium
Gait	Medium	Low	Low	High	Low	High	Medium
Keystroke	Low	Low	Low	Medium	Low	Medium	Medium
Odor	High	High	High	Low	Low	Medium	Low
Palm print	Medium	High	High	Medium	High	Medium	Medium
Facial-thermo	High	High	Low	High	Medium	High	Low

(i) Uniqueness is how well the biometric separates individually from another.

(ii) Permanence measures how well a biometric resists aging.

(iii) Collectability eases of acquisition for measurement.
(iv) Performance accuracy, speed, and robustness of technology used.
(v) Acceptability degree of approval of the technology.
(vi) Circumvention eases of use of a substitute.

Fingerprint Authentication

Fingerprint is one of the characteristics of the finger. Judging by the strong evidence that each fingerprint is always unique for each person. The scientific basis for friction ridges analysis is the fact that friction ridges wheels are stable and unique. Even identical twins don't have the same fingerprints.

Fingerprint recognition or fingerprint authentication refers to the automated process of checking the match between two human fingerprints. Fingerprints are waves that form on the surface of the fingers and thumb.

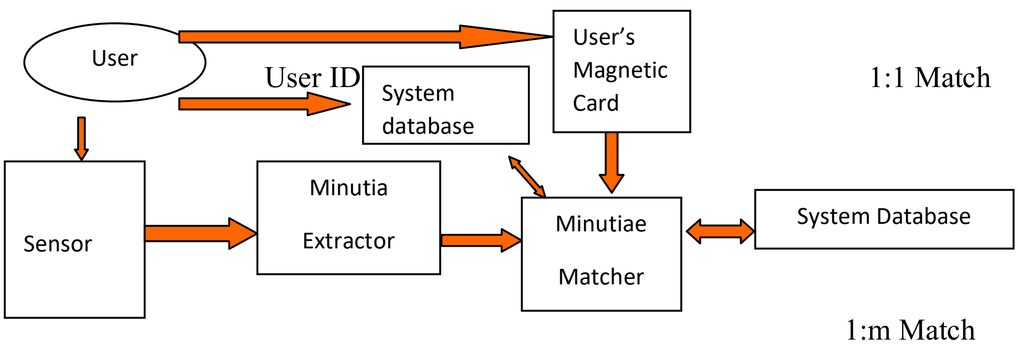


Fig 1.1 : Verification vs. Identification

ALGORITHM USED

Minutia-based algorithm

Minutia-based algorithm compare several minutia points (ridge ending, bifurcation, and short ridge) extracted from the original image stored in a template with those extracted from a candidate fingerprint. For each minutia point, a vector is stored into the template in the form:

$m_i = (w, type, xi, yi, \theta i)$ …………………. (1.1)

Where m_i is the minutia vector

type is the type of feature (ridge ending, bifurcation, short ridge) ,x_i is the x-coordinate of the location

y_i is the y-coordinate of the location , θ_i is the angle of orientation of the minutia

w is a weight based on the quality of the image at that location

(a) (b)

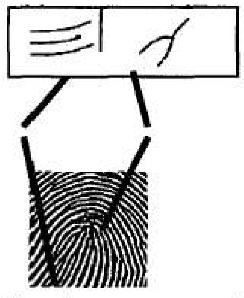


Fig 1.2: Minutia-based representation: (a) ending ridges (b) bifurcation ridges [17]

7. BIOMETRIC SYSTEM DESIGN

To implement a minutia extraction, a three-stage approach is used by researchers. They are preprocessing, minutia extraction and post processing stage see Fig 1.3.

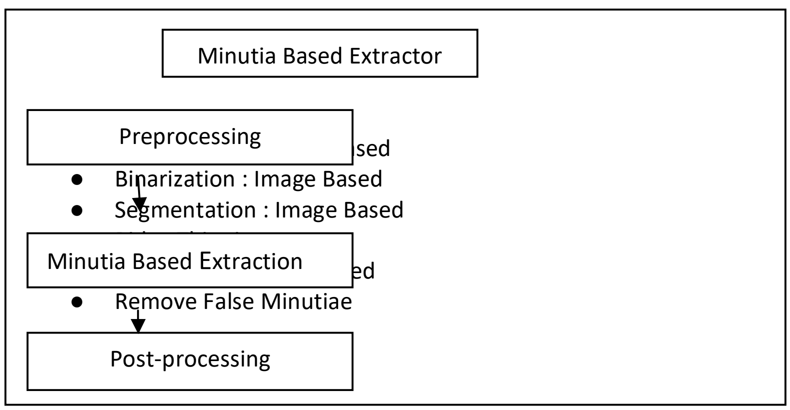


Fig 1.3: Minutia Based Extractor [16]

8. FINGERPRINT IMAGE PREPROCESSING

8.1 FINGERPRINT IMAGE ENHANCEMENT: Histogram Equalization: Histogram equalization is used to expand the distribution of image pixel values to improve perceptual information The histogram after the histogram equalization occupies all the range from 0 to 255 and the visualization effect is enhanced.

The probability density function of a pixel intensity level r_k is given by

$$P_r(h_k) = N_k / N \quad \text{……………………………..(1.2)}$$

Where: $0<=h_k<=1$ and k= 0, 1 ….255

N_k is the number of pixels at intensity level and N is the total number of pixels.

Gaussian Filter: Gaussian filter remove the noise and extra details from the original image. This filter attenuates the variation of light intensity in the neighborhood of a pixel.

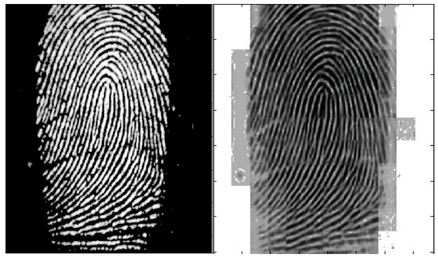


Fig 1.4: Fingerprint enhancement by Gaussian filter, Enhanced image (right), Original image (left)

The shown image at the left side of Fig 1.4 is also processed with histogram equalization after the Gaussian filter transform.

8.2 FINGERPRINT IMAGE BINARIZATION

Binarization is a method of transforming grayscale image pixels into either black or white pixels by selecting a threshold.

8.3 FINGERPRINT IMAGE SEGMENTATION

To separate foreground and background block wise variance threshold is used. In general, only a Region of Interest (ROI) is useful to be recognized for each fingerprint image.

8.4 ROI

The bound is the subtraction of the closed area from the opened area. Then the algorithm throws away those leftmost, rightmost, uppermost and bottommost blocks out of the bound so as to get the tightly bounded region just containing the bound and inner area.

Fig 1.5: the extracted ridge (left side) and the thinned ridge (right side)

8.5 FINGERPRINT RIDGE THINNING

Ridge Thinning is to eliminate the redundant pixels of ridges till the ridges are just one pixel wide.

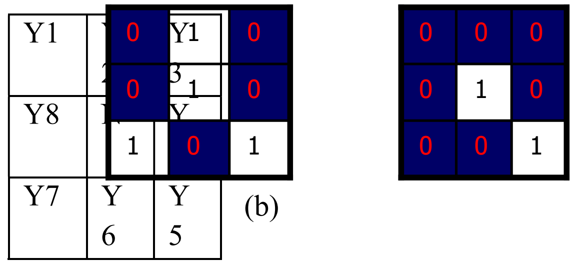
8.6 MINUTIA MARKING

This method, minutiae extraction is the intersection number (IN) concept, involves the use of the skeleton image where the ridge flow pattern is eight-connected. These minutiae are extracted by scanning the local neighborhood of each ridge pixel in the image using a 3□3 window.

A pixel M with its eight neighboring point (Y1,….., Y_8)are defined as well. The order of neighbors is assigned in a clockwise direction beginning from the upper left-hand corner. X (n) represents the value of pixel Y_n. If Y_n is a white pixel, then its value of X(n)will be 0. In addition, X(n) will be 1 if the pixel is black .The pixel N is determined as a ridge ending if it achieves the following condition [7,8].

$$IN=\Sigma h=1\ldots 8[X(h+1)-X(h)]=2, \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots.. \quad (1.3)$$

Where R (9) =R (1)



(a) (b) (c)

Fig 1.6(a): A 3□3 window ,(b) Bifurcation, (c) Termination

The pixel M is determined as a Bifurcation, the condition will be as follows

IN=Σk=1… 8[X (k+1) – X (k)] =6 …………………. (1.4)

In general, for each 3x3 window, if the central pixel is 1 and has exactly 3 one-value neighbors, then the central pixel is a ridge branch. If the central pixel is 1 and has only 1 one-value neighbor, then the central pixel is a ridge ending, see Fig 1.6 (b) &(c).

8.7 FALSE MINUTIA REMOVAL

The preprocessing stage does not totally heal the fingerprint image. For example, false ridge breaks due to insufficient amount of ink and ridge cross-connections due to over inking are not totally eliminated. These false minutias will significantly affect the accuracy of matching if they are simply regarded as genuine minutia.

MATCH SCORE: MINUTIA MATCH

Firstly we take the input query fingerprint image. Then Take the core point is located at the center of the feature map. After then locations of minutiae are mapped to corresponding sectors. Among the region of a sector, if one or more points are ridge endings or bifurcations, the value of the sector is added to denote number and kind of minutiae.

With the help of two equations find out the match score.

$$\sum_{j=b1}^{b2}\sum_{i=1}^{Nj}\left|S_k(Q_{ij})-T_{ij}\right|+\sum_{j=b3}^{b4}\sum_{i=1}^{Nj}\left|S_{2K}(Q_{ij})-T_{ij}\right|<TH \quad \text{………………. (1.5)}$$

where Qij is the i^{th} sector of j^{th} ring region in a query images, Tij is the corresponding sector in template images, Sk(y)means that x is rotated clockwise with k sector ,k=0,1,2,…..15.

TH is the threshold and the range of ring is $1<b1<b2$, $b2<b3<b4$ and $b4<N$.

matching score= N [$\sum_{i=1,2\ldots N}$exp (D_i)]$^{-1}$ …………………. (1.6)

The matching score can be computed according the formula [7].

$$D_j = \sqrt{\sum_{i=1}^{N_j}(Q_{ij}-T_{ij})^2} \quad \text{…………………. (1.7)}$$

Where Dj is the Euclidean distance between the two corresponding ring.

10. METHODOLOGY: BIOMETRIC CRYPTOSYSTEM

After the fingerprint authentication system as per algorithm 10.1 then again we use Elliptic Curve Diffie-Hellman Key Exchange algorithm for once more authentication see Fig 1.8:

10.1 BIOMETRIC CRYPTOSYSTEM ALGORITHM

Input Query Fingerprint

```
{
   if (Fingerprint matched with template)
      {
      then check the fingerprint of DBA's / Authorized Person of Organization
      if (Fingerprint matched)
            {
             // Again apply the cryptography key exchange scheme for authentication
                   Use Elliptic Curve Diffie-Hellman Key Exchange Algorithm
                   After process key matching then
          // Permission for accessing all secret data or Keys
           then print "You are an authorized person, please proceed"
            Generate or Show Secret message/Cryptography key / any secret data
            //The data generated to be used in concerned work and proceed further
            }
            else print "You are not an authorized person for the concerned work"
       }
      else print "Fake Input Query fingerprint Try Again"
}
```

11. THESIS WORK

The proposed approach was implemented on the FVC2004-DB1, a public domain database with 400 images (100 fingers 4 impressions each finger), cropped into 640x480 sizes, 500 dpi resolution. We apply the following step by step procedure and get correct result.

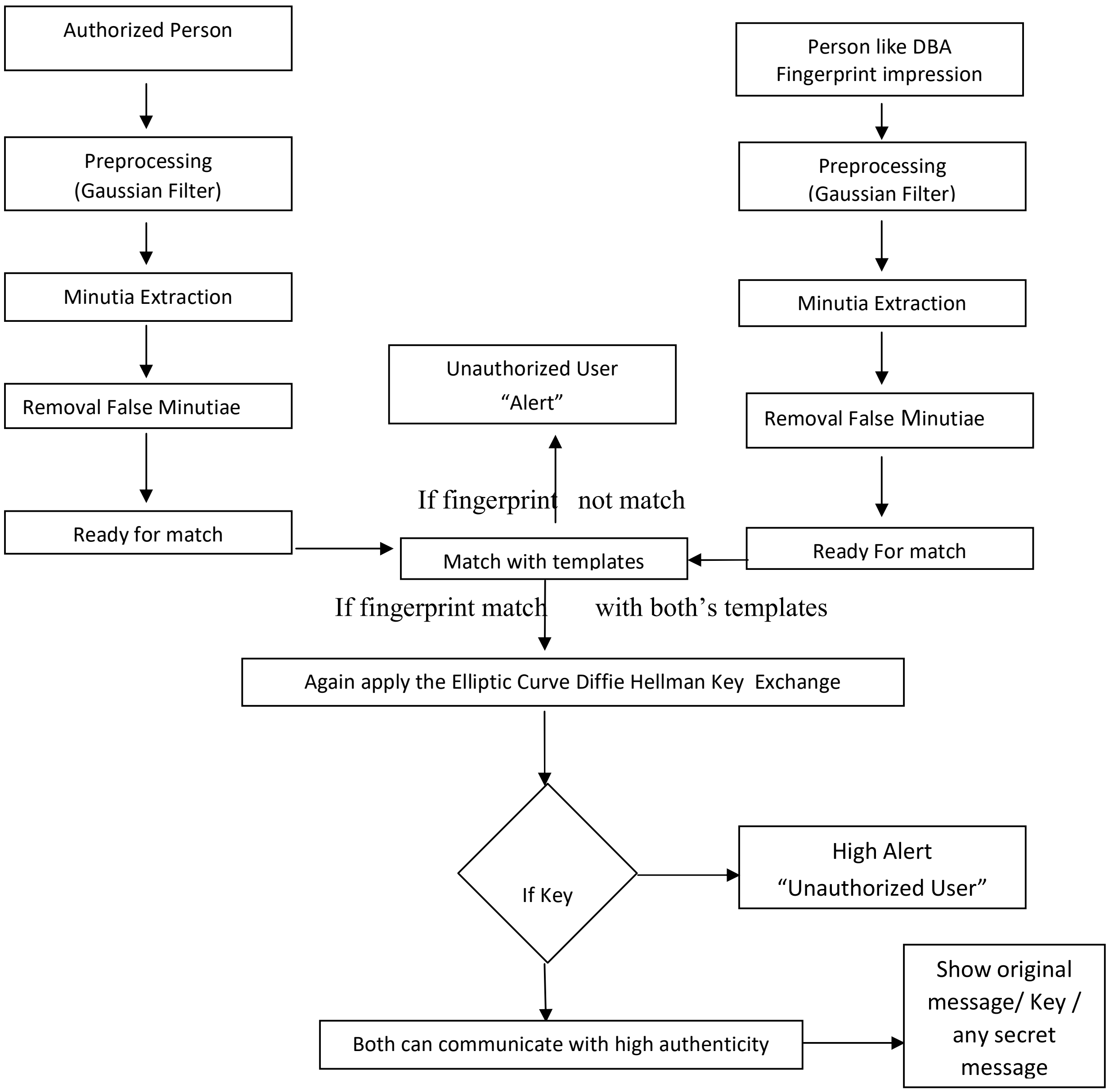


Fig 1.8: Biometric Cryptosystem Using Fingerprint Authentication and Cryptography Technique

12. EXPERIMENTATION RESULTS

Table 1.2: Simulation results of Gaussian filter based fingerprint matching with different Threshold value.

Gaussian Filter	TH_V=1	TH_V=2	TH_V=3	TH_V=4
FRR	16.0%	12.0%	10.0%	8.8%
FAR	0.20%	0.46%	1.80%	1.92%

The simulation results are shown in Table [1.2]. We get a better result by using Gaussian Filter, it is based on two parameter FAR and FRR.

13. CONCLUSION

Cryptography and biometrics are today's competitive technologies and are very useful in the digital environment for security reasons. The two technological activities developed are isolated, sometimes competing with each other. Based on this fusion system, biometric cryptosystems are categorized into many modes, such as using the RSA algorithm, using public key cryptosystems, etc., and in biometrics we can use filters and other methods. We can also use fingerprints as keys for cryptographic systems and in this work, if fingerprints match, then we use other key exchange methods, if current keys match, we provide cryptographic keys or secret messages or others freely other data to shared by this in a secure location, like a server, etc. The biometric cryptosystem can be implemented in three different modes: fingerprint matching, key matching or key generation, binding of both, and we can say that this is protection for three tires. Biometric matching is a very risky process and in this thesis we include two important aspects, firstly false acceptance rate (FAR) and secondly false rejection rate (FRR). Increasing FAR is more dangerous than FRR because when FAR is low anyone unauthorized can enter our system, so we have used the best filters to reduce FRR and increase FRR. In this paper, evaluation of image quality with fingerprints is carried out using Gaussian filter analysis. This algorithm uses a good level of analysis when evaluating fingerprint images. The advantage of this algorithm is that it ends with a decision to reject or accept the exposure, as well as the type of image enhancement technique required. It is developed by MATLAB (Matrix Laboratory) and related technologies.

References

Tabassam Nawaj, Saim Parvaiz,Arash Korrani, Azhar-Ud-Din,” Development of Academic Attendance Monitoring System Using Fingerprint Identification”, International Journal of Computer Science and Network Security (IJCSNS), Vol. 9, No.5, pp.164-168, 20 May 2009.

Peihao Huang,Chia Yung Chang, Chaur-Chin Chan” Implementation of An Automatic Fingerprint Identification System”,IEEE ,EIT,2007 Proceeding ,p.p. 412-417, 2007.

G.Sambasiva Rao, C.Nagaraju, Dr.L.L.S. Reddy, Dr.E.V.Prasad”A Novel Fingerprint Identification System Based on The Edge Detection”, International Journal of Computer Science and Network Security (IJCSNS), Vol. 8, No.12, pp.394-397,20 December 2008.

Lei Zhang , Mei Xei, " Realization of A New Style Fingerprint Recognition System Based on DSP" Proceeding of 2008 IEEE International Symposium on IT in Medicine and Education,p.p. 1107-1111, 2008.

Shunshan Li, Min Wie,Haiying Tang,Tiange Zhuang ,Michael H. Buonocore"Image Enhancement Method for Fingerprint Recognition Method", IEEE proceeding, Engineering in Medicine and Biology 27th annual Conference, Shanghai, Chaina, p.p.3386- 3389, September 1-4, 2005.

Xiaolong Zheng, Yangsheng Wang" Fingerprint Matching Based On Ridge Similarity ", IEEE proceeding ,ICASSP,p.p. 1701-1704, Year 2008.

Tsong-Liang Huang, Che-Wei Liu,Jui-Peng lin,Chien-ying li,Ting-Yi Kuo,"A Novel Scheme for Fingerprint Identification"IEEE ,CRV- 2005.

Milene Arantes, Alessandro Noriaki Ide, Jose Hiroki Saito "A System for Fingerprint Minutia Classification and Recognition" IEEE, vol. 5., pp-2474-2478, ICONIP-2002.

Bhagat, C., Mishra, A. K., & Aithal, P. S. (2022). Model for Implementation of e-Government Services in Developing Countries like Nepal. International Journal of Case Studies in Business, IT, and Education (IJCSBE), 6(2), 320-333. https://doi.org/10.5281/zenodo.7790868

Jha, P. B., Mishra, A. K., & Aithal, P. S. (2023). Operation of Vehicle Maintenance System in Context of Developing Countries Emphasizing Nepal. International Journal of Case Studies in Business, IT, and Education (IJCSBE), 7(1), 267-279. https://doi.org/10.5281/zenodo.7798162

Mishra, A. K. (2020). Project management: theory and practice from different countries. Tamilnadu: DK International Research Foundation. http://doi.org/10.5281/zenodo.4817542

Mishra, A. K., Jha, P. B., & Aithal, P. S. (2023). Business Operation Using Identification of Product in Context of Developing Countries Emphasizing Nepal. International Journal of Applied Engineering and Management Letters (IJAEML), 7(1), 112-126. https://doi.org/10.5281/zenodo.7798162

Mishra, A. K., Nepal, A., & Aithal, P. S. (2022). Industry 4.0 Concept for Nepal - Operating Virtual Farming Industry. In K. Prasad, P. S. Aithal, & A. Jayanthiladevi (Eds.), Proceedings on Future Trends in ICCT and its Applications in IT, Management and Education (pp. 31-35). ISBN: 978-81-949961-8-7. https://doi.org/10.5281/zenodo.7215189

Pokharel, R., Mishra, A. K., & Aithal, P. S. (2021). Practicability Assessment of Smart Village Project: A Case of Sandakpur Rural Municipality, Ilam Nepal. International Journal of Management, Technology, and Social Sciences (IJMTS), 6(2), 265-281. https://doi.org/10.5281/zenodo.5799392

A.K Jain, L. Hong, and R. Bolle, "On-Line Fingerprint Verification", IEEE Trans.Pattern Analysis and Machine Intelligence, vol. 19, no. 4, pp. 302-313. Apr. 1997,

Maya V. Karki, Dr. S.Sethu Selvi"a Novel Fingerprint Recognition system with Direction angles Difference ",IEEE, proceeding on ICCIMA, pp. 501-505, 2007.

Thai Raymond," Fingerprint Enhancement and Minutiae Extraction".

D. Simon-Zorita, J. Ortega-Garcia, S.Cruz-Llanas and J.Gonzalez-Rodriguez" Minutiae Extraction Scheme for Fingerprint recognition System" IEEE, pp. 254-257, vol-3 Oct, 2001.

Jiang and W.Yau,"Fingerprint Minutiae matching Based on the Local and Global Structure", proc. 15th Int'l Conf. Pattern Recognition, vol. 2,pp 1038- 1041, Sept. 2000.

Amengual, J. C., Juan, A., Prez, J. C., Prat, F., Sez, S., and Vilar, J. M. "Real-Time Minutiae extraction in Fingerprint Images", IEEE,Proceedings of the 6th InternationalConference on Image Processing and itsApplications, pp.871–875, July 1997.

A Wahab, S.H. Chin, and E.C. Tan,"Novel Approach to Automated Fingerprint Recognition", IEEE ,Proceeding on Vision, image and Signal Processing, vol. 145, no. 3, pp. 160-166, June 1998.

David Maltoni, Dario Maio, Anil k Jain, Salil Prabhakar," Hand Book of Fingerprint Recognition", Springer Verlag, New York, NY, USA, June 2003.

S.A. Cole. Suspect Identities " A History of Fingerprinting and Criminal Identification" ,IEEE, Harvard University Press, Cambridge, Massachusetts,London, England, 2001.

Marie Sandstrom, "Liveness Detection in Fingerprint Recognition System",A Thesis, Linkoping 10th June 2004.

[Markus Huppmann"Fingerprint Recognition by Matching of Gabor Filter-based patterns",15th January 2007.

Wu zhili" Fingerprint Recognition",Hong Kong Baptist University, A Thesis 19th April 2002.

N. Ratha, S. Chen and A.K. Jain, "Adaptive Flow Orientation Based Feature Extraction in Fingerprint Images", Pattern Recognition, Vol. 28, pp. 1657-1672, November 1995.

D.Maio and D. Maltoni" Direct Gray-scale Minutiae Detection in Fingerprints", IEEE Trans. Pattern Anal. And Machine Intell., vol-19(1), pp: 27-40, 1997.

L.C. Jain, U.Halici, I. Hayashi, S.B. Lee and S.Tsutsui "Intelligent Biometric Techniques in Fingerprint and Face Recognition", , the CRC Press. 1999.

http://www.biometrics.org.

S. Pannirselvam,P. Raajan " An Efficient Finger Print Enhancement Filtering Technique with High Boost
Gaussian Filter (HBG)" , International Journal of Advanced Research in Computer Science and Software
Engineering, pp- 370- 378,Vol 2, Issue 11, Nov 2012.

Ginu Thomas, K.Rahimunnisa, Sonima Parayil "Efficient Cryptographic Key Generation Using Fingerprint" International Journal of Scientific & Engineering Research,pp 942-945, Vol 4, Issue 4, April-2013.

Mouad .M.H.Ali , Vivek H. Mahale , Pravin YannawarA. T. Gaikwad ," Overview of Fingerprint

Recognition System" International Conference on Electrical, Electronics, and Optimization Techniques
(ICEEOT) - 2016 , IEEE, Nov 2016.

Jucheng Yang, Shanjuan Xie, Sook Yoon, Dongsun Park, Zhijun Fang, Shouyuan Yang, "Fingerprint matching based on extreme learning machine" in Neural comput& applic, London:Springer-Verlag, vol. 22, pp. 435-445, 2013.