IMPLEMENTATION OF IRIS RECOGNITION AS A SECURITY MEASURE AGAINST CYBER CRIME IN HYPERLEDGER FABRIC

Ramander Singh
AIIT, Amity University, Manesar, Gurugram, India
ramendera@gmail.com

Dr. Rajesh Kumar Tyagi
AIIT, Amity University, Manesar, Gurugram, India
rktyagi@ggn.amity.edu

Ashish Pandey
MCA, IMSEC, Ghaziabad, India
ashish.pandey@imsec.ac.in

Dr. Anil Kumar Mishra
Amity University, Manesar, Gurugram, India
akmishra2@ggn.amity.edu

Abstract— This paper is focused on reducing cyber crimes, which are based on identity-based authentication with respect to iris recognition. Today, we all depend on the technology developed for everything, and more new technology will be developed within the next two years. So every person needs a security system for their confidential data. They want to keep secrets. Lots of models are already implemented, such as traditional biometric technology, cryptographic technology, and even cyber crimes have increased very quickly. We proposed a model for digital authentication that provides a unique and safe identity for users because this is the most challenging issue in the mobility era for security, i.e., this model is based on a combination of mathematical algorithms and iris attributes that are unique for each and every person. Iris recognition gives more reliable and efficient security as compared to traditional cryptographic and biometric models.

Keywords— Ubiiris, Iris, Hyperledger, CASIA, Security, OTSU.

.

I. INTRODUCTION

Today, the big challenge faced in the COVID-19 pandemic is security, and the most important thing is authorization because authorization is the first and most important phase of network security. We know that the world totally depends on technology in this pandemic, and every day new technology is developed, as well as cyber crimes. In India during COVID-19 Feb 2021 approx 378.5 million peoples hunts of cyber crimes mainly which is based on brute- force – attack and side attacks by using mathematical equation and also 3.5 million peoples hunts in

financial sectors and also many attacks through apps such as 'Any desk app 'which is used to control users data in this days because authentication security is not strong.

In Jamtara district, Jharkhand which is the cyber hub of the India, they used phishing techniques to fools any people by telling him I am bank manager of any particular PSU bank your account will be closed in within 24 hours so bank send a OTP please tell me that OTP that is the way of techniques they used because the implemented model is based on traditional algorithm such as RSA, Diffi-Hellman, and so on. They know very well about these algorithm techniques, that's why they can easily dial any random number because this algorithm is based on random numbers which have key length is fixed. Jamtara district is also known as Deccan Chronicle because it trains thousands of students in phishing techniques and increases the cyber crime rate every day, which creates big challenging problems in financial sector.

So we proposed a model which is based on iris recognition, known as identity–based authentication. In India lots of organizations such as public and private organizations used traditional security models. In that place, we used the iris approach for more efficient security and hyperledger fabric as double security for all users . There are some examples:

- In financial sectors: In banking sector, we replace user ID, pin, or password in iris templates because a good iris scanner is easily affordable for banks if they replace signature and thumb in iris scanning because iris codes are unique for each and every person; this is more credible for customers and reduces the phishing rate in cyber crime.
- In online reservations: In recent days, there are lots of apps where users book their tickets by using any application. Generally, most of user use MakeMyTrip aap and search cheapest flight and then books but that particular flight every days reschedule. Then they called the customer service number for that specific flight, but they were told to call MakeMyTrip.Customers call care they instruct i am manager of that particular services Please open your phone pay account, BHIM account, or Net banking, and they will send a link to download the Any Desk app, which is a remote controller app, and they deduct all money of that particular customer. In this place if bank uses iris template instead of OTP then cyber theft not access any user accounts and reduce cyber rate. In these places if a bank uses iris template instead of OTP then cyber theft will not access any user accounts and reduce cyber rate.
- In the Digital Money Transfer application: we must use iris scanning in place of an OTP or PIN.
- In the name of Job: Now a days, every state have increased unemployed rate that's why there are 80% student post their resume in many social media, websites such as Indeed, Nokri.com, Facebooks, LinkedIn etc and so on . Then the cyber theft call them are you need job in good packages so I will send you link please registered and charges is 2000 After registration you give telephonic interview if you pass then we send your joining letter but you pay 10 lakh for security money before joining job because your payment is 80k , I will send bank details first you pay security money and send me screenshot in this ways they work of money laundry. There are lots of students who come under cyber crimes by using phishing.

In this way the cyber theft tricks customers and access their financial information so The RBI must adopt iris recognition in Banking sectors for protects money laundering, Money Frauds, and all financial crimes and reduce all cyber crimes because all cyber crimes done for only and only for money. And the RBI must be making rules for iris recognition in all financial sectors.

II. BACKGROUNDS

In 1936, Dr. Frank Burch was given the idea of using the iris for personal identification. He had identified the features of iris texture, which are complex and unique patterns. This part of the eye is used for security purposes. Because the iris is recognised by its characteristics, it is a unique feature for everyone. In the 1980s, the concept was given by Dr. Leonard Flom and Aran Safir [2] that no two iris are the same, even if these iris are in the same person. They researched and documented these concepts with the expectation of using the iris for identifying people, and they were awarded a patent in 1987 for these contributions for security purposes. After some time in 1994, Dr. John Daugman [1-4] implemented these concepts by using some mathematical algorithms using a canny detector for authentication. For the security purpose this model was proposed. Daugman [1-4] uses some classical and popular mathematical approaches for iris recognition, such as the band–pass Gabor filter for normalisation and segmentation of iris image for feature representation. This filter contains the real and imaginary parts of the iris, which are binarized to generate iris code, which is a compact and robust feature for the matching.

A. IRIS Recognition

The iris recognition system is used for verification, authentication, and identification that is in huge demand in security applications used for access control, authentication, banking systems, border control, forensics, etc. Iris recognition gives high security, more accurate and more reliable biometric identification systems, which are least invasive. Iris contains a random, complex texture and unique features, that's why it makes an ideal biometric recognition system. Irises are different between the same human eyes, and it also different between the both eyes i.e. left eye and right eye even both eye images are the same person. Iris has the ability to accurately measure iris textures and estimate a 1 in 1032 probability of false recognition rate because of a hundred degree rotation, which makes iris invasive in nature.

Now a days , new technology is being developed for real-life applications, in respect to security purposes, the iris recognition system is given a special place due to its high performance , reliability, uniqueness, and accuracy for identification.

There are mainly six phases to the iris recognition system.

1. Image Acquisition: Image collection or acquisition, we capture the image by using CCD cameras, an iris scanner, and also many ubiquitous/IoT recording devices.
2. Image pre-processing In image pre-processing, we remove all unwanted noise to improve image quality, control the size, color, and light of the image, the effect of spots/holes lying on the papillary part of the eye for the segmentation phase.
3. Segmentation: In segmentation, we detect the iris and pupil boundaries by subtracting the outer boundary from the inner boundary of the pupil.
4. Normalization: In normalization, we normalise the image of the iris for inconsistencies by using Rubber sheet Arrangement to normalise the Cartesian coordinates into polar with constant dimensions.
5. Feature extraction: In feature extraction, we extract the features of an image from a normalised image and encode this iris image for suitable recognition.
6. Matching: In matching, we compare the iris sample which is stored in the file's directories

and give the matching scores for verification.

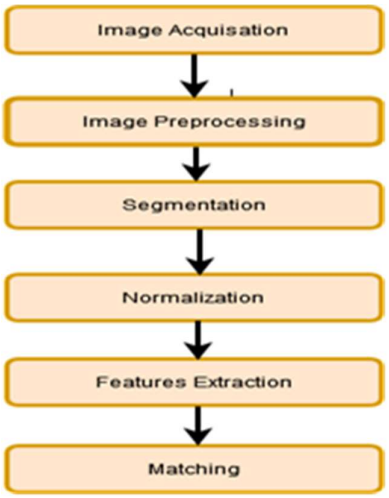

Figure 1. Phases of Iris Recognition

III. PREVIOUS WORK

Chengqiang and Mei [1] proposed a method for good iris feature extraction by using the Direct Linear Discriminant Analysis (DLDA) algorithm and the combination of Wavelet Transform (W T) algorithm and Direct Linear Discriminant Analysis for normalisation of the iris. For matching uses Euclidean distance (ED) to classify the iris templates. They experimented on version 2 CASIA databases,s which have 1200 images and achieved performance rate 1.44% and approximately 98.56% accuracy.

Kaushik and Prabir [2] proposed a model in which they tried to improve the feature extraction of the iris recognition system through chain code and zigzag collarette parts of the eye. In the segmentation phase we required useful parts of the iris so in this approach they get better efficiency as compared to previous. They used the Gabor wavelet (GW) algorithm for feature extraction and the SVM algorithm for matching. They experimented on version 2 CASIA databases that have 756 eye images and get a success rate approx 99.58%.

Ahmed M Sahran [3] proposed a method in which they used Discrete Cosine Transform (DCT) approach for features extraction of an iris image and Artificial Neural Network (ANN) for matching the image from database templates. This proposed method is tested on CASIA version 2 databases, which have 1200 eye images for 30 people, each people having 40 eye images for both eyes that is 20 for left and 20 for right were used, the dimension of image is 480*640 pixels. The total image size for this model was 600 and the achieved accuracy rate is 96.00% for the iris recognition.

Tallapragada and Rajan [4] proposed an approach in which they improve the performance rate of the iris recognition system. They used both approaches, i.e. Gray-Level Co-Occurrence Matrix (GLCM) and Haar Wavelet Transform (HWT) techniques, for feature extraction, which is stored in the database. For matching, they extract features by using an Artificial Neural Network (ANN). This proposed model is tested on 100 images of CASIA database and 95% accuracy rate approx.

Kumar, Raja, Chootaray, and Pattnaik [5] proposed a model in which they have adopted Principal Component Analysis (PCA) for features extraction by using a Discrete Wavelet Transform (DWT) of Iris pattern Iris code By using morphological techniques in different

principal such as K- Nearest Neighbors(KNN) , Support vector machine (SVM) and Random Forest (RF) on the CASIA database for achieving a different recognition rate or efficiency rate, such as 99.07% for KNN, 98.15% for RF and 97.23% for SVM.

Rashid, Shams and El-Awady [6] gave the new model i.e. based on local Binary Pattern (LBP) techniques for features extraction and matching they used two approaches i.e. Artificial Neural Network (ANN) and Learning Vectors Quantization (LVQ) on three database i.e. CASIA version 1, MMU version 1 and MMU version 2 of images for achieved accuracy rate of 99.87%.

Zhang and Guan [7] proposed a method based on the CASIA database version 1 of 756 images to achieved 99% recognition rate by using Empirical Mode Decomposition (EMD) algorithm for features extraction and by using K - Nearest Neighbors for matching.

Manisha and Sanjay [8] gave a model in which they applied both MMU and BATH database to achieved accuracy performance is 99.95%. For segmentation they used Daugman 's Integro - Differential Operator (IDO), for normalization Daugman 's Rubber sheet arrangement was used , Haar Transform (HT) for features filters and classification for Hamming Distance (HD)

Researcher	Database	Method	No. of image	Test image	Trained image	Accuracy
Chengqiang and Mei	CASIA V2	DLDA + ED	1200	—	—	98.56%
Kaushik and Prabir	CASIA V2	GW +SVM	756	—	—	99.57%
Ahmed M Sarhan	CASIA V2	DCT+ANN	600	400	200	96.00%
Tallapragada and Rajan	CASIA V3	(GLCM+HWT) + ANN	100	—	—	94.00%
Kumar, Raja, Chootaray and Pattnaik	CASIA V1	(PCA + DWT) + KNN, (PCA + DWT) + RF, (PCA + DWT) + SVM	756	108	648	99.07%, 98.15%, 97.23%
Rashad, Shams and El-Awady	CASIA & MMU1 & MMU2	LBP + (LVQ & ANN)	—	—	—	99.87%
Zhang and Guan	CASIA V1	EMD + KNN	756	99	666	99.00%
Manisha and Sanjay	MMU & BATH	(IDO + HT +DRS) + HD	—	—	—	99.95%

Table 1 comparison analysis

A. Limitation

The proposed model gives good recognition rate and performs accurately of the iris recognition system but still there are some problems:

1. If the image was not detected accurately then segmentation was not perfect, that's why it cannot segment the iris pattern successfully for eye images, so we can not get a secure model.
2. There is a need for a high security but low cost iris recognition system which can be easily affordable by various governments or other organizations from a security perspective.

IV. PROPOSED APPROACH

1. Preprocess the given image for removing unnecessary parts like noise, blurred, high

resolution

In image preprocessing we collect the image which are not always "useful" parts(IRIS), but there are some "unnecessary" parts are present in the image i.e. blurred, noise, high resolution etc and so on. In this phase we remove the effects of spots/holes laying on the papillary areas so first we convert the original color into grayscale image, then this image is changed into a binary image, and then this image is threshed by using Otsu threshing approaches, and also detect the iris and pupil for the next stages.

2. Segmented the given image using CASIA/UBIRIS.

Segmentation is the most important phase for iris recognition because it plays an important role for the system or model performance if improper segmentation can cause the wrong features to be extracted, that's why it reduces the efficiency of the system. The success of segmentation is dependent on the quality of the eye image. Also, light reflections may be occurring in the iris region that affect the iris pattern. So we use CASIA iris database eye images, which do not have light reflection.

3. Normalize the image

We see in segmentation phase iris is segmented completely of an eye image, then the next phase is normalization in which first we converts the iris pattern into constant dimension which allows the comparisons for features extraction for normalize the 'rectangular' forms of the iris templates which have constant radius. In normalization, Daugman's Rubber Sheet arrangement technique is used for converting a rectangular shape to a cartesian form by fixing the entire radius.

4. Do feature extraction using the OTSU approach.

After successfully completing the normalisation stage for the iris region, the iris pattern is to go for feature extraction. Before extraction, we binarized all the images for better extraction by using adaptive Gaussian and Ostu approaches because feature extraction plays an important role in the iris recognition system. Because the system depends on the IrisCode that is extracted from iris. In this stage, the Gabor filter is used to filter the accurate feature, and a combination of adaptive Gaussian and Ostu techniques are used for binarization.

5. Match the previous and present Image on the basis of matching score

In these steps of iris recognition, we use the Hamming distance (HD) approach to calculate matching scores by comparing the present and previous iris codes, which are stored in the database. If the matching score is 0.00, then this image belongs to the same image, and if the matching score is 0.3244 then the iris image belongs to two different images. Finally, we analysed all bits of the images.

6. Save the score on Hyper-ledger fabric.

In these steps of iris recognition we save all bits of the images on the Hyper-ledger fabric. No alteration can be done of saved data due to hyperledger blockchain, if any body is altered the bits of saved images new block is generated by which we can easily trace what and which time the data is changed. Hyperledger fabric is an open source enterprise permissioned blockchain, so that we may achieve double security. Hyper-ledger fabric is the most trending technology, which provides more security, reliability, and privacy over the cloud.

7. Verify and validate the result.

We have reached the last stage of the iris recognition process, in which we validate the matching score and store it on the Hyperledger fabric. If the administrator of the block chain

confirms that the user in question has permission to participate in the process, then the validation for the process is successful; otherwise, only login credentials are permitted.

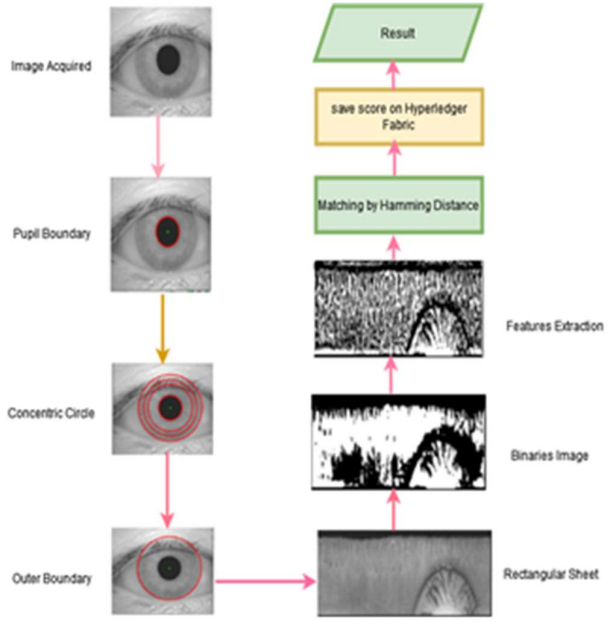

Figure 2: Results of all stages of CASIA database

V. Methodology

There are many phases in which different algorithm is uses as described in below table

Phases	Algorithm
Pre-processing	By using sensor, digital device
Segmentation	Hough transformation, OTSU approaches
Normalization	Rubber sheet model
Feature Extraction	Gabor filters
Matching	Hamming distance

Table 2.

A. Segmentation: The Hough Circle Transformation

The Hough Circle Transformation is a widely used algorithm for image processing which is used to detect the geometric shape of a digital image, such as lines, circles, and curves, which can be easily detected by the Hough Circle Transform and can be derive the radius and coordinate centre of the iris and pupil regions. Wildes et al.[1], Kong and Zhang [2], Tisse et al. [3], and Ma et al. [4] proposed segmentation which is based on the Hough Circle Transform. First of all, we generate an edge map, by calculating the average intensity of pixels in the eye image, and then we threshold the obtained results. From this edge maps we get Hough circles variable of circles which is passing through each and every points such as coordinates of center (Xc, Yc) and radius r, that can defined any circle by using given equation

$$Xc^2+ Yc^2-r^2=0$$

At the point of maximum radius, the coordinates of the circle give the best/maximum point of Hough Circle. So we convert its polar to Cartesian form for finding best point are given in

equation

$$Xc = r\cos(theta)$$
$$Yc = r\sin(theta)$$

Where (Xc, Yc) is the mean value of the circles and theta is angle of rotation with the axes.

Normalization: Daugman's Rubber Sheet Arrangement

This rubber sheet arrangement is mainly used for iris normalisation for the next step, i.e. feature extraction. The main objective of rubber sheet arrangement is to reset each edge point in the iris region to change into polar coordinates (r,θ) where r is the radius on the interval of [1,0] and θ is rotation of angle on the interval of [0,2π].

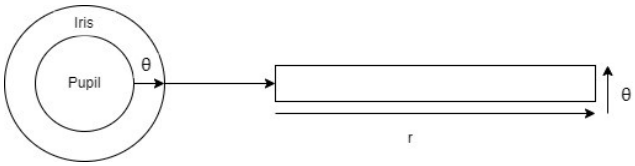

Figure 3: Daugman's Rubber Sheet Arrangement

Then converts the iris region from (X, Y) Cartesian coordinates in to the polar (r,θ) coordinates which are given below

$$I(X,Y) \quad I(r,\theta)\ldots\ldots$$

Where

$X(r,\theta) = X\cos(\theta)\ldots\ldots..$

$Y(r,\theta) = Y\sin(\theta)\ldots\ldots.$

Where I(X,Y) = image of the iris

(X,Y) = Cartesian coordinates

(r,θ) = Polar coordinates

(Xc &Yc) and (X&Y) are the coordinates of iris and pupil with respect to θ.

The rubber sheet arrangement has a problem with pupillary dilation, an unwanted region, and inconsistencies in size, so in order to remove this, we normalised the iris template in constant dimensions.

Features Extraction: - Gabor Filters

Gabor filters are generally applicable for feature extraction, which provides optimal solutions for the recognition of points and special frequencies. A Gabor filter is formed by applying the sine/cosine wave with the Gaussian theorem because this is able to localise in both space and recurrence. A sine wave is absolutely localised in recurrence, but not localised in space. By low quality of image of localization space, through with loss of localization in frequency. Gabor filters contain two parts, i.e., the real, which is specified by a cosine modulated Gaussian algorithm and gives even symmetric components, and another is an imaginary part, which is specified by a sine wave modulator and gives odd asymmetric components.

The Gabor filter is the standard algorithm for image processing, comes after Dennis Gabor, which is based on linear filters used for edge detection. Gabor filter use 2- Dimensional filter which is given below in equation is:-

$$G(x,y) = \exp\left(\frac{x2+\gamma 2y2}{2\sigma 2}\right)\cos\left(i\left(\frac{2\pi x'}{\lambda}+\Psi\right)\right)$$

Where $x' = x\cos(\theta)+ y\sin(\theta)$

$$Y' = -x\sin(\theta) + y\cos(\theta)$$

This equation shows the real and imaginary parts, which depend on the sign of the 2D filters.

Matching:- Hamming Distance

The Hamming Distance is an algorithm for classification that can recognise how many matching scores or bits are in the match between two iris samples or not. By using the hamming Distance(HD) algorithm of two bits samples , we can check whether the two patterns were generated from the same irises or from different irises for finding the correct matching score. The Hamming Distance Algorithm is the sum of bits i.e. the sum of the exclusive-OR operation between two template bits, that is A and B over N, which is the total number of bit patterns. The equation is given below:

$$HD = \frac{1}{N}\sum_{i=1}^{n} Xi\,(XOR)Yi$$

Because each individual iris pattern has unique characteristics with the high degree of the freedom, every iris pattern will create an Iris-Pattern that is different from each other which is generated by other iris pattern and also if we compare two iris pattern of the same iris will be high matching score i.e. 0.00000 and we compare two iris pattern of the different iris will give the matching score i.e. 0.34677.

B. Results

In this step, we pick a circle with the largest radius, which is in red, to compute concentric circles of the Hough Circle transform then prints these concentric circles in red color. The intensity of each pixel of the concentric circle is plotted in a graph to find a bigger radius for actual iris detection, as given below.

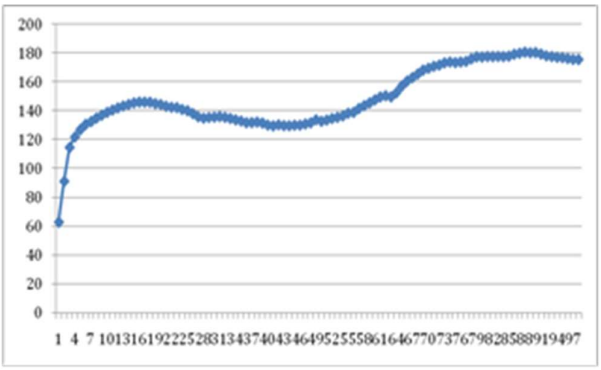

Figure: 4 Average intensity of radius at point 64 give best images at this point is in increasing orders

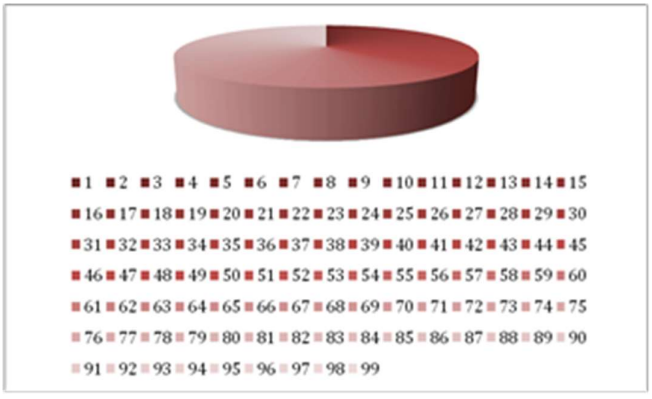

Figure: 5

In the figure 5 pie chart diagram, numbers 1 to 64 have correct image detection, which gives correct segmentation; that's why we have the best image quality for feature extraction, and numbers 65 to 99 have poor image quality, that's why we can't properly find iris templates.

VI. Future Work Application

There are many different applications in different places during COVID-19, such as:

- Biometric Attendance: Due to COVID-19, many places use fingerprint biometric attendance. This is not possible, so we can use iris biometric attendance instead of fingerprints for such places. But it is not possible to use every place of the iris scanner due to its highly cost effectiveness so we make a less cost effective application app which can be easily installed and easily controlled by organizations for verification.
- In Financial Institution: we know that today era is digital era that's why in India has increased rapidly cyber crime due to unaware of cyber crimes regarding transactions because mostly customers are belongs in villages and they are uneducated person. Mostly, these people are targeted by cyber criminals due to their unawareness, so in the future, banks must use iris recognition for authentication of users instead of a pin or password. Banks should be developing software which is less cost-effective but more reliability.

In Airport: If we use the iris recognition system in every airport, then we will recognise the illegal and unauthorised person who makes duplicate passports for their own profit. Further we can save the Iris data of any person on the block chain so that nobody can not alter or replace given information that is secured for the first time on the block chain technology. Like HyperLedger ledger fabric, HyperLedger ledger fabric is an open source enterprise permission block chain. Block chain supports the double security to the iris recognition model we would implement in future.

Figure 6.

VII Conclusion

In this model of iris recognition system, with the help of block chain technology, i.e., hyper ledger fabric, which gives better efficiency and a robust system for verification and authentication for security purposes, this model was based on two databases of gray-scale eye images, namely the CASIA database and the UBIRIS database, for better efficiency and to verify the performance of the iris recognition system, and implemented on "Python" for a less cost-effective system. The main objective of this model is to reduce cyber-crimes in financial sectors, the defence sector, healthcare, education, e-voting, e-governance, etc., by implementing iris recognition techniques for customers' safe transactions and ensuring that no

transaction can be accessed by any unauthorised users.

References:

1. J. Daugman. How iris recognition works. Proceedings of 2002 International Conference on Image Processing, Vol. 1, 2002.
2. R. Wildes. Iris recognition: an emerging biometric technology. Proceedings of the IEEE, Vol. 85, No. 9, 1997.
3. J. Daugman. Biometric personal identification system based on iris analysis. United States Patent, Patent Number: 5,291,560, 1994.
4. Daugman, J., How iris recognition works. IEEE Transactions on circuits and systems for video technology, 2004. 14(1): p. 21-30.
5. CASIA Database. http://www.cbsr.ia.ac.cn/english/IrisDatabase.asp.
6. UBIR Database. http://iris.du.ubi.pt/IrisDatabase.asp.
7. Database of Indian Institute of Technology Delhi. http://www.comp.polyu.edu.hk/~csajaykr/IITD/Database_Iris.htm.
8. L. Masek, "Recognition of human iris patterns for biometric identification," Ph.D. dissertation, University of Western Australia, 2003.
9. Raja, K., R. Chhootaray, and S. Pattnaik, PCA based Iris Recognition using DWT. Int. J. Comp. Tech. April, 2011. 2(4): p. 884-893.
10. Roy, K. and P. Bhattacharya. An iris recognition method based on zigzag collarette area and asymmetrical support vector machines. In 2006 IEEE International Conference on Systems, Man and Cybernetics. 2006. IEEE.
11. Sarhan, A.M., Iris Recognition Using Discrete Cosine Transform and. Journal of Computer Science, 2009. 5(5): p. 369-373.
12. Tallapragada, V.S. and E. Rajan. Iris recognition based on combined feature of GLCM and Wavelet transform. In Integrated Intelligent Computing (ICIIC), 2010 First International Conference on. 2010. IEEE.
13. Das, A., Recognition of Human Iris Patterns. 2012.
14. R. Wildes, J. Asmuth, G. Green, S. Hsu, R. Kolczynski, J. Matey, S. McBride. A system for automated iris recognition. Proceedings IEEE Workshop on Applications of Computer Vision, Sarasota, FL, pp. 121-128, 1994.
15. Y. Zhu, T. Tan, Y. Wang. Biometric personal identification based on iris patterns. Proceedings of the 15th International Conference on Pattern Recognition, Spain, Vol. 2, 2000.
16. Chand, M. "Do You Need A Blockchain." C# Corner, January 4, 2018, https://www.c-sharpcorner.com/article/do-you-need-a-blockchain2/.
17. Peck, Morgen E. "Do You Need a Blockchain?"IEEE Spectrum: Technology, Engineering, and science News, IEEE Spectrum 29, 2017, htpps://spectrum.ieee.org/computing/networks/do-you-need-a-blockchain.
18. Greenspan, G., "The Blockchain Immutability Myth,"MultiChain, May 4, 2017. https://www.multichain.com/blog/2017/05/blockchain-immutability-myth/
19. Z. Zhao and A. Kumar, "An Accurate Iris Segmentation Framework under Relaxed Imaging Constraints Using Total Variation Model," in 2015 IEEE International Conference on Computer Vision (ICCV). IEEE, 12 2015, pp. 3828–3836.
20. K. W. Bowyer and M. J. Burge, Handbook of iris recognition. Springer,2016.

21. J. Daugman, "How Iris Recognition Works ", IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 14, NO. 1, JANUARY 2004.
22. S. Minhas, M. Y. Javed,"Iris Feature Extraction Using Gabor Filter ", International Conference on Emerging Technologies, IEEE 2009.
23. S.Agarwal and N. Kumar, "Hyperledger: An industrial approach to block chain," in Hyperledger. USA: Elsevier, 2020, pp.2-21.
24. H. Zhang, X.Chen, X.Lan, H.Jin, and Q. Cao, "BTCAS: A Blockchain-based Throughly Cross- Domain Authentication Scheme," Journal of Information Security and Application, vol.55, Dec.2020, DOI:10.1016/j.jisa.2020.102538.
25. Sylim P, Liu F, Marcelo A, Fontelo P, "Blockchain Technology for Detecting Falsified and Substandard Drugs in Distribution: Pharmaceutical Supply Chain Intervention, " JMIR Res Protoc 2018;7(9):e10163, URL: https://www.researchprotocols.org/2018/9/e10163 , DOI: 10.2196/10163.
26. F. Jamil, L. Hang, K H .Kim and D.Kim , "A novel medical blockchain model for drug supply chain integrity management in a smart hospital," Electronics, vol.8, 2019, pp. 505-505
27.M .Uddin,"Blockchain Medledger:Hyperledger fabric enabled drug traceability system for counterfeit drugs in pharmaceutical industry", International Journal of Pharmaceutics, vol.597, Mar. 2021, DOI:10.1016/j.ijpharm.2021.120235.
28. K .Abbas, M .Afaq, T. Ahmed Khan andW-C.Song, "A Blockchain and Machine Learning-Based Drug Supply Chain Management and Recommendation System for Smart Pharmaceutical Industry", Electronics, vol.9,2020, pp.852-852.
29. F .Fournier, and I .Skarbovsky, "Enriching Smart Contracts with Temporal Aspects" in International Conference on Blockchain. Cham, Springer International Publishing, 2019,pp.126-141.
30. Chow SS, Weng J, Yang Y, Deng RH," Efficient Unidirectional Proxy Re-Encryption," In Bernstein, Daniel J, Lange, Tanja(eds) International Conference on Cryptology in Africa, Berlin, Heidelberg, Springer Berlin Heidelberg, vol.6055, pp:316-332.
31. N. Kumar S. and M. Dakshayini, "Secure Sharing of Health Data Using Hyperledger Fabric Based on Blockchain Technology," 2020 International Conference on Mainstreaming Block Chain Implementation(ICOMBI),Bengaluru,India,2020,pp.1-5, doi:10.23919/ICOMBI48604.2020.9203442.
32. S. Kim, J .Kim,and D .Kim, "Implementation of a Blood Cold Chain System Using Blockchain Technology," Applied Sciences, vol.10, 2020, pp. 3330-3330.