

Investigating Scope of Enhanced Biometric Security for IOT based Digital Wallet

Tanya Chauhan¹ and Ajmer Singh²

^{1,2}DCRUST/CSE, Murthal, India

Email: tanyachauhan9654@gmail.com, ajmer.saini@gmail.com

Abstract—Biometric Security System has been integrated to edge detection mechanism to improve performance while protecting Digital Wallet in IoT System. As we all know that the use of digital wallets is increasing day by day, therefore there is a need to develop such kinds of efficient model to secure different digital wallets. There have been several techniques or mechanisms available which are providing security of digital wallets but these existing methods or techniques have their limitations. Some of the existing security mechanisms provide limited security while some are performing poorly. Therefore iris-based biometric mechanisms with the integration of edge detection have been proposed for the security of digital wallets. The integration of canny based edge detection is made to decrease the space consumption of the biometric model. Moreover, it is also reducing the time consumption during a comparison operation. In the future, this iris-based digital wallet security system would be used as a secure system than other biometric techniques.

Index Terms— Biometrics, Iris recognition, Segmentation, Normalization, Canny edge detection, IoT.

I. INTRODUCTION

The need for IoT systems is increasing day today. Some of the IoT systems support digital wallets that are capable to store assets digitally. The security of such digital assets is a great challenge. To provide security to these digital wallets, biometric mechanisms [1, 2] are applied. The biometric system allows user to access their assets by authenticating themselves online by their biometric features and pattern [3, 4, 5]. These biometric features could be retina, Iris [6,7,8], voice, fingerprint. But some time use of a single biometric feature remains risky. Thus multiple biometric inputs are made to secure the digital assets from an unauthentic person. In other words, more than one physical trait is considered for biometric authentication.

But the issue of multiple biometric samples is space consumption and comparison time. Multiple biometric samples take a lot of space for the storage device. Moreover, the comparison time of multiple biometric samples is more as compared to a single one. So if multiple biometric samples are used to increase the security of IoT based digital wallet then performance gets degraded. In the research paper section, 1 has introduced the role of biometric security to protect the digital wallet in IoT systems. Section 2 is presenting the existing researches in the field of IoT and Biometric security along with the objective, methodology, and outcomes of those researches. Section 3 is presenting the research problem and section 4 has focused on the need for the proposed research. Section 5 has presented the research proposal where the proposed model has been compared with the traditional model and the flow chart of the proposed work is also described.

II. LITERATURE SURVEY

There have been several types of research in the field of IoT and biometrics. Several cryptos biometric [1] have been proposed that are making use of iris. Some biometric researchers have considered wavelet transformation [2] mechanisms to provide biometric security. Research work has been performed to propose fusion approaches in multi-biometric cancellable recognition [3] while some work has extracted biometric binary strings [4] with the minimal area. Research has made use of FRR curve for hamming distance classifier. Biometric-based previous researches have also introduced Multispectral scleral patterns [5] for ocular biometric recognition. On the other hand Face as well as Iris Recognition [6] in case of Mobile Engagement have been introduced. Previous research considered iris-based security [7] along with pattern recognition to protect systems from unauthentic access. Iris localization [11, 12, 13, 14] has been focused on frequently in order to enhance accuracy of biometric system. There have been several researches in field of biometric that are presenting the scope and limitations of biometric technology [16, 17, 18, 19, 20, 21, 22, 25]. Moreover some researchers have also used edge mechanism [23] to enhance accuracy at the time of localization of iris[24] based biometric system.

In 2012, R. Álvarez [1] proposed crypto-biometric mechanism. this system is depending on iris. They make use of fuzzy logic in their research. They stated that major utilization of Biometrics has been identification as well as authentication. This is performed with support of physiognomical characteristics of human being. Research has also consider the role of biometrics in offering support for Cryptography with support of biometric traits. Authors have also proposed a system to allow users to get key by their own biometric features. Features and efficiency to choose significant parameters is capable to give better security. Finding concluded that fuzzy logic has supported efficient decision making.

In 2012, GauravBhatnagar [2] did research to propose Fractional dual tree complex. Research is based on wavelet transform. Moreover research is considering its application in biometric security. They make use of Wavelet transformation in their research. Their research was contributed security for communication system. Research has considered Dual tree complex wavelet has been considered significant for transformation. Moreover author generalized advancement in signal as well image processing with the support of coalescing dual tree complex wavelet transform. It is also supporting fractional Fourier transform. Research is applicable in field of biometrics, image compression. Biometric has been selected as main application. Thus recent technique has been proposed to protect biometrics at the time of communication.

In 2013, Anne M.P [3] did research that is proposing fusion approaches. Approach is proposed for multi-biometric cancellable recognition. Research provided expert mechanism for biometric security. During research, author has adjusted ensemble structure that is to be utilized in case of biometric system. Researchers are using two biometric modalities that are voice and iris information for multi-biometrics. Research paper is specifically investigating performance in case of different fusion mechanism for context of recognition of multi-biometrics.

In 2011, C Chen [4] did Extracting biometric binary strings. Operation has been performed with minimal area. It has been implemented under FRR curve for hamming distance classifier. Research is suitable for biometric binary string extraction. Getting binary strings from real-valued biometric templates has been considered the fundamental step during template compression as well as protection. Research has considered fuzzy based commitment, and extractor. Researcher has provided theoretical model of HDC depending on error probabilities during quantization. Model is predicting false acceptance rate as well as false rejection rate. It has been considered as a function of Hamming distance threshold. Moreover research is proposing area under FRR curve that is having the optimized bit allocation.

In 2012, Simona Crihalmeanu [5] proposed Multispectral scleral patterns. The objective is to perform ocular biometric recognition. Research has supported Pattern Recognition Letters and considered Biometrics as science of recognizing people according to their physical as well as behavioral traits. These traits could be finger or palm print, face, iris, and voice. In all such features, ocular biometrics is gaining popularity because of major progress in area of iris recognition. Article is investigating utilization of sclera texture along with vasculature patterns that is clear in the sclera as a potential biometric. Experimental outputs are conveying potential of such biometric in ocular dependent recognition mechanism.

In 2014, Maria de Marisco [6] proposed face as well as iris recognition system. Research is suitable for mobile engagement. Research has considered that the growing use is mobile and smart phones their effect on technological advancement. Research has found face and iris recognition attractive because they are reliable. Moreover there is limited requirement of webcam. Research is describing Face as well as Iris Recognition in case of mobile Engagement. Research has considered biometric application depending on a multimodal recognition in case of face and iris. This mechanism has been developed for mobile devices. This research is known as FIRME that could perform regular reidentification as well as best sample selection.

In 2013, Javier Galbally [7] did work to perform image reconstruction that is related to iris. Operation is performed using binary templates. This work is suitable for binary templates. Binary iriscode has been considered compact visualization in case of iris graphics. The research work has proposed a novel probabilistic mechanism that is depending on genetic algorithms. Objective of mechanism is to perform reconstruct of iris images from binary templates. It is analyzing the similarity among reconstructed synthetic iris image as well as real one. The performance of reconstruction mechanism has been by finding the chances of successfully matching. The results shows that reconstructed images are looking realistic.

In 2013, Ujwalla Gawande [8] proposed bimodal biometric system. Research is performing feature level fusion in case of iris as well as fingerprint. Research is working on feature level fusion of iris. Research is making use of biometric systems that is trying to impersonate decisions that are made by humans to perform identification as well as comparison matching. Author has stated that several people in this world are making use of biometric due to various reasons. It has been observed that Iris scan is used by India's UID project Aadhaar. Moreover it is also using fingerprints to check people and provide them UID.

In 2014, Marta Gomez-Barrero [9] is proposing multimodal biometric systems. Author used pattern recognition as research methodology. Research has focused on application of face and iris fusion. Research has observed certain applications depending on multimodal interaction. It is crucial to confirm *who* is doing it along with what has been done. Research has focused on prevention of fraudulent use of system. This research has represented a highly efficient automatic recognition solution in case of such type of applications.

In 2011, Karen Hollingsworth [10] is performing genetically identical irises that are having texture similarity. Author make using of Image and vision. Research finding have resolved the issues of previous iris systems. Researchers have observed recognizable similarity in left and right irises of an individual. This mechanism is termed as Iris texture analysis that is differing from standard iris biometric algorithm. The research model is capable to answer questions that could not be answered by iris biometrics.

In 2012, Farmanullah Jan [11], did research to performing iris localization in image of frontal eye. Objective is to propose less constrained iris recognition mechanism. Research used Digital Signal Processing to fulfill objectives. Results concludes that research work is proposing less constrained recognition mechanism. Experimental results are concluding that model is tolerant to off-axis eye images. Moreover it is also tolerant to specular reflections and non-uniform illumination

In 2013, Farmanullah Jana [12] proposed Iris localization system depending on Hough transform. Research is considering a radial-gradient operator. This work has proposed Hough transform, a radial-gradient operator. It has been concluded that this research has provided efficient approach for biometric security. Research considered localizing iris in non-ideal data containing the noisy issues as performance degrading issues. Study is proposing reliable mechanism to localize iris in images robustly. Outputs of simulation are fetched from CASIA-IrisV3, CASIA-IrisV4, MMU V1.0, and MMU V2.0 iris databases. Outputs are showing superiority of proposed mechanism over contemporary mechanism.

In 2013, Farmanullah Jana [13] Proposed non-circular iris localization mechanism. Research is making use of image projection function as well as gray level statistics. Author makes use of Iris localization algorithm. This work is supporting non circular iris localization. According to research Iris recognition technology is identifying an individual from its iris texture with great precision. Author has proposed a reliable iris localization that is locating a coarse eye location in eye image with support of integral projection function at initial stage. Then they have localized the pupillary boundary in a sub image with the support of a reliable mechanism depending on histogram-bisection, image statistics, eccentricity, and object geometry. Then they localize limbic boundary using a robust scheme depending on radial gradients.

In 2013, Farmanullah Jana [14] has implemented reliable iris localization. Research is making use of Hough transform. Research has also considered histogram-bisection and eccentricity. The research is making using of signal processing mechanism. Research has provided reliable approach for biometric security. Author proposed a reliable iris localization mechanism. It is consisting localizing a coarse iris location in eye image with help of Hough transform and image statistics. Researcher has also performed localizing the pupillary boundary with support of bi-valued adaptive threshold. Simulation results states the superiority of proposed mechanism in some state of the art iris localization mechanism.

In 2013, Farmanullah Jana [15] has implemented dynamic noncircular iris localization mechanism. Research is dealing with non-ideal data. Research work is making use of Iris localization. Research has supported dynamic non circular localization. Research has tested on different public iris databases. These databases are CASA V1.0, CASIA-Iris-Lamp, IITD V1.0. Simulation results of this research have been compared to different state-of-the-art mechanism to endorse its performance that is satisfactory.

In 2018, Choudhury B [16] did research to perform survey of biometric system. Pros cons and working of various biometric system has been presented in this research. Work is presenting a review on state-of-the-art and analysis of various mechanism of biometric dependent authentication system. Research is considering cancelable biometric systems. It has focused on cancelable biometrics in order to show benefit of biometric. Author has proposed a highly secure mechanism for cancelable biometrics. They made use of non-invertible functions. These functions are depending over Discrete Cosine Transformation. Functions are also making use of Huffman encoding.

In 2015, Sharadha Tiwari [17] reviewed the latest updates in biometric. New trend and technology used in biometric security system is discussed. Research has presented the role of biometric systems for today's high security applications. Research paper is introducing fundamentals of biometric identification. It is also describing the main biometric mechanisms that are in current use. Conventional biometric identification systems like iris, fingerprint, face, DNA and speech are also discussed with their limitations. Research has also performed the survey of unimodal as well as multimodal biometrics.

In 2014, Gursimarpreet Kaur [18] performed comparative analysis of biometric modalities. Research has compared modalities in case of different biometric techniques. Research considers biometrics as inevitable tool for growing security concerns. Author has presented biometrics as technology of recognizing human according to their physical and behavioral features. These physical characteristics might be fingerprint, face, iris, signature etc. This is possible to confirm identity with help of biometric techniques. Researchers have considered different areas where biometrics has been used frequently such as forensic, identification, security and presented overview of biometrics. Different biometric modalities have been analyzed according to various perspectives. Research has also described the feature sets of modalities.

In 2013, Himanshu Srivastva [19] compared the different biometrics to recognize the suspicious person. Application of biometric for security has been considered in this research. Researcher described novel comparison according to different aspects to allow quick selection in case of biometric device deployment for particular environment. Research is showing comparison in different type of biometric systems that are available in present scenario. Present security system are used in banking, passport as well as credit cards. These are also used to provide security to smart cards and allow access control in network using identification mechanism. Research is introducing biometric systems for this purpose. Research is focusing on working mechanism of biometric systems.

In 2006, A K Jain [20] discussed biometric as tool of security. Role of biometric in forensic and security system has been elaborated. Research is providing overview of biometrics and explained several issues found in previous researches. These issues are required to be addressed. The objective of this research is to develop effective biometric mechanism to provide security to information. Research is in examining applications that make use of biometric scan to resolve problems related to security of information security. Moreover this work is also enumerating basic challenges faced in real application by biometric systems. This research has also provided solutions to resolve the problems of scalability as well as security. The application area of research is huge size authentication mechanism.

In 2004, Jain K Anil [21] considered the application and role of biometric based recognition. Research has made use of image processing during biometric implementation. Research has considered wide variety of systems that are requiring reliable personal recognition mechanism. Objectives of these types of mechanisms are to ensure that rendered services have been accessed by a legitimate user. Researchers have provided overview of areas of biometrics. Moreover the researchers have summarized its benefits, limitations, strengths. Privacy concerns are also considered in this research.

In 2016, Anil K Jain [22] explained the accomplishment, opportunities and challenges of biometric in last 50 years. Evolution of biometric explained with its applicability and issues in this research. First objective of research is to consider important progress which is achieved in area of biometric. The second objective of research has been to list issues related to biometric securities and providing solution to overcome those issues.

In 2016, Vineet Kumar [23] applied edge based mechanism to increase accuracy during pupil localization in case of iris images. Research has increased the accuracy during iris based biometric processing. Research has considered iris segmentation in case of iris recognition systems, a complex operation if environment is non cooperative. Researcher proposed a pupil localization mechanism in order to locate pupils in non-close-up and frontal-view iris images. These images are captured in near-infrared (NIR) illuminations. These images may contain noise. Initial researchers have proposed novel edge-map from iris based image. It is depending on integration of the conventional thresholding as well as edge detection dependent segmentation mechanism. Finally, general circular Hough transform has been utilized in order to check pupil circle parameters for edge-map. Research work is contributing to allow development of novel edge-map mechanism. This is minimizing

false edges in edge-map of the iris image drastically. Average accuracy of this model has been more than 99%. The average time cost for single image is approximately 0.727 second.

In 2016, Charan S G [24] performed feature optimization with support of iris based biometric recognition. Research has provided optimized solution during biometric processing. Research work is making use of two step feature optimization in order to enhance the rate of recognition. Initially author has improved sharpness of graphic content by making increment in peak value of pixel. Then it reduces crest pixel values depending on thresholds found using simulation. In second step author have enhanced feature vectors before performing selection of feature. It has been made by comparing ranks of value of pixel in case of feature vectors. Rank is calculated as per value of pixel. It enhances the selection of feature and also enhances the margin for classification. Research work has been applied over CASIA database. Maximum rate of recognition found was 100%. The average recognition rate was approximately 98%.

In 2004, R M Bolle [25] focused on different aspects of biometric science. This is the guiding for biometric that is presenting the scope and working of biometric technologies.

III. RESEARCH PROBLEM

Biometrics technique analyses and measures any physical or intrinsic behavior to identify uniquely human subjects. The human body features that are included in this are voice patterns, eye retinas, fingerprints, irises, hand measurements, and facial patterns. Biometric technologies are used by biometric systems. It allows the automatic verification or authentication and identification of a human being. On the other side demand for IoT applications is growing day today. However, there have been several pieces of research in the field of IoT and biometrics. The issue with previous researches that authors did limited works on biometric for IoT systems. Moreover, the biometric mechanisms used in existing research are time-consuming. There is the requirement of improving the accuracy and performance of biometric security mechanisms. There is a need to propose a biometric security mechanism that should be capable to work with an IoT environment with enhanced performance. Upcoming researches are supposed to improve the security as well as the performance of existing biometric security mechanism.

IV. NEED OF RESEARCH

To resolve the issues of existing researches the proposed work is supposed to integrate the biometric to digital wallet in IoT. The research would be considered edge detection to reduce the size of biometric content and reduce the comparison and validation time while implementing an iris-based biometric approach to overcome the limitation of previous researches. The objectives of the research are to study the existing research related to biometric security in IoT systems and investigating the scope of biometric security and the limitation of existing researches. Moreover, research is proposing a novel approach to reduce the time consumption during biometric security implementation in the IoT system. Finally, research would perform a comparative analysis of time, security, and storage consumption between tradition and proposed biometric security to provide a more reliable and secure approach.

V. RESEARCH PROPOSAL

The proposed research is providing biometric security to improve the protection of Digital Wallet in IoT System. As we all know that the use of digital wallets is increasing day by day, therefore there is a need to develop such kinds of efficient model to secure different digital wallets. There exist many techniques or mechanisms available which are supposed to enhance the security of digital wallets but these existing methods or techniques have their limitations. Therefore iris-based biometric mechanisms are introduced for the security of digital wallets. The integration of canny based edge detection is made to decrease the space consumption of the biometric model. In the future, this iris-based digital wallet security system would be used as a secure system than other biometric techniques.

In the proposed model, the multiple security layers for the iris and finger are considered for the verification of IoT-based digital wallets. The proposed work is providing multiple layers of security along with enhanced performance. The space consumption of the image set is reduced by performing edge detection.

The Canny edge detection model has been applied to eliminate the useless portion from the image. Moreover, the time consumption during verification gets reduced because there remains lesser image data for comparison because most of the image data is eliminated during edge detection. In model SL is presenting security layer

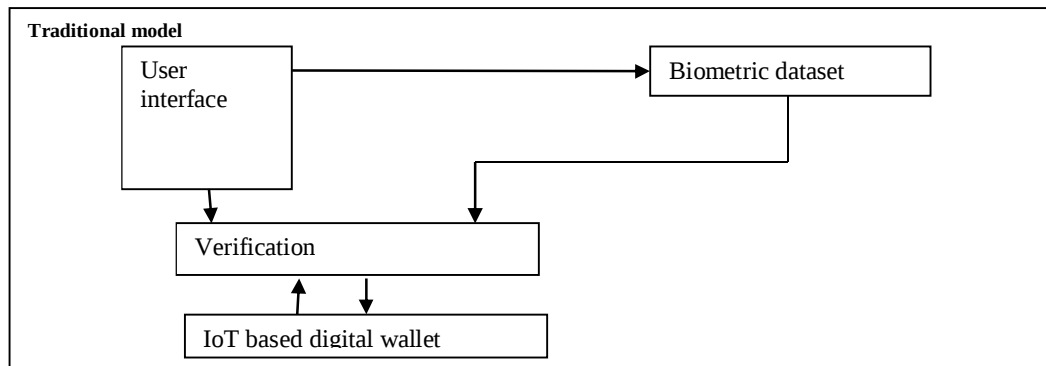


Figure 1. Working of Traditional Biometric model to provide security to IoT based digital wallet

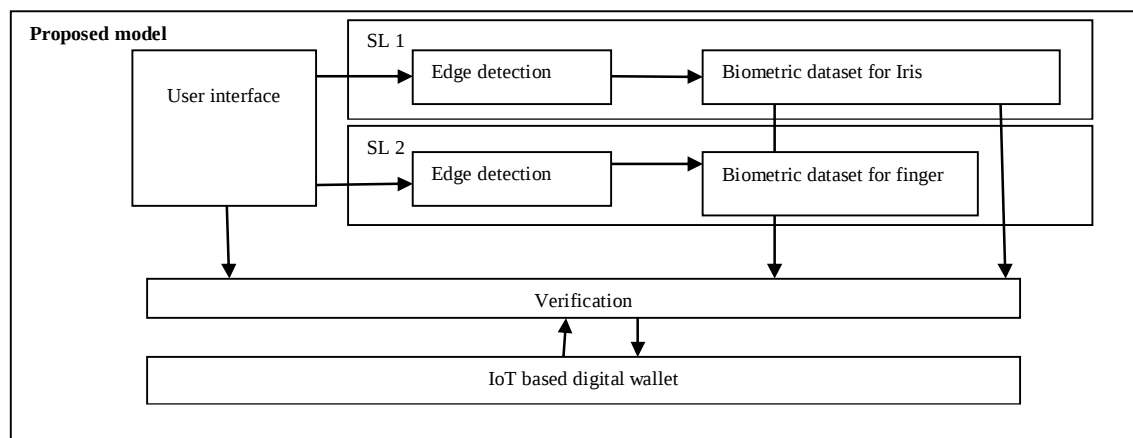


Figure 2. Working of Proposed model

The working of the proposed biometric recognition system is discussed here step by step.

1. **Image acquisition:** Digital coding is made from biometric samples. Thus more than one biometric image is captured during image acquisition.
2. **Pre-processing:** This step, involves edge detection from biometric samples. The contrast adjustment and multiplier are also considered here.
3. **Segmentation:** Localization of inner and outer boundaries is made. Additionally, the localization of the boundary is also performed.
4. **Normalization:** Conversion to Cartesian coordinates from polar is executed in this step. In addition, the normalization related to biometric image is made.
5. **Feature extraction:** Noise extraction to biometric sample is made. After that biometric sample code is generated.
6. **Classification and matching:** Comparing biometric code with the codes already saved in the database.

VI. CONCLUSION

The integration of edge detection mechanism to the biometric system would increase the accuracy. Moreover the space consumption of graphical contents also gets reduced. Proposed system would be able to compare the biometric content in less time in more accurate fashion. Such system is capable to increase the security of IoT based digital wallet. The system could play significant role in restricting unauthentic access by making use of multi layered biometric mechanism where multiple biometric technologies have been considered. Moreover the access to privileged person would be granted in less time.

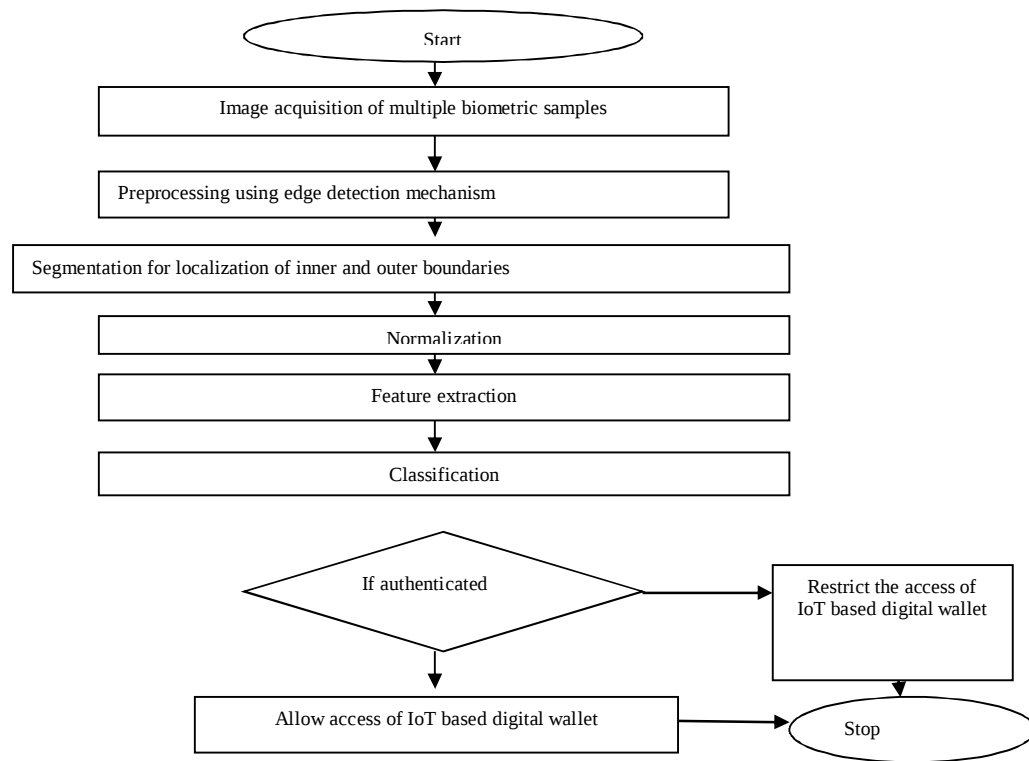


Figure 3. Flowchart to secure IoT based digital wallet using proposed biometric security mechanism

SCOPE OF RESEARCH

Such a security system could be applied to different digital payment methods. Such a system would secure digital wallets using iris as well as retina during the biometric comparison. The integration of canny based edge detection is required to reduce the space consumption of the biometric model. These mechanisms would operate at minimum time and space consumption. In the coming time, an iris-based module might be frequently used as a secure biometric system with an edge detection mechanism. It will be very helpful for secure transactions in banks and different financial associations.

REFERENCE

- [1] R. Álvarez Mariño, F. Hernández Álvarez, L. Hernández Encinas. (2012). A crypto-biometric scheme based on iris-templates with fuzzy extractor, *Information Sciences*, 195, p91-102.
- [2] GauravBhatnagar, Jonathan Wua, Balasubramanian Ramanb. (2012). Fractional dual-tree complex wavelet transforms and their application to biometric security during communication and transmission, *Future generation computer systems*, 28, 1, 2012, p254-267.
- [3] Anne M.P. Canuto, Fernando Pinto, João C. Xavier-Junior. (2013). Investigating fusion approaches in multi-biometric cancellable recognition, *Expert Systems with Applications*, 40, 6, p1971-1980.
- [4] C.Chen and R.Veldhuis. (2011). Extracting biometric binary strings with the minimal area under the FRR curve for the hamming distance classifier. *Signal processing*, 91, 4, p906-918.
- [5] Simona Crihalmeanu and Arun Ross. (2012). Multispectral scleral patterns for ocular biometric recognition. *Pattern Recognition Letters*, 33 (1), p1860-1869.
- [6] Maria De Marsico, Chiara Galdi, Michele Nappi, Daniel Riccioc. (2014). FIRME: Face and Iris Recognition for Mobile Engagement. *Image and Vision Computing*. P1161-1172.
- [7] Javier Galbally, Arun Ross, Marta Gomez-Barrero, Julian Fierrez, Javier Ortega-Garcia. (2013). Iris image reconstruction from binary templates: An efficient probabilistic approach based on genetic algorithms. *Computer Vision and Image Understanding*, 117 (1), p1512-1525.
- [8] Ujwalla Gawande, Mukesh Zaveri, Avichal Kapur. (2013). bimodal biometric system: feature-level fusion of iris and fingerprint. *Biometric Technology Today*, p7-8.

- [9] Marta Gomez-Barrero, Javier Galbally, Julian Fierrez. (2014). Efficient software attack to multimodal biometric systems and its application to face and iris fusion. *Pattern Recognition Letters*, 36 (1), p243-253.
- [10] Karen Hollingsworth, Kevin W. Bowyer, Stephen Lagree, Samuel P. Fenker, Patrick J. Flynn. (2011). genetically identical irises have texture similarity that is not detected by iris biometrics. *Vision and Image Understanding*, 115 (1), p1493-1502.
- [11] Farmanullah Jan, Imran Usman, Shahrukh Agha. (2012). Iris localization in frontal eye images for less constrained iris recognition systems. *Digital Signal Processing*, 22 (1), p971-986.
- [12] Farmanullah Jan, Imran Usman, Shahid A. Khana, Shahzad A. Malik. (2013). Iris localization is based on the Hough transform, a radial-gradient operator, and the gray-level intensity. *Optik - International Journal for Light and Electron Optics*, 124 (1), p5976-5985.
- [13] Farmanullah Jan, Imran Usman, Shahrukh Agha. (2013). A non-circular iris localization algorithm using image projection function and gray level statistics. *Optik - International* -241.
- [14] Farmanullah Jan, Imran Usman, Shahrukh Agha (2013). Reliable iris localization using Hough transform, histogram-bisection, and eccentricity. *Signal Processing*, 93 (1), p230
- [15] Farmanullah Jan, Imran Usman, Shahid A. Khan, Shahzad A. Malik. (2014). A dynamic noncircular iris localization technique for non-ideal data. *Computers & Electrical Engineering*, p215- 226.
- [16] Choudhury B, Then P, Issac B, Raman V and Haldar M K. (2018). A Survey on Biometrics and Cancelable Biometrics Systems. *International Journal of Image and Graphics*, pp. 1-28.
- [17] Shradha Tiwari, J N Chourasia and Vijay S Chourasia. (2015). A Review of Advancement in Biometric Systems. *International Journal of Innovative Research in Advanced Engineering*, vol. 2, no. 1, pp. 187-204.
- [18] Gursimarpreet Kaur and Chander Kant Varma. (2014). Comparative Analysis of Biometric Modalities. *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 4, no. 4, pp. 603-613, 2014.
- [19] Himanshu Srivastva. (2013). A Comparison Based Study on Biometrics for Human Recognition. *International Journal of Computer Engineering*, vol.15, pp. 22-29.
- [20] A K Jain, A Ross and S Pankanti. Biometrics. (2006). A Tool for Information Security. *IEEE Transactions on Information Forensics And Security*, vol. 1, no. 2, pp. 125-144.
- [21] Jain K Anil, Ross Arun and Prabhakar Salil. (2004). An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 4-20.
- [22] Anil K Jain, Karthik Nandakumar and Arun Ross. (2016). 50 years of biometric research, Accomplishments, Challenges and Opportunities. *Pattern Recognition Letters*, vol. 79, pp. 80-105.
- [23] Vineet Kumar, Abhijit Asati and Anu Gupta. (2016). A Novel Edge-Map Creation Approach for Highly Accurate Pupil Localization in Unconstrained Infrared Iris Images. *Hindawi International Journal of Electrical and Computer Engineering*, pp. 1-10.
- [24] Charan S G. (2016). Iris Recognition using Feature Optimization. *IEEE International Conference on Applied and Theoretical Computing and Communication Technology*, pp. 726-731.
- [25] R M Bolle, J H Connel, S Pankanti, N K Ratha, A W senior. (2004). *Guide to Biometrics*. Springer.