Raniah Ali Mustafa *et al*, International Journal of Computer Science and Mobile Applications,
Vol.10 Issue. 8, August- 2022, pg. 1-9 **ISSN: 2321-8363**
Impact Factor: 6.308
(An Open Accessible, Fully Refereed and Peer Reviewed Journal)

Subject Review: Securing Iris Authentication System

Raniah Ali Mustafa[1]; Haitham Salman Chyad[2]
[1,2]Computer Science Department, College of Education, Mustansiriyah University, Baghdad, Iraq
rania83computer@uomustansiriyah.edu.iq
dr.haitham@uomustansiriyah.edu.iq

DOI: 10.5281/zenodo.6971062

Abstract
Two components are available from a biometric system: authentication and verification. Both of these features must be utilized at the same time by the biometric authentication methods, which must be rigorous enough to support them. The use of biometrics as a key is intended to boost more effective security manner, reducing identification errors caused by human, improve user convenience, and automate security functions. Recognition of iris patterns is one of the most precise biometric authentication techniques. In essence, A biometric identification and authentication method is iris recognition that makes use of recognition algorithms on images of a person's eyes. In this study, we offer a thorough background analysis of a number of strategies, approaches, and techniques employed in the iris print authentication system using many different strategies and techniques. The dataset, pre-processing, feature extraction, authentication, and result technologies used in these security application technologies are also contrasted.
Keywords: Iris authentication, Biometric Recognition, Security, Hamming Distant (HD), False Acceptance Rate (FAR) and False Rejection Rate (FRR).

1. Introduction
Any access control system that demands a high level of security is ideally suited to the application of the personal authentication using biometrics approach depending on the human iris's pattern. Today, based on physiological traits, biometric recognition is a popular and trustworthy method of verifying a live person's identity. An identifiable physical trait, like as a fingerprint, iris pattern, face characteristic, hand profile, etc., is referred to as a physiological characteristic. Basically, this type of measurement cannot be changed or altered.

The automated systems for verifying a person's identity that use iris recognition are thought to be the most accurate because it is extremely unlikely to find two people with the same iris pattern. Because of this, iris recognition technology is increasingly being the use of biometrics for user identification in networked computer applications for access control. In contrast to a fingerprint, an iris is shielded from the environment by the cornea and the eyelid, is not affected by the negative effects of aging, and retains its small-scale radial features throughout life. Iris is a biometric characteristic that distinguishes persons from one another. Iris development started at three months of fetal life. But about a year from birth, Iris' distinctive pattern began to emerge. Iris's singular image has distinctive qualities that can be employed in authentication systems.

Accessing resources and services requires authentication as a necessary first step. The method of iris pattern recognition is one popular biometric-based on method of authentication. In an iris-relying on authentication system, users' iris images are taken, and features are retrieved for later matching in the authentication process. Each individual's iris is distinct. It can be used for authentication because it has distinctive textures and patterns. The drawbacks of conventional password-rely authentication systems, which are susceptible to brute force and dictionary-relying on assaults, can be avoided by iris-based authentication. Commercial iris-based tools like iridis and eyelock are readily accessible. According to the literature, iris-based authentication is increasingly being used in fields including online banking, immigration and border control.

2. Literature Survey

Several methodologies and procedures associated with the iris print authentication system have been proposed in recent years. Some of these methods will be covered in this section.

Albadarneh and et al. (Albadarneh et al., 2015) in this paper, a user authentication system utilizing iris recognition is presented. We studied and assessed recognizing iris patterns using four traits, included the Histogram of Oriented Gradients (HOG), coupled Gabor and Discrete Cosine Transform (DCT), and Grey level Co-occurrence Matrix, to build the proposed iris authentication method (GLCM). The UBIRIS.v1 IRIS dataset was used to evaluate the system, and the findings revealed that GLCM, rather than employing integrated features, provides the highest Euclidean distance among two images of iris for two separate users. Additionally, the Logistic Model Trees (LMT) classifier used by GLCM provides the maximum recognition accuracy. In light of this, GLCM is thought to be the most distinguished and efficient method for the suggested system for authenticating with iris.

Alqahtani, A. (Alqahtani, 2016) in this study, the image quality in various irises is investigated in relation to iris recognition. The primary goal of this study is to offer trustworthy evidence supporting the iris' superiority over other biometrics, particularly when there is noise present in the images the iris captures. The primary data source for the investigation was the iris database CASIA-IrisV3-interval. The system's application to the images in the iris database was also tested. In order to demonstrate that images of the iris provide a legitimate and extremely trustworthy form of individual identification, the CASIA-IrisV3-interval database now contains noise throughout the investigation. Using the Hamming Distant (HD) approach, the databases' images were compared before and after noise were added. The TPR and FPR values that were discovered as a result of this comparison were then utilized to construct ROC curves. The quality of the image as portrayed by the CASIA images was then assessed using the generated ROC curves.

Patil, C. M., and S. Gowda (Patil and Gowda, 2017) in this article, a secure authentication method based on iris recognition is presented. The enrollment phase and the authentication phase are two independent steps of a typical recognition system. The CASIA V4 iris database is regarded as a database in this suggested effort. preprocessing, feature extraction (FE), and classification are the set steps in the work. Utilizing techniques from the Histogram of Oriented Gradients (HOG), Gray Level Co-occurrence Matrix (GLCM), Hausdroff Dimensions (HD), Biometric Graph Matching (BGM), and 2D-Gabor filter, this procedure evaluates numerous iris pattern identification features. The patterns are then verified and authenticated using a State Vector Machine (SVM), Weighted Euclidian Distance (WED), Jaccard coefficient, and Dice coefficient classifier. As it relates to the iris authentication and identification system, that has been proposed, SVM is therefore considered the most distinctive and effective technique.

Daniel, D. M., &B. Monica (Daniel and Monica, 2010) this paper offers the Euclidean classifier, the MLP classifier, and the Hybrid classifier as three iris classification methods. When used in a system that permits the identification of the iris in conjunction using password authentication, we constructed classifiers and compared the effectiveness of each one. Utilizing Microsoft Visual Studio 2005, the application was created using a number of phases, including the use of a gratis iris database; the collection, processing, and encoding of human iris; managing codes; the construction of classifiers; and a comparison study of the efficacy a classifier of these.

de Santos Sierra and et al. (de Santos Sierra et al., 2008) this novel method compares the Iris templates directly in order to recognize and/or authenticate a user without using transformations. This new system, which builds on concepts from fuzzy logic and DNA alignment techniques, performs better than earlier algorithms in determining whether two templates belong to the same user. Additionally, this novel technique reduces access time by allowing comparison of several aspects of the entire saved template in a database and a piece of the template. Consequently, not only are the False Acceptance Ratio (FAR), False Rejection Ratio

(FRR).significantly lower than those of current algorithms, but also the time required for identifying and authenticating users is greatly reduced. In addition, the algorithm's local flexibility comparisons making it an algorithm with promise for use in any biometric system, not just iris detection systems.

Hongo, K., and H. Takano (Hongo and Takano, 2018) in this paper, we create a visible light iris authentication mechanism utilizing a standard RGB camera. Several preprocessing techniques were used in this study to images taken in a setting with comparatively corneal reflection is minimal. We provide the findings of a comparison between the precision of the locally varying brightness features and the precision of the characteristic of gradient direction of the iris pattern. According to the experimental findings, the gradient direction feature's EER (Equal Error Rate), a measure of performance assessment in biometric identification, was 5.03 percent. We also verified that as the capturing condition changes, iris authentication performance suffers.

Jagadeesh, N., and C. M. Patil (Jagadeesh and Patil, 2017) in this paper, sincere attempts are being made to develop some innovative methods of identifying a person in the form of creating a special biometric identification technique that has some great advantages compared to the existing approaches in the current scenario. The development of quick algorithms for processing takes the rate of computing into consideration (3–4 secs). The enormous database is taken into account first, then preprocessing, segmentation, normalization, feature extraction, and a scenario of matching with outcomes that are finally matched. The input eye image's features are compared to those previously saved in the database, and if they match, the associated eye image is recognized; otherwise, it stays unidentified. In light of a bitwise comparison is required for our investigation, the hamming distance (HD) is selected for identification. The speed of computation and ease of use of the biometric recognition system created so that it is user-friendly and any layperson can run it are two advantages of the methodology produced in the research work under consideration. In this work, we outline the methodology specifically, the algorithm that we used to create the algorithm for iris recognition in a vast collection of databases that were acquired.

Kadri, F. and et al. (Kadri et al., 2016) in this research, palmprint and iris are combined to create an effective system for multiple biometric recognition relying on matching score level fusion and employing the sum of scores technique. This system makes an effort to enhance the recognition performance of individual biometric systems. Using the Log Gabor filter, the traits of the palmprint and iris are recovered. When matching an iris or palmprint feature vector, the hamming distance is used. Using the same data, we tested the suggested method and contrasted its performance with that of the single biometric. The results of the experiments demonstrated that the proposed achieving system a superior recognition rate and offers greater security than an individual biometric system.

Nithyanandam and et al. (Nithyanandam et al., 2011) in this study, we describe a number of methods for creating using an iris template; make a distinctive, more secure cryptographic key. Images of the iris are processed to create an iris code or template that is used for encryption and decryption operations. The data is immediately encrypted and decrypted using a variety of cryptographic approaches, including AES, DES, add/subtract operations, Implementations of layered order encryption, the Reed-Solomon error-correcting algorithm, and fuzzy logic. With the use of biometric data, biometric cryptosystems have recently been developed as a trustworthy method of hiding private keys. A biometric cryptosystem known as a "fuzzy vault" can be utilized to securely store private keys and only allow authorized users to access them by entering their biometric information. The template matching identification procedure uses a distance metric like hamming distance. The practicality of the various systems is demonstrated by experimental results, which also reveal that the R-S cryptographic algorithm can provide stronger security with a lower false acceptance or rejection rate than another method.

Pattar, S. (Pattar, 2019) in this study, we suggested a novel model as an enhancement to the Chan-Vese method by using the B spline approach to segment the iris. The suggested approach now includes improved segmentation for less-than-ideal visible light iris images. For feature extraction, the GLCM (Gray Level Co-occurrence Matrix) and LBP (Local Binary Pattern) are used. As the B-spline work is divisible and is created as the consequence of n-1), 1-D, B-splines, this approach is able to execute each associated treating in 1-dimension. Compared to other approaches, this offers better control. According on experimental findings, the suggested technique for segmenting the iris significantly reduces the time needed to segment the iris without compromising segmentation accuracy. These are the key advantages of this algorithm: It can first handle the precise recognition of smooth objects. The second is that it can effectively manage noisy images. As a result, the real borders are appropriately recognized and retained. The comparative results with comparable iris segmentation techniques further demonstrate the advantages of the suggested approach in terms of precision and recognition of segmentation ability. To determine how well the suggested technique performs, a NICE. I It uses the iris image database.

Shelke, R., & S. Bagal (Shelke and Bagal, 2017) in this paper, the pupil and iris were used in this proposed system's segmentation technique to determine their shape, intensity, and localisation. The normalization technique turns the segmented region into a rectangular region. The texture-based characteristics are extracted using the Hausdorff Dimension (HD) and Gray Level Cooccurrence Matrix (GLCM). Through the use of supervised SVM machine learning, the retrieved characteristics were categorized. The effectiveness of the suggested system demonstrates its robustness.

Vishwakarma, N., and V. Patel (Vishwakarma and Patel, 2019) in this work, the initial systems created frequently used subpar edge identification techniques and filters. The field frequently uses a variety of recognition techniques, such as Canny Edge Detection, Huff Transform, Gabor Filters, and Dagman's Operator Iris. There are several limitations in the form of sophisticated computational strategies, a lack of accuracy for images, including sophisticated noise, an obstruction brought on by the lens, the eyelashes, and reflections seen during preliminary work. The structure suggests an iris identification system or a validation system that extracts iris features using the sobel age detection method. The strategy also shows how well the figurative depiction manages noise and decreases while taking into account low resolutions, specular reflections, and characteristics that cause obstructions to the sight. The exact feature extraction used in the suggested approach results in enhanced safety outcomes.

Zhang and et al. (Zhang et al., 2011) the objective of this study is to describe a two-phase approximation localization technique for authentication systems, which is an improved iris localization technique. We start by assessing the image quality and eschewing blurry images. Additionally, we calculate the iris boundary's center and radius. The algorithm then performs a second calculation of the center and radius using the voting method. The localization process takes an average of 2.0 seconds and is 99.70% accurate. Compared to Daugman's and Wilds' traditional methods, the method is substantially faster.

Choudhary and et al. (Choudhary et al., 2021) in this research, a method to distinguish between authentic and fake iris is presented. It involves pooling multi-scale BSIF and fine-tuned DenseNet features that are collected from unprocessed and normalized iris. Additionally, the research verifies the generalizability of the suggested strategy using a variety of attack types, iris sensors, and datasets. Aside from that, the trials carried out on the freely accessible LivDet 2017 datasets attest to the effectiveness of the suggested approach.

Gusain , R and et al. (Gusain et al., 2018) in this research provides methods for modifying the vascular pattern thinning algorithm to enhance the capabilities of iris scanner and palm vein detection systems. A system known as palm vein recognition (PVR) identifies a person's iris scanner and palm vein pattern for compares it to

information recorded in a database for authentication. This method is regarded as the most secure and effective for security reasons because it is very dependable, accurate, and reliable.

3. Comparison of Systems

Table 1 compares previous research investigations based on the dataset analysis, pre-processing, feature extraction, authentication, and security application approaches employed during the study and the findings.

Table 1: Comparative analysis of previous research studies

Reference	Dataset	Pre-processing and segmentation	Feature Extraction (FE)	Authentication/ security approaches	Accuracy achieved
Albadarneh et al., 2015	UBIRIS.v1 IRIS	first use the upper and lower eyelids can be fitted with a line using the linear Hough transform. another algorithms that use boundary localization include the Hough transform, clever edge detection, linear thresholding, and chain code for the detection of iris two circles, Localization is also applicable to iris-derived regions, like the collarette area, Another pre-processing step that can come after is image normalization.	Grey level Co-occurrence Matrix, coupled Gabor & Discrete Cosine Transform (DCT), and Histogram of Oriented Gradients (HOG)	Euclidean distance (ED)	LMT classifier-based GLCM provides the highest recognition accuracy.
Alqahtani, 2016	CASIA-IrisV3-interval	Segnent iris, Normalize iris	Encode Features	Hamming Distant (HD)	According to the TPR values, the study discovered that blurred images were formed at greater noise levels. However, the iris is still able to produce easily recognized iris images even when there is noise.
Patil and Gowda, 2017	CASIA V4 iris	Images are subjected to the histogram equalization procedure, which boosts the contrast of the original image.	Gray level co-occurrence matrix, Hausdroff dimensions, biometric graph matching, and 2D-Gabor filter, along with Histogram of Oriented Gradients (HOG),	A classifier composed of a State Vector Machine (SVM), Weighted Euclidian Distance (WED), the Jaccard coefficient, and the Dice coefficient	90 percent precision and 7% error rate.

Daniel and Monica, 2010	Iris Image Database for CASIA (version 1.0)	iris detection; cutting a new image to represent the iris; and deleting a 100-pixel field from the new image	provide a method to extract iris features that are unaffected by external influences (such as pupil size or position on the iris picture), person proximity to the scanning device, distance from the device, and the orientation of the eyes at the time of scanning;	Provides the MLP classifier, the Hybrid classifier, and the Euclidean classifier.	efficacy accuracy
de Santos Sierra et al., 2008	UPOL database	To ensure that only iris tissue is collected in following phases, a segmentation procedure is used to isolate the iris from a given eye image while ignoring both eyelashes and eyelids. Additionally, the pupil's center and radius are extracted.	fuzzy logic and DNA alignment techniques	Identification and authentication rates are 100% and 99.5%, respectively.	EER is equal to 0.3% while CMR is 99.7%.
Hongo and Takano, 2018	540 iris images are used to test authentication accuracy.	I polar coordinate conversion, background illuminance elimination, gray-scale conversion, histogram equalization, and image normalization are some of the processing steps.	A method using local luminance variation, Calculation of city block distance, Gradient directional feature	Euclidean distance	EER is 5.03 percent
Jagadeesh and Patil, 2017	UPOL database	After completing the necessary pre-processing, segmentation is used to create the primary edges of the eye, from which the iris border may be precisely localized.	The iris is then represented in less dimensions by first undergoing feature extraction on the segmented pictures. The Curvelets transform has been recommended at this step.	Support vector machines, or SVM, have been employed for classification purposes.	computation speed and biometric recognition system usability
Kadri et al., 2016	Hong Kong Polytechnic University's (PolyU) palmprint database and the CASIA Iris database	Segmentation (The Hough Transform in a circle is used to look for the boundaries. Eyelashes are isolated using a straightforward threshold technique, and eyelids are recognized by fitting two lines with the linear Hough Transform), Normalization (The segmented iris region must be	The image is smoothed using a Gaussian smoothing filter before the Region Of Interest (ROI) and using the Log Gabor filter, its characteristics are extracted	score level fusion and employing the sum of scores technique, hamming distance (HD)	The combined findings of the iris and palmprint are 100 percent, which is significantly higher than the corresponding individual results of 96.23 percent and 98.89 percent. The

		aligned to a specific size in order to compare irises)			experiment's findings show that the maximum accuracy was attained with the fusion at the score level.
Nithyanandam et al., 2011	IRIS databases were provided by CASIA, UBIRIS, and IIT New Delhi	The data is directly encrypted and decrypted using various techniques when the vector characteristic from the iris is extracted, including AES, DES, add/subtract operations, the Reed-Solomon error-correcting algorithm, layered order encryption, and fuzzy logic implementations	Based on regional iris traits, a trustworthy fuzzy vault system	The Hamming distance can be used to calculate how many bits are identical between two bit patterns.	The highest rate of accurate accept (60 percent) and reject (100 percent) is achieved by the XORECC approach utilizing Hadamard and Reed Solomon error correcting codes
Pattar, 2019	Database of iris images, NICE.I	The segmentation technique served as the primary function in iris authentication, Chan-Vese method by using the B spline approach to segment the iris, Lankton and Tannenbaum developed the localized segmentation technique.	The GLCM (Gray Level Co-Occurrence Matrix) and LBP (Local Binary Pattern)	To classify a person as authorized or unauthorized, SVM is used.	In comparison to the Chan-Vese approach, experimental results demonstrate that our proposed scheme offers 83.33 percent accuracy, 90 percent precision, and 90 percent sensitivity, as well as a more reliable performance in iris segmentation.
Shelke and Bagal, 2017	CASIA	To localize the inner and outer part is necessary since iris segmentation from the eye image is a crucial task. It is found via canny edge detection. Because eyelids are repressed in the vertical direction, only the vertical direction is taken into account in clever edge identification. Since the pupils and iris are shaped like circles, circular Hough transforms are applied. Higher calculation time is a benefit of the Hough transform, The normalizing method is based on the rubbersheet model of Daugman.	using the Hausdorff Dimension (HD) and Gray Level Cooccurrence Matrix (GLCM)	use of supervised SVM machine learning	93.75 percent precision

Vishwakarma and Patel, 2019		segmentation, normalization, ROI (region of interest)	sobel age detection method, Algorithm for Gradient Magnitude Sobel	For the recognition method, Canny Edge Detection and Gaussian Filter are used.	1.66 percent error rate and 98.34 percent accuracy
Zhang et al., 2011	Use 320px*240px images that were taken with our own camera for our proposed.	Prior to precise localization, the approach calculates the center and radius of the iris boundaries and casts votes on local scope points, based on the iris localization techniques of Daugman and Wilds		Daugman's and Wilds' traditional methods, the method is substantially faster.	997.10 percent
Choudhary et al., 2021	LivDet 2017 datasets	Iris localization, Iris normalization, Iris cropping	pooling various scales enhanced DenseNet features and BSIF	classifier SVM	Notre-Dame (Cross-Attacks)= 0.00 , 0.35 IIITD-WVU (Cross-Datasets)= 1.13, 6.53 Clarkson (Cross-Attacks)= 1.92 , 3.29
Gusain et al., 2018	taking an image of the iris using high-resolution cameras and sensors	Iris Segmentation, Iris normalization makes use of the Gabor filter.	The Local Binary Pattern is used to perform feature encoding.	The hamming distance Daugman used	achieved the highest level of security and effectiveness

4. Conclusion

In this review study, we concentrated on the key works that discussed the various techniques utilized in security applications based on iris authentication systems from 2008 to 2021. The iris is one of the most user-friendly biometrics because it effectively provides security and authentication while also allowing users to identify someone without having to make eye contact. A secure iris authentication mechanism was used in this investigation. This study focuses on leveraging better datasets, and the systems go through several stages, including preprocessing and segmentation, feature extraction, and authentication and security application approaches. After applying preprocessing and segmentation, the best features for iris images are extracted in order to improve authentication efficiency. In order to ensure performance, a more advanced algorithm for compressing the large database of iris prints and the database of the feature vectors (FV) has to be coded in order to provide a simpler database structure to reduce the complexity of the authentication process. The newly proposed iris authentication system has increased security, and unique authentication is now being developed on a daily basis. Because every technology has benefits and drawbacks, novel technologies are developing at an accelerating rate.

References

[1] Tisse, C.-l., L. Martin, L. Torres, & M. Robert (2002), Person identification technique using human iris recognition, paper presented at Proc. Vision Interface.

[2] Daugman, J. (2009), How iris recognition works, in The essential guide to image processing, edited, pp. 715-739, Elsevier.

[3] Gifford, M., D. McCartney, and C. Seal (1999), Networked biometrics systems—requirements based on iris recognition, BT technology journal, 17(2), 163-169.

[4] Shahriar, H., H. Haddad, & M. Islam (2017), An iris-based authentication framework to prevent presentation attacks, paper presented at 2017 IEEE 41st annual computer software and applications conference (COMPSAC), IEEE.
[5] López, F. R. J., C. E. P. Beainy, & O. E. U. Mendez (2013), Biometric iris recognition using Hough Transform, paper presented at Symposium of Signals, Images and Artificial Vision-2013: STSIVA-2013, IEEE.
[6] Albadarneh, A., I. Albadarneh, & J. f. Alqatawna (2015), Iris recognition system for secure authentication based on texture and shape features, paper presented at 2015 IEEE Jordan Conference on Applied Electrical Engineering and Computing Technologies (AEECT), IEEE.
[7] Alqahtani, A. (2016), Evaluation of the reliability of iris recognition biometric authentication systems, paper presented at 2016 International Conference on Computational Science and Computational Intelligence (CSCI), IEEE.
[8] Patil, C. M., & S. Gowda (2017), An approach for secure identification and authentication for biometrics using iris, paper presented at 2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC), IEEE.
[9] Daniel, D. M., &B. Monica (2010), Person authentication technique using human iris recognition, paper presented at 2010 9th International Symposium on Electronics and Telecommunications, IEEE.
[10] de Santos Sierra, A., C. S. Ávila, & V. J. Vera (2008), A fuzzy dna-based algorithm for identification and authentication in an iris detection system, paper presented at 2008 42nd Annual IEEE International Carnahan Conference on Security Technology, IEEE.
[11] Hongo, K., & H. Takano (2018), Personal authentication with an iris image captured under visible-light condition, paper presented at 2018 IEEE International Conference on Systems, Man, and Cybernetics (SMC), IEEE.
[12] Jagadeesh, N., & C. M. Patil (2017), Development of a new methodology for iris algorithm in biometric authentication using hamming distance concepts, paper presented at 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS), IEEE.
[13] Kadri, F., A. Meraoumia, H. Bendjenna, & S. Chitroub (2016), Palmprint & iris for a multibiometric authentication scheme using Log-Gabor filter response, paper presented at 2016 international conference on information technology for organizations development (IT4OD), IEEE.
[14] Nithyanandam, S., K. Gayathri, K. Raja, & P. Priyadarsini (2011), Recent trends in secure personal authentication for iris recognition using novel cryptographic algorithmic techniques, paper presented at 2011 International Conference on Process Automation, Control and Computing, IEEE.
[15] Pattar, S. (2019), A novel approach towards iris segmentation and authentication using local Chan-Vese method, paper presented at 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), IEEE.
[16] Shelke, R., & S. Bagal (2017), Iris recognition system: a novel approach for biometric authentication, paper presented at 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA), IEEE.
[17] Vishwakarma, N., & V. Patel (2019), Biometric Iris Recognition using Sobel Edge Detection for Secured Authentication, paper presented at 2019 2nd International Conference on Intelligent Communication and Computational Techniques (ICCT), IEEE.
[18] Zhang, Z., M. Li, F. Xia, & J. Ma (2011), An improved iris localization method for authentication system, paper presented at 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing, IEEE.
[19] Choudhary, M., V. Tiwari, & U. Venkanna (2021), Ensuring Secured Iris Authentication for Mobile Devices, paper presented at 2021 IEEE International Conference on Consumer Electronics (ICCE), IEEE.
[20] Gusain, R., H. Jain, & S. Pratap (2018), Enhancing bank security system using face recognition, Iris scanner and palm vein technology, paper presented at 2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU), IEEE.