*Asian Journal of Research in Computer Science*

***10(1): 18-33, 2021; Article no.AJRCOS.70240***
***ISSN: 2581-8260***

# A State of Art for Survey of Combined Iris and Fingerprint Recognition Systems

**Dindar Mikaeel Ahmed[1*], Siddeeq Y. Ameen[1], Naaman Omar[1], Shakir Fattah Kak[1], Zryan Najat Rashid[2], Hajar Maseeh Yasin[1], Ibrahim Mahmood Ibrahim[1], Azar Abid Salih[1], Nareen O. M. Salim[1] and Awder Mohammed Ahmed[2]**

*[1]Duhok Polytechnic University, Duhok, Kurdistan Region, Iraq.*
*[2]Sulaimani Polytechnic University, Sulaimani, Kurdistan Region, Iraq.*

***Authors' contributions***

*This work was carried out in collaboration among all authors. All authors read and approved the final manuscript.*

***Article Information***

DOI: 10.9734/AJRCOS/2021/v10i130232
Editor(s):
(1) Dr.Shivanand S.Gornale , Rani Channamma University, India.
Reviewers:
(1) Rajesh Bose, Brainware University,India.
(2) Saad Albawi, University of Diyala, Iraq.
Complete Peer review History: http://www.sdiarticle4.com/review-history/70240

***Review Article***

***Received 12 April 2021***
***Accepted 21 June 2021***
***Published 21 June 2021***

## ABSTRACT

Biometrics is developing into a technological science in this lifelong technology for the defense of identification. Biometrics is the technology to recognize individuals based on facial features, fingerprints, iris, retina, speech, handprints, etc. Biometric features are used for human recognition and identification. Much research was done in the last years on the biometric system because of a growing need for identification methods. This paper offers an overview of biometric solutions using fingerprint and iris identification, their uses, and Compare the data set, methods, Fusion Level, and the accuracy of the results.

*Keywords: Hyper biometrics; fusion level; iris recognition; fingerprint recognition; identification techniques.*

**Corresponding author: E-mail: dindar.ahmed@dpu.edu.krd;*

## 1. INTRODUCTION

With the development of the global economy and information technology, especially the advent of the worldwide Internet era, more and more fields require reliable identity authentication [1-3]. In the context of information, personal identity is gradually digitized and hidden [4-6]. How to accurately identify A person's identity and ensuring information security is an important challenge in the information age. Biometrics are recognized and studied in depth due to their stability and convenience [7,8]. Biometrics recognition technology and its system applications have been used in different areas and played an important role [9]. In identity authentication, biometric identification technology has advantaged that traditional cryptography does not have, such as easy to use, non-repudiation, and difficult to forge, so it gradually plays an important role in people's daily life Role [10-12].

However, humans naturally use "multi-biological feature recognition" to recognize individuals, such as through appearance (face recognition), speech appearance (voice recognition), walking posture (gait recognition), and finally, determine if it is the same person. a final decision is made based on the matching scores of these different recognitions, which is the fusion of multi-biological feature recognition based on the matching scores [13,14]. It is the secret of the too-high accuracy of the biometric recognition capabilities possessed by humans. Therefore, it can say that humans' identity recognition ability naturally has the characteristics of multi-biological identification based on matching scores [15,16]. Accordingly, after introducing the relevant knowledge of multi-biological feature recognition. Biometric identification refers to the process of confirming a person's identity through physiological or behavioral characteristics [17,18]. Human beings' biometric recognition function can also be divided into two stages: "registration" and "recognition " [19-21]. In the "registration" stage, many biometrics are stored by memory, while in the "recognition" stage, it needs to be recognized through recall and comparison Out of the individual. This recognition ability of humans requires a lot of storage and repeated training, which is costly [22,23]. At the same time, this recognition is not an exact match, The information contained in a single biological feature is limited, and it is also affected by the noise of data collection, which cannot meet the needs of some systems for high accuracy so there is a possibility of false acceptance and false rejection [24,25].

The iris and the fingerprint are used in many verification systems since these two features are easy to use for the user. The fingerprint is one of the traditional methods of identifying people, and it has been used widely, but it is not accurate enough. For example, it may be inconspicuous in the elderly on the other hand, the iris of the eye is one of the subtle and unchanging features with time [26-28]. Still, it suffers from some problems in the way the image is taken, as it can affect the distance, lighting, and direction of the person that can affect the quality of the captured image [29-31] , and this has led to the emergence of many studies and systems that Combines more than one biometric feature.

In contrast to a false synthetic or rebuilt sample, ensuring the actual presence of a genuinely valid characteristic is a major challenge in biometrics, and new and effective protective measures are required [32].

Biometric systems rely on the collection and authentication of human body characteristics [33]. Unimodal or multimodal biometric systems can be built depending on single or several biometric characteristics utilized for authentication. Human iris and fingerprints have a distinctive pattern of texture and may be used to identify the individual [34].

The biometrics area is currently getting enormous popularity. Gender is a major demographic characteristic for people to be classified [35]. There are many biometric characteristics used to classify the sex. But there is always less precision in a single feature [36].

The widespread, direct or spoofing fraudulent assaults by thieves have led us to put our primary attention on money security [37]. The precise use of biometrics is used significantly in identification [38].

The improvement in the degree of security owing to the application of biometric recognition systems compared to traditional identifying methods helps these systems to progress quickly [39]. It is deemed dependable and precise that Fingerprin or Iris recognition technologies are used. There are various inconveniences and faults in both systems [40]. A hybrid identification system using both fingerprint recognition and iris

recognition methods is proposed to minimise mistakes and to enhance accuracy [41].

Today the bulk of the biometric systems are verified or identified using information from one biometric technology [40]. Additional challenges such as increased population coverage and demographic diversity, a diverse use environment and more demanding performance criteria have to be fulfilled in large-scale biometric systems [42]. These objectives are difficult to satisfy today with the single-modality biometric systems, and a solution involves integrating other information sources to enhance decision-making [43]. To decide on the identification, the multibiometric system integrates information from several biometric characteristics, algorithms, sensors and other components [44]. In addition to enhancing the accuracy, the merging of biometrics offers several benefits such as increased population coverage, disincentive of spoofing and reduced registration failure [45]. In the past five years, the research and marketing efforts in this field have experienced an exponential increase and this trend will probably continue [46].

Often biometrically based on single-modal biometrics alone, owing to difficulties such as noisy data, intra-class variations, restricted liberties, non-universe, spooof attack and inacceptable error rates, it does not fulfill the necessary performance requirements for large user populations [47]. Multimodal biometry refers to the usage of a single identification system of a combination of two or more biometrical modalities [48]. Improving accuracy in recognizing the most compelling argument for combining multiple methods. This may be achieved when statistically independent characteristics of several biometrics [49].

Biometric recognition is commonly used for adults to identify an individual for a number of purposes. However, youngsters are unresolved in their biometric recognition [50]. To resolve that problem can protect children from identity theft and identity fraud, help bring children lost with their parents together, enhance border surveillance systems in the fight against trafficking in minors and support electronic registration systems [51]. Researchers gathered biometric information from youngsters in order to begin the creation of biometric recognition systems for children, including fingerprints, irises and the outside ears [52]. Each mode has various obstacles [53].

Conventional biometric multimodal identification systems tend to have a greater memory base, slower processing rates and increased deployment and operating costs [54].

Currently numerous applications in the field of cyber technology are being implemented that facilitate our lives. Because it's an open space, we need security technologies [55]. Authentication is a tool to check an entity's legitimacy against unauthorized access in cyberspace to a device or application. Recent smartphones already feature biometrics that can be authenticated via fingerprint and facial recognition. The most reliable biometric features is the identification of iris. It takes a significant computational power, though [56].

For the measuring of biological data, Biometric is employed. Measurement and registration of an individual's physical attributes for later use. A system that employs two or more biometric traits is the multimodal biometric authentication. More protection from spoofing is provided [57].

In today's life, the security system is the major problem. As the safety system develops, the recognition of iris and biometrics are becoming essential techniques of biometric identity systems [58]. These technologies have significantly enhanced the quality of personal authentication that has a key role to play in global, national and personal safety. Currently, iris recognition in terms of security is becoming common [59]. Iris pattern with ages, singularity, acceptance is more stable. Thus, iris recognition is utilized for extremely secure areas because to its high dependability and strong recognition rate. As ATM banking arrives, it is more easier and more accessible, too [60]. The product (ATM) is diverse because of the risks of smart thieves. Because of the risk and not security of financial services. This is progressing as biometric detection technology, such as fingerprint and iris scanning, are progressing enormously. Using selected item points, customers' password may be encrypted [61].

Currently, there has been increasing study on biometric recognition throughout the world [62]. Iris recognition is a form of biometric technology based on human body physiological features, compared to fingerprint, palm-sprint, face and sound, etc. feature recognition. Identity identification technology has lately become popular [63].

Human identification is a highly important area of safety in the last several years. The best way to do this is biometric recognition [64]. The two types of biometric systems are uni-biometric and multi-biometric. In the previous years, humanoid identification and safety systems are employed in uni-biotic systems. Instead of a mono biometric system, trends to multibiometric systems are being employed nowadays [65].

Today, the skimming of automated plate machine (ATM) systems is increasing dramatically. Action is thus necessary for the progress and safety of the ATM devices. An ATM is an electronic telecommunication device which aids bank clients in transactions and money transfer in their account [66]. ATM is an automated accounting machine. The consumer enters his unique PIN, that is, saved in the chip of the card [67]. The number of incidents of fraud has also dramatically grown due to the installation of ATM and the number of ATM card holders [68]. Technological advances have led to a rise in different skimming activities [69]. In order to make it more safe, convenient and dependable, advancements in the current systems are therefore included. The security system used must be high speed and long lasting [70].

The purpose of this article is to create a locker locker system for the protection of precious objects utilizing Face Recognition, Iris Scanner and Palm Vein technology (PVR). A face-identification system is a system that uses MATLAB software to identify and authenticate a user's picture [71,72]. Camera captures pictures of an individual entering an uncontrolled area and compared the image to an already existing legitimate user database [73]. Iris The mechanism of recognition employs abundant features in the body [74]. This technique is used for biometric authentication in categories such as immigration and border control, public safety, tourism and hospitality etc [75,76].

The digital and network information era has now invaded human civilization. The digitalisation of human identification is a distinctive aspect of our era [77]. There is constantly a global need for precise and reliable identification and verification and the function of biometric authentication technologies such as fingerprint, faces, finger veins, iris and DNA in our society is becoming ever more vital [78,79]. Thanks to the fast growth of cloud and Internet technology, biometric cloud authentication technology is becoming an important development path for the technology of biometrics. The identification of iris is an essential biometric technique among them [80].

In recent years, increased usage of biometric authentication systems has become increasingly crucial for spoof fingerprint and iris detection [81]. For a target application, biometrics must be able to differentiate subjects reliably by means of one or more physical or behavioral signals such as fingerprint, face, iris, voice, palm or writing signs [82]. Biometric technologies are based on information and have numerous benefits over traditional security approaches [83].

The use of biometrics needs to validate character or the capacity to perceive individuals accurately [84]. Biometric frameworks have significantly improved the recognizability of individual evidence and confirmation, which are crucial to personal, national and global safety [85]. Many systems need to authenticate the identity of a person before accessing resources [86].

Biometrics can allow a more comfortable and safe identification of individuals than conventional methods. Biometrics can operate in some cases as opposed to current security systems. This paper aims to survey an integration between the iris and fingerprint and combine them into a common framework.

## 2. BIOMETRIC RECOGNITION SYSTEM

Verification of people a primary important concern in security. A biometric system is a pattern recognition that identifies someone by definite physiological or behavioral feature [87-89]. Systems that use a single biometric feature for the purpose of identifying a person are called unimodal biometric systems [90,91]. There are several systems in place nowadays built using a single biometric feature [92]. Biometric verification systems operate on the principle of comparison between stored values and current values.

The biometric information is stored in a database after extracting the important features in return, when the identity of the person is verified, the same methods are used to extract the features and compare the result with those stored in the database in the event that the extracted characteristics match a certain percentage, and the system makes an authorized or unauthorized decision. [87]. The necessary steps of any typical

authentication biometric system comprise four steps Fig. (1).

Acquisition: Biometric sensor hardware is the core component of this device, collecting biometric data from individuals. There are camera sensors to take pictures of a person's face and iris image, scanner to extract fingerprint samples, etc. [93,94].

Feature extraction: The extracted biometric information is then stripped of all obsolete or corresponding data and isolated useful characteristics [95-97].

Matching component: In this stage, the unknown features are evaluated against the stored database results. The result represents the degree of similarity between a pair of biometric data using the same features [98,99].

Decision module: Here function vectors from an unknown topic are matched against data in a database. The matches are then placed into a matrix as scores representing the degree of relation between the unknown data and the stored reference data. For the same subjects with both positive and negative data, you need high and low scores and different issues and have other final scores [98,100].

## 2.1 Iris and Fingerprint Recognition System

### 2.1.1 Iris recognition

Iris recognition is an important and much preferred method of identification. Iris is a part of the eye located between the dark pupil and the white sclera that shows several gem-like characteristics. There's a variation in the texture of iris that's pretty much constant over a person's life [101,102]. The general method of iris identification is done within the following steps:

- Image Acquisition: Receives a picture of the eye.
- Iris Segmentation: This is localized the iris's spatial extent by it's away from other structures, such as the sclera, pupil, eyelids, and eyelashes.
- Normalization: A geometric normalization scheme is being used to convert the iris image from a Cartesian image to a polar image.
- Feature Extraction: The information needed to identify an individual is the most selective among the retina.
- Matching: find how closely the algorithm code matches the features encoded saved in the database.

### 2.1.2 Fingerprint recognition

People have long been using fingerprints as a form of personal identification [103-105] . There are four main steps for the implementation of a fingerprint recognition system:

Image acquisition: In this process, Fingerprint is first acquired using scanners and cameras. The quality of captured images can affect the fingerprint recognition system's performance, thus leading to blurred photographs.

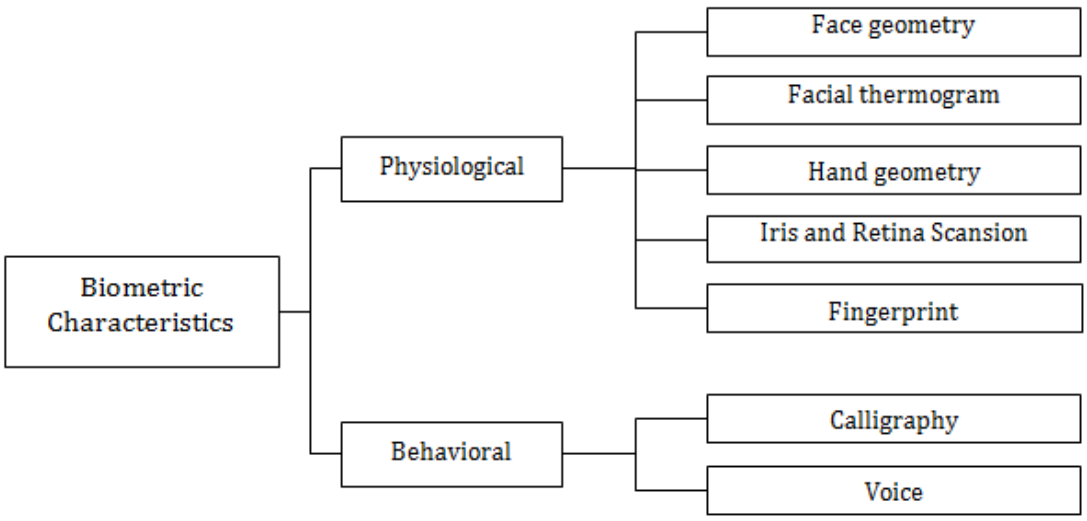


**Fig. 1. Biometric recognition system**

Image Enhancement: After image, the acquisition will occur. These kinds of wrinkles and defects can alter the consistency of the picture. It is difficult to recover the right ridge or valley of fingerprint picture in certain unrecoverable regions to recover the missing print.

Pattern Recognition: A pattern can be described as a sequence of attributes. The structure is a noticeable feature of a compound, rather than the essence of the elements of which it is composed. The topic of pattern recognition is divided into two parts: decision theoretic and structural.

Fingerprint feature extraction: The issue of developing a fingerprint recognition system is to decide what feature should be used and how features of a fingerprint should be categorized according to a system's intent. Tiny locally specific ridges and valleys' specific structures are also useful in detecting false data in fingerprint identification.

## 2.2 Quality Measurements

1-False Acceptance Rate (FAR): It is measured from the number of false acceptance out of the number of attempts [106].

$$\mathrm{FAR} = \frac{\text{number of false acceptance}}{\text{number of attempts}} \quad (1).$$

2-False Rejection Rate (FRR): It is measured from the number of rejections out of the number of attempts [106].

$$\mathrm{FRR} = \frac{\text{the number of rejections}}{\text{number of attempts}} \quad (2).$$

## 3. HYPER BIOMETRIC

Machine recognition technology based on digital images has become an important means of identifying target persons. The two biological features of iris and fingerprint have the advantages of good concealment and non-invasiveness. These two features are independent and orthogonal to each other in the feature space [107]. iris are two-dimensional images, which are affected by conditions such as illumination, expression changes, and posture, but the fingerprint will not be interfered by these environmental changes. The fingerprint will be affected by conditions such as the position of the fingerprint in relation to the scanner [108]. The fusion of these two different attributes of biological characteristics has the following advantages:

1. It can reduce the risk of theft and imitation of biological characteristic codes.
2. It can improve the recognition accuracy of the target person in harsh environments. In the complex environment of public places such as airports, military, and banks, dual-modal fusion can complement each other's strengths and improve the robustness of the overall identification system.

## 3.1 Fusion Levels

There are various kinds of approaches used in configuring the multimodal biometric authentication method [109,110]. It should be the first, most critical and fundamental element. There are multiple benefits and drawbacks involved with each of the fusion levels. In a multimodal biometric device, each of the essential components would be further match [111-113]. The four different stages of device fusion are listed below.

- Sensor Level: In this way, the collected data derived from various sensors are taken together. Multiple samples of biometrics should be taken, e.g. A camera can catch the image of the face or iris from multiple angles. The identical sensor may be used for taking other attributes, e.g., Facial pictures and voice recordings are made in a set time, or interval. Different sensors can be used for identifying different individuals using fingerprint, face and eyes.
- Feature Level: In the first step, all biometric traits are processed and then computed separately from them. In this way, input from several different sensors and biometrics are obtained from other individuals on different periods and combined to get a feature vector for effective public protection. To avoid unfortunate mate decisions, the traits from the varying array of sensors must be compatible.
- Score Level: in these cases, a match score is extracted from biometric results. It displays how close the function in the feature vector is to the stored prototype feature vector. Based on the test, scores are mixed. Biometric data of the individual

users is analyzed, and the results are then extracted and merged.

- Decision Level: Each of the biometric samples is pre-processed differently. First, the data is captured, then the features of each are extracted and then depending on this trait, they are whether good or poor. The results of each of the multiple steps are merged to get a product.
- Ranking: This method uses the principle of making a vote (majority), where the final value is determined by taking the majority value.

## 4. ASSESSMENT AND RECOMMENDA-TION

This section is deals with a research papers that used the iris and fingerprint. The comparison was made according to the data set, method, fusion level, and the accuracy of the results.

### 4.1 Iris and Fingerprint Research Direction

Iris and fingerprint feature fusion recognition involves multiple research directions such as image, processing and information fusion technology. In the past few decades, iris recognition and fingerprint recognition have made great progress, respectively, as an interdisciplinary frontier research topic. Bimodal biometric recognition is based on the development of iris and fingerprint recognition, and certain progress has also been made. The following is a Research used iris and fingerprint for recognition. Bhavya D. N. et al. [114]. The authors develop an identification method for fingerprints and Iris used biometric identifiers to children in the Children Multimodal Biometric Framework. Initially, the similarity between fingerprints and iris images was investigated

**Table 1. Existing biometric traits schedule**

| Authors | Year | Dataset | Method | Fusion Level | Performa-nce |
|---|---|---|---|---|---|
| Bhavya D. N, et al, [38] | 2020 | CMBD | KNN, SVM, NB | Decision | recognition rates=94 |
| Ahmed Shamil Mustafa et al, [39] | 2020 | CASIA-Iris AND FVC 2004 | KNN | Decision | Accuracy = 90% |
| K. Gunasekaran et al, [40] | 2019 | Benchmark/real dataset. | Deep Learning Template Matching Algorithm | Rank | FAR = 35% |
| Ashraf A. et al, [35] | 2015 | FVC2004 DB3_A, CASIA and faces94 databases | 1D log-Gabor Hamming distance | Score | Accuracy =99.7% |
| S. M. Rajhi et al, [41] | 2015 | CASIA v4 | DWT | Feature | EER =0.4573 |
| Sameer P P. et al, [42] | 2014 | IIT Delhi Database | Gabor filter | Decision, Score | FAR = 0.33% FRR = 3.1% |
| Houda B. et al, [43] | 2014 | CASIA-Iris | fuzzy logic | Decision | Accuracy = 98.3% |
| HEZIL N. et al, [44] | 2013 | CASIA V1.0 | Gabor transformation; | Score | FAR = 0 % FRR = 4.3% |
| Kamer V. et al, [45] | 2013 | SDUMLA-HMT CASIA-Iris-Lamp | Minimum Score, Maximum Score Simple Sum and User Weighting | Score | EER = 0.00010 % |
| Mahmood Al-k [46] | 2012 | CASIA V3 | Euclidean distance, Haar wavelet and ridge termination points Bifurcation | Feature | Accuracy = 98.4% |
| Vincenzo C. et al, [47] | 2010 | FVC2002 DB2 and BATH | ROIs and Log-Gabor | Template | Accuracy = 98.3% |

using Histogram of Gradients (HOG), Gabour and Maximum response. The fusion of all the feature vectors is emphasized as preferred by the characteristics of biometrics. Principal Component Analysis (PCA) is used to select features. The reduced features are fed into K-Nearest Neighbor (KNN), Support Vector Machine (SVM), and I Bayes decision law (NB). In multi measure biometric framework, features and classifiers combination for children is finished. Fingerprint recognition and face recognition has shown to be successful for criminal investigations. Furthermore, it advances the BMB strategy. Ahmed Shamil Mustafa, et al. [115]. This [approach] used fingerprints and iris biometrics which are captured by a laser iris scanner, using Gray-Level Co-occurrence Matrix (GLCM) for feature extraction and then the AND gate and it would be the final decision. Comparing outcomes of four personalization strategies on test users, the proposed fusion technique showed the most effectiveness, with 95 percent of final decisions being made correctly. K. Gunasekaran et al, [116]. This paper presents a multimodal biometric system which uses three traits (face, fingerprints and iris) for human recognition. To minimize feature vector dimension in the temporal domain, first pre-processing using Contourlet Transform Model is performed. The next step is to be applied to the pre-processed features where the specific feature is discriminant between two classes, which will increase efficiency in classification accuracy. Under weighted rank fusion, feature vectors from multiple modalities are combined to output the final biometric-based matching ranking (i.e. face, fingerprint and iris). In order to increase the object recognition rate of the multimodal biometric method, a deep learning framework is proposed. Ashraf Aboshosha et al, [109]. Acombination of fingerprint, retina, and facial features is used to enhance the device's accuracy. Scores are normalized first by applying a min-max normalization technique. So must use the product, the sum and the weighted sum rules to obtain fusion. The experimental results show that for multimodal biometric systems are better than single modal systems. S. M. Rajbhoj et al, [117]. A multi-biometric method using the image-level fusion of fingerprint and iris recognition is proposed in this paper. Using images obtained from iris and fingerprints are iris, and fingerprint image is incompatible, non-homogenous, and their relationship is not established. In this case pixel information is fused in the image and the developed, unique feature vector can be used for biometric systems. Features are stored as templates and are used for matching. Matching is carried out using the Hamming distance scale. Using standard database and database generated by us, evaluate the proposed structure. The system overcomes the limitations of the unimodal biometric system, and it has a low error rate equal to 0.4573. Sameer P Patil et al, [118] The authors, propose a biometric person identification system that employs both iris and fingerprint images. They aim to enhance the efficiency of Iris and Fingerprint recognition method. There are several ways to include biometric identification systems using one of the two modalities. The effect of multiple modalities has provided higher accuracy and reliability, as said by numerous experiments conducted. Houda Benaliouche et al, [119] In the research, examines the output of various automatic identity recognition systems with three different methods, classical sum rule, weighted sum rule, and fuzzy logic method. Biometric traits derived from the iris and fingerprint are fused at two scoring levels. The normalization of both scores is Min-max rule using for normalization of both scores. These experimental studies indicate that the fuzzy logic approach for assignment of scores combination is the best followed by the classical weighted sum rule and the classical rule as the sum of scores. Experimental findings are viewed as well as comparative results of previous works, which should be helpful. It can reproduce human thinking in a soft and comfortable way; therefore, it is cognitive. HEZIL Nabil et al, [120]. The paper introduces the biometric method using two forms of biometrics iris and fingerprint. The matching score applies at the stage of the match. Experimental results showed that the built system has a very high recognition rate. Kamer Vishi1 et al, [121]. Introduce a new biometric framework to combine iris and fingerprint features to authenticate using score-level fusion. After combining the individual scores for each iris and fingerprints collected, the four-category scores are designed (Minimum Score, Maximum Score Simple Sum and User Weighting). The fusion score is used to identify unknown users into the right owner or impostor. Mahmood Al-k. et al, [122]. The algorithm used for identifying the Iris image given by Ng et al. uses the rapid haar wavelet decomposition. In contrast, the algorithm used by Porapanomchai et al. is the Euclidean distance from the bifurcation point to the core point. After modifying and combining the two algorithms, the hybrid algorithm was developed. The simulation results show the improvement of the efficiency and the additional advantages of both recognition methods. Vincenzo Conti et al,

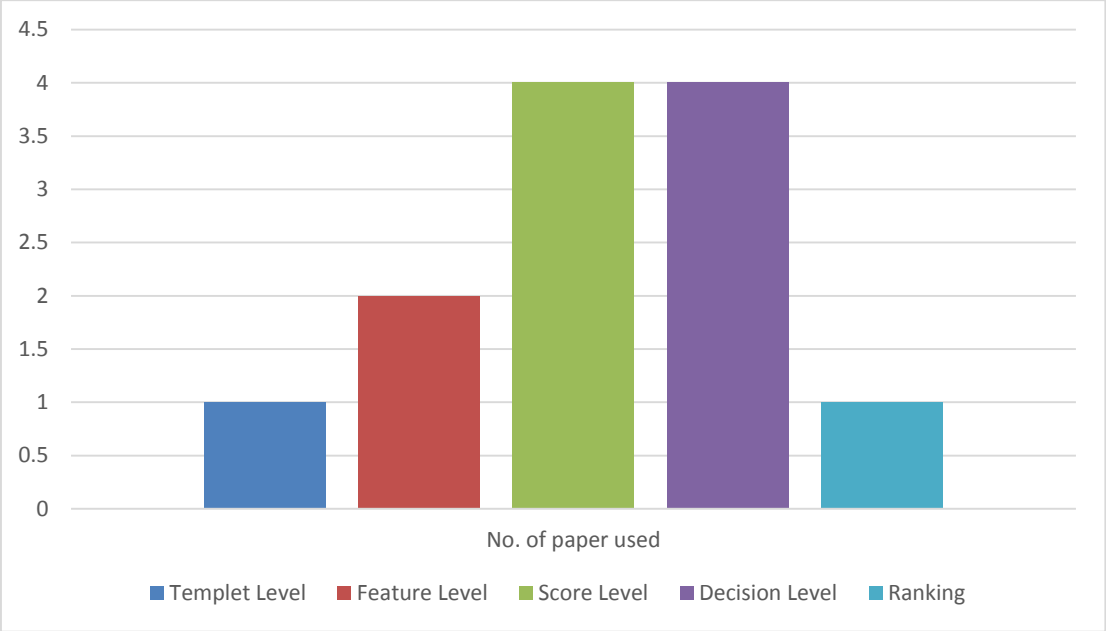


**Fig. 2. Fusion levels used in survey**

[123]. A multimodal biometric identification system based on iris and fingerprint traits is suggested. The paper is a state-of-the-art implementation of multi-biometric on features fusion is applied. With a frequency-based approach, a biometric vector is created that includes iris and fingerprint data. A multimodal framework reached a very interesting working point, with FAR = 0% and FRR = 5.71% using the entire DB2B and a randomly chosen same-size subset of the BATH database. In addition to the above, considering the BATH database and the FVC2002 DB2A database, it is obtained a further beneficial result with FAR = 0% and FRR = 7.28% ÷ 9.7%.

Much work has been done on iris and fingerprint biometrics. Table 1 shows the different work done by various authors in this area. Here the researchers have used iris and fingerprint biometric features and combined them using different fusion algorithms. Multimodal traits iris and fingerprint have been combined. The table shows the algorithms used for feature extraction of the different traits and the fusion levels used for combining the iris and fingerprint biometrics.

### 4.2 Discussing and Future Work

As shown in Table 1, much of the research used Decision fusion level and Score fusion level. Score fusion level achieved higher accuracy and less FAR compared to Decision fusion level in various methods. However, recent research trends for the year 2019-2020 have been directed to using decision fusion level with machine learning algorithms, like KNN and SVM NB. FAR is the main factor in accepting the results of methods and since most of the products indicate the preference of Score fusion level, which the matching score matches each output with the required value.

Fig. (2) show that feature and score fusion level and Decision Fusion Level are most used for hyperring biometric features. The preference for using the Score fusion level to match the results of recognition between iris and fingerprint is better, as recognition of each feature separately and matching these results improves the accuracy of the results. Future work may lead to the use of Score fusion level with a machine learning algorithm.

## 5. CONCLUSION

Biometrics feature is to use the characteristics of the body as the identification code. These features include unique behavior patterns such as face, eyeballs, fingerprints, palm shape, or voice. Biometric authentication technology in today's information society provides an ability to the best solution to improve the safety of use; people have gradually learned that biometric authentication technology and systems can bring convenience in life and a safer use environment.

Multiple biometric identification systems have advantages over single biometric identification systems. Researchers have developed several technologies that use fingerprint and iris for personal authentication. This paper showed that the iris and the fingerprint were combined by different authors using different combination methods and algorithms. Exacting challenges like the number of modalities, choice of a suitable model, best fusion level, and finest way of extracting features from the attribute still exit. For accurate authentication, better and efficient systems can be developed. This will be particularly beneficial for the systems where the security of the data is of main concern.

Biometric technology quickly become part of people throughout the world's everyday existence. Many of us engage everyday with some sort of biometric authentication via integration with mobile devices. Medicine, banking, marketing, and many other areas in which personal identifying is necessary are the future for biometric trends.

## DISCLAIMER

The products used for this research are commonly and predominantly use products in our area of research and country. There is absolutely no conflict of interest between the authors and producers of the products because we do not intend to use these products as an avenue for any litigation but for the advancement of knowledge. Also, the research was not funded by the producing company rather it was funded by personal efforts of the authors.

## COMPETING INTERESTS

Authors have declared that no competing interests exist.

## REFERENCES


1. Hammad M, Liu Y, Wang K. Multimodal biometric authentication systems using convolution neural network based on different level fusion of ECG and fingerprint. IEEE Access. 2018;7:26527-26542.
2. Olade I, Liang HN, Fleming C. "A review of multimodal facial biometric authentication methods in mobile devices and their application in head mounted displays," in 2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI). 2018;1997-2004.
3. Haji SH, Ameen SY. Attack and anomaly detection in iot networks using machine learning techniques: A review. Asian Journal of Research in Computer Science. 2021;30-46.
4. Tarannum A, Rahman ZU, Rao LK, Srinivasulu T, Lay-Ekuakille A. An efficient multi-modal biometric sensing and authentication framework for distributed applications. IEEE Sensors Journal. 2020;20:15014-15025.
5. Izadeen GY, Ameen SY. Smart android graphical password strategy: A review. Asian Journal of Research in Computer Science. 2021;59-69.
6. Dino HI, Zeebaree SR, Salih AA, Zebari RR, Ageed ZS, Shukur HM, et al. Impact of process execution and physical memory-spaces on OS performance; 2020.
7. Zabidi N, Norowi N, Wirza R. A Survey of user preferences on biometric authentication for smartphones. International Journal of Engineering and Technology. 2018;7:491.
8. Haji SH, Zeebaree SR, Saeed RH, Ameen SY, Shukur HM, Omar N, et al. Comparison of software defined networking with traditional networking. Asian Journal of Research in Computer Science. 2021;1-18.
9. Rui Z, Yan Z. A Survey on biometric authentication: Toward secure and privacy-preserving identification. IEEE Access. 2019;7:5994-6009.
10. Zhang Q. "Deep learning of electrocardiography dynamics for biometric human identification in era of IoT," in 2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON). 2018;885-888.
11. Nazarkevych M, Lotoshynska N, Brytkovskyi V, Dmytruk S, Dordiak V, Pikh I. "Biometric identification system with ateb-gabor filtering," in 2019 XIth International Scientific and Practical Conference on Electronics and Information Technologies (ELIT). 2019;15-18.
12. Bassi M, Triverbi P. "Human biometric identification through brain print," in 2018 Second International Conference on Electronics, Communication and

Aerospace Technology (ICECA). 2018;1514-1518.
13. Mei W, Deng W. Deep face recognition: A survey. Neurocomputing; 2018.
14. Hassan RJ, Zeebaree SR, Ameen SY, Kak SF, Sadeeq MA, Ageed ZS, et al. State of art survey for iot effects on smart city technology: Challenges, opportunities, and solutions. Asian Journal of Research in Computer Science. 2021;32-48.
15. Omran S, Salih M. Design and implementation of multi-model biometric identification system. International Journal of Computer Applications. 2014;99: 14-21.
16. Yasin HM, Zeebaree SR, Sadeeq MA, Ameen SY, Ibrahim IM, Zebari RR, et al. IoT and ICT based smart water management, monitoring and controlling system: A review. Asian Journal of Research in Computer Science. 2021;42-56.
17. Rinaldi A. Biometrics' new identity - measuring more physical and biological traits: Research into the characteristics that are unique to an individual is addressing the need to correctly identify people in a variety of medical, social and security contexts. EMBO reports. 2015;17.
18. Abdullah SMSA, Ameen SYA, Sadeeq MA, Zeebaree S. Multimodal emotion recognition using deep learning. Journal of Applied Science and Technology Trends. 2021;2:52-58.
19. Abdelwhab A, Viriri S. A survey on soft biometrics for human identification. Machine Learning and Biometrics. 2018;37.
20. Pititheeraphab Y, Thongpance N, Aoyama H, Pintavirooj C. Vein pattern verification and identification based on local geometric invariants constructed from minutia points and augmented with barcoded local feature. Applied Sciences. 2020;10:3192.
21. Aziz ZAA, Ameen SYA. Air pollution monitoring using wireless sensor Networks. Journal of Information Technology and Informatics. 2021;1:20-25.
22. Mahadi N, Mohamed MA, Mohamad A, Makhtar M, Abdul Kadir MF, Mamat M. A survey of machine learning techniques for behavioral-based biometric user authentication ed; 2018.
23. Amanuel SVA, Ameen SYA. Device-to-device communication for 5G security: A review. Journal of Information Technology and Informatics. 2021;1:26-31.
24. Malik J, Girdhar D, Dahiya R, Sainarayanan G. Reference threshold calculation for biometric authentication. International Journal of Image, Graphics and Signal Processing. 2014;6:46-53.
25. Abdullah DM, Ameen SY. Enhanced Mobile Broadband (EMBB): A review. Journal of Information Technology and Informatics. 2021;1:13-19.
26. Gao Q, Pinto D. "Some challenges in forensic fingerprint classification and interpretation," in 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT). 2016;1-7.
27. Panchal G, Patel G. "A recent trends and analysis of various techniques of false minutiae removal for fingerprint image," in 2017 International Conference on Intelligent Sustainable Systems (ICISS). 2017;681-684.
28. Khalid LF, Ameen SY. Secure Iot integration in daily lives: A review. Journal of Information Technology and Informatics. 2021;1:6-12.
29. Kumar V, Asati A, Gupta A. "An iris localization method for noisy infrared iris images," in 2015 IEEE International Conference on Signal and Image Processing Applications (ICSIPA). 2015;208-213.
30. Thavalengal S, Corcoran P. "Iris recognition on consumer devices—Challenges and progress," in 2015 IEEE International Symposium on Technology and Society (ISTAS). 2015;1-4.
31. Sharif KH, Ameen SY. "A review of security awareness approaches with special emphasis on gamification," in 2020 International Conference on Advanced Science and Engineering (ICOASE). 2020;151-156.
32. Hasan BMS, Ameen SY, Hasan OMS. Image authentication based on watermarking approach. Asian Journal of Research in Computer Science. 2021;34-51.
33. Hamed ZA, Ahmed IM, Ameen SY. "Protecting windows OS against local threats without using antivirus," relation. 2020;29:64-70.
34. Mohammed K, Ameen S. Performance investigation of distributed orthogonal space-time block coding based on relay selection in wireless cooperative systems; 2020.
35. Fawzi LM, Alqarawi SM, Ameen SY, Dawood SA. two levels alert verification

technique for smart oil pipeline surveillance system (SOPSS). International Journal of Computing and Digital Systems. 2019;8:115-124.
36. Al-Sultan MR, Ameen SY, Abduallah WM. Real time implementation of stegofirewall system. International Journal of Computing and Digital Systems. 2019;8:498-504.
37. Al Janaby AO, Al-Omary A, Ameen SY, Al-Rizzo HM. "Tracking high-speed users using SNR-CQI mapping in LTE-A networks," in 2018 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT). 2018;1-7.
38. Othman A, Ameen SY, Al-Rizzo H. Dynamic switching of scheduling algorithm for. International Journal of Computing and Network Technology. 2018;6.
39. Ameen SY, Ali ALSH. A comparative study for new aspects to quantum key distribution. Journal of Engineering and Sustainable Development. 2018;11: 45-57.
40. Fawzi LM, Ameen SY, Alqaraawi SM, Dawwd SA. Embedded real-time video surveillance system based on multi-sensor and visual tracking. Appl. Math. Infor. Sci. 2018;12:345-359.
41. Ali ZA, Ameen SY. Detection and prevention cyber-attacks for smart buildings via private cloud environment. International Journal of Computing and Network Technology. 2018;6:27-33.
42. Fawzi LM, Ameen SY, Dawwd SA, Alqaraawi SM. Comparative study of ad-hoc routing protocol for oil and gas pipelines surveillance systems. International Journal of Computing and Network Technology. 2016;4.
43. Farhan FY, Ameen SY. "Improved hybrid variable and fixed step size least mean square adaptive filter algorithm with application to time varying system identification," in 2015 10th System of Systems Engineering Conference (SoSE). 2015;94-98.
44. Othman A, Ameen SY, Al-Rizzo H. A new channel quality indicator mapping scheme for high mobility applications in LTE systems. Journal of Modeling and Simulation of Antennas and Propagation. 2015;1:38-43.
45. Othman A, Othman SY, Al-Omary A, Al-Rizzo H. Comparative performanceof subcarrier schedulers in uplink LTE-A under high users' mobility. International Journal of Computing and Digital Systems. 2015;4.
46. Othman A, Ameen SY, Al-Rizzo H. An energy-efficient MIMO-based 4G LTE-A adaptive modulation and coding scheme for high mobility scenarios. International Journal of Computing and Network Technology. 2015;3.
47. Ameen SY. Advanced encryption standard (AES) enhancement using artificial neural networks. Int J of Scientific and Engineering Research. 2014;5.
48. Ameen SY, Nourildean SW. Firewall and VPN investigation on cloud computing performance. International Journal of Computer Science and Engineering Survey. 2014;5:15.
49. Al-Khayat ON, Ameen SY, Abdallah MN. WSNs power consumption reduction using clustering and multiple access techniques. International Journal of Computer Applications. 2014;87.
50. Ameen SY, Yousif MK. Decode and forward cooperative protocol enhancement using interference cancellation. Int. J. Elect., Comput., Electron. Commun. Eng. 2014;8:273-277.
51. Ameen SY, Nourildean SW. "Coordinator and router investigation in IEEE802. 15.14 ZigBee wireless sensor network," in 2013 International Conference on Electrical Communication, Computer, Power, and Control Engineering (ICECCPCE). 2013;130-134.
52. Elzanati WM, Ameen SY. "Cost effective air-conditioning for bahrain domestic applications," in 2013 7th IEEE GCC Conference and Exhibition (GCC). 2013;535-540.
53. Ameen SY, Al-Badrany MR. "Optimal image steganography content destruction techniques," in International Conference on Systems, Control, Signal Processing and Informatics. 2013;453-457.
54. Ameen SY, Ahmed IM. "Design and implementation of e-laboratory for information security training," in 2013 Fourth International Conference on e-Learning" Best Practices in Management, Design and Development of e-Courses: Standards of Excellence and Creativity". 2013;310-317.
55. Ageed ZS, Zeebaree SR, Sadeeq MM, Kak SF, Yahia HS, Mahmood MR, et al. Comprehensive survey of big data mining approaches in cloud systems. Qubahan Academic Journal. 2021;1:29-38.

56. Abdulrahman LM, Zeebaree SR, Kak SF, Sadeeq MA, Adel AZ, Salim BW, et al. A state of art for smart gateways issues and modification. Asian Journal of Research in Computer Science. 2021;1-13.
57. Yazdeen AA, Zeebaree SR, Sadeeq MM, Kak SF, Ahmed OM, Zebari RR. FPGA implementations for data encryption and decryption via concurrent and parallel computation: A review. Qubahan Academic Journal. 2021;1:8-16.
58. Omer MA, Zeebaree SR, Sadeeq MA, Salim BW, Mohsin SX, Rashid ZN, et al. Efficiency of malware detection in android system: A survey. Asian Journal of Research in Computer Science. 2021;59-69.
59. Rashid ZN, Zeebaree SR, Sengur A. novel remote parallel processing code-breaker system via cloud computing; 2020.
60. Rashid ZN, Zeebaree SR, Shengul A. "Design and analysis of proposed remote controlling distributed parallel computing system over the cloud," in 2019 International Conference on Advanced Science and Engineering (ICOASE). 2019;118-123.
61. Malallah H, Zeebaree SR, Zebari RR, Sadeeq MA, Ageed ZS, Ibrahim IM, et al. A comprehensive study of kernel (issues and concepts) in different operating systems. Asian Journal of Research in Computer Science. 2021;16-31.
62. Rashid ZN, Zebari SR, Sharif KH, Jacksi K. "Distributed cloud computing and distributed parallel computing: A review," in 2018 International Conference on Advanced Science and Engineering (ICOASE). 2018;167-172.
63. Ibrahim IM. Task scheduling algorithms in cloud computing: A review. Turkish Journal of Computer and Mathematics Education (TURCOMAT). 2021;12:1041-1053.
64. Rashid ZN, Sharif KH, Zeebaree S. Client/servers clustering effects on CPU execution-time, CPU usage and CPU idle depending on activities of parallel-processing-technique operations. Int. J. Sci. Technol. Res. 2018;7:106-111.
65. Zebari IM, Zeebaree SR, Yasin HM. "Real time video streaming from multi-source using client-server for video distribution," in 2019 4th Scientific International Conference Najaf (SICN). 2019;109-114.
66. Jijo BT, Zeebaree SR, Zebari RR, Sadeeq MA, Sallow AB, Mohsin S, et al. A comprehensive survey of 5G mm-wave technology design challenges. Asian Journal of Research in Computer Science. 2021;1-20.
67. Ageed Z, Mahmood MR, Sadeeq M, Abdulrazzaq MB, Dino H. Cloud computing resources impacts on heavy-load parallel processing approaches. IOSR Journal of Computer Engineering (IOSR-JCE). 2020;22:30-41.
68. Sallow A, Zeebaree S, Zebari R, Mahmood M, Abdulrazzaq M, Sadeeq M. Vaccine tracker. SMS reminder system: Design and implementation; 2020.
69. Sadeeq MA, Zeebaree SR, Qashi R, Ahmed SH, Jacksi K. "Internet of Things security: A survey," in 2018 International Conference on Advanced Science and Engineering (ICOASE). 2018;162-166.
70. Yasin HM, Zeebaree SR, Zebari IM. "Arduino based automatic irrigation system: Monitoring and SMS controlling," in 2019 4th Scientific International Conference Najaf (SICN). 2019;109-114.
71. Sadeeq MA, Zeebaree S. Energy management for internet of things via distributed systems. Journal of Applied Science and Technology Trends. 2021;2:59-71.
72. Abdulazeez AM, Zeebaree SR, Sadeeq MA. Design and Implementation of Electronic Student Affairs System. Academic Journal of Nawroz University. 2018;7:66-73.
73. Sadeeq M, Abdulla AI, Abdulraheem AS, Ageed ZS. Impact of Electronic Commerce on Enterprise Business. Technol. Rep. Kansai Univ. 2020;62:2365-2378.
74. Alzakholi O, Shukur H, Zebari R, Abas S, Sadeeq M. Comparison among cloud technologies and cloud performance. Journal of Applied Science and Technology Trends. 2020;1:40-47.
75. Zeebaree S, Yasin HM. Arduino based remote controlling for home: Power saving, security and protection. International Journal of Scientific & Engineering Research. 2014;5:266-272.
76. Zeebaree S, Zebari I. Multilevel client/server peer-to-peer video broadcasting system. International Journal of Scientific and Engineering Research. 2014;5.
77. Maulud DH, Zeebaree SR, Jacksi K, Sadeeq MAM, Sharif KH. State of art for semantic analysis of natural language processing. Qubahan Academic Journal. 2021;1:21-28.

78. Shukur H, Zeebaree SR, Ahmed AJ, Zebari RR, Ahmed O, Tahir BSA, et al. A state of art survey for concurrent computation and clustering of parallel computing for distributed systems. Journal of Applied Science and Technology Trends. 2020;1:148-154.
79. Sallow AB, Sadeeq M, Zebari RR, Abdulrazzaq MB, Mahmood MR, Shukur HM, et al. An investigation for mobile malware behavioral and detection techniques based on android platform. IOSR Journal of Computer Engineering (IOSR-JCE). 2020;22:14-20.
80. Zebari SR, Yaseen NO. Effects of parallel processing implementation on balanced load-division depending on distributed memory systems. J. Univ. Anbar Pure Sci. 2011;5:50-56.
81. Jacksi K, Ibrahim RK, Zeebaree SR, Zebari RR, Sadeeq MA. "Clustering documents based on semantic similarity using HAC and K-mean algorithms," in 2020 International Conference on Advanced Science and Engineering (ICOASE). 2020;205-210.
82. Sadeeq MA, Abdulazeez AM. "Neural networks architectures design, and applications: A review," in 2020 International Conference on Advanced Science and Engineering (ICOASE). 2020;199-204.
83. Sadeeq MM, Abdulkareem NM, Zeebaree SR, Ahmed DM, Sami AS, Zebari RR. IoT and cloud computing issues, challenges and opportunities: A review. Qubahan Academic Journal. 2021;1:1-7.
84. Ageed ZS, Ibrahim RK, Sadeeq MA. Unified ontology implementation of cloud computing for distributed systems. Current Journal of Applied Science and Technology. 2020;82-97.
85. Sulaiman MA, Sadeeq M, Abdulraheem AS, Abdulla AI. Analyzation study for gamification examination fields. Technol. Rep. Kansai Univ. 2020;62:2319-2328.
86. Kareem FQ, Zeebaree SR, Dino HI, Sadeeq MA, Rashid ZN, Hasan DA, et al. A survey of optical fiber communications: Challenges and processing time influences. Asian Journal of Research in Computer Science. 2021;48-58.
87. Raju AS, Udayashankara V. A survey on unimodal, multimodal biometrics and its fusion techniques. International Journal of Engineering and Technology(UAE). 2018;7:689-695.
88. Bellaaj M, Khanfir Kallel I, Sellami D. Probability-possibility theories based iris biometric recognition system. ELCVIA: Electronic Letters on Computer Vision and Image Analysis. 2019;18:0020-37.
89. Al Janaby AO, Al-Omary A, Ameen SY, Al-Rizzo H. Tracking and controlling high-speed vehicles via CQI in LTE-A systems. International Journal of Computing and Digital Systems. 2020;9:1109-1119.
90. Gawande U, Golhar Y. Biometric security system: a rigorous review of unimodal and multimodal biometrics techniques. International Journal of Biometrics. 2018;10:142.
91. Zeebaree S, Ameen S, Sadeeq M. Social media networks security threats, risks and recommendation: A case study in the kurdistan region. International Journal of Innovation, Creativity and Change. 2020;13:349-365.
92. Oloyede M, Hancke G. Unimodal and multimodal biometric sensing systems: A review. IEEE Access. 2016;4:1-1.
93. Meng W, Wong D, Furnell S, Zhou J. Surveying the development of biometric user authentication on mobile phones. IEEE Communications Surveys and amp Tutorials. 2015;17:1268-1293.
94. Ageed ZS, Zeebaree SR, Sadeeq MM, Kak SF, Rashid ZN, Salih AA, et al. A survey of data mining implementation in smart city applications. Qubahan Academic Journal. 2021;1:91-99.
95. Majd B, Kallel I, Sellami D. Probability-possibility theories based iris biometric recognition system. Electronic Letters on Computer Vision and Image Analysis. 2019;18:20-37.
96. Ammour B, Boubchir L, Bouden T, Ramdani M. Face–iris multimodal biometric identification system. 2020;9.
97. Ageed ZS, Zeebaree SR, Sadeeq MA, Abdulrazzaq MB, Salim BW, Salih AA, et al. A state of art survey for intelligent energy monitoring systems. Asian Journal of Research in Computer Science. 2021;46-61.
98. Abdulkareem H. Fingerprint identification system using neural networks. Nahrain University, College of Engineering Jou rnal (NUCEJ). 2012;15:234.
99. Yahia HS, Zeebaree SR, Sadeeq MA, Salim NO, Kak SF, Adel AZ, et al. Comprehensive survey for cloud computing based nature-inspired algorithms optimization scheduling. Asian

Journal of Research in Computer Science. 2021;1-16.
100. Abdulqadir HR, Zeebaree SR, Shukur HM, Sadeeq MM, Salim BW, Salih AA, et al. A study of moving from cloud computing to fog computing. Qubahan Academic Journal. 2021;1:60-70.
101. Khanam R, Haseen Z, Rahman N, Singh J. "Performance analysis of iris recognition system," in Data and Communication Networks, ed: Springer. 2019; 159-171.
102. Albadarneh A, Albadarneh I, Alqatawna JF. "Iris recognition system for secure authentication based on texture and shape features," in 2015 IEEE Jordan Conference on Applied Electrical Engineering and Computing Technologies (AEECT). 2015;1-6.
103. Prasad RS, Al-Ani MS, Nejres SM. An efficient approach for fingerprint recognition. Image. 2015;4.
104. Ali MM, Mahale VH, Yannawar P, Gaikwad A. "Fingerprint recognition for person identification and verification based on minutiae matching," in 2016 IEEE 6th international conference on advanced computing (IACC). 2016;332-339.
105. Abdulla AI, Abdulraheem AS, Salih AA, Sadeeq MA, Ahmed AJ, Ferzor BM, et al. Internet of things and smart home security. Technol. Rep. Kansai Univ. 2020;62:2465-2476.
106. Hassan S, Shaar S, Raj B, Razak S. Online evaluation of classifier accuracy, false acceptance rate and false rejection rate; 2018.
107. Soares J, Gaikwad AN. "A self banking biometric machine with fake detection applied to fingerprint and iris along with GSM technology for OTP," in 2016 International Conference on Communication and Signal Processing (ICCSP). 2016;0508-0512.
108. Karunya R, Kumaresan S. "A study of liveness detection in fingerprint and iris recognition systems using image quality assessment," in 2015 International Conference on Advanced Computing and Communication Systems. 2015; 1-5.
109. Aboshosha A, Eldahshan K, Karam E, Ebeid E. Score level fusion for fingerprint, iris and face biometrics. International Journal of Computer Applications. 2015;111:975-8887.
110. Abdulraheem AS, Salih AA, Abdulla AI, Sadeeq MA, Salim NO, Abdullah H, et al. Home automation system based on IoT; 2020.
111. Walia GS, Singh T, Singh K, Verma N. Robust multimodal biometric system based on optimal score level fusion model. Expert Systems with Applications. 2019;116:364-376.
112. Zapata J, Duque C, Rojas-Idarraga Y, Gonzalez M, Guzmán J, Botero MB. "Data fusion applied to biometric identification–a review," in Colombian Conference on Computing. 2017;721-733.
113. Salih AA, Zeebaree SR, Abdulraheem AS, Zebari RR, Sadeeq MA, Ahmed OM. Evolution of mobile wireless communication to 5G revolution. Technology Reports of Kansai University. 2020;62:2139-2151.
114. Bhavya DN, CHK. Feature and decision level fusion in children multimodal biometrics. IJRTE 2020;8:6.
115. Al-Shayea ASM, Abdulelah A, Ahmed A. Multimodal biometric system iris and fingerprint recognition based on fusion technique. 2020;29:7423-7432.
116. Gunasekaran K, Jayamani R, Ramasamy P. Deep multimodal biometric recognition using contourlet derivative weighted rank fusion with human face, fingerprint and iris images. Automatika. 2019;60:1-13.
117. Rajbhoj S, Mane P. Transformation based approach of combining iris and fingerprint biometric at confidence level. International Journal of Computer Applications. 2015;116:1-5.
118. Ppatil S, Raka T, Sarode S. Multimodal biometric identification system: Fusion of Iris and fingerprint. International Journal of Computer Applications. 2014;97:31-36.
119. Benaliouche H, Touahria M. Comparative study of multimodal biometric recognition by fusion of Iris and fingerprint. TheScientificWorldJournal. 2014;829369.
120. Hezil N, Benzaoui A, Abdelhani B. Multimodal biometric system using Iris and fingerprint; 2013.
121. Vishi K, Yildirim Yayilgan S. Multimodal Biometric Authentication using fingerprint and iris recognition in identity management; 2013.
122. Alkhassaweneh M, Smeirat B, Ali T. A hybrid system of Iris and Fingerprint recognition for security applications; 2012.

123. Conti V, Militello C, Sorbello F, Vitabile S. A frequency-based approach for features fusion in fingerprint and iris multimodal biometric identification systems. Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on. 2010;40: 384-395.



*Peer-review history:*
*The peer review history for this paper can be accessed here:*
*http://www.sdiarticle4.com/review-history/70240*