Reviewing and analysing the current state-of-the-art recognition approaches for different traits to develop a Powerful multi-biometric system

Manvi Khatri [a], Dr. Ajay Sharma[b]

[a]Research Scholar, Department of Computer Science & Engineering, SRM University Delhi-NCR Sonepat, manvi.khatri.18@gmail.com
[b]Professor, Department of Computer Science & Engineering, SRM University Delhi-NCR Sonepat, ajay.s@srmuniversity.ac.in

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 4 June 2021

Abstract: Biometrics are intended to make human-machine interaction systems simpler, which makes them safer and more convenient. However, the vast majority of human-machine interfaces contain two opposing interests, contradicting needs: protection and privacy. Biometrics is much like any other type of computerised system: a working, functioning, and fast system are prerequisites. Finally, more importantly, biometric systems must overcome both the hesitancy in identification procedures and the fear of misuse of personal data in order to increase acceptance by the general public.

A problem with most widely adopted biometric technologies is the obtrusive process of gathering their required biometric features..

Keywords: Biometric, Traits, recognition, identification, fusion

1. Introduction

In the evolution of online threats, the use of user IDs and passwords is becoming a hindrance, so organisations are companies compelled to upgrade their technology to ensure the security of their digital identities almost 17.8 million hijacked domains and half a billion stolen accounts in 2017. In light of numerous examples of data breaches, many users have realised that traditional passwords are lacking, so they have shifted to more advanced authentication systems and see an increase in the potential for improving their overall computer security. Investing in Cybersecurity is no surprise at all. Cybersecurity concerns begin with keeping data and systems safe, especially those that comprise the digital world [1].

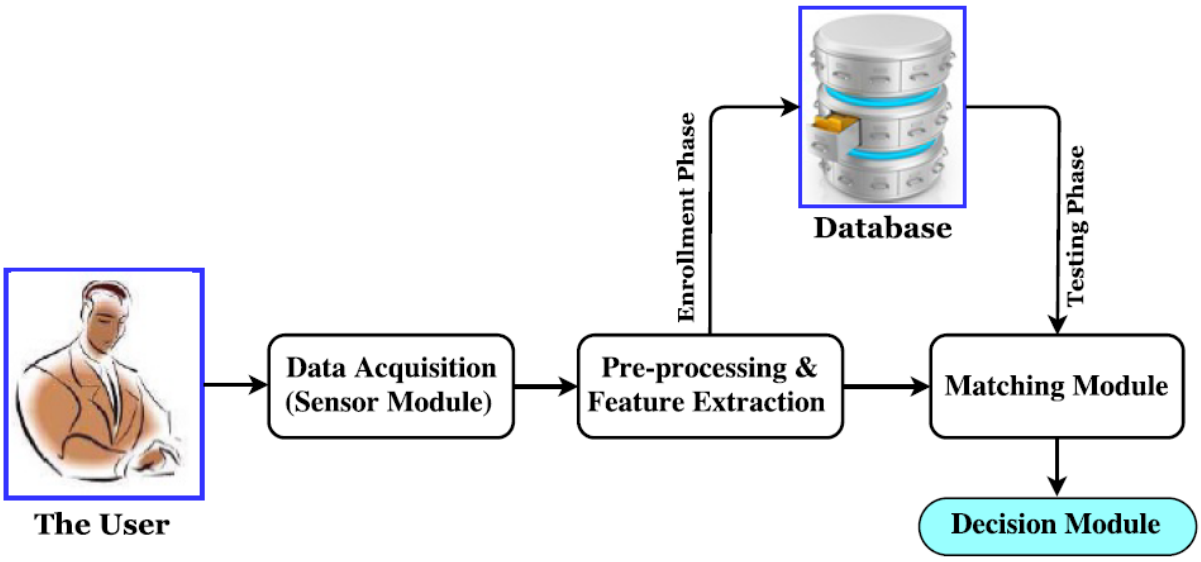

Figure 1.1: A general structure of a biometric system [6]

Emerging technologies, including fingerprints, as well as voice and facial recognition, lead to improvements in security and authentication systems In fact, biometrics offers more security and in some cases, if not all, and creates new market opportunities in other sectors as a result.

Tractica predicts that sales in the biometric industry will increase by 22.9% each year through to $69.8 billion until 2025. The majority of the new advances in biometrics will happen in smartphones, such as the integration of biometric technologies in a variety of fields such as the smart home, vehicle, healthcare, and financial service areas [2].

2. Principle of Biometric Recognition & Working

It uses physiological and behavioural characteristics to identify a person as a machine is creative It's built on hardware for computerised data acquisition that is able to compute the person's identity via mathematical algorithms. One can discern that a clear difference between biometric authentication and access control systems because the latter actually recognises the identity of those who has access, but the former doesn't know who the person is. Most commonly believed to be the main factors on which are used to determine individual identity using biometrics include: accuracy, security, and speed. Overall, the physiological characteristics are the most stable, but not always, while the behavioural ones are not as well.

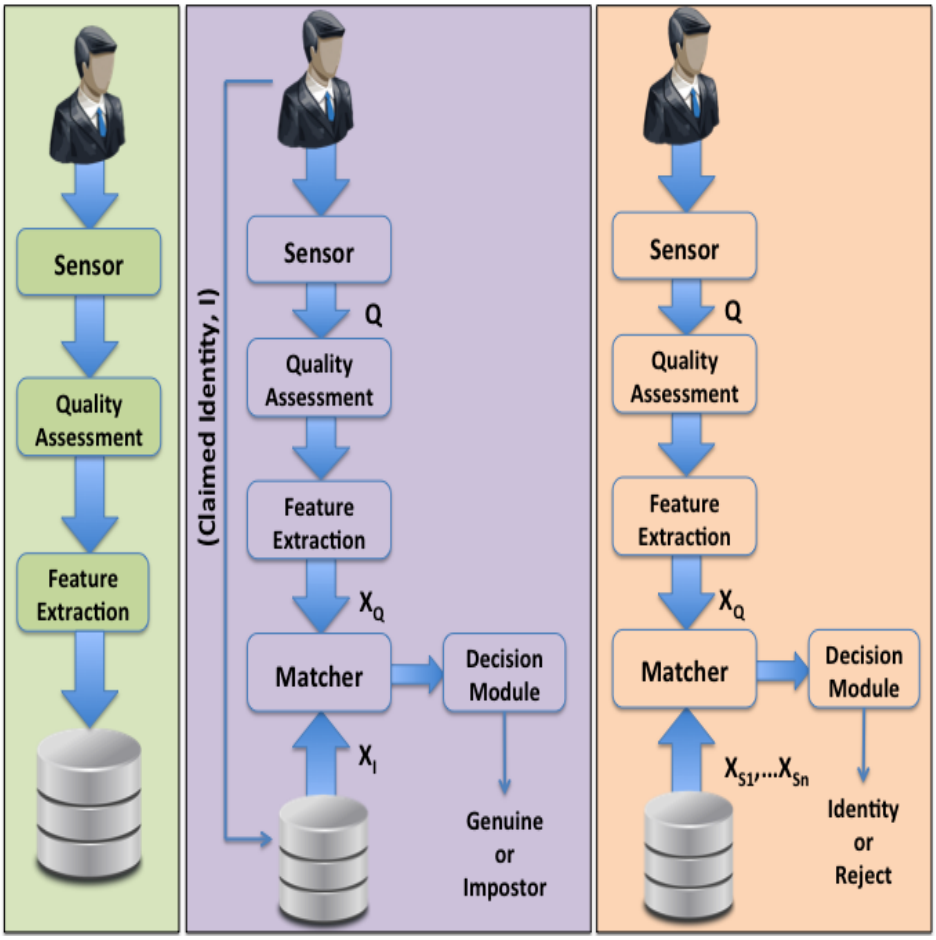

Figure 2: Enrolment, Verification and Recognition processes [10].

First and foremost (among the bodily characteristics, there are fingerprints, the height, weight, colour, and size of the retina; behavioural rather than verbal imprint, the clickety-clack of the keyboard, bodily movements, and so on [3].

What is biometric security for?

Different methods may be employed to verify or identify a person depending on the objective. The person declares his identity, which then establishes the reality of the sensors' ability to provide images or data by comparing them to an archive at the moment of detection.

In the case of a real-time process, biometric recognition occurs by comparing the image, data, and the information in the image and the existing database (one to many verification). Instead of creating a biometric identification based on creating biometrics based on stored and live physiological and behavioural characteristics. The new biometric system has reached its fullest potential because it offers extra protection while opening up new services for users.

Fingerprint recognition to the face and voice recognition, it is the most accurate. Current online security systems tend to frustrate potential buyers, leading to a higher number of failed attempts. The study, done by Mastercard and Oxford University, indicates that biometrics is preferred by customers over passwords.

Smartphones and laptops with fingerprint-recognition and face-ID systems have been around for quite some time and will most likely appear with the iPhone X. Because it is used to access the physical locations and digital services alike, the fingerprint is based on two unique characteristics: one, size and contour. Each individual has their own unique imprint.

Shortly after the use of fingerprints, there was a sharp increase in the use of iris scanning technologies. Currently, they are the most reliable in identifying individuals and verifying the uniqueness because the coloured portion of the eye provides an univocal code for each. In the last five years, we've seen two systems for recognising speech and face recognition enter the general population nearly effortlessly [4].

Vocal recognition is quite an outdated: it has existed since the first year that started to record spoken numbers in 1952 Analytics company predicted in early on that hardware products, such as Alexa and Google Home, will reach 15 million in 2022 versus 3 million in 2017. Two significant changes in facial recognition systems have grown by 27.7% each year in the time period 2013-2018. Even though, however firms expect that within the next six years will be very interested in facial recognition due to the advantages of a more streamlined experience for consumers and new business opportunities for software providers.

Among others, there are opportunities in the home automation, in automotive, and from digital payments to biometrics. Digital technology has increasingly become part of the daily routine, and people need biometric security that is fast and easy, which biometrics meet their needs: they allow consumers to access physical locations, speed up digital services, and guard against theft.

Because they are extremely user-friendly and simple to use, voice assistants and smart home systems have been widely adopted. These systems have both personal and general and domestic applications, and they are very simple to implement in a simple way. The systems themselves are not important [5].

Biometrics can also serves to monitor drivers, and distinguish between sleep and wakefulness in the transportation sectors, and to gather information which can benefit the healthcare industry in particular from their data. Technology from the user's perspective is the distinguishing characteristic in this case is a user-friendly experience. The same elements that will impact mobile digital payment in that will not only identify a user but also play a significant role in payment initiation is how they use biometrics. Mastercard recently announced a strategy to support financial institutions, as well as its customers, to leverage innovative technology like biometrics and artificial intelligence to offer greater security and an improved experience.

Why multimodal biometrics?

Fingerprint and face recognition authentication has the benefit of greatly across all channels, creating the "reduced friction" for traditional systems of identification. That means in other words, it is both the market and the users' desire to improve the experience that are increasing the prevalence of biometric systems. Methods of facial recognition will have a great impact on the user population; other technologies will be utilised in order to identify users in a more unspecific and secure way so as to facilitate financial transactions. Over the next few years, we'll see more machine learning, data analysis, and information from sensors be integrated with the game in order to deliver a totally different customer experience. A big, quick, reliable approach that offers significant cost advantages and scalability [6].

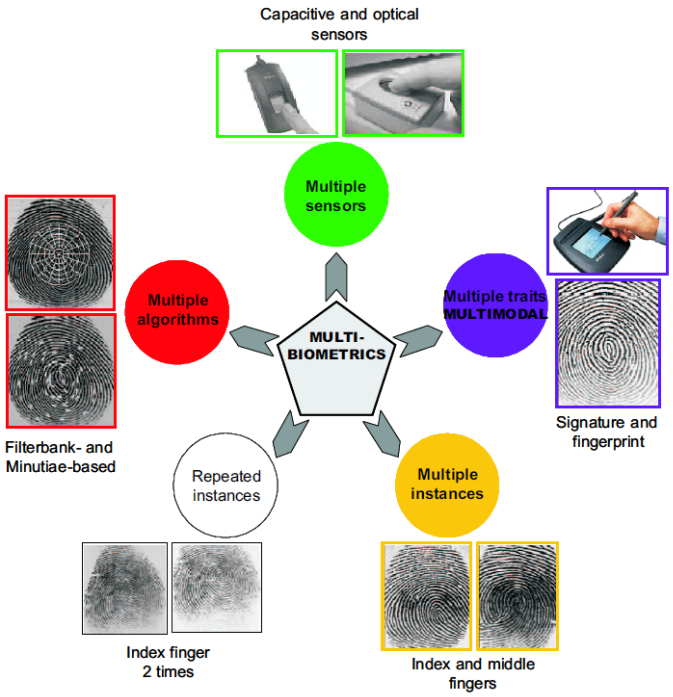

Figure 3: Multi-Biometric [11]

Finger and face recognition are among the most popular techniques, and the others include fingerprints, as well as pupil, iris, and DNA profiling. In addition to fingerprint and facial biometrics, it uses iris and retinal biometrics to enhance security and accuracy. Two different types of identification, for multi-modal biometrics Difficulties that are found in traditional modal systems can be overcome. They have been able to utilise several biometric features, such as the face and the iris or the fingerprints, in combination, for several years now and show clear improvement in their security.

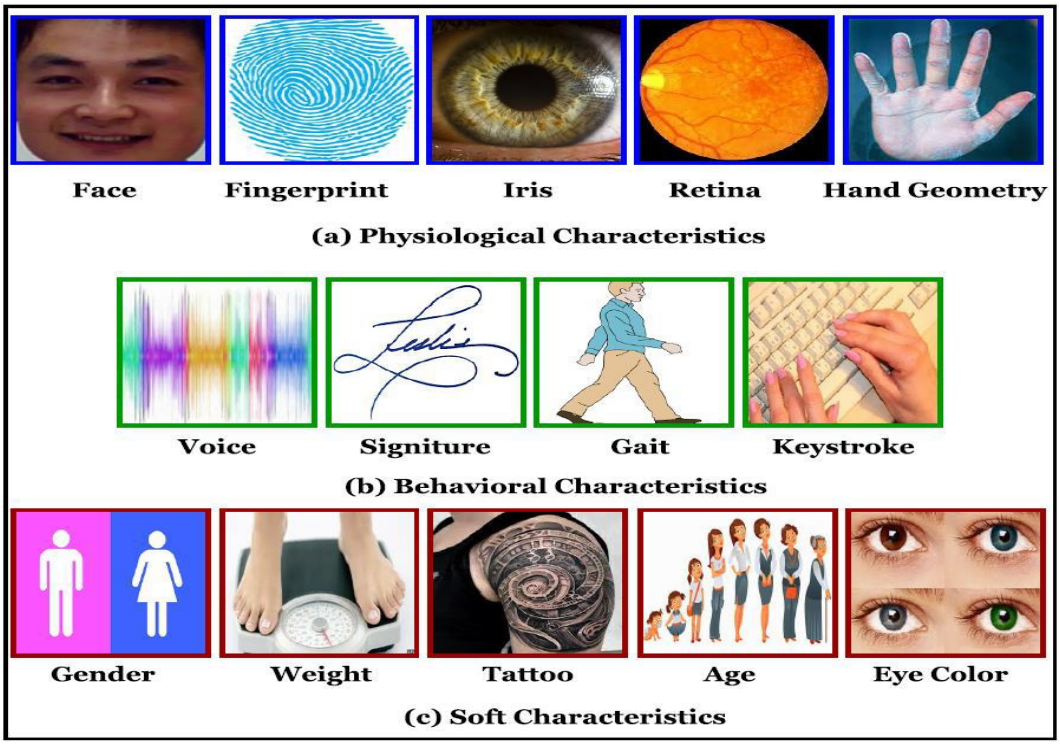

Figure 4: Examples of common biometrics: (a) Physiological, (b) Behavioral [15] and (c) Soft characteristics

Biometrics can be used in an additional authentication mechanism (MFA). The combination of geolocation, IP addresses, and patterns used to identify a user may be quite potent [7].

Advantages of biometrics

While biometrics such as fingerprints, handprints, facial characteristics, retina scans, palm prints, and palm and facial biometrics have many things in common, they all collect human characteristics.

- all-embrained and simple
- difficult to distinguish one from another
- unwavering and unswerving
- recorded (with or without consent)

Intangibles include hard-to-maintain values for future comparison (a face, a fingerprint) the characteristics of various biometrics. An intrinsic human characteristic is a biometric identifier. Those who identify solely with their physical characteristics and those who do not. The main benefits of physical entities are, for the most part, to be found in their invariance and device independence. Fingerprint readers have emerged in the last few years due to their widespread application to their current use on smartphones. Every electronic device has the capability to become a convenient and trustworthy fingerprint scanner. About one in two businesses use fingerprint scanning, according to Spiceworks.

If a device has a camera, it's simple to employ for verification. Facial recognition and retinal scans are two approaches that are used to identity people on the fly. The second most popular form of authentication, according to Spiceworks, is facial recognition at 14% of organisations. There are many different image-based authentication methods in use, such as hand geometry, iris and vein scanning, and retinal vein. Technologies have already applied voice recognition to user and customer identification and verification tools. Around 2% of companies in the company use voice recognition for user authentication.

Digital signatures are commonly found at the checkout and at financial institutions, as well as private enterprises, and they are a good option for situations where users and customers anticipate having to provide a signature. Not all that long ago, they were only employed in identifying criminals. The processing speed of DNA sequencing technology has, until recently, prevented it from being widely applied. This is beginning to look different. Last year, a $1,000 scanner was unveiled that does a DNA identification in minutes, and will further cut down on testing time and costs. This is more recent than previous methods and is used in combination with an alternative approach because it is less reliable. However, these behavioural characteristics may be more prominent in the further technology develops. Behavioralistic IDs have only the imagination as their bounding parameter, which means they can identify humans.

More and more modern applications, which may classify a person as a 'human' or 'robot' rely on this strategy today on machine learning. That allows a company to filter out junk and dictionary attacks. However, as technological systems get better, they become less successful at differentiating between people and machines [8]. The following are some typical approaches:

Typing styles are unique. An individual's propensity to communicate on the phone, their typing speed, and how long it takes to go from one letter to another have a message to the end result of the message are both associated with the impact of that communication on others

The characteristics of an individual gait allow their personality to be read like a book, and can be used as a means of positive identification in a building identification in locations where it is more critical.

- Interference: Interference from hand or mouse movements on trackpads or touch screens is specific to individuals, no additional equipment required.

- Technology usage: We use technology in a variety of ways. The manner in which we open and use apps, the rate at which we let our batteries go, when and when we use our phones, the way we hold them, and where we do it, and how we use the internet are all factually distinct traits that contribute to each individual's style. Until robots are able to mimic human behaviours, we can use these behavioural patterns to distinguish humans from other software agents. They can also be used with other authentication methods, or, should they improve enough, possibly used on their own in lieu of or alongside standard security measures.

Everything has a solution if you just keep searching long enough and hard enough. Individuals are typically motivated by the desire to keep their belongings and get to them at a quick and affordable price. A key challenge is confronted by governments and public administrations at the same time. To aid in passing through borders,

combat terrorism, and voter fraud, as well as immigration control, they have to streamline the process. All have to adhere to new international standards and regulations regarding security, with regards to production, as well as documentation of the systems, and checking of materials.

Let them spend within their means.

3. Problem Definition

Behavioural or physiological features is used in behavioural or biometric authentication. A biometric system such as fingerprint verification offers numerous advantages over systems that use possessions or special knowledge, like passwords, such as the person's fingerprint. It is very popular and is frequently used in day-to-to-to-day life. Usually, typical situations lookups are associated with security and authentication transactions. Due to the national security mandate, as well as demand for transactions to be private, this industry is quickly evolving.

Authentication versus Identification

In this essay, the claim is not that the use of a biometric identification tool means someone has been identified, but that he or she is verified as authentic.

There is no claim of identity in the latter; instead, the objective is to make the most probable answer. When there are more than one matching attributes in the database, there must be M ones. Classifying a biometric sample is challenging in an environment where all persons share the same set of traits. The game is to make the sample fit into either a category of J or to figure out who it is new. In applications such as access control where there is a small population, one may prefer to use a system that allows open identification rather than biometric authentication. an authorised user can provide his/her biometric identifier prior to gaining access to a secured resource, but is not required to state his/her identity [16] 1. Thus, the boundaries between applications do not make for a clear distinction, i.e.e. techniques developed in one case can be utilised in another.

Error Rates

If a biometric identifier is presented, the system should either grant or deny access (as it sees fit) (if the person is an impostor). By examining the system output relative to a goal threshold, this decision is in general can be described as follows: In the process of matching users, two errors can occur: the mistake of rejecting a real user, or the mistake of accepting a fake one. With respect to both rejected and accepted customers, the error rates are known as False Rejection Rate (FRR) and False Acceptance (FAR). These two measurements aid in understanding system performance analysis, using a DET curve. In the college-to-school match process, it is also common to use the metric of "Equal Error Rate" (or, Equal Error).

Desired Characteristics of Operational Biometrics

Automated, rapid, precise, and valid biometric authentication is beneficial. Two crucial criteria in the current generation of game development are using state-of-of-the-the-the-the-art multimedia sensors and powerful computers. On the other hand, accuracy and dependability remain two matters that are, as yet, not entirely resolved. Because no single type of biometric can produce a perfect authentication, they must be used in tandem to be certain. FAR and FRR have to be brought down to sustainable levels. Changing one type of error may also just increases the other types of errors. There needs to be a fundamental shift in accuracy for this to be improved. The same results should be expected every time a biometric sample is processed during testing.

According to the surveys, accepting an imposter is ten to one- or two orders of magnitude more costly, while refusing a client can vary greatly from one to a ten to one hundred. More training data: An earlier (day one) biometric system was more relaxed: You were not allowed to take any biometric samples during the start-up period, but had a great deal of biometric data: (less than four or so; in order not to annoy the user). means Building a statistical model or a machine-learning problem is thus. Data is said to be subject to “noise” risk. for facial occlusion as well as the user interactions (that over shorter time periods, such as capture devices, are not subject to optical changes, but over the long term, are especially influenced by external lighting and changes in muscle tissues) for example, skin change which is also an issue for recognition is extreme in recognition are facial recognition algorithms, among other things (e.g., appearance of wrinkles). A more reliable system means lessens the role of these extraneous influences [10].

Biometric verification for numerous computer systems

When two or more biometric systems are used together, both the system's accuracy and reliability can be increased. Choose any of the following approaches:

- Multimodal: measurement information from different viewpoints
- Multi-sensor: numerous body sensors, for example, fingerprint sensors

- Multi-presentation:: Many-to-to-one, distinct body sensor recording several measurements on one subject
- Multi-instance: the same sensor is applied by multiple feature extraction and classifiers

The focus of this thesis is on combinations of these types of biometrics, such as fusion biometrics. Thus, multi-system is the term is used in this thesis. We may call our approach to solving the multiple class problem a General Classifier (MCS). as this thesis only addresses above-novel approaches such as bagging, boosting, and error-correction coding, the more traditional ensemble algorithms like this This problem has been previously discussed, e.g., [9].

4. Fusion Techniques

Several techniques exist for integrating different types of information can be found in literature. The methods that utilise these concepts are known as fusion techniques. Fusion at the feature (features/song layer) is a standard (output of a single system). More often, the term 'between two' is used in literature. An article categorization method categorises three levels: one in which the scores are fused by taking the answers as probabilities, known as thesaurusical fusion, and a third method using a combination of scores as the most likely label (called decision level). I will only look at the score because the last two examples could also be using just labels, resulting in worse performance in practise.

Feature fusion

Concatenation at this level may lead to feature complexity, which is greater amounts of information, though still information fusion, in the form of posthocclusion Composite information has too many features, making it difficult for a given classifier to tackle. A feature, in particular, may not have the same features, i.e., one of varying sizes, types, and/countsizes. There certainly is something to be gained from a feature-fusion examination, but it will not be discussed here [31-36].

Working at the level of art instead hides the curse of dimensionality, on the other hand, feature compatibility is a problem of editing is avoided, on the other hand Furthermore, algorithms at the level of analysis can be separated from any form of biometric measurements. To tap into the available data, additional information must be fed externally. While this may appear contradictory, note that the biometric feature sets assume independence from one another as the feature level of fusion converges to the scoring system For multimodal biometric fusion, this assumption holds (LDA) [37]. If the dependency exists at the feature level, then it will likely also be present at the component. Such dependence can be handled at the level of the music.

Motivations

However, this is done elsewhere, e.g.g. in multi-band/ multi-features, multi-style identification, and the combination model. And in fact, multimodal biometric fusion has been studied as early as 1978." Biometric fusion has had nearly 30 years of proven use, so it has a track record of being implemented. All in all fairness, classifiers are problematic [38]. So, however, it may be argued, below are some other suggestions for a new theory on the subject:

- **Correlation and relative strength of systems:** While these two factors are recognised in regression problems, they are difficult to quantify and measured in classification problems [and are not well-defined here]." Because of this, a plethora of "diversity" metrics exist, but no one measures the fusion adequately: it is too weakly correlated with fusion effectiveness and highly prejudiced.
- **User-induced variability:** When the use of biometric systems was first observed, results from the system varied greatly from individual to another. It took 17 years, but eventually, this behaviour was identified [33]. Several questions must be addressed in the study of user-driven variability: whether this phenomena exists in all biometrically, and in all biometric systems; how to control it; and then how to go one step further, ways to deal with the claims of an identity being used to maximise overall performance.
- **Different modes of fusion:** Conventionally, modes of fusion has always had been done by looking at the outputs of all subsystems (and references herein). Functionality; for example, most of the time, one does not use all the subsystem features together in an application. Combining sub-systems in an efficient and accurate ways is advantageous.
- **On the use of chimeric users:** Due to the absence of vast multi-modal biometric bi-datas, it's also common to mix other biometrics with database biometrics to come up with chimaeras. the approach of using a chimeric database effectively allows for a large number of users, e.g., one thousand But this is a common practise, e.g., in the literature, e.g.,, [136], but it was challenged whether this was ethical, among others, in 2003 While the privacy is indeed obtained using chimaera, it remains unclear if it can be put to good use.

5. Design Issues In Multi-Biometric Systems

Three main requirements govern the design and implementation of a multi-biometric system: The architecture that will collect and process selected biometrics will be utilised in the multi-biometric system. Furthermore, six different data sources may be the source of the information that is required by the multi-biometric system. A third variable is also comes into play: the synthesis of the obtained traits and this place in the multi-dimensional system. Each aspect of the following will be covered in depth [12].

Multi-biometric Systems Architectures

One of the most difficult tasks in building a multi-bipart system is determining the appropriate biometric traits. A number of factors, including the type of application and its security and order, determine and select the best architecture. In the typical use, multi-biometric systems, they may be organised as either serial, parallel, or a combination of the two [21]. A tiereduction scheme known as the output of one trait can be used to prune the database size prior to acquiring the next Thus, the outcome of the subsequent trait is therefore dependent on the results of the previous trait. For example, using an iris and fingerprint biometric system, the best matching candidates are identified and the rest of the database is augmented with the fingerprint. As a result, the system throughput can be increased by gathering all the required modalities prior to making a decision. Furthermore, applied biometric traits must not be observed at the same time.

On the other hand, multiple biometric characteristics are acquired and then compared using an appropriate fusing technique to produce the final decision Because of this, the serial scheme is more convenient to the user, and the serial scheme requires less attention. As compared to the serial protocol, it has a higher security level, making it suitable for applications in the military.

Then, the serial and parallel schemes can be mixed in a third scheme. To combine multiple classifiers, as illustrated in the example in previous section, it is possible to handle missing biometric data and noisy biometric characteristics to form a tree-like structure (c). Butchery Since this type of multi-biometric architecture hasn't received a lot of attention in the research community, this remains speculative until further tests are completed [14].

Evidence Sources of Multi-biometric Systems

As shown in Figure 1, more than one biometric measurement source is needed to satisfy the multi-biometric concept, either physiological or behavioural. Under this category, you will find an explanation of the ways in which biometric data can be obtained in a multi-biometric system. There are 5 overall biometric themes and a sixth, which is the combination of two or more of these. The evidence provided by the multi-biometric system can be divided into five or more categories:

1) **Multiple Sensors/Single Trait:** Most facial traits can be detected using two different types of sensors, such as an infrared camera and a visible light camera, or using an optical sensor plus an ultrasonic one to capture the fingerprint.

2) **Multiple Algorithms/Single Trait**: To use a biometrics in this system, only one type of biometric is used to get combined results of feature extraction approaches and multiple classifiers Simultaneous multi-threaded applications are more economical than sequential multi-threaded ones due to just one sensor involvement and the reduced number of sensors needed. As a result, however, computational cost and time are increased by the need for multiple feature extraction and matching algorithms in multiple systems. Use, for example, a textural and minutiae-based algorithm.

3) **Multiple Samples/Single Trait:** This is employed to raise the system's resistance to biometric trait variability using a single sensor to represent more than one biometric property. For example, a single camera can recognise various facial traits, but not in a single orientation (frontal, left, or right).

4) **Multiple Instances/Single Trait:** Usually a single metrics are used to assess a number of characteristics, but here the information is extracted from multiple metrics. for example, one can identify the individual by extracting information from the individual's right and left iris trait, or by taking an impression of the individual's right and left index fingers. Classical systems are cost-effective, because no sensors, methods, or approaches for feature extraction or classification are required

5) **Multiple Biometric Traits:** This biometric system calls for multiple sensors to monitor the physiological and behavioural traits that work together to recognise the person, such as the fingerprints and iris. When the child's inherited traits (e.g., parents' fingerprints and irises) are independent, then performance improves substantially.

6. Current Status Of Biometrics

Despite constant biometric advancements, they have a long way to go. The following five questions have been answered with biometrics, followed by evidence.

Already biometrically authenticated?

The future is right around the corner. Every day across the biometric technologies have gained greater awareness, starting with border control, surveillance, and moving on to mobile devices Many governments, businesses, schools, and private organisations are already using biometrics to combat security threats, financial frauds, and personal identity theft. The U.S. government has, for example, established the Office of Biometric Identity (previously known as 'US-VIS') and various identity documents are being checked upon arrival at the port of entry. The business is doing everything possible to secure its facilities, websites, and online and databases, like HSBC, which offer customers 15 million biometric login credentials, utilises biometrics such as fingerprints and voices as an example. Likewise, the masses are also more and more accepting and open to biometric access methods like fingerprint, face, and iris for mobile phones, vehicles, as well as laptops, cell phones, and for example, and Apple's iPhone 5s and 5s uses of face recognition and Fujitsu's NX-04G cell phone can be automatically unlocked using face recognition and iris. The current type of biometrics are cheap and lightweight, and can be incorporated into any security system easily.

How are biometric technologies being updated?

The fingerprint-based traditional biometrics (such as biometrics requires user involvement, such as face), or high-speed tracking sensors (such as face recognition) (e.g., iris). In spite of this, biometrics and hardware are advancing rapidly. For things related to hardware, novel sensors based on thermal, ultrasound, multispectral, 3D, and mobile mechanisms, these new innovative solutions are available, these innovations offer the possibility of collecting biometric data in difficult conditions. for example, a scanner that reads biometric data from the epidermis is found in commercial products, as well as those that use dermal scanners Specifically, biometrics is improving in regards to the following characteristics: coping with heterogeneous and interoperability, as well as reliability, speed, privacy, and data Continue reading that combination of rapid hardware and software development has created a ‘on-the-the-fly' high-throughput biometric

These biometric systems can monitor and record an individual's movements from long distances Furthermore, new forms of non-traditional authentication systems are in development to differentiate at the individual level.

Are computer better than human for biometric recognition in terms of accuracy?

As is often the case, the case, the answer is unclear. These results stem mainly from modality type, application, ethnicity, and processing conditions, although few tests were done for face recognition, fingerprints, and demographic information, human beings are superior to algorithms under more difficult conditions (e.g., when very small samples are available). However, each year, deep learning algorithms continually achieve or approximate superhuman performance. Many users found they had an easier time with a high degree of recognition as a result of knowing what to expect. It is crucial to incorporating information and human thought processes into biometric systems [26].

A real threat to human health?

No, thanks. Biometrics has been in use for over 30 years, and so far, there have been no documented side effects many evaluation reports, such as ISO/IEC TR14-1:2008, analyse the health risks and benefits of biometrics, such as those found in governments and institutes. Face-to-to-to-face transactions (e.g., shaking hands, hugging) (e.g., touching a doorknob). Also, iris-laser users have long been rumoured to damage eyes; however, this is not because they receive far less near-infrared light than they do on a sunny day. Exciting research and innovation are under way to fight this apprehension; for example, sensors that make use of the invisible spectrum are under development. Commercial biometric systems in general pose no health risks, as they have been certified to meet the various safety and security guidelines (e.g., RoHS, EC).

Are there any biometric standards?

There are various kinds of standards for collecting, analysing, storing, and exchanging biometric data, as general rules.

- Additionally, several international and national standards for biometrics are being developed:
- ISO/IECCEN, ISO/IEC, IEC, ITU-T, and ANSI Non-Industry Components (also known as OASIS, FID, or the Biometric Consortium) (UAF)

- Other organisations, such as the ICAO, ILO SDO, work within their member states' legislative mandates as well as domain-specific requirements and in furthering the products'

The ISO/IEC JTC 1 Subcommittee has produced more than 30 standards to help IT departments on biometric acquisition, security, and other areas such as object identification, evaluation, among all [27].

6. Current Issues and Challenges Of Biometrics

The potential benefits of biometrics are well documented, but there are some issues that remain to be resolved.

What are the key challenges biometrics facing in recent years?

Despite recent advances, biometrics is vulnerable to many vulnerabilities. For biometrics, the biggest concern is the unreliability in the field abnormal show a wide range of disparity in their performance, which could include differences in light intensity, perception, and viewpoint (see Fig. 1e). In terms of total system performance, the cross-scenario compatibility between biometrics, datasets, and sensors is diminishing the likelihood of interoperability

As well, most existing biometric algorithms have severe flaws because they alter texture and appearance of traits after plastic surgery and before detection. The cultural and social influences on biometrics have an impact, too. facial adornments (such as hats or sunglasses) can protect a person's personal data from misuse, since they are irrevocably linked to biometric traits.

Currently, we're seeing a host of problems such as acceptance of digital signatures and personal characteristics as a biometrics An additional problem is that though the biometric standards share several commonalities, some differences remain unaddressed, like patent ambush and competition exist as well.

Is biometric negative identification an issue?

Many biometric systems can be distinguished as either ‘positive' or ‘negative' [1]. The system accepts the biometric trait submitted by the user as positive identification. the system only looks at his/her traits in the master template database. while, no claim is required to be made by the user to have negative identification for the current biometric data in the database, the user's biometric trait is compared against all the other individuals' biometric data. traditional person identification methods (e.g., passwords) have the ability to distinguish between positive and negative subjects to keep someone from having multiple identities (e.g., the passport issuing authority can check that the applicant does not already have a passport under different name). We use the well-known [unestablished]f trademarked designation, “USIT”.

Nevertheless, negative identification has several risks, for example, being used as a biometric trait that links disparate databases without the subject's consent, and engaging in an unmonitored manner can have an adverse effect on civil liberties In most cases, a false match may lead to someone getting thrown in jail or denied access to a police record. One of the benefits of the unified digital biometric system is the potential for placing your entire life history in a single database with the rest of the world. Likewise, inferences such as ethnicity, gender, age, and fingerprints can also serve as a method of discrimination, i.e.e. ethnicity, age, fingerprints, and eyes can be used as proof of ageism [28].

What about the missing data in multibiometric systems?

Multimetric systems provide multiple advantages, and large-scaled systems combine two or more characteristics (e.e. it is increasingly multimodal). There is an increased incidence of missing data in multimodal systems. Users with faces and fingerprints stored in a database may, for example, have lost one or more of their fingers. In addition, only certain aspects of the scene were able to be retrieved. Missing modalities may be in the template, in the query, or in the individuals being found outcome scores. An extended likelihood ratio-based score fusion algorithm (e.g., RLS) can effectively handle at least three categories of missing data without losing any of the evaluation criteria (accuracy).

Can biometrics differentiate identical twins?

The most similar genetic traits will be found in identical twins. The recent advancements have allowed for twins to be reliably distinguished by using their fingerprints, retinal scans, retinoscans, irisograms, and face patterns, for motion-sensitive information. In recent years, scientists have developed a DNA-based genetic test that is used in the courts, as well. To date, monozygotic biometric systems have shown slightly lower success in determining whether or not twins are identical. But multometric systems (e.g., fingerprinting with both fingerprints and eyes) have shown significant improvements in twin verifications [14].

Are there big data issues in biometrics as well?

In a broad sense, big data sense, biometrics could be considered the combination of different biometrics and varied needs, collection and analysis of millions of varied characteristics from millions of biometrics from many sources for diverse applications, including usability, persistence, availability, security, and maintainability. I e.e., UIDAI (the Unique Identification Authority of India) is a biometric identity system that serves all persons in India, identifying a population of 1.25 billion people. Combinations (immutable is going to play a major role), robustness (fake is going to be in a big way), and familiarity (users must become more accustomed to it over time) (multiple biometric identifiers). Big data is at the forefront of finding ways to help meet these issues.

7. Biometric Traits

Strictly speaking, no type of biometric trait exists that has all of the qualities we desire. Additionally, the features of the face do not remain constant throughout life, and likewise the identity of a hard worker cannot be seen via fingerprints. Nevertheless, some traits (e.g. fingerprint, palm, facial, hand, voice, etc.) have achieved at least a partial biometric functionality. Behavioral and physiological characteristics can be found in a biometric measurement.

Physiological based Traits

Amongst other well-known traits, this subsection covers some physiological characteristics. For physical characteristics, these include a face, fingerprints, a palmprint, an iris, and knuckles.

Face: Biometrics is one of the most commonly and easily detected facial characteristics. For instance, still photographs can be obtained from long distance, and extracts can be made from video as well. Typically, face recognition begins with an image capture, and feature extraction. These are placed in the database. In order to obtain the matching score, an appropriate algorithm is used. Faces are the most commonly between body points, such as the eyes, the nose, the mouth. There are several applications where real time is actually being used, including surveillance, identification of criminals, and access control. It's less invasive but is hampered by numerous difficulties like angle, occlusion, expression, and illumination problems.

- Advantages: For the most part, expressions are non-invasive, so face and can be represented using simple sensors. It is no longer controversial
- Challenges: The expression can vary with illumination. For some individuals, facial expressions can completely change the shape of the face. The challenge of ageing is great because facial features do not change in a consistent pattern with the person's age.

Fingerprint: Fingerprints are for personal identification for quite some time now. It's normal for every fingerprint to have some level of uniqueness. We see large quantities of unique and intricate textures, like curlicues, whorls over a fingerprint. Ridges that intersect or separate are referred to as detail features. It is assumed that these are unique and constant features. This type of pattern-recognition algorithms use minutiae coordinates along with the orientation of the co-ordinates. Getting fingerprints isn't that difficult, but getting a high-quality one is hard to do. Poor sensor quality or external factors may be responsible for low fingerprint readings. Workers have notoriously poor fingerprints due to the kind of jobs they hold [29].

- Advantages: Each person's fingerprints are different. Though to be honest, less user effort is required to get and document than the data and can be obtained through cheap sensors.
- Challenges: The most difficult obstacle is to obtain high-quality fingerprints.

Ear: Biometrics contain strong, unique, and discriminating characteristics in the line. In an ear recognition system, the raw image is split into four segments. Features derived from the ear are paired with prerecorded music from the database. The primary disadvantage of the ear is that it can be occluded by any other types of obstruction, including hair or ear jewellery such as earrings, caps, or earphones.

- Advantages: Like to and dislike can be measured noninvasively using sensors similar to this one. Their universal forms don't vary much in the world of mainstream media, the use of the ear is low.
- Challenges: Performance of earphones depends on how well they are handled, as well as their pose, lighting, and translation. Dealing with a large weights and the challenges of external body-occlusion

Iris: Iris has become one of the world's most famous fingerprinted traits. The central region of the ring is bounded by the white of the eye and the black of the iris. There are furrows and crypts in the iris as well. I'm not a particularly good photographer, so it's difficult for me to capture the Iris in the visible light. Therefor this reason, NIR (Infra-Red) light is used to get an iris image. Iris is laid out in strips and arranged into a size consistent shape. There are several Hamming Distance-based Texture features to extract for authentication [30]. Iris-based

recognition systems are highly reliable. In addition, the iris can be mimicked using contact lenses. the main difficulty with iris is user involvement in the process of capture. Iris is highly responsive to stimuli, and extremely difficult to regulate [30].

- Advantages: The iris has a wonderfully sharp and distinguished texture that is naturally protected. They are difficult to alter, and, and processing them is more difficult. You can take photos of irises even if you don't have teeth.
- Challenges: It is hard to produce good iris segmentation in fluctuating illumination. Motion blur and specular reverb and eyelid detail are important too. When being creative, o-angles also pose a significant challenges.

Palmprint: A fingerprint is considered to be a palmprint up to its first joint. There is a great deal of detail, fine lines, knots, and texture in addition to the palmprints. These are thought to be immutable. Several types of features are used to categorise binary content including both statistical and structure, as well as textural. Stability of palm print characteristics has not yet been investigated thoroughly.

- Advantages: Palmprints can be recorded using low-cost touch sensors A great deal of unique and discriminative information was found in the extracted palm printouts.
- Challenges: two of the main creative aspects are variation and handling of illumination and rotation.

Knuckleprint: Generally speaking, the outer portion of the hand is thought of as the knuckle of the finger. Any sensor will do. Drawing rules and structures from them can be established as discriminative rules. Several gabor-based features (e.g. texture and orientation) are employed in the machine learning process.

- Advantages: For all practical purposes, it is practically or naturally well protected and can be purchased using inexpensive sensors. Any differentiating features and differentiating characteristics are included in knprint.
- Challenges: Variable illumination and rotational movements are among the major problems that we face.

Behavioural

Here are some of the behavioural biometrics most popular among software designers:

Gait: Also known as gait, this is one of the behavioural traits. It's interested in detecting a person's ability to use various body characteristics, such as gait, when evaluating them. There are a number of methods to acquire gait data, including moving light displays and video streams. Furthermore, pressure and step patterns can be detected for identification purposes.

- Advantages: Acceptance can be non-intrusively acquired and from afar; thus, its user base is large.
- Challenges: Complex problems arise when there are background, clothing, or the terrain.

Signature: To write something yourself a hand-signed signature is an example of personal verification. Generally, this is used to confirm who a person's bank account or other documents belong to. the X and Y signature co-based features are extracted from any signature To put it another way, "They are combined with the available attributes of the claimed identity." Static features such as angle, break point, curvature, and general parameters are called 'breakpoints' while dynamic features, such as pen-time, are known as 'curves'. Such a system operates in two modes: either on-line or off-line. As a stylus is used to obtain an off-line signature, you get an impression of a handwritten signature with a device, a tablet or stylus is used to obtain a digital signature. It does not apply to everyone, because illiterate people don't know how to sign their names. It is unstable because it fluctuates with time and can be manufactured.

- Advantages: It's socially acceptable.
- Challenges: Signature can vary due to age, from when it was written to where it was written, as well as the fact that it presents a big challenge to computerised signature processing.

Voice: It pays attention to what the speaker says while observing how a person speak sounds. It is widely believed that every person has their own unique texture and cadence that are inextricably linked to their nasal tone, and that has been passed down by inheritance from their parents. Various voice-based features are extracted and incorporated into voice authentication. Features can be copied and replicated. One is not universally correct because it is impossible for the dumb to speak.

- Advantages: The general public believes in it.
- Challenges: People suffer from a range of age, emotions, and other environmental factors that affect the voice.

Table 1 Performance Comparison of different traits

Traits	**Universality**	**Uniqueness**	**Collectability**	**Permanence**
DNA	High	High	Low	High
Ear	Medium	Medium	Medium	High
Face	High	Low	High	Medium
Facial Thermogram	High	High	High	Low
Hand Veins	Medium	High	High	Medium
Fingerprint	Medium	High	High	Medium
Gait	Low	Low	High	Low
Hand Geometry	Medium	Medium	High	Medium
Iris	High	High	Medium	High
Palm Print	Medium	High	Medium	High
Retina	High	High	Low	Medium
Signature	Medium	Low	High	Low
Voice	Medium	Low	Medium	Low

8. Conclusion

Multi-biometric systems are said to have multiple advantages because of the fact that multiple pieces of evidence is provided, with the latter providing a list of advantages offered by uni-biometrics. Depending on the biometric information they can offer substantial improvement in accuracy. They make up for the lack of non-universality and undersupply in their research. It's becoming more difficult for a biometrically unaltered individual to mimic multiple characteristics. Single traits will not be sufficient in most cases, which means that different traits are required to track one individual in real time or on a logarithmic scale. Additionally, they may be described as tolerant of faults and resistant to noise, continuing to operate even when certain biometric sources, for example, fail due to malfunction or user de-imposed tampering.

Similarly, one behavioural biometric (i.e.e. a single-metric biometrics) misses many essential aspects when it comes to modern requirements such as being accurate. To the degree that this holds true with both for humans and with regard to machines, this becomes increasingly apparent, and despite the overwhelming evidence of how accurate this is, no significant effort is made. Non-conventional, unobtrusive biometrics tends to have poor recognition capabilities

By using behavioural multi-biometrics, we aim to mitigate some of the drawbacks of single-biometrics. Furthermore, a gap between conventional approaches and multi-modal methods will be narrowed, allowing personal information to become a central part of future endeavours.

In soft biometrics, soft biometrics function may be seen as an added on to multiple hard biometrics, as a distinct biometric. Multimodal systems must consider the expense of additional sensors and user interfaces, as well as the computational issues. It is also difficult to keep an acquisition process under control when attempting to acquire several characteristics (at the same time). An individual is known for these distinct characteristics as well as well as for these distinguishing marks, surface and texture features, such as the colour of the eyes and skin and hair and dress, for example

References

1. Jain, A.K.; Nandakumar, K.; Ross, A.A. 50 years of biometric research: Accomplishments, challenges and opportunities. Pattern Recognit. Lett. 2016, 79, 80–105.
2. Nandhinipreetha, A.; Radha, N. Multimodal biometric template authentication of finger vein and signature using visual cryptography. In Proceedings of the 2016 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 7–9 January 2016; pp. 1–4.
3. Datta, P.; Bhardwaj, S.; Panda, S.N.; Tanwar, S.; Badotra, S. Survey of Security and Privacy Issues on Biometric System. In Handbook of Computer Networks and Cyber Security; Springer: Berlin/Heidelberg, Germany, 2020; pp. 763–776.
4. Nagar, A.; Nandakumar, K.; Jain, A.K. Multibiometric cryptosystems based on feature-level fusion. IEEE Trans. Inf. Forensics Secur. 2012, 7, 255–268.
5. Ross, A.A.; Nandakumar, K.; Jain, A.K. Handbook of Multibiometrics; Springer: Berlin/Heidelberg, Germany, 2006.
6. Howell, K. IPSwitch. Available online: https://blog.ipswitch.com/3-reasons-biometrics-are-not-secure.

7. Kondapi, L.; Rattani, A.; Derakhshani, R. Cross-illumination Evaluation of Hand Crafted and Deep Features for Fusion of Selfie Face and Ocular Biometrics. In Proceedings of the 2019 IEEE International Symposium on Technologies for Homeland Security (HST), Boston, MA, USA, 5–6 November 2019; pp. 1–4.
8. Xin, Y.; Kong, L.; Liu, Z.; Wang, C.; Zhu, H.; Gao, M.; Zhao, C.; Xu, X. Multimodal Feature-Level Fusion for Biometrics Identification System on IoMT Platform. IEEE Access 2018, 6, 21418–21426.
9. Sandhu, N.K.; Patterh, M.S. A Biometric Fusion Based on Face and Fingerprint Recognition using ANN. Int. J. Recent Innov. Trends Comput. Commun. 2017, 5, 88–92.
10. Dinca, L.M.; Hancke, G.P. Fall of One, the Rise of Many: A Survey on Multi-Biometric Fusion Methods. IEEE Access 2017, 5, 6247–6289.
11. Scott, I. CPO Magazine, Breach of Biometrics Database Exposes 28 Million Records Containing Fingerprint and Facial Recognition Data. Available online: https://www.cpomagazine.com/cyber-security/breach-of-biometrics-database-exposes-28-millionrecords-containing-fingerprint-and-facial-recognition-data/ (accessed on 26 December 2019).
12. Ahmad, M.I.;Wai, L.W.; Satnam, S.D. Multimodal biometric fusion at feature level: Face and palmprint. In Proceedings of the CSNDSP, Newcastle Upon Tyne, UK, 21–23 July 2010; pp. 801–805.
13. Chanukya, P.S.; Thivakaran, T.K. Multimodal biometric cryptosystem for human authentication using fingerprint and ear. Multimed. Tools Appl. 2020, 79, 659–673.
14. Thepade, S.D.; Bhondave, R.K.; Mishra, A. Comparing Score Level and Feature Level Fusion in Multimodal Biometric Identification Using Iris and Palmprint Traits with Fractional Transformed Energy Content. In Proceedings of the 2015 International Conference on Computational Intelligence and Communication Networks (CICN), Jabalpur, India, 12–14 December 2015; pp. 306–311.
15. Guesmi, H.; Trichili, H.; Alimi, A.M.; Solaiman, B. Novel biometric features fusion method based on possibility theory. In Proceedings of the 2015 IEEE 14th International Conference on Cognitive Informatics & Cognitive Computing (ICCI* CC), Beijing, China, 6–8 July 2015; pp. 418–425.
16. Xing, X.; Wang, K.; Lv, Z. Fusion of gait and facial features using coupled projections for people identification at a distance. IEEE Signal Process. Lett. 2015, 22, 2349–2353.
17. Oveisi, I.S.; Modarresi, M. A feature level multimodal approach for palmprint and knuckleprint recognition using AdaBoost classifier. In Proceedings of the 2015 International Conference andWorkshop on Computing and Communication (IEMCON), Vancouver, BC, Canada, 15–17 October 2015; pp. 1–7.
18. Haghighat, M.; Abdel-Mottaleb, M.; Alhalabi, W. Discriminant correlation analysis: Real-time feature level fusion for multimodal biometric recognition. IEEE Trans. Inf. Forensics Secur. 2016, 11, 1984–1996.
19. Jagadiswary, D.; Saraswady, D. Biometric authentication using fused multimodal biometric. Procedia Comput. Sci. 2016, 85, 109–116.
20. Azom, V.; Adewumi, A.; Tapamo, J.R. Face and Iris biometrics person identification using hybrid fusion at feature and scorelevel. In Proceedings of the 2015 Pattern Recognition Association of South Africa and Robotics and Mechatronics International Conference (PRASA-RobMech), Port Elizabeth, South Africa, 26–27 November 2015; pp. 207–212.
21. Toygar, Ö.; Alqaralleh, E.; Afaneh, A. Symmetric ear and profile face fusion for identical twins and non-twins recognition. Signal Image Video Process. 2018, 12, 1157–1164.
22. Sharifi, O.; Eskandari, M. Optimal face-iris multimodal fusion scheme. Symmetry 2016, 8, 48.
23. Meena, K.; Malarvizhi, N. An Efficient Human Identification through MultiModal Biometric System. Braz. Arch. Biol. Technol. 2016, 59.
24. Minaee, S.; Abdolrashidi, A.; Su, H.; Bennamoun, M.; Zhang, D. Biometric recognition using deep learning: A survey. arXiv 2019, arXiv:1912.00271.
25. Talreja, V.; Valenti, M.C.; Nasrabadi, N.M. Multibiometric secure system based on deep learning. In Proceedings of the 2017 IEEE Global Conference on Signal and Information Processing (globalSIP), Montreal, QC, Canada, 14–16 November 2017; pp. 298–302.
26. Al-Waisy, A.S.; Qahwaji, R.; Ipson, S.; Al-Fahdawi, S.; Nagem, T.A. A multi-biometric iris recognition system based on a deep learning approach. Pattern Anal. Appl. 2018, 21, 783–802.
27. Zhang, Q.; Li, H.; Sun, Z.; Tan, T. Deep feature fusion for iris and periocular biometrics on mobile devices. IEEE Trans. Inf. Forensics Secur. 2018, 13, 2897–2912. [CrossRef]

28. Umer, S.; Sardar, A.; Dhara, B.C.; Rout, R.K.; Pandey, H.M. Person identification using fusion of iris and periocular deep features. Neural Netw. 2020, 122, 407–419.
29. Surendra, I.; Sashank, T.S.; Praveena, M.A.; Manoj, R.J. Deep feature fusion for IRIS based on industrial biometric engineering. In Proceedings of the AIP Conference, Bangalore, India, 17–18 January 2020; p. 040003.
30. Sharma, Ajay & ojha, Deo. (2011). A Multi-Biometric Template Security: An Application of Code-Based Cryptosystem. International Journal of the Computer, the Internet and Management Vol. 19. No.1 (January-April, 2011) pp 14 -24.
31. Jomaa, M.R.; Mathkour, H.; Bazi, Y.; Islam, M.S. End-to-End Deep Learning Fusion of Fingerprint and Electrocardiogram Signals for Presentation Attack Detection. Sensors 2020, 20, 2085.
32. Tiong, L.C.O.; Kim, S.T.; Ro, Y.M. Implementation of multimodal biometric recognition via multi-feature deep learning networks and feature fusion. Multimed. Tools Appl. 2019, 78, 22743–22772.
33. Leghari, M.; Memon, S.; Chandio, A.A. Feature-level fusion of fingerprint and online signature for multimodal biometrics. In Proceedings of the 2018 International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), Sukkur, Pakistan, 3–4 March 2018; pp. 1–4.
34. Imran, M.; Kumar, H.; Jabeen, N.S.; Alaei, F. Accurate person recognition on combining signature and Fingerprint. Int. J. Mach. Intell. 2011, 3, 277–281.
35. El-Alfy, E.S.M.; BinMakhashen, G.M. Improved personal identification using face and hand geometry fusion and support vector machines. In Proceedings of the International Conference on Networked Digital Technologies, Dubai, United Arab Emirates, 24–26 April 2012; Volume 294, pp. 253–261.
36. Gawande, U.; Zaveri, M.; Kapur, A. A novel algorithm for feature level fusion using SVM classifier for multibiometrics-based person identification. Appl. Comput. Intell. Soft Comput. 2013, 2013, 515918.
37. Rane, M.E.; Deshpande, P.P. Multimodal Biometric Recognition System Using Feature Level Fusion. In Proceedings of the 2018 IEEE Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), Pune, India, 16–18 August 2018; pp. 1–5.
38. Zhang, X.; Dai, Y.; Xu, X. Android-Based multimodal biometric identification system using feature level fusion. In Proceedings of the 2017 IEEE International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS), Xiamen, China, 6–9 November 2017; pp. 120–124.
39. Zhong, D.; Shao, H.; Du, X. A Hand-Based Multi-Biometric via Deep Hashing Network and Biometric Graph Matching. IEEE Trans. Inf. Forensics Secur. 2019, 14, 3140–3150.
40. Huang, Y.; Xu, D.; Nie, F. Patch distribution compatible semisupervised dimension reduction for face and human gait recognition. IEEE Trans. Circuits Syst. Video Technol. 2012, 22, 479488..