EasyChair Preprint

№ 9150

Security Issues in Biometric Systems

Anupriya Jain, Poonam Mishra and Mohit Sachdeva

October 26, 2022

Security Issues in Biometric System

Based on Pattern Recognition System

Dr. Anupriya Jain
Poonam Mishra
Mohit Sachdeva

Masters of Computer Applications
Manav Rachna International Institute of Research and Studies
India
4 September 2022

Abstract
Biometrics is a recent discussion in computer science that is defined as the study of creating computer models. It's significant in forensics, secure access, and government and commercial applications (such as international border crossing, making government identity proofs, etc). It is a branch of computer science that investigates a person's correct identification. It's a pattern recognition system that uses machine learning algorithms to process data from fingerprinting, iris scanning, retina scanning, hand geometry, face recognition, voice recognition, and odor biometrics, among other methods. These provide verified information to protect your identity, which is often adequate for your IDs. Uni modal and multi-modal biometrics are the two methodologies used in biometrics. Noise, spoofing, lower accuracy, and other issues might occur when uni-modal is used. Another option is multi-modal biometrics, which solves the problem of uni-modal biometrics by providing anti-spoofing techniques that make it harder for an attacker to infiltrate the security system. [8]The have a look at's predominant aim is to realize the position of deep learning in the authentication system in addition to its use within the enhancement of biometric device protection. We describe those methods and look at the constraints that hold to restrict biometric technology' full ability. The most critical are: developing robust authentication methods, assuring the security of enrolled templates, and protecting structures from various assaults.[4] In this have a look at, we observe the performance of several research in overcoming the aforementioned issues, as well as potential upgrades and destiny techniques on this field.
Keywords: Biometric, authentication, identification, Feature extraction

1 Introduction

Building access, computer systems, mobile phones, forensics, and other applications all demand dependable security measures. Biometrics in the past included a different technique of identifying a person that relied on distinguishing elements of the body such as physical features, scars, and other criteria such as height, eye, color, and complexion. Biometrics is an automated way of identifying and authenticating people. Faced with numerous security concerns such as document fraud and terrorism, cybernetics leads to the implementation of biometrics.[13] It is rapidly expanding, notably in document identification. It integrates with numerous security technologies such as smart ID cards and chips (electronic Passport and ATMs). Historically, a lack of a strong security mechanism led to a variety of frauds. Within the Master Card system. For example, the master card system costs the industry millions of dollars each year due to a lack of verification mechanisms. Biometrics is an automated method of identifying a person using two types of identifiers: physiological and behavioral. Physiological assessments are frequently biological or morphological. Fingerprints, hand shapes, iris scans, and vein patterns are morphological identifiers, whereas DNA, blood saliva, urine, and forensics are biological identifiers. Keystroke dynamics, speech recognition, and signature dynamics are examples of behavioral

measurements.[15],[17] Recent world events have generated a spike in interest in biometric security solutions. Biometric identification systems are utilized in a variety of fields, including law enforcement and public security, military intelligence, border control, health care, civic identity, and many more. A biometric system is frequently used as an identifying or verification method. Identification system: Biometrics is a technique for determining a person's identity without his knowledge or consent. The goal is to capture a person's data and compare it to a database that has already been recorded. In a crowd, for instance, consider facial recognition. The identification of a person is verified via a verification mechanism. The similarity of a person's data is determined by comparing it to that of another person. For example, finger scans can be used to access a laptop.[19],[9] In spite of identical twins, the opportunity of finding two comparable fingerprints is one in sixty-four billion, according to Sir Francis Galton's (Darwin's cousin) calculations (homo zygotes). Biometrics is intently tied to an individual's identity in this situation. Any place you pass, a biometric system is good.[2],[12]

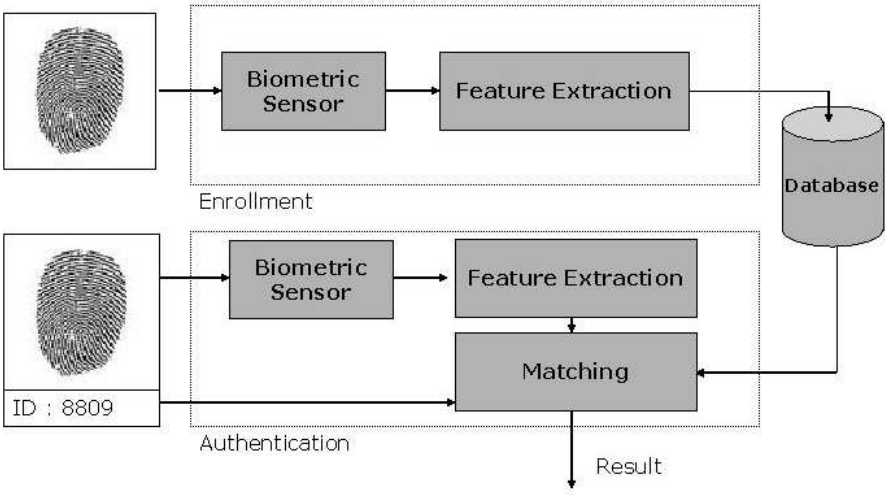

Figure 1 :A General Biometric System

Enrolment, live samples, and comparison are the steps involved in the biometric system. Four key components make up a simple biometric system: (a) An individual's data is collected by a sensor module. The fingerprint sensor, for example, can scan your fingerprints. (b)The characteristic extraction module takes the received statistics and extracts the features. Function extraction, for instance, is the system of figuring out the location and orientation of the fingerprint's microscopic factors. (c)The Matching Module compares function values to templates contained in the database. As an example, the wide variety of minuscule factors and the template are compared, and an identical rating level is decided. (d)An identical rating stage becomes supported inside the decision-making module at some stage in which the consumer's identity turned

into asserted or rejected.

Segment 2 goes via the biometric authentication process. Section three outlines the primary difficulties and possibilities holes that may be filled in biometric research. Section four discusses deep getting-to-know techniques with the intention to assist researchers in building robust strategies. Section 5 discusses the significance of deep mastering in enhancing the safety of biometric structures in the diffusion of contexts. Segment 6 brings the paper to be concluded.

1.1 Biometric measures

The words biometric are derived from the words bio, which means "life," and metrics, which means "measurements." However, this phrase is associated with a person's identification and verification. Other biometric measures are being examined for machine learning approaches.
(a) Individuality: Everyone has a distinct personality that can be harmed by an accident or disease.
(b) Measurability: Data attributes are easily obtained.
(c) Reducibility: The collected data is easily reduced and handled.
(d) Universality: This has the potential to discriminate against people. Some data capture methods are inseparable and cannot be simply learned. While some of the data is non-linear, the kernel approach is applied in this scenario, which employs the K – separability requirement.
(e) Property Invariance: It should remain constant across time.
(f) Singularity: Each statement is unique. Height, weight, and color are all unique assuming the most correct measurements but do not provide enough points of separation to be helpful for more than categorization. Individual confidentiality is guaranteed.
(g) Unrepeatable: The characters must be unreplicable. The less irreproducible it is, the more dependable it is.
(h)Cost-effectiveness: The entire process is cost-effective.
(i) Circumventable: the system's ability to identify attacks. This attribute serves as the machine's robustness for the learning algorithm. It can deal with intrinsic irregularities.
Fingerprint, face traits, hand geometry, voice, iris, retina, vein pattern, palm print, DNA, keystroke dynamics, ear shape, odor, and signature dynamics are examples of biometric technologies.

Table 1: Characteristics Of Biometric System
,[2]

Characteristics	**Fingerprints**	**Hand geometry**	**Retina**	**Iris**	**Face**	**Voice**
Ease of use	High	High	Low	Medium	Medium	High
Accuracy	High	High	Very high	High	High	High
User acceptance	Medium	Medium	Medium	Medium	High	High
Long term stability	High	Medium	High	Medium	Medium	Medium

Biometrics is divided into two modules: database preparation and training. The verification module is separated further into a matching module and a decision module.

1.2 Biometric Technology

(a) Fingerprint
(b) Facial features
(c) Hand geometry
(d) Voice recognition
(e) Iris, Retina Scan
(f) Vein Pattern
(g) Palm Print
(h)DNA, keystroke dynamics, ear shape, odor, signature dynamics.

The primary biometrics stage includes:

[12] (a) Fingerprint(optical, silicon, ultrasound, touchless), Facial Recognition (optical and thermal)
(b)Voice Recognition (not to be confused with speech), signature scan, iris scan, retina scan, and keystroke scan.

Exploratory levels consist of DNA, Ear shape, scent (human heady scent), Vein scan (in the back of the hand or beneath the palm), finger geometry (shape and structure of hands, and Gait popularity(way of on foot).[8],[11],[5]

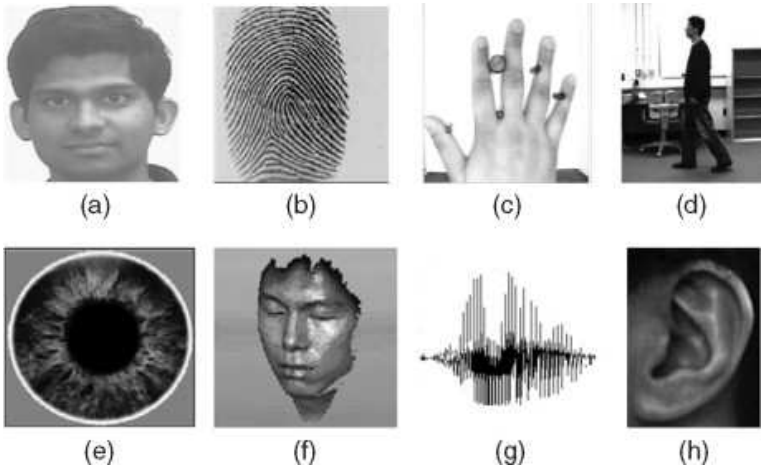

Figure 2 :Types of Biometric System
(a) Facial Recognition (b) Fingerprint (c) Hand geometry (d) Gait
(e)Iris scan (f) face thermogram (g) Voice recognition (h) Ear scan

(a) Fingerprinting recognition: A fingerprinting recognition refers to follow-

ing the pattern of ridges and furrows of a finger. Traditionally it had been done by inked finger but today in digital worlds it is done by digital machines to recognize the pattern of a finger. In real-time, this verification is acquired by feature extraction which corresponds to features and orientation called miniature points. [15],[19]
(b) Voice recognition: In this, the sensation of a person is measured and compared to the template.
(c) Signature recognition: It is used to process and identify the signature, dynamic signature, handwriting, speed, stroke, shape, and pen pressure to identify the identity of a client.
(d) Palm recognition: 3- A d image of a palm is identified[11] and the bulk of data is used but it has been done in a shorter period.
(e) Hand geometry scan: It has a 3-D image of the palm as well as finger feature extraction and compared it with datasets.[4] It takes 2 – 3 seconds to identify.
(f) Retina scan: It is based on the blood vessel pattern of the retina, it technology is older but this is recognition based on the eye. The retina is not properly visible so, infrared rays illuminate of eyes to identify the pattern.[18],[20] The retina scan is more susceptible to diseases that are also rare.
(g) Face recognition: This face reputation sample recognizes the 2-D photograph of the person matching[15] and matches it with the template. That is a pretty hard method because of human coloration, texture, expression, pose, and so on. The problem in addition is compounded by the presence of backgrounds and variable light conditions. A variety of strategies is used to perceive a person through face recognition. In this technique set of orthonormal vectors that span a lower computational subspace is the primary element analysis approach[2],[9] Matching of pix computing the Euclidean eigenvalues between the original face and detected picture[14].

2 The framework of the Recognition System

A biometric device contains phases: registration (or enrolment) and recognition[1]. The preliminary section is characteristic extraction and pre-processing. These functions are saved within the database as templates. Feature extraction is accompanied by way of choice-making by way of matching the identity with the saved templates in the course of verification in addition to identification (i.E. Authentication). The performance of a biometric machine can be assessed through the use of a long way (false take delivery of rate) or a long way (fake rejection charge)[1],[6].FAR (false be given price)[15] or FRR (fake reject rate)[15] at various tiers can be used to evaluate the performance of a biometric gadget. All biometrics have the symptoms of mistaken acceptance or rejection. If the system fails to recognize biometric data using a template provided in the database in the first condition. This is a phony rejection. If the machine identifies that the biometric data is different from the template data in the second example. It's a deceptive acceptance. A threshold is used to regulate the system.In the course of the matching of identities as an instance, if sample pairings have bet-

ter scores than t[1], it denotes that they're related people. They might in any other case belong to unique humans. The choice of a human trait for such systems is decided by means of the degree to which the conditions of strong point, area of expertise, permanence, person approval, and so on are fulfilled. Nowadays, the 3 most usually applied identity capabilities are fingerprint[19], face recognition[2], and iris[18]. While governments and agents have collected many facial and fingerprint datasets, the iris is an increasing number of being employed for big-scale authentication[7] when you consider that it is able to help achieve high accuracy in such structures.

3 Challenges and Research gap

(i) Identifying the appropriate representation method for a specific characteristic. The feature extractor should be able to reduce intra-subject variances.
(ii) Another significant problem in biometric systems is the development of robust algorithms for feature extraction. The properties of various attributes should be used to select matching algorithms.
(iii). Using a mask or a fake finger, hand, or signature to provide a fraudulent or counterfeit entry to the sensor (signature copy).
(iv) Transmission of signals stored from the first message, such as early voice or fingerprint registration. Changing the stored templates can allow the attacker to attack and update the database, especially if the database is dispersed across multiple servers.
On this paper, we study some of these troubles and the position of deep studying in addressing them. Those consist of detecting spoofing attempts and figuring out features in unconstrained environments[1]. We spotlight the prevalence of deep getting to know algorithms over today's methods, as well as potential future guidelines that researchers can also locate valuable.

4 Deep learning in Biometric

4.1 Deep Learning Architecture

4.1.1 Convolution Neural Network(CNN)

A Convolutional Neural network, or CNN, is a form of synthetic neural network used for picture/item popularity and classification in Deep mastering[3]. Pooling layers and completely connected layers come after convolutional layers. To construct a characteristic map for the next layer, the enter photograph matrix is convoluted with a filter matrix in convolution. CNNs are the area-invariant ways of using kernels, which prevents overfitting. And a final layer of paperwork is a nonlinear activation feature. The use of a CNN, Deep getting to know recognizes entities in an image. CNN's are used for a diffusion of obligations and purposes, along with photo processing, pc imaginative and prescient tasks which include

localization and segmentation, video evaluation, spotting obstacles in self-using motors, and natural language processing[2],[1].

4.1.2 Multilayer Perceptrons(MLPs)

MLPs are feedforward neural networks with many layers of perceptrons with activation features that belong to the class of feedforward neural networks. A multi-layer perceptron has one enter layer with one neuron (or node) for each input, one output layer with a single node for every output, and any quantity of hidden layers with nodes for every hidden layer[17]. A sigmoid activation function is used by each node in the multi-layer perception.[1] (x) = 1 /(1 + exp (-x)) Using the sigmoid formula, the sigmoid activation function translates real values to numbers between 0 and 1.

4.1.3 Long Short Term Memory Network LSTM

LSTM is a breakthrough within the improvement of recurrent neural networks, which are used to learn input sequences.[1]It's used to learn sequential data and outperforms RNNs, which have a vanishing gradient problem. Gates are employed in LSTM to pick which information to keep and which to dismiss[10]. These gates function similarly to neural networks.

5 Deep Learning to Enhance Security System

A biometric system can be secured towards diverse listed vulnerabilities with the help of deep gaining knowledge of Strategies.

5.1 Template Protection using Deep learning

The principle motive for implementing biometric systems is to prevent illegal access. It is possible, but, that the biometric templates are not relaxed. This could bring about a spread of protection issues, together with a denial of provider assault and a lack of consumer privacy[6].Protecting the templates in the database[8] is a key step in making biometric systems secure. These templates are features taken from an individual's biometric trait and saved as records.A Biometric Template Database Vulnerabilities. Customers of biometric packages have expressed issues about the vulnerability assaults at the biometric template within the database.Because of a person's privacy, public liberty violations, and trustworthiness, this is the case. The deliberate manipulation of an enrolled template by an impostor's pattern or biometric operator, for example, has hindered users' trustworthiness and anxiety in the technology[14]. One of the most challenging things in a biometric system is creating non-invertible and non-linkable templates while maintaining authentication accuracy. In the scenario that a biometric template is revoked, the original template should be recoverable[2] Furthermore, the biometric system's performance should not be compromised. When it comes to preventing any form of association between

the protected templates, robust frameworks are required.Several templates is every other great assignment for template protection in biometric systems that integrate records from or greater attributes[20].
Approach The measures that use a deep mastering algorithm to shield templates in a database. To comfortable the biometric facts template, a completely unique encryption-decryption technique based totally on the model View Template (MVT) design sample is developed[8]. The version organizes information logically, the view depicts information graphically, and the template offers with records migration into sample gadgets. The set up algorithm is primarily based on the Fernet key example's cryptography module[1]. To create two encrypted files (byte and text file), the Fernet keys are merged to create a multiFernet key[14]. These files are attached to Twilio messages[2] and stored safely in the database. Whilst an attacker attempts to access the database's biometric records template, the device notifies the consumer. Whilst an attacker attempts to access the biometric records template within the database, the gadget notifies the user and stops the attacker from gaining illegal get admission to, in addition to go-verifying the impostor based on the ownership validation. As a end result, it informs users and authorities approximately how comfortable an man or woman biometric information template is, and offers a high stage of protection for personal facts privateness[17].

5.2 Spoofing

If a false trait is supplied to the biometric system's sensor, spoofing attacks can occur. It is simple for these characteristics to be harmed. An invader who uses this stolen feature to get around the security system sensor. As a result, the algorithm will be unable to distinguish between genuine and fake traits[10]. With the help of some, An intruder can successfully hack a biometric system if they have prior knowledge of the input. This compromises an individual's security and privacy. Thus, One of the most difficult issues in building a biometric system is detecting spoofing attempts. When various materials are utilized during training and testing, the effectiveness of spoofing detection algorithms can suffer, according to the authors[2]. As a result, universal countermeasures must be developed that are unaffected by the substance used to construct the spoofs. Human elements such as pressure, humidity, and temperature, among others, can have an impact on the deep learning framework's performance. As a result, detecting spoofing attacks is one of the most difficult tasks when creating a biometric system.
Approach The countermeasure is liveness detection.Any technique for detecting a spoof strive via evaluating whether or not the source of a biometric sample is a dwelling person or a phony representation is referred to as liveness detection[14]. That is done the use of algorithms that have a look at information received from biometric sensors to identify if the supply is actual or faux. There are two types of liveness detection system atre occurs. Active: Invokes the user to take any action that is difficult to imitate with a spoof. Multiple

modalities, such as keystroke analysis or speaker recognition, could be used. The latter can use the movement of a mouth to assess whether or not it is alive. Passive: Without requiring human engagement, algorithms are used to detect indicators of a non-live image. The capture of high-quality biometric data during enrolment increases matching and liveness performance. An example of Antispoofing in a face recognition system For mobile authentication, facial recognition is an excellent biometric option. It's simple to use and adaptable to a wide range of mobile devices, with camera integration in many commercial devices. It utilizes a well-known "selfie" stance. Facial biometrics, on the other hand, are more vulnerable to spoofing due to the extensive availability of digitized facial photos via social media. As a result, robust liveness detection is crucial for mobile biometric authentication solutions that use facial recognition. The liveness detecting function is utilized in facial popularity to distinguish among a stay picture and a 2nd printed, three-D published, or virtual representation of a user's face[14].A 3D mask could be used in other spoof attempts. Spoofing attempts can be detected using algorithms that distinguish non-live sample artifacts, as well as "active" methods like a second modality (e.g. keystroke analysis or voice)[15]. Spoofing and other presentation attacks are substantially less effective when using liveness detection methods.

5.3 Surveillance in Unconstrained Environment

A few technologies may vicinity regulations on how a trait is obtained. Lifting latent fingerprints[19] from against the law scene, an instance, or iris sensors that require the iris to be near until the method is completed. If iris patterns can be gathered from a distance with the aid of iris sensors whilst the challenge is transferring, user popularity of the iris identity era can be appreciably multiplied[7]. However, due to excessive intra-elegance variances, it may not be very dependable. As an end result, this manner necessitates the usage of sturdy algorithms. Face recognition in surveillance applications[6] is hard to trouble to remedy on the grounds that pics acquired can be of low great. This could be because of the digital camera's low decision, the outstanding distance between the camera and the person, as well as lighting and occlusion troubles. Due to the fact the individual isn't always being captured, there may be versions in function and expression. It could be sporting add-ons, hats, or glasses. A topic may also attempt to cover. Moreover, in video surveillance, a series of face pix are in comparison to a gallery of nevertheless pics. In popular, it's miles not possible to predict which order of photos in a video collection could yield a nice outcome.As a result, authenticating faces from video adds another layer of complexity.Many CNN models attain near-perfect accuracy on popular benchmarks like Labeled Faces in the Wild (LFW), MegaFace, and YouTubeFace (YTF)[2]. These models, however, cannot guarantee the same performance in an actual setting. an uncontrollable environment Facial recognition is still a significant difficulty when it is in an unconstrained scenario or without the subject's cooperation.

Approach Our stepped-forward facial recognition system's deployment may be

divided into two principal obligations: data augmentation and CNN training[16]. These two principal jobs can be similarly segmented as follows. Enhancing photos in the education set to simulate the effects of various lighting settings on the advent of the face in the photo is how records augmentation is done. This simulation desires first to deduce a 3-D reconstruction of the face from the photo, observed with the aid of applying a light version to the 3D reconstruction to execute pixel-through-pixel adjustment of the obvious brightness of the photo pixel[6]. CNN training incorporates deploying training units to train the CNN to properly pick out one in all a limited variety of faces when given a facial image.

Figure 3 :Photometric Transformation

Information augmentation procedures the trouble of lighting fixtures fluctuation from a brand new perspective. Statistics augmentation, in preference to changing the authentic photograph before attempting recognition, makes use of the unmodified picture however complements the variant inside the schooling set. This makes system training greater rigorous, and the skilled network can address lighting variances better. These days, facts augmentation techniques for lights repayment had been evolved which can be based on 3-D reconstructions, taking into account a more particular estimation of the influences of illumination alternate. Face popularity (and, greater extensively, object type) may be divided into two steps: function extraction and class. The two responsibilities can be finished independently: making use of transfer learning, a pre-educated feature extractor may be utilized for class, in conjunction with an MLP or every other classifier.

6 Information fusion In Biometrics

Fusion means the combining of two or more traits together to enhance the security which is also called a multi-modal biometric system[16]. In the last several years, both the government and the corporate sector have been doing research into the application of multimodal biometric systems[8].Unimodal biometric structures have obstacles, which multimodal biometric structures help to overcome. This is performed by using combining rankings from many traits. As a end result, these systems boom reputation performance even as also presenting various other advantages to individual security and privateness[16],[13]. Fusion can occur at three levels:
(a) at the feature extraction level,
(b) at the matching score level,

(c) at the decision level.

(1)Fusion at the feature extraction level: Every sensor's facts is used to generate a feature vector. Due to the fact the capabilities taken from one biometric trait are awesome from the ones extracted from the alternative, concatenating the 2 vectors into a single new vector makes feel. The brand new characteristic vector is extra dimensional and expresses someone's identification in a one of a kind (optimistically greater discriminating) hyperspace. To extract usable traits from a bigger set of capabilities, feature reduction strategies can be used.

(2) Fusion at the level of the matching score:Every gadget affords an identical rating that indicates how near the characteristic vector is to the template vector. These rankings can be delivered together to affirm the stated identification. Strategies like to aggregate the rankings furnished through the 2 sensors, techniques which includes logistic regression can be applied.

(3) Fusion at the decision level: These strategies are looking for to lessen the FRR for a given a ways. Every sensor can gather several biometric information factors, and the resulting characteristic vectors may be looked after into certainly one of classes—receive or reject. To make the ultimate preference, a majority balloting approach, which includes that used in, can be used.

Although they contribute to achieving higher accuracy than traditional biometric systems, several gaps and issues need to be addressed. To begin with, many multimodal biometric systems studies combine two or more features from various unimodal databases. However, in actual-global packages, this doesn't preserve due to the fact capabilities from a unmarried person need to be connected. Second, most of those systems are inflexible, as accuracy suffers if one of the biometric functions is missing or unavailable. 1/3, it could bring about a high false attractiveness fee (some distance) and fake rejection price (FRR), as well as restricted discrimination skills, a overall performance upper bound, and a lack of permanence. As a result, these shortcomings need to be corrected.

7 Conclusion and Future Work

We have demonstrated how deep learning can be used to authenticate various features in biometric systems in this work. While biometric systems are primarily concerned with authentication, they also face several vulnerabilities, including attacks against enrolled templates and assaults utilizing forged identities. The research investigates the use of robust deep learning frameworks to address these issues, taking a variety of ways to solve the problems. In the future, we would concentrate on many aspects of the study that are still in their inception.
Our long-term goal is to work on large datasets with millions of features, which will necessitate complicated models such as GPT-3, which has roughly 175B

parameters and is trained on 45TB of data from multiple datasets. Every other option for making biometric structures more secure is to appoint blockchain, the technology that underpins cryptocurrencies like Bitcoin. You may shop consumer records in a disbursed ledger included via encryption on numerous computer systems all over the world the use of blockchain era. Because of this handiest legal parties have get entry to to the facts (or data blocks), and any try to alternate the information may be observed with the aid of some other blockchain consumer. It is also possible to establish private dispensed ledgers which might be simplest on hand to a restricted wide variety of customers.

References

[1] Shefali Arora and MPS Bhatia. Challenges and opportunities in biometric security: A survey. *Information Security Journal: A Global Perspective*, 31(1):28–48, 2022.

[2] Renu Bhatia et al. Biometrics and face recognition techniques. *International Journal of Advanced Research in Computer Science and Software Engineering*, 3(5):93–99, 2013.

[3] Ioannis G Damousis and Savvas Argyropoulos. Four machine learning algorithms for biometrics fusion: A comparative study. *Applied Computational Intelligence and Soft Computing*, 2012, 2012.

[4] Zoran Duric, Roman Goldenberg, Ehud Rivlin, and Azriel Rosenfeld. Estimating relative vehicle motions in tra c scenes. Technical report, Citeseer, 1998.

[5] Zoran Duric, Harry Wechsler, and James Yven. Adaptive and smart interface for vcr remote control using hand gestures. In *2002 International Conference on Pattern Recognition*, volume 3, pages 1035–1038. IEEE, 2002.

[6] Uday Bhanu Ghosh, Rohan Sharma, and Abhishek Kesharwani. Symptoms-based biometric pattern detection and recognition. In *Augmented Intelligence in Healthcare: A Pragmatic and Integrated Analysis*, pages 371–399. Springer, 2022.

[7] Ric Heishman, Zoran Duric, and Harry Wechsler. Using eye region biometrics to reveal affective and cognitive states. In *2004 Conference on Computer Vision and Pattern Recognition Workshop*, pages 69–69. IEEE, 2004.

[8] Nabil Hezil and Abdelhani Boukrouche. Multimodal biometric recognition using human ear and palmprint. *IET Biometrics*, 6(5):351–359, 2017.

[9] Anil K Jain. Biometrics: Proving ground for image and pattern recognition. In *Fourth International Conference on Image and Graphics (ICIG 2007)*, pages 3–3. IEEE, 2007.

[10] Martin Mihajlov, Borka Jerman-Blazič, and Saso Josimovski. A conceptual framework for evaluating usable security in authentication mechanisms-usability perspectives. In *2011 5th international conference on network and system security*, pages 332–336. IEEE, 2011.

[11] Midhuna Naveen, Pritty Mary Mathew, KJ Neethumol, and Sherin Joseph. Machine learning algorithms based palmprint biometric identification.

[12] Nicolas Ortiz, Ruben Dario Hernández, Robinson Jimenez, Mauricio Mauledeoux, and Oscar Avilés. Survey of biometric pattern recognition via machine learning techniques. *Contemporary Engineering Sciences*, 11(34):1677–1694, 2018.

[13] Ramaswamy Palaniappan and Danilo P Mandic. Biometrics from brain electrical activity: A machine learning approach. *IEEE transactions on pattern analysis and machine intelligence*, 29(4):738–742, 2007.

[14] Sonali D Patil, Roshani Raut, Rutvij H Jhaveri, Tariq Ahamed Ahanger, Pallavi V Dhade, Atul B Kathole, and Kapil N Vhatkar. Robust authentication system with privacy preservation of biometrics. *Security and Communication Networks*, 2022, 2022.

[15] Salil Prabhakar, Josef Kittler, Davide Maltoni, Lawrence O'Gorman, and Tieniu Tan. Introduction to the special issue on biometrics: Progress and directions. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(4):513–516, 2007.

[16] Arun A Ross, Anil K Jain, and Karthik Nandakumar. Information fusion in biometrics. *Handbook of Multibiometrics*, pages 37–58, 2006.

[17] Vikash Kumar Singh, Devendra Singh Kushwaha, and Roshni Tiwari. Study of biometric authentication systems and their security.

[18] S Sirohey, Azriel Rosenfeld, and Zoran Duric. A method of detecting and tracking irises and eyelids in video. *Pattern recognition*, 35(6):1389–1401, 2002.

[19] Aayushi Tamrakar and Neetesh Gupta. A study on machine learning approach for fingerprint recognition system.

[20] Harry Wechsler, Zoran Duric, and Fayin Li. Hierarchical interpretation of human activities using competitive learning. In *2002 International Conference on Pattern Recognition*, volume 2, pages 338–341. IEEE, 2002.