JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

INNOVATIONS IN RESEARCH DATASETS: SHAPING THE FUTURE OF BIOMETRIC AND FORENSIC TECHNOLOGY

***Manojnya Arasada*[1], *Thiruvaipaty Susrith Nath*[2], *Gowtham Penumarthi*[3],**

UG II Year Student, Department of Forensic Science, GIET Degree College, Rajahmundry.

UG II Year Student, Department of Forensic Science, GIET Degree College, Rajahmundry.

Assistant Professor, Department of Forensic Science, GIET Degree College, Rajahmundry.

ABSTRACT

Forensic biometrics is a real-time pattern matching system that involves using unique identifiers such as facial recognition, iris, voice recognition, ear prints, DNA, and fingerprints. Biometric technologies are widely used in various parts of society, including border crossing, logins, transactions, and security authentications. Biometrics are crucial evidence in almost all cases, and in the realm of solving crimes, the need for precise and swift identification has become absolutely essential. This is largely driven by the myriad facets of criminal activities ensuring accuracy and efficiency, has become a critical requirement in forensic applications.. The present study provides an overview of identification and applications where the principles of biometrics are successfully implemented in the field of forensic identification in law enforcement to solve critical problems. Biometric systems involve various recognition processes, encompassing feature extraction, feature robustness, and feature matching. The advent of forensic biometrics has expanded its applications to include both physical and cybercrime detection. This innovative approach addresses the shortcomings of conventional identification systems reliant on personal probabilities, signifying a fundamental transformation in the realm of criminal detection.

KEYWORDS

Biometric authentication, Cryptography, Fingerprint sensing, Amplification.

ABBREVIATIONS

DNA, PCR, FMR, CE.

1. INTRODUCTION

Using unique identifiers like fingerprints, DNA, voice, iris, palm or finger vein patterns and facial recognition etc, to solve crimes is known as forensic biometrics technology. Suspects can be identified using these identifiers, connected to crime scenes, and kept out of investigations. The accuracy and effectiveness of criminal investigations have significantly increased with the application of biometrics in forensic science [1]. Now a days Biometric systems have been used in various commercial, civilian and forensic applications as a means of establishing identity. The majority of biometric systems applied to real-world applications are unimodal, meaning they only take into account evidence like a digital fingerprint where your unique traits and behaviors seamlessly serve as the sole key to unlock and access your online identity. ***(Kant, Chander,2015).*** These systems must concern a number of cases, namely (a) Noise in data sensed: A voice sample manipulated with by cold, or a fingerprint image with a pock, are instances of data that is noisy. Additionally, noisy data may come from Unfavourable ambient conditions or malfunctioning or badly maintained sensors (such as inadequate illumination on a user's face in a face system of recognition). (b) collective differences: These changes are usually brought about by a user engaging with the sensor erroneously (e.g., by adopting an inaccurate facial position). During authentication, a sensor's parameters undergo modifications (e.g., optical versus solid-state fingerprint sensors). (c)Similarities between classes: Within a biometric system made up of a lot of users, there can be parallels between classes. (overlap) between several users' feature spaces ***(Arun Ross, Anil. k jain,2004).*** Since most passwords are so basic, it's simple to guess them (particularly using social engineering techniques) or to crack them using conventional onslaughts. It is not at all surprising that the most used password. The word "password" is used. Computerized data so secured by the security of a cryptographic algorithm relies on the password. In order to reveal the appropriate decrypting key or keys that can be utilised to verify the veracity of a user. As passwords are simple to figure out, security is weakened; Complex passwords can be difficult to remember, which makes them expensive to keep up. The limitations that are concerned with the use of passwords can be ameliorated by using the better methods for user verification like Biometric authentication ***(Anil.k jain, Sarath pankanti, Arun ross,2006).***

2. HISTORY OF BIOMETRICS

The word Biometry is derived from the Greek words, bios" means life and metrein" means to measure. As the word indicates, it deals with measuring parameters that are connected to life –parameters that are unique to every person and thus helps in identification of an individual. The identification that is based on bodily features itself has a long history. It has been used in the ancient Middle- and Far east to establish the identity of people by using height weight and special features. ***(K. N. A. R. Anil K. Jain, 2016.)*** For the first time the biometric features were used by Hungarian police to solve a crime in the year 1907. Alphonse Bertillon, a pioneering French police officer, invented criminal identification by developing a system that relied on unique bodily features, revolutionizing the field of forensic science. Galton and others discovered that fingerprints are unique feature to every person, enabling them for the usage of an individual in the year 1888. The important step in the history of biometrics was definitely the creation of the identification system and the related database that is supporting the system in 1960's. It resulted in the first version of AFIS (Automated (with the motto of making people use their eyes for further reference in any matter that is concerned in the state. Over the past two decades, developments in communications and computer science have raised demand for more advanced security solutions. In response to this need, security systems in the fields of communications and computer science have undergone significant advances, especially with the use of contemporary cryptosystems. The use of fractal image coding schemes is now a prominent trend in the development of biometric cryptosystems as an outcome of this. Thus, seven key biometric automations have been firmly established, including fingerprint, hand geometry, facial, iris, and retina recognition, along with voice, keystroke, and signature recognition. This progressive integration of the latest technologies highlights the ongoing development and sophistication of security protocols in modern systems. ***(Ahadullah, Md, Mohamad Rushdan Md Said, and Santo Banerjee, 2015.)*** may possibly elaborate a little on how Richard Edward Henry of Scotland Yard revived the practise of fingerprinting. A phrase or two explaining the significance of this revival might help the reader's comprehension. Although Karl Pearson's contributions to biometrics are mentioned, it would be helpful to include a quick overview of his specific findings and their significance for the field. This might provide readers a better understanding of Pearson's impact on the development of biometric research. The paragraph illustrates the evolution of signature biometric authentication procedures as it progresses from the early 20th century to the 1960s and 1970s. Mark Twain was the first author to use biometrics in his writing. "The Tradedegy of Pudd's Head Wilson" tells the story of a young lawyer who enjoyed collecting fingerprints as a hobby.

The changeover could be more seamless, though. Think about adding a sentence that defines and fills the gap**.** (Bhattacharyya, D., Ranjan, R., Alisherov, F., & Choi, M.,2009)

3. TYPES OF BIOMETRICS

Behavioural biometrics is based on measurements obtained from human behaviour, while physiological biometrics uses direct measurements from human body parts. The word "acquisition" draws attention to a crucial distinction: behavioural biometrics emphasises the temporal nature of this kind of biometric data by requiring measurements taken over a predetermined period of time.

Physiological Biometrics:

physiological measures that, for the most part, remain constant over time. the modalities mentioned, which include iris, retina, vascular pattern, hand geometry-based, ear geometry-based, fingerprint, hand geometry-based, facial recognition, and facial thermography. the significance of the application environment, highlighting how these technologies' performance is heavily reliant on the particular circumstances. For instance, face recognition technology can achieve high matching scores for real people in a controlled acquisition environment with ideal conditions like high image resolution, good lighting, and lack of occlusions. It does, however, correctly point out that these perfect circumstances might not hold true in all situations and that a lack of outside observation can cause a sizable decline in matching scores in various environmental circumstances.

Behavioural Biometrics:

Measuring users' behaviours over time is the main goal of the behavioural biometrics field. This type of biometric is more transparent, user-friendly, less intrusive, and convenient than physiological biometrics because it does not explicitly require user cooperation. It is crucial to remember that, in comparison to physical biometrics, behavioural biometrics typically have a lower degree of uniqueness and permanence. It performs exceptionally well in verification scenarios but may be less accurate for authentication purposes. Behavioural biometrics encompasses a variety of approaches that fall into classes like speaker recognition, gait recognition, mouse dynamics, and keystroke analysis-based authentication. (Buciu, I., & Gacsadi, A. 2016).

4. FINGERPRINT RECOGNITION

On the surface of fingertips, fingerprints possess distinctive pictorial patterns made up of ridges and valleys. Minute details are the precise locations where ridges split or terminate. Multiple strategies based on minutiae have been proposed for fingerprint representation. The basis for fingerprint identification is the unique fingerprint that each person has. Two basic hypotheses underpin this identification: singularity and invariance. The term "invariance" indicates that a fingerprint's properties don't change over the course of a person's life. According to the theory of singularity, no two individuals have the same fingerprint pattern. Uniqueness in biometric data refers to the absence of similarity in features between two different sets of data. For instance, no two humans, even if they are twins, share the same fingerprint features. (Ali, Mouad MH, et al., 2016).

Finger-scan technology stands out as the most widely employed biometric option. notably, its maturity assures a high degree of recognition accuracy, which makes it a strong option for a range of applications, including PC logon, physical access, and electronic commerce. Its reach is further increased by the accessibility of inexpensive, compact acquisition equipment. These devices' widespread popularity is partly due to their affordability and ease of use. Still, in spite of its advantages, there are some flaws that can reduce fingerprint recognition's efficacy. As an illustration, despite these difficulties, research and development are still being done to address these flaws, which will guarantee that fingerprint-scan technology will continue to advance.

Fingerprint Sensing:

Usually spreading ink on the finger and pressing it against a paper card was how fingerprint images were obtained. After then, the paper card is scanned to create a digital version. We call this procedure "off-line acquisition and is being applied in law enforcement. As of right now, it is feasible can obtain fingerprint images by applying pressure with the finger on a smooth surface of an fingerprint sensor that is electrical. We refer to this procedure as "online acquisition. (. Maltoni, D., Maio, D., Jain, A., Prabhakar, 2003).

Preprocessing And Feature Extraction:

The arrangement of interlocking ridges and valleys, as well as their parallel flow, termination, and bifurcation, are all well-described. A crucial level of detail is added with the introduction of global singularities, such as loop, delta, and whorl types. The local details—ridge ending and ridge bifurcation, in particular—are noted, which adds even more detail to our knowledge of fingerprint patterns. "We can see an example of loop and delta singularities (the whorl singularity can be defined)" is one sentence that seems unresolved and may need to be clarified. It seems to stop there and fails to carry on or make sense.

The process of separating the fingerprint area (foreground) from the background is called fingerprint segmentation. It is essential to segment the data in order to stop fingerprint features from being extracted from the noisy background. The paragraph points out that more reliable segmentation techniques are frequently used in place of global and local thresholding segmentation methods, which are not very effective. These methods capitalise on the existence of a non-oriented isotropic pattern in the background and an oriented periodical pattern in the foreground. (Mehtre, B.,1993).

Fingerprint Matching:

A template, that reflects a single user retrieved from the system database based on the claimed identity, will be contrasted with features extracted from the input fingerprint during the matching step. Either an acceptance/rejection decision or a similarity degree—often described as a matching score—is the outcome of this process. There are several fingerprint matching methods accessible some of which compare grayscale images (or subimages) directly by means of correlation-based techniques. This ensures that the grayscale image and the fingerprint template are compatible. (10)

Current Challenges:

A significant issue in fingerprint verification, particularly the inability to withstand degeneration of image quality. The quality of the fingerprint images being processed has an enormous effect on how well fingerprint recognition systems work. Overall fingerprint image quality is influenced by a number of factors, including user cooperation, sensor conditions, and skin conditions. An essential component of a fingerprint recognition system is the estimation of image quality because certain factors are unavoidable and others may shift over time. The overall efficacy and performance of the system can be impaired by spurious and missed features that arise from low-quality images. As a result, it is important to create fingerprint recognition systems that can precisely gauge the authenticity and quality of fingerprint images. (Alonso-Fernandez, F., Fierrez, J., Ortega-Garcia, et al ,2007).

5. IRIS RECOGNITION

The word iris comes from classical times. Iris is the coloured portion of the exterior eye. the stability and distinctiveness of iris structure, with research from two main sources. Clinical observations, in which ophthalmologists and anatomists have examined numerous eyes. They have repeatedly noted that the complex patterns of a person's iris, including the left and right iris of the same individual, show a great degree of their uniqueness. The information is presented in an organised way that makes simple to understand the evidence for the assertion that the iris structure is stable and unique. (I. Mann, 1950).

"Iris patterns present an effective replacement for accurate facial recognition, especially in situations where imaging can be performed at less than one metre away. This reduces the possibility of false matches despite the large number of possibilities, which is especially useful when searching large databases. Due to its immense pattern variability across individuals, the iris provides a significant mathematical advantage despite its small size (11 mm) and occasional imaging challenges. In addition, the iris is stable over time and is well-protected from environmental factors as it is an internal organ of the eye that's visible from the elsewhere. (A. Pentland and T. Choudhury, 2000). The main objective of iris biometric is to identify and stop the use of multiple IDs. It highlights that in order to accomplish this goal, an offline "each-against-all" cross-comparison has to be carried out during the card's issuance and ID registration. It is noteworthy because it illustrates how the number of biometric comparisons needed varies with population square. The passage also makes reference to the difficulty in maintaining decision confidence levels in order to keep the false match rate (FMR) low, considering the significant chances of false matches that come with a large population. When everything is considered, it does a good job of putting iris biometric ID systems in place to deal with issues including multiple IDs. (J. Matey, K. Hanna, R. Kolcyznski, et al, Nov. 2006).

Process Of Recognition:

The iris recognition image acquisition process, emphasising optical platforms meant for specific applications. These platforms utilise components such as a lens, frame grabbing board, monochrome CCD camera, and low-level LEDs for illumination to enable image capture at distances ranging from 3.5" to nearly meter. The system locates important iris features, maximises the usable area, and transforms these features into a 512-byte Iris code record for storage and comparison during recognition attempts—all of which are covered in detail in the following sections on iris definition, field optimisation, and image analysis. (Williams, Gerald O., 1996).

Advantages:

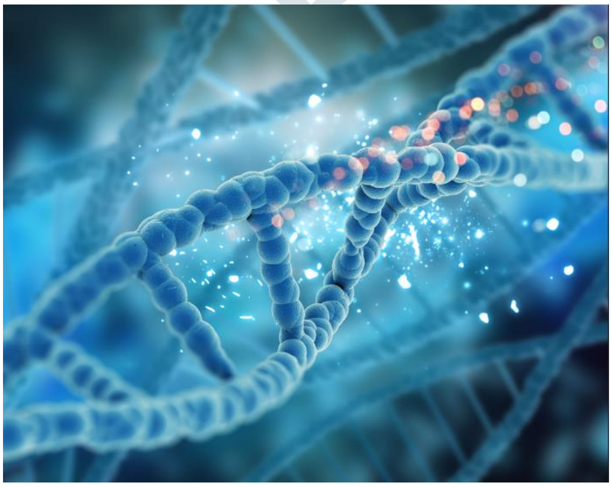
An Iris Recognition System has many advantages. First of all, iris patterns are not inherited because the iris, which is formed during prenatal morphogenesis, is stable throughout an individual's life and has a limited genetic impact. The iris's inherent ability to defend itself from the outside world and the capability to scan patterns at a distance both contribute to its increased effectiveness as a biometric identification tool. The robustness and uniqueness of iris patterns for biometric purposes are further highlighted by the impossibility of surgical modification without endangering vision, the confirmation of natural physiology through pupil size modification, and the tractable encoding.

Applications:

Particularly in the control of national borders, the application of biometrics in Physical Access Control systems is a highly commercialised field. In the past ten years, the field of automated iris recognition research has grown to include a significant practices. As a living passport for border security, iris recognition is essential to the management of national borders. This entails overseeing the entry and exit points for both citizens and foreign visitors in routine international transactions, such as airfield, maritime and industrial zones related to marine fishing, and external trade in goods. The identification of visitors, immigrants, workers, and temporary workers is the main duty. (] A. Sallehuddin, M. Ahmad et al, 2016).

6. DNA RECOGNITION

One of the most reliable biometric identifiers is deoxyribonucleic acid (DNA), which is mostly used in forensic applications. DNA provides a wealth of genetic identity information, providing insights into a person's identity and health. Because genetic data is sensitive, privacy concerns have surfaced despite its potential. Furthermore, the DNA verification process is intrinsically sluggish, frequently requiring days to weeks for confirmation. Furthermore, because identical twins have the same genetic code, the uniqueness of DNA presents difficulties and calls into question the accuracy of the method in differentiating between people.



DNA Sample Collection:

Numerous biological materials, such as bodily fluids, hair, nails, and used razors, can be used to extract DNA. It is obvious why buccal swabbing is important for biometric applications, emphasising its ease of use, comfort, and lack of discomfort. The method of collecting shed epithelial cells from the inside of the subject's inside of the jaw by wiping a small piece of filter paper or a cotton swab against it is explained in a clear and concise manner in the description of the buccal cell collection procedure. Practical details are added when it is pointed out to air dry or press the swab against a treated collection card for storage. The paragraph is generally well-written and offers useful information regarding the methods used to collect DNA samples. (Anderson T. D. et al. 1999).

DNA Amplification:

Kary Mullis is credited with discovering DNA amplification through polymerase chain reaction (PCR), and his Nobel Prize provides historical background. The enzymatic process of PCR is also thoroughly explained. The PCR's pattern of heat cycling and its quick amplification of particular DNA sequences. A modern viewpoint is added by mentioning recent developments, such as the capacity to PCR amplify 16 short tandem repeats (STRs) at once using commercial typing kits. (Mullis K. B. Faloona F. A. 1987).

DNA Separation And Detection:

Following STR polymorphism amplification via PCR, there is a DNA separation and detection procedure. It aptly illustrates why the minute variations in length between STR alleles necessitate accurate measurement. It is well-articulated how electrophoresis with denaturing polyacrylamide gels and the more recent use of fluorescence labelling with multi colour detection are used in forensic science. It also emphasises the advancements in separation techniques by tracing the development of electrophoresis platforms from slab-gels to capillary electrophoresis (CE). A useful perspective is added by the final statement regarding the total time needed for the process, which includes the extraction of DNA and the acquisition of data from 16 STRs. All things considered, the paragraph is coherently organised and instructive. (Slater G. W. et al. 2000).

7. VOICE RECOGNITION

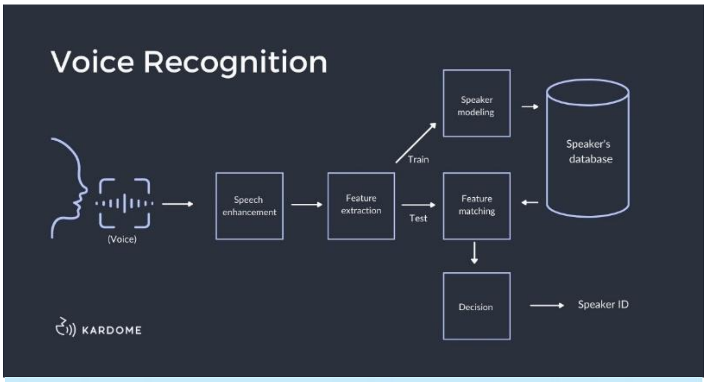
These days, many businesses and residential areas use various security systems, such as pin and User ID/Pin protection, to ensure that their property is safe. Regretfully, due to the possibility of pin code hacking and ID card theft and duplication, all security measures are completely unsecure. For these reasons, a completely new security system technology needs to be developed in order to restore civilian confidentiality about the anti theft system. A biometric method is one that uses the password to be the user's features. Everybody has distinct feature parameters, even if they are identical twins. Thus, the administrator user can safely use the speech recognition system. For humans, speaking is the most basic method of communication. Voice biometric technology is more accurate and convenient for user authentication. This is due to the fact that each person's biometric feature is distinct and remains private until the user passes away. Because there is nothing to carry or remember and there is no trouble of the ID card or password being stolen, it is handy for the user. (Shah, H. N. M., Ab Rashid, et al ,2014).

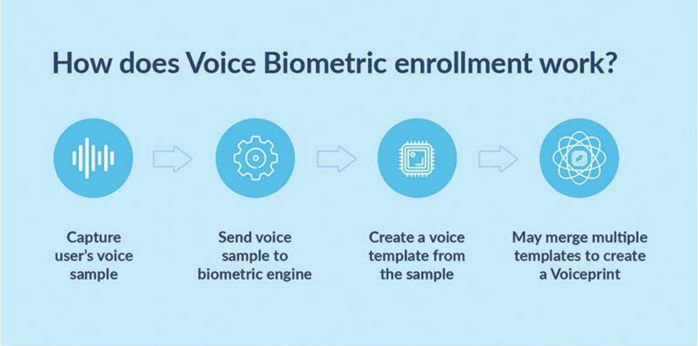
Process Of Recognition:

There are two phases to the voice recognition system: training and recognition. The system picks up the defining characteristics of the enrolled user during training. Subsequently, the user speech features are captured by the system and compared with the registered voice metrics by the speech recognition system. The user is approved if there is a match; if not, the verification system refuses the user. The main advantage of a voice-based biometric system is that it only uses sound recognition to verify identity—user speech is not recorded. The quantity of airflow and any obstacles in the path of the airstream, such as the tongue, gums, and lips, determine the type of sound that is produced. Therefore, maximum-risk and security systems are suitable for the advanced authentication technique (Thomas, P. A., & Preetha Mathew, K.2023).

Future Recommendations:

The use of distinctive physical characteristics as identification and verification mechanisms, increasing the prevalence of biometric technology by factors such as fingerprints, iris scans, voiceprints, facial recognition, signatures, and hand geometry. These technologies are essential in helping governments and companies fight fraud and identity theft, secure online proceedings, protect personal information, cut expenses, and enrich the level of service. Biometric voice recognition mechanization has its own set of difficulties. Improvements in microprocessor and signal processing technologies are opening the door for more precise measurements, even though they have taken longer to take off in many markets. However, issues like the high false reject rate brought on by external factors and background noise continue to exist. However, there is hope for the future of biometric voice identification technology because of continuing research and advanced algorithms that are constantly enhancing vocal measurements and turning them into distinct digital representations, or voice prints.




How does Voice Biometric enrollment work?
Capture user's voice sample
Send voice sample to biometric engine
Create a voice template from the sample
May merge multiple templates to create a Voiceprint

8. GAIT PATTERN BIOMETRIC RECOGNITION

The series of rhythmic, well-coordinated movements that make up a human's gait. It highlights how these motions must follow a precise temporal pattern in order for them to be considered a gait, with repetition taking place as a walker alternates between steps with different feet. Gait is special because it is cyclical and coordinated at the same time. The gait examples—running, jogging, walking, and climbing stairs—emphasize how these activities differ from non-locomotive coordinated actions like sitting, picking up, and tossing objects. The definition of gait recognition is defined as the process of recognising important characteristics from the coordinated, cyclic motions of human locomotion, such as identity, walking style, or pathology. (McGrath, B.,2003).

Advantages:

The best biometric for intelligent visual surveillance turns out to be gait. People in surveillance issues frequently stand far away from cameras, causing many standard biometric features unavailable. even though facial recognition is the main tool used by current systems for identification, this approach has major drawbacks, including the ability to be subject to unexpected view angles and occlusion, which can lead to incomplete face captures and low-resolution images because of the distance factor. On the other hand, gait, as a behavioural biometric, includes both the dynamic elements of a person's walking pattern and individual physical characteristics such as height, leg length, and shoulder width. In contrast to other biometrics, gait can be accessed remotely, is difficult to mimic, and is not easily concealed. Moreover, high-resolution photos, specialised tools, or collaboration are not required for the capturing process.

This image shows the gait pattern of normal walking and carrying conditions. (. S. Yu, D. Tan, and T. Tan, 2006).

Gait Cycle Detection:

a gait pattern must be bifurcated into cycles, each of which represents a full walking period. The majority of methods in the literature employ time series data that are obtained from measurements such as the total of silhouettes' foreground pixels. But because of its tendency to be noisy, this signal needs to be preprocessed before analysis. One approach suggested fitting a dynamic signal to the noisy uprooted signals using linear prediction, which offered a possible cycle partitioning solution. Before computing gait cycles using the minima of the foreground sum signal, an adaptive filter was also used to improve the signal's quality. the walking period and coefficients for the best filter to denoise the sum signal are calculated using autocorrelation. (J. Little and J. Boyd, 1998).

Process Of Gait Pattern Recognition:

The first step in the processing is to convert the uninterrupted motion of a person in a video into a stream of still images. Third-party Java classes, specifically "Media Listener Adapter" and "IMedia Reader," which are implemented via the Xuggle JAR file, are utilised in the process. These classes manage the related events and make it easier to read a video stream. The "IMedia Reader" class reads the video sequence as a stream when the path to a video file is supplied as an input parameter. The "Media Listener Adapter" reacts to events produced while the video file is being read. The "On Video Picture" event, which in this system is set to 200 milliseconds, creates an image frame from the video stream at predetermined intervals. 35 frames is the maximum number of predefined image frames that can be used. Each image frame's width and height are uniformly rescaled to 450 by 450 pixels in order to maintain consistency. (Carson, C., S. Belongie, et al,2002).

9. RECENT ADVANCEMENTS IN BIOMETRICS

The versatility of biosensor technology is effectively highlighted by the wide range of applications of biosensors in various fields, including clinical diagnostics, environmental processes, the food industry, and military use. The passage also deftly illustrates the expanding role of biosensors in various fields by introducing new applications in cybersecurity, biometrics, and forensics. The idea is made clearer by the way biosensors function, which depends on biorecognition components and allows for precise and quick outcomes in bio tendency-based reactions. the value of biodetectors in forensics, which can help investigators quickly focus their investigations by providing additional statistics in addition to DNA analysis. The relationship between biosensors and biometrics is clearly explained, especially when it comes to the idea that noninvasive biosensors help distinguish people without requiring invasive procedures. Electrochemical and enzymatic assays are the analytical techniques used. (D'Orazio, 2011).

The benefits of 3D acquisition systems becoming more accessible and affordable are emphasised, opening up the possibility of a wider range of environments for their use. There are two ways to use three-dimensional data in criminal investigations: creating synthetic two-dimensional views to compare with images of faces taken from crime scenes, and substituting standard mug shots with complete three-dimensional representations. The clear and informative language successfully communicates the possible improvements in identification performance made possible by 3D face recognition technology. (Tistarelli, Massimo, Enrico Grosso, 2014).

From the 1990s, considerable progress has been made in automatically identifying people based on their gait using machine perception. There has been a noticeable shift from smaller databases with tens of subjects to databases with thousands of subjects. Achieving a remarkable 97.5% correct classification rate, databases have grown to include over 4000 subjects due to advancements in computer power and memory affordability.

The polygraph exam is an advanced psychophysiological test envisioned to spot inaccurate data or diagnose specific psychophysiological traits that highlight unique aspects of a person. Often called a "lie detector," the polygraph plays a crucial role in collecting testimony in criminal investigations. The examinee's complete safety and innocuousness is ensured by this method. Polygraph-based psychophysiological tests have a high degree of accuracy in their results. (Borysenko, Igor V., et al. 2021).

The goal of recent developments in forensic cryptography has been to improve the dependability and security of biometric systems. Sophisticated cryptanalysis methods like secure multi-party computation and homomorphic encryption are being combined to safeguard private biometric data while it's being transmitted and stored. The goal of these advancements is to handle new issues with biometric authentication. (Daimi, Kevin et al, 2022).

Multimedia phylogeny, a concept in computer vision, highlights the difficulty of handling minute changes that result in a range of near-duplicates on the Internet and successfully introduces the idea of interpreting the trail of modifications in images or videos. Research on near-duplicate detection and retrieval is mentioned, which gives current field efforts more context. It helps us comprehend the necessity of figuring out the original image's root node and the connections between near-duplicates. The explanation is made more thorough by the mention of exploratory research that used picture dependencies and a minimal spanning tree (MST) to represent the hierarchical structure. (A.D. Rosa, F. Uccheddu, A. Costanzo et al, 2010).

10. CONCLUSION

Biometric technology is certainly the future game changer of this fast paced world where everything is getting digitalized which augurs well for populace in serving their needs and simplifying their lives. So, to say the introduction of Digi yatra in Airports is a welcome move which greatly reduces the passenger's waiting time, Facial recogniton and speech recognition in our mobile phones that makes our task easier, marking attendance of students, employees at their respective institutions and workplaces, utilising biometric for authentication to provide essentials like PDS and face recognition to identify criminals. But, not to forget the other side of the coin that brings issues with misuse of this technology. Misuse of biometric data present with the govt agencies can threaten the privacy of crores of people. For instance, hacking of AIIMS servers in return for ransom happened recently that put sensitive data of patients at risk. Not only this browser fingerprinting is another issue that could definitely pose a threat. So, Protection of collected and processed data is must and consent of individual is needed before collecting or using the data and the agencies must utilize these methods to promote good for the society rather than misusing them. By using biometrics crimes can be solved at a faster rate and at the same time data can be protected from unauthorised access. Crime rate can be reduced at a high level with proper usage of biometrics in daily life. Recently improving technologies are strengthing the security and introducing sophisticated ways to solve the crime.

11. REFERENCES

1. A.D. Rosa, F. Uccheddu, A. Costanzo, A. Piva, M. Barni, Exploring image dependencies: a new challenge in image forensics, vol. 7541, Media forensics and security II, 2010.
2. Ahadullah, Md, Mohamad Rushdan Md Said, and Santo Banerjee. "History, development and trend of fractal based biometric cryptography." In Chaos, Complexity and Leadership 2013, pp. 27-33. Springer International Publishing, 2015.
3. Ali, Mouad MH, et al. "Overview of fingerprint recognition system." 2016 international conference on electrical, electronics, and optimization techniques (ICEEOT). IEEE, 2016.
4. Alonso-Fernandez, F., Fierrez, J., Ortega-Garcia, J., Gonzalez-Rodriguez, J., Fronthaler, H.,Kollreider, K., Bigun, J.: A comparative study of fingerprint image quality estimation methods.Trans. on Information Forensics and Security (2007) .
5. Anderson T. D. et al. 1999 A validation study for the extraction and analysis of DNA from human nail material and its application to forensic casework. J Forensic Sci, 44(5): 1053 1056.
6. Bhattacharyya, D., Ranjan, R., Alisherov, F., & Choi, M. (2009). Biometric authentication: A review. International Journal of u-and e-Service, Science and Technology, 2(3), 13-28.
7. Bisresearch, biometrics in forensic science, Feb,2023.
8. Borysenko, Igor V., et al. "The modern development of new promising fields in forensic examinations." Journal of Forensic Science and Medicine 7.4 (2021): 137-144.

9. Buciu, I., & Gacsadi, A. (2016). Biometrics systems and technologies: A survey. International Journal of Computers Communications & Control.

10. Carson, C., S. Belongie, H. Greenspan, and J.Malik. Blobworld: (2002) Image segmentation using expectation-maximization and its application to image querying. IEEE Trans. Pattern Anal.

11. D'Orazio, P. Biosensors in clinical chemistry—2011 update. Clin. Chim. Acta 2011, 412, 1749–1761. [CrossRef]

12. Daimi, Kevin, Guillermo Francia III, and Luis Hernández Encinas, eds. Breakthroughs in digital biometrics and forensics. Springer Nature, 2022.

13. J. Little and J. Boyd, "Recognizing people by their gait: The shape of motion, Videre, Int. J. Computer Vision, vol. 14, no. 6, pp. 83–105, 1998.

14. J. Matey, K. Hanna, R. Kolcyznski, D. LoIacono, S. MangruO. Naroditsky, M. Tinker, T. Zappia, and W-Y. Zhao, "Iris on the move:Acquisition of images for iris recognition in less constrained Environments", Nov. 2006.

15. Jain, A. K., Ross, A., & Pankanti, S. (2006). Biometrics: a tool for information security. IEEE transactions on information forensics and security, 1(2), 125-143.

16. K. N. A. R. Anil K. Jain, „50 Years of Biometric Research: Accomplishments,Challenges, and Opportunities," Pattern Recognition Letters, p. 6, 2016.

17. Kant, Chander. "A multimodal approach to improve the performance of biometric system." BVICA M's International Journal of Information Technology 7.2 (2015): 891.

18. Maltoni, D., Maio, D., Jain, A., Prabhakar, S.: Handbook of Fingerprint Recognition. Springer, newyork,2003.

19. Mann. The Development. of the Human Eye. New York:Grune and Stratton, 1950.

20. McGrath, B.: The week in walks. The New Yorker June 2 (2003) 35.

21. Mehtre, B.: Fingerprint image analysis for automatic identification. Machine Vision and 1054 Applications (1993).

22. Mullis K. B. Faloona F. A. 1987 Specific synthesis of DNA in vitro via a polymerase-catalyzed chain reaction. Methods Enzymol, 155: 335 350.

23. Pentland and T. Choudhury, "Face recognition for smart environments," Computer, vol. 33, no. 2, pp. 50–55, 2000.

24. Ross, A., & Jain, A. K. (2004, September). Multimodal biometrics: An overview. In 2004 12th European signal processing conference (pp. 1221-1224). IEEE.

25. S. Yu, D. Tan, and T. Tan, “A framework for evaluating the effect of view angle, clothing and carrying condition on gait recognition,” in Proc. IEEE/IAPR Int.Conf. Pattern Recog., vol. 4, 2006, pp. 441–444.

26. S.A. Cole. Forensics without uniqueness, conclusions without individualization: the new epistemology of forensic identification. Law, Probability and Risk, 8(3):233–255 2009.

27. Sallehuddin, M. Ahmad, R. Ngadiran and M. Nazrin, “Score Level Normalization and Fusion of Iris Recognition”, International Conference on Electronic Design, 2016.

28. Shah, H. N. M., Ab Rashid, M. Z., Abdollah, M. F., Kamarudin, M. N., Lin, C. K., &Kamis, Z. (2014). Biometric voice recognition in security system. Indian journal of Scienceand Technology, 7(2), 104.

29. Slater G. W. et al. 2000 Theory of DNA electrophoresis: a look at some current challenges. Electrophoresis, 21(18): 3873 3887.

30. C Thomas, P. A., & Preetha Mathew, K. (2023). A broad review on non-intrusive active userauthentication in biometrics. Journal of Ambient Intelligence and Humanized Computing, 14(1), 339-3.

31. Tistarelli, Massimo, Enrico Grosso, and Didier Meuwly. "Biometrics in forensic science: challenges, lessons and new technologies." Biometric Authentication: First International Workshop, BIOMET 2014, Sofia, Bulgaria, June 23-24, 2014. Revised Selected Papers 1. Springer International Publishing, 2014.

32. Williams, Gerald O. "Iris recognition technology." 1996 30th Annual International Carnahan Conference on Security Technology. IEEE, 1996.