ISSN NO. 2320-5407

Journal homepage:http://www.journalijar.com
Journal DOI:10.21474/IJAR01

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH

RESEARCH ARTICLE

A REVIEW ON BIOMETRICS AND FACE RECOGNITION TECHNIQUES.

NehaAnot, K. K. Singh.
Department of Electronics & Communication Engineering, Amity University, Lucknow.

Manuscript Info

Manuscript History:

Received: 16 March 2016
Final Accepted: 19 April 2016
Published Online: May 2016

Key words:
Biometric, Biometric techniques, Eigenface, Face recognition..

***Corresponding Author**

NehaAnot.

Abstract

Biometrics is a rising technology, which has been broadly used in forensics, protected access and prison security. This biometric system is basically a type of pattern recognition system that identifies a person by defining the authentication through using his distinctive biological characteristics i.e. Thumb impression, retina-scan, iris scan, palm geometry, and face recognition are top physiological biometrics and behavioral traits are Speech recognition, keystroke-scan, and signature-scan. In this paper different types of biometric techniques such as Iris scan, retina scans and face recognition techniques are being discussed.

Introduction;-

Biometrics is automated methods of identifying a individual grounded on a physiological or behavioral features. The past historical of biometrics comprises the identification of individuals by distinguishing the physique features, scars or a group of further physiological criteria, such as a person's height, eye color and appearance. The current features are face recognition, impressions, handwriting, iris, speech, hand geometry, vein & retinal scan. Biometric method is now becoming the establishment of a wide array of highly protected identification and individual verification. While the level of security opening and transaction cheat increases, the necessity for sound and secured identification and private verification technologies are becoming apparent. Latest world procedures had lead to raise interest in security that will compel biometrics into common use. Areas of upcoming usage contain Internet connections, workplace and network access, mobile transactions and in transportable and tourism. Around distinctive types of biometrics: Some are very old or others are newest technology. The most acknowledged biometric technologies are fingerprinting, retinal scanning, hand geometry, signature verification, speech recognition, iris scanning and facial recognition. A biometric system can be whichever an 'identification' type of system or a 'verification' (authentication) type of system, which are well defined below.

Identification(1:n)–One-to-Many:- Biometrics can be utilized to decide a man's character even without his awareness or acceptance. For example, examining a group with the assistance of a camera and utilizing face recognition innovation, one can check matches that are as of now store in database.

Verification(1:1) One-to-One:- Biometrics can likewise be utilized to check a man's personality. For example, one can permit physical access to a safe range in a working by utilizing finger filters or can allow access to a financial balance at an ATM by utilizing retina examine.

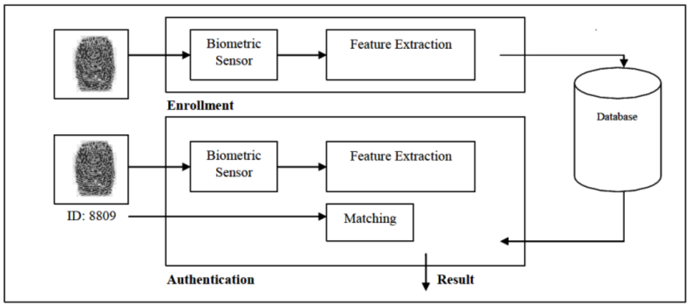

Figure 1:-General Biometric System[1]

Characteristics of biometrics:-

"Biometrics" indicates "life estimation" however the term is for the most part combined with the utilization of special physiological attributes to recognize a man, some different qualities of biometrics are:

Universal:- Every individual must have the trademark. The characteristic must be one that is all-inclusive and from time to time lost to mischance or ailment.

Measurability:- They ought to be consistent over quite a while. The characteristic ought not be center to significant contrasts taking into account age either wordy or endless ailment.

Singularity:- This ought to be appropriate for catch without holding up time and should be anything but difficult to accumulate the characteristic information inactively. Each outflow of the component must be particular to the individual. The attributes ought to have sufficient unmistakable properties to recognize one individual from other. Stature, weight, hair and eye shading are all components that are one of a kind expecting a generally precise measure, yet don't sufficiently offer purposes of detachment to be helpful for more than sorting.

Acceptance:- The catching ought to be conceivable in a way satisfactory to an expansive division of the inhabitants. Avoided are especially steady innovations, such advancements which is require a part of the human body to be taken or which (clearly) hinder the human body.

Reducibility:- The caught information ought to be capable of being diminished to a document which is anything but difficult to handle.

Reliability & tamper-resistance:- The credit ought to be illogical to cover or change. Procedure ought to ensure high dependability and reproducibility.

Privacy:- This procedure ought not break the security of the person.

Comparable:- They ought to have the capacity to decrease the quality to a state that makes it is digitally equivalent from others. It has less probabilistic for comparability and more tried and true on the recognizable proof.

Inimitable:- The attribute must be irreproducible by other way. The less reproducible the characteristic, the more probable it will be dependable.

Biometric innovations: unique mark, facial elements, hand geometry, voice, iris, retina, vein designs, palm print, DNA, keystroke flow, ear shape, scent, signature all fulfill the above necessities.

In biometrics, this biometric system can be categorized into subsequent modules:-

- Database Preparation
- Verification Module

Database Preparation Module are further subdivided into two sub-modules:-

- Enroll Module
- Training Module

Authentication Module:-
- ❖ Matching Module
- ❖ Decision Module

Technology of biometrics:-
- ❖ Impression Recognition.
- ❖ Speech Recognition
- ❖ Signature Recognition
- ❖ Facial Recognition
- ❖ Palm scan
- ❖ Iris-scan Recognition
- ❖ Retina-scan Recognition
- ❖ Finger geometry
- ❖ Sign.-scan
- ❖ Keystroke-scan

Fingerprint Recognition:-Unique mark output is the most broadly utilized biometric innovation. Finger impression (optical, silicon, ultrasound, touch less) uniqueness can be characterized by investigating the trivia of a person. Trivia incorporate sweat pores, separation stuck between edges, bifurcation. It is plausible that the probability of two people having the same unique mark is short of what one in billion. There are a few sub-strategies in fingerprinting, with variable degrees of exactness and rightness. Different can even identify when a live finger is available. Fingerprinting strategy has been produced throughout the years.

Speech Recognition:-Speech Recognition innovation does not gauge the visual components of the human body. In voice acknowledgment sound vibes of a man is measured and contrasted with a current dataset. The individual to be distinguished is typically required to talk a mystery code, which encourages the confirmation procedure.

Signature Recognition:-Signature Recognition is the procedure used to perceive an individual's written by hand or mark. Dynamic mark confirmation innovation utilizes the behavioral biometrics of a transcribed mark to affirm the character of a PC customer. Breaking down the pace, shape, stroke, and pen weight and timing data amid the demonstration of marking regular does this.

Palm-scale Recognition:- In Palm Recognition 3-dimensional picture of the hand is gathered and the component vectors are separated and contrasted and the database highlight vectors. These gadgets are cumbersome however recognizable proof is done in a brief timeframe.

Fingerprint Recognition:-Advantages-High precision, non-obtrusive biometric method. Most practical biometric PC client verification method, it is a standout amongst the most created biometrics, Easy to utilize, Small storage room required for the biometric layout furthermore diminishes the span of the database, It is standardized.
Disadvantages- For some individuals it is to a great degree meddling, in light of the fact that is very still identified with criminal confirmation, it can be create botches with the dryness or grimy of the finger's skin, and in addition with the age (is not proper with kids, on the grounds that their unique mark changes rapidly), Image caught at 500 dabs for each inch (dpi). Determination: 8 bits for every pixel.

Facial recognition:-

With a specific end goal to perceive a man, one regularly takes a gander at countenances, which separate one individual to another. FR is utilized to look for different pictures with coordinating elements [5]. Eyes specifically appear to recount a story about which some individual is, as well as about how that individual feels, where his/her consideration is coordinated, and so forth [1]. Face acknowledgment records the spatial geometry of one of kind components of the face. Principle concentrates on key components of the face. Face acknowledgment strategy is utilized to distinguish terrorists, offenders, and different sorts of persons for law authorization purposes. This is a non-nosy, shabby innovation. In fr 2d acknowledgment is influenced by change in lighting, the individual's hair, age, and if the general population wear glasses, low determination pictures [5]. It requires camera as hardware for client recognizable proof; along these lines, it is dubious to wind up famous until most pcs incorporate cameras as standard gear. Joined states utilized same innovations to keep individuals from getting fake ID cards and driver's licenses [9]-[10].

Steps for Facial Recognition System:-

❖ Obtain the required image.
❖ Locate the facial region.
❖ Facial detection procedure.
❖ Face recognition
❖ Person Identity

Face Recognition algorithms are of various types. They are Linear Discriminate Analysis, Pseudo 1D Hidden Markov model(HMM), Artificial neural network, Support Vector Machine (SVM), Principal Component Analysis (PCA) that use eigenfaces, Elastic Bunch Graph Match consuming the Fisherface algorithm, Multilinear, Subspace Learning using tensor representation, and the neuronal motivated dynamic link matching, Artificial neural network, and normalized correlation.

Conclusion:-

Biometrics is a quickly advancing innovation that is by and large broadly utilized as a part of crime scene investigation, security; counteract unapproved access in bank or ATMs, in phones, savvy cards, PCs, in working environments, and PC systems. There are various types of biometrics now being incorporated with innovation stages. It has been executed in broad daylight for brief time. There are loads of uses and arrangements in biometrics innovation utilized as a part of security frameworks, which can enhance our lives, for example, enhanced security, it is diminished con and secret key manager costs, simple to utilize and make life more secure and agreeable. In any case, it is impractical to state if biometric methods are fruitful run, it is vital to find elements that is lessen influence framework execution. Ace recognition technology are more reliable, non-intrusive, inexpensive and extremely accurate. Presently Face recognition technology is the greatest inspiring recognition technologies.

Acknowledgement:-

The authors are thankful to Hon’able C – VI, Mr. AseemChauhan (Additional President, RBEF and Chancellor AUR, Jaipur), Honáble Pro VC Maj. General K. K. Ohri (AVSM, Retd.) Amity University, Lucknow, Wg. Cdr. (Retd.) Dr. Anil Kumar, (Director, ASET), Prof. S. T. H. Abidi (Professor Emeritus), Brig. U. K. Chopra, Retd.(Director AIIT), Prof. H K Dwivedi (Director, ASAP), Prof O. P. Singh (HOD, Electrical & Electronics Engg.) and Prof. N. Ram (Dy. Director ASET) for their motivation, kind cooperation, and suggestions.

References:-

1. K P Tripathi, International Journal of Computer Applications (0975 – 8887) Volume 14– No.5, January 2011
2. Iridian Technologies, http://www.iriscan.com
3. EyeDentify, http://www.eyedentify.com/
4. Zdeneˇk R íhaVáclavMatyáš “Biometric Authentication Systems ”, FI MU Report Series, November 2000.
5. Bonsor, K. "How Facial Recognition Systems Work". Retrieved 2008-06-02.
6. YongshengGao; Leung, M.K.H., “Face recognition using line edge map”, Pattern Analysis and Machine Intelligence, IEEE Transactions on , Volume: 24 Issue: 6 , June 2002, Page(s): 764 -779.
7. Pentland, A.;Choudhury, T. “Face recognition for smart environments “, Computer, Volume: 33 Issue: 2, Feb. 2000, Page(s): 50 -55.
8. De Vel, O.; Aeberhard, S., “Line-based face recognition under varying pose”, Pattern Analysis and Machine Intelligence, IEEE Transactions on Volume: 21 Issue: 10, Oct. 1999, Page(s): 1081 -1088.
9. House, David. "Facial recognition at DMV". Oregon Department of Transportation. Retrieved 2007-09-17. "Oregon DMV is going to start using “facial recognition” software, a new tool in the prevention of fraud, required by a new state law. The law is designed to prevent someone from obtaining a driver license or ID card under a false name."
10. Schultz, Zac. "Facial Recognition Technology Helps DMV Prevent Identity Theft". WMTV News, Gray Television. Retrieved 2007-09-17. "Madison:The Department of Motor Vehicles is using... facial recognition technology [to prevent ID theft]" .
11. http://www.sony.net/SonyInfo/technology/technology/theme/sface_01.html