MAT JOURNALS

Journal of Optical Communication Electronics
Volume 4 Issue 3

An Innovation in Multi-model Biometric Techniques

[1]Prof.Ankur Kumar Aggarwal, [2]Mr. Himanshu Bansal
[1]Professor,[2]Student
[1]Department of Computer Science Engineering,
[2]Department of Electronics and communication Engineering
[1,2]ManavRachna University,Faridabad, Haryana, India
Email:*[1]Ankur_agg1987@yahoo.com,[2]himanshu8950036350@gmail.com*
DOI:

Abstract

In this paper gives an overview of working, challenges of face recognition and fingerprint recognition system. Multi-model recognition system is better as compare to single model because if one model is intruded another template is used. The paper presents the details of 3D face model acquisition and its recognition techniques. Challenges faced in face recognition system leads to 3D face recognition system. Different level of threats to the biometric system is discussed. Spoofing techniques are discussed on the basis of cooperative and non-cooperative methods so that the anti-spoofing techniques can be developed on the basis of hardware and software.

Keywords:*Biometric, Face recognition, Fingerprint, 3D face, Multi-model, Spoofing.*

INTRODUCTION

Authentication is that the method of providing access to services to somebody by confirming its identity. The authentication method will be divided into 3 major classes [1]. To start with is Verification by learning. The verifier surely understood data identifying with the guaranteed personality that can exclusively be notable or created by a central therewith character (e.g. international ID, secret word, Stick, survey). There are four types of confirmation by learning or secret word method [2]: gather passwords are notable to any or all clients inside the framework. These styles of passwords are risky for all frameworks. Unmistakable passwords for each individual are normally kept in a bit of paper instead of being remembered. This puts the security of the framework in threat. Non-remarkable passwords that are utilized to guarantee an asserted character. A short secret key is given to clients wherever recognizable proof relies upon a long range keep in a card (e.g. attractive card). Shockingly these numbers will be perused and modified.

Passwords that change each time a framework is gotten to have the detriment that a posting of secret word should be kept at the focal framework and a copy ought to be circulated to each client. The misusing of these rundowns may cause divulgence. The protected transmission of passwords from a key to lawful clients could be a huge downside. Second is Evidence by Ownership. The candidates will be affirmed by the ownership of a protest (e.g. attractive card, shrewd card, optical card). Also, third is Evidence by Property. The inquirer straightforwardly measures certain petitioner properties utilizing human attributes (e.g. biometrics).

BIOMETRIC SYSTEM

A biometric framework is fundamentally an example acknowledgment framework that perceives an individual in view of a component vector got from a specific physiological or behavioral trademark that the individual has [5]. Contingent upon the applying setting, a biometric framework for the most part works in one among two modes: confirmation or ID.

In check mode, the framework approves a man's personality by examination the caught biometric trademark with the

person's biometric demonstrate that is pre-put away inside the framework data. In such a framework, a man who wishes to be perceived cases a character—for the most part by means of a Stick, login name, keen card, or something like that—and the framework directs a balanced correlation with find regardless of whether the claim is valid. The framework check mode answer regardless of whether individual is that individual or not. Personality check is regularly utilized for constructive acknowledgment, wherever the point is to keep different people from utilizing an identical character.

Or on the other hand in distinguishing proof mode, the framework perceives a man via scanning the entire format data for a match. The framework directs a one-to-numerous correlation with build up a person's character (or comes up short if the subject isn't enlisted inside the framework database). The inquiry being addressed is, "Who is this individual?" Distinguishing proof could be a fundamental piece of pessimistic acknowledgment applications, inside which the framework builds up regardless of whether the individual is who she (verifiably or expressly) denies being. The motivation behind adverse acknowledgment is to thwart one individual from utilizing different characters. ID additionally can be used in positive acknowledgment for comfort (on the grounds that the client isn't required to assert a character). While the standard methods for individual acknowledgment like passwords, PINs, keys, and tokens work for positive acknowledgment, exclusively biometrics will be utilized for negative acknowledgment.

BIOMETRIC ERROR AND ISSUES

A biometric check framework can make two kinds of mistakes [5]:

• Mixing up biometric estimations from two unique people to be from a similar individual (called false match or false acknowledge).

• Mixing up two biometric estimations from a similar individual to be from two unique people (called false non-coordinate or false reject).

Issues of biometric framework which manages all biometric modalities are on assessing framework execution and another on biometric quality [6]. A portion of the confinements of the current strategies for assessment of biometric confirmation are because of exact observational examinations which are done on little or medium size of databases, factual displaying apparatuses can be utilized to gather the execution of biometric framework when the database estimate is substantial by utilizing another model of arbitrary impacts show together with a Bayesian derivation strategy [7]. Nature of biometric test is likewise a vital factor to conquer a portion of the issues which are looked in biometric framework because of the determination of test information for biometric handling. The term quality isn't utilized to allude to the devotion of the example be that as it may, rather, to the utility of the example to a mechanized framework: A great quality example is portrayed by high "matchability"[8]. There are numerous procedures for determination of value tests, for example, test substitution, calculation choice, edge adjustment, and so forth could be misused which will bring about change of general biometric framework execution. The nature of test information can be characterized in three terms; character: which characterizes the properties of the source, loyalty: which characterizes the unwaveringness to the source, and utility: anticipated commitment to execution. By increment in the nature of test information will gives bring down false dismissal rates and furthermore give less number of measurably unmistakable levels of execution.

BIOMETRIC TECHNIQUES

We can classify biometric techniques into two classes [3].In the first place is behavioral based methods which are Mark acknowledgment, Voice acknowledgment, Penmanship acknowledgment, Keystroke elements examination, Step investigation, and Hand signal acknowledgment. Second is Physiological-based techniques are Fingerprint recognition, Iris and retina scans recognition, Face recognition, Hand shape recognition, Palm-print recognition, Tongue shape recognition, Ear shape geometry, Human body shape, Vein pattern, Nail bed recognition, Odor recognition, Lips recognition, Hip-print authentication, Heart sound authentication and DNA.

Fingerprint recognition:

- Strengths: most widely used technology, proven technology capable of high accuracy, ability to enroll multiple fingers, wide range of deployment environments.
- Considerations: perception of law enforcement, forensic uses, impaired or damaged fingerprints, may require additional hardware and software, standards needed for interoperability.

Iris recognition

- Strength: Highly reliable, hands-free operation, high stability of characteristic over lifetime, is a rich source of biometric data, successful tests in air travel.
- Consideration: acquisition of iris image requires more training and attentiveness than most biometrics, hardware and software licensing costs, glasses with strong lenses may impact performance, potential for false non-matching.

Hand geometry

- Strength: ready to work in testing situations, set up, solid center innovation, saw as non-meddling
- Consideration: design complicate usage by certain populations, perception of bio-hazard, passing germs, possible hand changes over time.

Face recognition:

Face Location strategies partitioned into classes [9]. Yan, Kriegman and Ahuja introduced a characterizations that is very much acknowledged. Techniques are isolated into four classifications. These classifications may over-lap, so a calculation could have a place with at least two classifications. This characterization can be made as takes after: Learning based strategies: Decided based techniques that encode our insight into human countenances. Highlight invariant strategies: Calculations that attempt to discover invariant highlights of a face in spite of its edge or position. Format coordinating strategies: These calculations contrast input pictures and put away examples of countenances or highlights. Appearance-based strategies: A format coordinating technique whose example database is learnt from an arrangement of preparing pictures.

- Strength: may work without client consistence, use existing picture databases, just innovation fit for ID at a separation and reconnaissance.
- Consideration: Susceptible to high false match rates in one-to-one and one-to-many applications, lighting, camera angle reduce matching accuracy, changes in physiological characteristic reduce matching accuracy.

COMPARISON OF BIOMETRIC

Physical and Behavioral attributes should meet a few necessities with a specific end goal to be utilized as biometrics strategies. These prerequisites are either hypothetical or viable [4]. Hypothetical necessities include:

- Universality: Every individual ought to have the biometric trademark.
- Distinctiveness: Any two people are not equivalent as far as the trademark.
- Permanence:The trademark continues as before after some time or has not sudden changes.
- Colectabillity: The trademark ought to have the capacity to be estimated quantitatively.
- The viable prerequisites are customarily identified with the usefulness of the computational frameworks.
- Performance: The achievable acknowledgment precision and speed that the biometric framework can accomplish.
- Acceptability: The acknowledgment of the end-clients in utilizing the biometric framework in their everyday lives.
- Circumvention: The level of security of the framework given fake assaults.

Table: 1. *Comparison of biometric*

Biometric	Fingerprint	Face	Hand Geometry	Iris	Voice	Signature
Boundaries in Acquisition	Dirt, Dryness	Hair, Glasses, Age	Hand injury	Poor Lighting	Noise, clouds	Ink, Stroke
Universality	Medium	High	Medium	High	Medium	Low
Distinctiveness	High	Low	Medium	High	Low	Low
Permanence	High	Medium	Medium	High	Low	Low
Collectivity	Medium	High	High	Medium	Medium	High
Performance	High	Low	Medium	High	Low	Low
Acceptability	Medium	High	Medium	Low	High	High
Circumvention	Low	High	Medium	High	Low	Low

Factors of Evaluation for Biometric techniques

False acknowledgment rate (FAR) and false match rate (FMR): The likelihood that the framework erroneously announce an effective match between the information design and a non-coordinating example in the database. It gauges the percent of invalid matches. These frameworks are basic since they are ordinarily used to preclude certain activities by refused individuals.

False reject rate (FRR) or False non-coordinate rate (FNMR): the likelihood that the framework mistakenly announce disappointment of match between the information design and the coordinating layout in the database. It gauges the present of substantial sources of info being rejected.

Relative working trademark (RWT): by and large, the coordinating calculation plays out a choice utilizing a few parameters (e.g. a limit). In biometric frameworks the FAR and FRR can commonly be exchange off against each other by changing those parameters. The RWT plot is acquired by charting the estimation of FAR and FRR, changing the factors verifiably. A typical variety is the Discovery Mistake Tradeoff (DET) which is gotten utilizing ordinary go amiss scales

on the two tomahawks. This more straight diagram lights up the distinctions for higher exhibitions (uncommon mistakes).

Approach Mistake Rate (AMR): The rates at which both acknowledge and reject blunders are equivalent. ROC or DET plotting is utilized in light of the fact that how FAR and FRR can be changed, is demonstrated unmistakably. At the point when snappy examination of two frameworks is required, the Fail is generally utilized. Acquired from the ROC plot by taking the point where FAR and FRR have a similar esteem. The lower the EER, the more exact the framework is thought to be.

Inability to Enlist Rate: The level of information input is viewed as invalid and neglects to include into the framework. Inability to select happens when the information acquired by the sensor are viewed as invalid or of low quality.

Inability to Catch Rate: Inside programmed frameworks, the likelihood that the framework neglects to recognize a biometric trademark when displayed effectively is for the most part regarded as FTC.

Format Limit: It is characterized as the most extreme number of sets of information which can be contribution to the framework.

LIMITATION OF SINGLE BIOMETRIC MODEL

There is several limitation of using unimodel biometric techniques because where one system can work other system may not work [4].

Noise in sensed data: the data collected for identification or authentication process in acquisition stage may scanned with some noise, like dirt particle on fingerprint scanner which may lead to filling of gaps result in loss of minutia points values, or sound quality for voice recognition due to cold, etc.

Intra-class variations: there may be chance that the template data which is collected at the template registration varies with the sample for verification due to change in orientation of data or due to high change in lightning condition.

Distinctiveness: The template data for any type of biometric technique must be unique among individuals. But there can be some inter-class similarities in the feature sets. Hand geometry and face techniques have information contents or distinguishable patterns of high order of 10^5 and 10^3 respectively [10]. Thus Golfarelli et al. states that every biometric trait has some theoretical upper bound in terms of its discrimination capability.

Non-universality: There are chances that some of the features extraction from the individuals is not possible, due to poor quality of the ridges in fingerprint. Thus, result in failure to enroll (FTE) rate for single model biometric system.

Spoof attack: Biometric templates can be spoofed by an impostor and result in circumvent the biometric system. Spoof attack is mostly seen with the behavioral traits of biometric such as voice can be taped or signature can be copied with practice. However, the physical trait of biometric are also in spoof attack categories such as construction of artificial fingerprint [11].

CHALLENGES IN FACE RECOGNITION

There can be a challenge for face recognition of different image of single individual when there is a variation between faces due to poor or different illumination and if the view angle or posture of face is different [12]. The accuracy of system degrades with variation

of pose, expression, resolution, and illumination. Some of the advances have been there in system to improve recognition ration like use of eigenfaces, fisherfaces, active appearance models, and local binary patterns. Other challenges that are faced in forensic face recognition are facial aging, facial marks, forensic sketch recognition, and face recognition in video and near infrared face recognition.

FACE RECOGNITION TASKS

There are two major tasks that can be performed by human recognition system are verification or authentication and identification [13].

Check or confirmation is where balanced coordinating is performed wherein a man cases to be known to biometric framework. The facial element of the test (person whose check/confirmation is to be distinguished) is thought about against the display (database of individuals known to the framework). In the event that the likeness score between the two information is more prominent than the predefined edge, the petitioner is recognized as the guaranteed substance, generally dismissal as a sham. The execution of confirmation framework is accounted for in term of a beneficiary working trademark (ROC) bend and it is a plot of connection between the FAR and FRR [14].

Distinguishing proof process is one-to-numerous coordinating where an individual or test is coordinated inside the display (database) of all people and the nearest coordinates in exhibition are found. The execution of ID framework can be assessed as far as a total match qualities (CMC) bend [15].

3D FACE RECOGNITION SYSTEM PROCEDURE

It consist of following steps, firstly image acquisition step is performed where the image of face is captured and its 3d model is generated, secondly the pre-processing is done to normalize images into the same position, in third step the features are extracted from the normalized face images from the previous step, and lastly the classification where we design a classifier based on the feature extracted from the third step and perform the training of classifier with the dataset and validate for the classifier by performing several test operation.

3D Facial Model Acquisition

Acquisition of 3D facial model can be acquired in both active and passive technique. In active techniques, widely used is laser range finder [16, and 17]. A laser range finder recorder the reflection generated from the object on which light is projected. The depth detail of the object surface nearest to the camera is determined by triangulation. This technique generates more dense and accurate 3D facial mode, but with some restrictions like take long time for acquisition process, unsuitable for high screening application, requires stability of object surface and is intrusive for human eyes in process. The passive techniques include stereo imaging [18] and approaches based on structural light [19]. In stereo imaging different camera capture a face from different viewpoints. The depth detail is determined using camera calibration and great difference information determined from different viewpoints of camera. In the structured light approach, we use standard light patterns is projected on to the scene. Triangulation process is applied over deformation of the light pattern and camera calibration parameters to generate the depth at each point in the scene.

Another approach that can be used when there is only one or two image of scene (facial) is available in 2D; we can generate the 3D facial model by performing the morphing generic 3D facial model [20 ,21, 22 and 23].

Types of 3D facial model data

- Point-Cloud representation: the dataset are of point cloud where is 3-D coordinates (x,y and z) of the point of a face object. A face with M samples is simply represented in 3-coordinate vectors of x, y, and z of length M.
- Range Image: also referred to as a 2.5D surface or depth map, it is using linear interpolation, the z coordinate of the face points are mapped on a regular x-y grid. And, it has the same function as of the 2D function form I(x,y), where I is intensity. The function **is invariant to the change of illumination and color.** It can be produced by orthographic projection of surface meshes or 3D point cloud.
- Surface-normal based: the facial point cloud dataset is normalized using a 'n' value over a 3D-coordinate (nx, ny, nz) uint normal vector.
- Curvature based representation: The 3D vector and their derivatives are used, i.e., the mean (H) and Gaussian (K) curvatures are extracted from each facial surface point. The curvature based dataset are **invariant to rotations.**
- 3D voxel representation: The point cloud data is converted into a voxel structure, that can be denoted by Vd(x,y,z), by imposing a lattice.

Why Multi-model (face and fingerprint recognition) system?

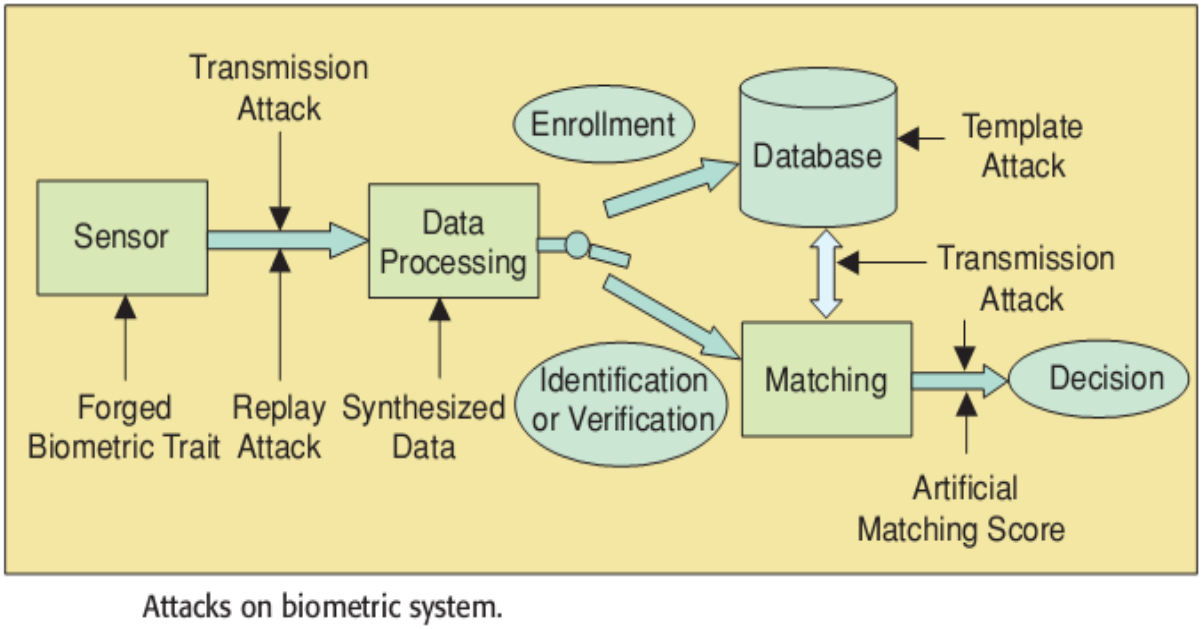
There are many techniques for biometric identification, but among all iris and fingerprint recognition techniques are best suited with high accuracy [24]. The only issue faced by these techniques that they require subject cooperation for data collection. Both of the techniques cannot be done over a surveillance system. Mostly biometric identification is done over some distance from the subject, so face recognition as a biometric modality requires less subject cooperation. Biometric system also requires better accuracy over surveillance applications and low cost components.

BIOMETRIC THREAT MODEL

A general biometric system can be designed as a pattern recognition system. There can be several types of attack that can be done over this system in many other stages [25, 26]. There are eight types of basic attack on generic biometric system. While there can be many other types of abuses of biometrics as discussed in [27].

- Forged Biometric trait attack: First type of attack can be done at the data acquisition stage of biometric system over sensor that collects data for identification or verification process. The false data can be easily generated like fingerprint, signature, face model in 2D or 3D, Gait, etc.
- Replay attack: In this attack, the old sample data is again provided to the biometric system bypassing the sensor or data acquisition phase.
- Transmission attack: This attack primarily extracts the original data that was acquired by the sensor or first stage of the system when the authorized person is providing the sample data for his/her identification or verification process.
- Synthesized Data/Override feature extract attack: There can a situation where the attackers intrude the system with some Trojan horse so that it would produce feature sets chosen by the hacker.
- Tampering with the feature representation attack: This attack uses the synthesized feature set rather than the feature extracted from the input signal. In biometric system there can be a situation where the extracted features are transmitted to another machine over a network, in that case it's easy to snoop on the TCP/IP stack inside the computer and alter certain packets.

- Matching override attack: There can a situation where the matching operation is attacked and it will always produce an artificially high or low match score.
- Template attack: The database of the template can be local or remote database or in distributed server. There can be direct attack over the database template which is used to authenticity of the person. This attack can be performed while at the time of template enrollment or afterwards it is stored. Some fraudulent person might get access to service or denial of service.
- Artificial matching score/ Decision override: At last the final decision made by the matcher function can be overridden by the attacker which can result in very dangerous situations. Whether the biometric system performs very effectively but the final decision can be forged.



Attacks on biometric system.

Fig: 1.*Attacks on biometric system*

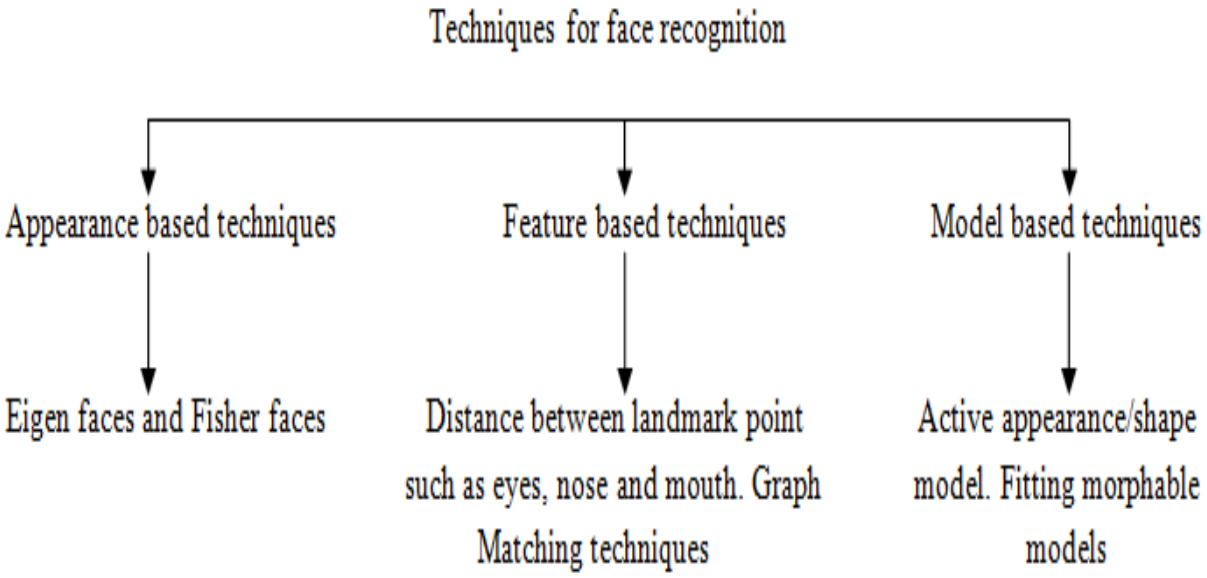


Chart: 1. *Technique for face recognition*

Why 3D face model for face recognition is better as compare to 2D face recognition system?

The functioning and cost for construction of 2D face recognition is easy and cheap respectively, whereas it is inadequate for robust face recognition system. FRVT 2002 test operation with HCINT (121,589 images from visa applicants collected from year 1996 to 2002) and MCINT (from NIST,NSWC, USF between year 1999 to 2002) data set was used to perform evaluation of several types of algorithms for their performance over different ambient illumination condition, or changeable facial pose. Among all, best three algorithms result was dropped to half with such varying condition of facial data set [28].

The issue and performance of algorithms over varying illumination and facial pose variation is improved when synthetic 2D frontal face image generated by employing 3D morphable model of the face is used to perform face recognition [29]. So it was concluded at that time the use of 3D face model is potential solution for varying pose issue for face recognition. The 3D faceRecognition system can devise either by using 3D algorithm or conjunction of 2D + 3D algorithm [30 and 31].

FINGERPRINT RECOGNITION INTRODUCTION

In Biometric recognition is classified on physiological and behavioral based. Fingerprint recognition is physiological based technique, attributes of fingerprints are extensively studied in biometric literatures and various techniques have been proposed and implemented for fingerprint recognition.

Fingerprint attributes are vulnerable to various types of attacks (including impersonation and obfuscation [32, 33]). Obfuscation of fingerprint refers to the intentional alteration of fingerprint attributes (burning or cutting of fingertips) to violate and hide from the watch-list (in criminal activities). The fingerprint attributes can also be imitated, by removing the portion of skin from the fingertip. Impersonation refers to the duplication of fingerprint, or referred as spoof artifacts. The fingerprint sensor-level attack is done by using well-duplicated fingerprint on sensor to gain access by an unauthorized user over a user (whose fingerprint used as spoof artifacts) who is enrolled in system as authorized user. There can be a spoof attack where using new attributes of fingerprints are enrolled into the system and gain access to unauthorized services.

Several anti-spoof measures have been studied for fingerprint recognition against artificial fingerprint generated from gelatin, moldable plastic, and silicon[34]. Spoof detection is an important aspect for designing anti-spoofing measures. The detection refers to the capability to identify whether the object placed on the fingerprint sensor system is a live finger or not [35].

Fingerprint characteristics and Acquisition

The fingerprint tip consists of features like ridges and valleys can be represented by using the global details like finger ridges or with local detail (characteristics of ridges on fingertip).

The fingerprint characteristics are classified at four levels. The first level discuss about the global detail of properties, like pattern type of ridges and valley. And, we can find distinct shape of ridges like loop, delta, or whorl. Second level consist of details related to ridge ending (minutiae point represented by its location in (x, y) and direction at location as (θ)) and its bifurcation (Galton characteristics). Third level defines the very fine level, details such as sweat pores and incipient ridges can be fetched from

the fingerprint image [36]. [37] On the basis of the position of the ridges, we can define a pore as open or close. At the ridges the pore is opened, whereas the closed pore is considered at the intersection of pore valley.

The acquisition of fingerprint attributes are done by using different technologies, and studied in literature [36]. First technique is by using optical sensor, where total internal reflection of sensor is done by placing finger on transparent prism, ridges absorb the light illuminated through one side of the prism, and the valley reflects the light. Spoof attacks can be done on this technique by using a material similar to the reflection property of skin. Capacitive devices are the second technique for acquisition of fingerprint where the finger is treated as the upper electrode and the metal plate is lower electrode. The difference of capacitive value between skin sensor and air sensor contact is used to calculate the ridges and valley of a fingertip for recognition. It's also vulnerable to the spoof attack.

Third technique is thermal sensor, where the temperature change due to contact of ridges to the thermal sensor chip and no change at valley as they are not in direct contact to the chip is calculated for generating the fingerprint. Fourth type of acquisition technique is ultrasound sensors, where the acoustic impedance is calculated between the ridge and valley by transmitting the acoustic waves towards the fingertip and the reflected wave or signal is measured at the receiver sensor. The spoofing of ultrasound sensor is more vulnerable to the artificial fingerprint where the property of material is equivalent to the response to acoustic wave of original finger.

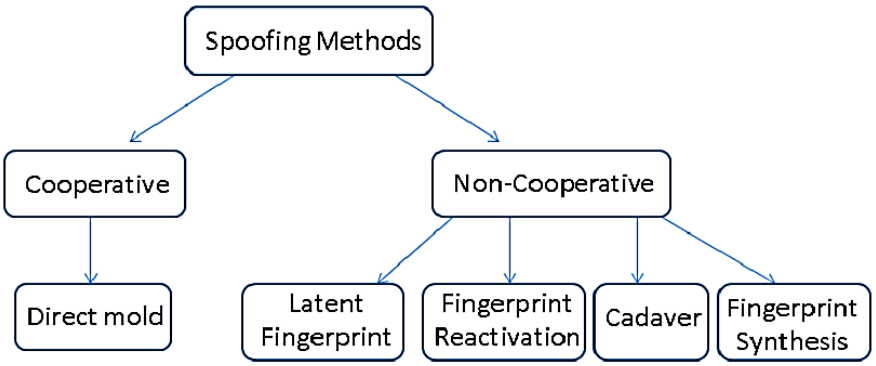


Fig: 2. *Spoofing/ artificial fingerprint methods*

Spoofing techniques of fingerprint can be classified under main categories of Cooperative and Non-cooperative mode. In cooperative method, the original fingertip is available to create an artificial fingerprint for performing spoofing. And in non-cooperative the physical availability of fingertip is not possible, so latent fingerprint is generated for spoofing [38, 39].

Cooperative spoofing: the spoofing is done by using the live finger mold. The finger of live is available for generating the mold by applying pressure on the plaster or dental impression material, and the mold is generated and if any correction is required before generating the artificial fingerprint is done there itself. Afterwards, the mold is filled with gelating or liquid silicon and the spoof is produced [40].

Non-Cooperative spoofing: There can be situation where physical presence of finger is not possible to generate its fingerprint or spoofing. There are several techniques by which spoofing can be done in non-

cooperative environment. First method is based on using latent fingerprint, where the fingerprint pattern is lifted from the object by the use of powder. The fingerprint which is not visible by eyes is visualized by powdering with a brush using powder. The fingerprint can be used on sensor thereafter. Another technique under latent fingerprint is based on photolithographic printed circuit board model. The fingerprint is enhanced by brushing with a black powder, and photographed and printed on a transparency for creation of mask for engraving the PCB. The mask is exposed to UV light, and the plaster cast is filled with silicon rubber to create wafer thin layer of fingerprint and can be used by placing the layer above live finger on the sensor. Last technique under latent fingerprint is based on recent technology which provides the ability to lift the fingerprint from the surface within few seconds. Example of such technique is based on electrospunnanofiber mat [41].
Second method is fingerprint reactivation by fetching data from the sensor, the graphite powder is used to reactivate the fingerprint deposited on a sensor. The sensor again sense the fingerprint and spoofing is done. Third technique is cadaver, where fingerprint is taken from the dead finger of a person. There can be scenario where authorization to some services even after their death.

Fourth technique is fingerprint synthesis by use of the fingerprint template (minutiae points) of a person whose services are enrolled in system [42]. The reversibility of the fingerprint template (minutiae) has been studied in several literatures [43, 44]. Once fingerprint is derived from the minutiae template, it can be transferred to a spoof artifact.

The involvement of the person cooperation, leads to the better quality of the artifacts as compare to the noncooperation techniques. But involvement ratio is less of person as cooperation technique, and the quality of the satire unique finger impression is likewise influenced by the weight of the finger on the cast and contact of finger on the sensor surface, these may bring about the changed or false unique finger impression shape. The nature of the shape is additionally a central point in parody quality. Both capacitive and optical gadgets are more powerless against the previously mentioned parodying methods contrasted with warm sensors. Besides, silicon fingerprints are generally dismissed by capacitive sensors however they represent a danger to optical sensors, while the conduct of these two sensors is inverse on account of gelatin fingerprints [45].

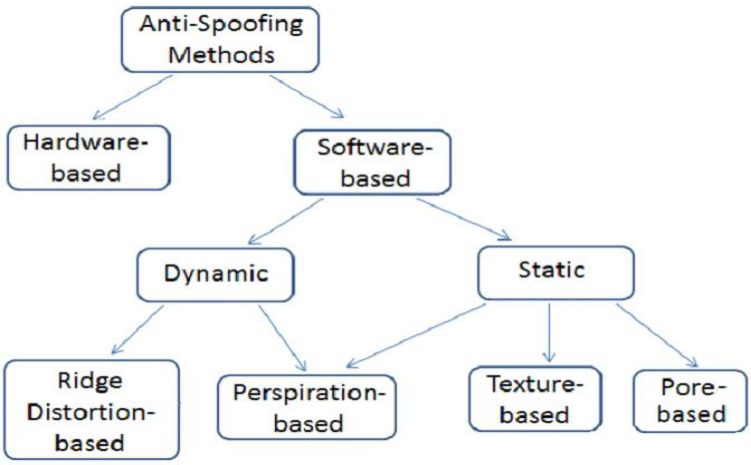


Fig: 3. *Anti-Spoofing methods for Fingerprint*

Anti spoofing perform the liveness detection of fingerprint to address the issues of spoofing and can be classified on the basis of hardware or software based as shown in above figure.

Hardware based techniques exploits the characteristics such as temperature of finger, electrical signal conductivity, pulse detection by oximeter and skin resistance [46]. The anti spoofing technique based on hardware required extra hardware with the biometric sensor which leads to the cost increase. But there are possibilities if the integration of extra hardware is improper. In very challenging scenario Electo-tactile signals are observed as response to finger electric pulses transmitted into the fingertip during process. In odor based technique the different sensor of chemical are used, when the finger is placed on the sensor, the voltage decrease when skin or gelatin is exposed to the sensor and voltage increases when the spoof artifact of silicon or latex is used [47]. OCT (optical coherence tomography) is studied in several literatures for detection artificial material use for spoofing optical fingerprint. The OCT is used to study the feature of the upper layer of skin as well as the internal features of multi layered tissue structure [48, 49, 50, and 51].

Software based techniques for exploiting the dynamics behavior of the live fingerprint such as ridge distortion, perspiration and static behavior of finger such as textural characteristics, ridge frequencies, and elastic property of skin [52].

The dynamic behavior of fingerprint images are taken over time duration and the difference between them are analyzed. Perspiration based method is studied over live finger, where the region between pores becomes dark due to sweat from pores. The live finger shows the non-uniformity of gray level along ridges due to sweat or perspiration form pores. Whereas, spoof fingerprints shows high uniformity even over time. Ridge distortion based method studied where the distortion in fingerprint ridges are studied when pressing and moving a real finger over a scanner, and in spoof fingerprint the distortion is less in this.

The static behavior for fingerprint is cheaper and faster as compare to dynamic behavior, where single print impression is compared. Features such as textural features, skin elasticity, and perspiration based features are used. Texture based method studied such as morphology, smoothness and orientation over live and spoof fingerprint. The noise presence in the fingerprint images is used to differentiate between live and spoof image, where the presence of noise features are due to the coarseness of the fake finger surface [53].

Pore based strategy is contemplated in writing where discovery of pores are finished by applying the sifting methods, for example, high pass and connection channels [54]. The working of high pass channel is utilized to extricate dynamic sweat pores, and a connection channel was utilized for finding the situation of pores in unique mark. The amount of pores amongst live and parody unique mark picture can be utilized to recognize and distinguish parody information [55].

Challenges in fingerprint recognition

- All the anti-spoofing techniques are designed by comparing and analyzing both live and spoof fingerprint, but if the material for generating the spoof fingerprint is unknown there may be chance that current techniques may not work, so generating the countermeasure for spoof detection with no impact of spoof fabrication material.

- The involvement of human factor interaction at the time of fingerprint acquisition on sensor may change the result of spoof detection algorithm, factors such as angle of placement, pressure, environmental condition such as humidity and temperature may affect the performance of algorithm.
- Fusion of spoof detection with verification system is one of the case, where the system should reject the spoof fingerprint and increase the FNMR (false non-match rate).
- At present sensors may not be able to detect the spoof fingerprint of material which is unknown. So, change in sensors are also needed for future spoof detection.

DECISION FUSION

Choice combination which incorporates numerous prompts has demonstrated useful for enhancing the precision of an acknowledgment framework [56], [57]. For the most part, numerous prompts might be coordinated at one of the accompanying three distinct levels:

1. Theoretical level; the yield from every module is just an arrangement of conceivable names with no certainty related with the names; for this situation, the straightforward dominant part control might be utilized to achieve a more solid choice;
2. Rank level; the yield from every module is an arrangement of conceivable names positioned by diminishing certainty esteems, however the certainty esteems themselves are not indicated;
3. Estimation level; the yield from every module is an arrangement of conceivable marks with related certainty esteems; for this situation, more exact choices can be made by coordinating distinctive certainty measures to a more educational certainty measure.

CONCLUSION

In this Research we have considered various methods which are used to perform biometric study of human based on various feature and characteristics. We have thoroughly studied about biometric analysis on fingerprint data, as it is reliable and do not change or degrade with time.

REFERENCE

1. Wood, H.M. "The use of passwords for controlled access to computer resources" National Bureau of Standards Special Publication 500-9, US Dept. of Commerce/NBS.
2. Anil K. Jain,Arun Ross, and SalilPrabhakar, “An Introduction to Biometric Recognition”, IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, No. 1, January 2004.
3. SalilPrabhakar, SharathPankanti and Anil K. Jain,” Biometric Recognition: Security and Privacy Concerns”, IEEE Security & Privacy, March/April 2003.
4. SalilPrabhakar, Josef Kittler, DavideMaltoni, Lawrence O’Gorman, and Tieniu Tan, “Introduction to the Special Issue on Biometrics: Progress and Directions”, IEEE Transactions on Pattern Analysis and Machine Intelligence, VOL. 29, NO. 4, APRIL 2007.
5. SinjiniMitra, MariosSavvides, Anthony Brockwell, “Statistical Performance Evaluation of Biometric Authentication Systems using Random Effects Models**”,**
6. Patrick Grother and ElhamTabassi,”Performance of Biometric Quality Measures”, Pattern Analysis and Machine Intelligence, IEEE Transactions on (Volume:29 , Issue: 4)
7. M.-H. Yang, D. Kriegman, and N. Ahuja. Detecting faces in images: A survey. IEEE Transactions on Pattern

Analysis and Machine Intelligence, 24(1):34–58, January 2002.
8. M. Golfarelli, D. Maio, and D. Maltoni, “On the error-reject tradeoff in biometric verification systems,” IEEE Trans. Pattern Anal. Machine Intell. , vol. 19, pp. 786 –796, July 1997.
9. T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, “Impact of artificial gummy fingers on fingerprint systems,” Proc. SPIE, vol. 4677, pp. 275–289, Feb. 2002.
10. Y. Moses, Y. Adini, and S. Ullman. Face recognition: The problem of compensating for changes in illumination direction. In European Conf. on Computer Vision, pages 286–296, 1994.
11. P. J. Phillips, H. Moon, P. Rauss, and S. A. Rizvi. The feret evaluation methodology for face-recognition algorithms. InComputer Vision and Pattern Recognition, 1997. Proceedings., 1997 IEEE Computer Society Conference on, pages 137–143, 1997.
12. S. A. Rizvi, H. Moon, and P. J. Phillips. The feret verification testing protocol for face recognition algorithms. InAutomatic Face and Gesture Recognition, 1998. Proceedings. Third IEEE International Conference on, pages 48–53, 1998.
13. P. J. Phillips, H. Moon, S. A. Rizvi, and P. J. Rauss. The feret evaluation methodology for face-recognition algorithms. Pattern Analysis and Machine Intelligence, IEEE Transactions on, 22(10):1090–1104, 2000.
14. K. I. Chang, K. W. Bowyer, and P. J. Flynn. An evaluation of multimodal 2d+3d face biometrics. Pattern Analysis and Machine Intelligence, IEEE Transactions on, 27(4):619–624, 2005.
15. X. Lu, A. K. Jain, and D. Colbry. Matching 2.5d face scans to 3d models. Pattern Analysis and Machine Intelligence, IEEE Transactions on, 28(1):31–43, 2006.
16. S. Lao, Y. Sumi, M. Kawade, and F. Tomita. 3d template matching for pose invariant face recognition using 3d facial model built with isoluminance line based stereo vision. InPattern Recognition, 2000. Proceedings. 15th International Conference on, volume 2, pages 911–916 vol.2, 2000.
17. C. BenAbdelkader and P. A. Griffin. Comparing and combining depth and texture cues for face recognition.Image and Vision Computing, 23(3):339–352, 2005.
18. V. Blanz and T. Vetter. Face recognition based on fitting a 3d morphable model. Pattern Analysis and Machine Intelligence, IEEE Transactions on, 25(9):1063–1074, 2003.
19. D. Nandy and J. Ben-Arie. Shape from recognition: a novel approach for 3-d face shape recovery. Image Processing, IEEE Transactions on, 10(2):206–217, 2001.
20. C. Zhang and F. S. Cohen. 3-d face structure extraction and recognition from images using 3-d morphing and distance mapping. Image Processing, IEEE Transactions on, 11(11):1249–1259, 2002.
21. M. W. Lee and S. Ranganath. Pose-invariant face recognition using a 3d deformable model.Pattern Recognition, 36(8):1835–1846, 2003.
22. N. K. Ratha, A. Senior, R. M. Boile, S. Singh, N. Murshed, and W. Kropatsch. Automated biometrics. In S. Singh, N. Murshed, and W. Kropatsch, editors, Advances in Pattern Recognition - ICAPR 2001. Second International Conference. Proceedings (Lecture Notes in Computer Science Vol.2013), pages 445–453. Springer-Verlag, IBM

Thomas J. Watson Res. Center, Yorktown Heights, NY, USA, 2001.
23. N.K. Ratha, J.H. Connell, and R.M. Bolle, "An analysis of minutiae matching strength", Proc.AVBPA 2001, Third International Conference on Audio and Video Based Biometric Person Authentication, pp. 223-228, 2001.
24. UmutUludag, Anil K. Jain, "Attacks on Biometric Systems: A Case Study in Fingerprints",
25. B.Schneier, "The uses and abuses of biometrics", Communications of the ACM, August 1999, Vol 42, No.8, pp. 136.
26. P.J. Phillips, P. Grother, R. J. Micheals, D. M. Blackburn, E. Tabassi, and J. M. Bone. Frvt 2002: Overview and summary. available at www.frvt.org, March 2003.
27. V. Blanz and T. Vetter. Face recognition based on fitting a 3d morphable model. Pattern Analysis and Machine Intelligence, IEEE Transactions on, 25(9):1063–1074, 2003.
28. Shalini Gupta, Mia. K. Markey, Alan C. Bovik, "Advances and Challenges in 3D and 2D+3D Human Face Recognition"
29. L. Akarun, B. Gokberk, and A. A. Salah. 3d face recognition for biometric applications. In 13th European Signal Processing Conference (EUSIPCO), Antalya, Turkey, September 2005.
30. Soweon Yoon, Jianjiang Feng, Anil K. Jain, "Altered Fingerprints: Analysis and Detection", IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, VOL. 34, 2012.
31. J. Feng, A. K. Jain, A. Ross, "Fingerprint Alteration", MSU Technical Report, MSU-CSE-09-30, Dec. 2009.
32. A. Abhyankar and S. Schuckers. 2009. Integrating a Wavelet based Perspiration Liveness Check with Fingerprint Recognition. Pattern Recognition 42 (2009), 452–464.
33. M. Sepasian, C. Mares, and W. Balachandran. 2010. Vitality Detection in Fingerprint Identification.Information Science and Applications4 (2010).
34. D. Maltoni, D. Maio, A. Jain, and S. Prabhakar. 2003.Handbook of Fingerprint Recognition. Springer.
35. A. Jain, Y. Chen, and M. Demirkus. 2007. Pores and Ridges: Fingerprint Matching Using Level 3 Features. IEEE Transactions on Pattern Analysis and Machine Intelligence29, 1 (2007), 15–27.
36. T. Fladsrud and R. Sollie. 2004. Circumvention of Fingerprint Scanners. (December 2004).
37. A. Wiehe, T. Søndrol, O. Olsen, and F. Skarderud. 2004. Attacking Fingerprint sensors.Gjøvik University College 200 (2004).
38. http://www.journalofaestheticsandprotest.org/4/fingerprint/fingerprint.pdf
39. S. Yang, C. Wang, and S. Chen. 2011. A Release-Induced Response for the Rapid Recognition of Latent Fingerprints and Formation of Inkjet-Printed Patterns. AngewandteChemie 123, 16 (2011), 3790–3793.
40. A. Franco and D. Maltoni. 2008. Fingerprint Synthesis and Spoof Detection.Advances in Biometrics(2008), 385–406.
41. A. Ross, J. Shah, and A. Jain. 2007. From Template to Image: Reconstructing Fingerprints From Minutiae Points. IEEE Transactions on Pattern Analysis and Machine Intelligence29, 4 (2007), 544–560.
42. J. Galbally, R. Cappelli, A. Lumini, D. Maltoni, and J. Fierrez. 2008. Fake fingertip generation from a minutiae template.19th International Conference on Pattern Recognition (ICPR)(Dec. 2008), 1 –4.

43. M. Sepasian, C. Mares, and W. Balachandran. 2010. Vitality Detection in Fingerprint Identification. Information Science and Applications4 (2010).
44. P. Reddy, A. Kumar, S. Rahman, and T. Mundra. 2008. A New Antispoofing Approach for Biometric Devices. IEEE Transactions on Biomedical Circuits and Systems2, 4 (2008), 328–337.
45. D. Baldisserra, A. Franco, D. Maio, and D. Maltoni. 2005. Fake Fingerprint Detection by Odor Analysis. Advances in Biometrics(2005), 265–272.
46. Y. Cheng and K. Larin. 2006. Artificial Fingerprint Recognition by using Optical Coherence Tomography with Autocorrelation Analysis.Applied Optics45, 36 (2006), 9238–9245.
47. S Chang, Y Cheng, Kirill V Larin, Y Mao, S Sherif, and C Flueraru. 2008. Optical Coherence Tomography used for Security and Fingerprint-sensing Applications.IET Image Processing2, 1 (2008), 48–58.
48. A. Bossen, R. Lehmann, and C. Meier. 2010. Internal Fingerprint Identification with Optical Coherence Tomography. Photonics Technology Letters, IEEE22, 7 (2010), 507–509.
49. S. Dubey, A. Tulsi, S. Chandra, and M. Singh. 2007. Fingerprint Detection using Full-field Swept-source Optical Coherence Tomography. Applied Physics Letters91, 18 (2007), 181106–181106.
50. C. Jin, H. Kim, and S. Elliott. 2007. Liveness Detection of Fingerprint based on Band-Selective Fourier Spectrum. Information Security and Cryptology4817 (2007), 168–179.
51. A. Abhyankar and S. Schuckers. 2006. Fingerprint Liveness Detection using Local Ridge Frequencies and Multiresolution Texture Analysis Techniques.IEEE International Conference on Image Processing (ICIP) (October 2006), 321–324.
52. N Manivanan, S Memon, and W Balachandran. 2010a. Automatic Detection of Active Sweat Pores of Fingerprint using Highpass and Correlation Filtering.Electronics Letters46, 18 (2010), 1268–1269.
53. M. Espinoza and C. Champod. 2011b. Using the Number of Pores on Fingerprint Images to Detect Spoofing Attacks.IEEE International Conference on Hand-Based Biometrics (ICHB)(2011), 1–5.
54. R. Brunelli and D. Falavigna, "Personal Identification Using Multiple Cues," IEEE Trans. Pattern Analysis and Machine Intelligence,vol. 17, no. 10, pp. 955–966, Oct. 1995.
55. J. Kittler, Y. Li, J. Matas, and M.U. Sanchez, "Combining Evidencein Multimodal Personal Identity Recognition Systems," Proc. FirstInt'l Conf. Audio Video-Based Personal Authentication, pp. 327–334,Crans-Montana, Switzerland, Mar. 1997.

Recognition Systems," Proc. FirstInt'l Conf. Audio Video-Based Personal Authentication, pp. 327–334,Crans-Montana, Switzerland, Mar. 1997.