INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT (IJSREM)
VOLUME: 06 ISSUE: 12 | DECEMBER - 2022 IMPACT FACTOR: 7.185 ISSN: 2582-3930

Non-Live Finger Print and Its Detection Methods

Mrs S.Subhashini , Research Scholar , Anna university Regional campus, Madurai

Mrs.P.Rajeswari, Assistant Professor, Dept of computer science , Mannar Thirumalai Naicker College, Madurai

***Abstract*— Finger print scanners are widely used to provide security in various fields such as defence control, immigration and law enforcement , health and subsidies, business transactions, forensics for identifying criminal and prison security , Banking security, Physical access control, Information system security, customs and immigration , population, verification of voters identity etc ., Because of uniqueness of finger print image and ease of use, it is extensively used for security in biometric systems. Usage of these systems have grown steadily and used as an alternative to passwords, personal identification number(PIN), key and tokens . Though these systems are more user friendly and widely used for security , they are more vulnerable to be hoaxed with non live finger print images by skilled imposters . Fraudsters can take off someone's identity or to obscure his own identity when they want to spoof biometric systems . Artificial fingerprints are created using low-cost hardware and software . Thus any secure biometric system must contain spoof detection module, which differentiates live and non live finger print images. Non live fingerprint detection techniques distinguishes between live and non live finger print images. Biometric authentication systems are now extensively used and non live fingerprint detection has become crucial.This article critically review the non live finger print detection methods and also effectiveness and possible limitations of these methods.**

***Index Terms*— Artificial material , Bio metric systems , Hardware based methods, Non live finger print detection , Software based methods.**

I. INTRODUCTION

A fingerprint is an impression which is left by the friction ridges of a finger on human being . It is minute detailed , unique, very difficult to alter. It is durable over the life of an individual. Finger print image is a representation of finger print in digital format. Three types of finger print features are level 1 features , level 2 features and level 3 features.

II FINGER PRINT LEVEL 1 FEATURES

First level features are macro details such as singular points and ridge flow pattern type which describes the direction of finger print ridge flow.

A. Singular points

Singular points are centers of regions where ridge orientation starts. For different impressions of same person's finger print , singular points locations are not unique. They may be same. Two types of singular points are a) Core point b) Delta point.

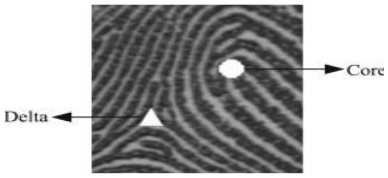

Fig 1 . Level 1- Singular Points

The topmost point on the innermost recurving edge of a finger print is called core point .It is called as an inner terminus. Delta point is a delta-like region which is found on ridge or nearest to the point where divergence of two ridges occur . It is called as an outer terminus. Delta point may be a dot, short ridge, recurving ridge, ending ridge, bifurcation which means meeting of two ridges. It is not located in the mid of a ridge running between the lines toward the core . But it is present at the nearest end only. Two or more number of delta points are present in a fingerprint.

B. Ridge Flow Patterns

Three types of finger print ridge flow patterns are arch , loop and whorl.

1) Arch

Arch is a ridge flow pattern which appears like an arch shape in a finger print . They are of two types

a) Plain arch

Plain arch is an arch like shape ridge flow pattern in which ridges enter into one side of the fingerprint and without backward turn it flow out of another side . It looks like a waveform pattern .

b) Tented arch

It is a ridge flow pattern in which ridges enters one side and it exit from opposite side with an angle or an upthrust (ridge ending). It is similar to plain arch .

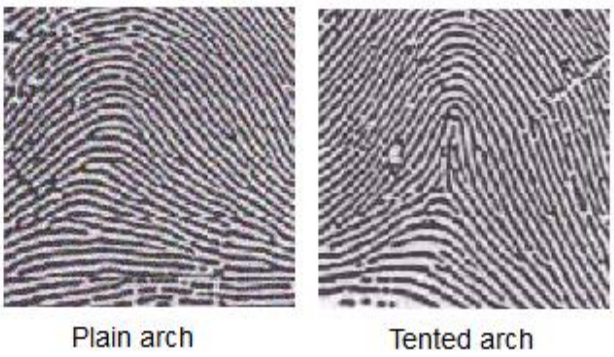

Fig 2. Level 1 - Ridge flow pattern -Arch Types

Singular points and ridge flow pattern are not unique for each finger print. Since they are not unique , they cannot be used for identification. But they can be used for indexing and classification, pattern interpretation and to determine orientation of finger print . Except arch , delta and core points can be defined for all finger print pattern types.

2.Loop

Loop shaped ridge flow pattern present in finger print . In loop , ridges enter on any one of the sides of the fingerprint, recurve, touch the line running from the core point to delta point. It is terminated in the side of the ridge where it has entered. Any loop can contain one delta point, one core point and ridge count.

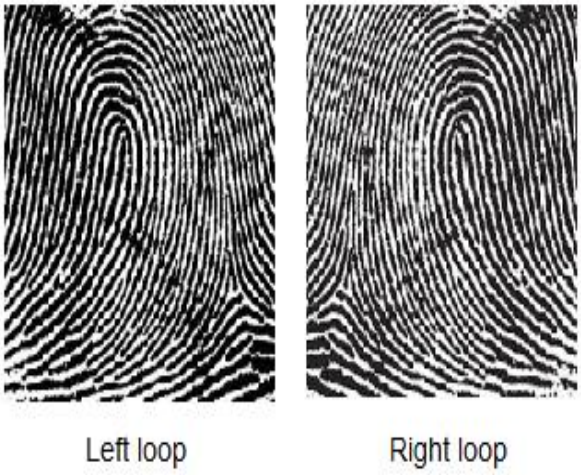

Fig 3. Level 1 - Ridge flow pattern Loop types

3.Whorl

Whorl is ridge flow pattern that looks like a small whirlpool. It is in the form of circular or spiral pattern. Four types of whorl ridge flow patterns are plain whorl , central pocket loop whorl, Double whorl , accidental loop whorl .

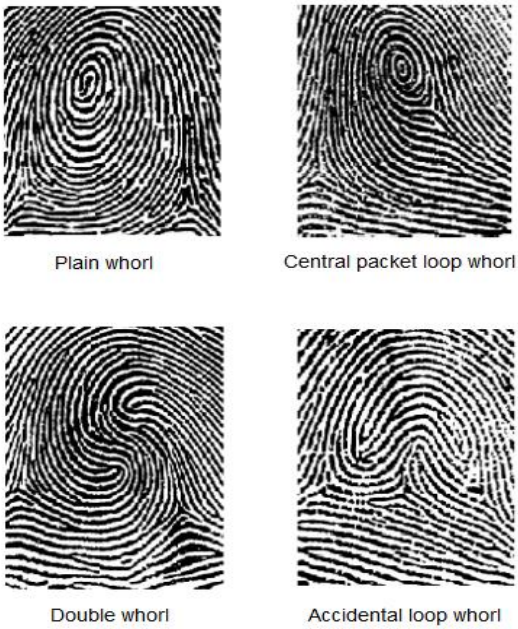

Fig 4 . Level 1- Ridge flow pattern – Whorl Types

a) Plain whorl

It consists of one or more ridges which make a complete circuit. It has two delta points.

b) Central packet loop whorl

In this pattern , whorl is present at the end and make a complete circuit which may be oval, spiral or circular.

c) Double loop whorl

It consist of two distinct separate loops which appears S like pattern.

d) Accidental loop whorl

It has the irregular shape with two different types of patterns.

III FINGER PRINT LEVEL 2 FEATURES

Level 2 features represent local ridge characteristics such as minutiae points . Minutiae are ridge discontinuities of the ridge structure .It is also called as Galton characteristics . They are most widely used for fingerprint representation and identification purpose. When sufficient number of minutiae points are same for two finger print images , then those two finger print images belong to a same person. A single finger print image can consists of 100 minutiae points. There are about 150 different types of minutiae points are available in finger print . Among these, ridge ending and ridge bifurcation are the two most commonly used minutiae points .

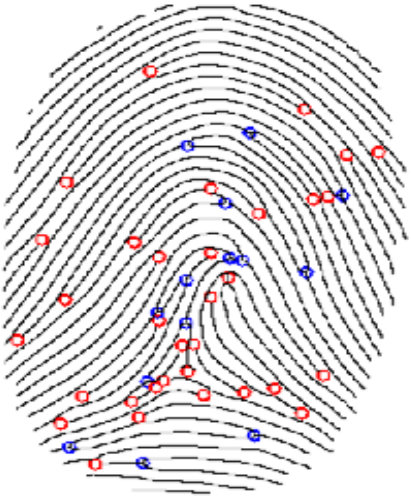

Fig 5 . Level 2 Feature- Minutiae Points

The different types of minutiae points are Ridge end, Bifurcation, Dot, Lake (Enclosure), Spur (Hook), Bridge, Island (Short ridge), Double bifurcation, Trifurcation, Ridge crossing.

a) Ridge end is an end point at which ridge terminates abruptly.
b) Bifurcation is a point of division of one ridge into two ridges.
c) Dot is an isolated ridge with same length and width .
d) Lake or Enclosure is a ridge that splits and rejoins in the same ridge.
e) Spur (Hook) is a ridge bifurcation in which short branching of a long ridge appears.
f) Bridge is a small ridge between parallel ridges.
g) Island is also a short ridge that travels for the short distance .
h) Ridge with two bifurcations is double bifurcation.
i) Trifurcation is a point of division at which one ridge is divided into three ridges.
j) Ridge crossing is a point at which two ridge lines intersect.

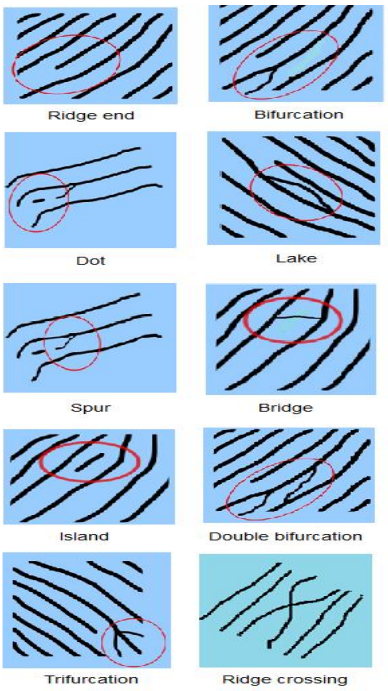

Fig 6 . Level 2 Finger print Minutiae Point Types

IV FINGER PRINT LEVEL 3 FEATURES

Micro level features of finger print images are level 3features . They are fine intra ridge details. Micro level features such as dimensional attributes of a fingerprint ridge such as deviation of ridge path , pores, ridge contour, ridge shape, ridge width, incipient ridges, creases, edge contour , scars and breaks are present. Most frequently used level3 features are ridge contour and pores. The Small sweat pores are present on every ridge of the fingerprint. Open pore and closed pore are two types of pores in finger print. Open pores always appears intersecting valley which exists between two ridges and Closed pores are fully closed by the ridge. Different pores count and distinctive pores shape, position and size are in finger print . Pores are unique so they are used for fingerprint matching process. Total number of pores required to determine the identity of a person ranges from 20 to 40 pores. Ridge contour contains valuable information about ridge width and ridge edge shape

V NON LIVE FINGER PRINT IMAGE AND ITS LIMITATIONS

Fake or artificial finger print images are finger print images created using inexpensive, soft flexible material and they are used as in lieu of real finger print image in biometric systems. Such fake finger print image is known as non live finger print image . They are constructed artificially by the fraudulent imposters . These imposters need representation of original fingerprint to create the artificial finger print image . They use casting material like latex , ecoflex , malleable material like plastic, or wax and other materials like play-doh, silicone, paper , Glue, clay, film, gelatin, rubber, dental impression etc for constructing the

spoof finger print image. In general, artificial finger prints are not moist in nature. But nowadays fake finger print that carries the optical, electrical, and mechanical properties of a live finger are also created using highly sophisticated technologies.

Fig 7 . Dummy fingerprint made by polymer

Fig 8 . Dummy fingerprint made by kitchen powder

Live finger print are clear, moist in nature, good quality of image, exhibits persipiration processes and its sweating processes can be measured . But non live finger print contains noise included in it .Quality of fake finger print image is not good. .No sweat and pores of persipiration present in nonlive finger print . A live finger print will produce more distortion than a spoof. Since there is no perspiration in non live finger print, it shows high uniformity. But live finger print exhibit non uniformity due to persipiration . Now a days non live finger prints are created using paper such as 2D matt and transparent printed paper ,School glue like wood glue, 3M Scotch gel which is a PVA resin-based glue ,Clay compounds like Crayola Model Magic, a well-known water-based modeling compound used by kids called play-doh ,Orange Play-Doh which is close to natural skin reflection , oil-based high precision modeling clay called plasticine, Gelatin is a collagen extracted from skin, bones, and tissues of animals ,Wax - an organic or petroleum-derived compounds ,Silly Putty-a brand of silicone polymers used by kids ,Silly Putty with metallic shade which is used for conductivity sensor ,Silly Putty and glow-in-the-dark paint , Silicones such as Polyvinyl siloxane or Ecoflex rubbers which is used for dental impressions and mold , electrically conductive paint such as bare paint and silicone , Silicone and graphite conductive coating ,Silicone with Colloidal Silver,Silicone and nanotips -conductive polyamide liquid solution that mimics the touch of human skin, used when you have gloves on and want to use your phone, a brand of high-performance silicone rubber dragon Skin which is used for skin effects and molds , Dragon Skin and conductive paint , Dragon Skin and graphic coating, Latex which is a natural rubber used for body paints ,Latex and gold coating etc.

A few limitations of the fake fingerprint image are as follows. Live Fingers create different pressure on the sensor on detection and takes a clear vision of (edge) ridge-valley structure but fake fingerprint contains noise. Due to distinctive elastic characteristics of fake finger print materials , different(weight) pressure is created and hence it produce different distortion than real finger print image . The flexible fake fingerprint has lesser elastic deformation than the real one . The fake fingerprint isn't better in quality contrasted with the genuine unique fingerprint. Spoof finger print do not contain perspiration pores and sweat but they are seen in the live unique fingerprint . Ridge lines of live and non live finger prints (e.g., fun-doh and gummy) have different gray level characteristics due to different characteristics of surfaces of live and non live fingers. Non live finger prints surface texture do not depends on various factors such as elasticity of skin , presence of pores, natural perspiration phenomenon and presence of sweat on surface, etc. Thus ridge pixels of a live finger print exhibit wide and random variation of gray level characteristics . Also there are significant differences in inter-ridge distances and ridge frequencies of live and non live fingerprints. Ridge widths of live and non live fnger print are different . Ridge line discontinuities are present in non live finger print .

Fig 9. a.Real Finger b.Fun doh Spoof c. Gummy finger

VI APPROACHES OF CREATING NON LIVE FINGER PRINTS

Now a days, artificial fingerprints are created using low-cost hardware and software. To create artificial fingerprint images, two different approaches are used , namely the cooperative and non-cooperative methods. In a cooperative approach, authorized user participates in the process and his/her finger is placed in a moulding material and after hardening negative fingerprint pattern is created. Subsequently, this mould is filled with the casting material like latex or ecoflex . Mold is created by pushing subject's finger into a malleable material like plastic or wax and then

mold is filled with a material such as gelatin , Play-Doh or silicone. Authorised user do not take part in non-cooperative method .Without his/her knowledge the fake fnger print is created **.** An attacker typically collect and enhance authorised user's latent finger print left on a surface, e.g., a CD, floor and then photographs it . Latent prints are collected using any one of the latent finger print collection techniques such as fuming , dusting and collecting in fingerprint tape. They use image editing techniques to enhance latent prints. Finally negative image is printed on a transparency print sheet and mold is created . Finally the mold is filled with a malleable material like glue or silicone to get spoof fingerprint.

Fig 10 . Casts

Fig 11 . Molds

VII FINGER PRINT SPOOF DETECTION METHODS

A technique used to evade the biometric scanners security by spoofing with artificial fingerprints is known as finger print spoofing . This Spoofing can even be easier than password cracking. It can be done using inexpensive and easily available material. In 1998 , NETWORK computing reported the first spoofing of fingerprint attack . Fraudsters make sensor spoofing attacks to crack the security of finger print scanners.

Spoof detection or liveness detection is a detection of finger print spoofing attempt by determining whether the given finger print image is a source of authorised user's finger print or fake one. Both live and non live finger prints possess many different characteristics and certain characteristics of live finger prints cannot be duplicated. The distinct features which cannot be duplicated are extracted and used in further analysis for spoof detection . Technologies like machine learning, deep learning and artificial intelligence are also used to bypass the security of scanners. Neural network , machine learning and artificial intelligence techniques are also used to synthesize human fingerprints to fool a touch based fingerprint authentication system.Since many new emerging technologies are used to create spoof , traditional spoof detection methods are not enough to detect finger print spoofing. Two categories of finger print spoof detection techniques are (i) Hardware based spoofing detection (ii) Software based spoofing detection .

VIII HARDWARE BASED DETECTION METHODS

In Hardware-based detection methods, explicit sensors like oxygen saturation sensors, optical coherence tomography scanning systems, multi-spectral imaging frameworks are used to detect whether signals such as the fingerprint temperature, pulse oximetry, sweat, skin distortion, blood pressure or odor are real or not. These hardware sensors are assimilated in to bio metric scanners and it capture both the subject's fingerprint and one or more of the signals to authenticate the user. This detection is more accurate. But this system is more complex and expensive. In hardware based finger print spoof detection methods

a) Skin details are analysed by extremely high-resolution sensors (1000 dpi) by capturing the details such as coarseness of the texture in finger print or sweat pores.
b) Dynamic properties such as blood pulsation ,pulse oximetry , skin perspiration and skin elasticity of finger are analysed.
c) Static properties such as impedance , temperature or other electric measurements etc., of finger are captured and analysed by adding hardware to bio metric scanners.
d) Odor-sensor based non live finger print detection systems are available . Characteristic pattern of an odor are analysed by the chemical sensors and it identifies whether given sample is real or spoof.
e) Pulse oximetry is used to detect spoof finger images by measuring the saturation of oxygen of hemoglobin (%Sp02) .
f) Blood pressure is also considered as a biosignal and it is used for discriminating real and fake finger prints.
g) Pores in live finger print can be caught by large-resolution scanners and event of pores can be interpreted for fake finger detection.

XI SOFTWARE BASED DETECTION METHODS

Software based finger print spoof detection methods are categorized into two classes : 1.feature based detection methods 2. deep learning based detection methods. In feature based detection method, fingerprint liveness is detected by extracting single feature point at an early stage and this method does not obtain good performance result for various fake finger print materials. Deep learning methods are used to detect fake fingerprints for the various types of spoof materials. Software based methods are much cheaper and flexible than hardware based methods . Two main techniques of software based detection are (i) Dynamic based methods (ii) static based methods. In dynamic based methods , two successive images are captured at a finite interval time and multiple frames of same finger print are processed for spoof detection. This dynamic based methods include ridge distortion and perspiration based methods. In ridge distortion based methods, ridge distortion is analysed by processing successive frames in sequence with very high frame rate . At the end of the process, if given finger print is detected as real one it wll contain more distortion than spoof finger print

image. In perspiration based methods, perspiration between skin of finger and other material is detected. As the sweat comes out from pores of the skin and diffuses along the ridges, it makes the region between pores darker. Then the moisture pattern obtained at that stage is captured and analysed . Since there is no perspiration in non live finger print, it show high uniformity. But live finger print exhibit non uniformity due to persipiration . Dynamic based methods are expensive and process in less speed than static methods.In static based methods, skin elasticity , textural characteristics, perspiration based characteristics or combined multiple features are also analysed for spoof finger print detection. Also minutae differences of real and spoof image are also analysed and presence of air bubbles in fingerprint spoof are analysed in static based methods. They use On-device encryption algorithms to encrypt fingerprint data.ata is always in encrypted form before it leaves the device .and fraudsters cannot use the encrypted data. Using Artificial Intelligence based software , tremendous efficiencies can be achieved in finger print spoofing detection. AI based software are easily upgradable for emerging spoofing attacks. Machine learning techniques and deep learning techniques are used for fake finger print detection . Machine learning technique are used to enhance the accuracy classification of live and non live finger prints. Deep learning techniques recognize spoof fingerprints accurately against various fabricated materials used for finger print spoofing and robust against different kinds of spoof forgeries using Play-Doh ,wood glue and Gelatin .

Fig 12. Spoof created with glue contains white air bubbles

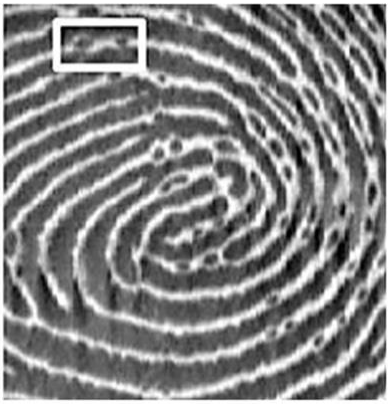

Fig 13. Real finger with minutae details but no air bubbles

X LIMITATIONS OF FINGER PRINT SCANNERS AND SPOOF DETECTION METHODS

Recently developed fingerprint scanners are more efficient for spoof fingerprint detection than ever . But they do not operate optimally in intense light, high radiation, high temperature or wet environment . They cannot easily scan and authenticate dry fingers. It needs regular maintenance to provide optimum performance. The most highly exposed vulnerability is finger print spoofing with artificial fingers created using Play-Doh , gelatin and silicone molds. Very cheap ordinary scanners with basic fingerprint spoofing detection techniques are available but they do not provide complete security. Even optimum fingerprint scanner can not provide complete security when our identity and information are spoofed by fraudsters. Though scanners with hardware based detection mechanisms are very expensive , it provides accurate spoof detection and more security than the ordinary scanners. Bio metric systems are also more vulnerable to cyber attacks , so the security of the finger print scanner is breached. Attackers can attempt SQL code injection attack to exploit finger print database vulnerability by injecting malicious SQL statements. Attacker can also find some vulnerability in biometric database and able to run SQL commands. He/she may manipulate finger print data , shuffle and mix identities of data in the database and more they can do. Spyware are used to steal finger print information from the biometric system

A. Hardware based methods limitations

Hardware based detection methods are accurate but it has disadvantages also. Some of the limitations of hardware based methods are as follows

1. It makes the detection very difficult and several problem arises when additional sensors are used to measure blood flow or pulse in the fingertip for liveness detection of a finger.

2. To spoof sensor , a pipe is added to fake finger and saltwater is pumped through the pipe in order to imitate blood flow .

3. When temperature is used as a liveness feature to differentiate non live finger from a real one , attackers uses artificial fingerprint created using silicone which still works in the sensor's margin temperature level

4. Another hardware-based detection method uses more complex optical sensor . Multispectral imaging technique is used to capture multiple images of fingertip surface and its subsurfaces for spoof detection . These sensor devices are more expensive .

5. Temperature that exist during finger print sample acquisition is considered for authentication detection. But people with blood circulation problem have larger deviation in skin temperature. Due to deviation in temperature , it may cause biometrics systems to be spoofed.

6. Temperature based mechanism fails to distinguish spoof if it is created with a very thin flexible material with good temperature conductivity.

B.Software based methods limitations

Software based methods depends on number of factors such as the finger pressure when applied, environmental moisture on finger , user cooperation when he presses his finger , elastic deformation of the skin etc ., Non live fingerprint recognition based on software extensively depends on the fabricated materials type which are used to create fake fingerprints . In software based detection , most of the general methods uses static extracted features of non live finger print for its detection. Texture based anti-spoofing techniques such as statistical feature analysis, Ridge based features, curvelet transform , Power Spectrum Fourier based features , Local Phase Quantization patterns , Local Binary Patterns etc.,. Many recent spoof detection methods combines multiple features for spoof detection and probably even multiple liveness detectors are combined . Limitations of software based methods are as follows

1. Traditional minutia based detection approach is not robust to detect poor quality fake fingerprint images.

2. Local binary pattern and wavelet-based spoof fingerprint detection does not show very low error rate of detection.

3. Single low level feature-based methods struggles to carry out various spoofing fingerprint materials.

4. Power spectrum-based fingerprint vitality detection shows high error rate of liveness detection.

5. Multiple features extraction is needed to distinguish between live and non live finger print when types of materials used for forgery is not known.

XI CONCLUSION

Though fingerprint authentication has several benefits over other biometric identification techniques such as iris recognition, face recognition and hand-geometry verification methods, finger print spoofing remains the biggest threat to biometric systems . Both hardware based and software based finger print spoofing detection methods have its own advantages and disadvantages. To overcome disadvantages of both methods , a combined software-hardware approach can be used for detection of non live finger print . To ensure security of biometric systems, first an authentication system with both, a PIN or password and finger print scan can be used to provide optimum performance in identification of the user and then effective encryption algorithms can be used to encrypt fingerprint data. This encrypted finger print data cannot be used by the attackers . Because the attackers cannot use encrypted finger print data after it leaves the device. Thus the finger print spoofing detection methods alone cannot provide complete security in bio metric system, only when very effective and reliable methods of finger print spoofing detection and prevention of cyber attacks in biometric systems is included and implemented in it . So that a great span of applications from government to private can use bio metric systems with well improved security. And biometric spoofing attacks are more easily detected by artificial intelligence-based computer systems in terms of speed and accuracy. AI based anti-spoof algorithms that detect non live fingerprint or any other presentation attacks can be used in biometric system for complete security. Thus trust worthy finger spoof detection techniques developed using artificial intelligence, deep learning and machine learning makes bio metric systems more secure and efficient for authentication of identity of an individual.

REFERENCES

[1] S.Prabhakar, ankanti and K. Jain, “Biometric recognition: security and privacy concerns,” IEEE Security Privacy, vol. 1, no. 2, pp. 33–42, Mar./Apr. 2003.
[2] J. Galbally, F. Alonso-Fernandez, J. Fierrez, and J. Ortega- arcia, “ high performance fingerprint liveness detection method based on quality related features,” Future Generat. Comput. Syst., vol. 28, no.1, pp. 311–321, Nov 2012.
[3] E. Marasco and A. Ross, ``A survey on antispoofing schemes for fingerprint recognition systems," ACM Comput. Surveys, vol. 47, no. 2, pp. 1_36,
Jan. 2015.
[4]P. V. Reddy, A. Kumar, S. M. K. Rahman, and T. S. Mundra, ``A new antispoofing approach for biometric devices," IEEE Trans. Biomed. Circuits Syst., vol. 2, no. 4, pp. 328_337, Dec. 2008.
[5]A. S. Abhyankar and S. C. Schuckers, ``A wavelet-based approach to detecting liveness in fingerprint scanners," in Proc. Int. Soc. Opt. Photon., Biometric Technol. Hum. Identi_cat., vol. 5404, Aug. 2004, pp. 278_286.
[6] A. Antonelli, R. Cappelli, D. Maio, and D. Maltoni, ``Fake finger detection
by skin distortion analysis," IEEE Trans. Inf. Forensics Security, vol. 1, no. 3, pp. 360_373, Sep. 2006.
[7] D. Gragnaniello, G. Poggi, C. Sansone, and L. Verdoliva, ``Local contrast phase descriptor for fingerprint liveness detection," Pattern Recognit.,vol. 48, no. 4, pp. 1050_1058, Apr. 2015.
[8] R. F. Nogueira, R. de A. Lotufo, and R. C. Machado, ``Fingerprint liveness detection using convolutional neural networks," IEEE Trans. Inf. Forensics Security, vol. 11, no. 6, pp. 1206_1213, Jun. 2016.
[9] T. Chugh, K. Cao, and A. K. Jain, ``Fingerprint spoof buster: Use of minutiae-centered patches," IEEE Trans. Inf. Forensics Security, vol. 13, no. 9, pp. 2190_2202, Sep. 2018.
[10] Gragnaniello, D., Poggi, G.: An Investigation of Local Descriptors for Biometric Spoofing Detection. J. IEEE Trans. Inf. Foren. Secur. **10**(4), 849–863 (2015)
[11] Ghiani, L., Marcialis, G.L., Roli, F.: Fingerprint liveness detection by local phase quantization.In: 21st Int. Conf. Pattern Recognit, pp. 537-540. IEEE Press, Tsukuba (2012)
[12] M. Tico, “Fingerprint Recognition using Wavelet Features,” in *IEEE International Symposium Circuits and Systems*, vol. 2, pp. 21–24,May 2001.

[13] C.-Y. Huang, L. Liu, and D. C. D. Hung, "Fingerprint analysis and singular point detection," *Pattern Recognition Letters*, vol. 28, no. 15, pp. 1937–1945, 2007.
[14] P.Sengottuvelan, Dr. A. Wahi," Analysis of Living and Dead Finger Impression Identification for Biometric Applications", International Conference on Computational Intelligence and Multimedia Applications
[15] K. Karu and A.K. Jain, "Fingerprint Classification," *Pattern Recognition*, vol. 29, no. 3, pp. 389-404,1996.
[16] Jain, A.K., Flynn, P.J., Ross, A.A.: Handbook of Biometrics, 1st edn. Springer,New York (2007)
[17] R. Derakhshani, S.A.C. Schuckers, L.A. Hornak, and L.O. Gorman, "Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners," *Pattern Recognition*, Vol. 36, pp. 383-396.2003
[18] A. Abhyankar and S. Schuckers: "Integrating a wavelet based perspiration liveness check with fingerprint recognition," *Pattern Recognition*, 42, (3), pp. 452-464.2009
[19] Y. S. Moon, J. S. Chen, K. C. Chan and K. C. Woo. "Wavelet based fingerprint liveness detection", *Electronics Letters*, vol. 41, no. 20,pp. 1112-1113, 2005

Mrs.S.Subhashini received MCA.,M.phil degrees from Madurai kamaraj University , India in 2008 .She is currently pursuing research in computer science with Anna university ,India . Her research interests include biometric identification, digital forensic, pattern recognition , machine learning and artificial intelligence.

Mrs.P.Rajeswari received ME.,degree from Thangavelu engineering college , India in 2013 .She is currently working as an assistant professor in the department of computer science, Mannar Thirumalai Naicker college, Madurai. Her research interests include image processing , computer networks, Data mining , machine learning and Deep learning

.