Techniques For Different Biometric Identification Of Human Traits: A Review

Israa Shaker Tawfic
Minisrty of Science and Technology
Baghdad- Iraq
e-mail: isshakeralani@yahoo.com

***Abstract*—Biometrics indicates measurements identified with human attributes. Biometrics is a sensible validation utilized as a type of distinguishing proof and access control. It is additionally used to distinguish people in bunches that are under observation. Biometric identifiers are then quantifiable, particular attributes used to label and portray people. Biometric authenticators are regularly marked as behavioral in addition to physiological qualities. This paper provides a review of different basic types of biometrics (Fingerprints, Iris, Ear Shape, Gait ..etc), The result of their critical analysis and comparison has been made and it demonstrated that some kinds of biometrics maybe not very vulnerable and could be hacking, so this review also assess the stability of the discussed methods and the risks to intrude and steal the control access information to their databases**

Keywords—Biometrics; Hacker; Recognition; Physiological; Behavioral

I. INTRODUCTION

Biometrics is computerized techniques for perceiving an individual dependent on a physiological or social trademark. Biometric advancements are turning into the establishment of a broad exhibit of exceptionally secure recognizable proof and individual check arrangements.

As the technology develop very fast over the years, the transaction fraud raises and the security methods infringes, the needs for profoundly secure recognizable proof and individual check innovations are become very necessary. Biometric arrangements can accommodate private financial exchanges and personal information protection [1].

In the civilized society exceptional security framework utilizes biometric everywhere throughout the world

In different places such as criminal investigation, Identification, country border, company's office, airports, security sector, banks, medical clinics and so on.

These days biometric based frameworks are in diffuse use and it play a dynamic role in human distinguishing proof [2]. Major biometrics use a part of human body as a password for involve some identity system or application of smart device since every human being have a unique biometrics distinctive that cannot be easily copied or shear.

Biometric can be divided into two parts a Physiological and Behavioral, the physiological are the Fingerprint, Hand Veins, Retina, Iris, etc., while the behavioral part are the signature, Keystroke, handwriting, voice, human walk, etc [3].

Also the biometric system can be a unimodal which use only one biometric characteristic of the human being , or multimodal which used two or more biometric of the person to improves the accuracy for matching the characteristic, reduce fraud and prevent attacked [4].

II. TYPE OF BIOMETRICS

When the word Biometric mention, it stuck in reader mind the fingerprint, face recognitions, or Iris, however there are a wide range of kinds of biometrics utilized today to distinguish and validate people. Regardless of whether for security, access, or stopping fraud, biometrics come in numerous structures, and the software need to gathering biometric data is developed very quickly in order to convoy the great development taking place in the use of biometric features. The different type of biometric can be divided into two group the Physiological and Behavioral and each one has different kind mentions as below:

A. Physiological:

Physiological biometrics are those that depend on one's physical attributes to decide personality. This biometrics type includes but not limit the following:

i- Fingerprints:

Is the oldest and most popular kind of biometric, the first one use to ensure person identity. As soon as the capturing of the print end, a different calculations and sophisticated start by utilize the image to deliver a unique biometric report. The report is then contrasted with new or existing scan to either verify of refute the match. The captured image is then carefully handled and digitally processed. The distinctive highlights are extracted and a unique mark is made. This digital template is put away and will be utilized for comparison and measure matching later as shown in figure (1)[5,6].

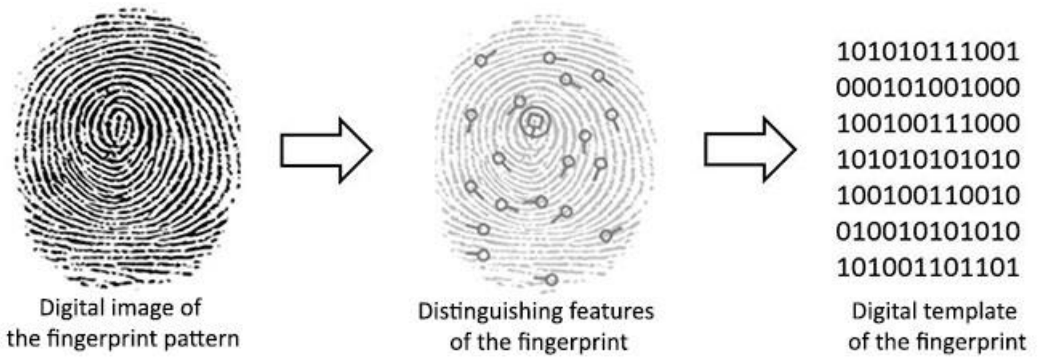
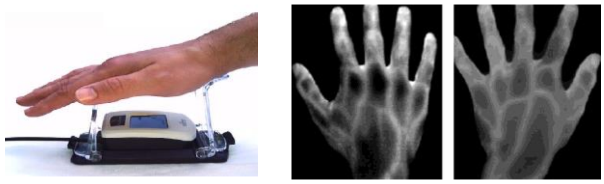

Digital image of the fingerprint pattern
Distinguishing features of the fingerprint
101010111001
000101001000
100100111000
101010101010
100100110010
010010101010
101001101101
Digital template of the fingerprint

FIG.1 HOW FINGERPRINT SCANNER WORKS

ii- Finger, hand veins

Human hand have a complex net of veins and blood vessels, which are only a couple of millimeters beneath the skin surface. Utilizing noninvasive and safe imaging strategies it is conceivable to catch a picture of the bigger veins and veins close to the skin surface in different pieces of the hand. These pictures are most acquired from the rear of the hand and the palm of the hand. This vein structure, which is for the most part is invisible to the natural eye, show an example of interconnecting lines which is different from one to another and utilized as a physiological biometric. Two imaging techniques can be utilized for protected, noninvasive imaging of veins close to the skin surface: (1) distance infrared thermography, and (2) close infrared imaging. distance infrared imaging recognizes heat transmitted from the hand and veins. Close infrared imaging recognizes infrared light reflected from a hand illuminated up by close infrared light [7,8]. Figure (2) illustrate this operation.



(a) (b)

FIG.2: HAND VEINS(A) DEVICE USED, (B) INFRARED MAGES OF THE BACK OF TWO DIFFERENT HANDS TAKEN IN A NORMAL OFFICE ENVIRONMENT

iii- Hand Geometry

It refers to hand characteristics measurement such as fingers length and width, their bowing, and their position relative in addition to other lineaments of the hand. Hand geometry is a biometric kind that separates people from their hands properties. It estimation of the customer hand and contrasts these measurements with the customer database. In mid-80's the first biometric to be utilized electronically to recognize clients is hand geometry. As figure (3) illustrate, Hand geometry works flawlessly when utilized various types of ID [9].

iv- Iris Recognition

The colored part of the eye, or iris, comprises of thick, string like muscles, By estimating the one of a kind folds of these muscles, By estimating the one of a kind folds of these muscles, biometric validation devices can confirm personality with extraordinary precision. Iris acknowledgment or iris filtering is the way toward utilizing noticeable and close infrared light to take a high-differentiate photo of a person's iris. It is a type of biometric innovation in a similar classification as face acknowledgment and fingerprinting [3,10,11]. Figure (4) illustrate the important parts of eye that can be used to prove person authentication.

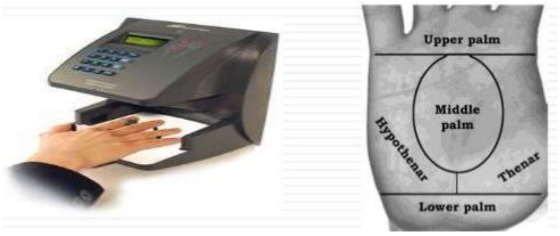


FIG 3. HAND GEOMETRY IDENTIFICATION TECHNOLOGY.

a-

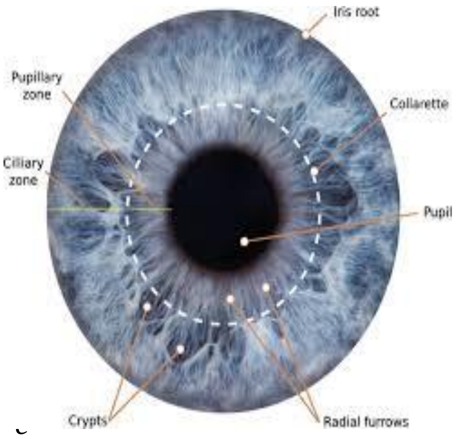


FIG.4 RECOGNITION BASED ON EYE BIOMETRIC, IRIS AND RETINA

a
n
:

The operation of scan retina is capture deeply the capillaries of the eye by using especial camera used near infrared. At the beginning, to enhanced the image, the operation of preprocessed is done for the image raw, then processed again and treat as a biometric template to use it in verification process [12].

b- Facial Recognition.

It just simply measure the face geometry by measuring the distance between the eyes , the distance between chin and forehead. Then gathering data to use it in smart algorithm make a transformation to an encrypted signature.
The operation is illustrated in figure (5), once it recognizes the face, facial recognition software identifies certain point on it and measures those in precise increments, down to the submillimeter. These measurements are used to great a pattern for the face. That pattern will be compared with others already stored in system [14].

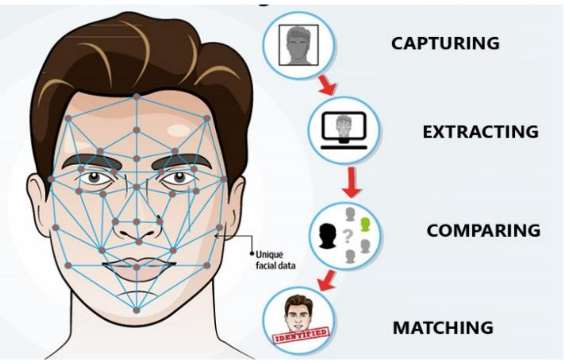


FIG.5 HOW BIOMETRICS FACE RECOGNITION WORK

c- Ear Shape

Ear recognition recently get a significant attention in security field because it rich with information (characteristics) that can be used. The Ear shape is not having problem that may be associated for other biometric that because the ear had stable shape with respect to age [14-16].

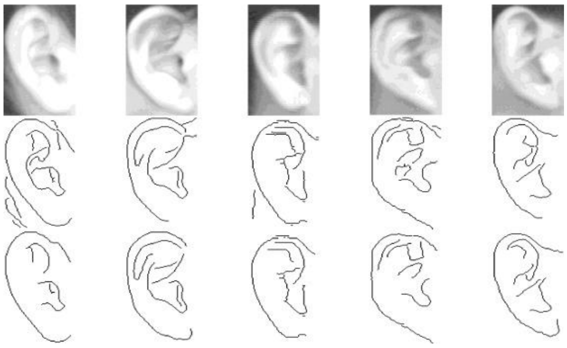


FIG.6 EAR SHAPE RECOGNITION

d- Voice recognition:

It can be fall under both type of biometric (physiological and behavioral).
Physically where it pours in terms of the speaking, shape of vocal tract containing mouth, nose to determines the sound generated. Behaviorally is the method of the person pronouncing the words and say something (Movement differences, speed, tone, accent...etc.) which is defiantly unique for each person. Merge data for both biometric (physical and behavioral) creates accurate vocal signature by mismatching in case of illness or any other reason could happen [17]. The procedure of analysis voice and save it is shown in figure (7).

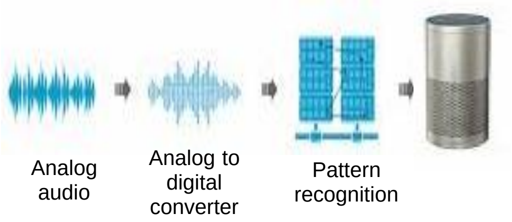


FIG. 7 VOICE RECOGNITION ANALYSIS AND STORE PATTERN

v- Thermography recognition

It’s a way to represent the infrared energy as temperature appropriation picture. Biometric facial thermography catches heat designs caused by moving blood underneath the skin. Since veins are exceptionally remarkable, relating thermograms are likewise one of a kind – even among indistinguishable twins. making this strategy for biometric confirmation much more exact than conventional facial a recognition programming [18,19].

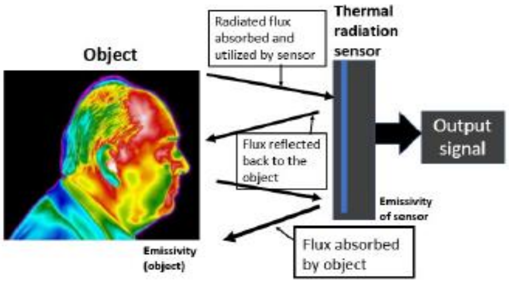


FIG.8. THERMAL RADIATION EXCHANGE BETWEEN OBJECT AND THERMAL RADIATION SENSOR

vi- DNA matching

Is the main type of biometrics that can follow familial ties. DNA coordinating is particularly important when managing missing people and disaster victim. Besides, other than fingerprints, DNA is the main biometric that can be "left behind" accidentally [20]. DNA contains Short Tandem Repeat groupings (STRs) as shown in figure (9).

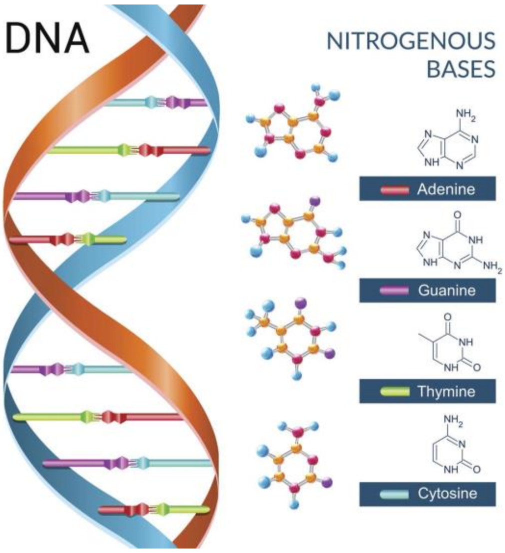


FIG.9 DNA STRUCTURE AND FUNCTION

There are another techniques available bur till now are not so widely adopted, such as Brain Waves and heartbeat

B. Behavioral Biometrics

This type of biometrics measures personal conduct standards instead of (or notwithstanding) physical qualities. The following is some examples of this kind of biometrics:

i- Gait (walk style)

Gait or Step biometrics records walk designs by means of video imaging, then send the mapped information into a scientific condition. This kind of biometric is inconspicuous making it perfect for huge group reconnaissance as it can fast distinguish individuals from a remote place [21]. Figure (10) illustrate this method.

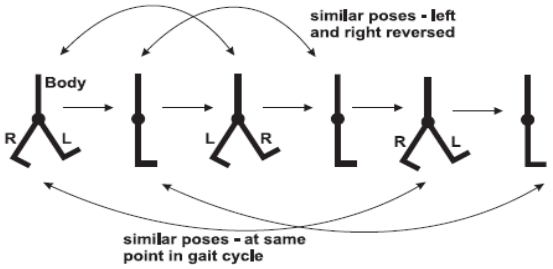

similar poses - left and right reversed
Body
R
L
L
R
R
L
similar poses - at same point in gait cycle

FIG.10 SELF SIMILARITY IN GAIT SEQUENCES. IMAGES SEPARATED BY A FULL OR HALF PERIOD OF THE GAIT TEND TO BE ALIKE.

ii- Lip Movement

One of the newer types of biometric validation includes estimating lip motion. Its like a hard of hearing (deaf) individual may follow lip development to figure out what is stated, biometric lip movement confirmation tracks and records exact muscle development around the lips to decide whether they follow a normal pattern. Biometric lip movement sensors regularly expect clients to verbalize passwords and record the relating lip movement to give or deny access [22,23].

iii- Signature recognition

It is one of widely person biometric authentication method used. Which it's a social biometric that estimates spatial directions, pen weight, slop, and pen stroke in both "disconnected" and "connected" applications. A digital tablet records estimations at that point utilizes the data to consequently makes a biometric profile for future verification [24].

iv- Keystroke

Keystroke move the standard passwords to the next stage by record the mood (rhythm) used to enter the secret key. Estimations may incorporate the time it take to press each key, delays between keys, characters composed every moment, etc. the patterns is work related wiht passwords and PINs to enhanced security endeavors [25]. This biometric is economical and easily can be integrated into the security system with minimal change and user interference.

III. BIOMETRIC HACKING:

Biometric distinguishing is the palm of each smart device. People can open their devices using their fingerprint, face, iris. Organizations have adopted biometric ID systems for section into workplaces and secure territories. Getting free access to frameworks is the objective for programmers. Thus, the chance of biometric information being hacked could present dangers to people and associations.

In this day, biometric confirmation is surrounding us. The techniques utilized by programmers to trick identification and imitative don't move toward the outrageous degree of eyeball substitution, yet creative strategies to move beyond checks are being utilized and created.

Displaying the hacking methods for some methods does not mean that they are not good for use in information security, and, in instead of, not mentioning the penetration of other methods does not mean that they are vulnerable and far from penetration or are 100% secure.

A. Fingerprint hacking:

The way that fingerprints can be lifted isn't generally up for debate. The unavoidable issue with TouchID was whether they could design a device that would oppose attacks utilizing lifted fingerprints? Indeed, TouchID has imperfections, and truly, it's conceivable to misuse those defects and open touch device. Hacking TouchID depends upon a mix of skills, existing academic research and the tolerance of a Crime Scene Technician. First you need to get a good print. An appropriate print should be unsmudged and be a totally print of the right finger that opens a device. The old technique and simple method to get a fingerprint is mention in [26]. In this technique, get a cleaned print picture without inverting it, use transparency film to print on it. After that you should use the film to unmask some thick copper clad photosensitive PCB table which is used by unprofessional electrical project. After improve the image by using PCB, process the PCB using etching (pattern) which remove all of the uncovered copper leaving behind only the fingerprint mold. Stain glue over this mold and leave it to dry, at the end you get a fake fingerprint.

Another method to get a fingerprint used by CCC (Chaos Computer Club) which it’s a club study the ability to break the touchpad security. First of all, the left fingerprint on the smart device is either shoot or scanned at resolution equal to 2400 dpi. After that the copy is converted to black and white, inverted and take a mirror to it. Next, printed the image onto transparent film with resolution = 1200 dpi. To get the mold, a mask is used to disclose the fingerprint pattern on sensitive photo PCB material. This PCB is then progress, drilling and cleaned. At this stage the meld is ready. Apply a thin coat of graphite spray to ensure an enhanced capacitive response and make it easy to remove the fake fingerprint. At the end, a thin white wood glue is stain into the mold. The fake fingerprint is ready after the glue is healing and it will be ready to use.

B. Iris Hacked:

A German hacker’s success to defeated a galaxy S8 by hacked the iris recognition feature in less than one month after the phone produce to the word. They used a dummy eye to fooled the security feature of the phone. They made an artificial eye by using only a printer and to match the curvature of the eye they use the contact lens. This artificial eye is formed using a picture of the iris capture by digital camera setting in night mode as the sensor work with infrared light. The infrared image is printed on laser printer. Then a contact lens is placed on the printed infrared image.

C. Voice recognition hack:

In the beginning of 2018 an international report from NPR and Edison Research show that 39 million Americans have smart speakers or what it’s called digital voice assistants [27]. The device start to merge a speaker with voice recognition, this assistant can be represented by Google home or Amazon Echo in case when you make orders. The digital voice assistant is perfect listener (too much perfect), because the smart speaker gathers information about you by hearing your request and save it on the server. At this point you don’t know who might access and acquire the information or what can do with it. A cybercriminal could send signal or sound to leading your device. There are two big warry about smart speakers:

1- They are constantly listening
2- Since it connects to different devices by acting like a hub which its possibly a start points of vulnerability that hackers can attack.

All possibility intruder has to do is just to collect a few samples of the victim speaking, with addition of voice morphing, can start the voice attacker into the victim.

D. Face recognition

By use a group of useful image of the victim taken from social media like Facebook , instream, or LinkedIn, can create naturalistic, textured, 3D facial models that break the security of application that depend upon face authentication [28]. This framework use virtual reality system (VR), mixed with some program of animations performing like smiling and eyebrow raising of the model to fraud liveness detectors to believing the 3D model is real face. The artificial face is show on the screen of the VR device. To monitoring face authentication system, the motion and depth allusion of the display match human face. Figure (11) illustrate this framework.

E. Hand veins hacking:

Security scientists demonstrated that they can crush the vein-based framework utilizing a uniquely planned wax hand [29]. To crush the vein-based framework, researcher acquired 2,500 photos of a hand with an adjust DSLR camera after takeoff its infrared filter. The pictures were used to create a wax hand with the exact same details of the veins of the person sculpted into it. In any case, researcher guarantee that the technique is difficult to reproduce since the procedure is concentrated and very tricky. However, it is worried that such a solid and apparently flawless confirmation system can be abused so effectively and economically. The producer of getting fake veins is showing in figure 12.

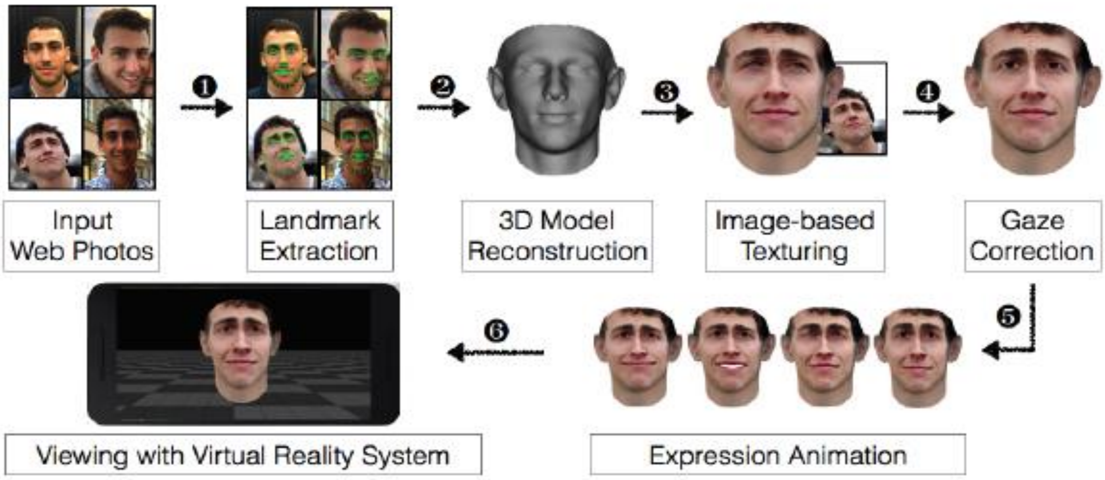


FIG.11 OVER VIEW OF THE FACIAL RECOGNITION HACKER FRAMEWORK

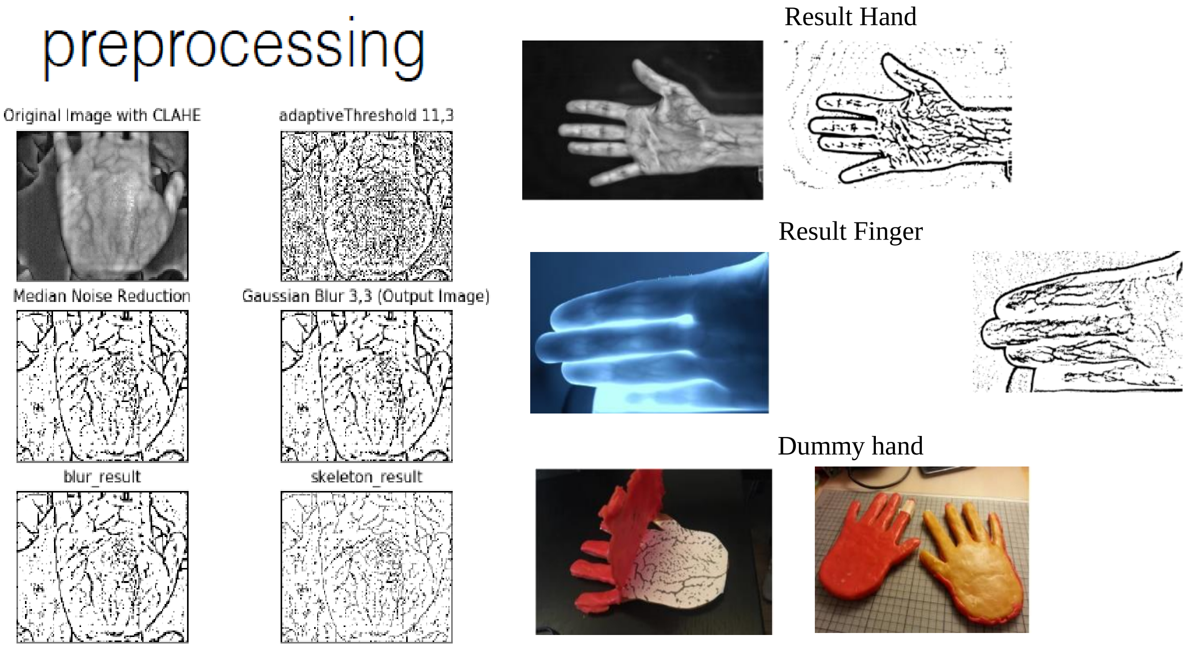


FIG.12 PROCESSING OF GETTING FAKE HAND VEINS

F. 3.6 Hacking DNA:

Even the fact that DNA examination isn’t widely utilized as a security effort, it’s delightful to realize that it might be used for evil reason. Researchers at the University of Washington encoded malware into a genetic molecule that was then used to assume responsibility for the PC used to break down it. While we are maybe far off from DNA hacking getting ordinary, it is an unmistakable update that fraudsters are continually thinking of new strategies [30].

IV. CONCLUSION

All the people around the world are mostly used Online Transactions, however, the users maybe are unaware of the security issues that exist even if they use their own biometric key. They are facing various risks represented by steals their personal information. This review illustrates the various biometrics used in transactions to make users aware and understand the nature of the technology used to give them a full picture of what's going on.

This review guides the reader to some efficiency, reliability, and simplicity of the biometrics method to helps him choose the best way depending upon the importance of the data he deals with in daily life. Using these biometric does not necessarily mean that the system is totally safe, as mentioned earlier in this survey, some methods have already been hacked with the use of counterfeiting to the biometric owner. As mentioned, the penetration that occurred for some method does not mean that it is not secure and should be avoided, as well as penetration of other methods that did not mention do not mean that they are 100% scure.

References

[1] Various Biometric Authentication Techniques: A Review, Kalyani CH, Journal of Biometrics & Biostatistics, DOI: 10.4172/2155-6180.1000371, 2017, 8

[2] “Neural Network Approach to Iris Recognition in Noisy Environment” Kamal Hajari, Ujwalla Gawande, Yogesh Golhar, International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015, Nagpur, INDIA, Elsevier

[3] Score Level Fusion Based Bimodal Biometric Identification Using Thepade’s Sorted n-ary Block Truncation Coding with varied Proportions of Iris and Palmprint traits, Manisha Madanea, Dr.Sudeep Thepade 7th International Conference on Communication, Computing and Virtualization 2016, Elsevier P,rocedia Computer Science 79 (2016) 466 – 473

[4] An Implementation of Electronic Passport Scheme Using Encrypted Security Along with Multiple Biometrics”, Dr.Israa Shaker Tawfic Archives of Information Science and Technology, VOLUME 2 | ISSUE 1 | DOI: 10.36959/863/75, March 16, 2019

[5] Fingerprint Biometric Systems”, Faridah Yahya, Kushsairy Kadir, Trends in Bioinformatics, 9(2):52-58 · September 2016, DOI: 10.3923/tb.2016.52.58,

[6] Security and Accuracy of Fingerprint-Based Biometrics: A Review”, Wencheng Yang , Song Wang, Jiankun Hu, Symmetry Open Access Journal 28 January 2019

[7] “Hand veins”, Graham Leedham , Encyclopedia of Biometrics, Springer DOI: https://doi.org/10.1007/978-0-387-73003-5_263,

[8] “Hand veins recognition system”, João Ricardo Gonçalves Neves Paulo Lobato Correia, IEEE, 2014 International Conference on Computer Vision Theory and Applications (VISAPP), ISBN: 978-9-8975-8133-5, October 2015

[9] “The new hand geometry system and automatic identification”, Shihab A. Shawkat, Khalid Saeed Lateef Al-badri , Ahmed Ibrahim Turki, Periodicals of Engineering and Natural Sciences, Vol. 7, No. 3, September 2019, pp.996-1008

[10] “Mobile iris recognition systems: An emerging biometric technology”, Jin-Suk Kang, International Conference on Computational Science, ICCS 2010, Elsevier.

[11] “Recognition-Based on Eye Biometrics: Iris and Retina”, Josef Hájek, Martin Drahanský, Biometric-Based Physical and Cybersecurity Systemsm, Springer pp 37-102, October 2018

[12] “Retina Recognition”, Yoichi Seto, Encyclopedia of Biometrics, Springer, doi.org/ 10. 1007/978-0-387-73003-5,2009

[13] “A Review of Person Recognition Based on Face Model”, Shakir F. Kak & Firas Mahmood Mustafa & Pedro Valente, Eurasian Journal of Science & Engineering, doi: 10.23918/eajse.v4i1sip157, 2018.

[14] “A Survey on Human Ear Recognition System Based on 2D and 3D Ear Images”, Durgesh Singh, Sanjay K. Singh, OPEN JOURNAL OF INFORMATION SECURITY AND APPLICATIONS, DOI: 10.15764/ISA.2014.02003 Volume 1, Number 2, September 2014

[15] “Ear Shape for Biometric Identification”,Bir Bhanu, Encyclopedia of Cryptography and Security,Springer, DOI: https://doi.org/10.1007/978-1-4419-5906-5_738, 2011

[16] “A novel geometric feature extraction method for ear recognition”, Ibrahim Omara, LiFeng Zhang Hongzhi, Zuo Wangmeng, Expert Systems with Applications, Volume 65, doi 10.1016 2016, 15 December 2016, Pages 127-135 ,

[17] “Speech Recognition by Machine: A Review”, M.A.Anusuya and S.K.Katti, (IJCSIS) International Journal of Computer Science and Information Security, Vol. 6, No. 3, 2009.

[18] “DEFECT RECOGNITION IN THERMOSONIC IMAGING”, Dapeng Chen , Naiming Wu and Zheng Zhang, Chinese Journal of Aeronautics, Elsevier , DOI: 10.1016/ s1000-9361(11)60431-7, 2011

[19] “Thermal imaging as a tool for pattern recognition and anomaly studies: identifying the changes in the condition of an object over time by spotting a trend of changing temperatures, Gordana Laštovička-Medin, RAD Conference Proceedings, vol. 2, pp. 198–206, 2017

[20] “Pattern Matching for DNA Sequencing Data Using Multiple Bloom Filters”, Maleeha Najam and Raihan Ur Rasool, BioMed Research International , HindawiDOI: 10.1155/2019/7074387.

[21] “Biometric Gait Recognition”, Jeffrey E. Boyd and J.J. Little, Lecture Notes in Computer Science, springer, DOI: 10.1007/11493648_2014

[22] “Impact of the Lips for Biometrics”, Yun-Fu Liu, Chao-Yu Lin and Jing-Ming Guo, IEEE

Transactions on Image Processing, DOI: 10.1109/TIP.2012.2186310

[23] “Understanding visual lip-based biometric authentication for mobile devices”, Carrie Wright and Darryl William Stewart , EURASIP Journal on Information Security, 2020, Article number: 3 (2020).

[24] “Off-Line Signature Recognition Systems”, V A Bharadi and H B Kekre, International Journal of Computer Applications (0975 - 8887), Volume 1 – No. 27, 2010

[25] “A Survey of Keystroke Dynamics Biometrics”, Pin Shen Teh and, rew Beng Jin Teoh and Shigang Yue, The Scientific World Journal, Hindawi,doi 10.1155/ 2013/408280.

[26] “Importance of open Discussion on adversarial analyses for mobile security technologies”, Tsutomu Matsumoto, ITU workshop on security, Seoul 2002.

[27] “DolphinAttack: Inaudible Voice Commands”, Guoming Zhang, Chen Yan and Xiaoyu Ji, arXiv:1708.09537v1 [cs.CR] 31 Aug 2017

[28] “Virtual U: Defeating Face Liveness Detection by Bulding Virtual Models from your Public Photos” Yi Xu, True Price, and Jan-Michael Frahm, 25th USENIX Security Symposium. August 2016.

[29] “Hack vein detection”, Jan Krissler annual Chaos Communication Congress (CCC) Hacking Conference Germany,2018

[30] “Computer Security, Privacy, and DNA Sequencing: Compromising Computers with Synthesized DNA, Privacy Leaks, and More”, Peter Ney, Karl Koscher and Lee Organick, USENIX Security Symposium; addition information,2017