**Available Online at www.ijcsmc.com**

**International Journal of Computer Science and Mobile Computing**

**A Monthly Journal of Computer Science and Information Technology**

**ISSN 2320–088X**

***IJCSMC, Vol. 2, Issue. 8, August 2013, pg.257 – 261***

**RESEARCH ARTICLE**

# An Overview of Biometric Identifiers with Emphasis on the Concept and Applications of Finger Vein Recognition

**Babafemi.O.Samuel[1], Olalere.A.Abass[2]**

[1]Department of Computer Science, Tai Solarin College of Education, Omu - Ijebu, Ogun State, Nigeria

[2]Department of Computer Science, Tai Solarin College of Education, Omu – Ijebu, Ogun State, Nigeria

[1] princefm@live.com; [2] Olaabass@fastmail.fm

***Abstract— Protection of data with codes that can be forgotten or cracked is often insufficient; furthermore security with what you have i.e. ID cards or keys that can be stolen or damaged is not the best. Data security is not just an issue to be treated with levity because leakage of data to an intruder can be disastrous.***

***This paper will discuss another approach to security through the concept of what we are i.e. (biometrics), give a brief overview of its classification and finally shed more light on a branch of biometrics which is new but has been found effective.***

***Keywords— A new dimension in biometrics; A new approach to vein identification; Broader platform; Light transmission technology; Biometric Identifiers***

## I. Introduction

In the past and till date, the major way of securing a system or data is through the use of password. Though the use of password is good; but in a constantly developing world like ours, with advancement in various technology, the use of password is inadequate, hence the need for a broader platform “biometrics” to provide adequate security.

Biometrics is defined as the process of validating each characteristic peculiar to human in order to ascertain or verify his identity. [12] In a nut shell, biometrics or biometric authentication is just a means of ensuring that a person’s claim of his identity is true. [2]

Every biological features of human that is special, measurable and can be used to describe him is called a biometric identifier. These biometric identifiers falls under two major group namely (physiological & behavioural characteristics).

A Physiological/Physical characteristic is based on the shape of human body. This group includes fingerprint, facial recognition, DNA, palm print, hand geometry, iris recognition and odour etc. Physical biometric identifier is not influenced by emotion hence it does not change. [3]

- Finger prints: It is also called hand identification. Among all the biometric identifiers, it is the oldest and has a wide range of acceptability. It involves comparing two examples of friction ridge skin from human fingers. [2]

- Face recognition: An individual's face is verified by matching a digital image taken from a video source with extracts in the database through a computer application. The process involved is automatic.[10]
- DNA: Deoxyribonucleic acid is the part of a cell of a living organism that is self-replicating. Conducting a DNA test is time consuming because it is not automated but it has proven to be the most appropriate form of biometric used to identify criminals. [9]
- Palm print: This refers to the capturing of the palm region of the hand with a biometric device which is not expensive. Both the palm print and finger print are similar in that they are based on light reflection technology but different in form of size i.e. the device used for palm printing is larger than that of the finger print. [16]
- Hand geometry: Hand geometry validates a user via the shape/measurement of the hand. It operates on the principle that the shape of one's hand is different and doesn't change over time. Though this method of biometrics is gradually becoming unpopular. It involves the measurement, recording of the height, length and distance between joints of the fingers. [14]
- Iris recognition: Authentication of the Iris which is commonly referred to as iris recognition takes place by dividing the iris into radial fashion. This is possible because the iris has a trabecular meshwork. Iris recognition is an accurate method of biometrics because damage to it is minimal due its protection by the eyelid, cornea and aqueous humour. Iris has an edge over all other types of biometrics due its stability throughout the whole life span of man. Its major limitation is that it requires an exact amount of illumination before capturing occurs (recognition of the iris must take place at a very close range). [18]
- Odour/Scent: Everybody has a unique odour; even identical twins do have different scent. Odour identification is done with the aid of a model called Electronic/artificial noses (ENoses) almost similar in nature to human nose. The ENoses consists of two major components namely the sensing system which is used to identify the odour and a pattern recognition system that classifies or group odorant through automated identification. [21]

A behavioural or psychological characteristic is a form of biometric identifier that centres solely on the actions of a person which is largely dependent on the mood/mental reasoning of that individual at a particular time. Identifiers under this group consist of voice, gait, typing rhythm etc. [2]

- Voice: The presentation of numerical model of sound is called voice print. [5] It involves taking a sample voice that will be analysed and presented in form of an algorithm, then the output of the algorithm is saved in a database. Validating a person's voice requires a match between the person's voice when analysed and measured with the saved voice template in the database. [19]
- Gait: Gait biometrics identifies an entity via the way he walks or sequence of his foot movements. It is not influenced by the speed of the person's walk. [15] It allows recognition at a distance even there is low resolution & poor illumination. Lastly the style of walking/identification can be affected by the surface whether sloppy or uphill, and depending on whatever the individual is wearing. [8]
- Typing rhythm: This is a technology which recognises a person through the way he or she types. It is more concerned with "how" things are written as against "what" is written. It is mostly applicable in areas that require computer login and network security. [20]

Having carefully explained the term "biometrics" and its major classification, this article goes further to discuss a new dimension in biometrics (finger vein recognition) that is gradually gaining acceptance among people.

## II. FINGER VEIN RECOGNITION

Finger vein recognition or vascular technology is a new method of biometrics which uses a captured image of the vein patterns beneath the finger to authenticate one's identity. Veins are invisible since they are underneath human skin, quite different for each finger and person, hence the urge to explore this biological trait which seems impossible to forge or copy led to the research and innovations on vascular technology.

Hitachi limited stumbled on the idea of finger vein recognition in the course of using near-Infrared light to observe the increase in the flow of blood in a sophisticated medical science research to measure brain-function activity. Finger vein biometric is based on the principle of "light transmission technology" see fig.1 which was developed by Hitachi Ltd between the year 1997 & 2000. [11]

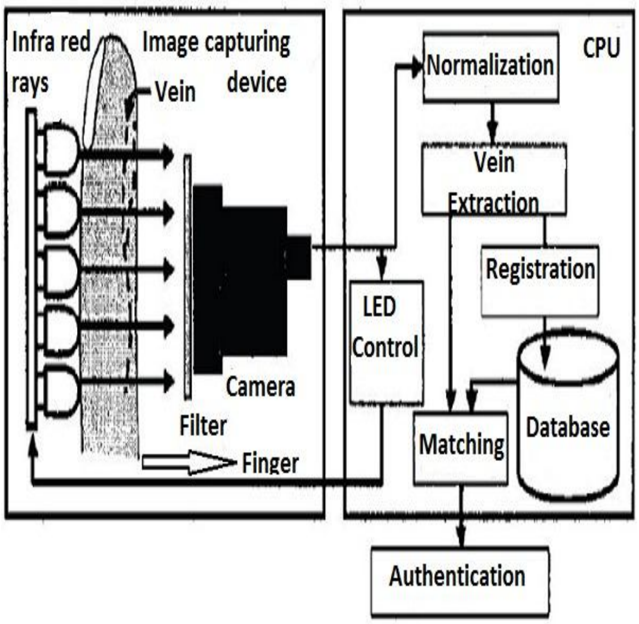

Figure 1: Principle behind finger vein recognition [13]

Most authors have stated categorically that a finger vein authentication device performs four major tasks but for purpose of clarity, those tasks have been splitted into stages involved in light transmission technology to give a concise and clear understanding.

Stage I: The finger is placed between a near Infrared ray generated by the light emitting diode (LED) and a camera.

Stage II: Light rays generated from the LED is transmitted through the finger and absorbed by the hemoglobin.

Stage III: Absorbed light rays in stage II appears in form of a dark area i.e. veins, then the image of the dark area is taken and captured by the camera.

Stage IV: Image taken by the camera is transferred to the memory of the CPU where the LED control adjusts its brightness to eliminate errors due to variations in the size of fingers.

Stage V: Normalization of the finger vein image takes place i.e.to project the outline of the vein patterns image in such a way that the slope remains constant.

Stage VI: Extraction of the vein patterns which is subsequently registered and stored as a template in a database.

Stage VII: It involves matching between the extracted vein patterns and registered pattern stored in the database. If the degree of correlation value is greater than the threshold value, then authentication occurs. [11]

## III. REASONS WHY FINGER VEIN RECOGNITION IS GRADUALLY GAINING ACCEPTABILITY

Finger vein biometrics in the past few years has achieved an explosive growth and popularity among people due to the following advantages stated below:

Accuracy - False acceptance rate (FAR) is the rate at which an intruder is authenticated as the true entity is less than 0.0001%, false rejection rate (FRR) is the rate whereby the true entity is not identified and granted access is less than 0.01% and the failure to enrol rate (FTE) is zero.

Compatibility - The new method of light transmission technology called “side lighting”[11] i.e. shinning of light through the sides of the fingers and scattering of light in the fingers has allowed Hitachi Ltd to develop a portable and compact device that can be embedded in various applications.

Speed - Authentication of finger vein patterns is very fast because it occurs in less than 0.5 seconds.

Greater security - Unlike other types of biometrics that uses the exterior part of human body for authentication which is susceptible to forgery. Veins are hidden beneath human skin hence it makes it impossible to duplicate thereby creating data security.

User friendly - Regardless of the texture of skin whether dry, wet or dirty, authentication can occur because there is no need for physical contact with the image sensor except for a minimal part of the finger coming in contact with the finger guide which doesn’t hurt.

Cost - When compared to biometric devices used for Iris and facial identification, the cost of purchasing and installing a finger vein recognition device is not on the high side. It is relatively affordable. [12]

## IV. APPLICATIONS OF FINGER VEIN TECHNOLOGY

Various sectors of different economy which requires consistent and adequate data security have tapped into the abundant opportunities inherent in finger vein biometrics. Below is a list of areas where vascular technology is being used.

Banks – ATM applications was developed by Hitachi in 2004 and commercialized in 2005. [11] The process involved in ATM end user verification is as follows; Customers are expected to open a biometric bank account with their vein patterns registered and stored on a smart card. Cash withdrawals on the ATM are only possible if there is a match between the customer's finger vein when inserted into the finger vein scanner on the automated teller machine and the save vein patterns on the smart card. With this process stated above, banks in japan and Asian pacific region since 2005 have been able to establish a vibrant financial sector reducing risk of fraud. [6]

Logical Access Control – The USB finger vein biometric scanner is applicable in areas where there is the need for encryption of data to & fro from the computer. It is also useful in firms that secures data through computer login because it reduces risk of password hacking and impersonation. The USB finger vein scanner is connected to a PC through the USB ports. The most popular type is the Hitachi H-1 model which is easy to use and compactible. [17]

Door Access Control System – This is a system that keeps records of different access granted to certain people before allowing them into a room or building. Access to such buildings is often through the use of ID cards. Shortcomings involved in using ID cards are that it may be misplaced or damaged thereby preventing access to the building. At present Hitachi Information & Control system Ltd and Laboratory of Hitachi Ltd have developed an electronic device which will only grant an individual access to a room/building via who they are using their finger vein as the key to authentication. The electronic device is referred to as SecuaVeinAttestor which houses a micro-computer system that is able to recall various biometric data stored in the database. It is installed on the wall very close to the door. An Individual only needs to insert his finger into the device and through the principle of light transmission technology, if there is a match between vein patterns extracted and those in the database. The door opens within seconds. Security of different offices has improved due to the invention of this system. [4]

Hospital – Vein identification is relatively new in health care but it has allowed consultants and management to keep track of patient's information. Now patients with the same name can be identified through their vein patterns on arriving at the hospital. This will also allow hospital management to determine when the patient visited the hospital last, what he/she was diagnosed and treated for etc. Lastly the issue of internal security breach and patient identity theft will be reduced drastically. [7]

Finally applications of finger vein biometrics are limitless. It cuts across so many sectors ranging from defence industries, border crossing, law enforcement, automobiles, education etc.

## V. FUSION OF VEIN TECHNOLOGY WITH EXISTING BIOMETRIC TECHNOLOGIES

In order to guarantee and provide efficient security system, vein technology can be fused with present day biometric technologies to provide one to many matching. This proposition will definitely reduce fraud, promote data consistency and completeness. Another quality which vein technology devices have that will make its integration with other methods of biometrics outstanding is its portability i.e. it uses a single-chip design. [1]

## VI. CONCLUSIONS

Vein biometrics has come to stay. A new approach to vein identification (Palm vein recognition) which extracts vein patterns on the palm is making wave over the globe. The principle behind both finger & palm vein technology is simple – to provide unparalled security by authentication of an invisible trait beneath human skin that is impossible to forge and duplicate.

## ACKNOWLEDGMENT

We sincerely appreciate authors whose articles were cited in this work.

## REFERENCES

[1] A. Ahmed, "Palm/Finger Vein Recognition – Seminar paper," 10th April 2013. [Online]. Available: http:/www.seminarpaper.com > electronics.

[2] A. Babich, "Biometric Authentication; Types of Biometric Identifiers," Bachelor's Thesis, Degree programme in Business Information Technology, HAAGA – HELIA University of Applied Sciences, 2012.

[3] A. Jain, L. Hong and S. Pankanti, "Biometric Identification," in Communication of the ACM, 2000, paper 43(2), p.91 -98..

[4] About Finger Vein: Hitachi Information & Control Solutions Ltd retrieved online from http://www.hitachi – ics.co.jp /product/ English/ about_fv.htm/

[5] Authentify Voice Biometric Authentication. [Online]. Availabe: http://www.authentify.com / Solutions/voicebiometrics.html

[6] Banking finger vein ATM recommendations for potential Nigerian Implementation retrieved online from http://environ-ng.com/ presentations/atmbanking.pdf

[7] Cynthia. E. Keen. (1st July,2011) Biometric ID Technology for healthcare is taken off. [Online].Available: http: // www.aunt.minnie.com / Index. aspx ?sec = sup & sub = ris & pag = dis

[8] Derawi Biometrics: Research on different biometric modalities, Gait. Retrieved online from http://biometric.derawi.com/?pageid=38/

[9] DNA as A Biometric Identifier, Retrieved online from http://www.cse.msu.edu/cse891/Sect60 /casestudy /DNA Biometric Identifier. pdf

[10] Dzh. H. Konnel, S. Pankanti , N. K. Ratha and E. U. Seno, "Guide to Biometric per English Rukovodstro po biometrii per S angl," 2007.

[11] Finger Vein Authentication: White paper, Copyright Hitachi Ltd. 2006.

[12] Finger Vein Biometric System, FAQ, Hitachi Asia Ltd. Copyright 2012.

[13] G. A. VonGraevenitz, "Biometric authentication in relation to payment systems and ATMs," 2007.

[14] Hand Geometry and Hand writing, The Global security website. [Online].Available: http:// www.globalsecurity.org/security/systems/biometrics-hand.htm

[15] J. E. Boyd and J. J. Little, "Biometric Gait Recognition," 2005.

[16] Lifang, Maylor. K. H. Leung, T. Shikhare, V. Chan and K. Fattchoon, "Palmprint Classification," School of Computer Engineering, Nanyang Technological University, Singapore 639798.

[17] Logical Access Control: Finger Vein Authentication Technology Retrieved online from http: // www. hitachi. co. jp / products / it / veined/global /....../logical_access.html

[18] P. Khaw, "Iris recognition technology for improved authentication," SANS Security Essentials (GSEC) Practical Assignment. Version 1.3, SANS Institute 2002.

[19] Salmat Speech. (6th July, 2010), what is a voice biometric.[Online].Available:http:// speech.salmat.com.au/be-educated/what-is-a-voice-biometric/

[20] V. Kacholia and S. Pandit, "Biometric authentication using random distribution (bioart)," Retrieved online from http: // www.researchgate.net/publication/228981955_Biometric authentication _ using _ random _ distribution_(bioart.)

[21] Z.. korotkaya, "Biometric Person Authentication: Odor," Department of Information Technology, Laboratory of Applied Mathematics, Lappeenranta University Technology. [Online]. Available: http://www2.it.lut.fi/kurssit/03-04/010970000/seminars/korotkaya.pdf