Int.J.HIT.TRANSC:ECCN.Vol.3: Issue 2A(1) (2017) Page 14-20 ISSN: 0973-6875

Available Online at www.hithaldia.in/locate/ECCN

ORIGINAL CONTRIBUTION

Finger Print and DNA Pattern Recognition

Syed Mahamud Hossein[1*], Biswapati Jana[2], Aditya Kumar Samanta[3], Susanta Mandal[3] and Suvasis Ghosh[3]

[1]*District Officer, Regional Office, Midnapore, DVET, Govt. of West Bengal*
[2]*Deptt. of Computer Science, Vidyasagar University*
[3]*Dept. Of Information Technology, Jalpaiguri Govt. Engg. College, West Bengal*

(Received Date: 20th August, 2017; Acceptance Date: 30th September, 2017)

ABSTRACT

This paper is a study and implementation of a fingerprint recognition system based on Minutiae based matching quite frequently used in various algorithms and techniques. Currently, we have noticed that the users use only one way security which only match the finger pattern as a result the hacker can easily make artificial fingerprint or other ways, as a result they are easily hacking the system. The motive of our work is that when the users match their fingerprint, this time the system will also check the DNA sequence, the hacker cannot make an artificial DNA sequence because the size of the genetic sequence [DNA(deoxyribonucleic acid)]is varying in the range of million to billions of nucleotides and two or three times bigger annually . Here we use some algorithms like pattern matching algorithms, compress algorithms, and security etc.

Key words: Image Segmentation; Minutiae; fingerprint

1. INTRODUCTION

The fingerprinting problem is that when user use finger printing on any system. System only scans the image of our finger. It can't scan our DNA sequence. So the system can be easily hacked by the hacker by using artificial fingerprint. Hacker can be hacked the system using some trial an error method, possible change to hacked the system. But in case of scanning the DNA of the particular fingerprint the chance of hacking is very less; also the matching DNA sequence in between two users is about 10-5 to 10-9, the probability of matching is very less like 0.01%.

Fingerprint authentication refers to the automated method of verifying a match between two human fingerprints. Fingerprints are used to identify and verify their identity [1-3]. In this reason use DNA fingerprints in our system for batter security. By using DNA fingerprinting to reduce machine system processing time and also reduce space .by using DNA fingerprinting user can easily handle the system.

Process how to be hacked it:

1: Hacker can use some kind of gale. She/he takes image of the user fingerprint and he/she made the feck image of user fingerprint.

2: Hacker can use soap .She/he take image of the user fingerprint and he/she made the feck image of user fingerprint and easily hacked the system.

3: Hacker can make artificial fingerprint. So they can easily hack the user fingerprint. This are the process hacker can hacked the user fingerprint image.

1. What is a Fingerprint?

A fingerprint is the feature pattern of one finger (Figure 1.1). It is an impression of the friction ridges and furrows on all parts of a finger. These ridges and furrows present good similarities in each small local window, like parallelism and average width.

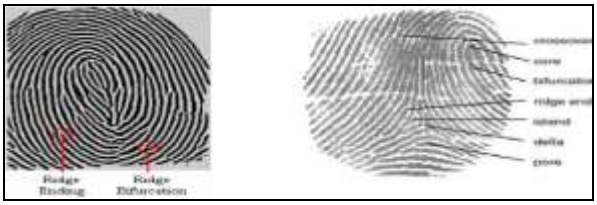
*Corresponding Author:mahamud123@gmail.com

Figure 1.1 Fingerprint image from a sensor

Figure 1.1 Fingerprint image from a sensor. However, it can be shown by intensive research on fingerprint recognition, fingerprints are not distinguished by their ridges and furrows, but by features called Minutia, which are some abnormal points on the ridges (Figure 1.2). Among the variety of minutia types reported in literatures [4], two are mostly significant and in heavy usage:

1: Ridge ending - the abrupt end of a ridge.

2: Ridge bifurcation - a single ridge that divides into two ridges .



(a) (b)

Figure 1.2 (a) Two important minutia features 1.2 (b) Other minutiae features

2. WHAT IS FINGERPRINTING RECOGNITION?

Fingerprint recognition or fingerprint authentication [4-11] refers to the automated method of verifying a match between two human fingerprints. Fingerprints are one of many forms of biometrics used to identify individuals and verify their identity.

3. THE STEPS OF DNA FINGERPRINTING PROCESS

DNA fingerprinting involves a number of intensive and important steps in order to fully complete and develop and DNA fingerprint of a father, a suspect or a person involved in an immigration problem. The process of DNA fingerprinting starts with isolating DNA from any part of the body such as blood, semen, vaginal fluids, hair roots, teeth, bones, etc.

Polymerase Chain Reaction (PCR) is the next step in the process. In many situations, there is only a small amount of DNA available for DNA fingerprinting. Because of this, in a test tube, DNA replication is must occur to make more DNA. The DNA and the cells will undergo DNA replication in order to make more DNA to be tested.

After the DNA is isolated and more copies of the DNA have been made, the DNA will be tested. The scientist will treat DNA with restriction enzymes (an enzymes that cuts DNA near specific recognition nucleotide sequences known as restriction sites).

-This will produce different sized fragments which are known as restriction fragment length polymorphisms (RFLPs).

-These fragments can then be observed doing an experiment called gel electrophoresis which separates DNA based on fragment sizes.Gel electrophoresis is the next step in this process of DNA fingerprinting. During gel electrophoresis, an electrical current is applied to a gel mixture, which includes the samples of the DNA.

-The electric current causes the DNA strands to move through the gel. This separates the molecules of different sizes.

-The fragments of separated DNA are sieved out of the gel using a nylon membrane (treated with chemicals that allow for it to break the hydrogen bonds of DNA so there are sing strands). The DNA (single stranded) is cross-linked against the nylon using heat or a UV light. The probe shows up on photographic film because the strands of DNA decay and

give off light. In the end, it leaves dark spots on the films which are also known as the DNA bands of a person. What make up the fingerprint are the unique patterns of bands. The patterns of bands are different as we are all different and unique (other than identical twins).Once the filter is exposed to the x-ray film, the radioactive DNA sequences are shown and can be seen with the naked eye. This creates a banding pattern or what we know as DNA fingerprints. This technique is called southern blotting. These fingerprints can be used to determine which hair strand belongs to which person for example: DNA fingerprints of children should be similar to their parents' fingerprints, although they may not be the same. Some bands will match one parent and other bands can match the other parent. With the bands of both of those parents, they make the bands and the identity of the child.

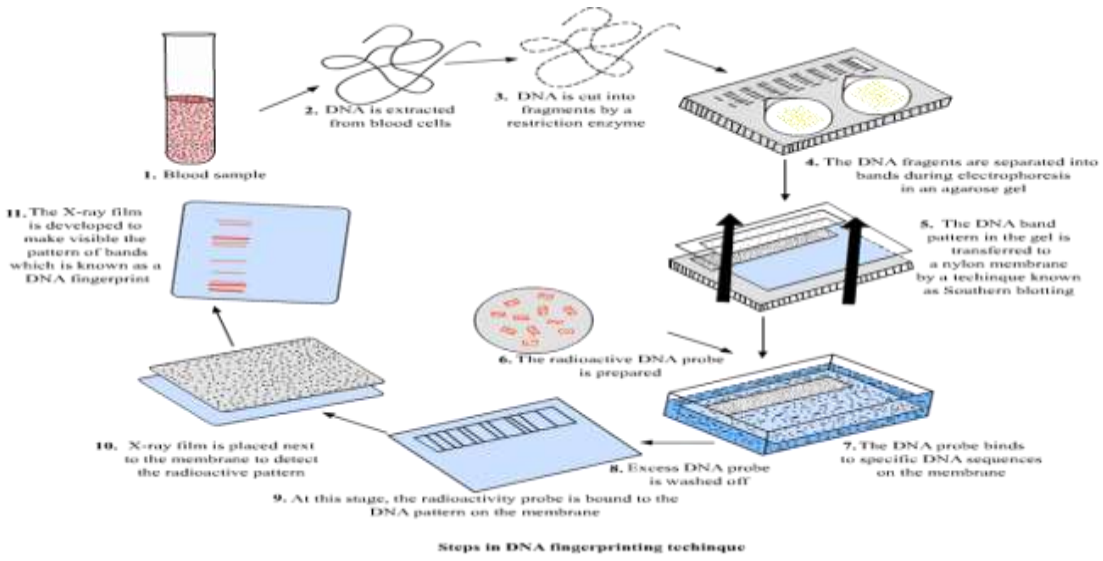


Figure 1.4(a): Steps in DNA fingerprinting technique

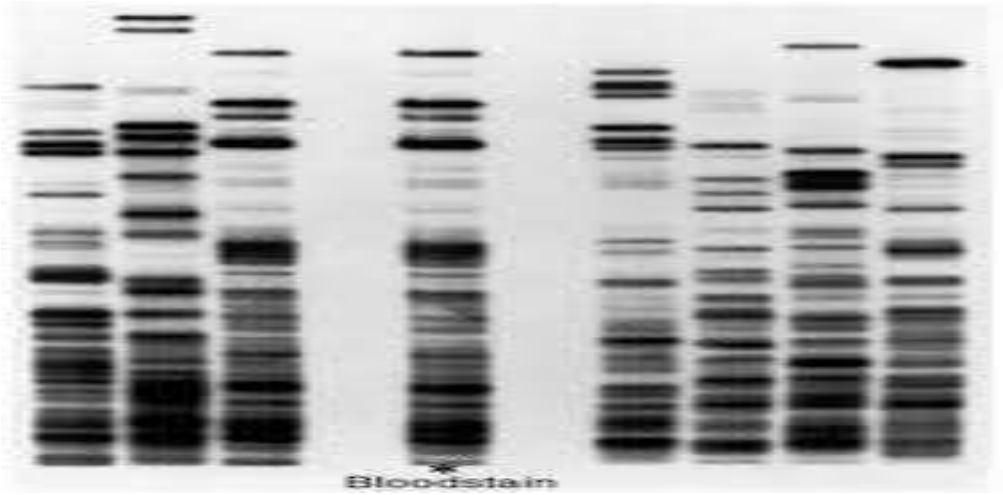
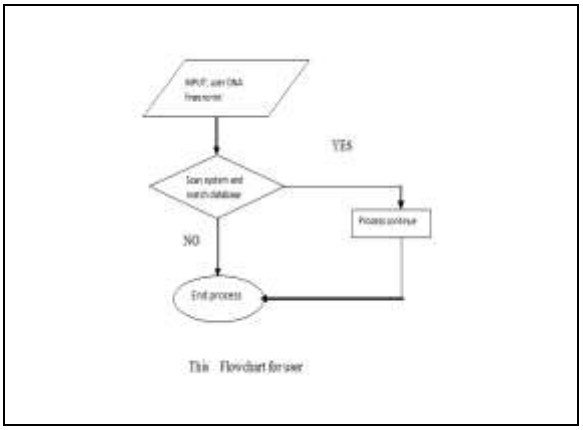
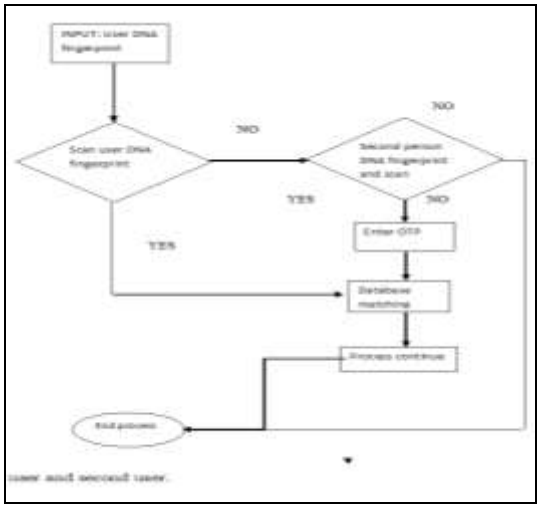


Figure 1.4(b): DNA fingerprinting X-ray film

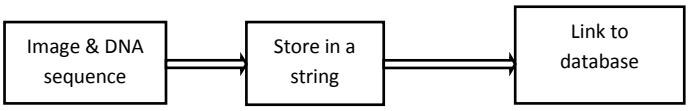
4. FLOW DIAGRAM OF OUR WORK



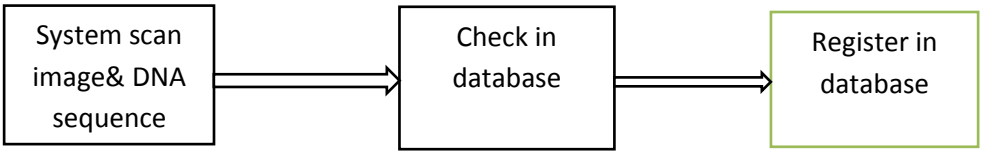


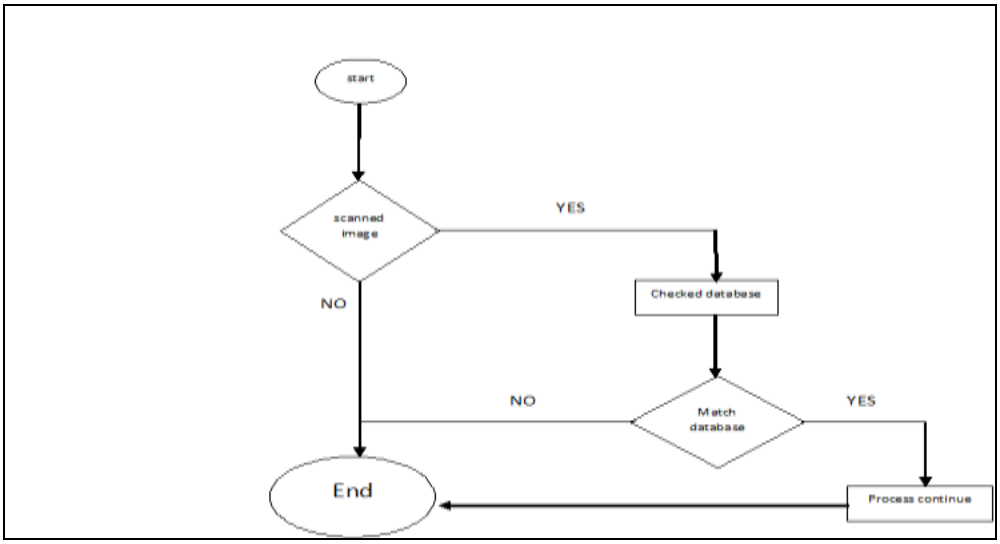
5. REGISTER AND LOGIN

In case of register time system at first scans the image and DNA sequence. Image and DNA sequence are stored in a string by using MATLAB and MY-SQL. Then the string is stored in database .When user logs in the system then system checks in database .If the scanned image and DNA sequence match then the process will continue otherwise process will end.



Store in database by using MATLAB





6. METHODOLOGY

1. When a user matching his fingerprint in a system .In this time the system scan the user fingerprint pattern as well as scanned the DNA sequence. We know from a research paper that a hacker can't make a artificial DNA. So this is impossible for the hacker to hack the system.
2. We can easily solve these problems by using some algorithms. In this algorithms we are store our DNA fingerprint in our system. When the system scan user fingerprints, then firstly scan our finger image and then it also scan our DNA sequence. We know that two persons DNA can't match. The different between two person DNA is 10-5to 10-9 which means that the probability of two parsons DNA sequence matching is 0.01% which is very negligible. So the system can't easily hacked by the hacker.

7. ALGORITHMS

We are design our process by use some algorithms. At first we will discuss about compress algorithms .We can use this algorithms to reduce the time and reduce space .We also use another algorithm .This algorithm is pattern matching algorithm .By using in this algorithm system can match our fingerprint pattern and also match our DNA sequence with database .If given pattern can't match then the process will be end and else process continue. And this pattern matching algorithm also check the given pin code. In case of second parson pattern matching algorithm can check the given OTP. If the given OTP is right then process will be continue otherwise process will be end.

8. RESULT DISCUSSION & CONCLUSION

1. This is a two level security system. Level one: It check the DNA finger pattern and DNA sequence, Level two:It also check pin code and OTP.

2. We use the compress algorithms in this paper which will also reduce the space and time complexity.

3. If user is ill or can't attend. Then second parson can excess this system by using his/her fingerprint, Pin code and OTP. In this case systems generate two OTP. One got user and another got second parson. After putting two OTP then process will be continue otherwise process will be end.

4. Hacker can't make an artificial DNA fingerprint. So person can't hacked the system .

9. FUTURE WORK

We will discuss about DNA fingerprinting scanning, registration process and the login process in our next paper.

ACKNOWLEDGEMENTS

The satisfaction we have on the successful completion of the project will be incomplete without the mention of the people whose constant endeavor guidance and encouragement has helped us to achieve success. Firstly, we offer our sincere gratitude to the Department Of Computer Science, VIDYASAGAR UNIVERSITY, for giving us the opportunity to pursue this project during our internship and thereby helping us to improve our career. We are also grateful Prof. Biswapati Jana of the same department and Mr. Syed Mahamud Hossein, District Regional Officer, DVET, Govt. of West Bengal for their endeavor support and invaluable help during the entire duration of the project. Their inspiring presence, constant encouragement, meticulous guidance and painstaking efforts helped us to tide over the problems encountered during the various phases of the project. It is also a pleasure to acknowledge the support received from Prof. Aditya kumar samanta, Department of Information Technology, Jalpaiguri Government Engineering College, Jalpaiguri, West Bengal for his guidance and encouragement during the ongoing project.

References

[1] H. Albin-Amiot, P. Cointe, Y.-G. Gu´eh´eneuc, and N. Jussien. Instantiating and detecting design patterns: Putting bits and pieces together. In proceedings of the 16th conference on Automated Software Engineering, pages 166–173. IEEE Computer Society Press, November 2001.

[2] Y.-G. Gu´eh´eneuc and H. Albin-Amiot.Using design patterns and constraints to automate the detection and correction of inter-class design defects. In proceedings of the 39th conference on the Technology of Object-Oriented Languages and Systems, pages 296–305. IEEE Computer Society Press, July 2001.

[3] Y.-G. Gu´eh´eneuc and N. Jussien.Using explanations for design-patterns identification, In proceedings of the 1st IJCAI workshop on Modeling and Solving Problems with Constraints, pages 57–64. AAAI Press, August 2001.

[4] Fingerprint Recognition using Image Segmentation, SangramBana and Dr. DavinderKaur, Department of Physics, IIT Roorkee, Roorkee

[5] G. Davida, Y. Frankel, B. Matt, On enabling secure applications through online biometric identification, in: Proc. of the IEEE 1998 Symp. on Security and Privacy, Oakland, Ca., 1998.

[6] T. Clancy, D. Lin, N. Kiyavash, Secure smartcard-based fingerprint authentication, in: ACM Workshop on Biometric Methods and Applications (WBMA 2003), 2003.

[7] P. Tuyls, A. H. M. Akkermans, T. A. M. Kevenaar, G. J. Schrijen, A. M. Bazen, R. N. J. Veldhuis, Practical biometric authentication with template protection, in: Proc. of the 5th International Conference on Audio and Videobased Biometric Person Authentication, Rye Town, NY, 2005, pp. 436–446.

[8] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, V. Kumar, Biometric encryption, in: R. Nichols (Ed.), ICSA Guide to Cryptography, *McGraw-Hill*, 1999.

[9] U. Uludag, A. Jain, Attacks on biometric systems: a case study in fingerprints, in: SPIE-EI 2004, Security, Seganography and Watermarking of Multimedia Contents VI, 2004.

[10] Germain, R., Califano, A., Colville, S., 1997. Fingerprint matching using transformation parameter clustering. *IEEE Comput. Sci. Eng.* 4 (4), 42–49.

[11] Jea, T.-Y., Chavan, V.S., Govindaraju, V., Schneider, J.K., 2004.Security and matching of partial fingerprint recognition systems. In: SPIE Defense and Security Symposium.

[12] Teoh, A., Ngo, D., Goh, A., 2004. Biohashing: Two factor authentication featuring fingerprint data and tokenized random number. *Pattern Recognition* 37 (11), 2245–2255.

[13] MATLAB, C, JAVA and MY- SQL Software