Authentication, Recognition, & Hacking Of Fingerprint

Amee Pandya
Department of Cyber security
Raksha Shakti University, Gujarat, India

Abstract- *The fingerprint recognition is now a worldwide hottest research topic because of its authentication "a person is fingerprint which is unique & permanent throughout the person life" that is the reason in India the AADHAR is link on biometrics so in this the loop falls & its strength how to recognition are known to knowledge for Indian citizens. Fingerprint recognition problem depends on two competing error rates: first one is The FALSE ACCEPT RATE (FAR), and the other one is FALSE REJECT RATE (FRR), need to be minimized. Advancement of computing capabilities to the development of Automated Fingerprint Authentication Systems (AFIS). That is the reason this fingerprints authentication is widely used in daily life for more than 100 years due to its feasibility, distinctiveness, permanence, accuracy, reliability, and acceptability. In this paper, I'll cover to give a comprehensive scoping of the fingerprint recognition, its hacking, design and implementation issues, and its future prospects.*

Keywords- biometrics authentication, fingerprint recognition, hacking, security..

I. INTRODUCTION

To make personal identification, Biometric relies on "something that you are" so it can inherently differentiate among who is an authorized person and who is a fraudulent person. Biometric authentication is a system that is used for unique physiological and behavioural characteristics of individuals for identification of a person to secure access. Biometric is not used for personal identification to establish absolute "yes" or "no" but used for identification to achieve "positive". Biometric is a measurable characteristics like facial structure, fingerprints etc. For measuring person's characteristics, we use Biometrics Devices which gives computer vision, pattern recognition etc. Biometric Authentication System uses following performances:

- Equal error rate
- False match rate
- Failure to enrol rate
- Template capacity
- Receiver operating characteristic
- False non-match rate
- Failure to capture rate

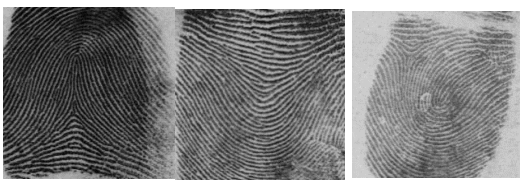
In my knowledge the Biometric authentication is the most fool proof or at least the hardest to forge or spoof, so I'll try to find hacking of it so in this project for partially complete types of hacking because of this hacking I'll try to overlap this hacking and making more secure biometric authentication system because of The value of a reliable user authentication is not limited to just computer access. Many other applications in everyday life also require user authentication, e.g. banking, immigration, and physical access control. These could also benefit from enhanced security. Automated biometrics technology in general, and fingerprints in particular, can provide a much more accurate and reliable user authentication method.

In this, a present in more detail the problems unique to biometric authentication systems and propose solutions to several of them. Though my analysis is very general and can be extended to other biometrics, so I'll focus on fingerprint recognition as an example throughout.

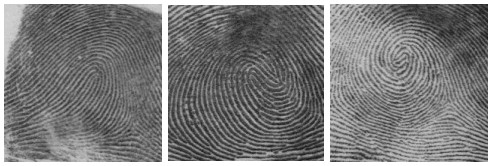
II. AUTHENTICATION & SECURITY OF BIOMETRICS

As uniqueness and permanence of fingerprint recognition is higher than other biometric recognitions, so we mostly use fingerprint authentication system as a means of identification of a person. Fingerprint of a person can never be changed throughout person's death except deep physical injuries and severe burns

Fingerprints present on human fingers are graphical flow-like ridges. On the surface of fingerprint, ridge patterns are formed in womb. Fingerprints are categorized into six categories i.e.:



a. Arch b. Left Loop c. Right Loop



d. TenTed Arch e.Twin Loop f. Whorl

Fig 1: Fingerprint classification involving all classes

fig 2: fingerprint feature.

III. HACKING OF FINGERPRINTS

They have so many types of hacking of fingerprints and this is very simple and cheaper.

Rubber Cement, or Silicone gel. Rubber cement is all kind of probably used in elementary school art class is one of the most reliable ways to make a copy of a finger print. Doing so typically requires the cooperation of the print owner. So simply make a plaster cast of the finger using modelling wax and pop to capture the print in a thimble shaped mould. Rubber cement or liquid silicone in then pressed into the mould using a pestle to create a thin, counterfeit print that can be slipped over the finger.

Gelatine (aka gummy finger). : In this if you say you make your false finger using Silicone Gel and it works. The gelatine has many of the same conductive properties as human skin and can fool more sophisticated readers designed to sniff out inorganic "fingers".

Tape. : "There are no good products, only good deployments" - That's the lesson from Japan where, in 2009, fingerprint scanner used to screen would be immigrants failed to detect a South Korean woman who used a fingerprint image on a simple piece of masking tape to gain admission to the country.

A Photocopy. : This is also a very simple hacking of fingerprint biometrics. Because of in this the use of material is inorganic as well as optical and ultrasound sensors.

Software based attacks. : As attractive as the notion of gummy fingers is, attacking the software running the scanner is at least as promising a technique as making fake finger. That was the approach taken by researchers at IBM, who looked at a variety of ways to fool print readers by attacking the software that runs them.

In this attack is used 'man in the middle' and also work as brute force attack.

In this the attacker use malicious software to manipulate the data received by the scanner.

IV. MAJOR IMPLEMENTION & DESIGN ISSUES

A fingerprint recognition system can make two types of errors: a false match, when a match occurs between images from two different fingers, and a false non-match, when images from the same finger are not a match. Thus the chief objective behind the design of a good fingerprint matching system is to reduce both these errors. However both the error rates cannot be reduced simultaneously as they are inversely dependent on each other.

Another important design issue is the security of the fingerprint recognition system itself along with the fingerprint template database. The unauthorized use or disclosure of fingerprint template information from such databases can be a serious security and privacy threat.

Although fingerprint recognition has been extensively studied, there are still many open research problems in this domain, for instance:

- Efficient Automated Fingerprint Classification
- Fully Automated Latent Fingerprint Recognition
- Altered or Fake Fingerprint Detection
- Efficient Compression of Fingerprint Templates
- Automated Artificial Fingerprint Generation

V. CONCLUSION

Fingerprint Authentication has been studied for well over a century. Its uses truly of knowing only in the last few years due development of fingerprint authentication.

And still its security is low and hackers hacking it manually as well as dynamically so it is not fool-proof but still

it is secure because of the knowledgeable hackers only hacking it otherwise it is secure.

REFERENCES

[1] R. Clarke, "Human identification in information system: Management challenges and public policy issues", Info. Technol. People, Vol. 7, No. 4, pp. 6-37, 1994

[2] Anil k. Jain, Lin Hong, Sharath Pankanti and Ruud Bolle, "An Identity-Authentication System Using Fingerprints",Proceedings of the IEEE, Vol. 85, No. 9, pp. 1365-1388,

[3] E. Newham, The Biometric Report. New York

[4] S. G. Davies, "Touching Big Brother: How biometric technology will fuse flesh and machine", Info. Technol. People, Vol. 7, No. 4, pp. 60-69

[5] H. C. Lee and R. E. Gaensslen, Eds., Advances in Fingerprint Technology, New York

[6] M. James Stephen and P. V. G. D Prasad Reddy, "Implementation of Easy Fingerprint Image Authentication with Traditional Euclidean and Singular Value Decomposition Algorithms", Int. J. Advance. Soft Comput. Appl., Vol. 3

[7] Virginia Espinosa-Durg, "Minutiae Detection Algorithm for Fingerprint Recognition", IEEE AESS Systems Magazine

[8] Fernando Alonso-Fernandez, Josef Bigun, Julian Fierrez, Hartwig Fronthaler, Klaus Kollreider and Javier OrtegaGarcia, "Fingerprint Recognition", Guide to Biometric Reference Systems and Performance Evaluation, Chp. 4

[9] Shrikhande, Santosh P., and H. S. Fadewar, "Finger vein recognition using Discrete Wavelet Packet Transform based features", 2015 International Conference on Advances in Computing Communications and Informatics (ICACCI)

[10] Anil Jain, "Introduction to Biometrics", Biometrics

[11] W. Balder, "Dermatoglyphics: Science transition", Vol. 9

[12] M. Kuchen, C. Newell, "A Model for fingerprint formation", Europhys letters, Vol. 68

[13] Gualberto Aguilar, Gabriel Sanchez, Karina To scano, Moises Salinas, Mariko Nakano, and Hector Perez, "Fingerprint Recognition", Second International Conference on Internet Monitoring and Protection

[14] Subhra Mazumdar and Venkata Dhulipala, "Biometric Security using Fingerprint Recognition"