Journal of Information Sciences and Computing Technologies ISSN 2394-9066

SCITECH
RESEARCH ORGANISATION|

Volume 1, Issue 1
December, 2014|

Journal of Information Sciences and Computing Technologies
www.scitecresearch.com

Review on: Approaches for Finding Correlation Between Fingerprints and Footprints of a Person

Amandeep Singh Dhillon
Research Scholar
Department of Computer Engineering, YCOE,
Talwandi Sabo (Bathinda), Punjab, India
aman_dhillon302@yahoo.com
Ashok Kumar Bathla
Assistant Professor
Department of Computer Engineering, YCOE,
Talwandi Sabo (Bathinda), Punjab, India
ashokashok81@gmail.com

Abstract— This paper analyse the most important and significant advancements in forensic science using fingerprint detection as a biometric sign for identification. Technological advancements from the dawn of the age of the computer to the beginning of the age of the internet, have all created easier and more efficient ways of criminal investigation. Police departments throughout the United States and in other countries now have ways to easily store and share information and eliminate problems that traditional paper records posed. In the case of difficulty in extracting orientation images reliably, a general purpose approach improving local image contrast is favoured. Today time with the increase in population crime increases day by day, and Police Department have over loaded work. To decrease the crime and to identify the theft and criminal, we try to make a new age safety system in which detect the theft by matching his /her Foot finger prints with Hand finger prints. Because due to plastic surgery sometimes criminal change their identity, and protect them self from punishment.

In this work fingerprint and foot finger prints are recognized with the help of minutia because the minutia is the one element of the footprint and fingerprint that helps to find the matching with same and different persons. In this work database is created with the help of different person's footprints and fingerprints. After creating the database the matching of footprints and fingerprints is done with the help of that database and the accuracy of the footprints and the fingerprints are calculated.

Keywords: Footprint; Fıngerprint; accuracy; criminals; identity etc.

I. INTRODUCTION

Along with fingerprints and the corresponding person's name, IAFIS contains a wealth of other information that can be useful. Corresponding mug shots, physical information including hair and eye color, height and weight as well as tattoos, scars and other unique marking, are contained in the records of a single fingerprint or fingerprint set [9]. There are many ways a person can end up in the database currently. Among the most commonly entered prints are those of suspects and other persons convicted of crimes, along with all current and past serving military personal and government employees.

Fingerprint identification is also known as dactyloskopy or also hand identification is the process of comparing two examples of friction ridge skin impression from human fingers, palm or toes. Method of fingerprinting helps police to investigate crimes during long period of time. Human skin has two layers: epidermis and dermis. Dermis has also two layers: papillary reticulated layer. In papillary layer find themselves in pairs pyramidal formations that are called papillary. Each pair of papillary is divided by channels of sweat glands. Such pairs make a row and covered by the layer of epidermis build comb of papillary lines. Papillary lines are situated chaotically but as streams. The first type of papillary pattern is arch papillary pattern. They are simplest in their structure and according to the frequency of meeting – 5%. There are many other civil employees whose fingerprints end up in the database for a variety of reasons [3].

Figure 1.6 Example of fingerprint

Fingerprints and criminal histories of individuals are currently submitted to the database voluntarily by local, state, and federal police agencies. The database currently is home to more than 70 million files in the criminal master file along with more than 31 million civil records [3]. In 2010, the database processed more than 61 million submissions. With all of these records, a typical comprehensive search takes about 27 minutes and a civil search takes about an hour and twelve minutes. Searches for similar prints can now take as little as ten minutes, a process that once took weeks [9]. The use of fingerprints has now expanded far beyond the identification of a corpse and the matching of an unknown print at a crime scene to a suspect.

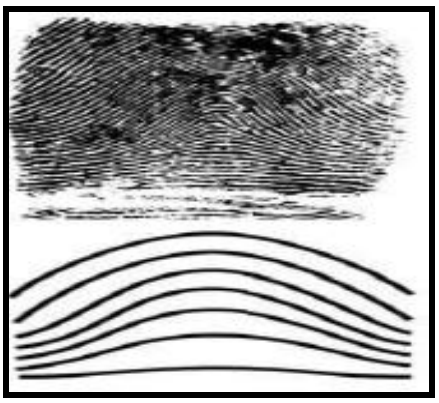

Figure 1.7 Example of arch pattern

The second type is loop papillary pattern. This type is the most popular; about 60%-65% of people have this type of pattern. The picture is built by three streams of lines. The central picture consists of one or more loops, lines start at the end of the pattern and going up, come to the same end. The loop has its head, feet and open part.

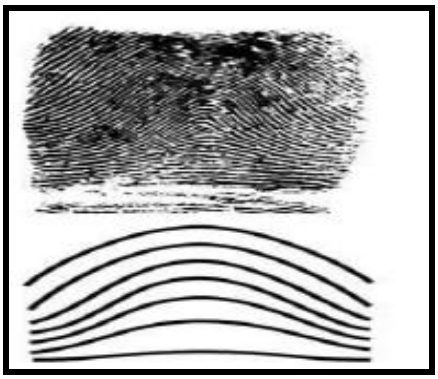

Figure 1.8 Example of loop pattern

The third type is whorl, is met at about 30% of people. The inner picture can be made by papillary lines as ovals, spirals, loops, or their combinations. The characteristic feature of this type is not less than two deltas, one of which is situated on the left side, another- on the right side from inner part of the pattern. As the previous types, this type is also subdivided into tree subtypes: plain whorls, accidental whorls, double loop whorls, central pocket loop whorls.

Private companies, along with most federal and state governmental agencies, use fingerprints in a number of capacities. Most commonly, they are used to help assist in the hiring of individuals and determining if a candidate is well suited for a position within a company. As part of the application and interview process, an increasing number of companies are asking applicants to be fingerprinted as part of a comprehensive background check before hiring [3]. Fingerprints are then sent to an AFIS database, typically the FBI, to be compared to all other prints in the system. This allows a company to know if an applicant has been fingerprinted and entered into the system for any reason, including military service and arrest in connection to a crime. These background checks can often be a deciding factor in whether or not an applicant gets hired. This practice was once only common to governmental hiring, including within the military, police, and other security related positions [3].

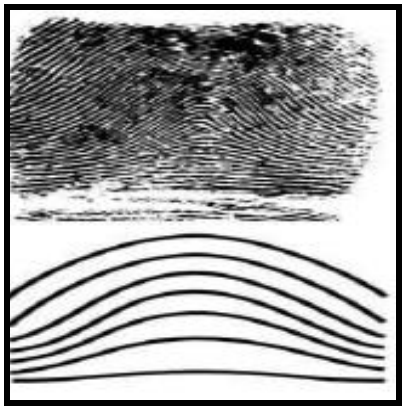

Figure 1.9 .Example of whorl pattern

As our world changes and the threat of terrorism and other crime increases, private companies have begun to

implement this practice. There is heated debate over this practice centering on whether or not it is an invasion of privacy [3]. Skeptics of fingerprinting job applicants also raise the concern of these prints being added to the databases and being used in criminal investigation. Both of these are concerns in today's society but will be discussed later on when focus is turned to the problems and concerns of fingerprint use in criminal investigation. Fingerprint databases now exist in almost every state as well as the FBI [3]. These systems are generally known as Automated Fingerprint Identification Systems, or AFIS. Within each state, it is common practice that most jurisdictions have access to all other jurisdictions' databases. This is not always the case, particularly when there are several versions of software being used in one state. Each company that produces fingerprint database software does not always make their software compatible with one another [3]. The need continues to exist, in many instances, for fingerprints to be sent to several places before a comprehensive search of all fingerprints can be completed. This is typically found to be an issue between the state and federal databases. Most states have a general practice of sending unknown fingerprints to the FBI periodically; helping to keep the nation unified as a whole and creating a greater central database [9]. Once the software for AFIS databases overcomes the differences, identifications will become more accessible and faster for all jurisdictions. This is not to say that the world of fingerprint identification has completely moved away from matches made by trained technicians. There are still many instances when manual identifications can be less time consuming and preferred over AFIS methods [9]. Identifications made in this manner are common when a relative or other person believes that the identity of a victim is known [3]. Reference prints are then taken from the person's home or workplace and used as a marker for comparison. Technician identification can also be used as preliminary method of identification of suspects or victims, or to determine if two prints are from the same person [9]. Once a preliminary match is made, it is often supported with an AFIS identification to be used in court or other legal documents and reports. The main issue with manual identifications, that have brought the field towards AFIS identifications, is that a greater level of uncertainty and possibility for mistake exists [9]. Computer systems allow a technician to overlay two prints and be able to see clearly if they line up and match one another, making certain that each point of comparison is identical on each print [3].

II. Types of Biometric Identifiers

Biometric characteristics of a person are unique. Most of such keys are impossible to copy and exactly produce. Theoretically these are ideal keys. But by using biometric identification a lot of specific problems appear.

All biometric identifiers can be divided into two big groups:

1) Physiological
2) Behavior

Though behavior biometrics is less expensive and less dangerous for the user, physio-logical characteristics offer highly exact identification of a person. Nevertheless, all two types provide high level of identification than passwords and cards.

Spheres of use:

- Criminalistics (biometric identifiers are used to recognize victims, unidentified body and protection of children against kidnapping).
- Marketing (methods of biometrics are used to identify owners of loyal cards).
- Time accounting systems at work, schools, etc.
- Security systems (are use to control the access to the rooms and control access to internet resources).
- Voting system (during the functionality of voting system identification/authentication of people, that take part in voting is demanded).
- According to actual international demands (for example, according to the standard of ICAO there should be biometric part in passport.)
- Biometric identifiers are used for registration if immigrants and foreign workers. It allows identifying people even without documents.
- For organization of distribution of social help.

Methods of biometric authentication differ according their degree of safeness:

- DNA
- Iris recognition
- Fingerprint and Footprint
- Face recognition
- Voice
- Typing Rhythm

Table : 1 Advantages and Disadvantages of biometrics:

No	Advantages	Disadvantages
1	Increase security	Security
2	Can not be copied	Adaptability to rate of change
3	Can not be shared	Scalability
4	Convenience	Miss use
5	Auditable trial	Regulation of use
6	Accuracy	Accuracy
7	Can not be lost	Financial cost
8	Minimize paper work	Privacy
9	Costs	Time

III. LITERATURE SURVEY

Barua et al. (2010) [1]: defines the Fingerprint identification is one of the most popular and reliable personal biometric identification methods. This paper describes an on-line fingerprint identification system consisting of image acquisition, edge detection, thinning, feature extractor and classifier. The pre-processing part includes steps to acquire binarized and skeletonzed ridges, which are needed for feature point extraction. Feature points (minutia) such as endpoints, bifurcations, and core point are then extracted, followed by false minutia elimination. Human fingerprints are richin details called minutiae, which can be used as identification marks for fingerprint verification. The goal of this project is to develop a complete system for fingerprint identification.

Drahansky et al. (2012) [2]: has studied that many people who suffer from some of the skin diseases. These diseases have a strong influence on the process of fingerprint recognition. People with fingerprint diseases are unable to use fingerprint scanners, which is discriminating for them, since they are not allowed to use their fingerprints for the authentication purposes. First in this the various diseases, which might influence functionality of the fingerprint-based systems, are introduced, mainly from the medical point of view. This overview is followed by some examples of diseased finger fingerprints, acquired both from dactyloscopic card and electronic sensors. At the end fingerprint image enhancement algorithm is described.

Habib et al. (2006) [4]: this paper presents a novel mono-vision virtual keyboard design for consumers of mobile and portable computing devices such as PDA's, mobile phones etc. Fuzzy approaches to gesture recognition are developed to reveal the key pressed over the printed sheet keyboard by analyzing the hand and finger gesture captured in the video sequence. Real-time system is developed by integrating SDIO camera with PDA in the application environment. Reliable results are experienced by the implementation of the proposed real time mono vision gestured virtual keyboard system.

Kulshrestha et al. (2012) [12]: have studied the Fingerprints are the most popular and studied biometrics features. Their stability and uniqueness make the fingerprint identification system extremely reliable and useful for security applications. Fingerprints are the oldest and most widely used form of biometric identification. Everyone is known to have unique, immutable fingerprints. Two approaches have been discussed in this that is based on minutiae located in a fingerprint and based on gabor filter which is used to matching the fingerprint.

kumar et al. (2012) [13]: the purpose of this work is to increase the security that customer use the ATM machine. Once user's bank card is lost and the password is stolen, the criminal will draw all cash in the shortest time, which will bring enormous financial losses to customer, so to rectify this problem we are implementing this project. The chip of LPC2148 is used for the core of microprocessor in ARM7, furthermore, an improved enhancement algorithm of fingerprint image increase the security that customer use the ATM machine.

Marasco et al. (2013) [17]: has presented the Biometric systems are widely deployed in governmental, military and commercial/civilian applications. There are a multitude of sensors and matching algorithms available from different vendors. This creates a competitive market for these products, which is good for the consumers but emphasizes the importance of interoperability. Interoperability is the ability of a biometric system to handle variations introduced in the biometric data due to the deployment of different capture devices. The use of different biometric devices may increase error rates. In this -scale empirical study of the status of interoperability between fingerprint sensors and assess the performance consequence when interoperability is lacking.

Modi et al. (2007) [19]: introduce the increasing use of automated fingerprint recognition puts on it a challenge of processing a diverse range of fingerprints. The quality control module is important to this process because it supports consistent fingerprint detail extraction which helps in identification / verification. Medical conditions such as arthritis may affect the user's ability to interact with the sensor, further reducing fingerprint quality. Because quality of fingerprints varies according to the user population's ages and fingerprint quality has an impact on overall system performance, it is important to understand the significance of fingerprint samples from different age groups. This research examines the effects of fingerprints from different age groups on quality levels, minutiae count, and performance of a minutiae-based matcher.

Paulino et al. (2008) [21]: has studied the Identifying suspects based on impressions of fingers lifted from crime scenes (latent prints) is a routine procedure that is extremely important to forensics and law enforcement agencies. In this paper, the author proposes a new fingerprint matching algorithm which is especially designed for matching latest. The proposed algorithm uses a robust alignment algorithm (descriptor-based Hough transform) to align fingerprints and measures similarity between fingerprints by considering both minutiae and orientation field information. To be consistent with the common practice in latent matching (i.e., only minutiae are marked by latent examiners), the orientation field is reconstructed from minutiae. Since the proposed algorithm relies only on manually marked minutiae, it can be easily used in law enforcement applications.

IV. RESEARCH GAPS

The above study of this research topic overcome the different research points of different researchers on the topic of finger prints matching based on their minutiae and the correlation of different points of the fingers. In this the different authors works on different techniques to find the correlation of finger print matching and their percentage of matching with same person and the different persons. There is the research gap between the correlation of footprints and the fingerprints matching based on their minutiae of different persons and the same person to identify the criminals. The previous work is representing the specification of the person for security, but some time

the minutiae is matched with more then one persons that creates the problem to identify the correct person. In this work I have removed the identification problem on the based on foot print and finger prints matching with correlation of same and different persons minutiae.

V. CONCLUSION

Biometrics system has a long history that starts from the very old time and is widely used in these days. This is very important because most of the people think that biometrics as a science appeared not long ago and just used in criminalistics. Although many people even do not realize that biometrics have many different methods. Each method is based on the uniqueness of the measured part of the body. Fingerprinting and Footprint is one of the oldest and most popular method of biometrics is widely used in criminalistics. The main idea of the method is that the picture of papillary pattern is unique for each person. The sample of papillary pattern can be easily taken from any surface that the person touches. It is also considered that fingerprints and footprints are the most popular evidences in the places of crime. In a day and age of advancing technologies, the field of forensic science should not be so quick to get wrapped up in the newest and "best" technology, but must be careful to ensure that there is data and research to back up the evidence before it can reasonably be brought into court. Today time with the increase in population crime increases day by day, and Police Department have over loaded work. To decrease the crime and to identify the theft and criminal, we try to make a new age safety system in which detect the theft by matching his /her Foot finger prints with Hand finger prints. Because due to plastic surgery sometimes criminal change their identity, and protect them self from punishment. In this work fingerprint and foot finger prints are recognized with the help of minutia because the minutia is the one element of the footprint and fingerprint that helps to find the matching with same and different persons. In this work database is created with the help of different persons footprints and fingerprints. After creating the database the matching of footprints and fingerprints is done with the help of that database and the accuracy of the footprints and the fingerprints are calculated. In this work the maximum accuracy of same person matching is 100% and the minimum 67.42% and the different person matching is maximum 57.66 % and below 50% is rejected cases.

VI. REFERENCES

[1]. Barua K., Bhattacharya S., "Fingerprint Identification", Global Journal of Computer Science & Technology, Vol. 11 (Issue 1), (Apr 2011).

[2]. Drahansky M., Dolezel M., "Influence of Skin Diseases on Fingerprint Recognition", Hindawi Publishing Corporation Journal of Biomedicine and Biotechnology, Vol. 26, (Feb 2012).

[3]. B.B., "Science vs. Crime: The Evolution of the Police Lab", Craigmont Publications: New York, (1979).

[4]. Habib H.A., Mufti M., "Real Time Mono Vision Gesture Based Virtual Keyboard System", IEEE Transactions on Consumer Electronics, Vol. 52 (Issue 4), (Nov 2006).

[5].Jain A.K., Bolle R., Pankanti S., "Biometrics: Personal Identification in a Networked Society", Kluwer cademic Publishers, (1999).

[6].James E.S., "A Critical Analysis of Selected Features of Fingerprinting", In Forensic Science and Law: Investigative Applications in Criminal, Civil, and Family Justice, Wecht, Cyril H., Rago, John T. Eds., Taylor and Francis Group: New York, P.P. 299-322.

[7].James M., "Catching the Killers: A History of Crime Detection", Ebury Press: London, (2001).

[8].Katherine R., "The Forensic Science of C.S.I.", Berkley Boulevard Books: New York, (2001).

[9].Kelly M.P., "The U.S. Forensic Laboratory System under Siege Forensic Science under Siege: The Challenges of Forensic Laboratories and the Medico-Legal Death Investigation System", Elssevier: New York, P.P. 51-107.

[10].Kelly M.P., "DNA: Convicting the Guilty, Exonerating the Innocent. Forensic Science Under Siege: The Challenges of Forensic Laboratories and the Medico-Legal Death Investigation System", Elssevier: New York, P.P. 291-340.

[11].Kulshrestha M., "Finger Print Recognition: Survey of Minutiae and Gabor Filtering Approach" International Journal of Computer Applications (0975 – 8887), Vol. 50 (Issue 4), (Jul 2012).

[12].Kumar D.V., Murthy M.R.K., "Fingerprint Based ATM Security by using ARM7", IOSR Journal of Electronics and Communication Engineering (ISSN: 2278-2834) Vol. 2 (Issue 5), (Sep-Oct 2012).

[13].Lopez A.C., Lopez R.R., Queeman R.C., "Fingerprint Recognition" This research is supported by Dr. Roman Lopez mastership thesis and is part of the Polytechnic University of Puerto Rico Capstone course, now in progress .

[14]Lorenzo V.L., Pellitero P.H., Torre J.I.M., Villar J.C., "Fingerprint Minutiae Extraction Based On FPGA and MatLab", DCIS, (2005).

[15].Maio D., "Second Fingerprint Verification Competition", IEEE CS Press, Vol. 3, P.P. 811–814 (2002).

[16]. Maltoni D., "Handbook of Fingerprint Recognition", Springer, (2003).

[17].Marasco L.L., "Interoperability in Fingerprint Recognition: A Large-Scale Empirical Study", IEEE/IFIP International Conference on Dependable Systems and Networks, P.P. 24 – 27, (Jun 2013).

[18].Michael L., Simon A.C., Ruth M., Kathleen J., "Truth Machine: The Contentious History of DNA Fingerprinting", University of Chicago Press: Chicago, (2008).

[19].Modi S.K., Elliott S.J., "Impact of Age Groups on Fingerprint Recognition Performance", IEEE, (2007).

[20].Norah R., Keith I., "Forensic Science Timeline", [Online], (Sep 2011).

[21].Paulino A.A., "Latent Fingerprint Matching Using Descriptor-Based Hough Transform" IEEE Transactions On Information Forensics And Security, Vol. 8 (Issue 1), (Jan 2013).

[22].Ramsland., Katherine., "Beating the Devil's Game: A History of Forensic Science and Criminal Investigation", Berkley Books: New York, (2007).

[23].Senior A., "A Combination Fingerprint Classifier", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 23 (Issue 10), (Oct 2001).

[24].Soni N., Siddiqua A., " Filtering Techniques used for Blurred Images in Fingerprint Recognition", International Journal of Scientific and Research Publications (ISSN 2250-3153), Vol. 3 (Issue 5), May 2013.