Everant.org/ETJ

Research Article

Engineering and Technology Journal ISSN: 2456-3358

Image Enhancement of Human Fingerprints Using Feature Extraction & Matching Techniques

Vikas

Assistant Professor ECE Department , SITM, Sonipat , Haryana, India

ARTICLE INFO

corresponding Author:
Vikas
Assistant Professor ECE Department , SITM, Sonipat , Haryana, India

ABSTRACT

Biometrics, which mentions to identification based on physical or behavioural characteristics, is being progressively adopted to provide positive identification with a high degree of confidence. Among all biometric techniques, fingerprint-based authentication schemes have established most attention because of long history of fingerprints and their extensive use in forensics. Fingerprints are a great source for identification of individuals. Fingerprint recognition is one of the forms of biometric identification. However obtaining a decent fingerprint image is not always easy. So, fingerprint image must be pre-processed before matching. The main objective of this work is to design an image matching algorithm which is applied to any image for matching. For efficient enhancement and feature extraction procedures, the segmented structures must be void of any noise. A pre-processing method containing of field orientation, ridge frequency approximation, filtering, separation and enhancement is performed. The attained image is applied to a thinning algorithm and subsequent minutiae removal. The organization of image pre-processing and minutiae extraction is deliberated. The simulations are performed in the MATLAB environment to evaluate the performance of the implemented algorithms. MATLAB provides a useful environment for these developments. Results and observations of the fingerprint images are presented at the end.

KEYWORDS- ***Fingerprinting, pattern recognition, feature extraction, image enhancement, fingerprints minutia.***

I. INTRODUCTION

Image processing is a rapidly growing area of computer science. Its growth has been fuelled by technological advances in digital imaging, computers and mass storage devices. Fields which traditionally used analog imaging are now switching to digital schemes, for their flexibility and affordability. Important examples are film and video construction, photography, remote sensing, and security monitoring. These and other sources produce huge volumes of digital image data every day, more than could ever be examined automatically [1].

Digital image processing is concerned primarily with extracting useful info from images. Ideally, this is done by computers, with little or no human interference. Image processing algorithms may be placed at three levels. Atlowermost level are those techniques which deal directly with raw, perhaps noisy pixel values, with de-noising and edge detection being good instances. In the middle are algorithms which utilise low level results for

Published Vol. 2 Issue 2 Feb. 2017
DOI: 10.18535/etj/v2i2.01
Page no.- 139-147

further means, such as segmentation and edge connecting. At the highest level are those methods which attempt to extract semantic meaning from the information provided by the lower levels, for example, handwriting recognition. Most images are the result of measuring a specific physical phenomenon, such as light, heat or energy. The measurement could take any numerical form [2].

Today there is almost no area of technical endeavour that is not impacted in some way by digital image processing. The regions of application of digital image processing [4] are so varied that some form of organization is desirable in attempting to capture the breadth of this field. One of simplest ways to develop a basic understanding of the extent of image processing applications is to categorize images according to their source (e.g., visual, X-ray, and so on). The main energy source for images in use today is the electromagnetic energy spectrum. Other important sources of energy contain acoustic, ultrasonic, and electronic. Image noise is generally regarded as an undesirable by-product of image capture because it causes distortions present in the image that can obscure the subject of the photograph. Although these unwanted fluctuations became known as "noise" by analogy with unwanted sound they are inaudible and can actually be beneficial in some requests, such asdithering [3].

An image signal gets corrupted with noise during acquisition, communication, storage and retrieval processes. Acquisition noise is mainly additive white Gaussian noise (AWGN) with very low variance. In various engineering applications, the acquisition noise is quite negligible. It is mostly due to very high quality sensors. In some applications like remote sensing, medical instrumentation, etc., the acquisition noise may be high enough. But in such a system, it is mostly due to the fact that the image acquisition system itself comprises of a transmission channel. So if such noise problems are measured as transmission noise, then it may be decided that acquisition noise is negligible. Therefore, the researchers are mainly concerned with the noise in a transmission system. Usually, the transmission channel is linear, but dispersive due to a limited bandwidth [5].

The paper is organized as follows. In section II, it provides introduction about biometrics. In Section III, It describes steps of fingerprinting system. In Section IV, it describesthe design and implementation algorithms used in fingerprinting image processing technique. The results are given in Section V.Finally, conclusion is explained in Section VI.

II. BIOMETRICS

Biometrics, which refers to identifying an individual based on his or her physiological or behavioural characteristics, has the ability to reliably distinguish between an authorized person and an imposter. Since biometric characteristics are unique, cannot be forgotten or lost, and the person to be authenticated needs to be physically present at the point of identification, biometrics is integrally more reliable and more capable than traditional knowledge-based and token-based techniques. Biometrics also has a number of difficulties. For example, if a password or an ID card is compromised, it can be easily replaced. However, once a biometrics is compromised, it is not possible to substitute it. Similarly, users can have a different password for each account, thus if the password for one account is compromised, the other accounts are still safe. However, if a biometrics is conceded, all biometrics-based accounts can be broken-in. Among all biometrics (e.g., face, fingerprint, hand geometry, iris, retina, signature, voice print, facial thermo-gram, hand vein, gait, ear, keystroke subtleties, etc.), fingerprint-based identification is one of the most mature and proven technique [6].

Published Vol. 2 Issue 2 Feb. 2017
DOI: 10.18535/etj/v2i2.01
Page no.- 139-147

1. Applications of Biometrics

Biometrics has been widely used in forensics applications such as criminal identification and prison security. The biometric technology is quickly evolving and has a very strong potential to be widely adopted in civilian applications such as automated banking, e-commerce, and access control. Due to a rapid increase in number and use of electronic transactions, automatic banking and electronic commerce are becoming one of the most important emerging applications of biometrics. These applications include credit card and smart card security, ATM security, check cashing and fund transferals, online transactions and web admittance. The physical access control applications have traditionally used token-based authentication. With the progress in biometric technology, these applications will increasingly use biometrics for authentication. Remote login and data access applications have traditionally used knowledge-based verification. These applications have already started using biometrics for person authentication. The use of biometrics will become more extensive in coming years as the technology matures and becomes more trust worthy. Other biometric applications include welfare disbursement, migration checkpoints, national ID, voter and driver registration, and time and attendance [7].

III. FINGERPRINTING PROCESSING

Fingerprints are the patterns formed on the epidermis of the fingertip. The fingerprints are of three types: arch, loop and whorl. The fingerprint is self-possessed of ridges and valleys. The interweaved pattern of ridges and valleys are the most evident structural characteristic of a fingerprint. The fingerprint of every individual is considered to be unique. No two persons have the same set of fingerprints. Also, Finger edge patterns do not alter throughout the life of an individual. This property makes fingerprints an excellent biometric identifier. So it is one of widespread and effective means for identification of an individual and used as forensic indication. Skin on human fingertips contains ridges and valleys which organized forms distinctive patterns. These patterns are fully established under pregnancy and are permanent throughout whole lifetime. Prints of those patterns are called fingerprints. Injuries like cuts, burns and bruises can provisionally damage quality of fingerprints but when fully healed, patterns will be restored [8].

Figure 1: A Fingerprint Image Obtained by Optical Sensor [4]

Due to above mentioned properties; fingerprints are very widespread as biometrics measurements. Unfortunately fingerprint matching is a complex pattern recognition problem. Manual fingerprint matching is not only time consuming but education and training of experts takes a long time [9].

1. Fingerprint Formation

Fingerprints are fully formed at about seven months of fetus development and finger ridge configurations do not change throughout the life of an individual except due to accidents such as bruises and cuts on the finger tips. This property makes fingerprints a very attractive biometric identifier. Biological organisms, in general, are the

Published Vol. 2 Issue 2 Feb. 2017
DOI: 10.18535/etj/v2i2.01
Page no.- 139-147

consequence of the interaction of genes and environment. It is assumed that the phenotype is uniquely determined by the interaction of a specific genotype and a specific environment. Physical appearance and fingerprints are, in general, a part of an individual's phenotype. In the case of fingerprints, the genes determine the general characteristics of the pattern. Fingerprint formation is similar to the growth of capillaries and blood vessels in angiogenesis. The general characteristics of the fingerprint emerge as the skin on the fingertip begins to differentiate.

However, the flow of amniotic fluids around the fetus and its position in the uterus change during the differentiation process. Thus, the cells on the fingertip grow in a microenvironment that is slightly different from hand to hand and finger to finger. The finer details of the fingerprints are determined by this changing microenvironment. A small difference in microenvironment is amplified by the differentiation process of the cells. There are so many variations during the formation of fingerprints that it would be virtually impossible for two fingerprints to be alike [10].

2. Fingerprint Individuality

Until recently, the testimony of latent fingerprint examiners was admitted in courts without much scrutiny and challenge. However, in the 1993, the Supreme Court ruled that the reliability of an expert scientific testimony must be established. Additionally, the court stated that when assessing reliability, the following five factors should be considered: (i) whether the particular technique or methodology in question has been subject to a statistical evaluation (hypothesis testing), (ii) whether its error rate has been established, (iii) whether the standards controlling the technique's operations exist and have been maintained, (iv) whether it has been peer reviewed, and published, and (v) whether it has a general widespread acceptance [11].

The two fundamental properties on which fingerprint identification is based are: (i) fingerprint details are permanent, and (ii) fingerprints of an individual are unique. The validity of the first principle has been recognized by empirical observations as well as based on the anatomy and morphogenesis of friction ridge skin. It is the second premise which is being challenged in recent court cases [12].

3. Fingerprint Sensors

The fingerprint images may be acquired either by an offline or an online process. The fingerprint images acquired by the offline process are known as the "inked" fingerprints while the images acquired by the online process are known as "live-scan" fingerprints. Inked fingerprints are of three types: (i) rolled, (ii) dab, and (ii) latent. In the rolled method of fingerprint acquisition, ink is applied to the finger and then rolled on a paper from one side of the nail to the other to form an impression. The rolled fingerprints have a larger ridge and furrow area due to the rolling process but have larger deformations due to the inherent nature of the rolling process. In the dab method of fingerprint acquisition, ink is applied to the finger and then pressed onto a paper without rolling. The paper is then scanned into a digital image. Typically, dab inked fingerprints have less nonlinear deformation but smaller area than the rolled inked fingerprints. Latent fingerprints are formed when the fingers leave a thin layer of sweat and grease on the surfaces that they touch due to the presence of sweat pores in our fingertips. Forensic scientists dye this impression which is typically found at the scene of a crime with color and then scan the fingerprint [13].

A live-scan fingerprint is attained directly from the finger without the in-between use of paper (at a resolution of 500dpi). Typically, live-scan sensors capture a series of dab fingerprints when a finger is hard-pressed on the sensor surface. For rolled live-

Published Vol. 2 Issue 2 Feb. 2017
DOI: 10.18535/etj/v2i2.01
Page no.- 139-147

scan fingerprints, the user rolls her/his finger from one end of the nail to the other on the sensor surface and the sensor capture a number of dab fingerprint images. The rolled fingerprint image is then constructed by mosaicking the multiple dab images captured during the rolling process [14].

4. Fingerprint Representation

The popular fingerprint representation schemes have evolved from an intuitive system developed by forensic experts who visually match the fingerprints. These schemes are either based on predominantly local landmarks (e.g., minutiae-based fingerprint matching systems or exclusively global information (fingerprint classification based on the Henry system. The minutiae-based automatic identification techniques first locate the minutiae points and then match their relative placement in a given finger and the stored template. A good quality inked fingerprint image contains between 60 to80 minutiae, but different fingerprints and different acquisitions of the same finger have different numbers of minutiae. A graph-based representation constructs a nearest neighbor graph from the minutiae patterns. The matching algorithm is based on inexact graph matching techniques. The point pattern-based representation considers the minutiae points as a two-dimensional pattern of points. Correlation-based techniques consider the gray level information in the fingerprint as features and match the global patterns of ridges and valleys to determine if the ridges align [15].

The global representation of fingerprints (e.g., whorl, left loop, right loop, arch, and tented arch) is typically used for indexing, and does not offer good individual discrimination. Further, the indexing efficacy of existing global representations is poor due to a small number of categories (typically five) that can be effectively identified automatically and a highly skewed distribution of the population in each category. The global representation schemes of the fingerprint used for classification can be broadly categorized into four main categories: (i) knowledge-based, (ii) structure-based, (iii) frequency-based, and (iv) syntactic [20]. The knowledge-based fingerprint representation technique uses the locations of singular points (core and delta) to classify a fingerprint into five major classes (whorl, left loop, right loop, arch, and tented arch). A knowledge-based approach tries to capture the knowledge of a human expert by deriving rules for each category by hand-constructing the models and therefore, does not require training. Structure-based approach uses the estimated orientation field in a fingerprint image. Frequency-based approaches use the frequency spectrum of the fingerprints for representation. Hybrid approaches combine two or more approaches for representation [16].

5. Fingerprint Classification

Large capacities of fingerprints are collected and stored every day in a wide choice of applications, including forensics, admittance control, and driver license registration. Automatic individuality recognition based on fingerprints requires that the involvement fingerprint be matched with a large number of fingerprints stored in a record (the FBI database currently contains more than 630 million fingerprints!). To reduce the search period and computational complexity, it is needed to classify these fingerprints in an accurate and reliable manner such that the input fingerprint needs to be matched only with a subset of the fingerprints in database. Fingerprint classification is a technique used to allocate a fingerprint into one of the several pre-specified types already recognized in the literature (and used in forensic applications) which can provide an indexing mechanism. Fingerprint classification can be viewed as a coarse level matching of the fingerprints. An input fingerprint is first matched to one of the pre-specified types and then it is

Published Vol. 2 Issue 2 Feb. 2017
DOI: 10.18535/etj/v2i2.01
Page no.- 139-147

compared to a subset of the database corresponding to that fingerprint type [17].

.

6. Fingerprint Verification

A biometric system can be operated in two modes: 1) verification mode and 2) identification mode. In the verification mode, a biometric system either accepts or rejects a user's claimed identity while a biometric system operating in the identification mode establishes the identity of the user without a claimed identity. Fingerprint identification is a more difficult problem than fingerprint verification because a huge number of comparisons need to be performed in identification. For example, in an ATM application, after a user has been registered and issued an ATM card, the acquired fingerprint needs to be matched only with a single template fingerprint stored on the ATM card on each transaction. A typical verification system can be divided into two modules: (i) enrolment and (ii) verification. The enrolment module scans the fingerprint of a person through a sensing device and then stores a representation (called template) of the fingerprint in the database. The verification module is invoked during the operation phase [18].

7. Information Fusion

A number of fingerprint verification systems have been developed and tested on large databases but most of them are not able to meet the rigid performance requirements in high security applications. Each fingerprint verification system uses different feature extraction and/or matching algorithms to generate a matching score which is used for authentication. It is well known in the pattern recognition literature that different classifiers often misclassify different patterns. This suggests that different classifiers offer rather complementary information about the given classification task. A combination scheme which harnesses various information sources is likely to improve the overall system performance. The outputs of various classifiers can be combined to obtain a decision which is more accurate than the decisions made by any one of the individual classifiers [19].

IV. DESIGN AND IMPLEMENTATION

In recent years, there have been significant advancements in algorithms and architectures for the processing of image. These advancements have proceeded along several directions.

A. Proposed Algorithm of Image Enhancement

1. Read the input RGB/ Gray Scale Image.
2. Set three ranges lies between 0 & 1.
   a. Lower limit=0.001
   b. Upper Limit=0.99
   c. Mid limit=0.5
   a. If (r=3) then
      - Mid limit2=0.02
      - Mid limit3=-0.02
   b. Convert RGB to gray scale & separate R, G & B.
   c. Mean Adjust= mid limit2- mean(Green Components) Image (green) = image (green) + mean adjust.
   d. Mean Adjust= mid limit3- mean(Blue Components) Image (Blue) = image (Blue) + mean adjust. Else
      - Divide image by 255.
3. Mean Adjust= mid limit- mean(Red Components)
   Image (Red) = image (Red) + mean adjust.
4. If (r=3) then
   - Convert gray to RGB.

   Else
   - Multiply with 255.
5. Find min. & max values by using lower and upper limits.
6. Find the slope of image, multiply with 255 and we get enhanced image.
7. Calculate Mean error and PSNR also.

Published Vol. 2 Issue 2 Feb. 2017
DOI: 10.18535/etj/v2i2.01
Page no.- 139-147

B. Proposed Algorithm of Fingerprinting Matching

1. Read two input images manually.
2. Find the enhancement of images by mean adjustment technique.
3. Separate R, G and B by image segmentation process.
4. Apply thresholding process to remove noise.
5. Find the thinning of images by morphological operations.
6. Find features of extracted images.
7. Find the differences of two images.
8. If differences are detected, then images are not same, else they are same.

V. RESULTS

The fingerprint image must be pre-processed before matching. For fingerprint matching, it requires two input images. One is of victim and one for comparison. The figure 2 and 3 show the original 1st and 2nd image respectively and figure 4shows the enhancement of image by mean adjustment technique. Enhancement of images is done by pixel approach. Using pixels, it can affect the intensity of images. Enhancement is calculated with help of mean square error and PSNR parameter.

Figure 2: Original Input First Fingerprint Image

Figure 3: Original Input Second Fingerprint Image

Figure 4:Enhanced Image

Segmentation is basically separation of R, G and B colours from the images. It can be done using segmented process. Firstly, it needs only gray scale images. So RGB is converted to gray scale image and then distinct these bands. Segmented output is shown in figure 5.

Figure 5:Segmented Image

Published Vol. 2 Issue 2 Feb. 2017
DOI: 10.18535/etj/v2i2.01
Page no.- 139-147

After thinning process, features of image are required to be extracted. So regionprops are used for feature extraction process. And complete features within original thinned image are found. After this, both images are applied to fingerprinting matching system which matches images pixel by pixel. For this, it calculates the difference of the images. If both are matched, then difference image shows no error. But if both are different, then it shows error image as shown in fig 9.

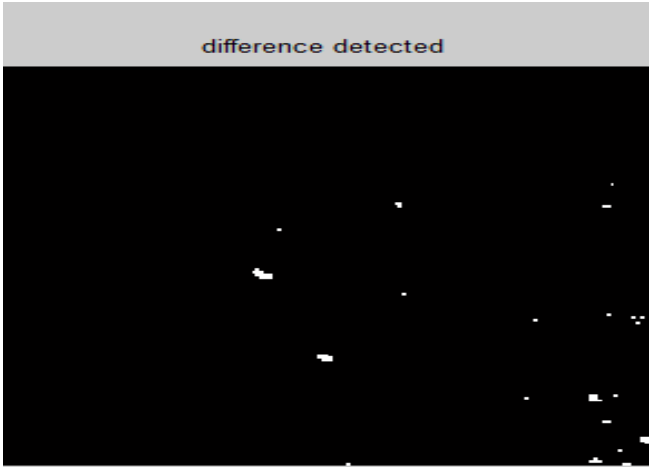

Figure 9:Difference Detected Output

Table 1: Performance Comparison Values

Peak Signal to Noise Ratio (PSNR) Comparison		
Images	PSNR (Proposed)	PSNR (Actual)
Image 1	24.14	11.25
Image 2	25.39	9.23
Computation Time Comparison of Pixel Based & Block Based Technique		
Computation Time	Proposed (Pixel based)	Full Search (16)	Full Search (32)
	16.9 sec	1089 sec	4225 sec

VI. CONCLUSION

The goal of this thesis is to design a system of image matching. It is used in the application of fingerprint matching system. It is used to study the security impact of partial fingerprints on automatic fingerprint recognition systems and to develop an automatic system that can overcome the challenges presented by partial fingerprint matching.The proposed algorithm is implemented in MATLAB. The reliability of any instinctive fingerprint system strongly relies on precision obtained in the minutia extraction process. A number of factors are harmful to the correct location of minutia. Among them, poor image quality is the most serious one. In this work, we have shared many methods to build a minutia extractor and a minutia matcher. The proposed system shows that it has less value of MSE than histogram technique. It also shows that it provides low computation time as compared to block based technique. The results provide good image matching software which is used to match any format of images or any size.

REFFERENCES

1. Josef StrömBartun,"Image Enhancement in the JPEG Domain for People with Vision Impairment," IEEE Trans. Biomed. Eng., vol. 50, no. 10, pp. 2013.
2. Madhuri, "Virtual Restoration of Ancient Chinese Paintings Using Color Contrast Enhancement and Lacuna Texture Synthesis," IEEE Trans. Image Process., vol. 13, no. 4, pp. 416-429, 2012.
3. Nasibe Akbariet. al. "Whiteboard Scanning and Image Enhancement," Digital Signal Process., vol. 17, no. 2, pp. 414-432, March 2012.
4. P. Fridman, "Radio Astronomy Image Enhancement in the Presence of Phase Errors using Genetic Algorithms," in Int. Conf. on Image Processing, Thessaloniki, Greece, Oct 2001, pp. 612-616.

Published Vol. 2 Issue 2 Feb. 2017
DOI: 10.18535/etj/v2i2.01
Page no.- 139-147

5. Y. Tsai, L. Yongbum, M. Sekiya, S. Sakaguchi, and I. Yamada, "A Method of Medical Image Enhancement using Wavelet Analysis," in 6th Int. Conf. Signal Process., Beijing, China, Aug 2002, pp. 724-726.
6. K. Teddy, "Fingerprint Enhancement by Spectral Analysis Techniques," in 31st Applied Imagery Pattern Recognition Workshop, Washington DC, WA, Oct 2002, pp15.18.
7. Andrés Almansa And Tony Lindeberg, Member, IEEE, Fingerprint Enhancement By Shape Adaptation Of Scale-Space Operators With Automatic Scale Selection, IEEE Transactions On Image Processing, Vol. 8, No. 12, December 2000.
8. HartwigFronthaler, Klaus Kollreider, And Josef Bigun, Local Feature Extraction In Fingerprints By Complex Filtering, IWBRS 2005, LNCS 3781, Pp. 76–84, 2005.Springer-Verlag Berlin Heidelberg 2005.
9. Koichi Ito1, Ayumi Morita1, Takafumi Aoki1, Hiroshi Nakajima2, Koji Kobayashi2, And Tatsuo Higuchi, A Fingerprint Recognition Algorithm Combining Phase-Based Image Matching And Feature-Based Matching, LNCS 3832, Pp. 315–325, 2005.
10. W. Armitage, and J. P. Oakley, "Noise Levels in Colour Image Enhancement," in Visual Inform. Eng., London, UK, July 2003, pp. 104-108.
11. A.M. Bazen and S.H. Gerez. An intrinsic coordinate system for fingerprint matching. In *Proc. Int. Conf. on Audio- and Video-Based Biometric Person Authentication(3rd)*, pages 198–204, 2001.
12. Kaijun Tang, JaakkoAstola, Member, IEEE ,and Yrjo Neuvo , Fellow, IEEE "multichannel Edge Enhancement in Color Image Processing" Vol-4 No-6 October 1994.
13. S. Chikkerur, C. Wu, and V. Govindaraju. A systematic approach for feature extraction in fingerprint images. In *International Conference on Biometric Authentication*,2004.
14. Asker M. Bazen A, Martijn Van Otterlo, A Reinforcement Learning Agent For Minutiae Extraction From Fingerprints, Dept. Of Electrical Engineering, Signals and Systems, Dept. Of Computer Science, TKI.
15. Fernando Alonso-Fernandez, Julian Fierrez-Aguilar, Javier Ortega-Garcia, An Enhanced Gabor Filter-Based Segmentation Algorithm for Fingerprint Recognition Systems, Fernando Alonso-Fernandez, Julian Aguilar, Javier Ortega-Garcia Biometrics Research Lab.- ATVS, Politecnica Superior Universidad Autonoma de Madrid, Spain.
16. I. Nedeljkovic, Zahumska, Serbia and Montenegro "image classification based on fuzzy logic worked Fuzzy logic is relatively young theory".
17. Milind kumar V. Sarode, Dr. S.A. Ladhake, Dr. Prashant R. Deshmukh "Fuzzy system for color image enhancement ". World Academy of Science and Engineering Technology 48 2008.
18. R. C. Gonzalez and R. E. Woods, "Digital Image Processing", Reading. MA: Addison Wesley, 2004.
19. David Salomon, Data Compression, The Complete Reference, 2nd Edition Springer-Verlag 1998.
20. Jain, Fundamentals of Digital Image Processing. EnglewoodCliffs, NJ: Prentice-Hall, 1989.

Published Vol. 2 Issue 2 Feb. 2017
DOI: 10.18535/etj/v2i2.01
Page no.- 139-147