

Biometrics Hand Geometry Using Discrete Cosine Transform (DCT)

Muzhir Shaban Al-Ani, Maha Abd Rajab*

Anbar University, Anbar, Ramadi, Iraq

Abstract Biometrics are used for identification of individuals based on their physical or behavioral characteristics. Biometrics have gained importance in today's world where information security is essential. Hand geometry is one of the most well-known biometrics that implemented in many verification systems with various feature extraction methods. Hand biometrics are extensively used for personal authentication. This paper is implemented to compute features extraction using two dimensional discrete cosine transform (2D-DCT). The evaluation of the system performance is calculated using matching metrics correlation.

Keywords Hand Geometric, DCT, Biometrics Recognition, Hand Biometrics, Correlation Matching

1. Introduction

Biometric technologies have been the source of much debate lately as governments have outlined their long term vested interests in them by proposing large scale implementations, such as biometric passports. Such interest from government has been reinforced by increasing commercial interest. As biometrics are intrinsically related to identification and authorization, security and privacy concerns become unavoidable. Inadequate handling of either aspect can severely jeopardize biometric data which are tightly linked with personal identity. The term biometrics comes from the combination of the Greek words 'bios', which means life, and 'metrikos', which in its turn means measuring. Biometric technologies aim primarily at identifying a person's unique features, be those physiological or behavioral. While physiological (or passive) biometrics refer to fixed or stable human characteristics, behavioral (or active) biometrics measure characteristics represented by skills or functions performed by an individual. Examples of physiological biometrics are fingerprints, iris patterns, hand geometry, DNA and facial image, while signatures, keystroke dynamics and mouse movements belong to behavioral biometrics. Two general uses of biometrics are identification and verification which both require the existence of reference data that the person's measured traits will be compared with reference templates or raw data. During these processes, a biometric data sample is compared against the respective biometric data of every person enrolled in the database or against a single reference

template of a particular enrolled individual in order to confirm the identity of that person respectively. When a biometric system correctly identifies a person, then the result of the identification process is a true positive, whereas if the system correctly rejects a person as not matching the respective enrolled template, the result is a true negative[9].

2. Personal Identification Technology

An individual's identity can be established based on an object or token that the person possesses, something that the person knows, or a physical characteristic of the person. Keys, identification cards, and credit and debit cards are all examples of objects that can be used to establish our identity and authorize our access to our homes, cars, workplaces, funds, and credit. Although physical objects are often effective means of identification, they can be lost, stolen, copied, or counterfeited. Information an individual knows can be a combination, an account number, a password, or some other information (such as mother's maiden name). This information can increase security when it is used properly, but it is often forgotten, or it is written where it can be copied or stolen. An individual physical and behavioral characteristic, which we will term biometric information, has often been used to supplement other types of information to increase security. Pictures, physical descriptions, and signatures are examples of biometric information that has been used to establish identity. Use of biometric information can avoid some of the problems that are present with physical tokens or specific knowledge. However, because biometric information is complex and may change over time, the process used to judge whether two biometrics come from the same individual is difficult and may be prone to error. Biometric identification technology uses automated methods

* Corresponding author:

mahaabd12@yahoo.com (Maha Abd Rajab)

Published online at <http://journal.sapub.org/scit>

Copyright © 2013 Scientific & Academic Publishing. All Rights Reserved

to recognize the identity or verify the claimed identity of an individual based on physical or behavioral characteristics (Mansfield & Roethenbaugh, 1998). A biometric identification device is capable of measuring individual biometric information, comparing the resulting measurement with one or more stored biometric reference templates, deciding whether they match sufficiently to indicate that they represent the same person, and indicating whether or not a recognition or verification of identity has been achieved. Devices differ according to the type of biometric information they collect and the algorithms they use to process the information and detect matches[2].

3. Biometrics

Biometrics is the term used to describe the use of biological, physical or behavioral characteristics used to identify a person. The word is derived from the Greek words *bios*, meaning life, meaning measure. It includes the use of measurable, robust and distinctive characteristics. Robust is the term used to describe the changeability of the characteristic over time. Biometrics have a long history and are inextricably linked with forensic sciences. Many of the emerging biometric areas are mature forensic disciplines and it is the use of biometrics for identification and authentication in IT systems that is the emerging technology. This view is supported by a number of recent surveys, including the 2005 CSI/FBI Computer Crime survey which indicated that only 15% of 687 respondents (organizations) are currently using biometrics⁷. A similar survey indicated only 4% of 181 Australian organizations are using biometrics⁸. There are some indications that biometrics were used by the ancient Egyptians by measuring people for identification purposes. In ancient Babylon, fingerprints were used on clay tablets for business transactions. In ancient China, thumb prints were found on clay seals. There are also some early records of the use of biometrics by the Chinese in the 14th century, recording children's palm and footprints, again for identification purposes. In the western world, the first recorded texts started appearing in the mid-17th century but it wasn't until the mid 19th century that the use of fingerprints was used. By the early 20th century several police forces were using fingerprints to assist in the prosecution of criminals. The use of biometric technologies has been in evidence since the 1970's but advances in all aspects of information technology, together with identification, authentication and security needs are now driving the development and implementation of biometric technologies[3].

3.1. Types of Biometrics

Today biometrics are used mainly for forensic purposes although identification and authentication uses are growing rapidly. Biometrics can be broadly grouped into four areas of biometrics with several techniques in each: Hands, Heads and face, Other physical characteristics and Behavioral

characteristics. Some biometric techniques are confined to the laboratory but as technology improves, these techniques may be developed into practical applications. The first three categories are physiological and are based on measurement of a physical characteristic. Except in the case of a serious accident or operation, these biometrics are generally unchanged or change very slowly over time. Examples include fingerprints, hand geometry, iris and retinal patterns and DNA. Behavioral characteristics also have a physiological component, for example, the physiology of the vocal cords, hand and finger dexterity. However, behavioral biometrics are generally seen as having two key components, a measurable action and a time reference for that action. For example, a gait biometric measures stride length and time as well as other characteristics. Behavioral biometrics are less consistent and can be subject to change over time, for instance signatures. They can also change when the individual is under stress, ill or tired. These are also sometimes known as bio-dynamics. There is a further category of acquired recognition characteristics including tattoos, scars, rings, brands and implanted devices such as RFID tags. These are often referred to as SMT (scars, marks and tattoos) but are not reliable indicators as they can change relatively easily. There are a number of desirable properties for any chosen biometric characteristic. These include:

- Universality. Everyone should have it;
- Uniqueness. It is not shared or reproduced in another;
- Permanence. It should be stable and not change over time; and
- Collectability. It can be (practically) measured[3].

Table 1 below lists current biometric techniques and provides a more detailed overview of biometric technologies [3].

Table 1. Biometric Techniques

Category	Biometric or Technique
Hands	Fingerprints
	Palm prints
	Hand geometry
	Hand, palm and wrist vein patterns
	Spectroscopic skin analysis
Heads and Face	Nailbed scanning
	Face recognition
	Iris
	Retina
Other Physical Characteristics	Ear shape and size
	Body salinity
	Blood chemistry
	Body odour
	DNA
	3D thermal imaging
Behavioural Characteristics	Neural wave analysis
	Gait
	Voice recognition, Signature recognition
	Signature recognition
	Keystroke dynamics

Fingerprints

Biometric fingerprints are digitized version of fingerprint systems used for over 100 years by law enforcement agencies. Fingerprinting is a well-established forensic technique with automated fingerprint systems first becoming commercially available in the 1970's. In biometric systems, users place a finger (usually the index finger or thumb) on a reader that scans and identifies the characteristic features. Template sizes range from 50 bytes to 1,000 bytes[3].

Hand/Finger Geometry

This biometric is the measurement of the characteristics of the hands and/or fingers. It does not analyze palm or fingerprints. In these systems the user places their hand onto a reader, usually with pegs or indentations to guide the placement of the hand. These systems have been in use for over 30 years in access control applications. Approximately 20 to 30 length and thickness measurements are typically recorded although some systems can take almost

100 measurements including knuckle size and shape and distance between joints. Barring injury, hand and finger geometry remains stable over the life of the individual although some changes can occur from disease, environmental or other factors. While hand and finger geometry is diverse it is not sufficiently distinctive to be used for identification purposes. Hand templates are typically 9 bytes and finger templates between 20 and 25 bytes in size [3].

Facial Recognition

Humans use facial recognition as their primary means of identifying other humans. This records the spatial geometry of facial characteristics such as the distance between eyes, size of mouth and so on. This technique is typically used to compare a current scan to a reference template such as in access control applications or to compare to a static image, such as digitized passport photograph. It is sensitive to environmental variables such as dust and lighting and other factors such as facial expression, facial hair, hats and spectacles. The use of video cameras make this the only biometric technique that can practically be used in surveillance applications. Templates are typically between 80 and 1,000 bytes in size[3].

Signature Verification

This biometric analyses signature characteristics such as total time, speed, acceleration, character direction, stroke order, stroke count, pressure and contact with the writing surface. These templates are typically 50 to 300 bytes in size[3].

Iris Scan

Iris scans measure and identify the characteristics of the iris, the colored ring surrounding the pupil of the eye. The camera can capture the image from a distance of up to one meter. Iris patterns are random thus left and right iris patterns are different as are those of identical twins. These patterns are formed in the eighth month of gestation and barring

injury, remain stable throughout the life of the individual. The color of the iris is not a component of this biometric as color is not sufficiently distinct. The iris can have approximately 270 distinct characteristics including the trabecular meshwork, striations, rings, furrows, freckles and a corona. A high-quality black and white image of the iris is taken for processing into a template that is typically around 256 bytes in size[3].

Gait

Human gait recognition system has many advantages as biometric option, such as being an unobtrusive technology, can be captured at a distance, it does not require the consent of the observed individual and it is very difficult to steal, fake or hide[1].

3.2. Applications of Biometric Technology

Although policing is primarily a law enforcement activity, those in the policing profession must have at least a working knowledge of a wide variety of other types of activities in order to become good at law enforcement. Biometrics are used in many areas other than law enforcement. To only consider the use of biometrics in the law enforcement realm would thus be limiting. Modern policing requires its practitioners to see beyond their realm in order to be truly effective[4]: Law Enforcement, Banking, Benefit Systems, Computer/Network Security, Immigration, National Identity, Physical Access., Prisons and Correctional Facilities, Telecommunications, Employee Monitoring[4].

4. Hand Geometry

Hand Geometry recognition systems are based on a number of measurements taken from the human hand, including its shape, size of palm, and lengths and widths of the fingers. Commercial hand geometry-based verification systems have been installed in various places around the world. The technique is very simple relatively easy to use, and inexpensive. Environmental factors such as dry weather or individual anomalies such as dry skin do not appear to have any negative effects on the verification accuracy of hand geometry-based systems. The hand images can be obtained by using a simple set up including a web cam. However, other biometric traits require a specialized, high cost scanner to acquire the data. The user acceptability for hand geometry based biometrics is very high as it does not extract detail features of the individual. Thus, for applications where the biometric features are needed to be distinctive enough for verification, hand geometry can be used. An individual's hand does not significantly change after a certain age. Unlike fingerprints, the human hand is not unique. Individual hand features are not descriptive enough for identification. However, hand biometric recognition systems are accurate for the verification purposes when combined with various individual features and measurements of fingers and hands[5].

4.1. Applications of Hand Geometry Biometrics

Hand biometric systems are currently among the most widely used biometric technologies.

- Cash Vault Application[5].
- Dual Custody Applications.
- Anti-pass Back.
- Time and Attendance.
- Point of Sale Applications.
- Interactive Kiosks.
- Parking Lot Application.

4.2. Hand Geometry: Advantages and Disadvantages

Hand geometry has several advantages, including:

- Ease of use. The technology is simple to use and has been in widespread use for many years. It does not carry the negative perceptions of fingerprints and is perceived to be less intrusive than iris and retinal scans. Most users have sufficient dexterity to easily use the devices, thus reducing user error rates.

- Resistant to spoofing. The principal spoofing technique is a cast or latex model of a hand which is difficult to execute, particularly if simple physical security measures are in place. Other spoofing techniques such as gloves or other devices are unreliable and more likely to be rejected.

- Small template size. Compared to other biometrics such as fingerprints,

- hand scan and iris scans, hand geometry is extremely small and can be accommodated on a variety of devices including magnetic stripe cards. The small template size allows fast processing, important where large volumes of users are processed.

- The readers are durable and able to process large volumes of users of several years without undue reader failure. They can also withstand wide temperature ranges and operate in hostile (such as high temperature and dusty) environments.

- The technology has been in use for many years and has proved reliable[6].

The are some disadvantages which include:

- Cost. Hand geometry scanners are relatively large and expensive and palm and hand scanners are equally or more costly. The size of the devices precludes use in portable applications or small devices such a computer mouse.

- Hand changes and injuries. While the basic structure of the hand changes little over time, injuries, swelling or diseases such as arthritis can obscure this structure and cause recognition difficulties. It is interesting to note that students need re-enrolment once or twice in their scholastic lives to accommodate growth.

- Accuracy. Hand geometry is not sufficiently distinctive to allow 1-to-many searches and is generally limited to 1-to-1 authentication uses. It's use is therefore limited to identity verification rather than identification of an individual from a database. This is, however, considered an advantage by privacy advocates.

- Hygiene concerns, from multiple users touching the

reader[6].

5. Literature Survey

Many papers are published related to signature recognition and below some of these works:

- I Ketut Gede Darma Putra, Made Ari Sentosa (2012), Hand shape feature is obtained by using a chain code method. Since the vector length of the hand shape chain code of each user is distinct tendency then Dynamic Time Warping (DTW) is suitable metrics to match of two chain code features[7].

- Weiqi Yuan, Lantao Jing (2011), proposed hand geometry recognition system based on the features were extracted by artificial measurement and matching experiments through the Euclidean distance[8].

- Alexandra L.N. Wong¹ and Pengcheng Shi², We propose a feature-based hierarchical framework for hand geometry recognition, based upon matching of geometrical and shape features. Rid of the needs for pegs, the acquisition of the hand images is simplified and more user-friendly[10].

- Cenker Oden¹, Aytul Ercil², Burak Buke¹, we propose implicit polynomials, which have proven to be very successful in object modeling and recognition, have been proposed for recognizing hand shapes and the results are compared with existing methods[11].

6. Hand Geometry System

Biometric hand recognition systems measure and analyze the overall structure, shape and proportions of the hand, e.g. length, width and thickness of hand, fingers and joints; characteristics of the skin surface such as creases and ridges. Some hand geometry biometrics systems measure up to 90 parameters. As hand biometrics rely on hand and finger geometry, the system will also work with dirty hands. The only limitation is for people with severe arthritis who cannot spread their hands on the reader. The user places the palm of his or her hand on the reader's surface and aligns his or her hand with the guidance pegs which indicate the proper location of the fingers. The device checks its database for verification of the user. The process normally only takes a few seconds. To enroll, the users place his or her hand palm down on the reader's surface. A hand geometry system is shown in figure (1)[5].



Figure (1). Hand Geometry System

The benefits of hand biometric systems are given below-

- Small amount of data required to uniquely identify a user, so a large number of templates can be easily stored in a standalone device: Hand biometric systems will generally only require a template size of 10 bytes, which is much smaller than most other biometric technologies e.g. fingerprint systems require 250 to 1,000 bytes and voice biometric systems require 1,500 to 3,000 bytes.

- Low FTE rates.
- Easy to use.
- Non intrusive[5].

7. Module of Hand Geometry Biometric System

The module of hand geometry biometric system is shown in figure (2).

A biometric system consists of five important module image acquisition, image preprocessing, feature extraction, matching, and decision. Firstly image of hand is captured through a digital camera/scanner then it is fed to the next module i.e. image preprocessing module. The role of the preprocessing module is to clean up the noise because the input image having some noise due to dust on the palm, atmospheric conditions. The processing module is used to prepare the image for feature extraction. The feature extraction module is very important module in a hand geometric system. The function of this module is to extract

and store features like finger length, finger width, palm width etc. The next module of this system is matching. Here the features extracted in the previous section are matched up with the feature of that individual previously stored in the database. Therefore, matching is a straight one to one comparison between scanned and stored data. The last module of the hand geometrics biometric system is decision module. The is module give a "yes" or "no" response to the question "am I who I claim to be?" to a high degree of accuracy[5].

7.1. Image Acquisition

Hand geometry can be captured by widely used based scanners, video cameras, Digital cameras and Digital Scanner, and traditional method. For our project, we used a high-resolution economic scanner (Canon MP 250) with (300 dpi resolution). The hand image captured was for the right hand and left hand and 3 images for each hands using scanner.

7.2. Image Preprocessing

Preprocessing is used to correct distortions, hand geometry. Research on preprocessing commonly focuses on the many steps shown in figure (3) : resizing the captured image to 128 The next step is convert gray scale image and find edge and applying the (sobel Filter) on the resized image to remove any noise caused by dust on the scanner surface. Finally, find the edge detection.



Figure (2). Module of Hand Geometry Biometric System

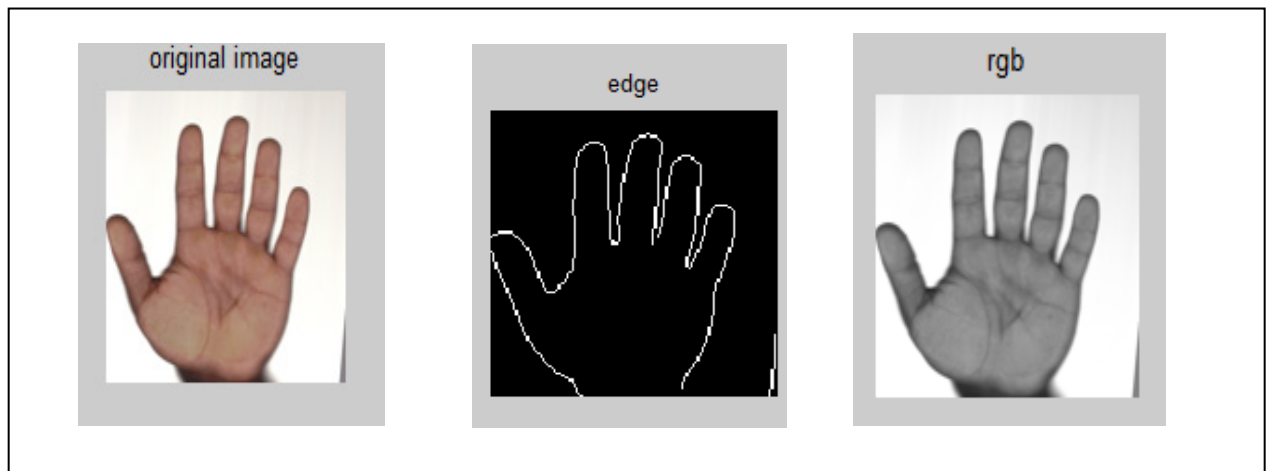


Figure (3). preprocessing steps

7.3. Feature Extraction

Feature extraction is an important part of hand geometry recognition system. Many features can be extracted from the hand geometry region. The hand geometry based an authentication system relies on geometric invariants of a human hand. Typical features include length and width of the fingers, aspect ratio of the palm or fingers ,thickness of the hand, etc. the first feature can be extraction is the length of finger .the second major feature is the width of the finger one or more measurement can be taken for the width at varying points along the finger. In the feature extraction using discrete cosine transform(dct2).

$$B_{pq} = \alpha p \alpha q \sum_{m=0}^{m-1} \sum_{n=0}^{n-1} A_{mn} \cos \frac{\pi(2m+1)p}{2m} \cos \frac{\pi(2n+1)q}{2n},$$

$$0 \leq p \leq m-1, 0 \leq q \leq n-1$$

7.4. Matching

The feature matching determines the degree of similarity between stored feature vector and claimed feature vector. The feature vector obtained from the input image is matched against the feature vector of images in the data base. Even under the best of conditions it cannot be expected that the features obtained match exactly with the features of the previous image of the same individual. The extracted features are in the form of positive integers. These are referred to as magnitude of the features. A correlation function is used to decide the match value.

8. Experimental Results

In the result the database currently contains hand images of 20 persons. For each person, we take six images three for the right hand and the other three for the left hand. The process of comparing is done by correlation and given the results as shown in Table (2).

Table (2). Result of hand matching

person	Corr left	Corr left	Corr right	Corr right
Person1	1	0.87	0.70	0.46
Person2	1	0.57	0.74	0.53
Person3	1	0.41	0.56	0.69
Person4	1	0.43	0.15	0.25
Person5	1	0.29	0.55	0.36

9. Conclusions

In this paper biometrics refers to an automatic recognition

of a individual based on her behavioral and/or physiological features. Many business applications will in future rely on biometrics since using biometrics is the only way to guarantee the presence of the owner when a transaction is made. Hand recognition systems have been proven to be very effective in protecting information and resources in a large area of applications. Biometric hand recognition system is implemented via discrete cosine transform. This approach leads to high performance compared with many separated systems.

REFERENCES

- [1] Muzhir Sh. Al-Ani, and Isra H. Al-Ani, "Gait Recognition Based Improved Histogram", CIS journal, Vol. 2, NO.12, December 2011.
- [2] Paul J. Sticha J. Patrick Ford, "Introduction To Biometric Identification Technology: Capabilities And Applications The Food Stamp Program", December 1999.
- [3] Chris Roberts, " Biometrics", November 2005.
- [4] Ann Cavoukian, Ph.D. Commissioner, "Biometrics and Policing: Comments from a Privacy Perspective", August 1999, Website: www.ipc.on.ca.
- [5] Vivek Yadav," Design of A Hand Geometry Based Verification System", Thesis, Thapar University, July- 2010.
- [6] Chris Roberts, "Biometric Technologies - Palm and Hand", May 2006.
- [7] Ketut Gede Darma Putra and Made Ari Sentosa "Hand Geometry Verification based on Chain Code and Dynamic Time Warping", Udayana University, Bali, Indonesia, Volume 38– No.12, January 2012.
- [8] Weiqi Yuan, Lantao Jing, "Hand-Shape Feature Selection and Recognition Performance Analysis", Shenyang University of Technology, 978-1-4577-0490-1/11/\$26.00 ©2011 IEEE.
- [9] "Guidelines regarding the introduction of biometric measures", 29th February 2008, <http://www.ip-rs.si/index.php?id=491>
- [10] Alexandra L.N. Wong1 and Pengcheng Shi2," Peg-Free Hand Geometry Recognition Using Hierarchical Geometry and Shape Matching", Hong Kong University of Science and Technology .
- [11] Cenker Oden1, Aytul Ercil2, Burak Bukel1," Combining Implicit Polynomials and Geometric Features for Hand Recognition",1Bogazici, 2Sabanci University, Istanbul Turkey.