

Image Matching using a Criminal Database

Kevan M. Bussey * and Patrick O. Bobbie**

* Florida Department of Law Enforcement
Tallahassee, Florida

**School of Computing and Software Engineering
Southern Polytechnic State University
1100 S. Marietta Parkway, Marietta, GA 30060

Abstract

The proposed research is on a user-interface and an image comparison subsystems that allows an criminal investigator to submit a facial image (photograph of a subject) and compare it to a set of facial images of criminals in a target database. A user interface is needed for the manipulation, or preprocessing, of the submitted image. Our comparison technique is based on similar to fingerprint minutiae-based and iris eye identification techniques. The ridges and furrows on the surface of a finger identify fingerprints. The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows as well as the minutiae points. Minutiae points are local ridge characteristics that occur at a ridge ending. Minutiae points for a facial image conceptually consist of multiple simple polygons (vectors). Iris identification also depends on vectors. The iris is located by plotting its x-y points using the polar coordinate system. The polar coordinate system is best suited for creating the vectors because of the circular shape of the iris. The vectors are translated into iris vector codes before they are submitted to a comparison system. Our image-matching system uses similar approaches used in iris identification and fingerprint matching. Further, a subset of the target image database is established using attribute filters such as sex, race, and data of birth. A subset is needed so that the subject image is not compared to every image in the database, thereby decreasing the search time and simplifying the computational complexity. The target facial images reside in an image database located at the Florida Department of Law Enforcement (FDLE). There are currently over 1800 images stored at FDLE. The proposed research is collaboration with the Investigative Division at FDLE.

Introduction and Problem Statement

This research strives to address a fundamental problem: A law enforcement officer takes a photograph of an alleged criminal (subject) at a crime scene. The photograph is transmitted electronically and digitized at the 'main' office for positive identification using a database of images of known (hot) criminals. What tools are required to provide near real-time feedback to the field officer or investigator?

The results of the collaboration project enhance current procedure for comparing a facial (subject) image to a large database of facial images at the Florida Department of Law Enforcement (FDLE). FDLE is a statewide law enforcement agency that provides a wide range of investigative and technical services to local criminal justice agencies. FDLE continues to strive in providing safety for the citizens and visitors for the state of Florida while battling the ever-changing criminal element. FDLE is the frontrunner in combating Florida's serious crime problems through effective and innovative programs and activities. To attain that goal the department provides criminal justice support services to every local sheriff and police agency in the state. FDLE is committed to

provide timely and accurate criminal justice information to prevent crime, solve cases and recover properly, and to identify persons with criminal warrants, arrests, and convictions. The department also provides statistical and analytical information about crime to policymakers and the public so that informed decisions can be made on the best way to combat and prevent crime [FDLE96].

FDLE maintains the central repository of criminal history records, as well as “ hot files” that provides data about wanted and missing persons; stolen guns, vehicles and other property; domestic violence injunctions, parole statuses; deported aliens; registered sexual predators; and images associated with most data – guns, vehicles, facial. These databases are accessible to all criminal justice agencies statewide using the Florida Crime Information Center (FCIC) network, which also links Florida agencies to other states via the National Crime Information Center (NCIC) network.

FDLE provides criminal identification screening services for criminal warrants, arrests, and convictions. This focus group may be applicants for jobs or licenses for certain professions, potential gun purchasers, or the subject of Public Records requests. The goal is to prevent persons with criminal histories from sensitive employment and licensing in certain professions, thus protecting vulnerable populations from them [FDLE96].

The wide range of FDLE activities require an enormous amount of internal support resources. Staying on top of current trends in technology and providing day-to-day operational support is vital to the organization’s success. Consequently, the law enforcement community benefits from the investigative, technical and forensic support, as well as the continuing education programs offered by FDLE.

Educational programs at FDLE continue to solicit institutes of higher learning for new cutting edge crime solving techniques. New research in image matching would lead to a reduction in crime solving time with an added crime-solving tool.

Implementation of the image database occurred in February 1999. The images stored are of criminals **wanted** locally and nationally. A law Enforcement Officer retrieves the images once key identifiers are entered. The identifiers are submitted to the FCIC system using a combination of the following attributes:

- ❖ Name
- ❖ Race
- ❖ Sex
- ❖ Data of Birth
- ❖ PCN Number
- ❖ NCIC Number
- ❖ FBI Number
- ❖ Case Number

An image is returned after submitting known attributes. The new challenge put before the investigator is the possession of the image with unknown attributes. Our image matching system provides a bridge to this challenge. A front-end interface component of the project allows the investigator to place vectors (rectangular markers) around the eyes, nose, and mouth. These vectors, and their associated pixels, are used by the image matching system. The system uses the vectors for comparison against a subset of vectored images in the criminal database. To assist the investigator, the image matching system returns to top five images that may potentially match the submitted image.

Background and Related Research

Minutiae of Fingerprint

The image matching process is based on the concept of fingerprint minutiae encoding and eye iris identification. Large volumes of fingerprints are collected and stored daily at FDLE. Identifying a potential criminal using their fingerprint requires that the input fingerprint be matched with a large number of fingerprints in a database. FDLE database contains approximately 5 million fingerprints! Fingerprints have ridge details and associated points that are never duplicated in different persons or even different fingers resulting in an existence of a infinite number of unique fingerprints [PI95].

To reduce the search time and computational complexity, the input fingerprint is matched against a subset of the fingerprints in the database.

Fingerprints are classified into five classes, namely *whorl*, *right loop*, *left loop*, *arch*, and *tented arch* [NIST99], as shown in Figure 1.

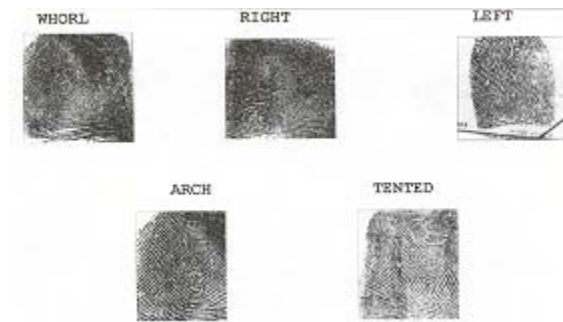


Figure 1. Five Classes of Fingerprints

Once the fingerprint classification has been established the next step is to check minutiae. Minutiae are points of identification on a fingerprint. There are two types of minutiae: ending ridges and bifurcations, as depicted in Figure 2. An ending ridge is a minutiae point where a ridge originates or terminates. Bifurcation is a minutiae point where a single ridge divides and forms parallel ridges [PI95].

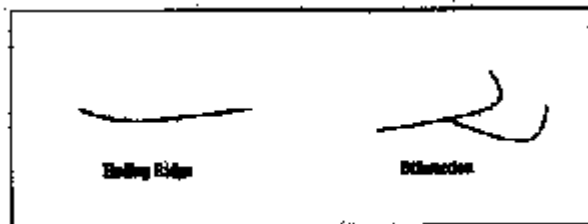


Figure 2. Two types of minutiae

There must be a minimum number of minutiae points located for acceptance. Figure 3 is a magnified fingerprint, showing the details of the minutiae points.



Figure 3. Details of Minutiae Points

The number of minutiae per finger varies. The plotted ranges must show a minimum of 40 minutiae, with a maximum of 180. (See Figure 3.) Before a search is initiated, a descriptor filtering is specified. Attributes used for filtering are sex, race, and year of birth (YOB). YOB is within allowable range of +/- 10 years. Meaning the search will filter in records where the YOB is any data greater (+) than the submitted data up to ten years. Also records are filtered in where the YOB is less (-) than the submitted data but not lower than ten years. A ten-finger match is not mandatory therefore a “fingers to match” filter is applied [PI95]. The search is initiated after the descriptor filtering and fingers to match have been specified. The search algorithm uses the input minutiae points and compares it to the subset of filtered minutiae points retrieved from the minutiae database.

Eye Iris Identification

Just like the uniqueness of a fingerprint pattern for a person, the eye iris pattern uniquely characterizes individuals. It has been proven that the iris is much more informative than the fingerprint, therefore person identification by the iris is much more simple and reliable. Ophthalmologists have suggested the possibility that the iris of the eye might be used as an alternative optical fingerprint for personal identification [Adl1965], [BCG1990], [Bri1988]. The ophthalmologists noted from clinical experience that every iris had a highly detailed and unique texture, which remained unchanged in clinical photographs spanning decades. The visible features of an iris such as the cornea, the meshwork of connective tissue, coloration, and freckles constitute a distinctive “fingerprint” that can be pattern-matched against a database of iris code vectors (i.e. minutiae) [Dau1997]. Figure 4 depicts an iris of the eye with concentric patterns, similar to those of fingerprints.



Figure 4. An Iris of the Eye

Criminal identification using the eye iris pattern is not a Law Enforcement utility. The iris pattern is compared to a known iris existing in the database. Possible applications of iris recognition are:

- Computer login: the iris as a living password.

- Telephone call charging without cash, cards, or PIN numbers.
- Premises access control (home, office, and laboratory).
- Driving licenses, and other personal certificates.
- Credit-card authentication.
- Automobile ignition and unlocking anti-theft devices.
- Secure financial transaction (electronic commerce, banking).
- Internet security; control of access to privileged information.
- Any existing use of keys, cards, PINS, or passwords [UC1999].

There are multiple iris algorithms in use worldwide. Though the degree-of-freedom (accuracy skew) varies, the underlying recognition premise is the same. The structure of the iris is broken down into vectors. This is performed in a polar coordinate system. Due to the circular shape of the iris, polar coordinates are best suited for creating the vectors. Using polar coordinates, which is based on an angle and a radius, is sometimes used as an alternative to simple X and Y coordinates on the complex plane [Cla2000].

The Image Matching Procedures/Methodologies

Facial comparison as a Law Enforcement tool is a needed venture that must be ensured. Research into minutiae and eye iris code creation sets the groundwork for image matching. Given an image database of wanted criminals, comparison checks could be run against an investigative photograph. The comparison system would use as input some specific parameters such as date of birth, race, sex, etc., and the vectors located within the investigative photograph (image). The comparison system would return the top five closely related matches from the image databases, with their associated criminal ID number.

There are currently over 1800 JPEG (Joint Photographic Expert Groups) images in the wanted database. The standard JPEG image is a rectangular array of pixels, with each pixel having the same number of color channels. Color channels are the (R) red, (G) green, (B) Blue color palettes. The investigative photograph would not be compared to the entire database. A front-end interface is needed to submit a standardized image format to the comparison system.

Vectoring and Facial Codes

The vectors (rectangular markings) created from the image are submitted to the comparison system. Attribute filters such as the sex, race, and date of birth are included in the submission. Once the vectors are submitted to the comparison system, facial codes from each of the vectors are generated. Facial codes generated using the coordinate points that mark/demarcate the features of the image: E.g., the left eye (rectangle with coordinates a, b, c, d), the right eye (rectangle with coordinates i, j, k, l), the nose (rectangle with coordinates m, n, o, p) and the mouth (rectangle with coordinates r, s, t, u).

The scaled and sheared image along with the coordinate points for each rectangle is then submitted to the comparison system. The image comparison algorithm uses the coordinates of the facial codes, and their enclosed pixels, looking for correspondences of the pixel points. This level of detail is necessary for precise/accurate matching due to the sensitive nature of the procedure. The investigative (subject) image is compared to the 'hot file' or target image in the database of facial codes. On completion, the comparison system selects the top five images that are

geometrically similar to the input (subject) image based on a 90% or greater accuracy/acceptance criterion. The investigator makes the final decision after reviewing the resultant images.

The interface would scale the image to a standardized size. Scaling the image to the standardized size will provide an origin for plotting the default locations.

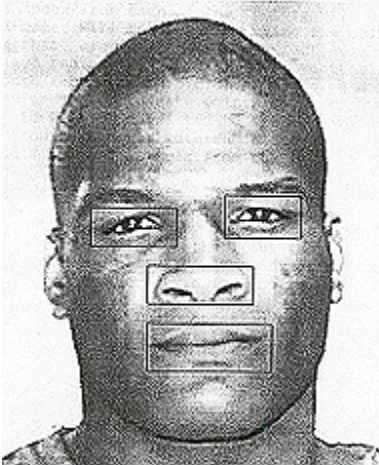


Figure 5. Vectorizing Image Features

The user interface subsystem to the matching system provides the user an opportunity to drag, expand, or decrease the default vector locations. Figure 6 shows a variant of Figure 5, where a user has the option of dragging the default vectors to suit or focus on significant feature of the image.

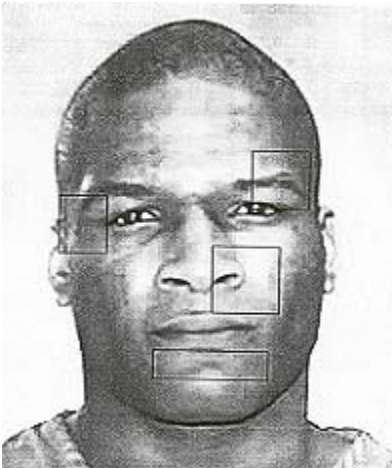


Figure 6. Changing/Dragging Default Vectors

The User-Interface Implementation Using Java 2D Graphics

The front-end interface of the proposed system is built using Java 2D Graphics API. Java 2D API is a set of classes that can be used to create high quality graphics and/or manipulate images through geometric transformation, bi-directional text layout, and antialiasing [Knu1999]. As stated previously, the front-end interface must allow human manipulation of the investigative image.

An image in its purest form is a two-dimensional array of colors. Each element in the array is called a pixel. The pixels of the image do not necessarily correlate with the pixels that are used to draw the image. An image has a width and height measured in pixels along with a coordinate system that is independent of any drawing surface [Har2000].

Java 2D objects live in a plane defined by Cartesian coordinates. This plane is commonly called User Coordinate space, or just user Space. A unit within the User Space transforms to a pixel.

The pixels are aligned with the x and y axes as shown below [Knu1999].

The x-axis increases from left to right, and the y-axis increases from the top to bottom. The origin would be placed at the upper left corner of the drawing surface. The origin is a major determinant for scaling the image.

Scaling is making something bigger or smaller. An image could be scaled to 300% of its original width and height. Java 2D has a method called *scale* within its API that allows this transformation to take place. All images submitted to the comparison system will be scaled to a fixed standardized size.

Scaling all images to the same size produces a fixed origin for all images. Thus, a common approach to establishing an origin ensures an accurate comparison of the subject image with the target images. Locating the origin and its x and y coordinates provides a basis for establishing the coordinate set of the default vectors for the eyes, nose, and mouth. Once the default vectors are set the investigator has the opportunity to modify the default vectors before submission to the comparison subsystem. Java 2D method *mouseDragged* allows the positioning of the vector to be changed. Java 2D has numerous methods defined along with the previously mentioned methods from which the front-end interface can be built. The following algorithm (or procedure) describes the implementation for the front-end interface.

Create frame and assign title

Supper “Hot File Image Matching System”

Create display image panel and add it to the main frame

Create a panel to add the control buttons - Combo Boxes – and add panel to the main frame

- **Scale X value**
- **Scale Y value**
- **Shear X value**
- **Shear Y value**

Add command button to create default vectors

Add action to handle events fired by combo boxes

- **If (Scale X) {}**
- **If (Scale Y) {}**
- **If (Shear X) {}**
- **If (Shear Y) {}**

Update panel to display scaled image

Add action to handle event fired by command button ‘Create Default Vectors’.

Create new frame and assign title

Supper “Place Vectors”

Create display image panel and add it to the main frame

Create panel to add command Button “Submit”

Load image from previous frame using scaling and shearing values

Place four rectangles on image based upon scaling and shearing values

- 1) *LeftEyeRect* = *new Rectangle2d.Double(a, b, c, d)*
- 2) *RightEyeRect* = *new Rectangle2d.Double(a, b, c, d)*
- 3) *NoseRect* = *new Rectangle2d.Double(a, b, c, d)*
- 4) *MouthRect* = *new Rectangle2d.Double(a, b, c, d)*

Add action to handle event fired by command button 'Submit'

Create new frame and assign title

Super "Resulting Comparison Image"

Create five display image panels and add them to the main frame (panels will display images from comparison system)

Create a display image panel (panel will show original image that was scaled and sheared)

Conclusion

The research project described in this paper is collaboration with the Florida Department of Law Enforcement. The resultant tool provides Law Enforcement a tool to identify a criminal from an offender's photograph. The underlying methods and techniques of the image matching system follow known techniques for identifying fingerprint and matching eye iris. The basic approach to the matching process is based on the concept of locating vectors within an investigative image. A front-end interface for generating image vectors is built using the JAVA 2D Graphics API.

References

- [FDLE96] Florida Department of Law Enforcement [Florida Crime Information Center II – Master Plan], 1996
- [NIST] U.S. Commerce Department's Technology Administration, Database Administration
http://www.nist.gov/srd/fing_img.htm
- [Adl1965] F.H. Adler, *Physiology of the Eye: Clinical Application* (fourth edition). London: the C.V. Mosby Company, 1965
- [BCG1990] A.C. Bovik, M. Clark, and W.S. Geisler, "Multichannel texture analysis using localized spatial filters" *I.E.E.E. Transactions on Pattern Analysis and Machine Intelligence*, Vol. 12, pp. 55-73, 1990.
- [Bri1998] R. Bright, *Smartcards: Principles, Practice, Applications*. New York: Ellis Horwood, Ltd., 1988.
- [Dau1997] John G. Daugman, *High Confidence Visual Recognition of Persons By a Test of Statistical Independence*, 1997
<http://www.labs.bt.com/library/papers/PAMIpaper/node6.html>
- [UC1999] University of Cambridge, The Computer Laboratory, 1999
<http://www.cl.cam.ac.uk/users/jgd1000/applis.html>
- [Cal2000] Johan Claeys Tutorial: Topics: Solved and unsolved problems, 2000
<http://www.ping.be/math/polar.htm>
- [Cla1999] Jonathan Knudsen, *JAVA 2D Graphics*, O'Reilly, 2000
- [Har2000] Vincent J. Hardy, *JAVA 2D API Graphics*, Sun Microsystems, 2000