Iris Recognition-based Security System with Canny Filter

Dr. Hassan Jaleel Hassan

Computer Engineering Department, University of Technology, Baghdad-Iraq
E-mail: hjhh2007@yahoo.com

Received: 8/9/2014

Accepted: 21/1/2015

Abstract – Image identification plays a great role in industrial, remote sensing, and military applications. It is concerned with the generation of a signature to the image. The human iris recently has attracted of biometric-based identification and verification research and development community. This iris is so unique that no two irises are alike, even among identical twins in the entire human population.
In this work we propose a security system based on Iris biometric feature extraction. The focus was on the eye image, which is devoid of the eyelid and eyelashes that is done by using a camera which has the ability to show the iris with white background (eye sclera) only, using a proper position of eye on camera. The system automatically acquires the biometric data in numerical format (Iris images) by using a properly located sensor. We are considering camera as a high quality sensor. Iris images are typically color images that are analyzed to three bands monochrome images (Red, Green, and Blue). Each band of monochrome image represents a grey scale image. Then the feature extraction algorithm is used to detect Iris Effected Region (IER) for each monochrome image, and then extract features from IER that are numerical characterization of the underlying biometrics. Later we identify the authorized person by comparing the features obtained from the feature extraction algorithm with the previously stored features by producing a similarity score. This score indicates the degree of similarity between a pair of biometrics data under consideration. Depending on degree of similarity, authorized person can be identified.
A successful identification rate of 100% was achieved for ten person iris images.

Keywords – Security System, Iris Pattern recognition, Feature extraction, Biometric identification.

1. Introduction

Today's buildings increasingly ask for comprehensive security solutions. The buildings demand system which offers the flexibility of controlling access throughout a secure room or any point of entry [1].

Most security system exists, from a simple password and automatic teller machine (ATM) card, this system suffers from a major drawbacks: only the validity of the combination of a certain possession (ATM card) and certain knowledge (the password) is verified. The ATM card can be lost or stolen, and password can be compromised. Thus some access methods have emerged, where the password has either been replaced by, or used in addition to biometrics such as the person's speech, face image or fingerprints [2].

In general, a biometric identification system makes use of either physiological characteristics (such as fingerprint, iris pattern, or face) or behavior patterns (such as handwriting, voice, or key-stroke pattern) to identify a person [3].

In the iris alone, there are over 400 distinguishing characteristics, or Degree of Freedom (DOF), that can be quantify an individual (Daugman, J. Williams, G. O. 1992). Approximately 260 of those are possible to capture for identification. These identifiable characteristics include: contraction furrows, pits, collagenous fibers, filaments, crypts (darkened area on the iris), serpentine vasculature, rings and freckles. Due to these unique characteristics, the iris has six times more distinct identifiable features than a finger print [4].

Plenty of works are done on Iris Recognition System. Most of the cases, authors claimed the better performance of speed in capturing images and recognition over the existing systems available at that time. To gather the knowledge, we have considered the following selective works. Hyung et. al. [5] introduced the invariant binary feature which is defined as iris key. Iris key is generated by the reference pattern, which is designed as lattice structured image to represent a bit pattern of an individual. Reference pattern and iris image are linked into filter. In the filter, iris texture is reflected according to the magnitude of iris power spectrum in frequency domain.

Pan et. al. [6] proposed a new iris localization algorithm, in which they adopted edge points detecting and curve fitting. After this, they set an integral iris image quality evaluation system that is necessary in the automatic iris recognition system.

Leila et. al. [7] proposed iris recognition algorithm based on covariance of discrete wavelet using competitive neural network. A set of edge of iris profiles are used to build a covariance matrix by discrete wavelet transform using neural network. They found that this method can discriminate noisy image very well.

Finally, Lenina et. al.[8] present the concept of application of ridgelets for iris recognition systems. Ridgelet transforms are the combination of Radon transforms and wavelet transforms. The technique proposed the Ridgelets to form an iris signature and to represent the iris.

In this paper, we proposed a security system based on iris recognition according to the following steps: The **first** step is to analyze color iris image in to three monochrome images (Red, Green, and Blue). The **second** step is to pass the resultant monochrome image through canny filter edge detector. The **third** step is represented by calculating three binary image features (Euler number, Area, and projections), so we shall get nine features for each iris image. Finally,in the **fourth** step, Euclidian distance is used to find the similarity score which indicates the degree of similarity and identifies the authorized person accordingly.

The remainder of this paper is organized into four sections: section 2 presents iris feature extraction. Section 3 outlines the proposed iris texture classification algorithm. Section 4 illustrates the practical results. Section 5 gives some conclusions.

2. Iris Feature Extraction

To extract object features, we need image segmentation and any necessary morphological filtering. This will provide us with clearly defined objects, which can then be labeled and processed independently. After all the objects in the image are labeled, we can treat each object as a binary image by assuming that the labeled object has a value of "1" and that everything else is "0". After we have labeled the objects, we have an image filled with object numbers. This image is used to extract the features of interest. The binary object features we will define include **area, Euler number,** and **projections.**

In order to provide general equation of area, a function$I_i(r,c)$ is defined as [9]:

$$I_i(r,c)=\begin{cases}1 & if\ I(r,c) = ith\ object\ number \\ 0 & otherwise\end{cases} \quad (1)$$

Where, r and care the image matrix coordinates.

Now the *area* can be defined as:

$$A_i = \sum_{r=0}^{N-1}\sum_{c=0}^{N-1} I_i(r,c) \quad (2)$$

The *Euler number* of an image can be defined as the number of convexities minus the number of concavities, which are found by scanning the image for the patterns that follow.

Convexities Concavities

$$\begin{bmatrix}0 & 0\\0 & 1\end{bmatrix}\begin{bmatrix}0 & 1\\1 & 1\end{bmatrix}$$

The *Projections* of a binary object, which also provide shape information, are found by summing all the pixels along rows or columns. If we sum the rows we have the horizontal projection; if we sum the columns we have the vertical projection. We can define the horizontal projection $h_i(r)$ as

$$h_i(r) = \sum_{c=0}^{N-1} I_i(r,c) \quad (3)$$

And the vertical projection $v_i(c)$

$$v_i(c) = \sum_{r=0}^{N-1} I_i(r,c) \quad (4)$$

A feature vector is one method to represent an image (an object), by finding measurements on a set of features. The feature vector is an n-dimensional vector that contains these measurements.

Euclidean distance is the most common metric for measuring the distance between two vectors and is given by the square root of the sum of the squares of differences between vector components. Given two vectors **A** and **B**; where, $A = [a_1 a_2 \ldots\ldots a_n] and\ B = [b_1 b_2 \ldots\ldots b_n]$then the Euclidean distance is given by:

$$\sqrt{\sum_{i=1}^{n}(a_i - b_{i)}^2} = \sqrt{(a_1 - b_1)^2 + (a_2 - b_2)^2 + \cdots (a_n - b_n)^2} \qquad (5)$$

Edge detection is the approach used most frequently for segmenting images based on local changes in intensity. The edge detection methods are based simply on filtering an image with one or more masks, with no provisions being made for edge characteristics and noise content. Canny edge detector (which is used in this work before the calculation of Iris features) is an advanced technique that makes an attempt to improve on simple edge detection methods by taking into account factors such as image noise and the nature of edges themselves. Canny's approach is based on three basic objectives: Low error rate, Edge points should be well localized and single edge point response [10].

3. The Proposed Algorithm

The proposed security system algorithm consists of two phases: Building the reference set phase, and testing phase.

a) Building the reference set.

This phase deals with the problem of how to create reference set. The procedures of generating image templates are given below;

1- Input a color iris image to the generating algorithm.
2- Resize the image into N×M pixels.
3- Analyze the color image into three monochrome images (Red, Green, and Blue).
4- Pass each monochrome image through Canny edge detector.
5- Calculate Area, Euler number, and Projection for each monochrome image.
6- Save the calculated values for three monochrome images in one vector which represents the main feature vector.
7- Repeat all above steps for all images related with proposed system.

Figure (1) shows the steps of building the feature vector for the iris color image taken by a digital camera.

a) *Testing Phase.*

In this phase*, Euclidean distance* metric is use to measure the distance between the entered image and all the feature vectors stored in the reference set. Depending on degree of similarity between each two vectors (entered image vector with one of reference set) authorized person can be identified.

Figure (2) shows the main block diagram of the access control system based on Iris Recognition.

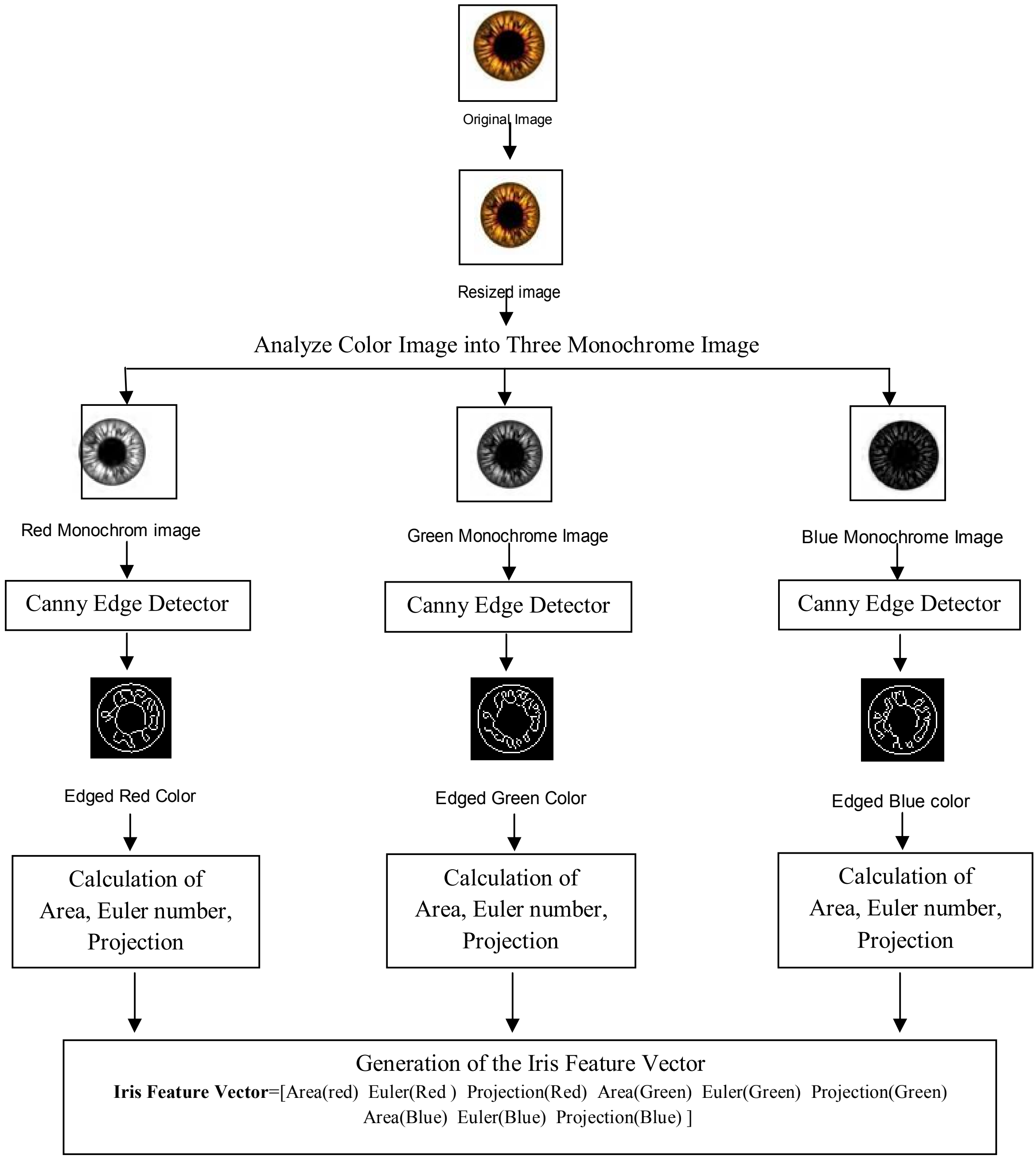

Figure 1 steps of building the feature vector for the color iris image taken by a digital camera

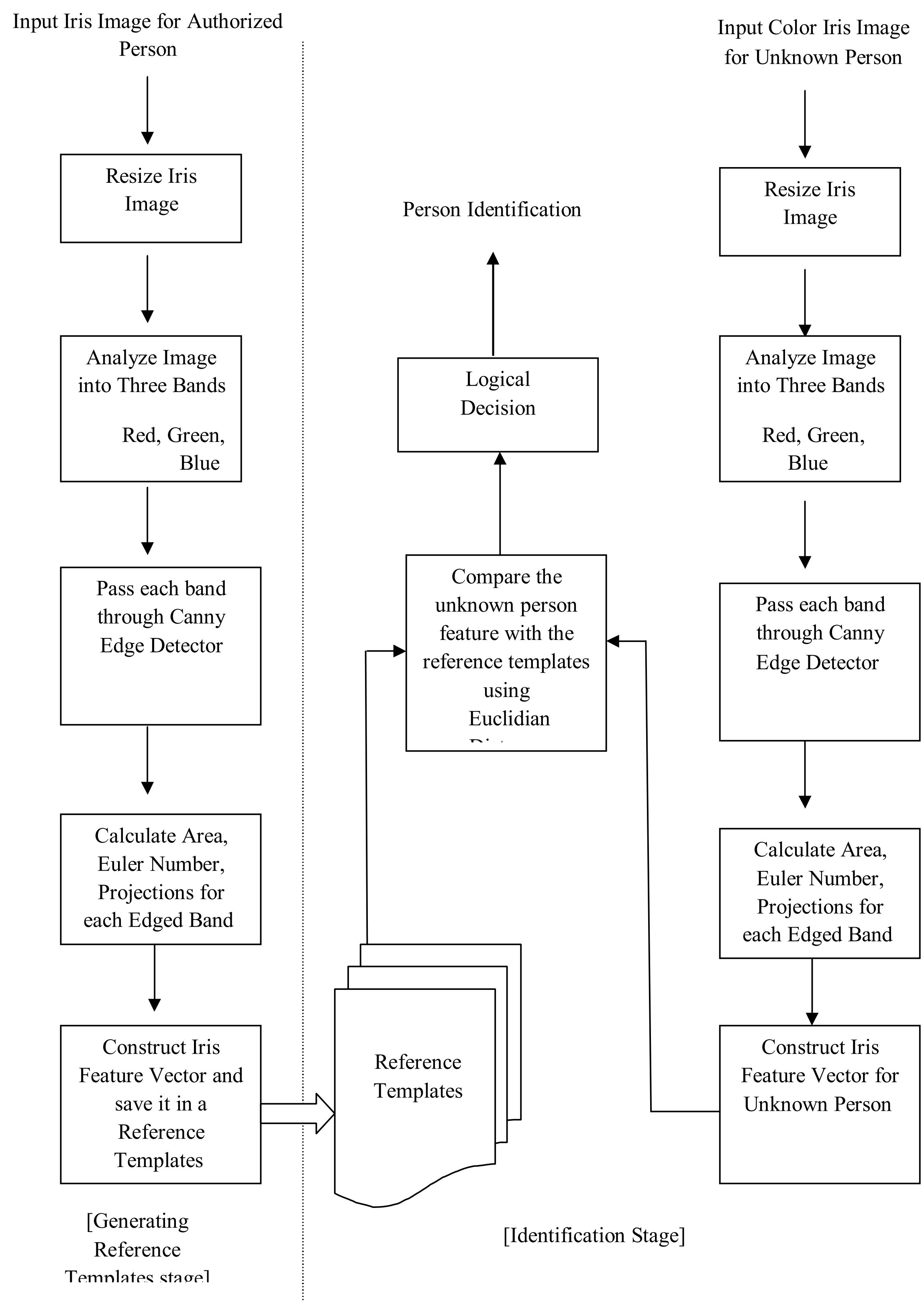

Fig. 2: the main block diagram of the access control system based on Iris Recognition

4. Results

In this work, Ten Iris Images for different persons are used in building the reference testing sets. These images have been extracted from the location (http://dimandportraiture.wordpress.com). Table (1) shows the results often feature vectors which contain the calculated values of *Area, Euler number*, and *Projections* for all color images represented by their monochrome bands.

The security system gives the authorization for ten persons only and prevents all others to access. Equation 5 has been used as a metric for measuring the distance between each two vectors, which reflected the accuracy rate of recognition, and it was (accuracy rate) 100% for ten images data base.

Table 1: The calculated feature values for ten iris

Iris Image number	Red band Area	Green band Area	Blue band Area	Red band Euler Number	Green band Euler Number	Blue band Euler Number	Red band Projections	Green band Projections	Blue band Projections
1	257.75	296	314	5	6	5	234	268	284
2	316	426	420	3	4	4	288	387	382
3	377.75	374.125	450.875	2	3	5	341	338	407
4	355.5	442.5	381.5	3	2	2	322	401	346
5	292.375	328.125	257	8	8	4	264	297	235
6	155.5	398.875	373.625	0	8	-2	142	360	337
7	336.375	3409.25	289.5	5	2	2	307	309	262
8	432.75	416.5	420.125	5	8	0	391	375	376
9	419.25	417.875	480	5	3	3	381	377	431
10	464.75	495.25	484.52	7	12	12	419	449	438

Let us take an example:

When, one person tries to enter a secure place (say; person 5), he will need to lean his eye to a detector (digital camera) and then, iris sample is analyzed according to the program prepared for that purpose. The program calculates the distance between the vector of the eye of the person who wants to enter and comparing it with the database stored in advance of the ten people who are allowed to enter. After this is done, the person can be authorized or not according to the calculated distance. Table 2 shows the distance between the iris vector of person number 5 with other persons.

The smallest distance = 0.0000

The test image is classified as class label 5.

Table 2: The distance between the test image (Person 5 iris images) with other ten persons

Reference Set Images	Distance to Test Image
Person 1 Iris	351.57
Person 2 Iris	156.63
Person 3 Iris	389.90
Person 4 Iris	160.189
Person 5 Iris	363.853
Person 6 Iris	381.06
Person 7 Iris	296.58
Person 8 Iris	83.26
Person 9 Iris	0.0000
Person 10 Iris	121.70

Another **example** can be taken. Person 9 tries to enter the secure place. The same procedures have to be done as in previous example. Table 3 shows the distance between the iris vector of person number 9 with other persons.

Table 3: The distance between the test image (Person 9 iris images) with other ten

Reference Set Images	Distance to Test Image
Person 1 Iris	98.158
Person 2 Iris	218.229
Person 3 Iris	289.561
Person 4 Iris	251.449
Person 5 Iris	0.0000
Person 6 Iris	257.841
Person 7 Iris	76.648
Person 8 Iris	342.988
Person 9 Iris	363.756
Person 10 Iris	444.320

From the previous examples, and by looking at table 2 & 3, one can see that minimum distance with canny filter is useful way of determining the similarity of a set of values from an "unknown" sample to a set of values measured from a collection of "known" samples. The accuracy of using this algorithm was 100% for ten persons.

5. Conclusions

The objective of this paper is to develop an access control system based on biometric iris features. Toward this goal, an algorithm depends on extraction binary object features has been proposed. The binary object features includes *Area, Euler Number, and Projections*. *Area* tells us something about when the object is, while two another features (*Euler Number, Projections*) tell us something about shape of the object. The following points are concluded from the test of iris features for ten persons.

1- The proposed algorithm reflected the effectiveness of using Canny filter to find the edge inside the iris, which showed that this iris is so unique that no two irises are alike.
Compared with the rest of the types of filters visually, the usefulness of using Canny filter seems clearly its potential of highlighting the accurate implicit information represented by different identifiable characteristics of iris such as, contraction furrows, collagenous fiber, pits, filaments, crypts, and freckles.

2- Because Irises exist in different colors, this feature gave us a wide range to extract implicit information, and that increased the robustness of the proposed access control system.

References

[1] Honeywell International Corporation, "Symmetr E^{TM}", 35 Dynamic Drive, Toronto, Ontario MIV 4z9, Canada, 2001. At: http//www.honywell.com.

[2] Ravi S. Sandhu., "Access Control: Principles and Practice", ISASSE Department, MS 4A4, George Mason University, Fairfax, VA22030. Voice: 703-993-1659, Fax: 703-993-1638, (1992).

[3] Yongsheng G., Maylor K. H. Leung, "Face Recognition using Line Edge Map", IEEE Transactions on pattern Analysis and Machine Intelligence, Vol. 24, No. 6, June 2002.

[4] Debnath Bhattacharyya, Samir Kumar Bandyopadhyay, and Tai-hoon Kim, "Iris Texture Analysis and Feature Extraction for Biometric Pattern Recognition", International Journal of Database Theory and Application, 2008.

[5] Hyung Gu Lee, Seungin Noh, Kwanghyuk Bae, Kang-Ryoung Park and Jaihie Kim, "Invariant Biometric Code Extraction", IEEE ISPACS, pp. 181-184, Nov. 2004.

[6] PAN Lili, XieMei, "The Algorithm of Iris Image Processing," Fourth IEEE Workshop on Automatic Identification Advanced Technologies (AutoID'05), pp. 134-138, Oct. 2005.

[7] Leila F.Araghi, Hamev S., "Iris Recognition Using Neural Network", Proceeding of the International Multiconference of Engineers and Computer Scientist, Vol. I, March 2010. Hong Kong.

[8] Lenina Birgale and Manesh Kokare, "Iris Recognition Using Ridgelets", Journal of Information Processing System, Vol. 3, No. 3, September 2012.

[9] Gonzalez, R. C., Woods, R. E., "Digital Image Processing", Adison-Wesely Publishing Company 1992.

[10] Gonzalez, R. C., Woods, R. E., "Digital Image Processing", Third Edition, Pearson Prentice Hall, 2009.