Biometric(s) Detection and Steganography

Sara Kh. Ayoub¹, Dr. Ahmed S. Nori²

¹²Computer Science Dept. College of Computer Science and Mathematics Iraq, Mosul, Mosul University

E-mail: ¹saraalsultan93@yahoo.com, ²asn2203@yahoo.com

ABSTRACT

The term "biometrics" is derived from the Greek words bio means “life” and metric means “to measure”. In this paper, a detailed experimental study of physiology biometrics (face, iris) detection, face detection algorithms based on “Skin Color” has been made. Three color spaces RGB, YCbCr and HSI are of main concern. We have compared the algorithms based on these color spaces and have combined them to get a new skin color based face detection algorithm which gives higher accuracy. Use morphology for iris detection, after detection extract feature use PCA algorithm and steganography using Logical exclusive-XOR.

Keywords: Biometric, Detection, Feature Extraction, Steganography.

1 INTRODUCTION

A biometric is defined as a unique, measurable, biological characteristic or trait for automatically recognizing or verifying the identity of a human being. Statistically analyzing these biological characteristics has become known as the science of biometrics [1].

Steganography is the art and science of hiding information by embedding messages within other, seemingly harmless messages.

Steganography means “covered writing” in Greek. The goal of steganography is to hide the presence of a message and to create a covert channel [2].

Steganographic technologies are a very important part of the future of Internet security and privacy on open systems such as the Internet [3].

Steganographic research is primarily driven by the lack of strength in the cryptographic systems on their own and the desire to have complete secrecy in an open-systems environment.

The word “biometrics” came from Greek and we can divide it into two roots: “bio” means life and “metrics” – to measure. Biometrics is the process of making sure that the person is who he claims to be [4].

2 RELATED WORK

2.1 Biometric(s) Detection

Vivek Desai and others have proposed and implemented the face detection system in three phases. In the first phase of this method, the skin region of the human is detected from the still image or video clip. The second phase deals with grouping and connected component analysis. The final phase deals with finding the face region and creating the boundary across the face region [5].

T. Barbu proposes a robust face detection approach that works for digital color images. Our automatic detection method is based on image skin regions, therefore a skin-based segmentation of RGB images is provided first. Then, we decide for each skin region if it represents a human face or not, using a set of candidate criteria, an edge detection process, a correlation based technique and a threshold-based method. A high face detection rate is obtained using the proposed method [6].

Naveen Singh and others describe the novel techniques developed to create an Iris Recognition System, in addition to an analysis of our results used a fusion mechanism that amalgamates both, a
Canny Edge Detection scheme and a Circular Hough Transform, to detect the iris’ boundaries in the eye’s digital image then applied the Haar wavelet in order to extract the deterministic patterns in a person’s iris in the form of a feature vector. By comparing the quantized vectors using the Hamming Distance operator, we determine finally whether two irises are similar. Our results show that our system is quite effective [7].

G. Sathish and others design system for Iris recognition the objective of this work is to present abiometric authentication system for high security physical access control based on iris pattern. The proposed iris recognition with improvement in segmentation and matching stages using Hamming distance provides match for iris pattern if hamming distance is below 0.15. The CASIA IRIS image database of Chinese Academy of Sciences Institute of automation is used and the system is implemented in MATLAB. The proposed approach found to report higher verification accuracy of 99.2% [8].

3 CHARACTERISTIC OF BIOMETRIC TECHNOLOGY

1) Universality: something that each person has.
2) Uniqueness: something that separates this very person from others. This means that not all characters can be suitable for biometrics.
3) Permanence: biometric measurement should be constant over time for each person.
4) Measurability (collectability): it should be easy to measure, should not demand too much time and cost.
5) Performance: speed, accuracy and robustness.
6) Acceptability: how well people accept biometrics.

Circumvention: how easy it is to fool the system [9].

4 CLASSIFICATION OF BIOMETRIC(S)

Biometric classified as shown in figure 1

1) Physiological: related to the shape of body.
2) Behavioral: related to the behavior of person.

![Biometric characteristics](image)

Fig. 1. Biometric characteristics[12]

5 FACE DETECTION

Our face detection system consists of three steps. The first step is to classify each pixel in the given image as a skin pixel or a non-skin pixel. The second step is to identify different skin regions in the skin detected image by using connectivity analysis. The last step is to decide whether each of the skin regions identified is a face or not.
5.1 Skin Color Segmentation

Color is a useful piece of information for skin detection. The skin detection is the most common and first approach for detecting meaningful skin color, skin color detection may avoid exhaustive search for faces in an entire image. In this step, we describe how non-skin color is rejected from an image so that the image contains only skin-like areas, which will be our skin color segmented image for further processing.

From different types of color models, in HSV color model, Hue (H) is not reliable for the discrimination task when the saturation is low. Also in YCbCr color model, the distribution of skin areas is consistent across different races in the Cb and Cr color spaces, the RGB color model is lighting sensitive. Therefore, when we use different color models under uncontrolled conditions, and we get consequently result for skin color detection. The accuracy of skin detection depends on both the color model and the method of skin pixels classification or detection. Hence, the challenge problem is how to select color models that are suitable for skin pixel classifications under different varying conditions. There are three color models used for skin color segmentation or detection of skin pixels. These are RGB, YCbCr, and HSV color models. The combination of these color models overcomes all varying lighting conditions and changes in illumination, and it gives better result than individual color model result [11].

5.1.1 Skin Color Based Face Detection in RGB Color Space

Detected skin color pixels in RGB color by Eq. (1) [13].

\[
\text{skin} = \begin{cases} 
R > 95 \text{ and } G > 40 \text{ and } B > 20 \text{ and } \\
\max(R, G, B) - \min(R, G, B) > 15 \text{ and } \\
|R - G| > 15 \text{ and } \\
R > G \text{ and } R > B 
\end{cases}
\]

(1)

5.1.2 Skin Color Based Face Detection in YCbCr Color Space

Detected skin color pixels in YCbCr Color space by Eq. (2) [13].

\[
\text{skin} = \begin{cases} 
177 > C_r \text{ or } C_r > 137 \\
127 > C_b > 77 \\
215 > C_a + 0.6C_r > 190 
\end{cases}
\]

(2)

5.1.3 Skin Color Based Face Detection in HSV Color Space

The skin color pixel should satisfy the following condition [14].

\[
0 \leq H \leq 0.25 \\
0.15 \leq S \leq 0.9
\]

(3)

5.2 The Proposed Algorithm

Steps for face detection see figures 3 and 7.

1) Convert the input RGB image (rgb(i,j)) into HSV image (hsv(i,j)) and YcbCr image(Ycbcr(i,j)) Extraction of skin tone pixels from all 3 image modes.

2) Calculate connected components for each segment.

3) Calculation of ratio of length: width for each segment.

4) Use Golden ratio to confirm the region is a face or not.

5) Calculate boundary for image.

6 THE HUMAN IRIS

The iris is a thin circular anatomical structure in the eye. The iris’s function is to control the diameter and size of the pupils and hence it controls the amount of light that progresses to the retina. A front view of the iris is shown in Figure 2. To control the amount of light entering the eye, the muscles associated with the iris (sphincter and dilator) either expand or contract the centre aperture of the iris known as the pupil.

The iris consists of two layers: the pigmented front fibro vascular called as stroma and beneath it are the pigmented epithelial cells. The stroma is connected to the sphincter muscle which is responsible for the contraction of the pupil and also to the set of dilator muscles, responsible for the enlargement of the pupil which it does by pulling the iris radially. The iris is divided into two basic regions: the pupillary zone, whose edges form the boundary of the pupil and the ciliary zone which constitutes the rest of the iris [15].

Fig. 2. A front view of the Human Iris [15]
7 IRIS DETECTION

Iris is detected using morphological operations. Dilation and erosion are two major operations which are used with 3 by 3 operators. Skin color detection helps to reduce noise which can appear in further processing. Image is segmented with the help of threshold to convert it into two-tone image, which generates iris, eyelids and eyebrows as a white portion [16].

7.1 Morphological Operation

Morphology is a broad set of operations that process images based on shapes. The operations of morphological are erosion and dilation used to smooth the object boundary without changing their respective area. The purpose of using erosion and dilation is to improve the efficiency of iris detection.

The dilation process is to add pixels in the boundary of an object where the erosion is used to remove the boundary pixel from an object. Adding or removing the pixel from an object is fully based on the size or shape of the Structuring element, which defines the neighborhood pixel. First the image is dilated and then eroded by using the same structuring element then this process is called closing operation.

The opening operation performs eroded the image and then dilate the eroded image [17].

7.2 The Proposed Algorithm

Steps of Iris detection see figures 8 and 15.

1) Read image.
2) Convert it to gray.
3) Convert to binary.
4) Inverse binary image.
5) Apply canny edge detection.
6) Apply morphology operation.
7) Delete small object.
8) Calculate boundary for image.

8 FEATUR EXTRACTION USING PCA ALGORITHM

Principal Component Analysis (PCA) method used for global feature extraction is a powerful technique for extracting global structures from high-dimensional data set and has been widely used to reduce dimensionality and extract abstract features of faces for face recognition. This provides an effective technique for dimensionality reduction [20].

8.1 PCA Algorithm Steps

A) Calculate the mean

\[ \mu = \frac{1}{M} \sum_{i=1}^{M} X_i \]  

(4)

B) Subtract the Mean:

\[ A_i = X_i - \mu \quad i = 1, 2, \ldots, M \]  

(5)

C) Calculating the covariance matrix:

\[ S = A \cdot A^T \]  

(6)


9 STEGANOGRAPHY

9.1 Steganography Using Logical Exclusive-XOR

Algorithm steps: see Figures 16 and 19.

Step1: Read the image (after detection).
Step2: Calculate boundary for image (minx:maxx, miny:maxy).
Step3: Call PCA function (MY_PCA)
Step4: Read text from file.
Step5: Convert the text to binary.
Step6: If message not end

- Put the value of PCAS in coverbyte array.
  - If coverbyte >0
    - Convert coverbyte to binary.
    - Xor between first bit of message and second bit of pca.then put result in first bit of pca.

Step7: Call My_PCAR function to retrieved image.
Step8: Print retrieved_image.

9.2 The extracting process of the proposed system

Step1: Read the image (after detection).
Step2: Calculate boundary for image (minx:maxx, miny:maxy).
Step3: Call PCA function (MY_PCA)  
Step4: Read text from file.  
Step5: Convert the text to binary.  
Step6: If message not end.  
  - Put the value of PCAS in coverbyte array.  
    - Xor between first and second bit of pca. then put result in msg array.  
Step7: Write file text result.

10 RESULT

10.1 Biometric(s) Detection

(a) Face Detection

(b) Iris Detection

Fig. 3. Original Image

Fig. 4. Convert RGB 2 YCbCr and HSV

Fig. 5. Skin Detection

Fig. 6. Face Or Not Face

Fig. 7. Boundary

Fig. 8. Original Image
10.2 Steganography

- Face

Fig. 16. Image (a) before (b) after steganography. Message size=1889

Fig. 17. Image (a) before (b) after steganography. Message size=505

- Iris

Fig. 18. Image (a) before (b) after steganography. Message size=1889
11 MEASURING PERCEPTUAL QUALITY OF STEGANOGRAPHY IMAGE [18, 19]

11.1 Peak signal to noise ratio (PSNR)

It is the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. PSNR is usually expressed in terms of the logarithmic decibel. PSNR is given by:

$$PSNR = 10 \log_{10} \left( \frac{255^2}{MSE} \right) \quad \text{(4)}$$

11.2 Mean Square Error (MSE)

It measures the average of the square of the "error." The error is the amount by which the pixel value of original image differs to the pixel value of modified image

$$MSE = \frac{1}{MN} \sum_{x=1}^{M} \sum_{y=1}^{N} (S_{xy} - C_{xy})^2 \quad \text{(5)}$$

Where, $M$ and $N$ are the height and width of image respectively. $f(i, j)$ is the ($i, j$)th pixel value of the original image and $f'(i, j)$ is the ($i, j$)th pixel value of modified image.

See Tables (1, 4)

Table 1: Measure message for face size=1889

<table>
<thead>
<tr>
<th>IMAGES</th>
<th>IMAGE SIZE</th>
<th>MSE</th>
<th>PSNR</th>
</tr>
</thead>
<tbody>
<tr>
<td>face1</td>
<td>400*320</td>
<td>0.2243</td>
<td>54.6219</td>
</tr>
<tr>
<td>face2</td>
<td>300*400</td>
<td>0.2154</td>
<td>54.7992</td>
</tr>
<tr>
<td>face3</td>
<td>225*225</td>
<td>0.1993</td>
<td>55.1348</td>
</tr>
</tbody>
</table>

Table 2: Measure message for face size=505

<table>
<thead>
<tr>
<th>IMAGES</th>
<th>IMAGE SIZE</th>
<th>MSE</th>
<th>PSNR</th>
</tr>
</thead>
<tbody>
<tr>
<td>face1</td>
<td>400*320</td>
<td>0.2167</td>
<td>54.7716</td>
</tr>
<tr>
<td>face2</td>
<td>300*400</td>
<td>0.2071</td>
<td>54.9689</td>
</tr>
<tr>
<td>face3</td>
<td>225*225</td>
<td>0.1960</td>
<td>55.2092</td>
</tr>
<tr>
<td>face4</td>
<td>240*210</td>
<td>0.2094</td>
<td>54.9212</td>
</tr>
<tr>
<td>face5</td>
<td>156*125</td>
<td>0.2097</td>
<td>54.9148</td>
</tr>
<tr>
<td>face6</td>
<td>257*196</td>
<td>0.2126</td>
<td>54.8543</td>
</tr>
<tr>
<td>face7</td>
<td>261*193</td>
<td>0.2066</td>
<td>54.9798</td>
</tr>
</tbody>
</table>

Table 3: Measure message for Iris size=1889

<table>
<thead>
<tr>
<th>IMAGES</th>
<th>IMAGE SIZE</th>
<th>MSE</th>
<th>PSNR</th>
</tr>
</thead>
<tbody>
<tr>
<td>iris1</td>
<td>295*194</td>
<td>0.1917</td>
<td>55.3054</td>
</tr>
<tr>
<td>iris2</td>
<td>281*197</td>
<td>0.2142</td>
<td>54.8221</td>
</tr>
<tr>
<td>iris3</td>
<td>295*194</td>
<td>0.1917</td>
<td>55.3054</td>
</tr>
<tr>
<td>iris4</td>
<td>295*194</td>
<td>0.1915</td>
<td>55.3102</td>
</tr>
<tr>
<td>iris5</td>
<td>281*197</td>
<td>0.2142</td>
<td>54.8221</td>
</tr>
<tr>
<td>iris6</td>
<td>295*194</td>
<td>0.2206</td>
<td>54.6945</td>
</tr>
</tbody>
</table>

Fig. 19. Image (a) before (B) after steganography. Message size=505
12 CONCLUSION

Face detection on skin color, connectivity component and grouping has been proposed, and also detect the faces or non-faces in the input images. Use morphology for iris detection. So, the algorithm consists of PCA feature extraction exclusive-XOR method of steganography. The results show a good numbers.

13 REFERENCES


[14] S. Chitra, G. Balakrishnan," Comparative Study for Two Color Spaces HSCbCr and


