IRIS DETECTION AND STEGANOGRAPHY

Sara Kh. Ayoub, Dr. Ahmed S. Nori

Computer Science Dept, College of Computer Science and Mathematics, Mosul University, Mosul, Iraq.
E-mail: Saraalsultan93@yahoo.com, Asn2203@yahoo.com

ABSTRACT

The term "biometrics" is derived from the Greek words bio means “life” and metric means “to measure.” The iris recognition system that was developed proved to be a highly accurate and efficient system that can be used for biometric identification. In this paper, for preprocessing canny edge detection then use morphology operation for iris detection, pca algorithm apply for extract feature. and steganography using Logical exclusive-OR.

Keywords: biometric, morphology, detection, feature extraction, steganography.

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. [6]

Steganography is the art and science of hiding information by embedding messages within other seemingly harmless messages. Steganography means “covered writing” in Greek. As the goal of steganography is to hide the presence of a message and to create a covert channel. [7]

Steganographic technologies are a very important part of the future of Internet security and privacy on open systems such as the Internet. [2]

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. [3]

Related work

1-iris detection

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. [14]

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%. [11]

2-Steganography

Barve S. and others proposed method is Biometric Steganography, the Biometric feature used to implement Steganography is Skin tone region of images. Proposed method introduces a new method of embedding secret data within the skin portion of the image of a person, as it is not that much sensitive to HVS (Human Visual System). Instead of embedding secret data anywhere in image, it will be
embedded in only skin tone region. This skin region provides excellent secure location for data hiding. So, firstly skin detection is performed in cover images and then Secret data embedding will be performed in DWT domain as DWT gives better performance than DCT while compression. This biometric method of Steganography enhances robustness than existing methods. [5]

Raghuvanshi S. and others describe methods to embedded data into some regions of the skin and not to the whole region. To separate the skin and non-skin regions, skin tone detection is performed using HSV color space. To increase the security, cropping and circular folding is performed on the B plane of the cover image. The secret data is embedded into the high frequency sub-band coefficients of DWT domain. Because human eyes are less sensitive in this sub-band, security is improved. In this paper, we analyze both cropping and non-cropping cases. This results into more security with cropping than without cropping with almost same PSNR.[10]

Characteristics of BIOMETRIC Technologies
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  
7) Circumvention- how easy it is to fool the system [12]

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.

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 [1]

Iris Detection
Iris is detected using morphological operations. Dilatation 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 twotone image, which generates iris, eyelids and eyebrows as a white portion.[4]

**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. [4]

**The Proposed Algorithm**

Steps of Iris detection see figures(3)-(9)
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.

**Feature Extraction using pca algorithm**

**PCA**

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. [15]

**PCA Algorithm Steps:**

A. Calculate the mean

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

B. Subtract the Mean:

\[
A = X_i - \mu \quad i = 1, 2, ..., M
\]

C. Calculating the covariance matrix:

\[
S = A A^T
\]  

D. Calculating the eigenvector and eigenvalue of the covariance matrix. [10]

**Steganography Using Logical Exclusive-XOR**

**Algorithm steps: see figure(7)**

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.

**The extracting process of the proposed system**

**Algorithm steps: see figure(8)**

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.

**Results**

1. Iris detection

Fig.(3) Original Image
2-Steganography

Fig. (7) image (a) before (b) after steganography. Message size=1889

Fig. (8) image (a) before (b) after steganography. Message size=505

Measuring Perceptual quality of steganography image [9][13]

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:

\[
PSNR = 10 \log_{10} \left( \frac{2 \times 255^2}{MSE} \right)
\]

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.

\[
MSE = \frac{1}{MN} \sum_{x=1}^{M} \sum_{y=1}^{N} (f(x, y) - f'(x, y))^2
\]
Normalized Correlation (NC): It measures the similarity representation between the original image and modified image.

\[
NC = \sum_{x=0}^{m-1} \sum_{y=0}^{n-1} steg\_im(x,y) \times cover\_im(x,y) / \sum_{x=0}^{m-1} \sum_{y=0}^{n-1} (cover\_im(x,y))^2
\]

(6)

See Tables (1),(2)

**TABLE1** MEASURE MESSAGE SIZE=1889

<table>
<thead>
<tr>
<th>IMAGES</th>
<th>IMAGE SIZE</th>
<th>MSE</th>
<th>PSNR</th>
<th>NC</th>
</tr>
</thead>
<tbody>
<tr>
<td>iris1</td>
<td>295*194</td>
<td>0.1917</td>
<td>55.3054</td>
<td>0.9999</td>
</tr>
<tr>
<td>iris2</td>
<td>281*197</td>
<td>0.2142</td>
<td>54.8221</td>
<td>1</td>
</tr>
<tr>
<td>iris3</td>
<td>295*194</td>
<td>0.1915</td>
<td>55.3102</td>
<td>0.9999</td>
</tr>
<tr>
<td>iris4</td>
<td>281*197</td>
<td>0.2142</td>
<td>54.8221</td>
<td>1</td>
</tr>
<tr>
<td>iris5</td>
<td>295*194</td>
<td>0.2206</td>
<td>54.6945</td>
<td>0.9999</td>
</tr>
<tr>
<td>iris6</td>
<td>227*222</td>
<td>0.2256</td>
<td>54.5979</td>
<td>0.9998</td>
</tr>
</tbody>
</table>

**TABLE2** MEASURE MESSAGE SIZE=505

<table>
<thead>
<tr>
<th>IMAGES</th>
<th>IMAGE SIZE</th>
<th>MSE</th>
<th>PSNR</th>
<th>NC</th>
</tr>
</thead>
<tbody>
<tr>
<td>iris1</td>
<td>295*194</td>
<td>0.1892</td>
<td>55.3620</td>
<td>0.9999</td>
</tr>
<tr>
<td>iris2</td>
<td>281*197</td>
<td>0.2129</td>
<td>54.8498</td>
<td>1</td>
</tr>
<tr>
<td>iris3</td>
<td>295*194</td>
<td>0.1896</td>
<td>55.3528</td>
<td>0.9999</td>
</tr>
<tr>
<td>iris4</td>
<td>281*197</td>
<td>0.2129</td>
<td>54.8498</td>
<td>1</td>
</tr>
<tr>
<td>iris5</td>
<td>295*194</td>
<td>0.2191</td>
<td>54.7245</td>
<td>0.9999</td>
</tr>
<tr>
<td>iris6</td>
<td>227*222</td>
<td>0.2235</td>
<td>54.6388</td>
<td>0.9998</td>
</tr>
</tbody>
</table>

Conclusions

In this work, the filed steganography has been used in an efficient manner.

So, the algorithm consists of PCA feature extraction exclusive-XOR method of steganography.

The results show a good numbers.

References

8. Mr. Kumar, T., & Mr. Kumar, K. (aprial 2008). mr.tapas kumar,mr.kiran kumar,"SEMINAR REPORT ON BIOMETRICS".

