Implementation of IRIS recognition for Securing Online Payment
B. KrishnaKumar¹, M. KishoreKumar², L. Karthikeyan³
Dhanalakshmi College of Engineering, Kancheepuram District, Tamilnadu, India

ABSTRACT
Iris Recognition is considered as the best among all the biometric security due to its high recognition rate, iris is unique for every human and even uncorrelated for twins. The proposed document focuses on implementing the iris recognition in online payment system by this users identity is more secured. Increase in the credit card fraudulent thefts needs further security for protecting them from phishing attack. The proposed concept also combines the visual cryptography algorithm along with iris recognition. Upcoming mobile phones are to be added with the feature of iris recognition. This method utilizes this feature for its implementation, thereby increasing customer confidence and decreasing identity theft.

Keywords: Iris Recognition, Visual Cryptography, Segmentation, Localisation, Visual Cryptography, Log Gaber Wavelet

I. INTRODUCTION
E-commerce has become one of the vital parts of the modern life. Online payment is the supportive application for the payment of money for the products we buy. For the past years online security breach created a major problem and lots of money had been stolen. The proposed document deals by securing the payment through iris recognition [1]. This method also adds the method of using visual cryptography for securing the user credentials. This visual cryptography method was formerly invented by Moni Naor and Adi Shamir in 1994[6].

II. METHODS AND MATERIAL

A. Image Acquisition
In this step user iris image is captured with high quality of iris. Images are obtained with needed resolution and sharpness. Images of iris can even be captured from 3 meters from the camera.

B. Image Processing
In this step initially iris localization is processed for finding the inner and outer boundary of the iris and then the image quality of the captured image is enhanced and the blur in the image are removed [2]. Further the segmentation is made to identify the individual regions perfectly. Then the segmented parts are normalized together and the enhancements were made. Then finally the discriminating characteristics of the iris textures are extracted. At last the image is stored in data base.

Figure 1: Graph showing proper capture of image

Figure 2: An Eye image

Figure 3: after localization, the segmented inner and outer boundary of Iris
Image Feature encoding was done with 1D Log-Gabor wavelet. 2D the pattern was normalized into a number of 1D signal. The rows belong to circular ring in the iris region. The angular direction is taken on the column side. The features extracted will be in code of 0 and 1.

C. Matching Results For User Validation

The user who needs to do online payment will launch into their mobile phone embedded with iris recognition and they will send their scanned image to the bank for verification which will be scanned with the image in the bank data base. Once verified a notification about valid user will be sent to the user.

D. Implementing Visual Cryptography

The account credentials given by the user are encrypted by initially encrypting them by text steganography and further for visual cryptography where ‘n’ number of shares are made and they were shared with the bank.

E. Verifying Shares

Once the share reaches the bank it is stored in data base. Then the share from the customer is verified with the share in the bank. Once the share gets verified then it gets redirected to the further transaction.

IRIS RECOGNITION AND VISUAL CRYPTOGRAPHY

In proposed method Iris Recognition is done by using Daugman algorithm[2][5]. Iris Sample is encoded into a 256 byte iris code. Then demodulating it with 2D Gabor wavelets. The generated iris code is unchangeable under translations and dilations. Iris images are matched by using the Hamming Distance (HD). For a project iris image the unwanted areas covered by eyelids, deep shadows, specular reflections are removed and the boundaries of pupil and iris are gathered by field optimization. Iris code which is to be matched is changed into 512 bytes[3].
Normally the hamming distance for images to be matched is 0.342. Daugman algorithm has the potential for comparing 14 billion iris samples in just a time span of less than 2 seconds. Also the Daugman algorithm has an accuracy level of more than 99.90%.

Daugman algorithm excludes the upper and lower portions of eyelids this helps the algorithm to work even faster. Integro-Differential operators are then used to detect the centre and diameter of the iris then the pupil is also detected using the differential operators.

The next algorithm utilized in this proposed system is Visual Cryptography (VC). It is a cryptographic technique in which data to be secured is mapped into the image and they were converted into ‘n’ number of shares. All these individual shares are meaningless which will never reveal any data. When any one of the image share is stolen it can never be utilized in any of the ways. Only when all the shared images are collected they can be decrypted and produces the original image.

As the name suggests visual cryptography is linked to human visual system[7]. To decrypt the shared images all the shared images are stacked together and it reveals the secret image.
The above diagram shows how the visual cryptography works and the method of working only if all the shares are stacked together. So, the shares of the customer and the bank are verified and only then the payment page gets redirected and the payment gets completed.

**PROPOSED PAYMENT METHOD**

The proposed method is more suitable for implementing in mobile phones. As the upcoming mobile phones are embedded with an iris recognizing biometric systems, with which the user can secure the online payment by this proposed method. When a user needs to perform an online payment then the user needs to log in by using the concerned person’s iris scan. The inbuilt iris recognizer captures the current user iris image and preprocesses the image then transfers the processed image to concerned bank. Bank database already contains the iris image of every registered user. The iris sample of the current user is matched with the whole bank database and if a match is found then the bank notifies the user and the user is redirected to the payment page.

Once the iris recognition gets succeeded then the user is redirected to the payment page where the user needs to provide their account credentials and all those details will be converted into ASCII values and then to their corresponding binary values which will be of 8 bits and those will be split into two 4 bits. For all those 4 bits corresponding English alphabet will be chosen from the Vedic numeral table [6].
Table 2: Vedic number assignments

<table>
<thead>
<tr>
<th>Letter</th>
<th>Number assigned</th>
<th>Letter</th>
<th>Number assigned</th>
</tr>
</thead>
<tbody>
<tr>
<td>E</td>
<td>15</td>
<td>M</td>
<td>7</td>
</tr>
<tr>
<td>A</td>
<td>14</td>
<td>H</td>
<td>7</td>
</tr>
<tr>
<td>R</td>
<td>13</td>
<td>G</td>
<td>6</td>
</tr>
<tr>
<td>I</td>
<td>13</td>
<td>B</td>
<td>5</td>
</tr>
<tr>
<td>O</td>
<td>12</td>
<td>F</td>
<td>4</td>
</tr>
<tr>
<td>T</td>
<td>11</td>
<td>Y</td>
<td>4</td>
</tr>
<tr>
<td>N</td>
<td>11</td>
<td>W</td>
<td>3</td>
</tr>
<tr>
<td>S</td>
<td>10</td>
<td>K</td>
<td>3</td>
</tr>
<tr>
<td>L</td>
<td>10</td>
<td>V</td>
<td>3</td>
</tr>
<tr>
<td>C</td>
<td>9</td>
<td>X</td>
<td>2</td>
</tr>
<tr>
<td>U</td>
<td>8</td>
<td>Z</td>
<td>2</td>
</tr>
<tr>
<td>D</td>
<td>5</td>
<td>J</td>
<td>1</td>
</tr>
<tr>
<td>P</td>
<td>7</td>
<td>Q</td>
<td>0</td>
</tr>
</tbody>
</table>

Once the corresponding alphabet is chosen then those modified string will be sent for visual cryptography where the image shares are produced and then shared with bank and the sender. For the payment to complete the sender will be sharing his corresponding share with the bank and once the bank verifies the shares the payment gets completed.

IV. CONCLUSION

The proposed payment system combines the Iris recognition with the visual cryptography by which customer data privacy can be obtained and prevents theft through phishing attack [8]. This method provides best for legitimate user identification. This method can also be implemented in computers using external iris recognition devices.

By using SQRT Normalization method we can achieve false match to a minimum of 1 in 100 billion.

V. REFERENCES