Abstract: Biometrics deal with automated methods of identifying a person or verifying the identity of a person based on physiological or behavioral characteristics. Visual cryptography is a secret sharing scheme where a secret image is encrypted into the shares which independently disclose no information about the original secret image. As biometric template are stored in the centralized database, due to security threats biometric template may be modified by attacker. If biometric template is altered authorized user will not be allowed to access the resource. To deal this issue visual cryptography schemes can be applied to secure the iris template. Visual cryptography provides great means for helping such security needs as well as extra layer of authentication.

Keywords: Template, Watermarking, Embedding, Extraction; Authentication.

I. INTRODUCTION

Biometrics is a technology that uses physiological or behavioral characteristics to authenticate identity of persons. For automated personal identification biometric authentication is getting more attention. There are various application where personal identification is required such as passport control, computer login control, secure electronic banking, bank ATM, credit cards, premises access control, border crossing, airport, mobile phones, health and social services, etc. Many biometric techniques are available such as facial thermo gram, hand vein, gait, keystroke, odor, ear, hand geometry, fingerprint, face, retina, iris, palm print, voice and signature. Among those iris recognition is one of the most promising approach because of stability, uniqueness and non-invasiveness. Biometrics systems are more consistent and more user friendly. Still there are certain issues particularly the security facet of both biometric system and biometric data. As template is stored in centralized database, they are vulnerable to eavesdropping and attacks. Thus alternative protection mechanisms need to be considered. For these reasons various researches have been made to protect the biometric data and template in the system by using cryptography, Stegnography and watermarking. In this paper a system is proposed by applying visual cryptography technique to biometric template (iris). Visual cryptography technique has been applied on to the iris template to make it secure from attack in centralized database as well as extra layer of authentication to the users.

II. RELATED WORK

A. Security Enhancement of Biometrics System

Recognizing a person using passwords is not sufficient for reliable identity determination because they can be easily shared, or stolen. A biometric system is essentially a pattern recognition system that recognizes a person based on a feature vector derived from a specific physiological or behavioral characteristic that the person possesses. Advantages of using biometrics characteristics are reliability, convenience, universality, and so on. But biometrics system does not provide privacy because biometric data is not replaceable and is not secret. There exist several types of attacks possible in a biometric system. Ratha et al., describe eight basic sources of attack as shown in Fig.1.

![Fig.1. Possible attack points in generic biometric systems](image)

Protecting the template is a challenging task in the biometric system (attack on point 6). Many researchers have been made to protect fingerprint and iris data and template. Davida at al, make the use of error-correcting codes in designing a secure biometrics system for access control. Following the work, Juels and Wattenberg broaden the system by establishing a different way of using error-correcting codes and approach is known as “fuzzy commitment”. Chander Kant et al, presented the idea for biometric security using
Steganography to make system more secure. While encoding the secret key (which is in the form of pixel intensities) will be merged in the picture itself, and only the authentic user will be allowed to decode. Khalil Zebbiche et al, proposed wavelet based digital watermarking method to hide biometric data (i.e. fingerprint minutiae data) into fingerprint images. This provides a high security to both hidden data (i.e. fingerprint minutiae) that have to be transmitted and the host image (i.e. fingerprint).

To protect fingerprint images presented an efficient technique for use in fingerprint images watermarking. The underlying principle of the technique is embedding the watermark into the ridges area of the fingerprint images which represents the region of interest. The viability of template-protected biometric authentication systems was exhibited with a fingerprint recognition system by introduced an amplitude modulation-based watermarking method in which they hide a user’s biometric data in a variety of images. By combining asymmetric digital watermarking and cryptography as a powerful mechanism was proposed by Nick Bartlow et al, to store raw biometric data in centralized databases. Shenglin Yang et al, presented a template protected secure iris verification system based on the Error Correcting Code (ECC) cryptographic technique with the reliable bits selection to improve the verification accuracy. In the scheme a transformed version of the iris template instead of the plain reference is stored for protecting the sensitive biometric data. Jing Dong et al, proposed biometric watermarking for protecting biometric data and templates in biometric systems. The scheme suggest protection of iris templates by hiding them in cover images as watermarks (iris watermarks), and protection of iris images by watermarking them.

B. Visual Cryptography

The basic visual cryptography scheme was proposed by Naor and Shamir’s. In this scheme for sharing a single pixel p, in a binary image Z into two shares A and B is illustrated in Table I. If p is white, one of the first two rows of Table I is chosen randomly to encode A and B. If p is black, one of the last two rows in Table I is chosen randomly to encode A and B. Thus, neither A nor B exposes any clue about the binary color of p. When these two shares are superimposed together, two black sub-pixels appear if p is black, while one black sub-pixel and one white sub-pixel appear if p is white as indicated in the rightmost column in Table 1. Based upon the contrast between two kinds of reconstructed pixels can tell whether p is black or white. Performance of visual cryptography scheme mainly depends on pixel expansion and contrast. Pixel expansion refers to the number of sub pixels in the generated shares that represents a pixel of the original input image. It represents the loss in resolution from the original picture to the shared one. Contrast is the relative difference in weight between combined shares that come from a white pixel and a black pixel in the original image. Plenty of research has been made to improve the performance of basic visual cryptography scheme. Many authors have proposed the visual cryptography schemes in which pixel expansion is 1. These schemes can be used as quality of retrieved images is good.

<table>
<thead>
<tr>
<th>Z</th>
<th>A</th>
<th>B</th>
<th>A&amp;B</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

III. PROPOSED METHOD

The aim of our biometric recognition system is to improve the template protection by embedding the iris data to hand vein images based on watermarking technology. The proposed technique of embedding of iris data to hand vein images using watermarking technology consist of following steps, i)preprocessing of iris and hand vein images, ii)iris template extraction, iii)Vein extraction, iv)Embedding of iris pattern to vein images based on region of interest, v) Storing embedded images.

A. Iris Image Pre-processing and key generation

The initial stage of our proposed method is pre-processing in which the iris images are acquired and process to extract the iris key. By subsequent localization, the information related with iris part is selected from the entire image.

1. Iris Localization

Nevertheless, localization can be said successful, when it is accomplished with minimum absences in the number of pixels inside the circle boundary. The reduction of number of pixels inside the circle boundary leads to fast and easy computation.

2. Image Normalization

The next stage after iris segmentation is normalization to generate iris key and their comparisons. Normalization process is comprised of two steps that are unwrapping the iris and conversion of it into polar equivalent. This can be done using Daugman's rubber sheet model.

3. Encoding

Generation of iris key is defined as the final process for which the most unique feature in the iris pattern is extracted. As the assigned phase angles are independent to the image contrast, only the phase information from the pattern is used. Due the dependency of amplitude information with inappropriate factors, it is not used.

B. Hand Vein image pre-processing and feature extraction

In this the dorsal hand vein images are acquired by an array of infrared light-emitting diode (LED) and a thermal camera.
Further to reduce the noise, the obtained hand vein image is pre-processed initially. Then apply mask to the pre-processed hand vein image. The size of the image obtained after masking is same as the input. Then find the values greater than zero values in the obtained masked image. After this the blood vessels from the hand vein image are obtained by using kirsch's template extraction method. It takes a single masked pixel of a hand vein image with a size of 3 x 3 and determines it strength of the edges by rotating it in 45 degree increments through all 8 directions.

Fig.2. Watermark Embedding.

IV. RESULTS AND DISCUSSION
In this section we analyzed and discussed about the proposed technique. The experimental setup and evaluation metrics are discussed in section IV.A. The dataset description is given in section IV.B. The experimental result is given in section IV.C. The performance evaluation is given in section IV.D.

A. Experimental Setup and Evaluation metrics
We had implemented the proposed method using MATLAB in a system having 6 GB RAM and 2.6 GHz Intel i-7 processor. Also, the evaluation metrics used here is the accuracy. The accuracy in multimodal biometric is computed based on FAR (False Acceptance Rate) and FRR (False Rejection Rate). Here, FAR is rate for which the system identifies the non-authorized person. It occurs due to the wrong matching of template with the input. False Rejection Rate is the rate of authorized person incorrectly rejected by the system. Here FAR is represented as,

$$\text{FAR}(t) = \frac{\text{GMS}}{\text{NGRA}}$$

Where, GMS means genuine matching score and NGRA means Number of Genuine Recognition Attempts Also the FRR is calculated by

$$\text{FRR}(t) = \frac{\text{IMS}}{\text{NIRA}}$$

IMS→+ Imposter Matching Score
NIRA→+ Number of Impostor Recognition Attempts

B. Dataset Description
In conjunction with the University of Bath, Smart Sensor Limited has collected a significant database of high quality iris images for use in research and evaluation. The pixel resolution of the collected iris image is 1280 x 960. Currently the full database consists of 800 people, i.e., 1600 eyes with 20 images of each left and right eye. A deliberate decision has been taken to start off with images of pristine quality, as there is a significant need in the scientific and research community to understand how iris recognition performance is affected by various image degradations including focus blur, motion blur, image compression, occlusions and gaze angle. Many of these degradations can be simulated for the purposes of research under mathematically calculated conditions which are usually unavailable when capturing images from commercial iris cameras. In addition to the high quality images, large numbers of 'non-ideal' images from the same subjects can also be made available on request. The hand vein database is a sample consists of images of 100 hands where each hand has 5 images, hence totaling to 500 images. Each has 5 images per person per each hand and hence it is associated to 50 distinct person for left and right hands of which the first 50 are for the right hands, the last 50 are for the left hand of the same person hand. So 1 in first set is RH HV and 51 is left hand to same person 1 in RH. This dataset is for both females and males in the range of 16-65 years age. Subjects are of healthy conditions and are from all folks of life including students, professors, engineers' workers, house wives, etc.

C. Experimental Result
The result obtained at various stage of our method IS shown below.

Fig.3 (a) Original Iris Image
Fig.3 (b) Iris Image with Boundaries
Initially the original iris image obtained is shown in the Fig. 3(a). Further the obtained original iris image is processed to obtain the boundaries of the image using the canny edge detector which is shown in the Fig. 3(b). After obtaining the boundaries the iris image is segmented as shown in the above Fig. 3(c). Then the boundaries from the segmented image are obtained that contain information which is shown in the Fig. 3 (d). The Fig. 3 (e) represents the polar array obtained after iris image normalization process. Finally the iris key feature is extracted from the boundaries. The next stage of our proposed method is vein image extraction. Here the original hand vein image is shown in the Fig. 4 (a).

After this the obtained original hand vein image is preprocessed at various stages to obtain the vein feature which is shown in the Fig. 4(b). After this the iris key extracted in the first stage is embedded in the pre-processed vein image. Finally the watermarked vein image obtained is shown in the Fig. 4(c).

D. Performance Evaluation

The performance analysis is made based on the evaluation metrics such as accuracy, FAR and FRR. Here, the iris key generated from the iris image is embedded in the plain image. The evaluation metrics may vary based on varying the bit position. The accuracy, FAR and FRR obtained for the 151 bit substitution is shown below.

---

**Fig. 3(c) Segmented Irish Image**

**Fig. 3 (d) Segmented Irish Image with Boundaries**

**Fig. 3 (e) Polar array obtained after Normalization**

**Fig. 4(b) Vein Image after Preprocessing**

**Fig. 4(c) Watermarked hand vein Image**

**Fig. 4 (a) Original hand vein Image**

**Fig. 5. Accuracy for 1st Bit substitution.**
For the 1st bit substitution the accuracy for both sum and product rule is obtained by varying threshold value. Here, the accuracy obtained for the product rule is not much increasing than the sum rule for varying threshold. Likewise, the false acceptance rate for both sum and product rule is obtained by varying threshold. From the FAR we noted that the FAR for sum rule is not varying with varying threshold but for product rule there is a lighter variation with varying threshold. Similarly from the False Rejection Rate obtained we found that, the FRR for the product rule is decreasing slightly with varying threshold and also for sum rule the FRR is very low when threshold is very high.

Table I. Accuracy, FAR and FRR Obtained for Sum Rule

<table>
<thead>
<tr>
<th>Threshold</th>
<th>Accuracy</th>
<th>FAR</th>
<th>FRR</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2</td>
<td>0.913242</td>
<td>0.050228</td>
<td>0.03653</td>
</tr>
<tr>
<td>4.25</td>
<td>0.929224</td>
<td>0.054795</td>
<td>0.015982</td>
</tr>
<tr>
<td>4.3</td>
<td>0.931507</td>
<td>0.06621</td>
<td>0.002283</td>
</tr>
<tr>
<td>4.35</td>
<td>0.929224</td>
<td>0.070776</td>
<td>0</td>
</tr>
<tr>
<td>4.4</td>
<td>0.924658</td>
<td>0.075342</td>
<td>0</td>
</tr>
<tr>
<td>4.45</td>
<td>0.920091</td>
<td>0.079909</td>
<td>0</td>
</tr>
</tbody>
</table>

Similarly the accuracy, FAR and FRR obtained for product rule for different threshold is given in the below Table II.

Table II. Accuracy FAR and FRR Obtained For Product Rule

<table>
<thead>
<tr>
<th>Threshold</th>
<th>Accuracy</th>
<th>FAR</th>
<th>FRR</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2</td>
<td>0.863014</td>
<td>0.102857</td>
<td>0.011429</td>
</tr>
<tr>
<td>4.25</td>
<td>0.858447</td>
<td>0.106667</td>
<td>0.011429</td>
</tr>
<tr>
<td>4.3</td>
<td>0.863014</td>
<td>0.108571</td>
<td>0.005714</td>
</tr>
<tr>
<td>4.35</td>
<td>0.860731</td>
<td>0.110476</td>
<td>0.005714</td>
</tr>
<tr>
<td>4.4</td>
<td>0.863014</td>
<td>0.112381</td>
<td>0.001905</td>
</tr>
<tr>
<td>4.45</td>
<td>0.863014</td>
<td>0.112381</td>
<td>0.001905</td>
</tr>
</tbody>
</table>

V. CONCLUSION

Various approaches adopted by researchers to secure the raw biometric data and template in database are discussed here. In this paper a method is proposed to store iris template securely in the database using visual cryptography. Experimental results indicate that by applying visual cryptography techniques on iris template for more security, matching performance of iris recognition is unaffected with extra layer of authentication. Speed of iris authentication system is slower it can be also improved using other systems. Here generated shares are meaningless using other visual cryptography techniques which generates meaningful share can also be applied.

VI. REFERENCES