Iris Cryptography for Security Purpose

1Srighakollapu Ajith, 2M Balaji Ganesh Kumar, 3S Latha, Dhanalakshmi Samiappan, 4P Muthu
1,2,3 ECE Department, SRM Institute of Science & Technology, Kattankulathur, Chennai – 603203
4 Biomedical Engineering Department, SRM Institute of Science & Technology, Kattankulathur, Chennai – 603203
Email: latha.su@ktr.srmuniv.ac.in

Abstract. In today's world, the security became the major issue to every human being. A major issue is hacking as hackers are everywhere, as the technology was developed still there are many issues where the technology fails to meet the security. Engineers, scientists were discovering the new products for security purpose as biometrics sensors like face recognition, pattern recognition, gesture recognition, voice authentication etcetera. But these devices fail to reach the expected results. In this work, we are going to present an approach to generate a unique secure key using the iris template. Here the iris templates are processed using the well-defined processing techniques. Using the encryption and decryption process they are stored, traversed and utilized. As of the work, we can conclude that the iris cryptography gives us the expected results for securing the data from eavesdroppers.

1. Introduction
Cryptography is exclusively concerned with establishing the secrecy between the communication bodies . The word cryptography means the art of writing or solving the codes in this world either ever thing is secret or everything is open to all for free access. Cryptography emerges from the ancient Greeks it is actually means encoding of the text which we need to communicate with other people . This encoded text is passed through the common communication channel so that no eavesdropper can understand the plain text even he hold that cipher text. There are also different types of cryptographic techniques like shift cipher, vigenere cipher , one time pad , visual cryptography etc.

1.1 Shift Cipher:
Here the key which is used to encode the date will be of very small length of at most one character the attacker can easily guess the plain text because the plain text which we are going to use is in the form normal English there are at most twenty six characters in this language so the probability of guessing the correct plain text is 100% If attacker know which language communicating body is using. Before the invention of the vegenere cipher this method is considered to be efficient according the frequency distribution of the letters in the normal English the correct plain text can be found. The xor operation of the key with the message is considered more efficient than the add operation because the xor operation is reversible the xor of the key with the key is equal to zero and this makes the sense that the xor of the zero with the message is always the message

Let X=X’ MOD N, Which means that N divides the value X-X’
M={Set of all lower case letters }
Shift cipher satisfies the lower case letters. Let the key K belongs to any of the letter from English alphabets {0,1,2,3,4……25}. The probability of selecting the key from the set of all English is 1/26. Then the encryption scheme follows as Let C be the cipher text Then Ci=[Mi +K MOD 26]
Outputs are \{c_1,c_2,c_3,c_4,\ldots\,c_i\} and the messages are \{m_1,m_2,m_3,m_4,\ldots,m_i\}. The decryption is as follows \[ M_i = [C_i - K \mod 26]. \] The shift cipher follows the Laws like Kerckhoff's principle, which states that encryption schemes which are used to not to be considered secret the only secret should be the key.

1.2. Vegenere Cipher:

In vigenere cipher the key which we are going to use should be of length at least two by using the vegenere cipher we can encrypt the message and the key which is shared by the communicating bodies can decrypt the message here the job of eavesdropper become tough because the key used here will be of length greater than two and for decryption purpose it will become the tough job. In the vigenere cipher the plain text will be in ascii characters and the key will be in the hexadecimal resulting to the hexadecimal number.

1.3. One Time Pad:

The decryption of one time pass word is more tougher job than the remaining two methods here the key can take any random values for suppose if the key length is 5 then the total number of values choosen will be of 12 million as \(26*26*26*26*26=12 \text{ million}\)

Let \(M=\{0,1\}^n\)

It means that the message can be of any length ranging from 0 to n and the values of the message will be 0 and 1. Similarly \(k=\{0,1\}^n\). Key is uniform n bit string \(\text{enc}(m)=k\oplus m\)

\[ \text{DEC}(c)=k\oplus c \]

In one time pad the encrypted message will be secret if the \(p(M=m/C=c)=p(M=m)\). The probability of the cipher is

\[ p(C=c)=\sum_m p(C=c/M=m)p(M=m) \]

\[ =\sum_m p(K=m\oplus c)p(M=m) \]

\[ =\sum_m p(C=c/K=m\oplus c) \]

Because the key used will be fixed with respect to the message and the cipher since the one time pad chooses the key uniformly of n bits. So let the length of the key is ‘n’. The the total possible values of the key are \(2^n\). The probability of selecting the one key from the set \(2^n\) keys is \(1/2^n=2^{-n}\). Then the probability of cipher will be \(2^{-n}\). According to the bayes theorem the probability of message with given initial condition is cipher is

\[ p(M=m/C=c)=p(C=c/M=m)p(M=m)/p(C=c) \]

\[ =2^{-n}(p(M=m)/2^{-n}) \]

\[ =p(M=m) \]

This is the required condition for the message to be secure in one time pad. The length of the key which we are using should greater than or equal to the length of the message.

1.4. Visual Cryptography:

Visual cryptography is technique in which the visual information to be encrypted the encrypted image can be decrypted by the user with the set of all keys. Visual cryptography is the visual sharing scheme in which the image to be shared is broken in to the pieces up to n shares. The individual with all shares can only decrypt the image, while n-1 shares cannot reveal the image.
2. Iris cryptography

Nowadays providing security to the information stored became a crucial process so many techniques were evolved such as fingerprint, motion detector’s, voice detector’s, iris detectors among them the iris biometrics were believed to be providing the more accurate security as we believe that no two persons in the world has same iris pattern, so it paves the way for security. Iris cryptography basically means of storing the eye templates of the user in a database for authentication purpose.

The iris authentication is done in the following steps initially the user eye template is collected and then the preprocessing steps were carried out here the carried template will go for segmentation because each small part of the collected template is useful so we are visualizing it carefully next the segmented parts are normalized converting the polar coordinates to the rectangular coordinates and then storing the templates. Careful measures to be taken for storing the templates because the templates stored may be hacked.

![Figure 1. Conversion of the circular coordinates to rectangular coordinates](image)

3. Authentication of User

Authentication can be done in many ways password based authentication can be one of the best choice but can be hacked. Device based authentication involves providing the soft and hard tokens the soft tokens actually means giving the user the user name, password and the keyword to enter. Hardware tokens are like using the (eg. ATM where we use the ATM cards along with the password) they can also be hacked easily. Among all the most secure and the powerful method is biometrics where the iris authentication is providing the better accuracy.

4. Visual Cryptography

This is a cryptographic technique which allows visual information i.e. pictures, text, etc. to be encrypted in such a way that decryption can be done by human visual system without the use of computers.

5. Literature Review

5.1. Hough Transform:

The Hough transform is a standard computer vision algorithm that can be used to determine the parameters of simple geometric objects, such as lines and circles, present in an image. The circular Hough transform can be employed to deduce the radius and center coordinates of the pupil and iris regions. An automatic segment algorithm is done on the image.

5.2. Segmentation:

This is the process of segmentation where the captured images are segmented to get the required region of interest.

5.3. Normalization:

For normalisation of iris regions a technique based on Daugman’s rubber sheet model was employed. The centre of the pupil was considered as the reference point, and radial vectors pass through the iris region, as shown in Figure A number of data points are selected along each radial line and this is defined as the radial resolution. The number of radial lines going around the iris region is defined as
the angular resolution. Since the pupil can be non-concentric to the iris, a remapping formula is needed to rescale points depending on the angle around the circle.

![Figure 2. Hough transform results of the given eye template](image)

**Figure 2.** Hough transform results of the given eye template

6. Architecture

Visual cryptography is used for protecting the iris templates from attackers and to avoid an unauthorized access. The system consists of two modules one is enrollment module and the other is authentication module.

Enrollment phase: During the enrollment module the information is collected from the person. The system administrator collect all biometric information from an authorized person.

SNF module: it is the processing step in the enrollment module. During this phase the eye images of the authorized person will be passed to the SNF module which has three steps one is segmentation, and other is normalization and the last step is feature extraction. The extracted iris image is stored in the database it is named as any system generated random number. The png image will be sent to the VC module. The main role of the segmentation is extract the iris template from the eye image. Only the center part of the eye image is used for the future purpose of authentication. So the main role of segmentation is to extract the center part of the eye retina. In normalization the iris image is transformed from the polar coordinates to the required coordinates specified.

In feature extraction accurate recognition of individuals is obtained. The most essential information of the iris must be extracted. Only the desired feature of the iris must be encoded so that template can be compared.

VC module: Using the random number generator algorithm the extracted eye image is stored in a database. This number is given to the input to the vc module and then two share are generated. Out of which one share is stored in the database and the other is with the employee.

Authentication phase: In this phase eye image of the user will be passed to the SNF process. Then this extracted image and the iris template will be compared. If the template matches then the user is authorized user.

7. Improvements

The proposed method will work only for monochrome images. The future work is to be on the colored eye image. The shared should be generated using the color visual cryptography.

8. Applications

Secure Banking sector there is a chance of encountering forged signature for transaction. And in the net banking system, the password of user may be hacked and misused. Thus security is still a challenge to the users. A scheme is proposed for securing the user information and to prevent the possible forgery signature and of password hacking. The concept of image processing, in visual cryptography know as iris cryptography is used.
9. Conclusion

There are many techniques for storing the iris templates but the visual cryptography method is the most secure one. The visual cryptography proposed in this paper will generates the meaning full shares which reduces the problem of existing method .In existing method, the shares generated are of poor quality compared to the original image. The improvement techniques need to be encouraged.

10. References

[1] Libor masek Handbook on the Recognition of Human Iris patterns for Biometric Identification
[2] Sneha kallapur Enhancing the iris scanning using the visual cryptography
[3] Jonathan katzAn on Introduction to Cryptography (coursera:University of MaryLand)
[4] R.Sruthi, M.Rakhunde and ManishaGedam Survey on Visual Cryptography Techniques, Advantages and Applications
[5] Unnikrishnan, C.E. Pantofaru and M. Hebert on Toward objective evaluation of image segmentation algorithms (IEEE Transactions on Pattern Analysis and Machine Intelligence) vol.29, no.6, pp. 929-943, 2007.