Iris Recognition Based on Visual Cryptography

Vithya G,ME student
Department of Electronics and Communication Engineering,
communication system
Mahendra Engineering College,Mallasamudram,Tamilnadu,India

Abstract— **Cryptography is a technique which uses mathematics to encrypt and decrypt data. Using cryptography information can be transmitted through secure channel so that only the intended recipient can access .The secret key is extracted from the iris image so that security improves. This key is used to encrypt the data to be sent. Different tests are conducted to check the randomness of the key. A novel iris recognition method is presented.In this method, the iris features are extracted using the oriented separable wavelet transforms (direction lets) and they are compared in terms of a weighted Hamming distance. The feature extraction and comparison are shift-, size- and rotation-invariant to the location of iris in the acquired image. The generated iris code is binary, whose length is fixed (and therefore commensurable), independent of the iris image, and comparatively short. The novel method shows a good performance when applied to a large database of irises and provides reliable identification and verification. At the same time, it preserves conceptual and computational simplicity and allows for a quick analysis and comparison of iris samples.**

Index terms-Hamming Distance

I. Introduction

Total words should not In today's information technology world, security for systems is becoming more and more important. The number of systems that have been compromised is ever increasing and authentication plays a major role as a first line of defence against intruders. In the present scenario, fast growth in online application results in data security problem. In order to get secure internet, users need secure communication method for sending secret messages and data through internet. Iris Recognition and Cryptography technology is an efficient way to provide a secure internet. The three main types of authentication are password, a card or token, and biometric. Passwords are notorious for being weak and easily crack able due to human nature and our tendency to make passwords easy to remember or write them down somewhere easily accessible. Cards and tokens can be presented by anyone and although the token or card is recognisable, there is no way of knowing if the person presenting the card is the actual owner.

Biometrics, on the other hand, provides a secure method of authentication and identification, as they are difficult to replicate and steal. If biometrics is used in conjunction with something you know, then this achieves two-factor authentication. Two-factor authentication is much stronger as it requires both components before a user is able to access anything. Biometric identification utilises physiological and behavioural characteristics to authenticate a person's identity. Some common physical characteristics that may be used for identification include fingerprints, palm prints, hand geometry, retinal patterns and iris patterns. Behavioural characteristics include signature, voice pattern and keystroke dynamics.

II. Cryptography and Object of Dissertation

Cryptography is the study of hiding some confidential information. Cryptography uses mathematical algorithms to create three types of encoded messages. Single Key Cryptography uses the same key shared by the message writer and reader to encode and decode standard language messages. Public key, or asymmetric cryptography, uses two separate keys: one for encryption and another for decryption.

The key length of AES algorithm is much longer the DES. Both of them is widely applied on the copyright protection, commercial image transaction, content authentication, and trusted camera. For watermarking it concentrates on the public key verification watermark, which is the extension of the secret key scheme. Regard to the visual cryptography, is not only refers the conventional visual secret sharing (VSS) system but also the size invariant VSS, which is the refined vision of conventional VSS. Finally, the integration between the data hiding and the visual cryptography is introduced**.**

Currently the system has a text file for storing iris encodings. This could be improved to mirror a real-world application deployment by interfacing with a database. Although due to the one of many searches involved with iris recognition database querying could potentially become a bottle neck. Another area worth exploring is implementing the software with a client/server architecture whereby the iris is encoded client side, and compared server side. Again, this more accurately mirrors real world deployment of iris recognition software. This would then require further investigation into security and encryption methods for the system. IRIS recognition has tremendous potential for security in any field. The iris is extremely unique and cannot be artificially impersonated by a photograph. This enables security to be able to restrict access to specific individuals. An iris is an internal organ making it immune to environmental effects. Since an iris does not change over the course of a lifetime.

The pressures on today's system administrators to have secure systems are ever increasing. One area where security can be improved is in authentication. Iris recognition, a biometric, provides one of the most secure methods of authentication and identification to the unique characteristics of the iris. Once the image of the iris has been captured using a standard camera, the authentication process, involving comparing the current subject's iris with the stored version, is one of the most accurate with very low false acceptance and rejection rates. The technology is accurate, easy to use, non-intrusive, and difficult to forge and, despite what people may think, is actually quite a fast system once initial enrolment has taken place. However, it does require the co-operation of the subject, needs specific hardware and software to operate and administrators need to ensure they have a fall back plan should the resources required to operate the system fail.

III. Review of Literature

Iris Recognition is a rapidly expanding method of biometric authentication that uses pattern-recognition techniques on images of iris to uniquely identify an individual. Algorithms produced by Professor John Daugman [1] have proven to be increasingly ac- curate and reliable after over 200 billion comparisons [2]. The aim of this group project is to implement a working prototype of the techniques and methods used for iris recognition, and to test these methods on a database of irides provided by the Chinese Academy of Sciences' Institute of Automation (CASIA) [3], which consists of 756 images of iris from 108 individuals

Security and the authentication of individuals is necessary for many different areas of our lives, with most people having to authenticate their identity on a daily basis; examples include ATMs, secure access to buildings, and international travel. Biometric identification provides a valid alternative to traditional authentication mechanisms such as ID cards and passwords, whilst overcoming many of the shortfalls of these methods; it is possible to identify an individual based on "who they are" rather than "what they possess" or "what they remember" [4].

Iris recognition is a particular type of biometric system that can be used to reliably indentify a person by analysing the patterns found in the iris. The iris is so reliable as a form of identification because of the uniqueness of its pattern. Although there is a genetic influence, particularly on the iris' colour, the iris develops through folding of the tissue membrane and then degeneration (to create the pupil opening) which results in a random and unique iris [5].

In comparison to other visual recognition techniques, the iris has a great advantage in that there is huge variability of the pattern between individuals, meaning that large databases can be searched without finding any false matches [1]. This means that iris can be used to identify individuals rather than just confirm their given identity; a property that would be useful in a situation such as border control, where it might be important to not just show that an individual is not who they say they are but also to show exactly who they are.

The objective of this project was to produce a working prototype program that functions as an iris recognition tool using the algorithms described by Professor John Daugman [1] and other techniques in order to implement this in an accurate and useful way that is also user-friendly. Commercial iris recognition systems are available that implement similar algorithms to these; however, there does seem to be an absence of open source implementations. This is the hole that this project sets out to fill: providing a fast, usable program that can easily be extended.

A biometric system provides automatic identification of an individual based on a unique feature or characteristic possessed by the individual. Iris recognition is regarded as the most reliable and accurate biometric identification system available. Most commercial iris recognition systems use patented algorithms developed by Daugman, and these algorithms are able to produce perfect recognition rates. However, published results have usually been produced under favourable conditions, and there have been no independent trials of the technology.

The work presented in this thesis involved developing an 'open-source' iris recognition system in order to verify both the uniqueness of the human iris and also its performance as a biometric. For determining the recognition performance of the system two databases of digitised greyscale eye images were used. The iris recognition system consists of an automatic segmentation system that is based on the Hough transform, and is able to localise the circular iris and pupil region, occluding eyelids and eyelashes, and reflections. The extracted iris region was then normalised into a rectangular block with constant dimensions to account for imaging inconsistencies. Finally, the phase data from 1D Log-Gabor filters was extracted and quantised to four levels to encode the unique pattern of the iris into a bit-wise biometric template.

The Hamming distance was employed for classification of iris templates, and two templates were found to match if a test of statistical independence was failed. The system performed with perfect recognition on a set of 75 eye images; however, tests on another set of 624 images resulted in false accept and false reject rates of 0.005% and 0.238% respectively. Therefore, iris recognition is shown to be a reliable and accurate biometric technology.[1]

IV. Algorithm Implemented

A biometric system works by capturing and storing the biometric information and then comparing the scanned biometric with what is stored in the repository. Out of all the various physical characteristics available, irises are one of the more accurate physiological characteristics that can be used. Iris recognition is the process of recognizing a person by analysing the random pattern of the iris. The automated method of iris recognition is relatively young, existing in patent only since 1994. The iris is a muscle within the eye that regulates the size of the pupil, controlling the amount of light that enters the eye. It is the coloured portion of the eye with colouring based on the amount of melatonin pigment within the muscle. The fact that the iris is protected behind the eyelid, cornea and aqueous humour means that, unlike other biometrics such as fingerprints, the likelihood of damage and abrasion is minimal.The iris is not subjected to the effects of aging which means it remains in a stable form from about the age of one until death.

The stages involved in Iris reorganization are,

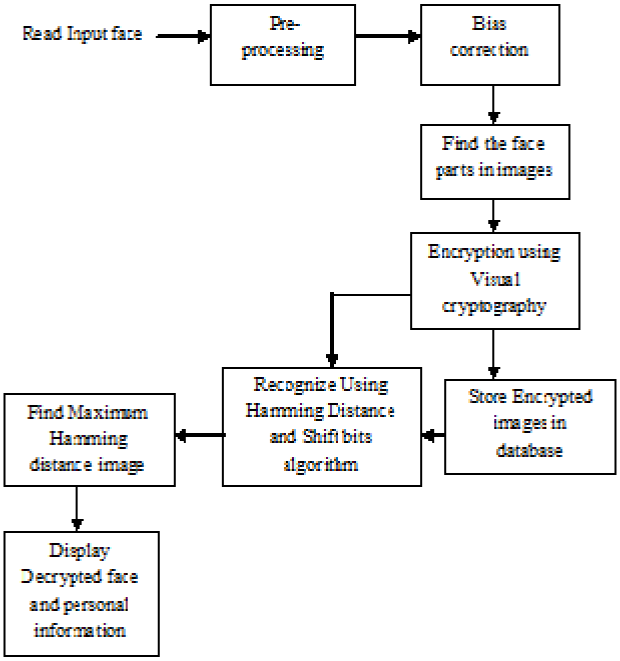
Read Input face
Pre-processing
Bias correction
Find the face parts in images
Encryption using Visual cryptography
Store Encrypted images in database
Recognize Using Hamming Distance and Shift bits algorithm
Find Maximum Hamming distance image
Display Decrypted face and personal information

Figure 1: **Frame work ofIRIS recognition**

A.ACQUISITION

Iris image acquisition is the first step in iris recognition. The small size of the iris combined with the possibility of varying iris colours means a special camera must be used, especially for people with darker coloured irises. At the time of acquisition, the user has to stand in a range of 10-50 cm (4-20 inches) from the acquisition device and stare at the acquiring window with eyes widely open so that a clear iris image can be acquired.

B.SEGMENTATION

The first stage of iris recognition is to isolate the actual iris region in a digital eye image. The iris region is approximated by two circles, one for the iris/sclera boundary and another for the iris/pupil boundary.

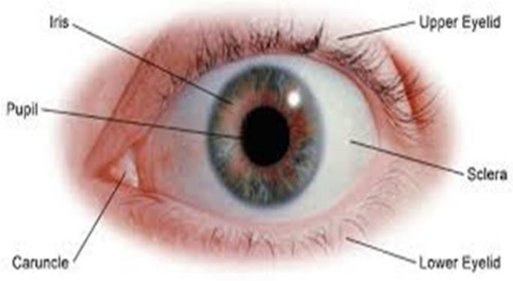

Figure 4.3: **Segmentation Process**

C.Locating the IRIS Image

The iris is captured in an image by a camera.

The camera needs to be able to photograph a picture in the 700 to 900 nanometers range so that it will not be detected by the person’s iris during imaging (Daugman,2003b). The camera may or may not have a wide-angle lens yielding a higher resolution, but in either case a mirror is used to utilize feedback for the image. These conditions must be met in order for the iris image to have the necessary 50-pixel minimum size of the iris radius.

Once the image of the iris is obtained, the iris needs to be located within the image. There are three variables within the image that are needed to fully locate the iris: the center coordinates, the iris radius, and the pupil radius (Daugman, 2003b). An algorithm determines the maximum contour integral derivatives using the three variables to define a path of contour inte- gration for each of the variables. The complex analysis of the algorithm finds the contour paths defining the outer and inner circumferences of the iris. Statistical estimation changes the circular paths of the integral derivatives to arc-shaped paths that best fit both iris boundaries.

D.Encoding the IRIS Image

once the iris has been located it must be encoded into an iris phase code.The iris image is encoded using two-dimensional Gabor wavelets(Daugman,2003a) .A wavelet is a correspondence to a signal in a waveform of a finite length. A wavelet transform may be used to compile raw data,like an image,and encode it into a comrpessed file.This application can be used directly in iris recognition for the encoding process.Daugman uses wavelets to create more than two thousand phase bits from a raw imagein a dimension- less polar coordinate system(2004).The system is dimensionless to allow for more flexibility when comparing iris images of different size and quality.Polar coordinates are used because they represent these curves in a simler way compared to other coordinate systems,

Although a recognition system can use the unwrapped iris directly to compare two irises, most systems first use a feature extraction routine to encode the iris’s textural content. The iris is encoded to a unique set of 2048 bits which serve as the fundamental identification of that person’s particular iris. These iris bit codes can be stored in a database and then compared to uniquely identify a person. The size of 2048 is sufficiently large to store the data of several particular filters on most angles of the iris, while also being sufficiently small to be easily stored in a database and manipulated quickly.

H.Hamming Distance

The Hamming Distance is a number used to denote the difference between two binary strings. The Hamming Code earned Richard Hamming the Eduard Rheim Award of Achievement in Technology in 1996, two years before his death. Hamming's additions to information technology have been used in such innovations as modems and compact discs..The Hamming distance gives a measure of how many bits are the same between two bit patterns. In comparing the bit patterns X and Y, the Hamming distance (HD) is defined as the sum of disagreeing bits (sum of the exclusive-OR between X and Y) over N, the total number of bits in the bit pattern. Since an individual iris region contains features with high degrees of freedom, each iris region produce a bit- pattern which is independent to that produced by another iris.

On the other hand, two iris codes produced from the same iris will be highly correlated. If two patterns are derived from the same iris, the Hamming distance between them is close to 0.0, since they are highly correlated and the bits should agree between the two iris codes.

I.BIT SHIFTS

The bit shifts are sometimes considered bitwise operations, because they treat a value as a series of bits rather than as a numerical quantity. In these operations the digits are moved, or shifted, to the left or right. Registers in a computer processor have a fixed width, so some bits will be "shifted out" of the register at one end, while the same number of bits is "shifted in" from the other end; the differences between bit shift operators lie in how they determine the values of the shifted-in bits.

E.VIOLA–JONES Object Detection Framework

The Viola–Jonesobject detection framework is the first object detection framework to provide competitive object detection rates in real-time proposed in 2001 by Paul Viola and Michael Jones. Although it can be trained to detect a variety of object classes, it was motivated primarily by the problem of face detection. This algorithm is implemented in Open CV as cvHaar Detection Objects. The basic problem to be solved is to implement an algorithm for detection of faces in an image. This can be solved easily by humans. However there is a stark contrast to how difficult it actually is to make a computer successfully solve this task. In order to ease the task Viola–Jones limit themselves to full view frontal upright faces. That is, in order to be detected the entire face must point towards the camera and it should not be tilted to any side. This may compromise the requirement for being unconstrained a little bit, but considering that the detection algorithm most often will be succeeded by a recognition algorithm these demands seem quite reasonable.

F.MATCHING OF IRIS CODE

The question remains, what constitutes a match? Specifically, the number of iris phase bits that need to correspond for a match must be determined (Daugman, 2004). The number of phase bits required for a match is decided based on the specific application regarding how many irises need to be compared. Irises need to be matched regardless of their size, position, or orientation. This is accomplished by placing the image into a dimensionless polar coordinate system. Since the inner to outer boundary range of the iris is defined to be the unit interval, the pupil dilation and location becomes invariant. The criteria used to decide if iris codes match is called the Hamming distance criterion, which is the integration of the density function raised to the power of the number of independent tests.

A density function is the sum of all probabilities of a possible outcome given a random variable, which in this case is the Hamming distance of an iris phase code. A smaller criterion results in an exponentially decreasing chance of having a false match. This allows the strictness of matching irises to easily change for the particular application. A Hamming distance criterion of 0.26 gives the odds of a false match of 1 in 10 trillion, while a criterion of 0.32 gives the odds of 1 in 26 million. The numeric values of 0.26 and 0.32 represent the fractional amount that two iris codes can differ while still being considered a match in their respective instances.

G.DECRYPTION OF IRIS

Decryption is the process of retrieving the original data from the Encrypted data. After the biometric authentication is completed the customer will give his share. The two shares from the application side and the client side would be superimposed and if they match the secret would be revealed. This would be done for each level and the embedded secrets at each level will also be revealed. Decryption requires a secret key or password. There are of course a wide range of cryptographic algorithms in use.

V.VISUAL CRYPTOGRAPHY

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes a mechanical operation that does not require a computer. Moni Naor and Adi Shamir demonstrated a visual secret sharing scheme, where an image was broken up into n shares so that only someone with all n shares could decrypt the image, while any n − 1 shares revealed no information about the original image. Each share is printed on a separate transparency, and decryption was performed by overlaying the shares. When all n shares were overlaid, the original image appears.

A.(2, N) Visual Cryptography Sharing Case

Sharing a secret with an arbitrary number of people N such that at least 2 of them are required to decode the secret is one form of the visual secret sharing scheme presented by MoniNaor and Adi Shamir in 1994. The schemes have a secret image which is encoded into N shares printed on transparencies. The shares appear random and contain no decipherable information about the underlying secret image, however if any 2 of the shares are stacked on top of one another the secret image becomes decipherable by the human eye.

For instance in the (2, 2) sharing case (the secret is split into 2 shares and both shares are required to decode the secret) complementary matrices are used to share a black pixel and identical matrices to share a white pixel. Stacking the shares have all the sub pixels associated with the black pixel now black while 50% of the sub pixels associated with the white pixel remain white. Every pixel from the secret image is encoded into multiple sub pixels in each share image using a matrix to determine the color of the pixels.

B.Cheating the (2, N) Visual Secret Sharing Scheme

Horng proposed a method that allows N − 1 colluding parties to cheat an honest party in visual cryptography. The advantage of knowing the underlying distribution of the pixels in the shares is to create new shares that combine with existing shares to form a new secret message of the cheaters choosing.

Two shares are enough to decode the secret image using the human visual system. But examining two shares also gives some information about the 3rd share. Knowing where black pixels exist in another party's share allows them to create a new share that will combine with the predicted share to form a new secret message. In this way a set of colluding parties that have enough shares to access the secret code can cheat other honest parties.

VI.RESULTS AND DISCUSSION

The most computation intensive stages include performing the Hough Transform, and calculating Hamming distance values between templates to search for a match. Since the system is implemented in MATLAB interpreted language, speed benefits could be made by implementing computationally intensive parts in C or C++.The result shows that the databases that was stored already of a person and his/her detected eyes with their personal details are shown in fig:2.

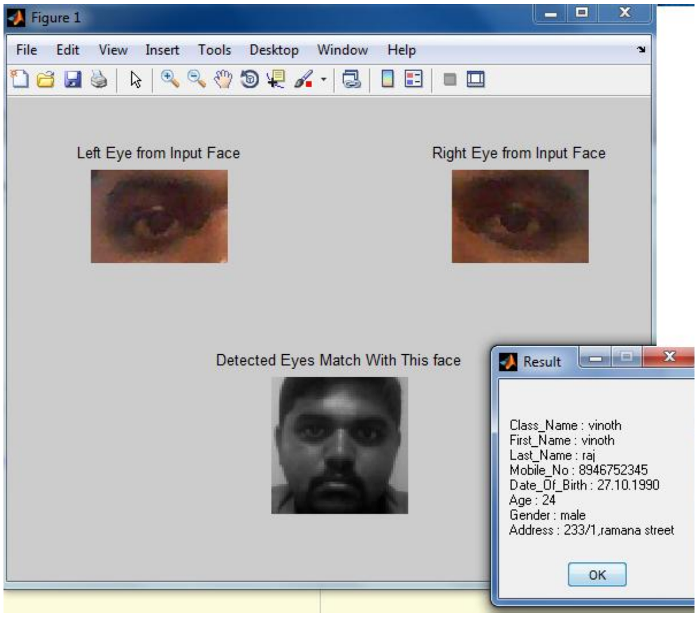
Figure 1
File Edit View Insert Tools Desktop Window Help
Left Eye from Input Face
Right Eye from Input Face
Detected Eyes Match With This face
Result
OK

Class_Name : vinoth
First_Name : vinoth
Last_Name : raj
Mobile_No : 8946752345
Date_Of_Birth : 27.10.1990
Age : 24
Gender : male
Address : 233/1,ramana street

Figure 2

In comparison to other visual recognition techniques, the iris has a great advantage in that there is huge variability of the pattern between individuals, meaning that large databases can be searched without finding any false matches [1]. This means that iris can be used to identify individuals rather than just confirm their given identity; a property that would be useful in a situation such as border control, where it might be important to not just show that an individual is not who they say they are but also to show exactly who they are.If the person is unauthorized to a certain sector then his/her databases never shown . This is mainly used for security purpose so that only authorized person can access into that certain sector.

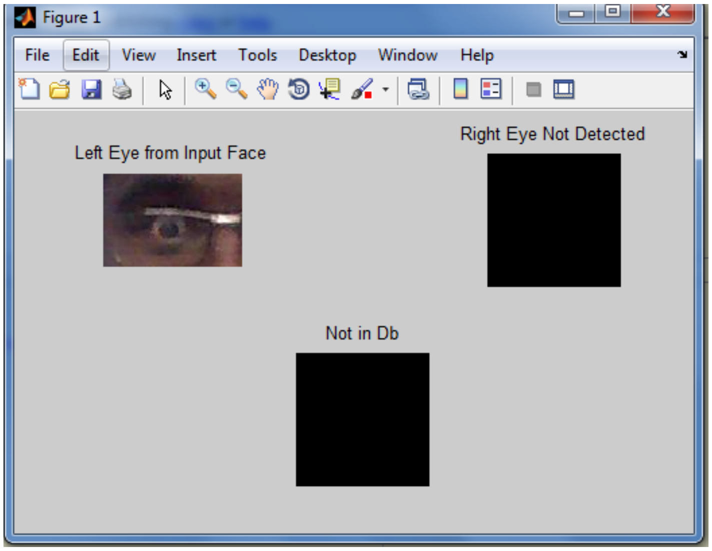

Figure:3

VII.CONCLUSION:

This paper presented the iris features are extracted using the oriented separable wavelet transforms (direction lets) and they are compared in terms of a weighted Hamming distance. The feature extraction and comparison are shift-, size- and rotation-invariant to the location of iris in the acquired image. The generated iris code is binary, whose length is fixed (and therefore commensurable), independent of the iris image, and comparatively short. The novel method shows a good performance when applied to a large database of irises and provides reliable identification and verification. At the same time, it preserves conceptual and computational simplicity and allows for a quick analysis and comparison of iris samples.

The system presented in this paper is able to perform accurately, however there are still a number of issues which need to be addressed. First of all, the automatic segmentation was not perfect, since it could not successfully segment the iris regions for all of the eye images in the two databases. In order to improve the automatic segmentation algorithm, a more elaborate eyelid and eyelash detection system could be implemented. An improvement could also be made in the speed of the system. The most computation intensive stages include performing the Hough Transform, and calculating Hamming distance values between templates to search ®for a match. Since the system is implemented in MATLAB interpreted language, speed benefits could be made by implementing computationally intensive parts in C or C++.

REFERENCES:

[1] A. Ahmed and I. Traore, "A New Biometric Technology Based on Mouse Dynamics," IEEE Trans. Dependable and Secure Computing, vol. 4, no. 3, pp. 165-179, July/Sept. 2007.

[2] T. Boult, "Robust Distance Measures for Face-Recognition Supporting Revocable Biometric Tokens," Proc. Seventh Int'l Conf. Automatic Face and Gesture Recognition, pp. 560-566, Apr. 2006.

[3] T. Boult, W. Scheirer, and R. Woodworth, "Revocable Fingerprint Biotokens: Accuracy and Security Analysis," Proc. IEEE Conf. Computer Vision and Pattern Recognition, pp. 1-8, June 2007.

[4] X. Boyen, "Reusable Cryptographic Fuzzy Extractors," Proc. 11th ACM Conf. Computer and Comm. Security (CCS '04), pp. 82-91, 2004.

[5] J. Bringer, H. Chabanne, G. Cohen, B. Kindarji, and G. Zemor, "Theoretical and Practical Boundaries of Binary Secure Sketches," IEEE Trans. Information Forensics and Security, vol. 3, no. 4, pp. 673-683, Dec. 2008.

[6] I. Buhan, J. Breebaart, J. Guajardo, K. de Groot, E. Kelkboom, and T. Akkermans, "A Quantitative Analysis of Indistinguishability for a Continuous Domain Biometric Cryptosystem," Proc. 4th Int'l Workshop, and Second Int'l Conf. Data Privacy Management and Autonomous Spontaneous Security, pp. 78-92, 2010.

[7] I. Buhan, J. Doumen, P. Hartel, and R. Veldhuis, "Constructing Practical Fuzzy Extractors Using QIM," Technical Report TR- CTIT-07-52 2007.

[8] R. Cappelli, A. Lumini, D. Maio, and D. Maltoni, "Fingerprint Image Reconstruction from Standard Templates," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 29, no. 9, pp. 1489-1503, Sept. 2007

BIOGRAPHY

I am G.VITHYA.i was born in krishnagiri on 27th october 1991 and i received my B.E degree in Electronics and Communication Engineering from Sengunthar college of engineering.i am currently doing my M.E degree in Communication Systems from Mahendra engineering college(Autonomous),Mahendrauri..My research interest include Iris Recognition and Visual Cryptography Technique.