VC of IRIS Images for ATM Banking

S. Koteswari
Associate Professor,
Department of ECE ,
D.N.R Engineering College,Bhimavaram,W.G.Dist, Andhra Pradesh. India.

P. John Paul
PhD, Professor, Dept of CSE,GATES Engineering College,Gooty, Ananthapur,Andhra Pradesh, India.

S. Indrani
Assistant professor
Dept of CSE , S.R.N. Adarsh College, Bangalore, India.

ABSTRACT
It is of great importance over a past few years, the increasing concern to preserve the privacy of biometric data over personal information that is stored in computer systems. It mostly has increased interest in data security. For possible use in biometric identification and protection, in this paper it applies visual cryptography(VC) which is a perfectly secured method of maintaining image security. The basic concept of visual cryptography is to divide secret images in to random shares using key and decryption is performed by superimposing the shares using the similar key which is used at encryption side. In this process it required special software for cryptographic computations and in this paper it is implemented using mat lab 7.9.A modified version of pixel sieve method is proposed in this paper for iris images to achieve more security than existing pixel sieve method. It is the modified version of pixel and is based on key shifting scheme. The simulations results show that the quality of the encrypted and decrypted images is better than existing pixel sieve method.

Key words
Visual Cryptography (VC), Iris image, DCT, DHT, key shifting, encryption, decryption.

1. INTRODUCTION
Security of data has been a major issue from many years. Using the age old technique of encryption and decryption has been easy to track for people around. Providing security to data using new technique is the need of the hour. This project uses the technique of Visual cryptography and providing biometric authentication. Thus using the above technique, recursive visual cryptography would be implemented. As computing power becomes more and more fast, our older cryptographic systems becoming less secure because an attacker can attempt larger number of random attack attempts in shorter time. Hence, there is the need for security of biometrics in which information security is one of the most important issues in growing information technology environment. The need for very efficient security systems for preventing confidential information from being accessed by unauthorized persons is achieved through this paper. Our approach is presented for iris images and it can also applicable to other biometrics such as facial images, using grayscale and natural images such as face, pictures, fingerprint images using more biometric samples into meaningful shares in an authentication security system[2,3]. The results are shown clearly in this paper.

2. VISUAL CRYPTOGRAGHY
Visual Cryptography(VC) and biometrics have been identified as the two most important aspects of digital security. In this paper, we proposed a new method for the preparation and secure transmission of iris images using VC schemes. It allows confidential messages to be encrypted in to k-out –of-n secret sharing schemes. In 1995 Naor and Shamir[4] have suggested for the first time to solve the secret sharing problem by the means of new cryptographic structure called Visual Cryptography(VC).In the proposed approach the secret is divided in to two shares, which are printed on to the two transparencies and can reconstruct the secret by superposition of shares. And one important issue over here is one cannot recover a secret without the other one. In Shifting of key of pixel sieve method[11] each pixel of the key sieve encrypts only the corresponding pixel in the original image. Encryption and decryption process of other pixels are not effected by the any pixel of the key. Hence, if we use a key with some incorrect pixels to decrypt then, only corresponding pixels will be decrypted incorrectly while other pixels are decrypted successfully. To remove this problem key shifting method is proposed.

3. PROPOSED METHOD
As protecting template in the database securely is one of the challenges in any biometric system. Here visual cryptography technique is applied to iris authentication system. In this system there are two modules: Enrollment module and Authentication module. For accessing any secure resource by authenticated users this system can be used especially for ATM (automatic Teller Machine) banking.

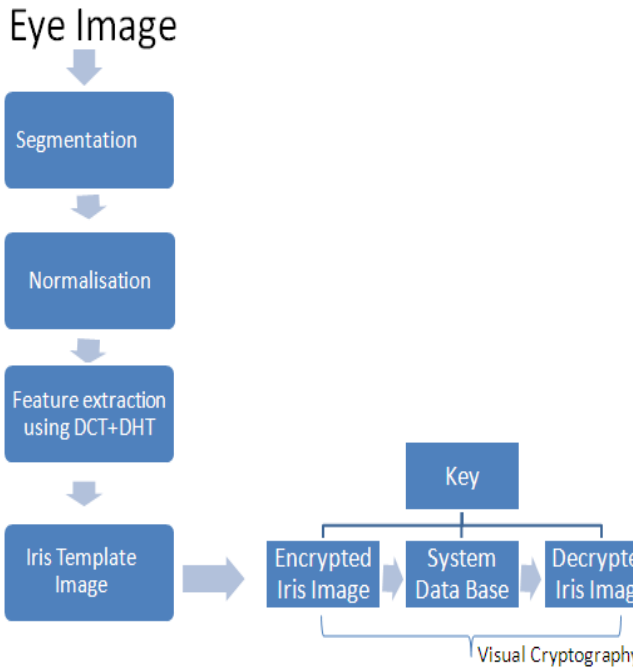

Figure 1: Iris Enrollment module

In Iris Enrollment modules shown in the figure 1, the eye image which need to be stored in the data base for ATM banking is given as the input to the processing section as shown in the figure of the eligible users those are having access to secure resource. The enrolled eye image is required to be processed so characteristic iris features can be extracted using the hybrid transform(DCT+DHT), for this purpose algorithms are developed . Three steps are involved ,that are: segmentation, normalization, and feature extraction[11] are performed as conferred below. further for the security of the data base of iris images the visual cryptography is adopted.

3.1 Segmentation

It is performed to extract the iris from the eye image. By employing circular Hough transform boundary of iris is searched. By fitting two lines using the linear Hough Transform eyelids are detected and eyelash is separated by threshold technique.

3.2 Normalization

The normalization of iris region is carried out using Daugman's rubber sheet model. This model re-maps each pixel within the iris region to a pair of polar co-ordinates. The center of the pupil is considered as the reference point and the radial vectors circle through the iris region.

3.3 Feature Extraction

It is responsible for extracting the patterns of the iris, taking into account the correlation between adjacent pixels. After performing lots of research and analysis about this topic, we decided to use Hybrid transform, and more specifically the "DCT+DHT Transform".

3.4 Hybrid Transform

Using the DCT, an algorithm is proposed[1] to extract distinctive features from the iris image, where in the iris images used in this study were obtained from the CASIA database (version 2.0). This database contains 1200 iris images. The images are of 30 persons. For each person, 20 iris images were captured for the left eye and another 20 images for the right eye giving total of 40 images for each person. The original size of each image is 320x280 pixels, with 256 grey levels per pixel.

The DCT equation (1) computes the i[th] and j[th] entry of the DCT of an image.

$$D(i,j)=\frac{1}{\sqrt{2N}}C(i)C(j)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}p(x,y)\cos\left[\frac{(2x+1)i\pi}{2N}\right]\cos\left[\frac{(2y+1)j\pi}{2N}\right] \quad (1)$$

$$C(u)=\begin{cases}\frac{1}{\sqrt{2}} & if\ u=0\\ 1 & if\ u>0\end{cases} \quad (2)$$

The DCT decomposes a signal into its elementary frequency components. When applied to a mxn image/matrix, the 2D-DCT compresses all the energy/information of the image and concentrates it in a few coefficients which are located in the upper-left corner of the resulting real-valued mxn DCT or frequency matrix[6].

DHT (Discrete Hartley Transform):

The Discrete Hartley transform has the advantage of solving the problem of phase wrapping from which the Fourier transform suffers. The magnitude and phase compression using this transformation (DHT) have proved better performance than those of the Fourier Transform. Magnitude and phase were processed separately. The quantization of frequency samples in fewer bits has increased the compression ratio. Furthermore, the distributions used to generate the noise significantly influence the result .A nonlinear filter for smoothing the resulting image would be suitable for image enhancement. The Discrete Hartley Transform (DHT) is defined as [7]

$$H(k\Omega_v)=\frac{1}{\sqrt{N}}\sum_{n=0}^{N-1}h(nT)cas(k\Omega_v nT) \quad (3)$$

The inverse DHT is

$$h(nT)=\frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}H(k\Omega_v)cas(k\Omega_v nT) \quad (4)$$

3.4.1Combined Discrete Hartley and Discrete Cosine Transform DCT_DHT:

The relationship between the DHT and DCT coefficients can be brought from the fundamental equations. Using eq (1) and eq. (3) the Hartley transform can be expressed in terms of cosine transform as

$$H(k/2)=\frac{D(i,j)}{\sqrt{2N}C_iC_j} \quad (5)$$

Finally the binary image template formed using energies in DCT-DHT domain.

3.5Matching algorithm:

The matching algorithm consists of all the image processing steps that are carried out at the time of enrolling the encoded iris template in database. User also needs to input the same password to form user key (K). Once the bit encrypted bit pattern B' corresponding to binary image formed is extracted, by using simple Boolean XOR operation it is tried to match with all stored encrypted bit patterns B. By using Hamming Distance (HD), the dissimilarity measure between any two iris bit patterns is computed and which is given as

$$HD = \frac{1}{N_l} \sum_{l=1}^{N_l} X_l (XOR) Y_l \quad (6)$$

Where, Nl =total number of bits in each bit pattern. As HD is a fractional measure of dissimilarity with 0 representing a perfect match, a low normalized HD implies strong similarity of iris codes.

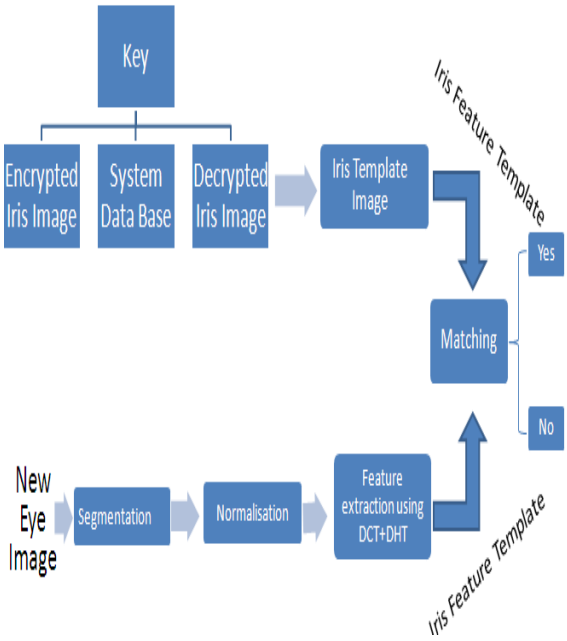

Figure 2: Iris Authentication module

In Iris Authentication module the reverse operation to that of enrollment module is performed as shown in figure 2.And the results are shown in figures below.

4. EXPERIMENTAL RESULTS

4.1 Simulation Results:

To test the method a small software application is written in MATLAB 7.9. This application contains minimum tools to test the both proposed schemes.The resultant in obtained on the screen as shown in figure 3.

The process that actually happens:

1.Generate the key using generate key button. The key is generated randomly for testing purposes. As shown in figure below

2.An iris image which is obtained from the hybrid transform is loaded for encryption by using encryption button. And after the encryption , the image is displayed and stored.

3.For retrieving the original image decrypted button is used and the original iris image is produced , after the decryption process and is stored as shown in figure below.

4.Key at the encryption end and at the decryption end must be the same and if the key varies at encryption and decryption end the original image cannot be retrieved. The results in MATLAB as shown in figures below. These figures represent the process that actually happens on running the test program.

Figure 3: Result of VC in MATLAB 7.9

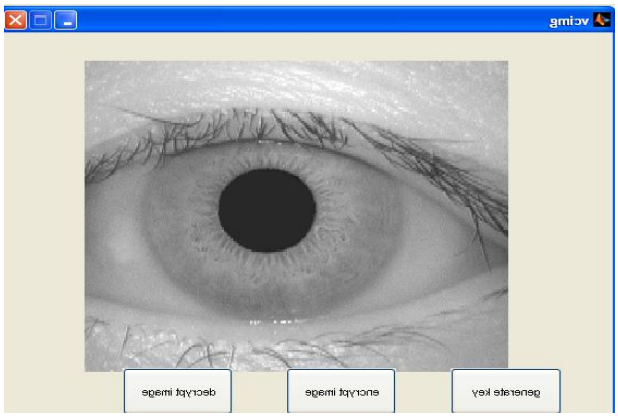

Figure 4: The iris image on which VC is performed

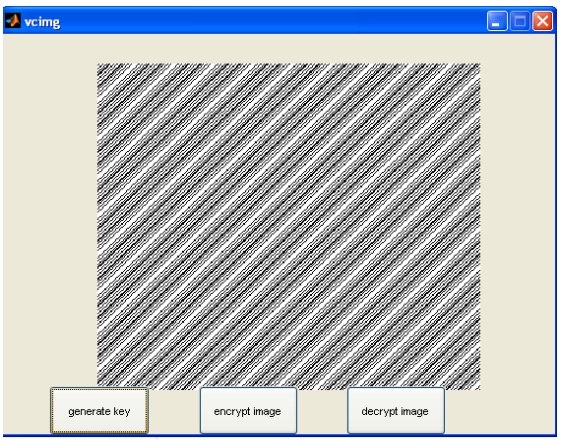

Figure 5: Generated key

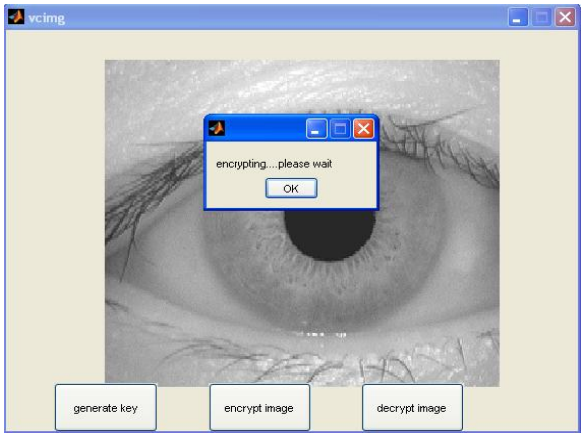

Figure 6: Encrypting the iris image

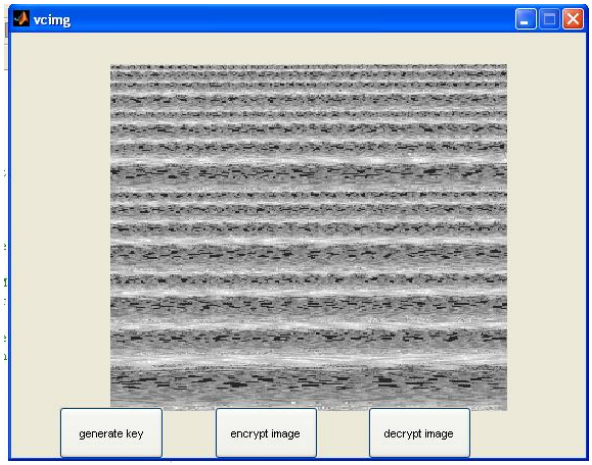

Figure:7 Encrypted Image of Iris

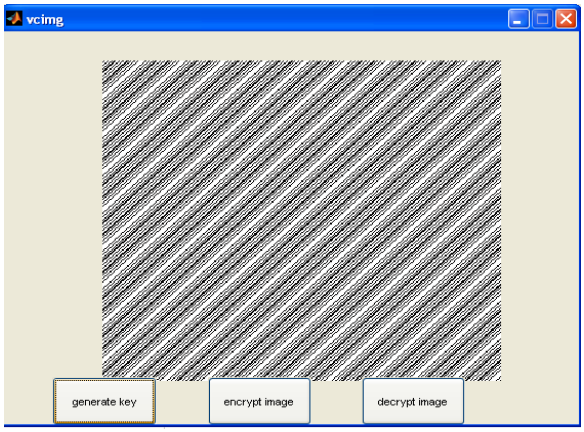

Figure 8:Key for Decryption

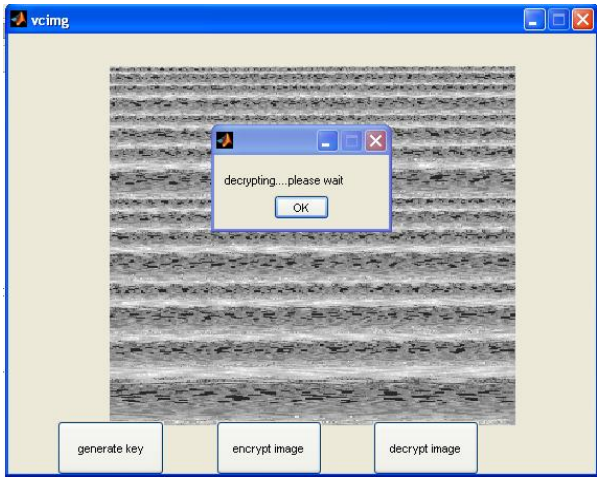

Figure 9: Decrypting the Iris image

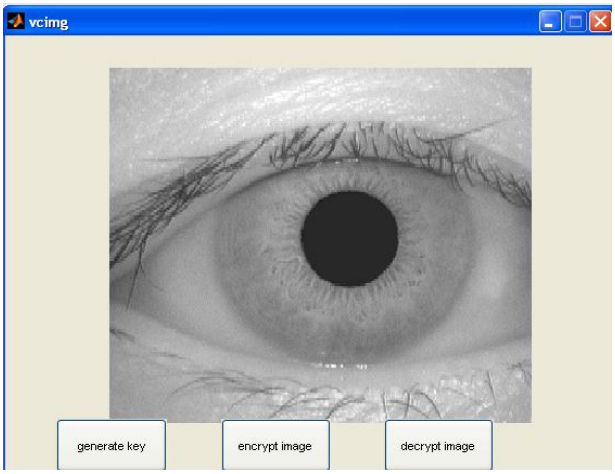

Figure 10: Image after decryption

4.2 Synthesis Results:

. Synthesis results are implemented on Xilinx FPGA platform and the device is 6vlx75tff484-3. Table 1 represents the comparison results of DHT and DCT[15]. Table 2 results represents the results obtained by using the feature extraction using DCT_DHT it is the device utilization summary.

Table 1: Comparison of DHT and DCT in [15]

scheme	Adder matrix	Adder bit-width
DCT	9 ALU +6	850
Proposed DHT	4 ALU +7	452

Table 2. Comparision of DCT_DHT(device utilization summary)

Logic utilization	Used	Available	Utilization
Number of slice registers	566	93120	0%
Number of slice LUTs	1589	46560	3%
Number of fully used LUT-FF pairs	402	1753	22%
Number of bonded IOBs	786	240	327%
Number of BUFG/BUFGCTRLs	1	32	3%

The below table 3 represents the final register report

Table 3. Final register report

Macro statistics	No's
Registers	506
flip-flops	506
Shift registers	27
4-bit shift registers	27

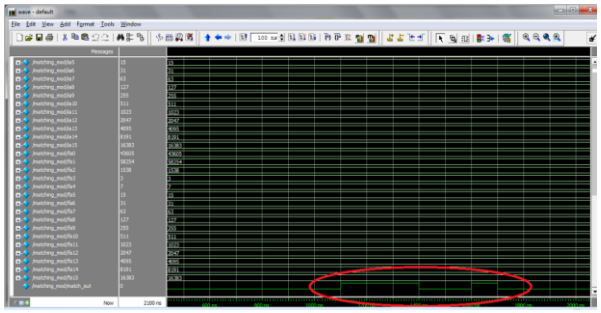

Figure 11: Hardware result implementation of top module

5. CONCLUSIONS

We have successfully developed a new Iris Recognition system using hybrid transform (DCT_DHT) capable of comparing two digital eye-images. For the protection of data bases for ATM banking, Visual cryptography (VC) for iris images is developed in MATLAB 7.9.the synthesis results are obtained using xilinx FPGA platform. This identification system is quite simple requiring few components and is effective enough to be integrated within security systems that require an identity check. The errors that occurred can be easily overcome by the use of stable equipment. Judging by the clear distinctiveness of the iris patterns we can expect iris recognition systems to become the leading technology in identity verification in ATM banking

6. REFERENCES

[1] Daugman, J., "Complete Discrete 2-D Gabor Transforms by Neural Networks for Image Analysis and Compression", IEEE Transactions on Acoustics, Speech, and Signal Processing, Vol. 36, no. 7, July 1988, pp. 1169-1179

[2] Daugman, J. "How Iris Recognition Works", available at http://www.ncits.org/tc_home/m1htm/docs/m1020044.pdf.

[3] Daugman, J., "High Confidence Visual Recognition of Persons by a Test of Statistical Independence,"IEEE transactions on pattern analysis and machine intelligence, vol. 15, no.11, November 1993, pp. 1148-1161.

[4]. An improved pixel sieve method for visual cryptography by vaibhav choudhary et al.

[5] Biometric data security using recursive visual cryptography,by lakshmi madhuri.K et al

[6] Gonzalez, R.C., Woods, R.E, *Digital Image Processing*, 2rd ed., Prentice Hall (2002).

[7] Lim, S., Lee, K., Byeon, O., Kim, T, "Efficient Iris Recognition through Improvement of Feature Vector and Classifier", ETRI Journal, Volume 23, Number 2, June 2001, pp. 61-70.

[8] C.H Daouk,F.D. Kammoun"Iris Recognition", IEEE ISSPIT 2002,pp.558-562

[9]P.John Paul , P.N.Girija, "A High Performance Novel Image Compression Technique using Hybrid Transform for Multimedia Applications" IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.4, April 2011.pp119-125

[10] Wildes, R.P, "Iris Recogntion: An Emerging Biometric Technology", Proceedings of the IEEE, VOL. 85, NO. 9, September 1997, pp. 1348-1363

[11] Moni Naor and Adi Shamir. Visual Cryptography, EUROCRYPT 1994, ppl- 12.

[12] Shamir, Adi. "How to share a secret". Communications of the ACM 22 (II): 1979,6 12-613.

[13] A.Incze, "Pixel Sieve method for secret sharing & visual cryptography". 9th RoEduNet IEEE International Conference 2010.

[14]P.S.Revenkar, Anisa Anjum, W .Z.Gandhare. " Survey of Visual Cryptography Schemes ". International Journal of Securityand Its Applications ,Vol. 4, No. 2, April, 2010.

[15]Peng Chungan, Cao Xixin, Yu Dunshan, Zhang Xing, "A 250MHz optimized distributed architecture of 2D 8x8 DCT," *7th International Conference on ASIC*, pp. 189 – 192, Oct. 2007.