Secured Biometric Authentication using Visual Cryptography and Transforms

Priya Pradeep Bhirud
M.E. Computer Engineering Department
K.J.Somaiya College of Engineering, Mumbai
Mumbai University, India.

Nandana Prabhu
Information Technology Department
K.J.Somaiya College of Engineering, Mumbai
Mumbai University, India.

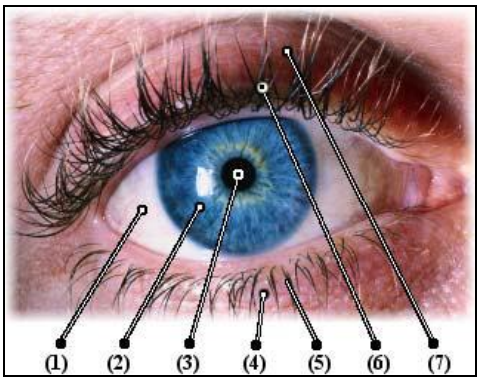
ABSTRACT
Protection of biometric data is gaining importance because its uniqueness and digital watermarking techniques are used to protect the biometric data from either accidental or intentional attacks. Here introduces a novel secured authentication method using wavelet decomposition and Visual Cryptography to hide an iris image.

In this report gives exhaustive study on a scheme in which iris image is secured by using a technique called Visual Cryptography (VC). In this technique, iris image is embedded in cover image and then using wavelet transform this output image is decomposed into four shares. These four shares are compressed at sender site. At receiver side, to obtain original iris image inverse DWT is obtained and finally bit matching procedure has been applied. The result shows that Stegnography and Visual cryptography implementation on biometrics, secures Iris and related textual information from getting identity forged. In comparison with existing approach quality of final watermarked cover images and Iris has been maintained which could be used for matching of it for authentication. Along with quality, goal of higher security and bandwidth reduction by reducing size of shares is achieved. Also technique of three least significant bits applied successfully that allows secret message of increased length by maintaining quality of Iris.

Keywords
Selected Least Significant Bit (SLSB) Method, LSB, Visual Cryptography, Wavelet Decomposition

1. INTRODUCTION
Biometrics deal with automated methods of identifying a person or verifying the identity of a person based on physiological or behavioural characteristics. Biometrics systems are more consistent and more user friendly. Commonly used biometric features are facial features, fingerprints, voice, facial thermo grams, Iris, posture/gait, palm print, hand geometry etc.

If comparison is made with other biometric characteristics iris is the most stable and hence the most reliable biometric characteristic over the period of a lifetime.



Due to the vibrant colour and texture of the iris it is typically the most visible and distinguishable part of the human eye.

Human eye shows (1) is sclera, (2) iris, (3) pupil, (5, 6) eyelashes and (4, 7) eyelids.

Still there are certain issues particularly the security facet of both biometric system and biometric data. As biometric template are stored in the database, due to security threats biometric template may be altered by attacker. If biometric template is altered authorized user will not be allowed to access the resource. For these reasons various researches have been made to protect the biometric data and template in the system by using cryptography, stenography and watermarking. Visual cryptography is one of the techniques among them. 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. Visual cryptography provides great means for helping such security needs as well as extra layer of authentication.

1.1Organization of Paper
The paper is organized as follows: section 2 discusses literature survey along with proposed system. Section 3 presents investigations on proposed system done and also requirements of system. Section 4 Practical results and discussion, analysis of results. Section 5 concludes work carried out. Section 6 indicated future work to be carried out. Section 7 represents references of papers and websites used.

2. LITERATURE SURVEY
2.1. Cryptography

Cryptography, deals with the development of techniques for converting information between intelligible and unintelligible

forms during information exchange that deals with the content confidentiality and access control. By using cryptography, only authorized parties holding decryption keys can access the content (text or image). **Cryptanalysis** is the term used for the study of methods for obtaining the meaning of encrypted information without access to the key It is the study of how to crack encryption algorithms or their implementations.

Cryptography systems can be broadly classified into **symmetric-key** systems that use a Single key (i.e., a password) shared by both the sender and the receiver Public-key systems uses two keys, a public key known to everyone and a private key is associated only with the recipient of messages. Study of methods for decrypting cipher messages and detecting hide messages are called cryptanalysis.

Symmetric-key cryptography

Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key (and, less commonly, in which their keys are different, but related in an easily computable way).Only one kind of encryption i.e. symmetric key encryption was publicly known until June 1976. Symmetric key ciphers are implemented as either block ciphers or stream ciphers. A **block cipher** encrypts input in blocks of plaintext. Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) are block cipher designs which have been designated cryptography standards by the US government block ciphers have been designed and released, with considerable variation in quality [20]. **Stream ciphers**, create an arbitrarily long stream of key , which is combined with the plaintext bit-by-bit or character-by-character, like the one-time pad. In a stream cipher, the output stream is created based on a hidden internal state which changes as the cipher operates. That internal state is initially set up using the secret key material. RC4 is a widely used stream cipher.

The third cryptographic algorithm uses hash function. It can take an input message of variable length, and generates a short, fixed length hash output which can be used for a digital signature. For good hash functions, an attacker cannot find two messages that produce the same hash. MD4, MD5 also widely used but broken in practice. SHA-1 is widely deployed and more secure than MD5, hash function design competition is underway and meant to select a new U.S. national standard, to be called SHA-3,by2012.[20].Message authentication codes (MACs) are like cryptographic hash functions, but in MAC on a secret key can be used to authenticate the hash value upon receipt.

Public-key cryptography

Symmetric-key cryptosystems use the same key for encryption and decryption of a message, though a message or group of messages may have a different key than others. A significant disadvantage of symmetric ciphers is the key management necessary to use them securely. Each distinct pair of communicating parties, share a different keys (private and public). The number of keys required increases as the square of the number of network members, which very quickly requires complex key management schemes to keep them all straight and secret.

2.2 Watermarking System

During embedding process, an algorithm accepts the host and the data to be embedded and produces a watermarked signal [9]. The extraction or detection algorithm is used to extract the hidden watermark from the transmitted image. The watermarking schemes are generally classified into robust watermarking schemes and fragile watermarking schemes. Both the schemes are designed for different applications. Among them, robust watermarks are generally used for copyright protection and ownership identification because they are designed to withstand attacks such as common image processing operations. In contrast, fragile watermarks are mainly applied to content authentication and integrity attestation because they are fragile to attacks, i.e., it can detect any changes in an image as well as localizing the areas that have been changed. In robust watermarking applications, the extraction algorithm should be able to correctly produce the watermark, even if the modifications were strong. In fragile watermarking, the extraction algorithm should fail if any change is made to the signal [20].

2.3 Visual Cryptography

Naor and Shamir have suggested for the first time to solve the secret sharing problem by the means of new cryptographic structure called Visual Cryptography (VC) in 1995. In the proposed approach the secret is divided into two shares, which are printed onto the two transparencies (shares) and given to the participants. Only these two participants who possess the transparencies can reconstruct the secret by superposition of shares. One cannot recover a secret without the other one. In the visual threshold scheme, the shares are images represented on transparencies consisting of black and white (transparent, actually) pixels. The visual systems perform a Boolean operation, which is easy to visualize using the (2, 2) Visual Threshold Scheme. Later in 2001 the engineers from Taiwan have claimed that during the encoding process shares are generated in such a way that they contain random dots to create a chaos for preventing intruders of random guesswork. They propose two algorithms for secret sharing and secret recovery derived from the least significant bit substitution method. Thus generation of shares could be also done using so called cover images. Visual cryptographic has been applied to many applications, including but not restricted to information hiding, general access structures, visual authentication and identification. The solutions normally operate on binary inputs. After its initial introduction, many researchers have found different variations of VC [14]. The improvement varies from binary image to halftone images, gray scale and colour images.

The concept of VC to color images was introduced by Verheul and Tilburg[15]The disadvantage in this was that the quality of the recovered image was poor and the sharing was meaningless. This work motivated several others to produce more advanced schemes ([3], [4], [16]). All these works used techniques where a colored image was hidden into multiple meaningful cover images

2.4 Bit replacement algorithm

The best known stegnographic method that works in the spatial domain is the LSB (Least Significant Bit), which replaces the least significant bit of pixels selected to hide the information [11]. SLSB (Selected Least Significant Bit) improves the performance of the method LSB hiding information by selecting only one of the three colours at each pixel of the cover image to hide the message. The algorithm chooses green colour pixels and uses the two LSBs of the pixel to store the secret message. A colour image is made of three planes, namely, red, green and blue. In HSV, blue planes

appear dark, red plane appear over bright and therefore green planes are chosen for embedding.[5]

3. METHODOLOGY

This section presents methodology for proposed system implementation .Along with that, it also provides results obtained and analysed from implementation of module 1 and module 2, module 3. From the results, it is analysed that DWT HAAR Filter gives good results so that can be used for biometric which is to be embedded in cover image.

MODULE 1: Cover image and Iris Image read and Secret Message Representation.
This module is designed to read Cover and Biometric image and display the image. According to the RGB scheme, Ri, j , Gi, j and Bi, j are all integers in the range (0,255) and correspond to the pixel Pi, j.

MODULE 2: Iris analysis
Iris image is analysed to extract its features. First Iris is converted from RGB to Gray scale Image. Using Morphological Structuring
create shape of Iris in image. Dilate Image to convert pixels obtained from previous 0(black) and 1(white) pixel. Then Pupil detection is carried out.

MODULE 3: DWT Transform is carried out. By using this wavelet transform no. of pixels used to represent iris image is reduced. Wavelet transform has been used to form four sub bands of Iris image namely HH, HL, LH, LL .Among them HH is to selected as it has maximum information .This HH sub band has been compared with gray scale Iris image in terms of parameter such as no. of pixels required to represent image. Iris image which is to be embed in cover image for security will be decomposed by wavelet transform using various filters like Daubechies Orthogonal filter, HAAR filter and Biorthogonal filter using DWT. For performance evaluation Comparison of Gray scale Iris image with wavelet decomposed Iris is performed. This comparison will be carried out on basis of two parameters

1. Number of pixels
2. PSNR (peak signal to noise ratio)

MODULE 4: Bit Replacement Procedure
Each cover pixel is divided into two bits strings .Most Significant Bits (MSB) and Least Significant Bits (LSB) and bit replacement process is carried out accordingly to obtain stegnographic image. Now biometric is embedded in this stegnographic images by watermarking procedure and compressed using JPEG compression.DWT Transform is applied to watermark Image and is decomposed into four bands. It is then sent to receiver.

MODULE 5: Final Output
At receiver side, IDWT is carried out to merge all shares. Decompression is carried out. This image is then dewatermarked to obtain iris image. The results are projected in terms of MSE and PSNR of the cover image before and after jpeg compression.
Also comparison is made of the cover image after watermarking and before watermarking for various transforms like Discrete Cosine Transform and Fast Walsh Hadamard transform.

4. PRACTICAL RESULTS AND DISCUSSION

This section presents provides results and analysis from final outputs obtained after implementation of all modules. In terms of PSNR.
From the results of implemented modules i.e. module 1, 2, 3, we have concluded that among various Transforms like Hadamard, Discrete Cosine Transform and Discrete Wavelet Transform, DWT with Haar filter provides average value of PSNR with less number of pixels. Considering this result further work of Implementation of Stegnography and Watermarking is carried out with the various variations in parameters like levels of DWT, resize of iris and compression of final image.

Table 5.1 shows results with Filters of Discrete Wavelet Transform with compression and resize factor**.**

Table5.1

Sample databases		**Discrete Wavelet transform**					
		HAAR Filter (PSNR)		**Daubechies Orthogonal Filter (PSNR)**		**Biorthogonal Filter (PSNR)**	
		Iris Image	Cover Image	Iris Image	Cover Image	Iris Image	Cover Image
Kenkare Iris		30.1354	0.3805	27.2213	0.3226	31.2354	0.3227
Kenkare Iris		29.9734	0.3805	27.0849	0.3226	31.3400	0.4563
Phoenix	Left Iris	31.0344	0.4123	27.4023	0.4849	30.8745	0.3376
	Right Iris	31.0555	0.4757	27.0964	0.3226	31.5643	0.3200
Phoenix	Left Iris	31.0455	0.4727	27.6319	0.3221	31.0032	0.3226
	Right Iris	30.0555	0.4752	27.6974	0.3200	30.6534	0.3123

Four Level DWT with Resize and Compression

Also this proposed work has been carried out with Discrete cosine transform and Hadamard transform as shown in following table 5.2.

Table5.2

Sample databases		**Discrete Cosine Transform (PSNR)**		**Fast Walsh Hadamard Transform (PSNR)**		**Discrete Wavelet Transform (HAAR) (PSNR)**	
		Iris Image	Cover Image	Iris Image	Cover Image	Iris Image	Cover Image
Kenkare Iris		1.5893	0.2438	2.2024	0.4780	31.2354	0.3805
Kenkare Iris		1.6909	0.2525	2.2024	0.4780	31.3400	0.3805
Phoenix	Left Iris	1.1666	0.2440	2.2024	30.8745	30.8745	0.4123
	Right Iris	0.1904	0.4783	2.2024	31.5643	31.5643	0.4752
Phoenix	Left Iris	0.1904	0.4783	2.2124	31.0032	31.0032	0.4757
	Right Iris	1.2024	0.4783	2.2013	30.6534	30.6534	0.4752

Comparison : HAAR Vs Resize and compression with DCT and Hadamard Transform

Above results shows that only DCT and Hadamard Transformation cannot give good results for Iris as well as cover Image .With DWT quality of iris is maintained, but with compression it gives very poor results for cover image so we will move on with results of DWT with variations in parameters of comparison. The results for 5.1 shows that, four level DWT(HAAR) and resize of iris image and compression provides higher PSNR as compared to DWT(Daubechies filter) i.e. Quality of Iris is maintained. With compression Bandwidth reduction has been achieved but cover image quality is not maintained which is desired in the security issues. So further it's carried out with two levels DWT with compression and without compression as shown in following tables 5.3 and 5.4.
Following table 5.3 represents results after two levels DWT with resize and Compression.

Sample databases		**Discrete Wavelet Transform**	
		HAAR Filter(PSNR) *(2L Decomposition)*	
		Iris Image	Cover Image
Kenkare Iris		29.1754	0.4811
Kenkare Iris		29.1654	0.4616
Phoenix	Left Iris	39.8588	0.4805
	Right Iris	39.4816	0.4814
Phoenix	Left Iris	39.1816	0.4813
	Right Iris	39.0816	0.4813

Table 5.3

Two Level DWT with Resize and Compression

With the variation in decomposition level up to second level increases quality of Iris image but cover image quality is still poor which is not desirable. To maintain quality of Iris and Cover Image Compression parameter is removed and with two levels of decomposition and resize of iris image results are obtained as shown in table 5.4

Table 5.4

Sample databases		**Discrete Wavelet Transform**	
		HAAR Filter(PSNR) *(2L Decomposition)*	
		Iris Image	Cover Image
Kenkare Iris		29.1754	39.4811
Kenkare Iris		29.1654	39.4616
Phoenix	Left Iris	39.8588	53.4805
	Right Iris	39.4816	53.4814
Phoenix	Left Iris	39.1816	53.4831
	Right Iris	39.0816	53.4831

Two level DWT with Resize, No compression

Above results shows that by removing just compression parameter it's possible to maintain quality of both Iris and cover image, but final image may become bulky thereby increasing the bandwidth**.** Finally method of no Compression, No DWT and No Resize parameters is tested and following results are obtained this gives good results but larger bandwidth**.**

Table 5.5

Sample databases		**PSNR**	
		Iris Image	Cover Image
Kenkare Iris		28.9125	39.4811
Kenkare Iris		28.8965	39.4816
Phoenix	Left Iris	32.0476	39.8588
	Right Iris	31.4288	39.4816
Phoenix	Left Iris	32.9304	39.1816
	Right Iris	31.6275	39.0816

No DWT No Compression No Resize

Because of requirement of more bandwidth this method is discarded, as with quality reduced bandwidth requirement is desired. So best method among all by considering all results obtained proves that best quality of Iris and cover image with reduced bandwidth can be obtained using two levels DWT, resize but without compression of final image. In the proposed work for Stegnography process selected least significant bits i.e. two least significant bits are used for replacement with secret message. Similar process of Stegnography is carried out with three least significant bits .Following table 5.6 shows result for this method.

Table5.6

Sample databases		**Discrete Wavelet Transform(PSNR)**	
		Iris Image	Cover Image
Kenkare Iris		31.6851	31.4054
Kenkare Iris		31.1567	31.5045
Phoenix	Left Iris	28.9968	31.8588
	Right Iris	28.9100	31.4816
Phoenix	Left Iris	28.1567	31.1816
	Right Iris	28.6523	31.0816

Results with Three Least significant bit Replacement with two levels DWT, resize

From the above results it can be concluded that even if we replace three least significant bits for Stegnography, quality of Iris image is still retained however cover image quality is slightly reduced but acceptable. So this three least significant bit replacement with two levels of DWT with Resize is ideal method for providing security to biometric i.e. Iris in this case**.**

5. CONCLUSION

In the present work, the biometric image is embedded in cover image and secured with Visual Cryptography. The originality of the scheme is to use wavelet decomposition and use the sub bands as share images. To begin with Stegnography is implemented for embedding secret message inside cover image using Three Least Significant bits instead of SLSB(Two Least Significant bits) .

From the work that has been accomplished, it is observed that, using various filters for wavelet transforms, images of different size are obtained. Moreover we get images with number of pixels reduced as compared to original iris image, while maintaining quality of image using HAAR transform. With reference to these results final procedure of Stegnography and watermarking is implemented by considering various parameters like compression, Decomposition levels and Size of Iris Image, SLSB techniques enhancements. Among all variations of this proposed work, best results with high Quality of Iris and cover image with reduced bandwidth requirement could be obtained with Two Levels of Wavelet Decomposition of Iris with resize without compression of final watermarked image . Along with it Three Least Significant Bit replacement for Stegnography is implemented successfully so that size of secret message to be embedded can be increased, still maintaining quality of iris.

6. FUTURE SCOPE

This system is successfully implemented for Iris security. It was observed that using JPEG compression for reducing bandwidth detoriated the quality of cover image. So to obtain both quality and bandwidth requirements some efficient lossless technique maybe used which will be suitable for all biometrics also.

7. REFERENCES

[1] Mrs.D.Mathivadhani1, Dr.C.Meena,"Biometric based Authentication using Visual cryptography and Wavelet Transform", IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011.978-1-4577-0590-8/11/$26.00 ©2011 IEEE. June 3-5 , 2011

[2] Yunhong Wang, Yong Zhu, Tieniu Tan, "BIOMETRIC PERSONAL IDENTIFICATION BASED ON IRIS PATTERN", ACTA AUTOMATICA SINICA, 2002, 28 (1): 1-10(in Chinese).

[3] Chang, C., Tsai, C. and Chen, T. (2000) A new scheme for sharing secret colour images in computer network, Proceedings of International Conference on Parallel and Distributed Systems, Pp. 21–27.

[4] Chang, C.C. and Yu, T.X. (2002) Sharing a Secret Gray Image in Multiple Images, in the Proceedings of International Symposium on Cyber Worlds: Theories and Practice, Tokyo, Japan, Pp.230-237.

[5] Chang, C.C., Wang, Z.H. and Yin, Z.X. (2009) An Ingenious Data Hiding Scheme for Colour Retinal Image, Proceedings of the Second Symposium International Computer Science and Computational Technology(ISCSCT '09) Huangshan, P. R. China, Pp. 1-6.

[6] Daugman J and Downing C (2001) Epigenetic randomness, complexity, and singularity of human iris patterns, Proceedings of the Royal Society, B, 268, Biological Sciences, Pp 1737 - 1740.

[7] Dharwadkar, N.V., Amberker, B.B. and Joshi, S.R. (2010) Visual Cryptography for Color Image using Color Error Diffusion, ICGST - GVIP Journal, Vol. 10, Issue 1, Pp. 1-8.

[8] Dobes, M. and Machala, L. (2010) Iris Database, http://www.inf.upol.cz/iris.

[9] Hartung, F. and Kutter, M.(1999) Multimedia Watermarking Techniques, Proc. of IEEE, Tutorial, Survey, and Special Issue onData Hiding & Security, pp.1079-1107.

[10] Hou, Y.C. (2003) Visual cryptography for color images, Pattern Recognition, Vol. 36, Issue 7, Pp. 1619-1629

[11] Kurak, C. and McHugh, J. (1992) A Cautionary Note on Image Downgrading, Proceedings of IEEE 8th Annual Computer Security Applications Conference. San Antonio, USA, Pp. 153-155.

[12] Lin, C. (2000) Watermarking and Digital Signature Techniques for Multimedia Authentication and Copyright Protection, PhD Thesis, Columbia University.

[13] Naor, M. and Pinkas, B. (1997) Visual authentication and identification, Advances in Cryptology CRYPTO'97, Lecture Notes in Computer Science, Vol. 1294, Pp. 322–336.

[14] Yang, C.N. (2010) Visual cryptography: An introduction to visual secret sharing schemes, Department of Computer Science and Information Engineering National Dong Hwa University Shoufeng, Hualien 974, TAIWAN, Last accessed on July 04, 2010, http://sna.csie.ndhu.edu.tw/~cnyang/vss/sld001.htm

[15] Verheul, E. and Tilborg, H.V. (1997) Constructions and properties of kout of n visual secret sharing schemes, Designs, Codes and Cryptography, Vol. 11, No. 2, Pp.179-196.

[16] Yang, C. and Laih, C. (2000) New colored visual secret sharing schemes. Designs, Codes and Cryptography, Vol. 20, Pp.325–335.

[17] Youmaran, R., Adler, A., Miri, A., (2006) An Improved Visual Cryptography Scheme For Secret Hiding, 23rd Biennial Symposium on Communications, pp. 340-343

[18] Phoenix library for Iris Images. http://www.phoenix.inf.upol.c/Iris/

[19] Gonzalez Image Processing with matlab codes .Second edition.

[20] Wikipedia http://en.wikipedia.org/wiki/Cryptography

[21] Kekare's database