ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 2, February 2015

VLSI Implementation of Multimodal Biometric Recognition Using Iris Based on Fuzzy

Mr.M.Madhivhanan

PG Scholar,
Department of Electrical and Electronics Engineering,
Arignar Anna Institute of Science and Technology, Chennai
E-mail: madhivhanan@gmail.com

***Abstract*- Iris recognition is an automated method of biometric identification that uses mathematical pattern-recognition techniques on video images of one or both of the irises of an individual's eyes, whose complex random patterns are unique, stable, and can be seen from some distance.. The (n, n)-NVSS scheme shares one secret image over n-1 selected natural images(also called natural shares) and one generated noise-like share. The natural shares may be photos or hand-painted pictures in digital form. The noise-like share is obtained using these natural shares and the digital secret image. The unaltered natural shares are different and not harmful thus reducing the transmission risk problem.**

***Keywords* - Visual secret sharing scheme, noise-like share, natural images**.

I. INTRODUCTION

Retinal scanning is a different, ocular-based biometric technology that uses the unique patterns on a person's retina blood vessels and is often confused with iris recognition. Iris recognition uses video camera technology with subtle near infrared illumination to acquire images of the detail-rich, intricate structures of the iris which are visible externally. Digital templates encoded from these patterns by mathematical and statistical algorithms allow the identification of an individual or someone pretending to be that individual.[1] Databases of enrolled templates are searched by matcher engines at speeds measured in the millions of templates per second per (single-core) CPU, and with remarkably low false match rates. Several hundred millions of persons in several countries around the world have been enrolled in iris recognition systems for convenience purposes such as passport-free automated border-crossings, and some national ID programs. A key advantage of iris recognition, besides its speed of matching and its extreme resistance to false matches is the stability of the iris as an internal and protected, yet externally visible organ of the eye.

Conventional shares have random and meaningless pixels and these shares satisfy the security requirements to protect

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 2, February 2015

the secret contents [3]. But they have two drawbacks: First, they have a high transmission risk because the noise-like share has less display quality and hence make the attackers' suspicion about the secret content [6],[8]. Second is that the meaningless shares are not user friendly. As the number of meaningless noise-like shares increases, it is more difficult to manage the shares. In conventional method, the meaningless shares are obtained by altering the secret image [10]. So the meaningless share can expose the possibility of hidden information. Since the shares contain noise-like pixels, it will be easy to detect the secret by naked eye. Some systems tried to improve the friendliness of VSS schemes for participants but they reduce the display quality of the recovered images [1], [5]. In steganography techniques, the secret image is embedded into cover images. The cover image may be halftone gray images and true-color image. Steganography is concealing the presence of communication by embedding secret image into cover images. Hence the stego-images will be detected by steganalysis methods [7].

In order to reduce the transmission risk, a natural image based (n. n) NVSS scheme is proposed. In this scheme the natural shares are obtained from photographs, hand-painted pictures. The noise-like share is obtained from the features of natural images and the secret image. In the proposed scheme, the secret image is not altered hence it reduces the transmission risk greatly. The alteration is done only on the natural images. Since the proposed scheme only one noise-like share it reduces the transmission risk and also manages the shares easily. The hand-painted pictures can also be used as a natural share [4]. It can be transmitted through different transmission channels (postal, e-mail) so that the transmission risk is reduced further. The proposed scheme not only reduces the transmission risk but also provides user friendliness and manageability. It also enhances the security of participants and the shares.

II. PROPOSED SCHEME

The proposed (n, n) NVSS scheme, $n \geq 2$ shares the secret image using n-1 selected natural images and one generated noise-like share. The objective of this scheme is to reduce pixel expansion, transmission risk of both the participants and the shares and to improve the display quality of recovered image. The natural shares can be any photos or hand painted pictures either in digital form or in printed form. The unaltered natural shares are different and innocuous. The noise-like share is generated based on these natural shares and the secret image. This scheme has two main phases: feature extraction and encryption. In the feature extraction process, the binary feature images are extracted from each natural share. In the encryption process, the n-1 feature images are XOR-ed with the secret image to generate one noise-like share.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 2, February 2015

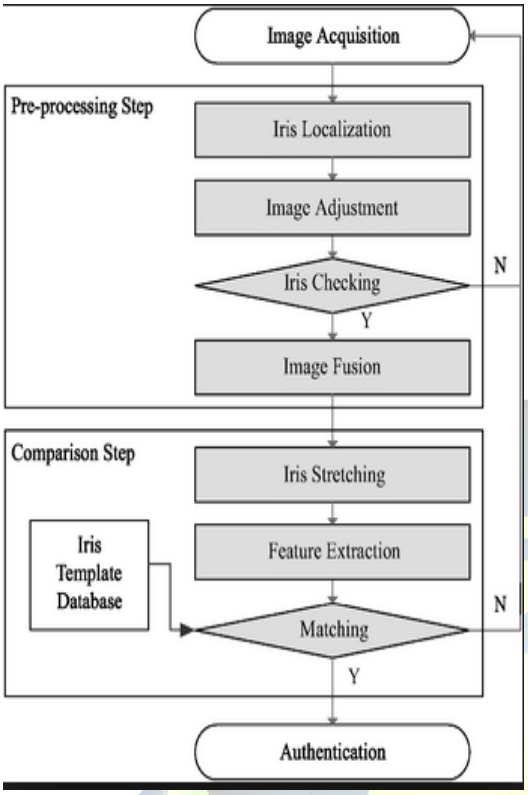


Fig. 1. Flow Diagram of proposed scheme

Here the digital image and the printed image are the natural images. These two images may be of any size. The natural image will be a color image.

A. Preprocessing

In the preprocessing process, printed images are filtered and resized to the size of natural image and the secret image. In this process all the images used are made to the same size. The natural images are divided into the blocks and for each block feature extraction process is performed. Since the natural image is a color image pixel values in each color plane has to be calculated. The pixel value will be the sum of the pixel values in the Red, Green and Blue plane. The pixel value P is calculated by the following expression

$$P = P_R + P_G + P_B \quad (1)$$

Where, P_R, P_G, P_B will be the pixel values in the Red, Green and blue planes respectively.

B. Feature Extraction process

It involves three steps: Binarization, stabilization, chaos. In the binarization process, the binary feature value of a pixel is determined by a simple threshold function F. Median values for each block is found out and set as threshold. The threshold function is found as follows

$$F = \begin{cases} 1, & P \geq M \\ 0, & otherwise \end{cases} \quad (2)$$

where, P is the pixel value and M is the median value.

In the stabilization process, the number of black and number of white pixels are made equal. The unbalanced black pixels are found by

$$S = \sum P - \frac{b^2}{2} \quad (3)$$

Where, b is the block size.

The chaos process is used to eliminate the texture on the extracted feature image. In this process, C number of black and C number of white pixels is selected randomly from each block and then the values of these pixels are changed. In natural images, same or approximately same value may cluster together. These clustered pixels may reveal some textures of the natural image. Hence the pixel values are disordered by

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 2, February 2015

adding noise in the matrix. In this process the clustering of pixels has been reduced. The value of C is obtained as follows

$$C = \frac{b^2}{2} \times P_{noise} \quad (4)$$

Where, P_{noise} is the probability of noise to be added into the matrix. Here the P_{noise} is set to 0.5

C. Encryption / Decryption

In encryption process, the feature image obtained from the natural image and the secret image is XOR-ed. After applying logical XOR, the output image will be t he encrypted image. The decryption process is the reverse of encryption process. In decryption process, the feature image is extracted from the natural shares and then logical XOR is performed to the extracted feature image and the secret image. After the decryption process, the secret image is recovered.

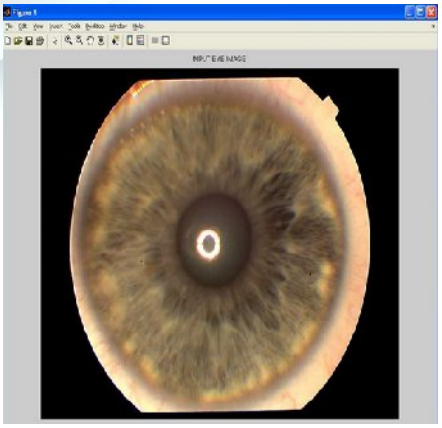
D. Algorithm

Assume that the size of the natural shares and the secret image are w × h pixels and each natural share is divided into a number of b × b pixels before the feature extraction process starts. The pixel value for every block is calculated. Then the median value for each block is calculated separately. The pixels are then converted to the binary values and the white and black pixels are made equal. The pixel values are swapped and circular shift is performed. Then the secret image is XORed with the natural shares. The steps of the (n, n) NVSS scheme are explained below

1. Divide the natural images into b × b pixels.
2. Calculate the pixel values in the natural shares P by eqn (1) and calculate the median M
3. Calculate the threshold function F by eqn (2)
4. Calculate S by eqn (3)
5. Calculate C by eqn (4). Alter the pixel values.
6. Repeat steps 2- 5 for each block.
7. Output feature matrix.
8. XOR the feature matrix and the secret image.
9 .Output encrypted image.

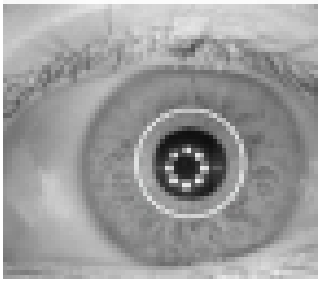
III. RESULTS AND DISCUSSION

In this section, the proposed (n, n) NVSS scheme is illustrated using MATLAB. Here, (3, 3) NVSS scheme is implemented. In this scheme, two natural images and one noise-like share is used. The selected natural images are digital color image. One is the digital image with the size of 1024 × 768 pixels and other is the printed image with the size of 600 × 450 pixels. These natural shares are resized to the size of 256 × 256 pixels as shown in fig (2) and fig (3).

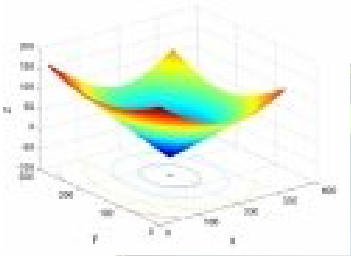


ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 2, February 2015

Fig.2 a. Input Iris Image



The secret image is a color image with the size of 256 × 256 pixels which is shown in fig (4). The pixel values of the secret image range from 0-255 in each color plane. These natural images and the secret image is XOR-ed to form an encrypted image which is the generated noise-like share. The noise-like share thus generated is shown in fig (5).



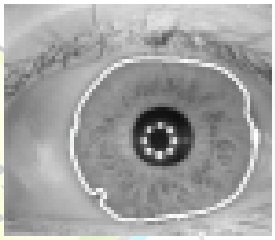
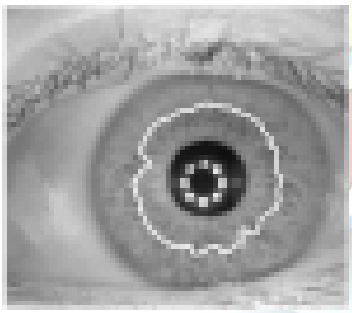


Fig. 2 b. Printed Input Image with histogram



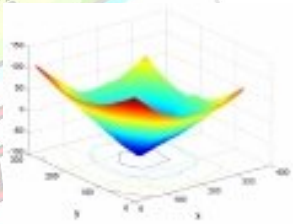


Fig. 4. Boundary Detection Image with historgram

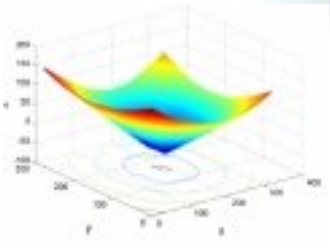


Fig. 3. Gray Scale input Image with histogram

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 2, February 2015

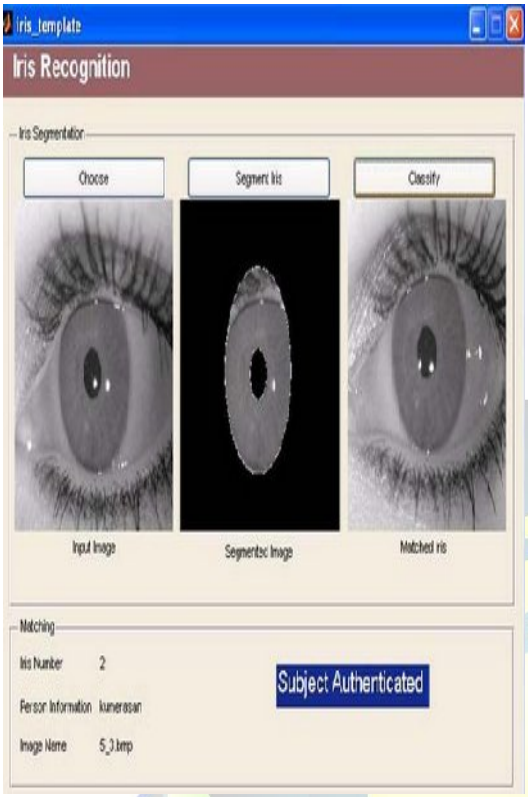


Fig 5 Overall Process Diagram

Using the selected natural shares and the generated noise-like share the secret image is recovered. The recovered image is shown in fig (6).

IV. CONCLUSION

The iris of the eye has been described as the ideal part of the human body for biometric identification for several reasons: It is an internal organ that is well protected against damage and wear by a highly transparent and sensitive membrane (the cornea). This distinguishes it from fingerprints, which can be difficult to recognize after years of certain types of manual labor. The iris is mostly flat, and its geometric configuration is only controlled by two complementary muscles (the sphincter pupillae and dilator pupillae) that control the diameter of the pupil. This makes the iris shape far more predictable than, for instance, that of the face. It also reduces the pixel expansion problem which occured in the conventional method. The display quality of the recovered image and the shares are improved. Hence, we conclude that the proposed scheme can be used as an optimization method to solve the problems concerning transmission risk, pixel expansion in visual secret sharing scheme.

REFERENCES

[1] Prateek Verma, Maheedhar Dubey, Praveen Verma , "Comparison of Various Segmentation Techniques in Iris Recogniti on" LAMBERT ACADEMIC PUBLISHING (LAP), GmbH & co. KG, Dudweiler Landstrabe, Saarbrücken, ISBN 13: 978-3-659-13597-2, Germany, MAY -2012.

[2] Daugman, John (January 2004). "How iris recognition works" (PDF). IEEE Transactions on Circuits and Systems for Video Technology 14 (1): 21–30.doi :10.1109/TCSVT.2003.818350. http://www.cl.cam.ac.uk/users/jgd1000/iris recog.pdf.

[3] Zhaofeng He, Tieniu Tan, Zhenan Sun and Xianchao Qiu (15 July 2008). "Towards Accurate and Fast Iris Segmentation for Iris Biometrics". IEEE Trans Pattern Anal Mach Intell 31 (9): 1670–84.doi :10.1109/TPAMI.2008.183 . PMID 19574626 http://www.cbsr.ia.ac.cn/users/zfhe/publi cations.html.

[4] Wang.R.Z, Y. C. Lan, Y. K. Lee, S. Y. Huang, S. J. Shyu, and T. L. Chia, (2010) "Incrementing visual cryptography using

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 2, February 2015

random grids," Opt. Commun., vol. 283, no. 21, pp. 4242–4249.

[5] Wu.X, D. Ou, Q. Liang, and W. Sun, (2012) "A user-friendly secret image sharing scheme with reversible steganography based on cellular automata," J. Syst. Softw., vol. 85, no. 8, pp. 1852–1863.

[6] Zhou.Z, G. R. Arce, and G. D. Crescenzo, (2006) "Halftone visual cryptography," IEEE Trans. Image Process., vol. 15, no. 8, pp. 2441–2453