Egyptian Informatics Journal (2012) 13, 217–224

Cairo University

Egyptian Informatics Journal

www.elsevier.com/locate/eij
www.sciencedirect.com

ORIGINAL ARTICLE

LDPC and SHA based iris recognition for image authentication

K. Seetharaman, R. Ragupathy *

Department of Computer Science and Engineering, Annamalai University, Annamalai Nagar, Chidambaram 608 002, India

Received 3 August 2012; revised 14 September 2012; accepted 3 October 2012
Available online 4 November 2012

KEYWORDS

Error correction code;
Low density parity check;
Integer wavelet;
Secure hash algorithm;
Iris recognition system

Abstract We introduce a novel way to authenticate an image using Low Density Parity Check (LDPC) and Secure Hash Algorithm (SHA) based iris recognition method with reversible watermarking scheme, which is based on Integer Wavelet Transform (IWT) and threshold embedding technique. The parity checks and parity matrix of LDPC encoding and cancellable biometrics i.e., hash string of unique iris code from SHA-512 are embedded into an image for authentication purpose using reversible watermarking scheme based on IWT and threshold embedding technique. Simply by reversing the embedding process, the original image, parity checks, parity matrix and SHA-512 hash are extracted back from watermarked-image. For authentication, the new hash string produced by employing SHA-512 on error corrected iris code from live person is compared with hash string extracted from watermarked-image. The LDPC code reduces the hamming distance for genuine comparisons by a larger amount than for the impostor comparisons. This results in better separation between genuine and impostor users which improves the authentication performance. Security of this scheme is very high due to the security complexity of SHA-512, which is 2^{256} under birthday attack. Experimental results show that this approach can assure more accurate authentication with a low false rejection or false acceptance rate and outperforms the prior arts in terms of PSNR.

1. Introduction

As the need for security increases, research for more permanent form of biometric, which is difficult to replicate, is considered. One such biometric is human iris. Iris recognition is based on visible features, i.e., rings, furrows, freckles, and corona and is considered very challenging, as they possess a high degree of randomness. The iris is completely formed by 8th month of adults, and remains stable through life. Statistically more accurate than even DNA matching since the probability of two irises being identical is 1 in 10 to the power of 78. Iris is

* Corresponding author. Tel.: +91 4144 223651; fax: +91 9443 530346.
E-mail addresses: kseethadde@yahoo.com (K. Seetharaman), cse_ragu@yahoo.com (R. Ragupathy).

Peer review under responsibility of Faculty of Computers and Information, Cairo University.

Production and hosting by Elsevier

1110-8665 © 2012 Faculty of Computers and Information, Cairo University. Production and hosting by Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.eij.2012.10.001

unique and best biometrics that is mainly used for the establishment of instant personal identity[1]. Compared with other biometric technologies, such as face, speech and finger recognition, iris recognition can easily be considered as the most reliable form of biometric technology [2].

In recent years, the use of iris for human identification has significantly grown due to the outstanding advantages with respect to traditional authentication methods based on personal identification numbers (PINs) or passwords. In fact, since iris is intrinsically and uniquely associated with an individual, they cannot be forgotten, easily stolen or reproduced. However, the use of iris may also have some drawbacks related to possible security breaches. Since iris characteristics are limited and immutable, if an attacker has access to the database where they are stored, the system security may be irreparably compromised. To deal with this problem, iris systems with secure template storage were introduced. In these systems, irreversible cryptographic transformations, such as hash functions, are used to produce secure templates before storing them. Unfortunately, slight differences in the acquired iris data due to acquisition noise, result in a large difference in the cryptographic functions output. In these conditions, even comparisons between templates acquired from the same user will fail. To deal with this acquisition noise, an Error Correction Codes (ECCs) can be used. Since the application of the ECCs has a great influence on the FRR and FAR values of the system, the choice of the code must be done carefully. In this paper, the ECCs properties which influence the performance of the system are analyzed. To illustrate how these properties influence the performance of the system, LDPC codes and RS codes are used, which are two of the most commonly used ECCs in iris systems with secure template storage. LDPC codes are used with a hash function to provide secure iris template storage [3]. To enhance the security of these kind of systems, a universal mask which selects only the 5142 most reliable bit positions of the 9600 bits in the iris templates was introduced [4]. Sutcu et al. [5] and Nagar et al. [6] developed secure biometric systems based on LDPC codes and fingerprints. Kanade et al. [7] concatenated Hadamard and RS codes for iris template secure storage on smart cards. We use LDPC code for correcting the errors in the iris templates.

In the field of Pattern Recognition, Daugman [8] proposed an algorithm for iris recognition. Subsequently many researchers used that algorithm as a benchmark. It finds the iris in a live video image of a person's eye, defines a circular pupillary boundary between the iris and the pupil portions of the eye, and defines another circular boundary between the iris and the sclera portions of the eye. The algorithm fits the circular contours via Integro-differential operator and normalizes the iris ring to a rectangular block of a fixed size. After that it finds a 2048-bit iris code according to the real and imaginary parts of 2D Gabor filters outputs. By using the Hamming Distance (HD), the algorithm compares the code with stored iris codes. In this paper we use the IRS proposed by Seetharaman and Ragupathy [9], which presents a novel approach on iris recognition. We use CASIAIrisV3 [10] iris database for conducting experimental tests.

Recent idea of using message digest algorithm to make cancellable biometrics enable us to use SHA. The SHA is a series of cryptographic hash functions published by the National Institute of Standards and Technology (NIST). The NIST published SHA as Federal Information Processing Standard Publication (FIPS PUB) 180-2 [11] consisting of four algorithms, namely SHA-160, SHA-256, SHA-384 and SHA-512. For transforming the error corrected iris code into cancellable iris code, SHA-512 is used. In this paper, SHA-512 hash is employed for authentication due to its security and uniqueness.

Digital watermarking is the well-known approach for image authentication reported in the literature. The traditional digital signature authentication methods have some drawbacks. As the signature is appended to a digital image, it increases the file size and it can also be removed easily. In digital watermarking, the file size keeps unchanged after embedding the watermark also. Authentication watermark is very sensitive to any modifications imposed upon an image and can be used for tamper localization with high accuracy. In most conventional authentication techniques based on watermarking, the original image is distorted permanently due to the authentication itself. Typically, this distortion cannot be removed completely due to quantization, bit-replacement, or truncation at the grayscale 0 and 255. Although the distortion is often quite small, these distortions are not allowed in some sensitive applications, such as medical or legal imagery or images with a high strategic importance in certain military applications. Thus, it is desired to undo the changes introduced by authentication if the image is verified as authentic. Data embedding techniques satisfying this requirement, are referred to as reversible (also known as lossless) image authentication techniques. To achieve the reversibility, invertible integer-to-integer wavelet transforms [12] are used. Yang et al. proposed a reversible watermarking scheme based on an integer discrete cosine transform (DCT) [13]. Tian [14] embeds the data using the difference expansion technique, which is one of the best reversible data hiding methods. Further, Xuan et al. [15] embedded into the least significant bit-plane (LSB) of high frequency (Cohen–Daubechies–Fauraue) CDF $(2,2)$ integer wavelet coefficients whose magnitudes are smaller than a certain predefined threshold, resulting in one of the best reversible data hiding methods among all reported in the literature. So, this paper utilizes the lossless data hiding using IWT and threshold embedding technique proposed by Xuan et al. [15] for digital image authentication reasons.

Embedding the iris in the form of cancellable biometrics into an image increases the secrecy and use of reversible watermarking does not degrade the quality of original image i.e., with naked eye no one can find the differences between original image and watermarked-image, since data are embedded in the LSB of IWT coefficients. In this paper, we propose a new way to authenticate an image using LDPC and SHA based iris recognition method with reversible watermarking scheme, which is based on IWT and threshold embedding technique. The rest of the paper is organized as follows. Section 2 exhibits the lossless data hiding using IWT and threshold embedding technique. The idea of enrolment process of proposed system is presented in Section 3. How verification process (authentication) works in the proposed system is discussed in Section 4. Some experimental results and performance analysis are given in Section 5. The conclusion is drawn in Section 6.

2. The lossless data hiding using integer wavelet transform and threshold embedding technique

We decided to use the CDF $(2,2)$ integer wavelet transform, adopted by JPEG2000 for image lossless compression, to obtain the wavelet coefficients. Because of what is called frequency mask, the data embedded into in the first level high frequency sub-bands will have less visible artifact to human eyes. In the enrolment process of the proposed authentication system embeds parity checks, parity matrix and SHA-512 hash of iris code (generated in the phase quantization process of iris recognition system [9]) lossless into the first level high frequency sub-bands of images using threshold embedding technique.

To embed parity checks, parity matrix and SHA-512 hash of iris code into a high frequency coefficient x, the absolute value of the coefficient is compared with predefined T. If $|x| < T$, the coefficient value is doubled and the to-be-embedded bit is appended as the right-most bit. The resultant coefficient is denoted by x'. Otherwise, if $x \geqslant T$, the coefficient will be added by T, if $x \leqslant -T$, the coefficient will be subtracted by $(T-1)$, and no bit is embedded into this coefficient. These rules can be summarized as

$$x' = \begin{cases} 2 * x + b, & \text{if } |x| < T \\ x + T, & \text{if } x \geqslant T \\ x - (T-1), & \text{if } x \leqslant -T \end{cases} \tag{1}$$

Histogram modification is performed prior to the embedding to ensure no overflow/underflow will take place. The bookkeeping data of histogram modification, parity checks, parity matrix and SHA-512 hash string of iris code are embedded into the high frequency IWT coefficients. The Watermarked-image carrying hidden parity checks, parity matrix and SHA-512 hash is obtained after inverse IWT.

In the authentication process of proposed system, simply by reversing the embedding process the original image, parity checks, parity matrix and SHA-512 hash are extracted back from watermarked-image. Then this extracted parity checks, parity matrix and SHA-512 hash are used to authenticate the original image by matching with the new hash generated from the live person. At first, IWT is applied on Watermarked-image to find eligible sub-bands then bookkeeping data of histogram modification, parity checks, parity matrix and SHA-512 hash are extracted from these sub-bands. For a coefficient, if it is less than $2T$ and larger than $(-2T+1)$, the LSB of this coefficient is the bit embedded into this coefficient. Otherwise, we jump to the next coefficient since the current coefficient has no hidden bit in it. Concretely, each high frequency coefficient can be restored to its original value by applying

$$x = \begin{cases} \left\lfloor \frac{x'}{2} \right\rfloor, & \text{if } -2T+1 < x' < 2T \\ x' - T, & \text{if } x' \geqslant 2T \\ x' + T - 1, & \text{if } x' \leqslant -2T+1 \end{cases} \tag{2}$$

After extraction, inverse IWT is applied with untouched sub-band and processed sub-bands with parity checks, parity matrix and SHA-512 hash. Finally, original image is recovered by making inverse histogram modification.

3. Enrolment process of proposed system

The IRS proposed by Seetharaman and Ragupathy [9] is used for generating n number of iris codes from n number of eye samples collected from same person on different time interval. From the n number of iris code a unique iris code x is constructed by using majority voting scheme. LDPC encoding scheme operates on x and produces codewords, also called as Error Corrected Iris Code (ECIC). These ECIC consist of iris code and parity checks p. Simultaneously, SHA-512 produces hash h from code x. Finally, parity checks p of ECIC, parity matrix H and hash h from SHA-512 make code's, which is embedded into a digital image using integer wavelet transform and threshold embedding technique. The entire enrolment process is depicted in Fig. 1.

The novelty of IRS includes improving the speed and accuracy of the iris segmentation process, fetching the iris image so as to reduce the recognition error, producing a feature vector with discriminating texture features and a proper dimensionality so as to improve the recognition accuracy and computational efficiency. The Canny edge detection and circular Hough transforms are used for the segmentation process. The segmented iris is normalized using Daugman's rubber sheet model from $[-32°, 32°]$ and $[148°, 212°]$. The phase data from 1D Log-Gabor filter is extracted and encoded efficiently to produce a proper feature vector using phase quantization method. The results of process of segmentation, normalization and phase quantization for a sample eye image from CASIA-IrisV3-Interval database is given in Fig. 2. Once the iris region is successfully segmented from an eye image, the next stage is to transform the iris region so that it has fixed dimensions in order to allow comparisons. The dimensional inconsistencies between eye images are mainly due to the stretching of the iris caused by pupil dilation from varying levels of illumination. Other sources of inconsistency include, varying imaging distance, rotation of the camera, head tilt, and rotation of the eye within the eye socket.

Construction of unique iris code x from n number of iris code is done in a simple method called majority voting. Fabrication of such unique iris code x from three sample iris codes is explained in Fig. 3. From the unique code x, ECIC is formed by LDPC and hash version h is transformed by SHA-512. First, we discuss LDPC encoding and then we deliberate SHA-512.

In general, LDPC codes are defined by a sparse parity-check matrix. This sparse matrix is often randomly generated, subject to the sparsity constraints. Fig. 4 is a graph fragment of an example LDPC code using Forney's factor graph notation. In this graph, n variable nodes in the top of the graph are connected to $(n–k)$ constraint nodes in the bottom of the graph. This is a popular way of graphically representing an (n,k) LDPC code. The bits of a valid message, when placed on top of the graph, satisfy the graphical constraints. Specifically, all lines connecting to a variable node (box with an '=' sign) have the same value, and all values connecting to a factor node (box with a '+' sign) must sum, modulo two, to zero (in other words, they must sum to an even number). After construction of unique iris code x, each column in the iris code x is considered as message in LDPC encoding and encoded to make ECIC with the help of generator matrix G.

After forming ECIC by multiplying all columns with G, segregate the parity checks p form each codeword of ECIC. Following example illustrates the method of LDPC encoding. Ignoring any lines going out of the picture, there are 8 possible 6-bit strings corresponding to valid codewords (i.e., 000000, 011001, 110010, 101011, 111100, 100101, 001110, 010111). This LDPC code fragment represents a 3-bit message encoded as six bits. Redundancy is used here, to increase the chance of recovering from channel errors. This is a (6, 3) linear code, with $n = 6$ and $k = 3$. By ignoring lines going out of the picture, the parity-check matrix representing this graph fragment is given in the following equation:

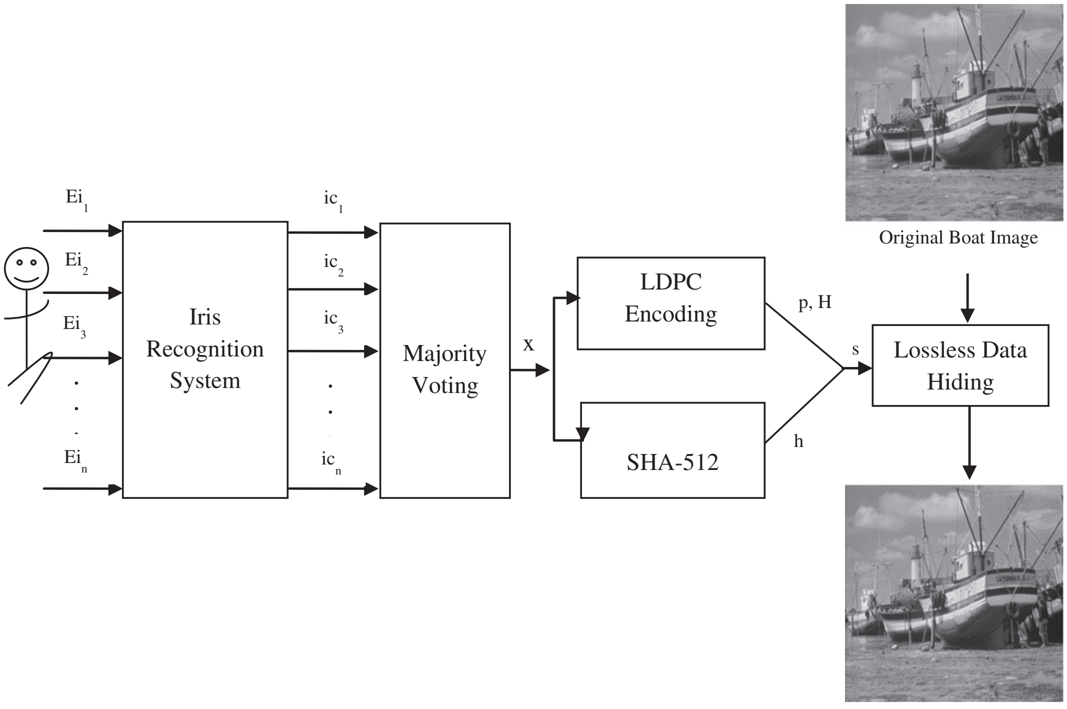
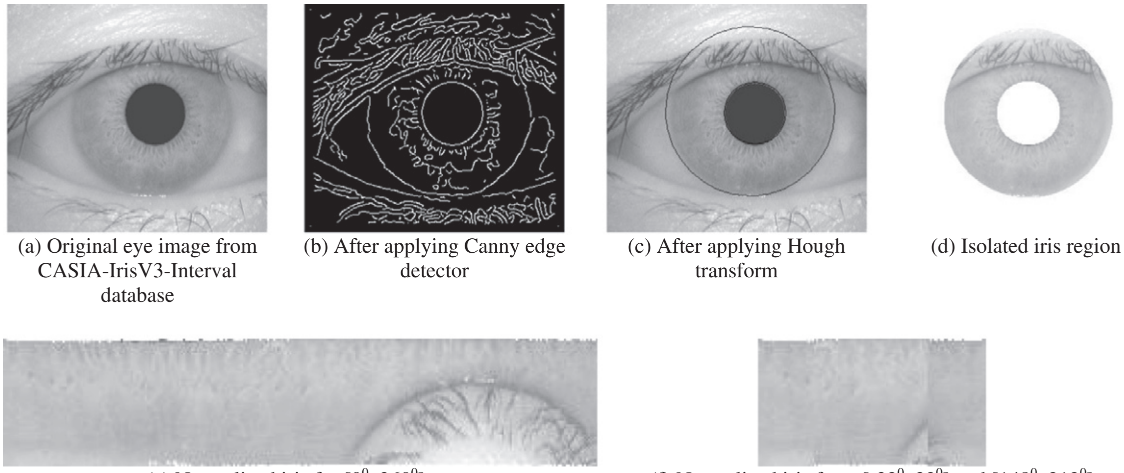


Figure 1 Block diagram of enrolment process of the proposed system.



(a) Original eye image from CASIA-IrisV3-Interval database

(b) After applying Canny edge detector

(c) After applying Hough transform

(d) Isolated iris region

(e) Normalized iris for [0^0, 360^0]

(f) Normalized iris from [-32^0, 32^0] and [148^0, 212^0]

```
-3.14 -i0.23   -1.44 -i2.82   1.75 -i2.69   3.23 +i0.17   1.44 +i2.92   -1.84 +i2.64 …..        00 00 10 11 11 01…..
-3.68 -i0.27   -1.67 -i3.31   2.06 -i3.14   3.76 +i0.21   1.68 +i3.42   -2.15 +i3.10…..         00 00 10 11 11 01…..
-3.33 -i0.23   -1.58 -i3.00   1.86 -i2.92   3.48 +i0.17   1.55 +i3.15   -1.98 +i2.82…..         00 00 10 11 11 01…..
-3.32 -i.018   -1.61 -i2.97   1.82 -i2.92   3.46 +i0.14   1.57 +i3.11   -1.93 +i2.82…..         00 00 10 11 11 01…..
-3.28 -i0.09   -1.66 -i2.89   1.73 -i2.92   3.14 +i0.07   1.61 +i3.02   -1.82 +i2.82…..         00 00 10 11 11 01…..
-3.37 -i0.32   -1.53 -i3.07   1.95 -i2.92   3.53 +i0.25   1.51 +i3.25   -2.09 +i2.82…..         00 00 10 11 11 01…..
                                            .                                                           .
                                            .                                                           .
                                            .                                                           .
```

(g) After convolution with 1D Log-Gabor wavelet filter using FFT and inverse FFT

(h) Iris template

Figure 2 Segmentation, normalization and phase quantization processes of iris recognition system.

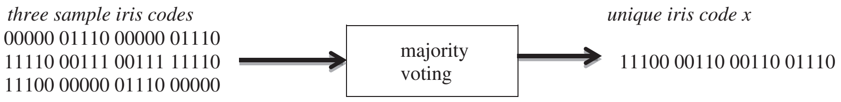


Figure 3 Construction of unique iris code.

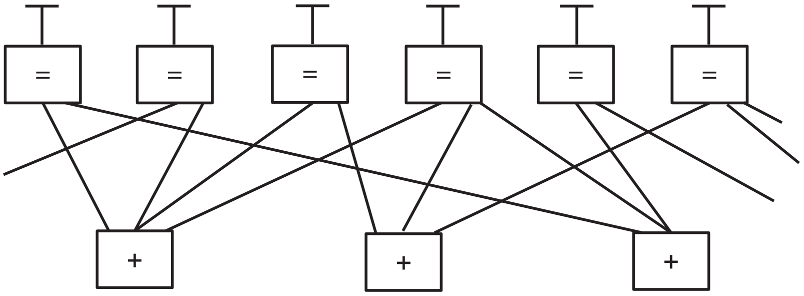


Figure 4 Graph fragment of an example LDPC encoding.

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 \end{pmatrix} \tag{3}$$

In this matrix, each row represents one of the three parity-check constraints, while each column represents one of the six bits in the received codeword. In this example, the eight codewords can be obtained by putting the parity-check matrix H into this form $[-P^T|I_{n-k}]$ through basic row operations as shown in the following equation:

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \end{pmatrix}$$
$$\sim \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \tag{4}$$

From this, the generator matrix G can be obtained as $[I_k|P]$. The obtained generator matrix from Eq. (4) is shown in Eq. (5). Note that in the special case of this being a binary code $P = -P$

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix} \tag{5}$$

Finally, by multiplying all eight possible 3-bit strings by G, all eight valid codewords are obtained. For example, Eq. (6) shows the codeword obtained for the bit-string '101'.

$$(1 \quad 0 \quad 1) \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix} = (1 \quad 0 \quad 1 \quad 0 \quad 1 \quad 1) \tag{6}$$

Simultaneously, the unique iris code x is transformed to hash h, also called as cancellable iris code by SHA-512 message digest algorithm. SHA-512 found in FIPS PUB 180-2 documentation is adapted for this system. Sample hash h from SHA-512 for a unique iris code x is given in Fig. 5.

4. Verification process of the proposed system

Iris code $\hat{x}$ is generated by IRS of eye sample collected from live person. LDPC decoding scheme operates on $\hat{x}$ and produces $\tilde{x}$ with the help of parity matrix H and parity checks p, which are extracted from watermarked-image using IWT and threshold embedding technique. Like in enrolment process SHA-512 produces hash $\tilde{h}$ from code $\tilde{x}$. Finally, hash $\tilde{h}$ from SHA-512 and hash h extracted from watermarked-image is compared for authentication. This verification process is illustrated in Fig. 6.

To illustrate LDPC decoding, assume that the first three bits from live person and the next three bits are appended from parity checks. Consider that the valid codeword 101011, from the example discussed in Section 3. If the first bit of iris code from live person is changed then we get 001011. Since the iris code must have satisfied the code constraints, the iris code can be represented by writing them on the top of the factor graph.

SHA-512 hash length: 64
SHA-512 hash value: -36 92 34 -113 105 56 -58 -1 -32 -64 86 -66 19 87 -85 -67 36 29 59 108 -91 -22 102 82 53 103 116 -1 -23 -126 -99 9 -113 -14 25 -38 -109 113 -86 -75 114 110 -28 71 109 -40 -11 70 -13 77 -94 -35 117 -86 29 62 -80 -119 -36 37 102 15 74 96
SHA-512 hash string length: 128
SHA-512 hash string:
dc5c228f6938c6ffe0c056be1357abbd241d3b6ca5ea6652356774ffe9829d098ff219da9371aab5726ee447
6dd8f546f34da2dd75aa1d3eb089dc25660f4a60

Figure 5 Sample hash h of SHA-512.

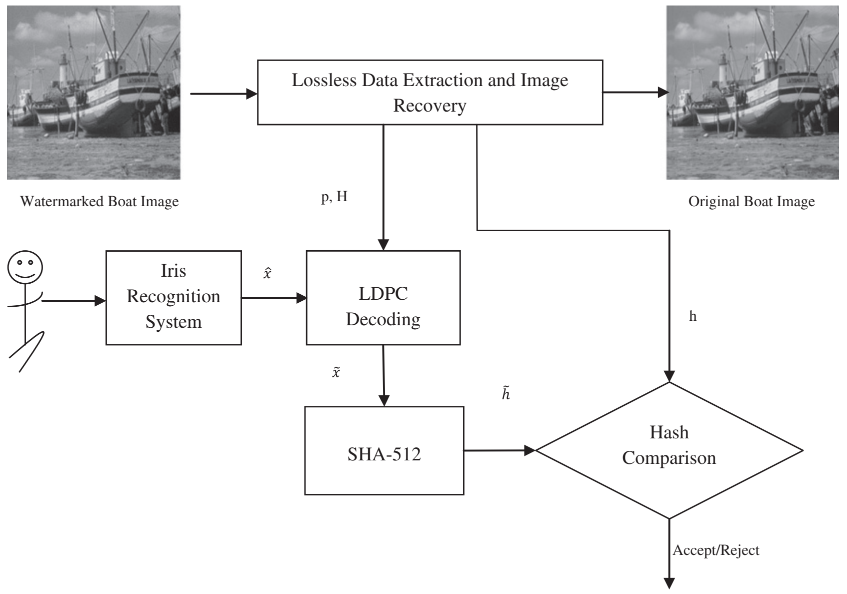


Figure 6 Block diagram of verification process of the proposed system.

The result can be validated by multiplying the corrected codeword r with the parity-check matrix H in Eq. (3).

$$z = Hr = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \tag{7}$$

As the outcome z (the syndrome) of this operation is the 3×1 non-zero vector in Eq. (7), look at column 1 of H which is the only equivalent to the outcome z. So flip the first bit as 1 and continue the validation. Thus, the iris code can be decoded iteratively.

$$z = Hr = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \tag{8}$$

Now in Eq. (8), outcome z (the syndrome) of this operation is the 3×1 zero vector, the resulting codeword r is successfully validated.

5. Experimental results

From the public database CASIAIrisV3 [10], we choose 200 classes (eyes) and 1500 images in the subset labeled as CASIA-IrisV3-Interval. For each iris class, we choose four samples for enrolment process. In verification process, rest of the iris image in the database is compared with the other entire iris. The total number of comparisons is $(1500 \times 1499)/2 = 1$, 124, 250, where the total number of intra-class comparisons is 7648 and that of inter-class comparisons is 1,116,602. Fig. 7 shows distributions of intra-class (solid line) and inter-class (dashed line) matching distance for CASIA-IrisV3-interval data sets. From Fig. 7, we can find that the distance

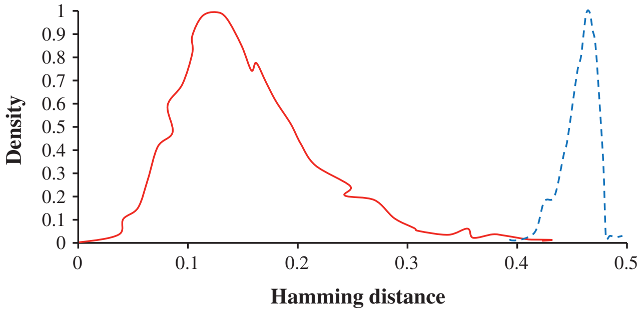


Figure 7 Distributions of intra-class and inter-class distance for CASIA-IrisV3-Interval database.

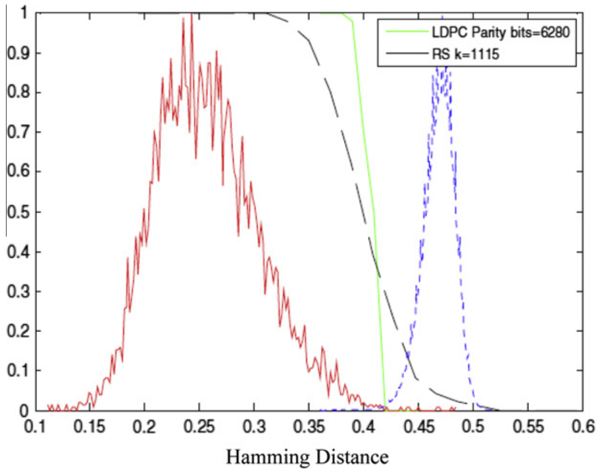
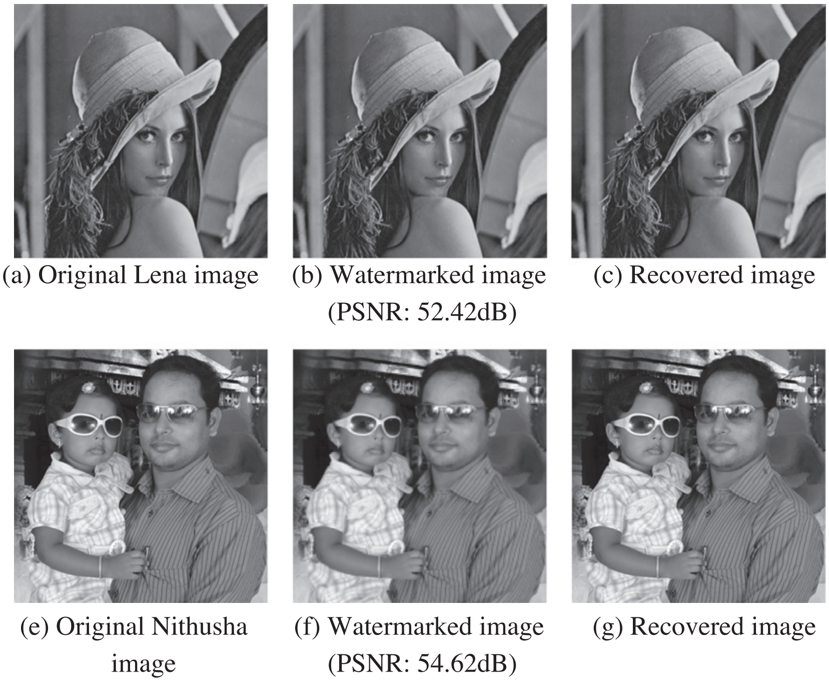


Figure 8 RS (with $k = 1115$) and LDPC code (with 6280 parity bits) codes overlaid on top of the genuine and impostor normalized HD distributions.


(a) Original Lena image (b) Watermarked image (PSNR: 52.42dB) (c) Recovered image

(e) Original Nithusha image (f) Watermarked image (PSNR: 54.62dB) (g) Recovered image

Figure 9 Results of loss data hiding and extraction.

between the intra-class and the inter-class distribution is large, and the portion that overlaps between the intra-class and the inter-class is very small. So that almost, 100% correct recognition rates are obtained on CASIA-IrisV3-interval data sets.

To show the error correction capability of LDPC, we consider Reed Solomon (RS) code from the family of ECC. Fig. 8 shows selected curves of the RS (with $k = 1115$) and LDPC code (with 6280 parity bits) codes overlaid on top of the genuine and impostor normalized HD distributions. As can be easily observed, the RS correction curves are significantly less steep than the LDPC curves. Moreover, the RS code is also less granular than the LDPC. This leads to performance degradation, with False Rejection Rate (FRR) and False Acceptance Rate (FAR) values varying from 0.08% to 21.293% and from 0.014% to 57.36%, respectively. The corresponding Equal Error Rate (EER) value is 2.44%. But for LDPC, the resulting FRR and FAR values range from 0.754% to 1.87% and from 0.036% to 0.365%, respectively. For this situation, the estimated EER would be 0.41%.

We tested the proposed scheme with Lena image, Boat, Baboon, Pepper, House, Nithusha image (our own new image) etc., and various eye images in the CASIAIrisV3 database for authentication purpose. The quality of watermarking is generally measured with PSNR. If it is more than 30 dB, it is good and cannot be identified by naked eye. For most of the test using IWT and threshold embedding technique, it is more than 45 dB. Example test results of Lena and Nithusha are shown in Fig. 9. In which, PSNR of watermarked image with original Lena image is 52.42 dB for $T = 6$, which is 2 dB more than difference expansion method [14] and 4 dB more than DCT method [13]. Similarly, PSNR of watermarked image with original Nithusha image is 54.62 dB for $T = 6$, which is also approximately 2 dB more than difference expansion method and 4 dB more than DCT method.

6. Conclusion

In IRS, iris is segmented by a simple and fast technique, which is based on Canny edge detector and Hough transform and introduced the 32° normalization method to eliminate Regions 1 type of noise i.e., obstructions due to eyelids and eyelashes in the lower and upper iris regions. Consequently, the detection time of upper and lower eyelids and 64.4% cost of the polar transformation are saved. The maximum FRR and FAR for Daugman's method are 2.0% and 0.38%, where as our method's FRR and FAR are 1.87% and 0.365%. Compared with Daugman's method, a significant decrement of the error rates are observed. Using majority voting scheme and LDPC, the fuzziness i.e., the variability and Regions 2 type of noise (reflections of external light sources) in the iris code is solved. LDPC codes have shown to lead to better recognition performance results than RS codes, due to the better steepness and granularity properties. Low FRR and FAR is achieved by using LDPC codes in this system. MD5 algorithm could produce identical hashes for two different messages if the initialization vector could be chosen, so we cannot adapt MD5 for authentication. As we use SHA-512, Security of this scheme is very high due to the security complexity of SHA-512 is 2^{256} under birthday attack. For authenticating the image, we embedded cancellable iris code in the form of SHA-512 hash using IWT and threshold embedding technique, which performed better than difference expansion method and DCT method. As a conclusion remarks, it can be stated that, the proposed system has superior performance in terms of security, accuracy and consistency compared with other published technology.

Acknowledgment

Portions of the research in this paper used the CASIA Iris image database collected by Institute of Automation, Chinese Academy of Sciences.

References

[1] Kumar Ajay, Passi Arun. Comparison and combination of iris matchers for reliable personal authentication. Pattern Recogn 2010;43:1016–26.

[2] Sanderson S, Erbetta J. Authentication for secure environments based on iris scanning technology. IEE Colloq Vis Biometrics 2000.

[3] Vetro A, Rane S, Yedidia J. Distributed source coding: theory, algorithms and applications. Elsevier: Securing Biometric Data; 2009.

[4] Santos T, Soares LD, Correia PL. Iris verification system with secure template storage. In: European signal processing conference (EUSIPCO). Aalborg, Denmark; 2010.

[5] Sutcu Y, Rane S, Yedidia JS, Draper SC, Vetro A. Feature extraction for a slepian-wolf biometric system using LDPC Codes. In: IEEE international symposium on information theory (ISIT); July 2008. p. 2297–301.

[6] Nagar A, Rane S, Vetro A. Privacy and security of features extracted from minutiae aggregates. In: IEEE international conference on acoustics speech and signal processing (ICASSP); March 2010. p. 1826–9.

[7] Kanade S, Camara D, Krichen E, Petrovska-Delacretaz D, Dorizzi B. Three factor scheme for biometric-based cryptographic key regeneration using iris. In: Biometrics symposium (BSYM); September 2008. p. 59–64.

[8] Daugman J. Biometric personal identification system based on iris analysis. Patent no. 5291560; 1994.

[9] Seetharaman K, Ragupathy R. Iris recognition for personal identification system. Procedia Eng 2012;38:1531–46.

[10] Chinese Academy of Sciences. Institute of Automation (CASIA), Iris image database CASIA-Iris-V3. <http://www.cbsr.ia.ac.cn/IrisDatabase.htm>.

[11] National Institute of Standards and Technology. Secure hash standard. Federal Information Processing Standards Publications FIPS PUB 180-2; 2001.

[12] Daubechies I, Sweldens W. Factoring wavelet transforms into lifting steps. J Fourier Anal Appl 1998;4(3):245–67.

[13] Yang B, Schmucker M, Funk W, Busch C, Sun S. Integer DCT-based reversible watermarking for images using companding technique. In: Proc SPIE, security, steganography, and watermarkingof multimedia contents, San Jose, CA; January 2004. p. 405–15.

[14] Tian J. Reversible data embedding using a difference expansion. IEEE Trans Circuits Syst Video Technol 2003:890–6.

[15] Xuan G, Shi YQ, Yao Q, Ni Z, Yang C, Gao J, et al. Lossless data hiding using integer wavelet transform and threshold embedding technique. In: Proc of IEEE international conference on multimedia and expo; 2005. p. 1520–3.