A Novel Biometric Cryptosystem using LDPC and SHA based Iris Recognition

K. Seetharaman
Associate Professor
Department of Computer Science and Engineering
Annamalai University, Annamalai Nagar,
Chidambaram, Tamil Nadu-608002, India

R. Ragupathy
Assistant Professor
Department of Computer Science and Engineering
Annamalai University, Annamalai Nagar,
Chidambaram, Tamil Nadu-608002, India

ABSTRACT

We use Low Density Parity Check (LDPC) error correction code to solve fuzziness i.e., the variability and noise in iris code generated from Iris Recognition System (IRS) and Secure Hash Algorithm (SHA-512) to transform unique iris code into hash string to make them as a Cancellable Biometric. SHA-512 hash string is used as a key for 512 bits Advanced Encryption Standard (AES) encryption process. In the decryption process, Hash comparison is made between new hash generated by SHA-512 from error corrected iris code and hash stored in smart card. If authentic, 512 bits AES decryption is accomplished. Experiments indicate that, use of LDPC code results in better separation between genuine and impostor users which improves the performance of this novel cryptosystem. Security of this system is very high, which is 2^{256} under birthday attack. AES algorithm is enhanced by using 512 bits key and increasing the number of rounds.

General Terms

Iris Pattern Recognition, Cryptography, Computer Security.

Keywords

Error Correction Code, Low Density Parity Check, Secure Hash Algorithm, Advanced Encryption Standard, Iris Recognition System.

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 8^{th} month of adults, and remains stable through life. Statistically more accurate than even DNA matching since the probability of 2 irises being identical is 1 in 10 to the power of 78 [1]. Iris is unique and best biometrics that is mainly used for the establishment of instant personal identity [2]. 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 [3]. 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 (ECC) 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. To illustrate how LDPC codes properties influence the performance of the system, we compared with RS codes in this paper, which are two of the most commonly used ECCs in iris systems with secure template storage. Sutcu *et al.* [4] and Nagar *et al.* [5] developed secure biometric systems based on LDPC codes and fingerprints. Wu*et al.* [6] proposed a biometric cryptosystem using the iris and RS codes. Also, Wu *et al.* [7] used RS codes and the logical XOR operation to encrypt biometric palmprint data.

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 2,048-bit iris code according to the real and imaginary parts of 2D Gabor filters outputs. By using the hamming distance, the algorithm compares the code with stored iris codes.

In this paper we use the IRS proposed byK. Seetharaman and R. Ragupathy [9], which presents a novel approach on iris recognition. The Canny edge detection and circular Hough transforms are used in the segmentation process, which improves the speed and accuracy of the iris segmentation process. The segmented iris is normalized using Daugman’s rubber sheet model from [-32^0, 32^0] and [148^0, 212^0]. The iris image is fetched in such a way that it reduces the recognition error. The phase data from 1D Log-Gabor filter is extracted and encoded efficiently to produce a proper feature vectorwith discriminating texture features and a proper dimensionality so as to improve the recognition accuracy and computational efficiency.Using hamming distance, two iris codes are compared for person identification. For conducting experimental tests,we use CASIAIrisV3 [10] iris database,which is collected by Institute of Automation, Chinese Academy of Sciences.

Recent idea of using message digest algorithm to make cancellable biometrics enable us to use Secure Hash Algorithm (SHA). The SHA is a series of cryptographic hash functions published by the National Institute of Standards and Technology (NIST). NIST proposed several

FederalInformation Processing Standard Publication namely FIPS PUB 180 [11], FIPS PUB 180-1 [12], and FIPS PUB 180-2 [13]. SHA-512 algorithm is published FIPS PUB 180-2 [13].For transforming the error corrected iris code into cancellable iris code, SHA-512 is used. In this paper, SHA-512 is employed to generate the key for 512 bits AES scheme due to its security and uniqueness.

The Rijndael algorithm was adopted as an encryption standardby the NIST as FIPS PUB 197 on November 2001 [14]. The AES algorithm was believed to provide more security than the DES [15]. The AES algorithm was designed to have resistance against all known attacks, speed and code compactness on a wide range of platforms and design simplicity [16]. AES has three variable key lengths but block length is fixed to 128 bits [14]. The three key sizes of AES are 128, 192 and 256 bits. Their number of possible keys is 3.4 x 10^{38}, 6.2 x 10^{57} and 1.1 x 10^{77} respectively [14]. There are on the order of 10^{21} times more AES 128 bits keys than DES 56bits keys. AES with 128 bits keys has stronger resistance to an exhaustive key search than DES. Biham*et al.* [17] introduced a newest attack combined boomerang and the rectangle attack with related-key differentials. It uses the weaknesses of few nonlinear transformations in the key schedule algorithm of ciphers, and can break some reduced-round versions of AES. It can break 192bits 9-round AES by using 256 different related keys. Ferguson *et al.* proposed some optimizations that reduce the work factor of the Square attack [18]. This attack breaks a 256bits 9-round AES with 2^{77} plaintexts under 256 related keys, and 2^{224} encryptions. In order to provide a stronger encryption method, in this paper we uses AES algorithm with increased number of rounds by using the key length to 512 bits.

In this paper, we propose a novel Biometric Cryptosystem using LDPC and SHA Based Iris Recognition. The rest of the paper is organized as follows. Section 2 exhibits the 512 bits AES scheme adapted for this scheme. The idea of encryption process of proposed system is presented in Section 3. How decryption process 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. 512 BITS AES SCHEME

AES is a block cipher, substitution-permutation network and the most popular algorithm used in symmetric key cryptography. The complexity of AES encryption and decryption increases,when the number of rounds is increased in AES. The number of rounds (N_r) in this AES algorithm depends on the length of main key (N_k) and the number of block columns (N_b), i.e. $N_r = N_k+N_b+\text{abs}(N_k-N_b)$. So, we decided to use the outcome of SHA-512 (hash h or hash $\tilde{h}$) as a key in order to increase the number of rounds. The input to the encryption and decryption algorithms is a single 128-bits block and the 512 bits key. Same key is to be used for both encryption and decryption.

AES operates on a 16x32 array of bytes, termed as state. Each entry in S-box of AES 512 is 9 bits long, since 9 bits are required to represent the value 512. The encryption process of AES 512 has been illustrated in Figure 1. Each round in AES 512 encryption includes four different round transformations namely Substitute Bytes, Shift Rows, Mix Columns and Add Round Key. The Mix Columns transformation is not included in the last round of AES 512 encryption.

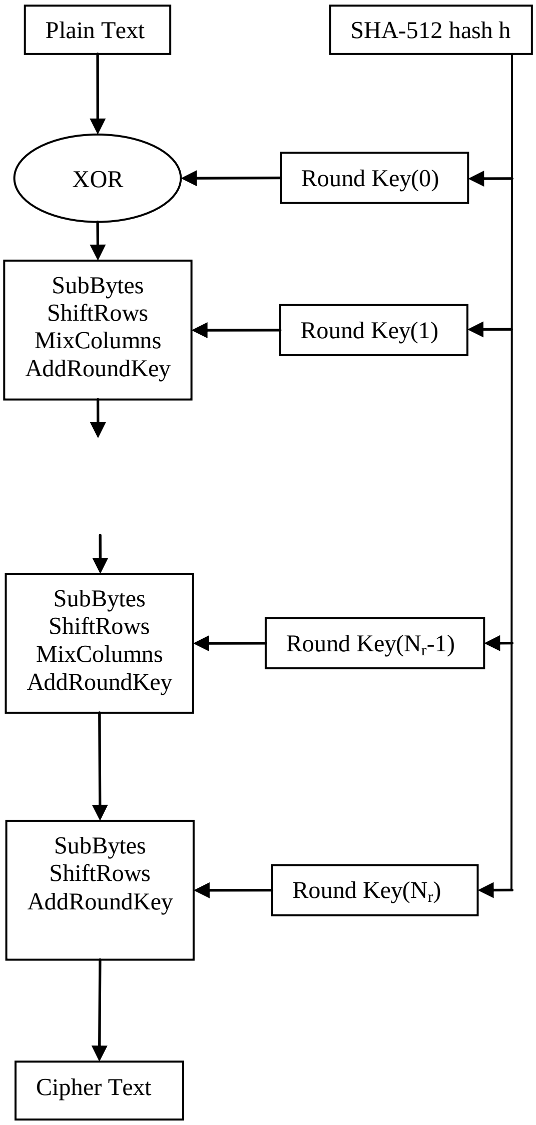


Fig 1: Encryption process of AES 512

The cipher is specified in terms of repetitions of processing steps that are applied to make up rounds of keyed transformations between the input plain-text and the final output of cipher-text.In the SubBytes transformation, each byte in the state matrix is replaced with a SubByte using a substitution box, the Rijndael S-box. This operation provides the non-linearity in the cipher. The ShiftRows transformation operates on the rows of the state and it cyclically shifts the bytes in each row by a certain offset.In the MixColumns transformation, the four bytes of each column of the state are combined using an invertible linear transformation.In the AddRoundKey transformation, the subkey is combined with the state. For each round, a subkey is derived from the main key using Rijndael's key schedule; each subkey is the same size as the state. The subkey is added by combining each byte of the state with the corresponding byte of the subkey using bitwise XOR.

To transform cipher-text back into the original plain-text, a set of reverse rounds are applied using the same encryption key.

Add Round Key, Inverse Mix Columns, Inverse Shift Rows and Inverse Substitute Bytes are the four reverse transformations used. The inverse S-box contains 512 values in its 16x32 array of bytes. Except first round, each round in decryption of AES 512 includes all the four reverse transformations. In the last round of encryption, the Mix Column transformation does not occur, so the InverseMix Columnis breached in the first round of decryption. The decryption process of AES 512 is illustrated in Figure 2.

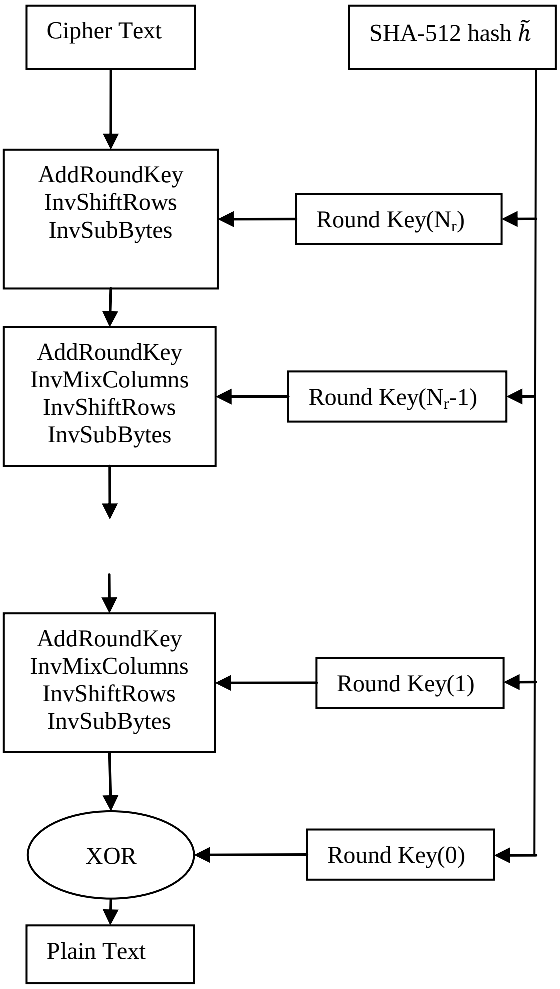


Fig 2: Decryption process of AES 512

3. ENCRYPTION PROCESS OF PROPOSED SYSTEM

The IRS proposed by K. Seetharaman and R. 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.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 segmented iris is normalized using Daugman’s rubber sheet model from [-32^0, 32^0] and [148^0, 212^0]. The phase data from 1D Log-Gabor filter is extracted and encoded efficiently to produce a proper feature vector also called as iris code. From the n number of iris code a unique iris code x is constructed by using majority voting scheme. Fabrication of such unique iris code x from three sample iris codes is explained in Figure. 3.

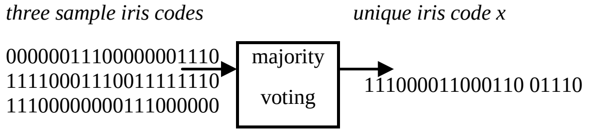


Fig 3: Construction of unique iris code

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.In general, LDPC codes are defined by a sparse parity-check matrix. This sparse matrix is often randomly generated, subject to the sparsity constraints. Figure 4 is a graph fragment of an example LDPC code using Forney's factor graph notation.

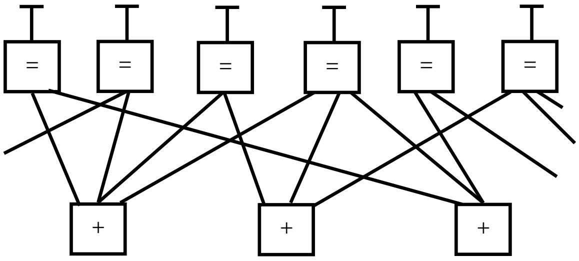


Fig 4: Graph fragment of an example LDPC encoding

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 aneven 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 generatormatrix *G*.

After formingECIC by multiplying all columns with *G*, segregate theparity 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. Once again ignoring lines going out of the picture, the parity-check matrix representing this graph fragment is

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

In this matrix, each row represents one of the three paritycheck 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 paritycheck matrix H into this form $\left[-P^T \mid I_{n-k}\right]$ through basic row operations

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

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

From this, the generator matrix G can be obtained as $\left[I_k \mid P\right]$ (noting that in the special case of this being a binary code $P = -P$), or specifically

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

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

$$\begin{pmatrix} 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

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 Figure5.

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:

dc5c228f6938c6ffe0c056be1357abbd241d3b6ca5ea66523567
74ffe9829d098ff219da9371aab5726ee4476dd8f546f34da2dd
75aa1d3eb089dc25660f4a60

Fig 5: Decryption process of AES 512

Finally, parity checks p of ECIC, parity matrix H and hash h from SHA-512 make code s, which is stored into a smart card for decryption process. This smart card consists of the AT90S8515 microcontroller which is a low-power CMOS 8-bit microcontroller and the AT24C64 EEPROM which provides 65,536 bits (8KB) of serial electrically erasable and programmable read only memory [19]. The smart card programmer has been designed to enable read/write from/to the smart card. The programmer is connected to the PC using the parallel port, due to its higher speed compared with serial port and the ability to generate multiple signals at the same time. Time taken for reading and writing is very minimal for this type of card i.e. Smart card reading and writing time for 380 bits out of 8kb are 3sec and 6 sec respectively.Outcome of SHA-512 is used as a key to encrypt the plain text into cipher text using 512 bits AES encryption method as discussed in section 2.The entire encryption process is depicted in Figure6.

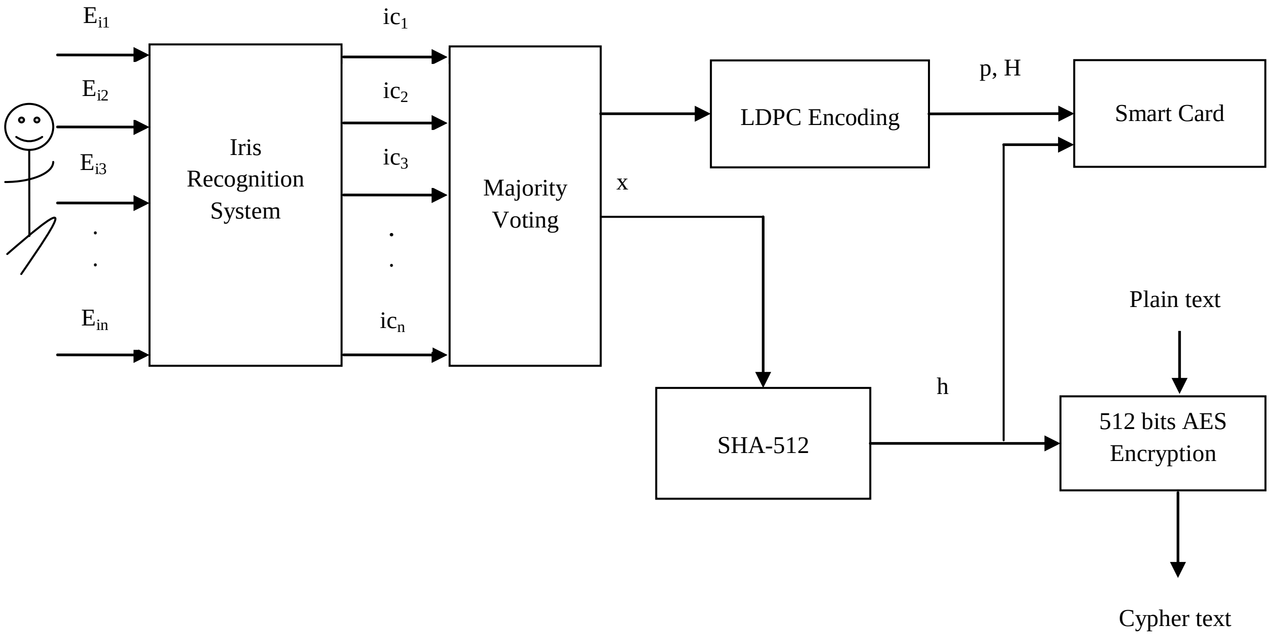


Fig 6: Encryption process of proposed system

4. DECRYPTION PROCESS OF PROPOSED SYSTEM

Like encryption, the IRS proposed by K. Seetharaman and R. Ragupathy [9] is used for generating n number of iris codes from n number of eye samples collected lively from same person on different time interval. From the n number of iris code a unique iris code $\hat{x}$ is fabricated using majority voting scheme. LDPC decoding scheme operates on $\hat{x}$ and produces $\tilde{x}$ with the help of parity matrix H and parity checks p, which are retrieved from smart card. Like in encryption process SHA-512 produces hash $\tilde{h}$ from code $\tilde{x}$. Finally, hash $\tilde{h}$ from SHA-512 and hash h retrieved from smart card is compared for authentication. If it is authentic then decryption is carried out using 512 AES decryption method as discussed in section 2 otherwise decryption is not possible. Thecomplete decryption process is illustrated in Figure 7.

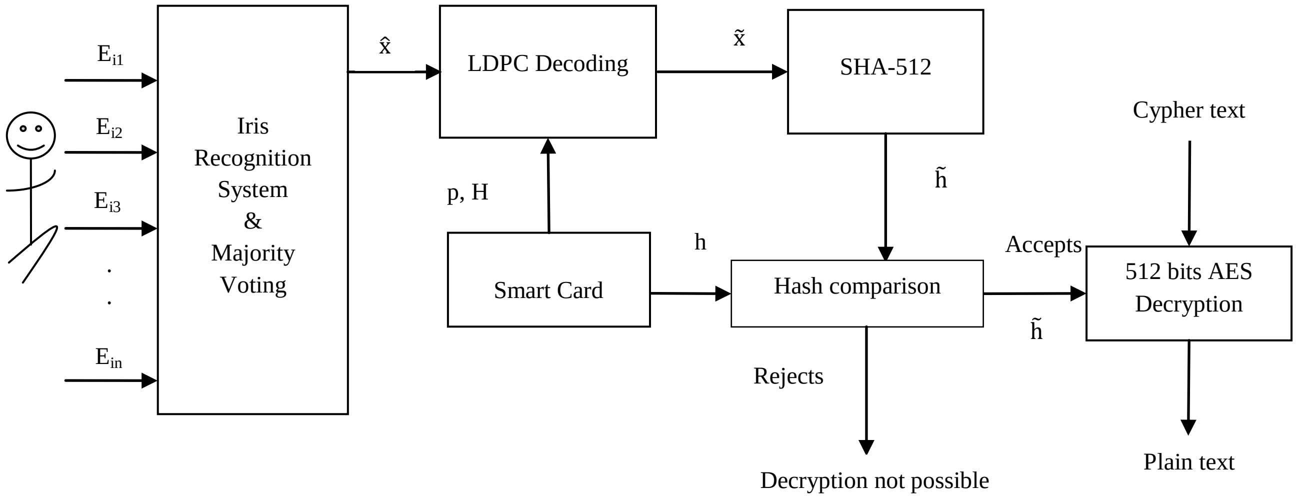


Fig 7: Decryption process of proposed system

To illustrate LDPC decoding, assume that the first three bits from $\hat{x}$ of 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. The result can be validated by multiplying the corrected codeword *r* by the parity-check matrix *H*

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

Because the outcome *z* (the syndrome) of this operation is the 3 × 1 non-zero vector, look at column 1of *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

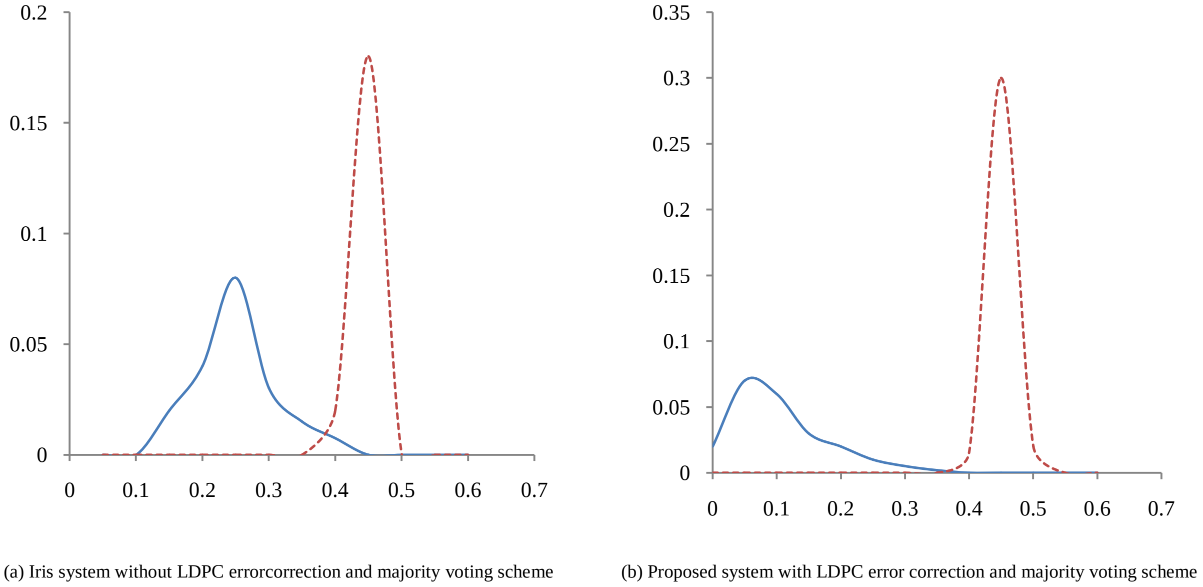
$$z = Hr = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

Now, the 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 labelled as CASIA-IrisV3-Interval. For each iris class, we choose four samples for encryption process. In decryption process, rest of the iris images in the database are used for comparison with the other entire iris. The total number of comparisons is (1500 X 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. Almost, One hundred percent correct recognition rates are obtained on CASIA-IrisV3 data sets. So we got the plain text back from cipher text for all the genuine cases but decryption is not carried out for impostures.

The LDPC scheme decreases the Hamming Distance (HD) for genuine comparisons and majority voting scheme increases the HD for impostorcomparisons which results in improvement in the verification performance. This effect can be seen from the HD distribution curves in Figure8.To show how it is achieved, 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 in Figure 9.It can be noted that, 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%.



(a) Iris system without LDPC errorcorrection and majority voting scheme

(b) Proposed system with LDPC error correction and majority voting scheme

Fig 8: Effect of LDPC Error Correction and majority voting scheme on genuine (thick line) and impostor (dotted line) Hamming distance distributions for the CASIA-IrisV3 data sets

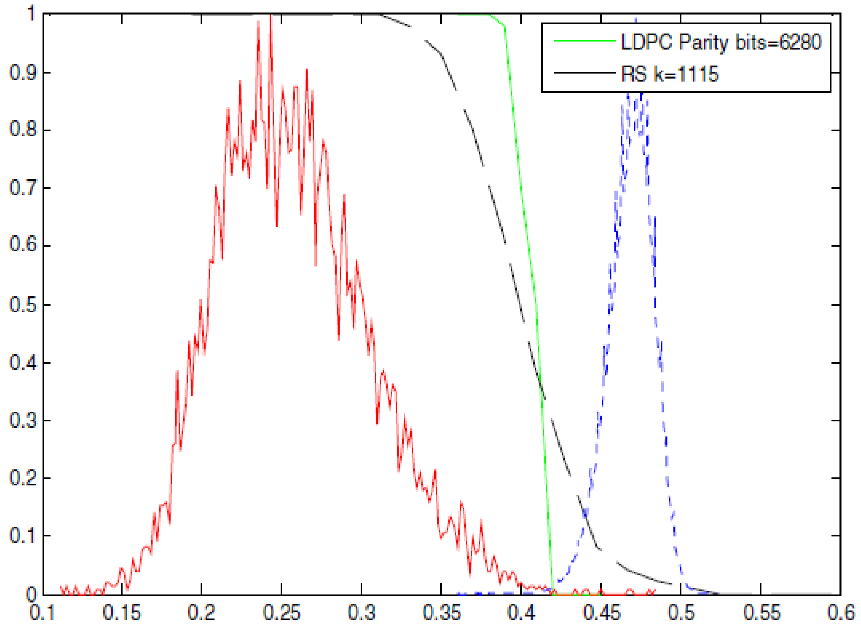


Fig 9: RS (with k=1115) and LDPC code (with 6280 parity bits) codes overlaid on top of the genuine and impostor normalized HD distributions

6. CONCLUSION

Canny edge detector and Hough transform are used to segment the iris in a simple and fast way. To eliminate Regions 1 type of noise i.e., obstructions due to eyelids and eyelashes in the lower and upper iris regions, 32^0 normalisation method is introduced. Compared with Daugman's method, a significant decrement of the error rates is 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. Since MD5 algorithm could produce identical hashes for two different messages if the initialization vector could be chosen and the security complexity of SHA-512 is 2^{256} under birthday attack, we use

SHA-512, so security of this scheme is very high. We use 512 bits AES scheme, which increases the number of rounds involved as number of rounds depends on the length of the key used when compared with other schemes. Thus the increase in length of the key gives the AESscheme strong resistance against the new attacks and has an acceptable speed of encryption and decryption.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.

7. ACKNOWLEDGMENTS

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

8. REFERENCES

[1] J. Daugman and C. Downing , "Epigenetic randomness, complexity, and singularity of human iris patterns", Proc. of the Royal Society, Biological Sciences, pp. 1737 – 1740, 2001.

[2] Ajay Kumar, Arun Passi, "Comparison and combination of iris matchers for reliable personal authentication", Pattern Recognition, vol. 43, pp. 1016–1026, 2010.

[3] S. Sanderson, J. Erbetta, "Authentication for secure environments based on iris scanning technology", IEE Colloquium on Visual Biometrics, 2000

[4] Y. Sutcu, S. Rane, J.S. Yedidia, S.C. Draper, A. Vetro, "Feature Extraction for a Slepian-Wolf Biometric System using LDPC Codes", IEEE International Symposium on Information Theory (ISIT), pp.2297- 2301, July 2008.

[5] A. Nagar, S. Rane, A. Vetro, "Privacy and Security of Features Extracted from Minutiae Aggregates", IEEE International Conference on Acoustics Speech and Signal Processing (ICASSP), pp.1826-1829, March 2010.

[6] X. Wu, N. Qi, K. Wang, D. Zhang, "A Novel Cryptosystem Based on Iris Key Generation", Fourth International Conference on Natural Computation (ICNC), vol.4, pp.53-56, October 2008.

[7] X. Wu, K. Wang, D. Zhang, "A Cryptosystem Based on Palmprint Feature", 19th International Conference on Pattern Recognition (ICPR), pp.1-4, December 2008.

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

[9] K. Seetharaman, R. Ragupathy, "Iris Recognition for Personal Identification System", Procedia Engineering, Elsevier, Accepted, 2012.

[10] Chinese Academy of Sciences' Institute of Automation (CASIA), Iris image database CASIA-Iris-V3, Available online: 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, May. 1993.

[12] National Institute of Standards and Technology, "Secure hash standard", Federal Information Processing Standards Publications FIPS PUB 180-1, 1995.

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

[14] National Institute of Standards and Technology, "Advanced Encryption Standard", Federal Information Processing Standards Publications FIPS PUB 197, pp. 1-51, November 2001.

[15] J. Daemen and V. Rijmen, "The Design of Rijndael: AES - The Advanced Encryption Standard", Springer-Verlag, Berlin Heidelberg, 2002.

[16] J. Daemen and V. Rijmen, "The Block Cipher Rijndael", Lecture Notes in Computer Science, vol.1820, pp.277-284, Berlin: Springer-Verlag, 2000.

[17] E. Biham, O. Dunkelman, and N. Keller, "Related-Key Boomerang and Rectangle Attacks", Lecture Notes in Computer Science, vol. 3494, pp. 507-525, Berlin: Springer-Verlag, 2005.

[18] N. Ferguson, J. Kelsey, S. Luckset *et al*. "Improved cryptanalysis of Rijndael", Lecture Notes in Computer Science, vol. 1978, pp. 213-230, Berlin:Springer-Verlag, 2001.

[19] Mohammed A. M. Abdullah, F. H. A. Al-Dulaimi, Waleed Al-Nuaimy, Ali Al-Ataby, "Smart card with iris recognition for high security access environment", IEEE, pp. 382-385, 2010.