Multimedia Tools and Applications
https://doi.org/10.1007/s11042-020-08971-x

A safe and secured iris template using steganography and cryptography

Oluwakemi Christiana Abikoye[1] · Umar Abdulraheem Ojo[2] · Joseph Bamidele Awotunde[1] · Roseline Oluwaseun Ogundokun[3]

Received: 11 May 2019 / Revised: 7 February 2020 / Accepted: 22 April 2020
Published online: 10 June 2020

Abstract

This study combines Cryptography (Twofish and Triple data decryption (3DES)) algorithms and Steganography (Least Significant Bits) to solve the problem of attacking or hacking biometric template for a malicious act, which has become a huge problem in the iris recognition system. Twofish and Triple data encryption are good and secured cryptography algorithms which are used to change readable secret data (plain image) into an unreadable format (cipher image) while least significant bits (LSB) is a steganography algorithm which embeds ciphertext/image directly into a cover image to produce an image known as stego image. In this work, Hough transform, Daugman rubber-sheet model and Log Gabor filter were used for iris image segmentation, normalization and feature extraction and the iris template generated was encrypted using 3DES and Twofish algorithms. The cipher image was then embedded into a cover image to produce stego image using LSB. The result of this work slightly changes the master file after embedding the secret image (stego file) that cannot be identified by the physical eyes and only a JPEG image was used as the master or cover file. The two levels of security technique provide high embedded capacity and eminence stego images that will able to withstand attackers.

Keywords Iris recognition · Cryptography · Steganography · Algorithm

✉ Roseline Oluwaseun Ogundokun
ogundokun.roseline@lmu.edu.ng

Oluwakemi Christiana Abikoye
abikoye.o@unilorin.edu.ng

Umar Abdulraheem Ojo
Ojo_raheem@yahoo.com

Joseph Bamidele Awotunde
Awotunde.jb@unilorin.edu.ng

Extended author information available on the last page of the article

1 Introduction

The utmost need for applications of biometrics-based authentication in access control, banking, healthcare among other in recent years are for reliable and accurate identification among users [12]. There are still various privacy and performance issues exist in biometrics-based system such as absence of revocability in biometric system techniques, lack of uniqueness, noisy data, sensitivity to outliers, and identity invasion [20]. Therefore, the two main parameters issue for biometric-based recognition systems are security and performance, thus there is need for a system that can achieve template protection and as well as performance improvement to produce strength to the biometric system [2]. To prevent any possibility of security theft and ensure the privacy of any user [2, 9], three criteria must be satisfied namely: diversity, revocability, and non-invertibility, [14]. Diversity implies that from original template several templates can be derive, revocability means that a new template must be issued if a stored protected template gets compromised and non-invertibility implies the original biometric template should not be improved from the protected one. There are still few worries raised because of the sensibility of biometric data to outliers in spite of the benefits of biometric-based authentication systems, like low performance caused due to intra-class variations and privacy invasion caused by information leakage [5].

Iris recognition is one of the utmost dependable, unique, steady and sure preference traits of all biometric system. Iris templates are extracted features from the iris sample, which are used during the verification process. Though the iris system enhances security, it is still prone to attacks. Imposters can break through the system deceitfully in the name of a genuine user. Hence, there is a need to secure the iris template.

Despite the existence of different images and data security technique, attackers or hackers are not relenting in developing new means of stealing the biometric template for malicious act. This has become huge problem in the iris recognition system.

Cryptography is the science and art of concealing the messages to introduce secrecy in information security. It provides several encoding schemes for achieving the security while communicating in a public domain or network. Steganography is related but adds another measurement to cryptography. In steganography, people not only want to protect the secrecy of an information by concealing it, but they also want to make sure any unauthorized person gets no evidence that the information even exists.

Through the use of cryptography the fundamental aspects of information security cannot be ensured, thus other methods like steganography are needed to guard against the threats such as denial of service or complete breakdown of information system. It can be difficult to access even for legitimate user at a crucial time of decision-making using a strongly encrypted, authentic, and digitally signed information in cryptography, so to reduce this during crucial decision-making a better algorithm has to be combined. A selective access control cannot be realized through the use of only cryptography, which is another fundamental need of information security, thus steganography was combined since administrative controls and procedures are required to be exercised for the same. Cryptography does not guard against the vulnerabilities and treats that emerge from the poor design systems, protocols and procedures. Hence, there is need to fixed it with another method through proper design and setting up of a defensive infrastructure. In steganography if image is subject to attack such as translation and rotation, message is hard to recover. Message is difficult to recover, if significant damage occurs to picture appearance in steganography and relatively easy to detect. The iris images can be vulnerable to the third party using only one of these techniques, thus the combination of

Steganography and Cryptography will enhance the security and robustness of iris template protection [21]. Therefore the algorithms were combined to enrich and complement each other.

This paper focuses only on the security problem of iris template which results into possible attacks on the iris templates. A hybridized system using cryptography (Triple Data Encryption Standard (3DES) and Two fish) algorithms and steganography (Least Significant Bits (LSB)) was used to secure iris template stored in a database.

2 Related work on biometric protection

Several systems have been projected to safeguard the biometric (iris) templates from any unlawful or unintentional tampering. Some of the suggested techniques are as follows:

Grover et al. [7] proposed a hybrid approach that is based on Run Length Encoding together with Steganography for Iris template security. The proposed technique accomplished a compression of the template together with providing two-fold security of the iris template. The original template is compressed in the proposed technique and the subsequent template is extra safeguarded when compared with the application of steganography only. The method fail to reported on the difficulty of access even for legitimate user at a crucial time of decision-making using a strongly encrypted, authentic, and digitally signed information in cryptography.

Taha et al. [21] conducted a survey on the use of steganographic and cryptographic techniques to achieve a hybrid system and reports the differences between both techniques. After the comparison between the two methods, it was established that steganography cannot be used as an alternate to Cryptography as each aspect has its individualities and uniqueness; Cryptography is the act of deciphering of encoded and enciphering messages, while Steganography are ways of concealing in a manner that its existence is completely hidden a secret message into a cover message.

Yang et al. [23] propose a system to provide user authentication and secure the original iris data called cancelable iris and steganography-based user authentication system. The paper established that most existing cancelable iris biometric systems need a user-specific key to guide feature transformation because this user-specific key is compromised, some useful information can be leaked and exploited by attackers to restore the original iris feature data. Therefore, to overcomes the risk, the paper enhances the system security by integrating an effective information-hiding technique called steganography. This increased the overall system security and complementing the protection offered by cancelable biometric techniques by concealing the user-specific key. The paper suggested the use of different types of transformation functions and studies how to properly hide the secret key.

Chai et al. [3] proposed a cancelable iris key binding scheme without Elliptic Curve Cryptography and an alignment-free. The system protects the binary biometric data IrisCodes, from security and privacy attacks through a strong and size varying non-invertible cancelable transform. Through the controllable hashed code length. The system provides flexibility in system storage and authentication speed. Also, the system included a fast key regeneration without re-enrollment or constant storage of seeds. But the proposed system fails to protect useful information that can be leaked and exploited by attackers through cancelable iris biometric systems.

Maček et al. [13] designed an iris based system in mobile banking using modular authentication framework. System keeps biometric templates encrypted or at least cancelable during all stages of storage, transmission and verification. As templates are stored on clients in encrypted form and decryption keys reside on bank's authentication server, original plaintext templates are unavailable to an adversary if the phone gets lost or stolen. The system considered only public key cryptography and pseudorandom number generator on small-sized templates without consider the disadvantaged of this method and application on smaller size, make it over simple compare to the propose system.

Anuja et al. [1] conducted a survey of iris template security using different techniques. The focuses are on the security aspects of iris biometric recognition system and based on various template protection systems. Template transformation methods, biometric cryptosystems, steganography, and visual cryptography among other are schemes proposed to provide security to iris templates in a database. The paper suggested that a single template protection scheme might not be sufficient to fulfill the needs of requests. Therefore, hybrid systems that are build use of the benefits of various template protection approaches should be created. Though some of these types of systems have been built but more robust system in this direction can still be create. Kayode et al. [8] secured a iris template using steganography technique. To decrease the dimensional inconsistencies between iris region areas, Hough transform (HT) was use for segmentation of iris region. The LSB algorithm was chosen to secure the iris template, but the system does not considered the drawbacks of the algorithm.

Zhao et al. [25] designed a system using local ranking to secure iris template. The iris data are first XORed (Exclusive OR operation) with an application-specific string; and divide the results into blocks and then partition the blocks into groups. The blocks in each group are ranked according to their decimal values, and original blocks are transformed to their rank values for storage. The paper extended the basic method to support the shifting strategy and masking strategy, which are two important strategies for iris recognition. But the system can still be enhanced by introduce steganography or cryptography to further secure the iris template. The authors suggested that future research can extend the proposed method to support some other widely used strategies in iris template security and recognition. Kumar et al. [10], designed a system that focused on generating cancellable iris templates by using discrete logarithm. The paper applied 1-D log Gabor filter on the iris images, iris codes were generated. A row vector is formed by appending next row to the previous one, thus the row vector is partitioned and converted into decimal vector. To achieve security or non-inevitability decimal, vector is subjected to discrete logarithm over a prime field. A hybridize system will still enhance the system by combining either steganography or cryptography with discrete algorithm.

Chaudhary and Nath [4] used steganography approach to protect the iris template with random number based entrench in LSB steganography to enhance security. Bit are embedded into LSB for more security of the blue pixel only The IrisCode bits are entrenched across three LSB randomly. The result shows that the template is more secure since the iris template were stored after embedding in cover image but not as original biometric. The performance of the system found to be better in terms of Peak Signal to Noise Ratio (PSNR) value, histogram plot and Receiver Operating Characteristic (ROC) curve plot. But the difficulty of the steganography in term of damage occurs to picture appearance and that it is relatively easy to detect. Li et al. [11] proposed iris image data hiding for privacy protection with a novel distortion function that measure the impact of the data embedded on iris recognition. Iris image was embedded with privacy personal data such that its impact on it is minimized. Distortion function was used to measure the impact of the data embedded. The result show that the system protect iris image with high recognition accuracy and the integrity was highly maintained with great embedded cost. But the proposed system failed to protect iris image from attackers.

Thanki et al. [22] used Discrete Wavelet Transform (DWT) hypothesis structure accompanied by a novel watermarking method for the safety of biometric template matcher modules of biometric system and on the communication channel between system database. One other researcher suggested another technique using a medium regulated cryptosystem for protecting template storage. The results from experiment show that the proposed system enhanced verification and authentication performance of the multibiometric system. But the system only protect the biometric template against spoofing and modification attack at system database is major issue in multibiometric system fails to protect the biometrics against diversity, revocability, and non-invertibility.

Emanuele et al. [6] used digital modulation paradigm to protect iris template with the properties of modulation constellations and turbo codes softecoding. The system guarantee proper security against brute-force and statistical attacks in terms verification rates and security. The proposed system was evaluated finding the effectiveness on the Interval subset of the CASIA-IrisV4 database. The system only considered the rotection of brute-force and statistical attacks but to protect the system against diversity and non-invertibility.

Ouda et al. [15] used one-factor cancelable biometric scheme for protecting IrisCodes. The proposed system satisfies the desires of non-invertibility, revocability, and diversity on iris template without deteriorating the recognition performance. The performance of the system was confirmed using CASIA-IrisV3-Interval. The result also shows the effectiveness of the system on the iris template, thus better than the token-based authentication systems and traditional knowledge-based.

Radman et al. [16] performed extraction of the optimum features of an iris using Principal Component Analysis (PCA) based on Discrete Wavelet Transformation (DWT). The system reduces the runtime needed for iris templates classification. Therefore, DWT behind PCA reduce the resolution of the iris template by converting the iris image into four frequency sub-bands. The authors only work on segmentations of iris image and not on the iris template security.

Zaheera et al. [24] used LSB to enhance the temopral-spatial domain algorithm as the new model to converts iris images to binary stream and hides into a proper lower bit plane The n will inserted into the binary values in the stego key from the plane that hidden the information; the iris codes, m where n is the input parameter in binary values. These values produce the output which is the new iris stego image after binary conversion. The system fails to guard against the vulnerabilities and treats that emerge from the poor design systems, protocols and procedures.

Revenkar et al. [19] used visual cryptography technique on the iris template. The technique was applied to secure the iris template from attack in a centralized database and created an extra layer of authentication to the users.

In view of the above, cryptography and steganography algorithms can be combined to improve information/data security because either cryptography or steganography alone confirms to be secure but vulnerable to attack. This research work solves these problems by developing a new scheme which improves the quality of stego images in addition to increasing the security of confidential image.

3 Methodology

This work combined Twofish, 3DES, and LSB to develop improved security for iris template in the database. The iris template is divided into two segments, segment A and segment B.

Segment A was encrypted with Twofish to produce a cipher image A while segment B is encrypted with 3DES to produce cipher B. Both ciphers were embedded into the cover image using LSB, this produces a stego image that will not display the cipher image while the cover image is visible. The process will be reversed to get the iris template. The step by step procedure of the entire system is as follows:

Step 1: Load iris image
Step 2: Generate an Iris Code/ Iris Template

(a) Segmentation of an Iris from an image
(b) Change the segmented iris into normalized iris
(c) Generate Iris Template/features from normalized iris

Step 3: Template is segmented into two A and B.
Step 4: Generate secret key using Twofish.
Step 5: Apply Twofish Encryption to segment A using the generated key.
Step 6: Generate secret key using Triple DES
Step 7: Apply 3DES Encryption to segment B using the generated key.
Step 8: Select cover image and change the cover image to binary format
Step 9: Manipulate the LSB of each pixel of the cover image and change the cover image of the LSB with each bit of secret image one by one.
Step 10: Output stego image
Step 11: Save the stego image.

3.1 Loading of iris image

The Chinese Academy of Science -Institute of Automation (CASIA) eye image database dataset was used for this research work. The iris images are extracted and stored in a database and the images were loaded from the database.

3.2 Generation of template

3.2.1 Iris segmentation algorithm using Hough Transform

Hough transform for circles detection This can be connected to distinguish the nearness of a circular shape in a given image. It is utilized to distinguish any shape or to find the iris in. The characteristic equation of a circle of radius r and center (a, b) is given by:

$$(x-a)^2 + (y-b)^2 = r^2 \tag{1}$$

This circle can be explained by the two following equations:

$$\begin{aligned} x &= a + r\cos(\theta) \\ x &= b + r\sin(\theta) \end{aligned} \tag{2}$$

It is used to work out the radius and center of the user and iris circles. To detect the edges in the iris image, the Canny edge detection operator is utilized.

Hough Algorithm

Step 1: Read Image and change image into a grayscale level.
Step 2: Minimal blurring was used to remove noise on the eye image to prevent making the boundary hard to visualize.
Step 3: Smoothing the image on the original intensity image was done using a filter.
Step 4: To detect the iris boundary, pupil center parameter is feed as detected in to circle Hough transform.

3.2.2 Iris Normalization algorithm

The next phase is to a fixed size of the image in order to allow comparisons by transforming the iris region. Generally, the dilation of a pupil from difference illumination resulted in stretches of the iris image. The remap of each iris region‘s point to the polar coordinates (r,θ) was done using Daugman’s rubber sheet model. Where r is the distance (0,1) and the angle θ is (0,2π).

The (x, y) Cartesian coordinates to the normalized non- concentric polar representation is the remapping of the iris region that is demonstrated as

$$l(x(r,\theta),y(r,\theta))\rightarrow l(r,\theta) \tag{3}$$

$$x(r,\theta) = (1-r)x_p\ (\theta) + rx_1\ (\theta) \tag{4}$$

$$y(r,\theta) = (1-r)y_p\ (\theta) + ry_1\ (\theta) \tag{5}$$

Iris region is represent by $l(x, y.)$

The original Cartesian coordinate is (x, y) and are:

The normalized polar coordinates is represent as (r, θ) are

The coordinates of the pupil and iris boundaries along the θ direction are represented by p_y, p, x, y and x, y. The accounting pupil dilation and size inconsistencies using the rubber sheet model is valuable for and the constant dimensions can be a normalized representation. But this model does not recompense for rotational irregularities.

Algorithm Daugman’s rubber sheet model is used for normalization of iris regions because the pupil can be non-concentric to the iris, the formula for remapping is required to rescale points, which depending on the angle around the circle. The formula is given as:

$$r' = \sqrt{\alpha\beta} \pm \sqrt{\alpha\beta^2 - \alpha\, r_l^2} \tag{6}$$

Where $\alpha\beta$ represent the centre of the pupil in relation to the centre of the iris as shown by X_o, y_o, r' represent the distance between the edge of pupil and the edge of iris at an angle, θ is around the region while Ir is the radius of the iris

Data points occur along the pupil border this was done in order to avoid non-iris region data from corrupting the normalized representation.

$$\begin{aligned} a &= O_x^2 + O_y^2 \\ \beta &= \cos\left[\pi - arcton\left[\frac{O_y}{O_x}\right] - \theta\right] \end{aligned} \tag{7}$$

3.2.3 Iris feature extraction using Log-Gabor Filters

Log-Gabor Filters Modification to Gabor function is the log Gabor function that served as an amendment to the basic Gabor function, which the frequency response is a Gaussian on a log frequency axis as defined. The Log-Gabor filter, which is the frequency response is shown as;

$$G(f) = exp\left[\frac{-(log(f/\ f_o))^2}{2(log(a/\ f_o))^2}\right] \tag{8}$$

Where f_0 is the centre frequency, and σ is the bandwidth of the filter

3.3 Iris template encryption

The iris template generated is divided into two segments. Segment A and B

Step 1: Load the iris template
Step 2: Divide the template into two to give template A and B

3.3.1 Encryption of segment a with 3DES algorithm

- Key dimension: 64 bits - 56 key bits and 8 parity bits.
- Effective key dimension: 56 bits.
- Block dimension: 64 bits.
- Rounds of algorithm: 16.
- Substitution and Permutation are the type of cipher.

The use of many and different length keys led to the use of Triple-DES algorithm by applied DES three times. The triple length key is assumed of having three 56-bit keys represented as K1, K2, K3. Then the encryption is as follows:

- Encrypt with K1
- Encrypt with K2
- Encrypt with K3

3.3.2 Encryption of segment B with two-fish algorithm

Step 1.

1. Input A as much as 128 bits would be divided into four sections, each for 32 bits using little-endian convention.

2. Two parts of the bits will be the right part, the two parts of the other bits will be left.
3. Bit-XOR input in advance with the four key parts (whitening).

$$R_{0,1} = p \oplus K_i; i = 0, \ldots, 3 \tag{9}$$

Where M is the key, Mi means the sub key where i = 0, ...,3.

4. The first two 32 bits (X_0& X_1) are passed into an F-function to produce F_o and F_1.

i. F_0 is XORed with R_2 and the result is rotated to the right by one bit to give Y_2.
ii. R_3 is first rotated to the left by one bit and the result is XORed with F_1 to produce C_3.
iii. The new result is $X_{0,}$ $X_{1,}$ Y_2 and $Y_{3.}$ The result is swapped (to give Y_2, Y_3, X_0& X_1) before it passed into the next round.

$$\left(F_{r.0,}F_{r,1}\right) = F\left(X_{r,0,}X_{r,1,}r\right) \tag{10}$$

$$X_{r+1,0} = ROR\left(X_{r,2}\oplus F_{r.0,}1\right) \tag{11}$$

$$X_{r+1,0} = ROL\left(X_{r,3,}1\right)\oplus F_{r.1} \tag{12}$$

$$X_{r+1,2} = X_{r,0} \tag{13}$$

$$X_{r+1,3} = X_{r,1} \tag{14}$$

ROR and ROL are values that rotate their initial argument (a 32-bit word) left or right by the number of bits showed by their second argument and r = 0,. .., 15. The process is repeated 16 times, and that is why it is called the Twofish rounds.

5. Function g, which consists of four steps:

- The word X is the input that divide into four bytes.
- The four bytes runs through its own key-dependent called S-box. The S-box is bijective, which takes 8 bits of input, and generates 8 bits of output.
- By using the field GF(2^8) for the computations, the four outcomes are shown as a vector of length 4 over GF(2^8), and times by the 4 × 4 MDS matrix.
- The solution of g is the output vector which is interpreted as a 32-bit word.

6. S boxes Key: Two fish constructs four bijective key-dependent 8 × 8-bit S-boxes utilizing a key (shown for a 128-bit key) as show below:

$$s0(x) = p1\left[p0\left[p0[x]\wedge k0\right]\wedge k1\right] \tag{15}$$

$$s1(x) = p1\left[p0\left[p1[x]\wedge k2\right]\wedge k3\right] \tag{16}$$

$$s2(x) = p1\left[p1\left[p0[x]\wedge k4\right]\wedge k5\right] \tag{17}$$

$$s3(x) = p0\left[p1\left[p1[x]\wedge k6\right]\wedge k7\right] \tag{18}$$

The two fixed 8-bit permutations were represented by p0 and p1.

Table 1 Evaluation of steganography and cryptography algorithms

NO	BASE	Steganography without cryptography	Steganography with cryptography technique
1.	Security	One level security	Two level security
2.	Key size	No key present	Random size of key
3.	Steps involve in encryption of data	No step	Depend on the key size
4.	Brute force attack	No need	Very hard to attack

7. MDS Matrix:

   a) v = Mu. Which implies

4 × 4 matrix multiply over GF (256)

b) The main diffusion mechanism in Twofish is Maximum Distance Separable (MDS) property assurances that there are at least five non-zero bytes in u and v.

c) For reserves MDS property for single byte, the Minimum binary Hamming weight output for single byte input difference is 8 bits. But the input difference even after single-bit "rotate right" of v (Which is treated as a 32-bit quantity).

8. The simple, fast, and reversible diffusion mechanism used is the Pseudo-Hadamard Transform (PHT), and is as follows:

$$A^{'} = A + B$$

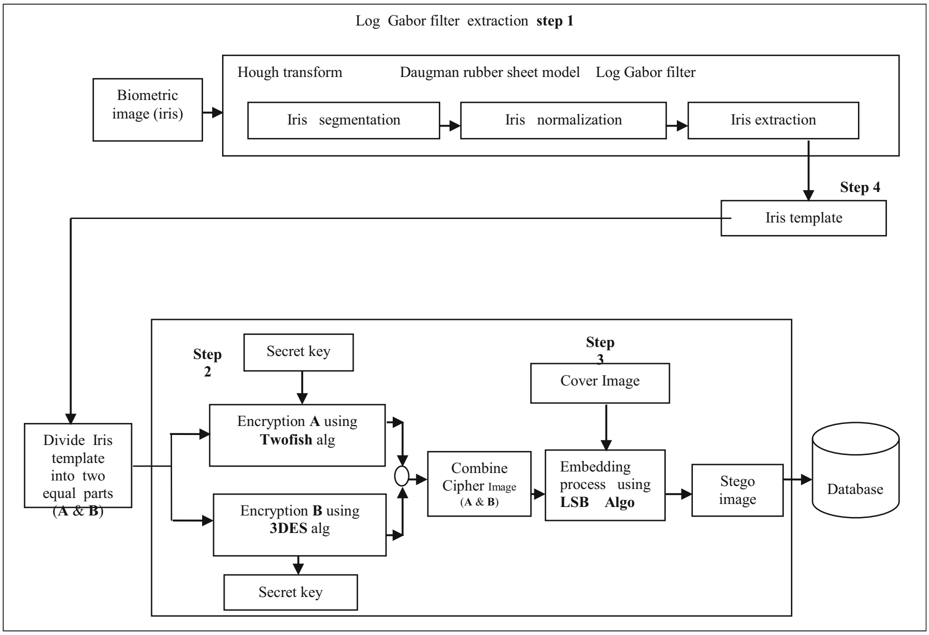

Log Gabor filter extraction step 1
Hough transform
Daugman rubber sheet model
Log Gabor filter
Biometric image (iris)
Iris segmentation
Iris normalization
Iris extraction
Step 4
Iris template
Step 2
Secret key
Encryption A using Twofish alg
Encryption B using 3DES alg
Secret key
Divide Iris template into two equal parts (A & B)
Combine Cipher Image (A & B)
Step 3
Cover Image
Embedding process using LSB Algo
Stego image
Database

Fig. 1 Block diagram for encryption process

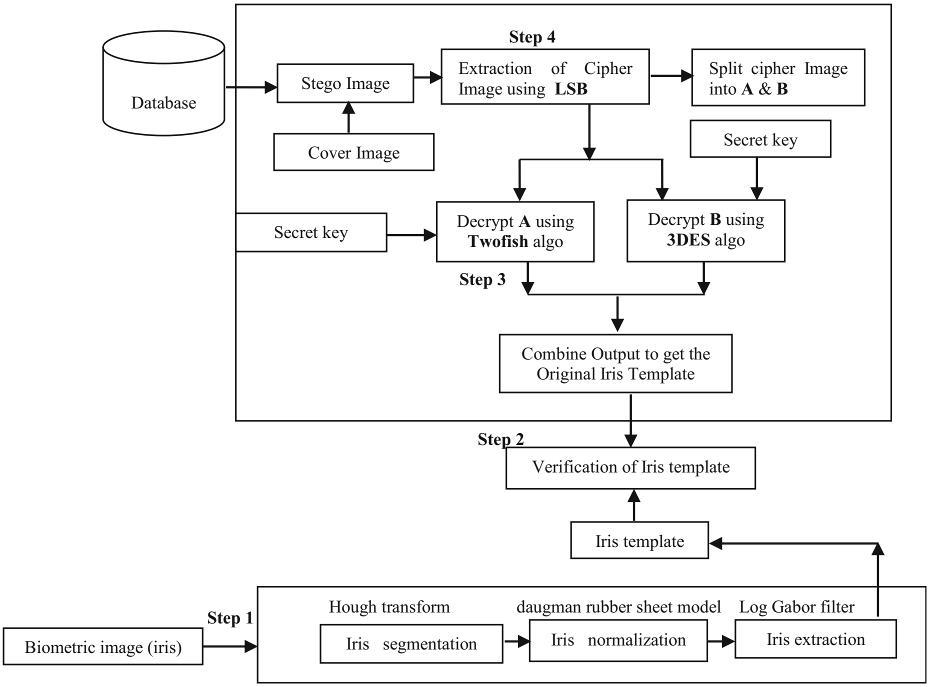

Database
Stego Image
Cover Image
Step 4
Extraction of Cipher Image using **LSB**
Split cipher Image into **A** & **B**
Secret key
Secret key
Decrypt **A** using **Twofish** algo
Decrypt **B** using **3DES** algo
Step 3
Combine Output to get the Original Iris Template
Step 2
Verification of Iris template
Iris template
Step 1
Biometric image (iris)
Hough transform
Iris segmentation
daugman rubber sheet model
Iris normalization
Log Gabor filter
Iris extraction

Fig. 2 Block system for decryption

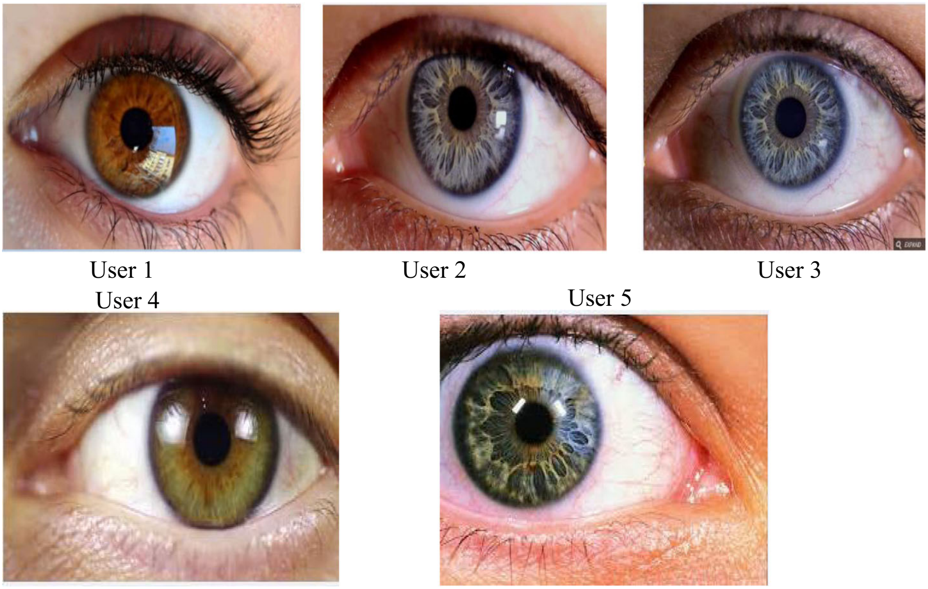


Fig. 3 Iris samples

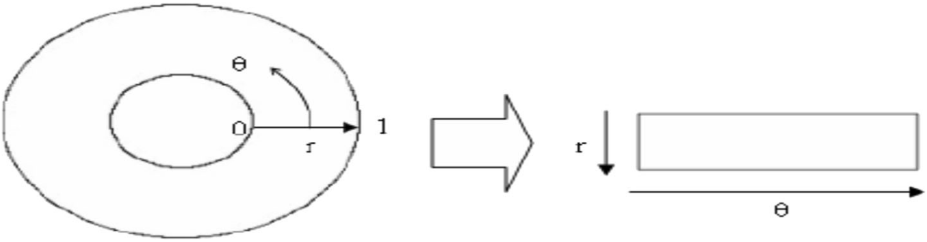
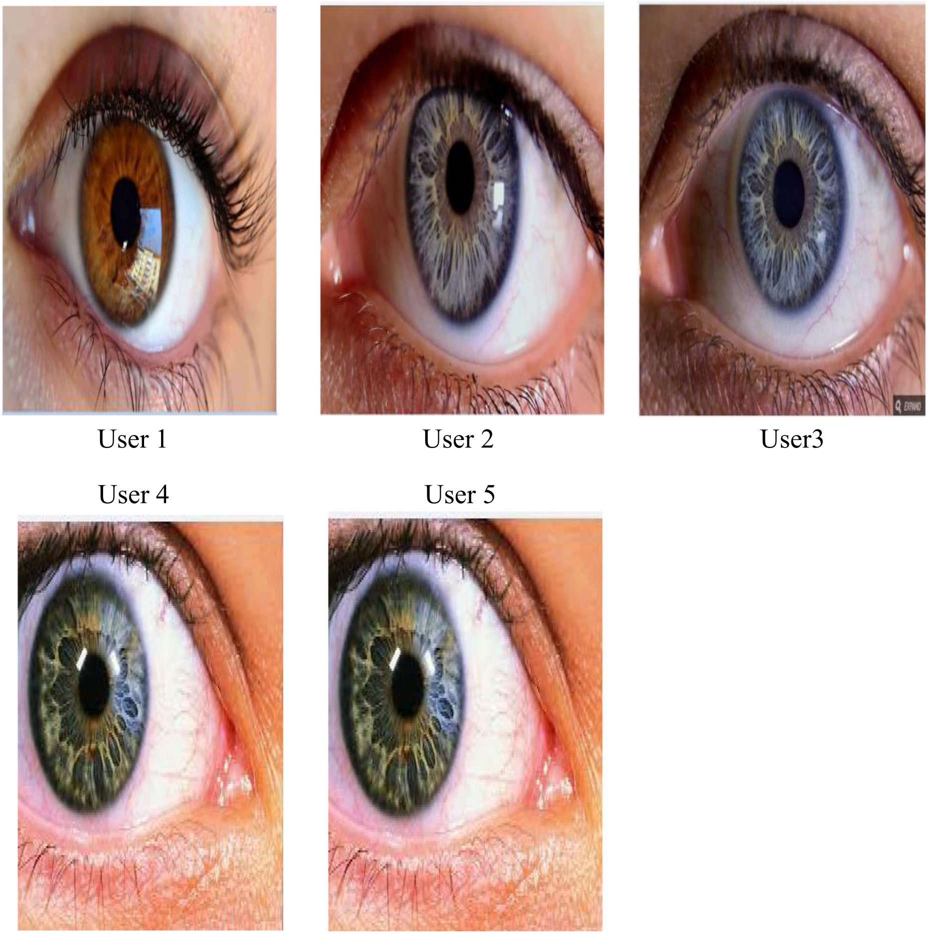


Fig. 4 Iris normalization

$$B^{'} = A + B^{*}2$$

Twofish utilize 32-bit PHT on pairs on MDS outcome.


User 1

User 2

User3

User 4

User 5

Fig. 5 Sample iris images

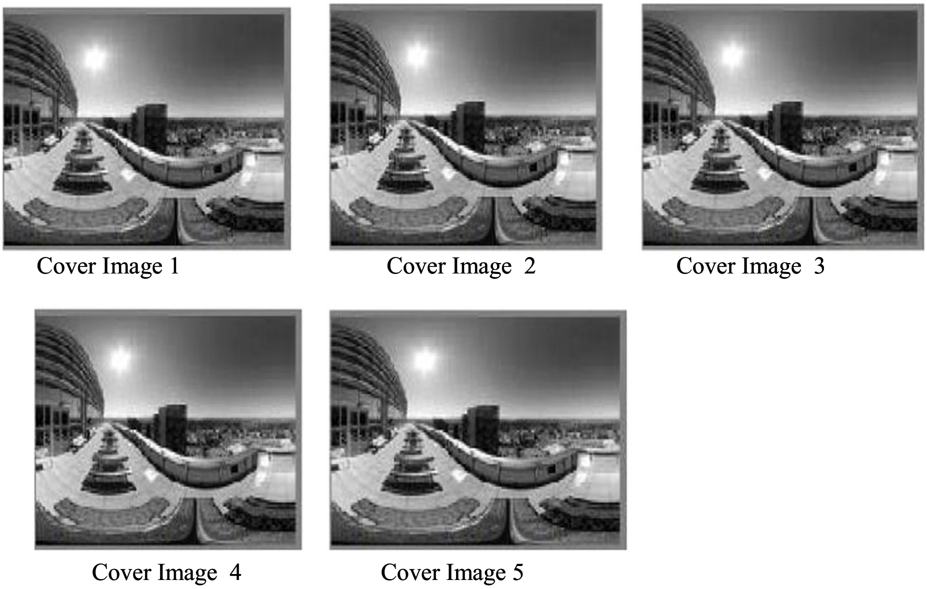


Fig. 6 Sample cover images

9. All the four 32-bit amount in the block is used once in every of the eight possible bit positions (mod 8). 1-bit Rotation is utilized in each Twofish round to split up the byte-aligned nature of other operations.
10. The subkeys are based on equal building as key dependent S-boxes, it can be pre computed on the fly.

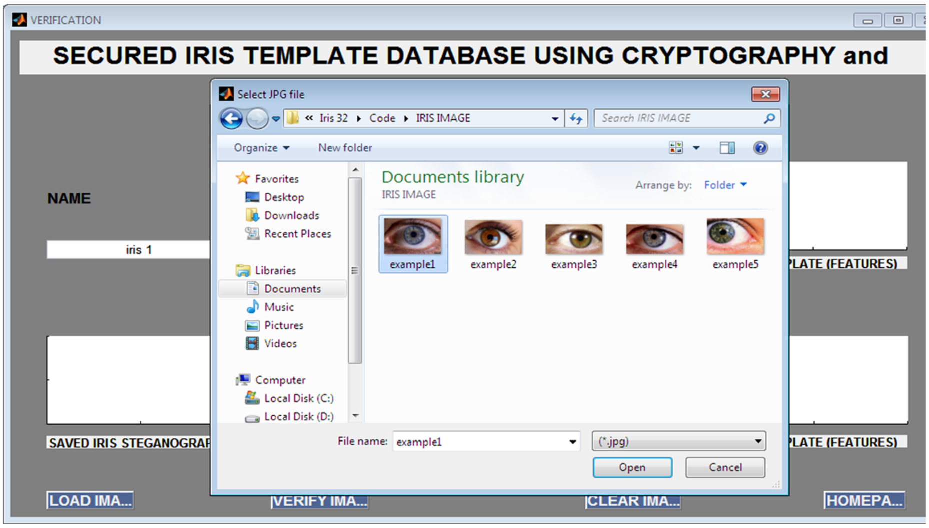
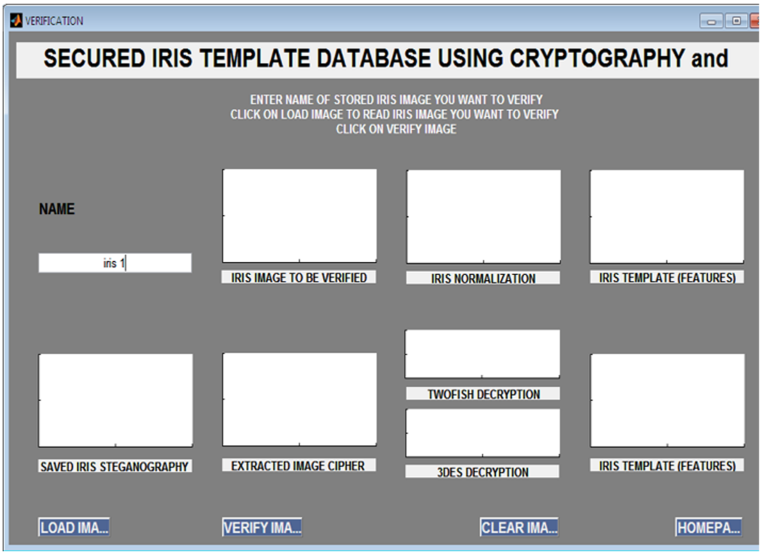


Fig. 7 Loading of iris images

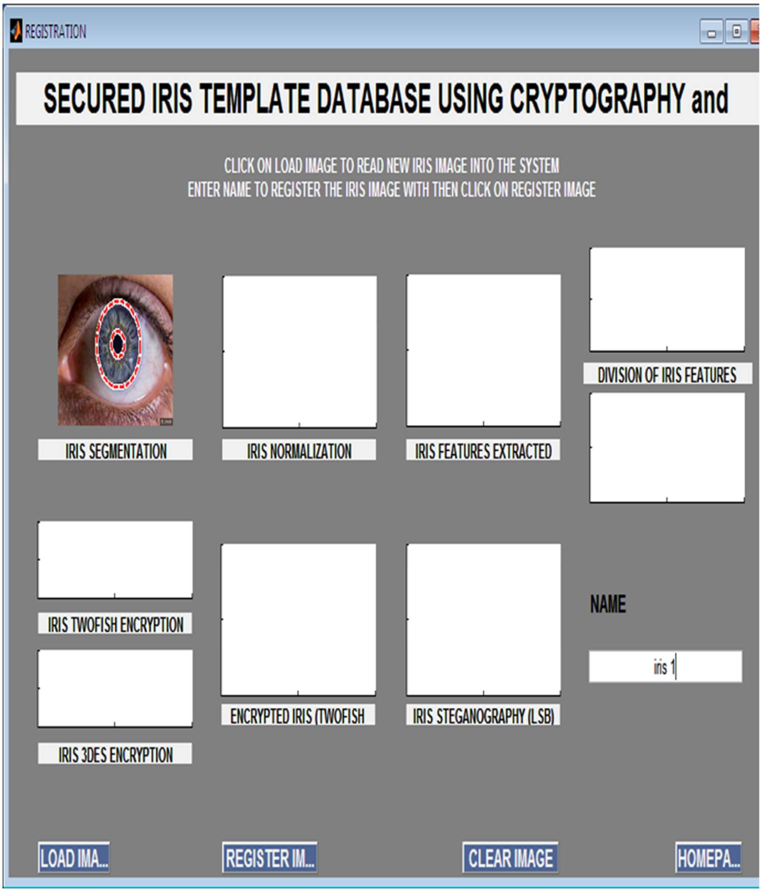


SECURED IRIS TEMPLATE DATABASE USING CRYPTOGRAPHY and

ENTER NAME OF STORED IRIS IMAGE YOU WANT TO VERIFY
CLICK ON LOAD IMAGE TO READ IRIS IMAGE YOU WANT TO VERIFY
CLICK ON VERIFY IMAGE

NAME: iris 1

Fig. 8 Naming of iris image

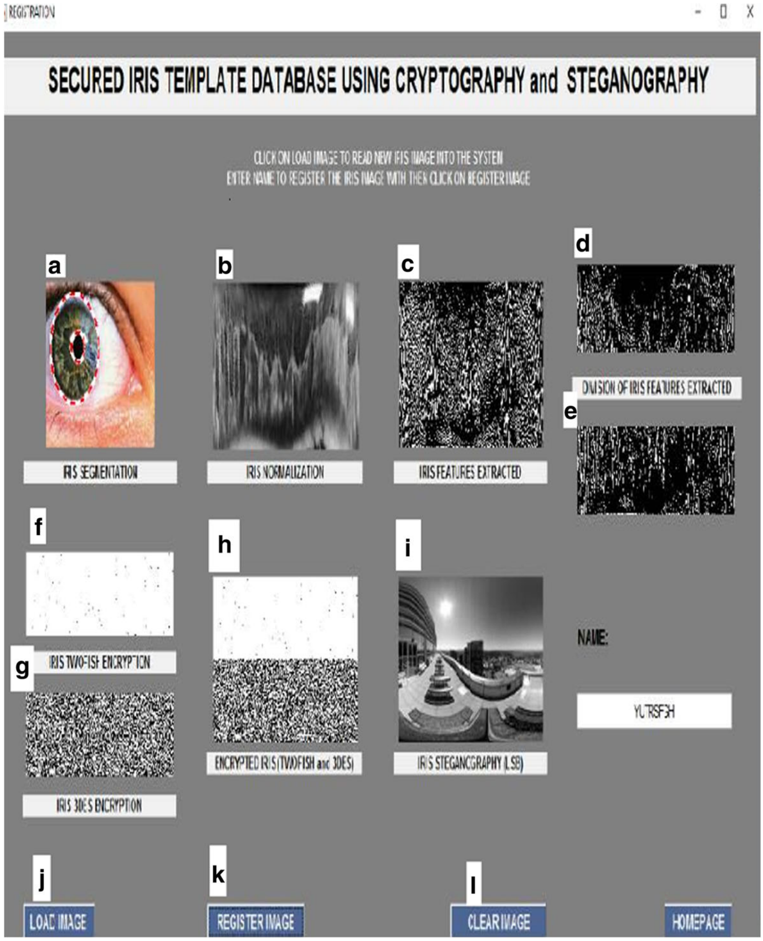


SECURED IRIS TEMPLATE DATABASE USING CRYPTOGRAPHY and

CLICK ON LOAD IMAGE TO READ NEW IRIS IMAGE INTO THE SYSTEM
ENTER NAME TO REGISTER THE IRIS IMAGE WITH THEN CLICK ON REGISTER IMAGE

NAME: iris 1

Fig. 9 Loaded iris image



REGISTRATION

SECURED IRIS TEMPLATE DATABASE USING CRYPTOGRAPHY and STEGANOGRAPHY

CLICK ON LOAD IMAGE TO READ NEW IRIS IMAGE INTO THE SYSTEM
ENTER NAME TO REGISTER THE IRIS IMAGE WITH THEN CLICK ON REGISTER IMAGE

NAME: YUTRSF3H

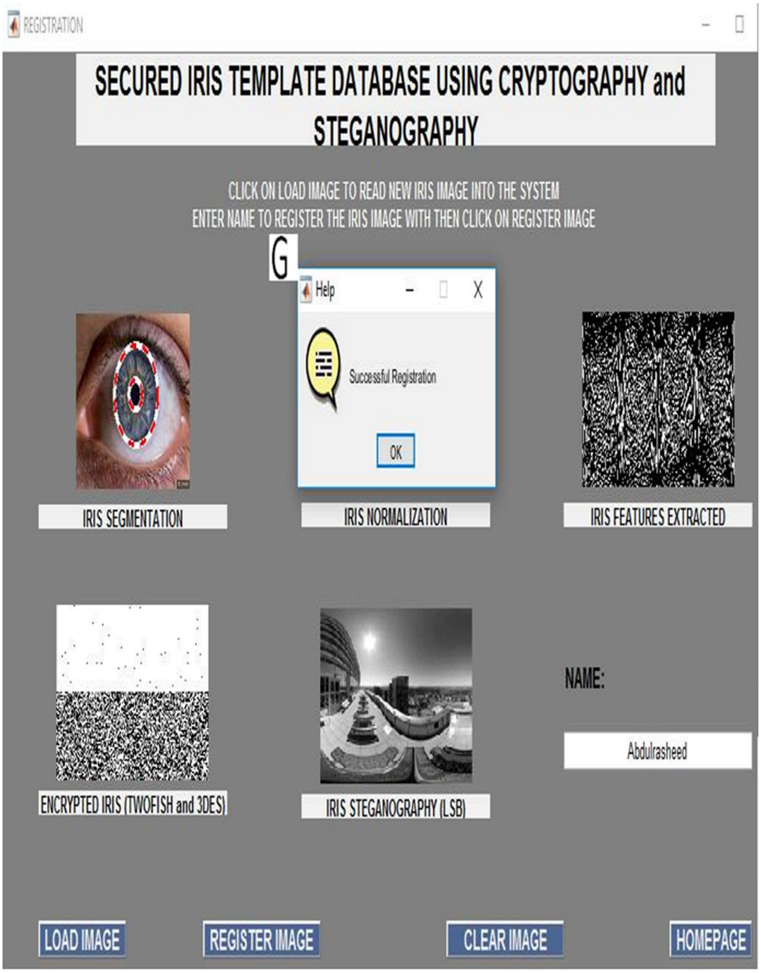
Fig. 10 a: Stego iris template generated for user 1. b: Registration process for User 1

3.4 Embedding of cipher image

The encrypted iris cipher image A and B was combined to get cipher image C and embedded into a cover image using LSB, then the stego image was loaded into the database (Table 1).

Algorithm to embed the secret message using least significant bits

Step 1: Get the cover image and the two ciphers images
Step 2: Change to binary format the two ciphers and cover image.
Step 3: Compute LSB of each pixel of the cover image.
Step 4: Change and substitute the cover image of the LSB with each bit of two ciphers one by one.
Step 5: Write Stego image



SECURED IRIS TEMPLATE DATABASE USING CRYPTOGRAPHY and STEGANOGRAPHY

CLICK ON LOAD IMAGE TO READ NEW IRIS IMAGE INTO THE SYSTEM
ENTER NAME TO REGISTER THE IRIS IMAGE WITH THEN CLICK ON REGISTER IMAGE

Successful Registration

NAME: Abdulrasheed

Fig. 10 (continued)

4 Result and discussions

This work implements a secured iris template database using the combination of Twofish, 3DES and Least Significant Bits. MATLAB 2013A was used to designed the system, the platform is preferred for it powerful integral mathematical, signal and image processing functions. Iris images were selected from CASIA Iris Image Database V3.0. After performing segmentation, normalization and feature extraction the iris template is created, a unit eye image is selected from CASIA database for enrollment. Iris template is then divided into two portions, part one and part two. The first part is then secured using Twofish and the second using 3DES and the encrypted templates are then hidden in an image using LSB to produce an image called stego images (Figs. 1, 2, 3, 4, 5 and 6).

4.1 Sample of iris

4.2 Samples of stego image

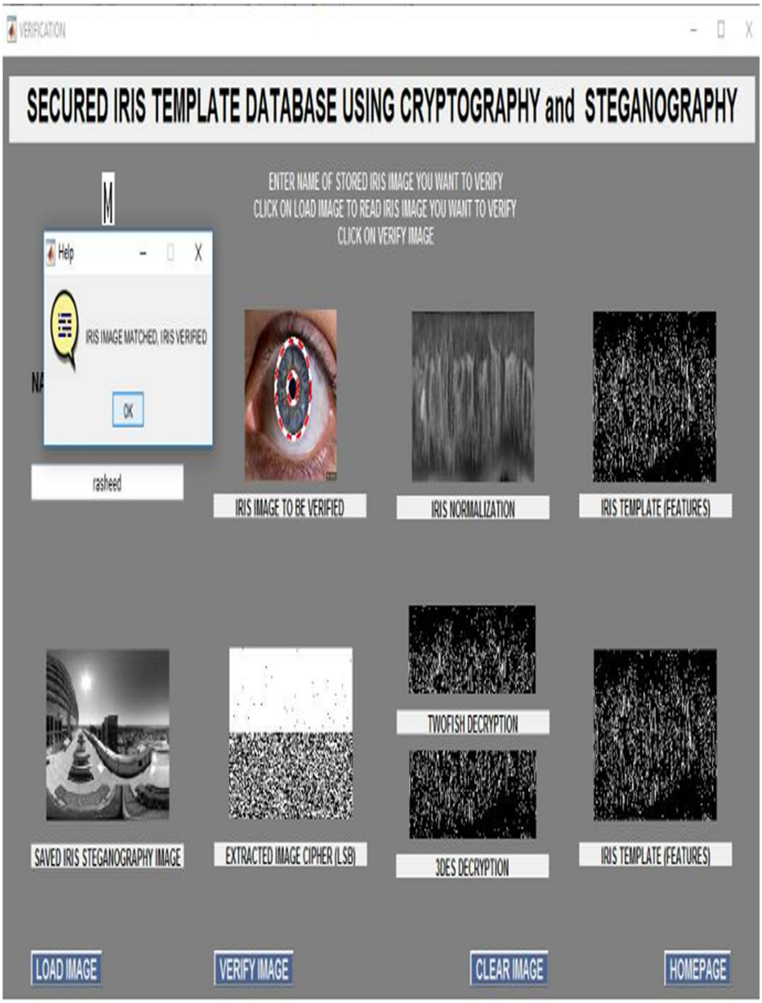
4.2.1 Enrollment stage

Figure 7 shows the interface that allows the system to load iris image for necessary registration of user's name, image processing and encryption.

Figure 8 shows the interface where the iris image loaded from the database will be named.

Figure 9 shows the loaded iris image and its name that will be stored.

In Fig. 10, Image A represents the segmented iris image from the original iris image. Image B represents the normalized image of the segmented iris image. Image C represents the template extracted from the normalized iris. Image D and E are the division of image C.



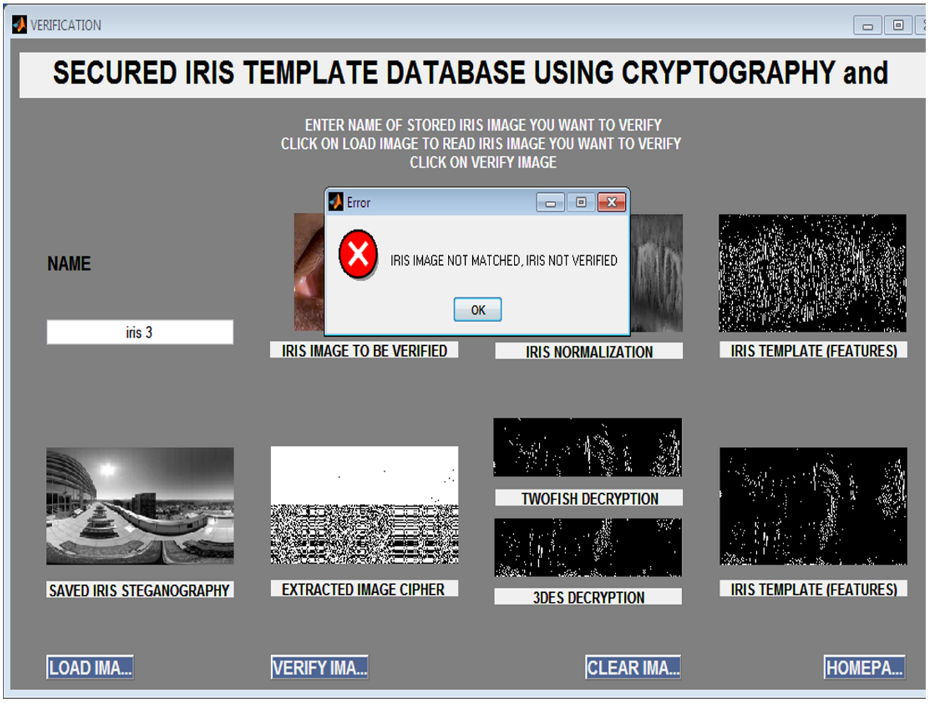
SECURED IRIS TEMPLATE DATABASE USING CRYPTOGRAPHY and STEGANOGRAPHY

ENTER NAME OF STORED IRIS IMAGE YOU WANT TO VERIFY
CLICK ON LOAD IMAGE TO READ IRIS IMAGE YOU WANT TO VERIFY
CLICK ON VERIFY IMAGE

IRIS IMAGE MATCHED, IRIS VERIFIED

rasheed

Fig. 11 Matching & verification process for user 1



VERIFICATION

SECURED IRIS TEMPLATE DATABASE USING CRYPTOGRAPHY and

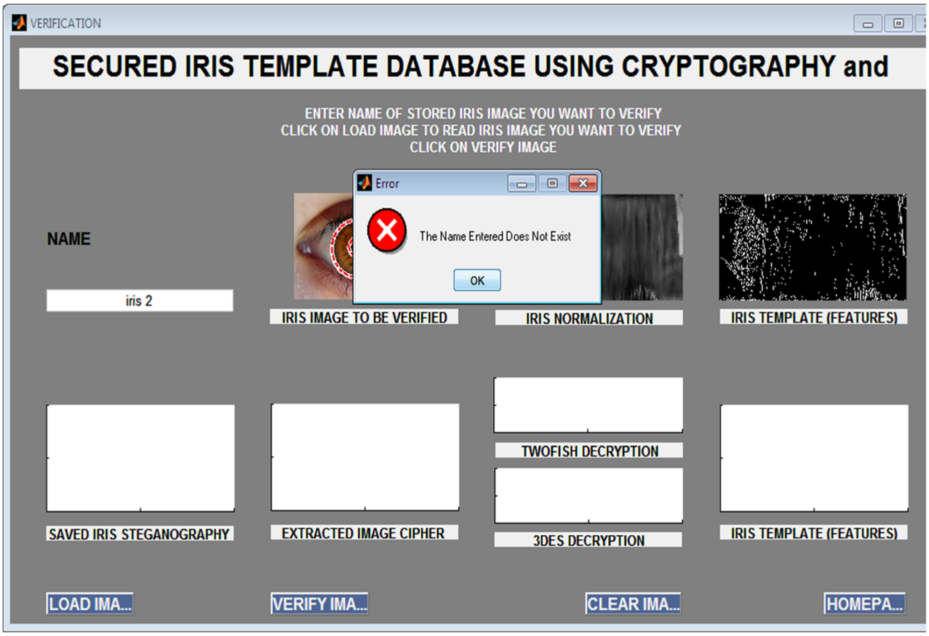
ENTER NAME OF STORED IRIS IMAGE YOU WANT TO VERIFY
CLICK ON LOAD IMAGE TO READ IRIS IMAGE YOU WANT TO VERIFY
CLICK ON VERIFY IMAGE

Error

IRIS IMAGE NOT MATCHED, IRIS NOT VERIFIED

NAME: iris 3

Fig. 12 Iris image not matched



VERIFICATION

SECURED IRIS TEMPLATE DATABASE USING CRYPTOGRAPHY and

ENTER NAME OF STORED IRIS IMAGE YOU WANT TO VERIFY
CLICK ON LOAD IMAGE TO READ IRIS IMAGE YOU WANT TO VERIFY
CLICK ON VERIFY IMAGE

Error

The Name Entered Does Not Exist

NAME: iris 2

Fig. 13 Wrong name not matched

Table 2 Summarized results of the performance comparison

Methods	GAR (%)	FAR (%)
[18]	95.08	0.00%
[15]	96.00	0.00%
[25]	98.11	0.01%
[17]	95.00	0.01%
Proposed system	98.70	0.00%

Image F is the encrypted template with TwoFish algorithm while Image G is encrypted with 3DES. Image H is the combination of Image F and G. Image I is the embedded image of H. Image I is called the stego image. Image I is then stored in the database.

4.2.2 Matching and verification of image

Figure 11 shows the interface that allows users to load stego image for necessary matching and verification. Stego undergo reverse order of the process to produce the template for matching and verification. Image M show that the presented image matches the stored template in the database

Figure 12 shows a situation where wrong fake iris is loaded in to the system.

Figure 13 shows a situation where wrong user enter name in to the system.

5 Performance comparison

The result of the proposed system was compare with some existing iris template protection that use different methods. Genuine Acceptance Rate (GAR) was used as the benchmark for the performance evaluation. The probability of confusing two identities is FAR, and the GAR is defined as follows

$$\mathrm{GAR} = 1{-}\mathrm{FRR} \tag{19}$$

where the rejection probability of the authorized users is the false reject rate (FRR),.

Rathgeb and Uhl [18] successfully applied fuzzy commitment scheme to iris after conducted a survey on compiling the key binding methods in iris biometric cryptosystems. Afterward analyzing the error distribution of IrisCodes of different iris recognition algorithms, performance evaluation on the iris based fuzzy commitment scheme was applied and recorded a GAR of 95.08% at 0.00% FAR. Zhao et al. [25] applied local ranking to protect iris template reported a GAR of 98.11% at 0.01% FAR using CASIA-IrisV3-Interval dataset for evaluation. Rathgeb et al. [17] in their recent work improve the security and performance of the fuzzy vault scheme using multi-biometrics and recorded GAR of 95.00% achievement with security levels at 0.012% FAR and for the fuzzy vault using single iris recorded a lower GAR of 90.00% with similar security levels at 0.00% FAR. Ouda et al. [15] in their work recorded GAR of 96.00% at 0.00% FAR. Summarized results of the performance comparison of iris template preotection methods are shown in Table 2 below.

To validate the performance of our method, we compare our proposed hybrid system using cryptography (3DES) with Two fish and steganography (LSB) with other recent methodologies in literature. As described in performance evaluation, it can be observed that the proposed method performs optimally than the other approaches with respect to GAR and FAR in Table 2. The superior performance is due to the hybrid of two algorithms, thus helps in revocability and separability between the genuine and imposter distributions. This also proves that the proposed method is less sensitive to the outliers since the separability between distributions is significantly higher than the existing methods.

6 Conclusion

Iris recognition is one of the strongest biometric in existence with several practical uses in many fields, which including live passwords and forensics. Governments use its codes as matchless code to identify a person. The biometric (iris recognition) system is considered as secured, matchless and possible, but is still prone to some vulnerability. Different attacks like indirect and direct attacks can be performed in iris templates. The main shortcoming of biometrics is that at anytine the biometric information or template is stolen, it is until the end of time stolen and unable to be is that once biometric data or template is stolen, it is stolen forever and cannot be reissued because of that; template security has come to be crucial issues in biometric recognization techniques. Therefore, constant review of the existing security measures is needed to overpower the security threat posed by the eavesdroppers. In this study, securing iris template before it is stored in database is done using Twofish, Triple Data Encryption system algorithm and Least Significant Bits of image steganography. The developed system performs two main operations which are securing and retrieving. Each of these operations accept two inputs, iris template and cover image for securing, stego image and cover image for retrieving. At the end of each successful operation a single output is obtained that is, stego image and iris template form securing and retrieving operation respectively. The negligible changes in the master file after embedding the secrete text message or stego file cannot be identify by the human eyes. In conclusion, it is shown that the system strength lies in the implemented steganography algorithm which ensures a highly secured iris template from un-authorized access. With the level of security of the system, the problem of panicking with information in transit or information stored in the database will be reduced to the barest minimum if not totally eradicated in information communication technology environment. The application of steganography and cryptography in iris recognition brings about stronger security platform

References

1. Anuja JS, Praveen K, Amritha PP (2019) A survey of Iris template security aspects. International Journal of Pure and Applied Mathematics 119(15):1471–1481
2. Canuto AM, Pintro F, Xavier-Junior JC (2013) Investigating fusion approaches in multi-biometric cancellable recognition. Expert Syst Appl 40(6):1971–1980
3. Chai TY, Goi BM, Tay YH, Jin Z (2019) A new design for alignment-free chaffed cancelable Iris key binding scheme. Symmetry 11(2):164
4. Chaudhary S, Nath R (2015) A new template protection approach for Iris recognition, 4th international conference on reliability. Inf Technol Opt
5. Rudresh D, Somnath D (2019) A novel hybrid score level and decision level fusion scheme for cancelable multi-biometric verification. Appl Intell 49(3):1016–1035
6. Emanuele M, Patrizio C, Alessandro N (2014) Iris template protection using a digital modulation paradigm. Int Conf Acoustic Speech Signal Process 3759–3763

7. Grover D, Devi K, Gupta P (2016) A Two_Fold security approach an Iris template. International Journal of Pharmacy and Technology 8(3):19094–19103
8. Kayode SY, Olaniyi AS, Olaolu AM, Babatunde AN (2018) Development of Iris biometric template security using steganography. Comput Inf Syst 22(3)
9. Kelkboom EJC, Zhou X, Breebaart J, Veldhuis RNJ, Busch C (2009) Multialgorithm fusion with template protection. In: 2009 IEEE 3rd International Conference on Biometrics: Theory, Applications, and Systems. pp 1–8
10. Kumar MM, Prasad MV, Raju USN (2018) Iris template protection using discrete logarithm. In proceedings of the 2018 2nd international conference on biometric engineering and applications (pp 43–49). ACM
11. Li S, Chen X, Wang Z, Qian Z, Zhang X (2018) Data hiding in Iris image for privacy protection. IETE technical review 35(sup 1):34–41
12. Li SZ, Jain AK (2009) Encyclopedia of biometrics, vol. 1. Springer Science & Business Media
13. Maček N, Adamović S, Milosavljević M, Jovanović M, Gnjatović M, Trenkić B (2019) Mobile banking authentication based on cryptographically secured Iris biometrics. Acta Polytechnica Hungarica 16(1)
14. Nandakumar K, Jain AK (2015) Biometric template protection: bridging the performance gap between theory and practice. IEEE Signal Process Mag 32(5):88–100
15. Ouda O, Tsumura N, Nakaguchi T (2010) Tokenless cancelable biometrics scheme for protecting iris codes. In 2010 20th international conference on pattern recognition (pp 882–885). IEEE
16. Radman A, Jumari K, Zainal N (2013) Fast and reliable iris segmentation algorithm. IET Image Process 7(1):42–49
17. Rathgeb C, Tams B, Wagner J, Busch C (2016) Unlinkable improved multi-biometric iris fuzzy vault. EURASIP J Inf Secur 2016(1):26
18. Rathgeb C, Uhl A (2011) The state-of-the-art in iris biometric cryptosystems. State of the art in Biometrics 179–202
19. Revenkar PS, Anjum A, Gandhare W (2010) Secure Iris authentication using visual cryptography. International Journal of Computer Science and Information Security 7(3):217–221
20. Sadhya D, Singh SK (2018) Construction of a bayesian decision theory-based secure multimodal fusion framework for soft biometric traits. IET Biometrics 7(3):251–259
21. Taha MS, Rahim MSM, Lafta SA, Hashim MM, Alzuabidi HM (2019) Combination of steganography and cryptography: a short survey. In IOP conference series: materials science and engineering (Vol 518, no 5, p 052003). IOP publishing
22. Thanki R et al (2015) Multibiometric template security using CS theory – SVD based fragile watermarking technique. WSEAS Trans Inf Sci Appl 12(1):1–10
23. Yang W, Wang S, Hu J, Ibrahim A, Zheng G, Macedo MJ, Johnstone MN, Valli C (2019) A cancelable iris- and steganography-based user authentication system for the internet of things. Sensors 19(13):2985
24. Zaheera ZA, Mazani M, Abdul SS (2011) A new model of securing Iris authentication using steganography, conference on Communications in Computer and Information Science, part I. CCIS 179:547–554
25. Zhao D, Fang S, Xiang J, Tian J, Xiong S (2018) Iris template protection based on local ranking. Security and Communication Networks 2018. https://doi.org/10.1155/2018/4519548

Oluwakemi Christiana Abikoye is an Associate Professor at the Department of Computer Science, Faculty of Communication and Information Sciences, University of Ilorin, Ilorin, Nigeria. She received her B.Sc, M.Sc. and Ph.D degrees in Computer Science from University of Ilorin, Ilorin. She is the author or coauthor of more than 50 papers in international national and local refereed journals and conference contributions. Her research interests include Cryptography, Computer and Communication Network (Cyber) Security, Biometrics, Human Computer Interaction and Text and Data Mining.

Umar Abdulraheem Ojo is currently a Computer lecturer in the Department of Computer Science in FCT college of Education Zuba, Abuja, Nigeria. He holds an NCE in Mathematics/Computer at The Federal College of Education (Tech) Bichi-Kano, Nigeria 2002 and B.Tech. Mathematics/Computer Science at Federal University of Technology, Minna, Niger State, Nigeria in 2007 and M.Sc in Computer Science in University of Ilorin, Ilorin 2016.

Joseph Bamidele Awotunde (Ph.D) is a Lecturer at the Department of Computer Science, Faculty of Communication and Information Sciences, University of Ilorin, Ilorin, Nigeria. He received the B. Tech. Mathematics/Computer Science from Federal University of Technology, Minna, Nigeria Ph.D. and M.Sc. degrees in Computer Science from University of Ilorin, Ilorin, Nigeria. He is the author or coauthor of more than 30 papers in international, national and local refereed journals and conference contributions. His research interest includes Social Computing, Biometrics, Artificial Intelligence, Information Security, and Information Science.

Roseline Oluwaseun Ogundokun is a Lecturer at the Department of Computer Science, College of Pure and Applied Sciences, Landmark University, Omu Aran, Kwara State, Nigeria, She holds Bachelor of Science in Management Information System from Covenant University, Ota; Master of Science in Computer Science from the University of Ilorin, Ilorin; Post Graduate Diploma in Education (PGDE) from the National Teachers' Institute (NTI), Kaduna and; currently a PhD student in the Department of Computer Science, University of Ilorin, Ilorin. Her research interest includes Steganography and Cryptography, Information Security, Data Mining, Information Science and Bioinformatics.

Affiliations

Oluwakemi Christiana Abikoye[1] • **Umar Abdulraheem Ojo**[2] • **Joseph Bamidele Awotunde**[1] • **Roseline Oluwaseun Ogundokun**[3]

[1] University of Ilorin, Ilorin, Nigeria

[2] FCT College of Education, Zuba, Abuja, Nigeria

[3] Landmark University, Omu Aran, Kwara State, Nigeria