Available online at http://icsejournal.com/index.php/JCSE
Journal of Computer Science and Engineering (JCSE)
e-ISSN 2721-0251
Vol. 3, No. 2, August 2022, pp. 60-70

Enhance Facial Biometric Template Security using Advance Encryption Standard with Least Significant Bit

Gbolagade Morufat D[1], Moshood A. Hambali[2*], Oluwadamilare H. Abdulganiyu[3], E. Lawrence[4]

[1] Al Hikmah University, Adeta Rd, 240281, Ilorin, Nigeria
[2,4] Federal University Wukari, PMB 1020, Katsina Ala Rd, Wukari, Nigeria
[3] Euro-Mediterranean University in Fez, BP 51Fez Fes-Meknes Morocco
[1]dammyconsult@gmail.com; [2] hambali@fuwukari.edu.ng*; [3] h.abdulganiyuoluwadamilare@ueuromed.org;
[4]lawrence@fuwukari.edu.ng
* corresponding author

ARTICLE INFO

Article History:
Received Juny 16, 2022
Revised August 15, 2022
Accepted August 25, 2022

Keywords:
Biometric templates,
Cryptography,
Steganography
Stego-image,
LSB

Correspondence:
E-mail:
hambali@fuwukari.edu.ng

ABSTRACT

Security of data has been a major issue for many years which has lead to several challenges; loss of data and also allure hackers to where data are been stored. Biometric system to some extend has helped in combating these security issues, the major issues with the biometric system is how to properly secure the template been generated from hackers and unauthorized users. In this paper we combine cryptography and steganography to enhance security of biometric templates using the advance encryption standard (AES) and the least significant bit (LSB) technique to encrypt these templates and secure it from hackers, Cryptography and Steganography are the two widely employed techniques for securing and hiding data. The center of attention of this paper is the potency of combining cryptography and stenography techniques to improve the security of biometric templates.

1. Introduction

In recent years, biometric systems have been employed in a variety of large-scale projects and applications such as access control, banking, healthcare, attendance management, among others, for dependable and accurate user identification [1]–[3]. In biometrics-based systems, there are still a number of privacy and performance difficulties, such as the lack of revocability in biometric system approaches, susceptibility to outliers, noisy data, lack of uniqueness, and identity invasion [4]. As a result, biometric recognition systems have two most important factors they are, security and performance. As a result, any system that can accomplish performance enhancement and at the same time protect the template is required to provide the biometric system more strength [5], [6]. Three requirements must be met to avoid security theft and maintain user privacy [5], [7], they are diversity, revocability, and non-invertibility [8]. Revocability indicates that if a stored protected template is tampered with, a new template has to be supplied, and non-invertibility means that the initial template of biometric must not be amended from the secure one. While diversity signifies that quit a few number of templates can be developed from original template. Despite the advantages of biometric authentication systems, there are still some trepidations about biometric data's sensitivity to outliers, such as low performance caused by intra-class differences and violation of privacy resulted leakage of information [9].

Biometric template is a representation of the physical or behavioural trait being recorded or assessed. This may be anything from the form of hand to the shape of the finger, or the eyes, or even the way we talk. This picture is then used to create the master profile, which extracts the unique features of each biometric and converts them into mathematical representations. This

http://dx.doi.org/10.36596/jcse.v3i2.527

representation might be a statistical model or a binary representation. These mathematical representations, not the pictures collected or created, are referred to as biometric templates.

Despite the presence of several image and data security techniques, attackers or hackers continue to find new ways to acquire biometric templates for nefarious purposes. In the biometric recognition system, this has become a major issue. In order to maintain communication secrecy and ensure secure delivery of messages, two key strategies are employed. Cryptography and steganography are two well-known ways for keeping data safe from prying eyes.

Cryptography is defined as the transfer of data to a receiver using a key that is encrypted using a predetermined method [10]. The receiver receives and decodes the incoming encoded message if it holds the key. The receiver will not be able to solve the message if it does not have the key. Passwords may now be readily cracked and critical information gained thanks to new technologies that have been developed. There are two types of cryptography systems: The private key is the single key applied for both encrypt and decrypt a file in symmetric encryption cryptography. In asymmetric cryptography two keys are required for encryption and decryption: the private key for encryption and the public key for decryption. Both symmetric and asymmetric cryptography systems employ a variety of techniques. One of the most widely used approaches is AES, which is a symmetric technique that employs a single key for both encryption and decryption. Other symmetric techniques include triple DES, DES, BLOW FISH, etc. The RSA, Diffie-Hellman Algorithm, are popular examples of asymmetric approaches. Steganography is the second method for secure data transfer in a computer system. Steganography is derived from the Greek terms *steganos*, which means "covered, concealed, or shielded," and *graphein*, which means "writing" [11], [12]. The steganography goal is to generate a stego object by hiding crucial message within a usual cover item (picture, sound, video, text, etc.) and sending it to the intended recipient. The receiver that is not the rightful person will not be able to perceive the covert data since it is not visible to the human eye. Steganography can be grouped into two types: linguistics steganography and technical steganography. Linguistics steganography is refered to as text-based steganography. Technical steganography is the application of steganography to sounds, images, and movies. The stego object shows the contents of the cover object to unauthorized person that try to access document. The vital message is concealed in the stego object for recipients. For many decades information hidden has been utilised and will still be relevant in the future. Lot of message concealing approaches had been developed and new techniques are being presented as the improvements in technology. Medical photos, audio recordings, written documents, and other information-hiding strategies are often employed in many locations nowadays. The least significant bit (LSB) is a popular steganography method [12].

Using cryptography alone, the fundamental security of information cannot be guaranteed, therefore other techniques such as steganography are required to safeguard against the threats of hackers or unauthorized persons access the vital information in the system. Even some time, it can be stressful for legitimate user to have access to information at a critical time of decision-making using a toughly encrypted, authentic, and digitally signed information in cryptography. Thus to minimize this during vital decision-making, there is need to combine an enhanced algorithm together. Also, cryptography cannot safeguard against the treats and vulnerabilities that arise from the poor procedures, protocols and systems design. Therefore, it is essential to secure it with another technique using suitable strategy and putting up of a more defensive set-up. Attack or force accessing the message in steganography can easily detect because information is hard to recuperate, if substantial damage occurs to picture appearance while trying to access the information. The biometric template can be susceptible to the unauthorized user by employing only one of these methods, hence the combination of Cryptography and Steganography will augment the robustness and security of biometric template protection [13]. Consequently, the two techniques were combined to complement and enrich each other. This paper aims at developing a hybridized

http://dx.doi.org/10.36596/jcse.v3i2.527

system using cryptography (advance encryption standard (AES)) algorithm and steganography (Least Significant Bits (LSB)) was adapted to protect the face template in the repository. The proposed approach has the following benefit over the existing approach in the literature: 1) the combination of cryptography and steganography were employed to strengthen the safety of face template. 2) A new approach is proposed, in which each character represented by six bits only, while in conventional LSB each character represented by five bits. That means increasing the capacity. 3) The combined method enhance security. The remaining sections of this work is organized as follows: Section 2 discusses the review of related works, Section 3 presents the methodology employed while Section 4 and 5 present the results and discussion, and conclusion respectively.

Lot of techniques had been proposed to protect biometric templates from unintentional or unlawful tampering. The following are some of the techniques that have been suggested: Ref[14] proposed a comprehensive review on Biometrics and Steganography Integration. The combination of steganography with biometrics to have additional level of defense-in-depth security model has also gotten a lot of attention, and it has the prospective of improving both access restrictions control and protection of sensitive biometric data transmitting over a media. In spite of these efforts, the combination of biometric and stenographic techniques has yet to make the leap from the research center to real-life usages. They suggested that is need for future study to look in the direction of finding a satisfactory level of embedding stenographic in biometric data for both academic and industry. Three noninvertible transforms for creating cancelable fingerprint templates were developed and analysed by [15]. The researchers used a notion of performing at most one mapping per minutia appears in the first mention of a perturbation-based noninvertible fingerprint transform.

Ref[16] introduced the concepts of secure sketch and fuzzy extractor of key generation for biometrics template. The researchers devised a robust fuzzy extractor with post-application strength that generates a exchanged secret key of up to $(2m- n)/2$ bits (it is condition to security parameters and error-tolerance), such that n is the length bit and m is the entropy of W. Ref[17] compress the secret information, perform encryption on it using the receiver's public key alongside with the stego key. The BLINDHIDE method, which is one of the easiest approach of hiding secret message in an image, was used by the researcher. It hides invisibly because it starts pixel by pixel from top left corner of the image and the moves across (down - in scan lines) of the image. As it progresses, the LSB of the pixel colours are transformed to match the message. The decoding process are done by starting the LSB from the top left and read off down across the image. It is stress-free to read off the LSB, so this is not very secure. Though it was represented as that, but it is not very ingenious - if the message did not entirely cover up the available space and the top portion of the image is tarnished with, while the bottom remains untouched, making it simple to detect any modification done with the image. Traditional cryptographic techniques were employed to encrypt the data, and visual steganography techniques were utilised to disguise the encoded data, according to [18].

Ref[19] applied LSB to improve the domain of temopral-spatial approach and create a novel model for converting iris pictures to binary streams and hiding them in an appropriate plane of lower bit. The n was placed in the binary values of the stego key from the plane that concealed the message; the iris codes, m, where n is the binary input parameter. After binary conversion, these data generate new iris stego picture as the output. The approach fails to protect against the susceptibilities and treatments that arise as a result of ineffective design systems, protocols, and processes.

Ref[20] developed an encrypting system that used cryptography, steganography, and data concealment methods. The researchers utilised a single level of data encryption, encrypting the message twice before hiding the cypher within the picture in encoded format for later usage. It employs a reference matrix to choose which passwords to use based on the image's attributes. The

http://dx.doi.org/10.36596/jcse.v3i2.527

picture with the concealed data can be utilised for a variety of applications. To embed data in colour photographs, Ref[21] suggested a unique approach based on steganography and cryptography. The data was first encrypted by the researcher before being placed in a picture using a novel Steganography process. The approach is believed to be particularly efficient, especially when used on pictures with uniformly distributed pixels and tiny amounts of data. The provided image is divided into four level blocks, with data encoded in four diagonal sub-blocks whose values are determined by the key. This technique has fewer stages and can efficiently incorporate data without discarding the picture. In order to embed 4 bits of information in a 4*4 pixel block, very few pixels must be changed on average. Furthermore, the stego-images created are of higher quality than those produced by other procedures. When this technique is utilised, the quality of the stego-image is considerably increased. A novel high capacity Steganographic technique based on 3D geometric models is proposed by [22].

To improve security, [23] employed a steganography strategy to safeguard the iris template, using a random number based algorithm in LSB steganography. For enhanced security of the blue pixel only, bits are inserted in LSB. The Iris Code bits are spread out over three LSB at random. The template is more secure as a result of the iris template being saved after embedding in the cover picture rather than as the original biometric. In terms of Receiver Operating Characteristic (ROC) curve plot, histogram plot, and Peak Signal to Noise Ratio (PSNR) value, the system performed better. However, the complexity of steganography in terms of causing harm to the appearance of the image and the fact that it is very easy to detect.

Ref[24] suggested using Steganography and Blockchain to secure images with fingerprint data. The hash value of the picture created via steganography that is stored in the blockchain is obtained using MD5 hash. The non-mutable indexing characteristic of the blockchain assures non-repudiation, i.e. the legitimate user cannot argue that he or she did not take the photo. This can also assist ensure security by guaranteeing that an adversary who obtains user fingerprint data and embeds it into an image using steganography is unable to deposit the image hash into the blockchain. Ref[25] used steganography to secure an iris template. The Hough transform (HT) was used for iris region segmentation to reduce dimensional discrepancies between iris region sections. The LSB method was selected to protect the iris template, however the system failed to take into account the technique's disadvantages.

In light of the foregoing, steganography and cryptography techniques can be joined together to increase data (information) security, since either steganography or cryptography is secure yet, vulnerable to attack on its own. This study addresses these issues by devising a novel method that enhances the quality of stego photos while also enhancing the security of sensitive template in the database.

3. Method

This paper employed both LSB and AES to develop an enhanced security for biometric template in the database.

3.1 Least Significant Bit

Least significant bit (LSB)-based steganography is one of the easiest methods of hiding secret information in the LSBs of pixel values without traceable alterations. With naked eye, modification of the LSB value are undetectable. Messages can be embedded randomly or simply, LSB substitution techniques, Matrix embedding, are common spatial domain approaches.

Many versions of spatial steganography are available in literature, all involve in replacement of some image pixel bits values to hide information. The LSB is the last significant bit in the byte value of the image pixel. The LSB based image steganography implants undisclosed information in the least significant bits of pixel values of the cover image (CVR). To demonstrate LSB approach,

http://dx.doi.org/10.36596/jcse.v3i2.527

the example below provides insight into the technique. Assume the CVR has two pixel values as follow:

(0100 0100 1100 0001 1000 1010)

(0000 1011 0011 1100 1010 1001)

Also, let the secret bits be: 101010. After implanting the hide message in the CVR bits, the outcome of pixel bit values are:

(0100 0101 1100 0000 1000 1011)

(0000 1010 0011 1101 1010 1000)

The bits with red colour show the bits that were altered from their initial bit. Just three bits in the CVR were customized. Typically, almost half of the bits in the CVR will be customized when inserting the covert picture. Some advantages of the LSB are:

- This execution considerably simplifies memory access because it links one covert byte to one cover pixel. Manipulating and Accessing information at the bytes edge simplifies hardware design and decreases power and design area.
- The size of undisclosed is the third in the cover size, which is significantly better than LSB with1-bit.
- The 2/3-LSB produces a better image metrics when compare with 2-bit and 3-bit LSB, the 2/3-LSB presentation is in among 2-bit and 3-bit LSB.

3.2 Advance Encryption Standard

Advance Encryption Standard (AES) is a symmetric block encryption that has 128bits of Block size and Cipher keys of 128, 192 or 256 bits. Majorly, encryption algorithms can be categorized into three major groups – substitution, transposition, and transposition – approach. AES algorithm applies a round function which compare transformations of four different byte-oriented which include Add round key, Mix column, Shift row, Sub byte. The round number to apply is based on the key length for instance, 10 rounds for 128 bit key, 12 rounds for 192-bit key and 14 rounds for 256 bit keys. AES was developed with the following features:

- Simplicity in design.
- Has strong resistance against attacks.
- Code compactness and execute faster on a difference platforms.

The steps involve in implementation of the proposed system can be seen in the fig 1.

1. Firstly, creation of face database. Live face data were collected from individual (four sample of face from individual).
2. The database (dataset) is partition into training and the testing dataset whereby the training dataset will contain 70% of the data collected while the testing dataset will have the remaining 30%.

Fig 1. Sample of face Images Collected

http://dx.doi.org/10.36596/jcse.v3i2.527

e-ISSN 2721-0251

Table 1. Database Settings

Database settings	Value
Total Number of datasets	96
No of Training sets	72
No of Testing sets	24
No of Images per Subjects	4
No of Subjects	24

3. Extraction and Recognition Phase: The principal component analysis (PCA) technique is used to extract important features from the face, then the adaptive equalization helps to reduce the contrast of the images.
4. After the normalization, the AES is then used to encrypt the extracted features (templates). After encryption, the output of the AES is passed down as the input of the LSB for further encryption. The LSB embeds in the output as a cover image. The simple LSB technique implant the covert information in the image; in each pixel of the cover image, the last bit are used to hide the stream of binary code. Stego-image and private key are accomplished.
5. Finally system evaluation is performed on the secured templates.

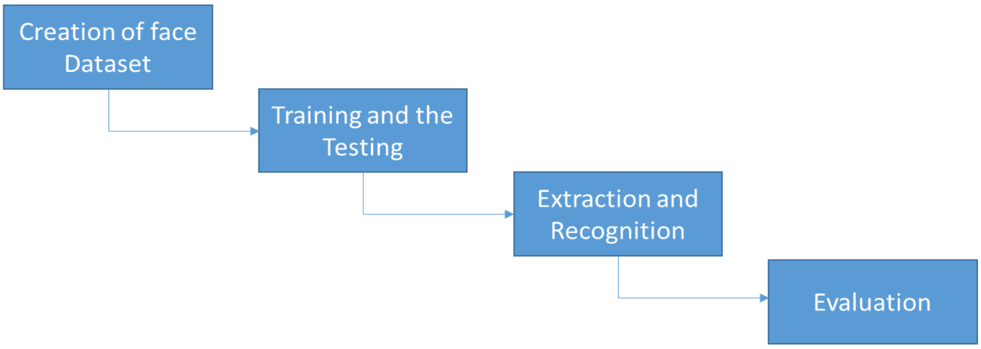

Fig 2. The steps involve in implementation of the proposed system

4. Results and Discussion

For effective production of good images, images from the databases were passed through geometric normalization. The face dataset was first passed through a gray scaling leveling and then they were further preprocessed using adaptive histogram equalization technique for illumination compensation and contrast improvement.

Sample of face images collected such as in Fig 1. were stored in the database; the system is trained using PCA algorithm to generate a face space (Eigen Vector space) in Fig 3. Four facial images are collected from each individual, whereby three out of these images are used to train the system while remaining one reserved for testing. Table 1 presents dataset summary.

The second method for extracting gainful information from the preprocessed and normalized images so as to generate a reduce features for training the system the extracted feature vector was the normal dot principal component analysis.

http://dx.doi.org/10.36596/jcse.v3i2.527

e-ISSN 2721-0251

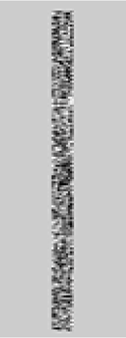

Fig 3. PCA Feature Vector

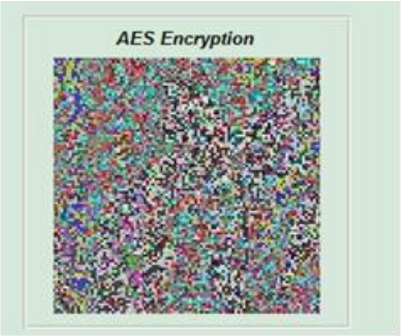

Fig 4. AES Encryption

Fig 5. LSB Stenography (stego image)

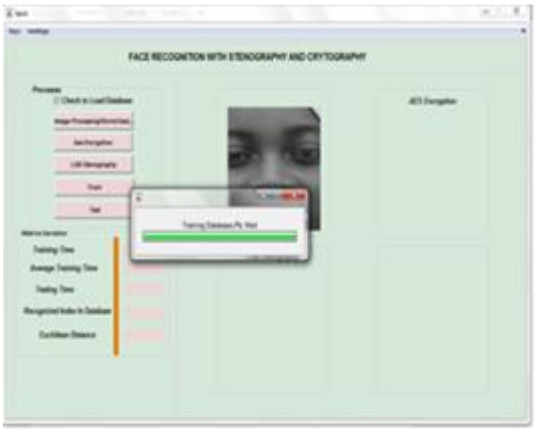

Fig 6. Training faces

Fig 4 shows the encrypted face by the advanced encryption algorithm, after the normalization and feature extraction, the AES is then used to encrypt the extracted features (templates). After encryption, the cipher generated is passed down as the input to the LSB for further processing. The LSB embeds secret message into the image as a CVR. Each pixel last bit are used to hide the stream of binary code in the CVR. Fig 5 shows the interface when a LSB stenography was applied on the image face database. Fig 6 shows the outcome after training of the system. The system will be tested by clicking on test trigger button which will navigate to the test database to choose one of the images from the testing database, which then prompts the encrypted image of the individual and then prompts a modal dialogue for the encryption key as shown in Fig 7. After correct decryption by the private key for the AES algorithm the system will prompt the next phase of security which is the LSB stego images which prompts another dialogue for LSB key as presented in Fig 8.

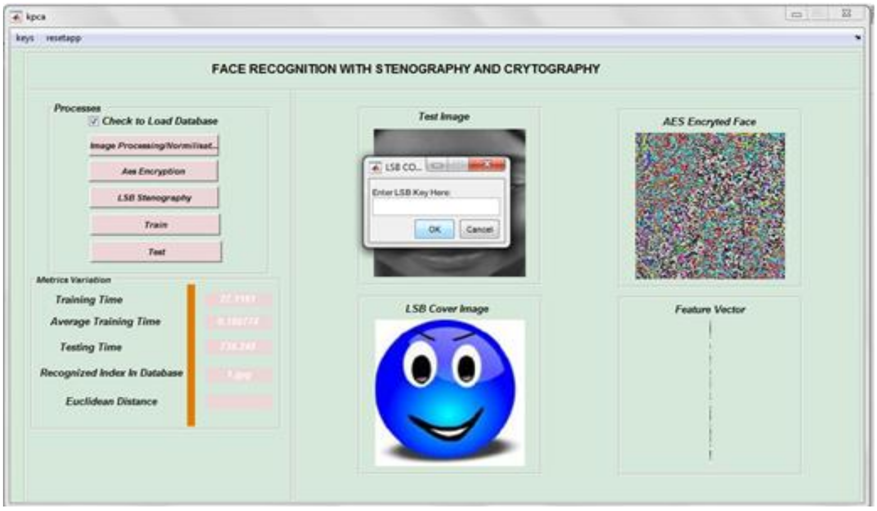

Fig 7. AES key

http://dx.doi.org/10.36596/jcse.v3i2.527

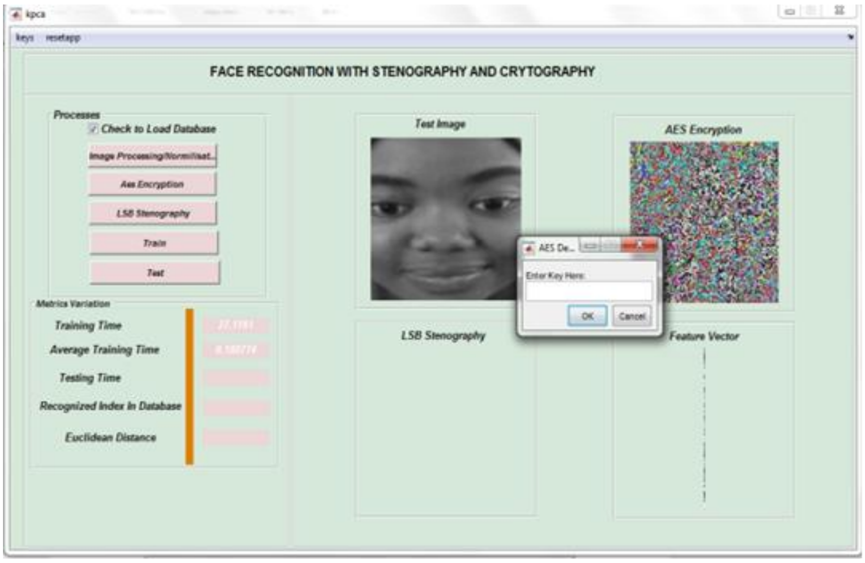

Fig 8. Testing Phase 2

After correct LSB key the system uncovers the covered stego image and opens the exact equivalent match of an individual as well as the PCA Eigen Vector as shown in Fig 9.

Table 2. Imposter Result

No of faces	True Negative	False Positive
4	3	1

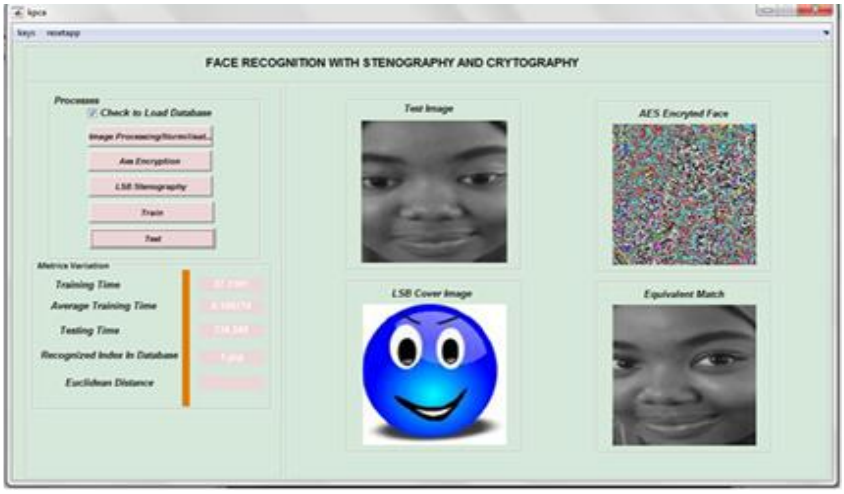

Fig 9. Testing Phase 3

4.1 System Evaluation

In this section, system evaluation was carried out to determine the performance of the approach.

Imposter: This occurs when someone fools a biometric security system, for example by taking a facial biometric of a user and bypassing the entry mechanism that processes that facial recognition. According to this research, Four imposter faces where used to test if the system will be able to recognize the faces.

Table 2 presents the result of the imposter evaluation. Three faces were detected as True Negative while one was considered as False Positive, which shows that the system recorded above 75% Accuracy.

Total Training Time: The system operates at a very good training time while the testing time is signifying high optimization process.

http://dx.doi.org/10.36596/jcse.v3i2.527

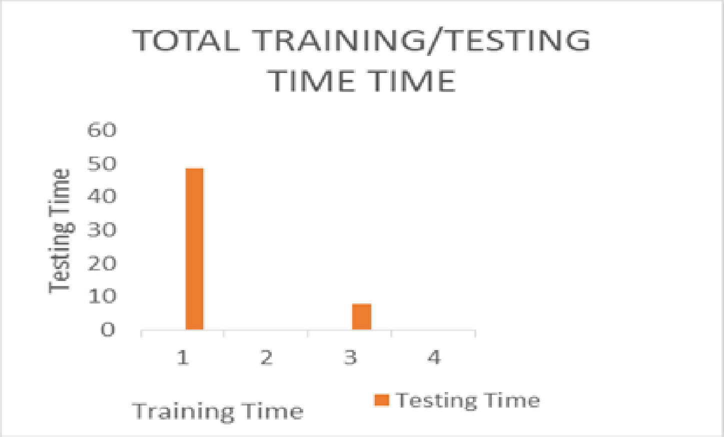

Fig 10. Training and Testing Time (in Sec.)

Table 4. Confusion Matrix

TP (True positive)= 20	**FP(False positive) = 1**
TN(True negative) = 3	**FN(False Negative) = 4**

Table 5. Statistical Metric for Testing Set

Precision	Sensitivity	Specificity	Classification Accuracy	Error	Misclassified Accuracy
0.95	0.83	0.75	0.82	0.18	0.12

According to Table 4, Confusion Matrix result shows that the true positive is 20, true negative is 3, false positive is 1 while false negative is 4. The result indicate that recognition accuracy for the training facial biometric is 75%. Table 5 and Fig 11 indicates that after evaluation, above 80% of the facial images were classified correctly with error rate, precision value, sensitivity and specificity of 18%, 95%, 83% and 75% respectively. This shows that the system performance is very much efficient. Fig 11 shows the statistical chat of Classified Correctly and Classified Incorrectly facial biometric images.

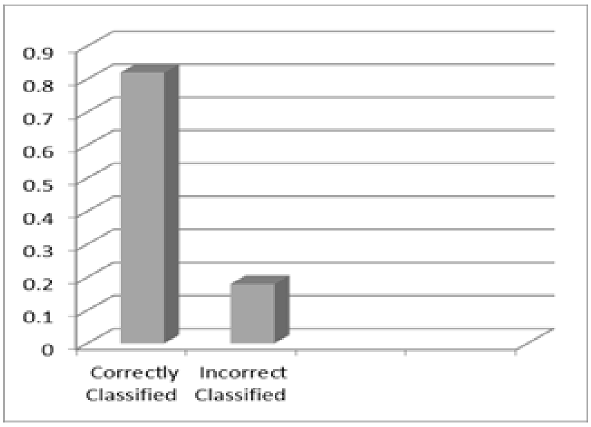

Fig 11. Classified Correctly and Classified Incorrectly facial biometric images

5. Conclusion

The biometric system is regarded as safe, unmatched, and practicable but is still susceptible to certain weakness. In biometric templates experience many attacks, including direct and indirect attacks, can be carried out. The fundamental drawback of biometrics is that if the biometric data or template is taken at any time, it is permanently lost and cannot be recovered. For this reason,

http://dx.doi.org/10.36596/jcse.v3i2.527

template security has become a key concern in biometric recognition methods. To counter the security danger posed by eavesdroppers, ongoing assessment of the current security measures is required. The Least Significant Bits of picture steganography and the Advanced Encryption standard method are used in this work to secure the face template before it is stored in the database. The developed steganography algorithm, which provides a highly protected face template from unauthorised access, is proved to be the system strength. With the level of this proposed system, the issue of panicking with information in transmission or information saved in the database will be minimised, if not completely eliminated, in computing environment. A stronger security foundation is created by using steganography and cryptography in facial recognition system.

References

[1] M. A. Hambali and R. G. Jimoh, “Performance Evaluation of Principal Component Analysis and Independent Component Analysis Algorithms for Facial Recognition,” *J. Adv. Sci. Res. Its Appl.*, vol. 2, pp. 47 – 62, 2015.

[2] Y. K. Saheed, M. A. Hambali, I. A. Adeniji, and A. F. Kadri, “Fingerprint Based Approach for Examination Clearance in Higher Institutions,” vol. 2, no. 1, pp. 2–5, 2017. doi: 10.46792/fuoyejet.v2i1.46

[3] S. Z. Li, *Encyclopedia of Biometrics: I-Z.*, vol. 2. Springer Science & Business Media, 2009. doi: 10.1007/978-0-387-73003-5

[4] D. Sadhya and S. K. Singh, “Construction of a Bayesian decision theory-based secure multimodal fusion framework for soft biometric traits,” *IET Biometrics*, vol. 7, no. 3, pp. 251–259, 2018. doi: 10.1049/iet-bmt.2017.0049

[5] A. M. P. Canuto, F. Pintro, and J. C. Xavier-Junior, “Investigating fusion approaches in multi-biometric cancellable recognition,” *Expert Syst. Appl.*, vol. 40, no. 6, pp. 1971–1980, 2013. doi: 10.1016/j.eswa.2012.10.002

[6] O. C. Abikoye, U. A. Ojo, J. B. Awotunde, and R. O. Ogundokun, “A safe and secured iris template using steganography and cryptography,” *Multimed. Tools Apllication*, 2020. doi: 10.1007/s11042-020-08971-x A.

[7] E. J. C. Kelkboom, X. Zhou, J. Breebaart, R. N. J. Veldhuis, and C. Busch, “Multi-algorithm fusion with template protection,” in *2009 IEEE 3rd international conference on biometrics: Theory, applications, and systems*, 2009, pp. 1–8. doi: 10.1109/BTAS.2009.5339045

[8] K. Nandakumar and A. K. Jain, “Biometric template protection: Bridging the performance gap between theory and practice,” *IEEE Signal Process. Mag.*, vol. 32, no. 5, pp. 88–100, 2015. doi: 10.1109/MSP.2015.2427849

[9] R. Dwivedi and S. Dey, “A novel hybrid score level and decision level fusion scheme for cancelable multi-biometric verification,” *Appl. Intell.*, vol. 49, no. 3, pp. 1016–1035, 2019. doi: 10.1007/s10489-018-1311-2

[10] M. A. Hambali, M. D. Gbolagade, and Y. A. Olasupo, “Cloud Security Using Least Significant Bit Steganography and Data Encryption Standard Algorithm,” *GESJ Comput. Sci. Telecommun.*, vol. 1, no. 58, pp. 17–29, 2020.

[11] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, “Digital image steganography: Survey and analysis of current methods,” *Signal Processing*, vol. 90, no. 3, pp. 727–752, 2010. doi: 10.1016/j.sigpro.2009.08.010

[12] Y. Yiğit and M. Karabatak, “A stenography application for hiding student information into an image,” in *2019 7th International Symposium on Digital Forensics and Security (ISDFS)*, 2019, pp. 1–4. doi: 10.1109/ISDFS.2019.8757516

[13] M. S. Taha, M. S. M. Rahim, S. A. Lafta, M. M. Hashim, and H. M. Alzuabidi, “Combination of steganography and cryptography: A short survey,” in *IOP conference series: materials science and engineering*, 2019, p. 052003. doi: 10.1088/1757-899X/518/5/052003

[14] I. McAteer, A. Ibrahim, G. Zheng, W. Yang, and C. Valli, “Integration of biometrics and steganography: A comprehensive review,” *Technologies*, vol. 7, no. 2, p. 34, 2019. doi: 10.3390/technologies7020034

[15] R. M. Bolle, J. H. Connell, and N. K. Ratha, “Biometric perils and patches,” *Pattern Recognit.*, vol. 35, no. 12, pp. 2727–2738, 2002. doi: 10.1016/S0031-3203(01)00247-3

[16] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, “Fuzzy extractors: How to generate strong keys from biometrics and other noisy data,” *SIAM J. Comput.*, vol. 38, no. 1, pp. 97–139, 2008. doi: 10.1007/978-3-540-24676-3_31

[17] M. Umamaheswari, S. Sivasubramanian, and S. Pandiarajan, “Analysis of different steganographic algorithms for secured data hiding,” *IJCSNS Int. J. Comput. Sci. Netw. Secur.*, vol. 10, no. 8, pp. 154–160, 2010. http://paper.ijcsns.org/07_book/201008/20100825.pdf

[18] P. Marwaha and P. Marwaha, “Visual cryptographic steganography in images,” in *2010 Second international conference on computing, communication and networking technologies*, 2010, pp. 1–6. doi: 10.1109/ICCCNT.2010.5591730

[19] Z. Zainal-Abidin, M. Manaf, and A. S. Shibghatullah, “A New Model of Securing Iris Authentication Using Steganography,” in *International Conference on Software Engineering and Computer Systems*, 2011, pp. 547–554. doi: 10.1007/978-3-642-22170-5_47

[20] S. Usha, G. A. S. Kumar, and K. Boopathybagan, “A secure triple level encryption method using cryptography and steganography,” in *Proceedings of 2011 International Conference on Computer Science and Network Technology*, 2011, vol. 2, pp. 1017–1020. doi: 10.1109/ICCSNT.2011.6182134

[21] P. Bharti and R. Soni, “A new approach of data hiding in images using cryptography and steganography,” *Int. J. Comput. Appl.*, vol. 58, no. 18, 2012. https://research.ijcaonline.org/volume58/number18/pxc3883716.pdf

[22] P. Thiyagarajan, V. Natarajan, G. Aghila, V. Prasanna Venkatesan, and R. Anitha, “Pattern based 3d image steganography,” *3D Res.*, vol. 4, no. 1, pp. 1–8, 2013. doi: 10.1007/3DRes.01(2013)1

[23] S. Chaudhary and R. Nath, “A new template protection approach for Iris recognition,” in *2015 4th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO)(Trends and Future Directions)*, 2015, pp. 1–6. doi: 10.1109/ICRITO.2015.7359306

[24] S. Pramothini, Y. S. Pavan, and N. Harini, “Securing images with fingerprint data using steganography and blockchain,” *Int. J. Recent Technol. Eng.*, vol. 7, no. 4, pp. 82–85, 2018. https://www.ijrte.org/wp-content/uploads/papers/v7i4s2/Es2042017519.pdf

[25] K. Y. Saheed, A. S. Olaniyi, A. M. Olaolu, and A. N. Babatunde, “Development of Iris biometric template security using steganography,” *Comput. Inf. Syst.*, vol. 22, no. 3, pp. 8–18, 2018. link.gale.com/apps/doc/A562690777/AONE?u=googlescholar&sid=googleScholar&xid=0a7f27f6