Computer Systems Science & Engineering
DOI: 10.32604/csse.2023.031893
Article

Tech Science Press

Face Attribute Convolutional Neural Network System for Data Security with Improved Crypto Biometrics

S. Aanjanadevi[1,*], S. Aanjankumar[2], K. R. Ramela[3] and V. Palanisamy[4]

[1]Department of Computer Applications, Alagappa University, Karaikudi, 630003, Tamilnadu, India
[2]Department of Computer Science and Engineering, Sri Raaja Raajan College of Engineering and Technology, Amaravathipudur, 630301, Tamilnadu, India
[3]Department of Electrical and Electronics Engineering, Ultra College of Engineering and Technology, Madurai, 625020, Tamilnadu, India
[4]Department of Computer Applications, Alagappa University, Karaikudi, 630003, Tamilnadu, India
*Corresponding Author: S. Aanjanadevi. Email: aanjanadeviphd@gmail.com

Received: 29 April 2022; Accepted: 10 June 2022

Abstract: Due to the enormous usage of the internet for transmission of data over a network, security and authenticity become major risks. Major challenges encountered in biometric system are the misuse of enrolled biometric templates stored in database server. To describe these issues various algorithms are implemented to deliver better protection to biometric traits such as physical (Face, fingerprint, Ear etc.) and behavioural (Gesture, Voice, tying etc.) by means of matching and verification process. In this work, biometric security system with fuzzy extractor and convolutional neural networks using face attribute is proposed which provides different choices for supporting cryptographic processes to the confidential data. The proposed system not only offers security but also enhances the system execution by discrepancy conservation of binary templates. Here Face Attribute Convolutional Neural Network (FACNN) is used to generate binary codes from nodal points which act as a key to encrypt and decrypt the entire data for further processing. Implementing Artificial Intelligence (AI) into the proposed system, automatically upgrades and replaces the previously stored biometric template after certain time period to reduce the risk of ageing difference while processing. Binary codes generated from face templates are used not only for cryptographic approach is also used for biometric process of enrolment and verification. Three main face data sets are taken into the evaluation to attain system performance by improving the efficiency of matching performance to verify authenticity. This system enhances the system performance by 8% matching and verification and minimizes the False Acceptance Rate (FAR), False Rejection Rate (FRR) and Equal Error Rate (EER) by 6 times and increases the data privacy through the biometric cryptosystem by 98.2% while compared to other work.

Keywords: FACNN; biometric cryptography; AI; FAR; FRR; EER

1 Introduction

1.1 Biometric Authentication and Encryption

Knowledge-based authentication, which uses PINS, passwords, and graphical pins for identification, is used in traditional authentication systems. The biggest disadvantage is that passwords and pins can be easily discovered, falsified, and stolen by intruders. As a result, the user is asked a lot of questions concerning the data's secrecy and legitimacy. To provide assistance regarding trustworthiness and confidentiality the use of biometric authentication and encryption is made possible.

For secret data transmission, user authentication is very necessary for many companies and researchers to authenticate and verify that the data can only be accessed by the verified user. Today, biometric technology is used in a variety of industries and applications to verify authenticity. The genuineness Biometric technology is being used in a variety of sectors and applications to verify the authenticity of users through two phases: enrolment and verification. Physical based authentication (facial, fingerprint, iris, retina, etc.) and behaviour-based authentication (gesture, voice, etc.) are the two basic kinds of biometric authentication systems. It compares both physical and behavioural templates that have already been confirmed and saved in the database to verify the user's authenticity. Authentication is confirmed if both biometric data templates match; otherwise, authentication is rejected. Biometric tokenization is a type of biometric encryption that combines biometric and cryptographic techniques. By combining the qualities of public key architecture, it is utilised to provide security as well as ensure system authentication. It considers the advantages of using facial, iris, retina, and fingerprint authentication. Dispersed cryptography is used in biometric cryptography.To ensure the biometric qualities that are stored in various devices with biometric authentication capabilities, an architecture model was created. This mechanism notifies service providers of any faults with the central database.

1.2 Cryptography

Cryptography is the science of developing and testing systems to prevent third parties from hacking confidential data. Modern cryptography emphasises information privacy, firmness of information, substantiation, and non-reflective, among other aspects of information security. For security purposes modern cryptography is now implemented in all fields such as science and management. Some current cryptography techniques can only keep their keys secret provided specific mathematical conditions are met. Integer factorization and discrete logarithm issues are hard hence there are profound linkages with abstract mathematics. There are just a handful of cryptosystems that have been demonstrated to be completely secure. Claude Shannon proved that the one-time pad is one. A few key algorithms have been proven secure under particular conditions.

2 Related Works

Hao et al. [1] proposed a key agreement-based ECC-based ID-based remote mutual authentication system. This protocol is designed to address a variety of fine-recognised security and competence concerns. However, the approach has a prospective error that might lead to a masquerade attack [2,3]. Biometrics is playing a bigger role in offering extremely safe identity and own authentication solutions [4]. Fingerprints [5], handwritten signatures [6], and facial features [7] are all examples of keystroke patterns. Biometric keys can be extracted using any of these approaches.A smart card-centred biometrics-based remote user verification mechanism was suggested by Carrara et al. [8]. Because they use one-way hash functions, biometric verification, a smart card, and a nonce, their method is secure. In terms of computing, the technique is extremely cost-effective. In comparison to other analogous systems, which has been demonstrated to be low [9].

Biometric data confidentiality and protection have established a lot of attention in this era of rapid growth in alphanumeric technology and network facilities. The multidimensional safety dispensation system based on visual cryptography technologies offers a high parallel processing power. To protect biometrics data, many scholars have recommended the use of digital and optical ciphering methods [10]. The authors of [11] proposed employing CBRS for biometric credentials in cloud computing facilities, which is based on deep learning. A CBRS for multi-biometric authentication and validation was proposed by the authors of [12]. In the proposed CBRS, a surreptitious produced key from another biometric picture is used to convert a biometric doppelgänger to a safe and cancellable biometric pattern using resourceful bit-wise encryption methodologies. The recommended CBRS preserves the number of min mistakes in both the secured and innovative biometric traits, ensuring recognition effectiveness comparable to the defenceless structure. On a range of iris and face databases, the results of the comparison with literature biometric security techniques revealed that the recommended CBRS delivered decent and considerable recognition competence, as well as high-level authentication and protection. Volna et al. [13] investigated back-propagation NN in cipher system. This system changes the contribution data to alphanumeric cypher, extracts the bit structure for every cipher, divides it into 6-min layers, and uses it as a contribution to the enciphered process. The cipher key is a NN containing a contribution stratum, concealed stratum, productivity stratum, and reorganized loads. The suggested method has been verified using a range of original text numbers, and the outcomes confirm that it is safe. A General Regression Neural Network-based encryption scheme was introduced by Noaman et al. [14]. A NN is used to develop an effectual enciphered system by an everlastingly varying key. Aanjanadevi et al. suggests a biometric cryptosystem which generates a key with binary codes and extract the face features using a fuzzy extractor algorithm with 96% efficiency [15].

3 Proposed Methodology

The proposed methodology can be split into various sections. In the first section, the face attribute of a human is detected and recognized using FACNN technique, in the second section we discuss a generation of a key from the facial features extracted after the face detection and recognition process finally the cryptography technique is implemented using the key generated from biometric face attribute to provide high entropy security to the data transferred through the network.

3.1 Convolutional Neural Network

CNN’s are extremely powerful neural networks that are a regularised form of Multilayer Perceptrons (MLPs). The application of the convolutional mathematical process by the network is referred to as a “convolutional neural network.” When two functions are shifted over each other, convolution is a form of linear operation that indicates the degree of overlap between them. Simple neural networks having at least one layer that uses convolution instead of standard matrix multiplication are known as convolutional networks. CNN-based architecture for encoding and decoding features has the following advantages, according to published studies:

CNN efficiently leverages neighbouring pixel information to effectively downsample the image first by convolution and then employs a prediction layer at the end to extract features from the images.

CNN is more accurate and performs effectively. One can get a decent idea of the patterns of natural photographs by using a deep neural network, in this case, a CNN. The network will be able to determine which areas are redundant, allowing additional pixels to be buried in certain areas. The amount of hidden data can be raised by saving space on superfluous areas. The network will hide the data that no one can see because the structure and weights can be randomised.

3.2 Pre-Processing

3.2.1 Face Detection and Face Recognition Using CNN

The biometric system's main goal is to identify and approve the user with the authority to access the full system based on physiological or behavioural characteristics. The first step in this suggested system is to use a biometric method to detect a digital image of an individual. By capturing the image with a camera, an individual's biometric digital image is enrolled into the system. Following the input, the face is detected and stored in the database for later processing using the face detection method as shown in Fig. 1.

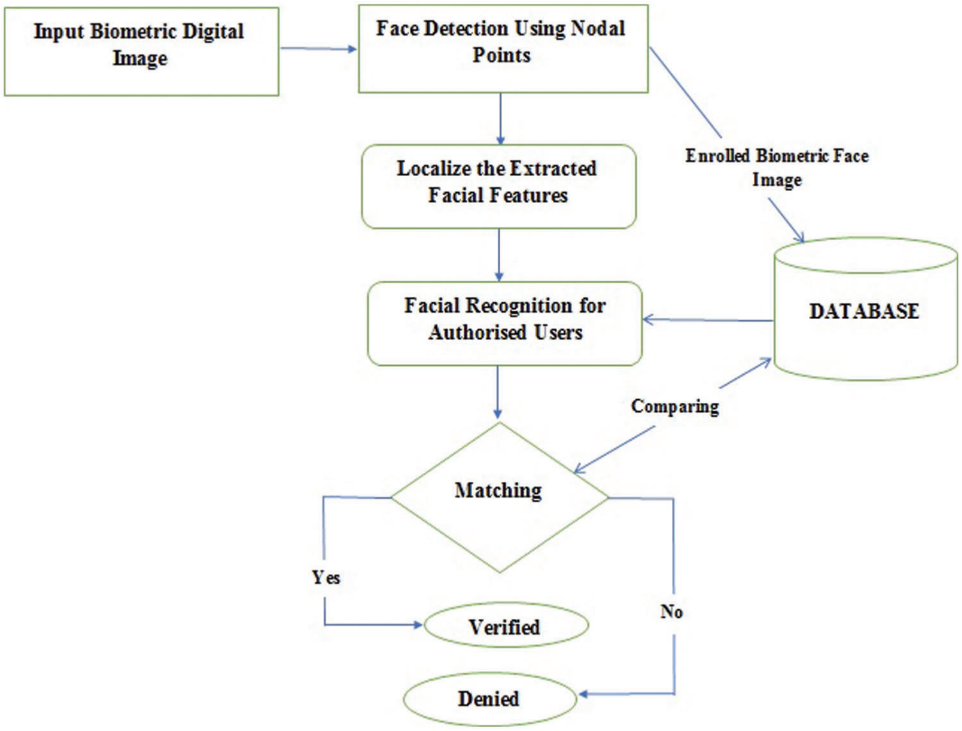
Input Biometric Digital Image
Face Detection Using Nodal Points
Localize the Extracted Facial Features
Enrolled Biometric Face Image
DATABASE
Facial Recognition for Authorised Users
Comparing
Matching
Yes
No
Verified
Denied

Figure 1: The architecture flow of pre-processing process of biometric face

Following face detection, the face recognition procedure is started; this approach is used to verify the registered user by comparing the input face image with the enrolled biometric template stored in the database, and only if the input and enrolled images match, the user is given authority. The nodal points, which are unique to each individual for their own identification, can be used to recognise the face image. Here CNN technique is used for facial recognition which efficiently recognises the person with higher accuracy. During the enrolment process, certain layers of a convolution neural network are used to recognise a specific person’s face among a large number of face data saved in the database. CNN recognises a human face by detecting nodal points, which are then utilised to extract facial features. The CNN algorithm works with biometric input face for face recognition described as follows.

At first, the input image is captured and the face is identified then concentrates on removing noise from the face image such as blurring, turned faces and bad lighting during enrolment.

Identify the authorized person’s face within the database.

Nodal points are taken for comparing the input image with already stored biometric template during enrolment phase.

Finally, the matching occurs the person is verified and allowed to access the system if matching doesn't occur the person cannot access the entire system for data transmission.

3.2.2 Normalization of Face Attribute

Certain nodal points are taken for normalization of face feature vectors especially the distance between eyes, size of the eyes, shape and structure of the face, width and length of the nose etc.

Fig. 2 shows how the face image is captured using a web camera and how the face is detected after the face detection process the original image is converted into grayscale image. Then the face feature extraction is done through marking nodal points and extracted face images with noisy datasets are further normalized into an original dataset. During the verification process, the face template is compared with the original face dataset for the verification process to provide authenticity.

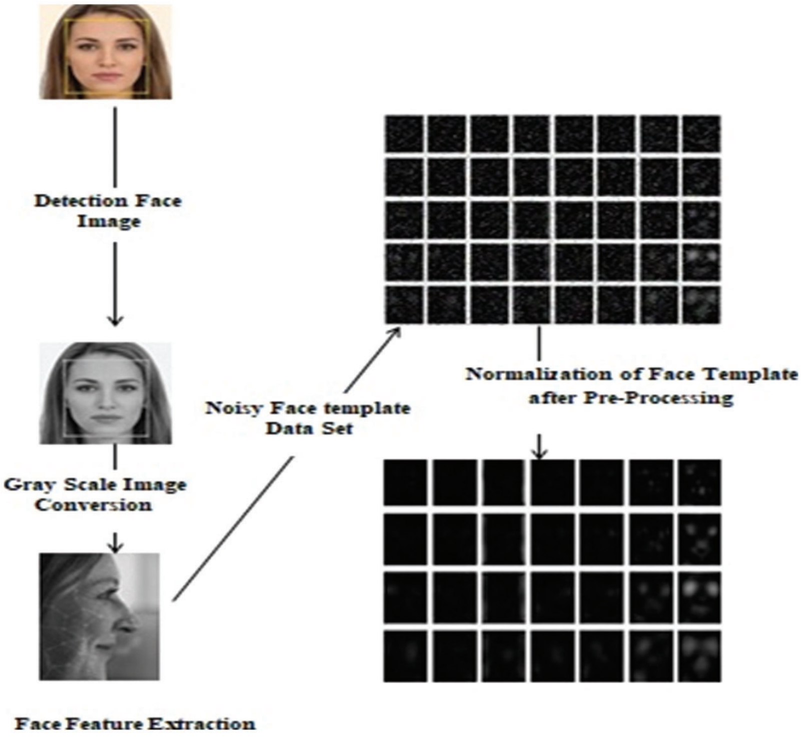
Detection Face Image
Gray Scale Image Conversion
Face Feature Extraction
Noisy Face template Data Set
Normalization of Face Template after Pre-Processing

Figure 2: Process of face template storage in a dataset

Various nodal points are marked which is used to extract the facial feature for storing and identifying process. Fig. 3 shows the steps involved in biometric face normalization. Normalization of facial features doesn't depend on shape, size and dimension of biometric face features.

3.2.3 Key Generation

After the pre-processing of the biometric face attribute the FACNN generates bio codes which is the binary code (0 & 1) from the biometric face feature vector by marking nodal points for identifying each face uniquely from the database. Each and every time bio codes are generated uniquely for every biometric face image enrolled as well as updating of the previously stored image. The bio codes forms a strong key with maximum entropy of key length from FAK (face attribute key) = 256, 512, 1024 etc. higher the key length stronger the key is.

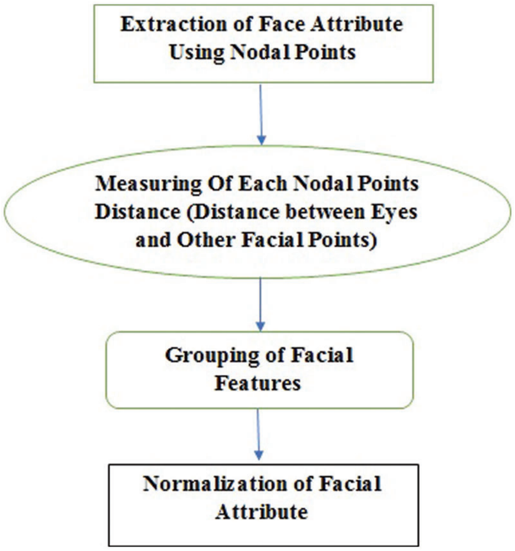
Extraction of Face Attribute Using Nodal Points
Measuring Of Each Nodal Points Distance (Distance between Eyes and Other Facial Points)
Grouping of Facial Features
Normalization of Facial Attribute

Figure 3: Biometric face normalization

Here the facial feature attribute FA where FA = $\{fa_1,\ldots,fa_n\}$extracted by marking nodal points N. Where FA∈N

Face attribute with 3D vector using CNN with facial attribute FA with subset of fa' of dimension D.

BI is the input of face feature attribute can be written as

$$BI(fa')= concat\{L(fa^e,D^e)\} \quad (1)$$

where L is the number of layers taken for comparison and verification of the image

The size of the key K generated from the face attribute FA can be quantization can be derived as K = log K.

Based on the size of bio codes the key can be generated with high efficiency for 3D face feature vector. FACNN take various layers of face attributes which are connected to one another with higher key size from 256 up to 1024 bit bio codes for further processing. Depending on number of connected layers the key size is fixed and taken for a cryptographic process by minimizing FAR and Maximizing FRR of biometric face data.

3.2.4 Biometric Cryptography

This is the major process in this system, here the key generated from the bio code **(i.e; binary codes 0's and 1's)** which acts as cryptographic key for encipherment and decipherment of confidential data transmitted over network. Asymmetric cryptographic system takes place here for the enhancement of data security and robustness of the system. In this proposed approach various keys are generated from biometric facial features One key is used for encryption, while the other is used for decryption.

Initially the sender encode the data with public $SFAK_u$ and private keys $SFAK_v$ (bio codes) generated from face attribute of sender along with public key $RFAK_U$ of receiver as shown in Fig. 4. After the transmission of data over network the data received at the receiver end is decrypted using authenticated receiver's corresponding Public RFAKu and private key $RFAK_v$ along with sender's public key $SFAK_u$ to access the original data. The keys can be verified by matching the bio codes (keys) with previously assigned and stored bio codes of an authenticated individual input data already stored in database during enrolment. If the matching of bio codes of senders and receivers occurs the system allows the receiver to access the data with original image otherwise it cannot be accessed. The proposed methodology improves security, privacy, and authentication verification, and the system becomes more reliable, protecting data from hackers. And also because of the usage of own biometric face attribute as key for a cryptographic process we can avoid data loss, theft or forged.

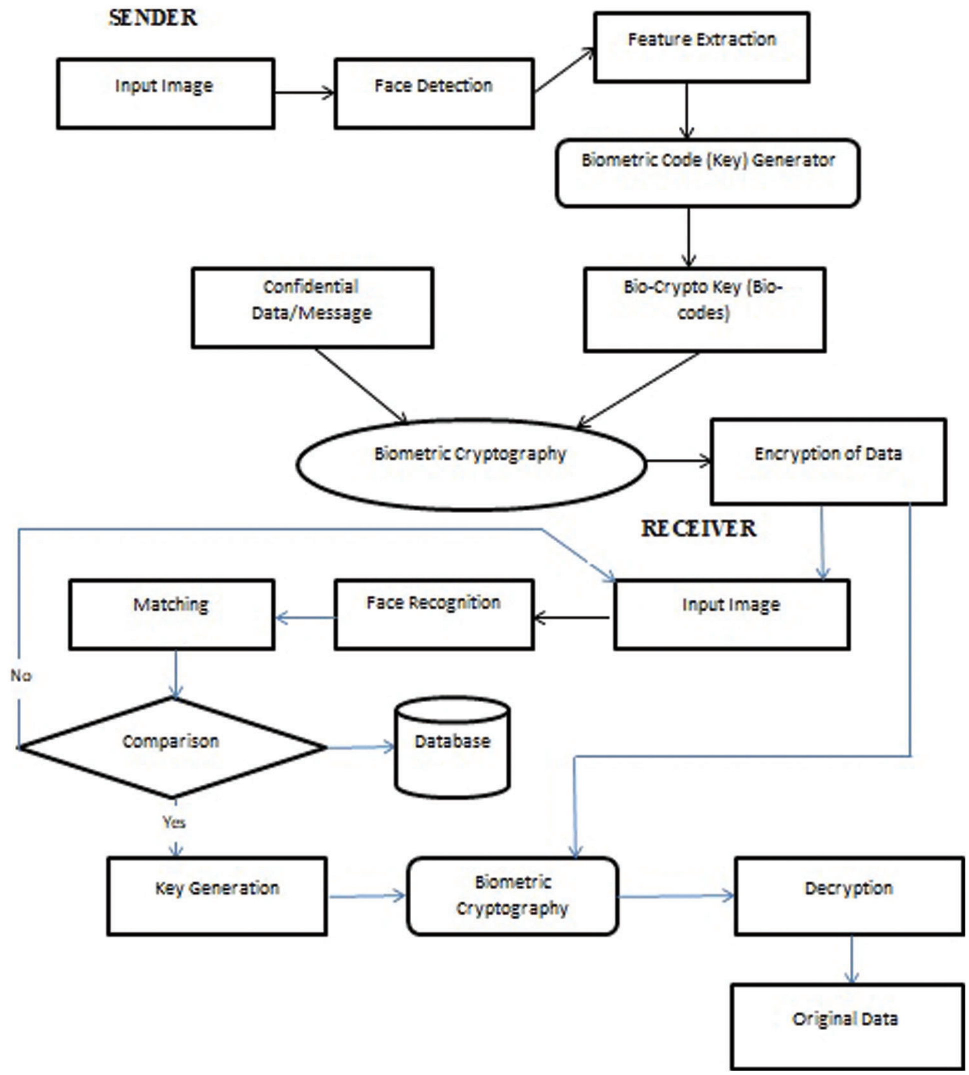

Figure 4: Architectural flow of biometric cryptographic system

The FACNN algorithm process is as follows

1. Input biometric face is captured and enrolled in database.
2. Face image is recognised as an authenticated person by comparing and matching.
3. If the current and previous input face images are identical,
4. Authenticity is verified.
5. Face image normalization take place by marking the nodal points.
6. Bio codes i.e key FAK(Face Attribute Key) is generated from the face feature extraction using nodal points.
7. Nodal points are independent of shape, size and dimension of face.

8. Bio codes length can be calculated based on nodal point length.
9. Bio codes are binary codes consists of 0’s and 1’s.
10. 0 for minimum nodal point length and 1 for maximum number of nodal points.
11. Then biometric cryptography takes place.
12. The bio codes are differentiated into Public FAK_u and private keys FAK_v.
13. Each sender S and receiver R having different keys for encryption and decryption.
14. Confidential data CD can be encrypted using sender’s public SFAKu and private key $SFAK_v$along with receiver’s public key RFAKu.
15. At the receiver end the bio codes which is the binary key generated from the fface attribute undergoes verification process for authentication.
16. At other end the receiver decrypt the original data after the matching occurs using his own public RFAKu and private key $RFAK_v$ along with sender’s public key $SFAK_u$.

4 Experimental Verification and Discussion

This section includes four subsections which describe evaluation metrics comparisons, experimental verification, result and discussion and finally security efficiency.

4.1 Evaluation Metrics

In this section, we consider Equal Error Rate (EER), False Acceptance Rate (FAR) and as evaluation metrics. The trained facial feature vectors are involved in various test cases with the maximum threshold values to obtain EER efficacies and generate the verification and identification of authorized users depending on FAR rates with various layers and the number of trained faces during pre-processing method. EER and FAR rates are shown in Tab. 1 by using various test cases, and threshold values and based on a number of trained face attributes.

Table 1: Comparison of evaluation metrics

Test cases	Threshold value	Number of trained face attribute	EER	FAR
Fake and unprotected face attribute	0	100 real	14.0	1.5
Protected face attribute	0	75 binary	17.6	0.4
Protected face attribute	1	1000 binary	12.5	0.15
Protected face attribute	2	1750 binary	10.3	0.002
Protected face attribute	4	2500	6.4	0.001

To report the problem mentioned above, use a fusion approach to enhance protection for biometric face attributes than the previous algorithm, for improved system performance. In this project for template protection, the hybrid method combines both the transform-based approach and the biometric cryptosystems approach. Our work's key contributions are summarised below:

1. We look into the use of one-shot enrolment in template protection enabled biometric systems, where only one image of the user's biometric trait (here face) is used for enrolment. We also use multi-shot enrolment for performance comparison, which uses more than one image of the user's biometric trait (here face) for enrolment.
2. Deep CNN is used to protect face templates. During the enrolment phase, the deep CNN learns a robust mapping from the users' face images to the unique binary codes (bitwise randomly

generated) assigned to the users. The deep CNN extracts feature vectors using the pre-trained Face model and maps them to the bit-wise randomly generated unique binary codes assigned to each user. The use of pre-trained Face architecture allows the proposed deep CNN to capture uniqueness in the extracted feature set of each user, maximising inter-user variation.

3. While mapping the extracted feature vector to the bitwise randomly generated unique binary codes assigned to each user, the robust mapping network minimises intra-user variations. Given an input face image of a user, it predicts the binary code assigned to the user during enrolment during verification. The predicted binary codes corresponded to the actual binary code assigned to the user during registration.
4. For the evaluation of our method, we use three face datasets: CMU-PIE, FEI, and Color FERET. We compare the performance (EER, FAR, and FRR) of our face template protection method to that of the other algorithms on the CMU-PIE dataset. When compared to related work, the proposed method improves matching performance by 6% and reduces Equal Error Rate (EER) by about 4 times while providing high template security.

4.2 Experimental Verification

The proposed system of FACNN (Face Attribute Convolutional Neural Network) is used for pre-processing of biometric facial features by mapping the nodal points and generating binary codes (0's and 1's) that act as a key for a cryptographic key for further secure data transmission. The generation of bio codes (key) is explained below. System efficiency is shown in the Tab. 2 depending on the size of the face attribute key (FAK), EER, FRR, FAR rates.

Table 2: Experimental verification

FAK	EER	FAR	FRR	System efficciency
64	4.1	0.3	0.35	91.1
128	3.7	0.25	0.275	94.2
256	3.55	0.11	0.2	95.78
512	3.21	0.05	0.15	96.6
1024	2.11	0.0125	0.005	96.9
2058	1.5	0.0015	0.0025	97.8
4096	1.011	0.001	0.0012	98

To mine the biometric face attribute feature, here we use 25 layers in CNN with 10 blocks which are interconnected to each layer of enrolled biometric face images. Each block consists of a unique number of filters from 64 to 4096 and each face attribute can be split into 3 × 3 matrix format for extracting face features for pre-processing. After pre-processing of biometric face attributes the nodal points are marked and each nodal point for each and every individual are unique from the others.

These points are used to extract the face features and based on the size of nodal points the size of the bio codes (Keys) is generated. The length of the key size started from 256 binary digits to 4096 binary digits size key. The higher the size of bio codes stronger the security is. System efficiency is shown in Fig. 5.

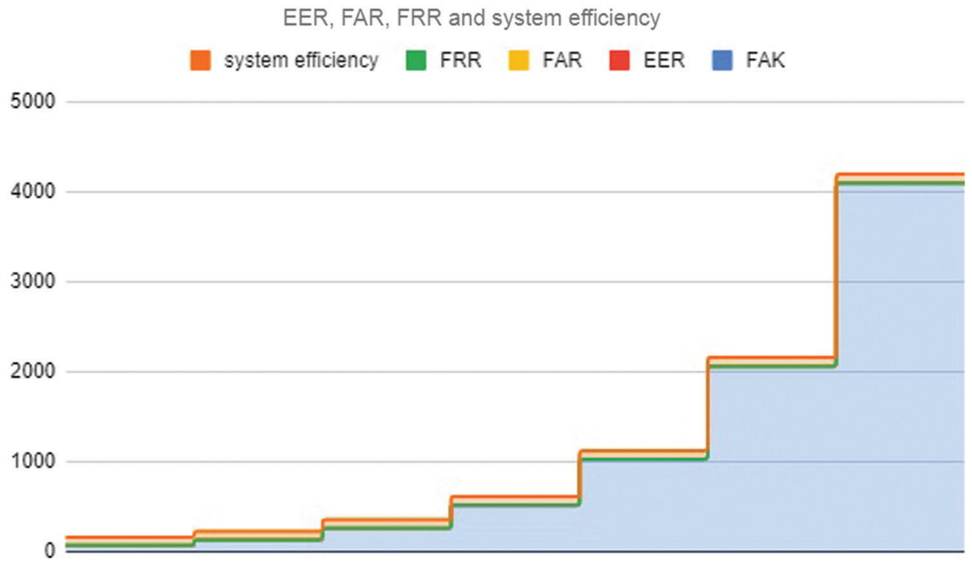

Figure 5: System efficiency comparisons in terms of EER, FAR and FRR

After the generation of bio codes from the biometric face image, the FACNN verifies the bio codes with the matching biometric face image by comparing the bio codes (0's and 1's) with already stored face attributes. If FACNN values are 1 for matched face and 0 for false face i.e mismatched face thus denied the accessing operation and authenticity is denied.

4.3 Result and Discussion

The above Fig. 6 shows the efficiency of the system by means of a face attribute key generated from bio codes by mapping the nodal points and on the biometric face attribute for feature extraction. Based on the length of the key the Error Equal Rate, False Acceptance Rate and False Rejection Rate are analysed. EER, FAR and FRR or 10 training samples of face attribute are taken for performance analysis. Using this algorithm, the proposed method provides a higher efficiency system with a low FAR and FRR rate with the highest matching value for bio codes being 1. During the enrolment and verification phases, the efficiency of the system is 96.6% by using the face attribute convolutional neural network approach. Here we take the size of the key for evaluation to check the system efficiency of providing security with minimal EER, FAR and FRR.

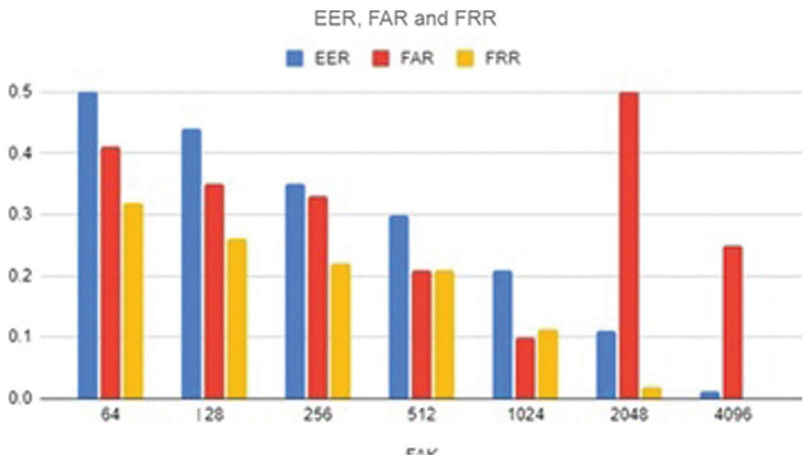

Figure 6: EER, FAR And FRR rates based on key size (FAK)

Depending on the size of the key starting from 64 binary values up to 4096 binary values the EER, FAR and FRR are low for every bit increased in key size. As the result after comparison with FACNN algorithm, the bio codes generated with different dimensionality result in a lesser EER of 0.5% for key size of 64 bits. Each time we compare the result by increasing the key size up to 4096 bits the EER, FAR and FRR are very low at the rate of 0.01% with approximately 97.8% of system efficiency.

4.4 Performance Analysis Based on Security

Here we discussed about the security performance analysis of the proposed work. In this proposed approach uses FACNN approach for generating bio codes i.e, key which is used to provide security to the confidential data transmitted over a network. In a traditional cryptographic system, the key is generated as alphanumeric codes that can be easily accessed and predicted by the intruders to access the data. But here due to generating a key from their own biometric face attribute the intruders cannot easily access or predict the key to access the data. Not only biometric key generation but also, use an asymmetric cryptographic approach for providing an enhanced level of security to the information transmitted over a network. Because of using asymmetric cryptography different keys are generated from the face attribute for encryption and decryption by doing this we can enhance the system security.

In order to attack the system creating a false imposter of an individual is made but due to the usage of FACNN methodology, the imposter undergoes a comparison and matching mechanism for generating keys by marking the nodal points for key extraction it is not possible for matching nodal point face extraction. The access is denied and authority is not.

Given when there is mismatching of nodal points of face attribute. The Fig. 7 represents the system efficiency using size of FAK (Face Attribute Key), EER, FAR and FRR rates. To enhance the security to the entire system we use highest number of face attribute keys FAK = 1024 to FAK = 4096 with strong security key which cannot be broken, identify or predicted. Higher the size of the key higher the security to be with minimal EER, FAR and FRR.

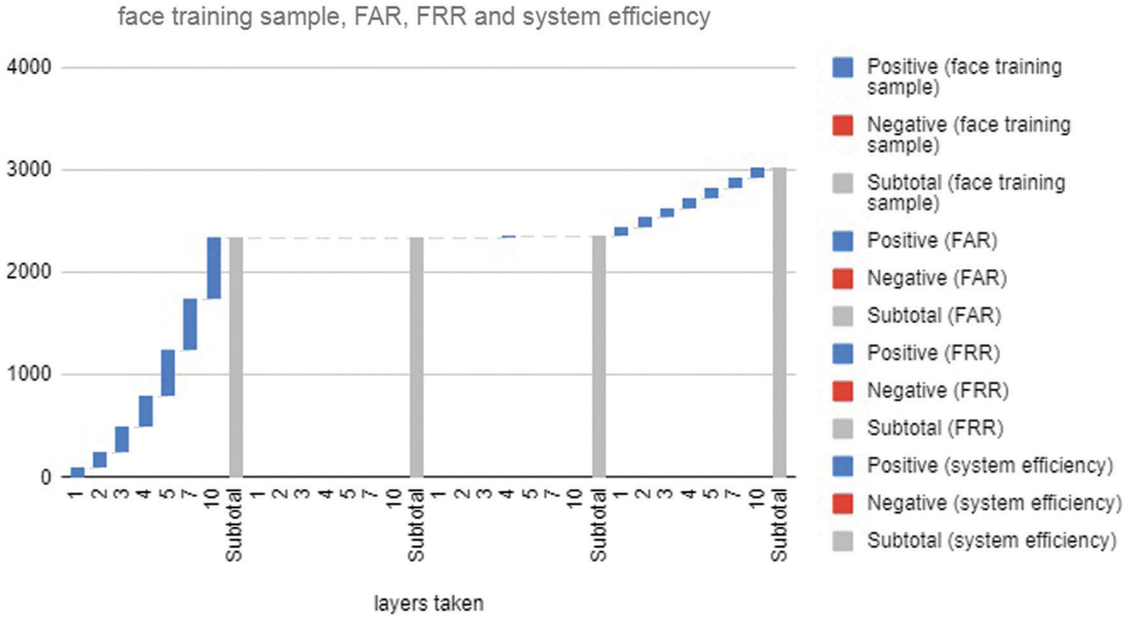

Figure 7: System efficiency graph of proposed system

5 Conclusion

This paper mainly focused on rectifying the security issues of theft of data, data manipulation etc. during transmission from one node to another using a network as well as we concentrate on verifying the authorized user who has the rights to access the data. In this proposed work we build an AI-based biometric cryptosystem for the secure transmission of data over the internet. Here we combine biometric technology along with cryptography to provide a more robust, reliable and secure system for data transmission. In this proposed scheme we use AI-based FACNN technique for generating a cryptographic key from the biometric face attribute of an individual by doing a biometric process of enrolment and verification and then using various layers for generating strong bio codes which act as cryptographic keys. Based on the length of bio codes the strength of the key is predicted. Initially, the size of the key is taken as 64 bits then increases the length of the key up to 4096 bits for a strong cryptographic process. For the key with high entropy with higher bits for face attribute we obtained minimum EER which is approximately 0.21% with lesser FAR and FRR rates with a system efficiency of 98%.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] F. Hao, R. Anderson and J. Daugman, “Combining crypto with biometrics effectively,” *IEEE Transactions on Computers*, vol. 55, no. 9, pp. 1081–1088, 2006.

[2] A. Goh and D. C. Ngo, “Computation of cryptographic keys from face biometrics. Communications and multimedia security,” *Advanced Techniques for Network and Data*, vol. 1, no. 1, pp. 1–13, 2003.

[3] F. Monrose, M. K. Reiter and Q. Li, “Cryptographic key generation from voice,” in *Proc. of the 2001 IEEE Symp. On Security and Privacy*, Oakland, CA, USA, pp. 192, 2001.

[4] J. Liao, J. Xiao and Y. Qi, “ID-based signature scheme without trusted pkg,” *Information Security and Cryptology*, vol. 5, no. 8, pp. 53–62, 2005.

[5] J. Schmidhuber, “Deep learning in neural networks: An overview,” *Neural Networks*, vol. 6, no. 4, pp. 192–203, 2015.

[6] A. Selwal and S. K. Gupta, “Template security analysis of multimodal biometric frameworks based on fingerprint and hand geometry,” *Perspectives in Science*, vol. 20, no. 1, pp. 705–708, 2016.

[7] W. Yang, S. Wang and J. Hu, “Security and accuracy of fingerprint-based biometrics: A review,” *Symmetry*, vol. 11, no. 2, pp. 141–152, 2019.

[8] B. Carrara and C. Adams, “You are the key: Generating cryptographic keys from voice biometrics,” in *Proc, IEEE Symp. on Security and Privacy*, Ottawa, Canada, pp. 1012–1019, 2001.

[9] C. T. Li and M. S. Hwang, “An efficient biometrics-based remote user authentication scheme using smart cards,” *Journal of Network and Computer Applications*, vol. 5, no. 5, pp. 1–5, 2010.

[10] G. Chen, Y. Mao and C. K. Chui, “Asymmetric image encryption scheme based on 3D chaotic cat maps,” *Chaos Solitons Fractals*, vol. 21, no. 3, pp. 749–761, 2004.

[11] N. K. Ratha, “Privacy protection in high security biometrics applications,” *Ethics and Policy of Biometrics*, vol. 20, no. 12, pp. 62–69, 2010.

[12] S. Aanjanadevi, V. Palanisamy and S. Aanjankumar, “An improved method for generating biometric cryptographic system from face feature,” in *Proc. of the Third Int. Conf. on Trends in Electronics and Informatics (ICOEI 2019)*, Tirunelveli, India, pp. 153–165, 2019.

[13] E. Volna, M. Kotyrba and V. Kocian, “Cryptography based on neural network,” in *Proc. 26th European Conf. on Modelling and Simulation*, Ostrava, pp. 712–723, 2012.

[14] K. Noaman and H. Jalab, “Data security based on neural networks,” *Task Quarterly*, vol. 9, no. 4, pp. 409–414, 2005.

[15] S. Aanjanadevi, V. Palanisamy and S. Aanjankumar, “A secure authenticated bio-cryptosystem using face attribute based on fuzzy extractor,” *New Trends in Computational Vision and Bio-inspired Computing*, vol. 1, no. 1, pp. 379–385, 2018.