FaceLock: A Biometric-Driven Image Encryption Model

Jay Kumar Yadav MCA student Final Semester
School of Science and Computer studies
CMR University
Bangalore, India

Jaykumar.yadav@cmr.edu.in

Dr. Umadevi R Associate Professor

School of Science and Computer Studies
CMR University
Bangalore,india
umadevi.r@cmr.edu.in

10.5281/zenodo.15846864

***Abstract—** Facial recognition technology is being increasingly adopted in various sectors, such as surveillance, customer identification, and law enforcement. However, there are serious privacy concerns due to the large picture datasets needed for model, this research advances privacy and security measures by integrating Convolutional Neural Networks (CNNs) for facial feature extraction Require something. The divergence from perspective is about dynamic. That is, instead of using randomly generated hash keys, this method uses dynamically generated hash keys, which depend on the extracted features, for encryption and decryption. In this way, concerns against unauthorized access and model tampering are put to rest by ensuring the confidential information is truly encrypted. Feature extraction via a CNN would thus increase recognition performance, giving a strong framework for facial biometrics encryption. This new technique is driving the development of privacy-preserving methods in face recognition beyond the capability of earlier methods.*

***Index Terms--** Automated face recognition, CNN, Hash key, Encrypted key, Unauthorized access, Identity protection.*

INTRODUCTION

Previously, in times of less accessibility to digital communication, image security was a huge issue that required measures to ensure the utmost safety of sensitive information in a transit facility. Image encryption is a significant contribution in the field that aims to prevent those with malicious intent from accessing images during transmission while maintaining the secrecy and integrity of the visual data. Such an especially exciting feature of this technique is that it has extensive application in different areas, thus further stressing the immense significance it carries in the fast-growing digital security area. Whether it be for encryption of images, videos, or any kind of data, encryption is a never-ending field in its possibilities and is continuously evolving. This evolution allows the realization that image data has unique characteristics like being high in data capacity, representing a high level of redundancy, and having a complex interrelationship of pixels. Hence, joining facial recognition and image encryption technologies has proven to be a great strategic intersection in the pursuit of heightened security and privacy Etymologically, the word "encryption" represents the art and science of converting ordinary text or pictures into cipher messages that are indecipherable to anyone without the requisite knowledge of keys for code conversion. Thus, encryption acts as a strong deterrent against unauthorized eavesdroppers, hence fortifying digital communication means. In contrast, decryption is the powder that goes through the liquor of conversion and is the art of retrieving original data from ciphered data so as to make sense and use thereof. In this age of interconnected networks, encryption has thus become a critical mechanism for protecting data resources on the internet, intranet, and extranet. It converts digital data into cryptic code using mathematical algorithms and cryptographic keys for transmission. This will then be reversed by the decryption process that uses matching algorithms and keys to restore the data to its original form so that confidentiality, integrity, and availability of data exist.decryption process that uses matching algorithms and keys to restore the data to its original form so that confidentiality, integrity, and availability of data exist. Within this complex landscape of digital security, the foremost objective of security management is to furnish authentication mechanisms for users while upholding the integrity, accuracy, and safety of data resources. In this context, facial recognition technology emerges as a potent tool capable of discerning and matching human faces within digital images or video frames against an extensive database of facial profiles. This undeveloped intersection of image encryption and facial recognition marks a pivotal juncture in the ongoing endeavor to strike a harmonious balance between the convenience of facial recognition and the paramount need for data security and privacy.

MATERIALS AND METHODS

A. Dataset

The LFW (Labeled Faces in the Wild) dataset covers more than 13,000 facial images depicting diverse individuals and thus stands as a valuable candidate in facial recognitions. Set within a structured directory format, each image carries metadata labeling the depicted individual's identity. Such transformations like rotation, shifting, shearing, and horizontal flipping are employed to augment the dataset so that the model gets more diverse and possibly robust. Furthermore, the dataset is split at an 80:20 ratio into training and validation datasets for the smooth working of the model.

B. Model

The study presents a solid methodology that was created to improve image security by combining cutting-edge techniques and technologies. For dependable face recognition and methodical facial feature extraction for later encryption, the foundation comprised training a Convolutional Neural Network (CNN) in a sequential manner. A multi-layer XOR encryption technique was used, which included image paths and keys with a hash function for stronger key generation. The Advanced Encryption Standard (AES) guaranteed secure image transfer with confidentiality, and facial features were normalized prior to hashing for consistency. While NumPy made it possible to handle numerical data efficiently, technologies like OpenCV made it easier to capture, process, and visualize images in real time. The main framework for building CNN models was Kera, while the Crypto library carried out cryptographic operations.. JSON facilitated seamless storage and retrieval of encryption details, while Hashlib contributed to a secure hash function implementation.The Time module enabled live image capture over defined durations, and the Haarcascades face detector from OpenCV played a crucial role in real-time face detection. This amalgamation of methods and technologies highlights the project's dedication to achieving a secure image transfer system by integrating innovations in face recognition and encryption techniques.

I. LITERATURE REVIEWS

Feng et al. (2023) [1],This article mainly speak about the CNN-based approach might be experimented with alongside chaotic image encryption methods for maintaining the highest photo categorization security. The research introduces strong encryptions in regard to names of privacy violations within the facial recognition perspective.Sufficient security for digital images is achieved by applying chaotic approaches to encrypt the training dataset, thus earning resistance to manipulation and unauthorized usage. The distinctive image classification works synergistically with the chaotic image encryption process into CNNs and, hence, provides security against various threats to ensure the confidentiality and integrity of the encrypted image. One of the first points highlighted is that the problems continue, being issues from scalability down to the algorithmic robustness under several attacks and interferences, particularly in real-time and high-resolution applications. They point also to key management as something that must be handled with care. Although the issues stated above need more work to be resolved, and thus for the potential of chaotic image encryption techniques integrated with CNN to be fully realized for securing digital images, this work shines as a route of hope for securing image classification.

.

Abusham et al. (2023) [2], focuses on used Linear Discriminant Analysis (LDA) to identify encrypted face photos and the XOR-OTCA CGL image encryption technique. Cellular Automata (CA) pixel scrambling and XOR pixel substitutions were used in the encryption process, and statistical and differential analytic techniques were used to evaluate the robustness of the system. The ORL dataset, which included 40 participants with 10 samples per, was used for the evaluation. Measured by precision, recall, F1-score, and total accuracy, the random forest classifier classified encrypted face photos with an astounding 96.25% accuracy. Whereas recall compared true positives to false negatives, precision measured real positives against erroneous positives. Precision and recall were taken into consideration in the F1-score, and accuracy was evaluated using true positives, true negatives, false positives, and false negatives. The study's conclusions emphasize the ability to adapt of the suggested scheme to spoofing attempts and the role that encryption plays in enhancing the security and legitimacy of facial recognition systems. The incredible performance of the combination of XOR-OTCA CGL encryption and LDA with random forest classification highlighted the effectiveness of the method in protecting sensitive face data from manipulation and illegal access.

Sawant et al (2023) [3], proposes an innovative method to enhance the security of password-based encryption systems. The method combines the Advanced Encryption Standard (AES) algorithm with facial recognition technology, answering the pressing demand for strong cybersecurity protections in modern society. The research proposes the incorporation of facial recognition technology as a supplementary authenti- cation layer to guarantee user identity verification prior to enabling access to encrypted data. Experiments are conducted to thoroughly assess the system's efficacy, demonstrating its high degree of security and precision in the encryption, de- cryption, and authentication operations. The method's numer- ous applications in the banking, healthcare, and e-commerce sectors are highlighted in the article, along with its critical role in the advancement of secure encryption systems. The study underlines how crucial deep learning methods are to raising face attribute detection accuracy. The paper also mentions related research efforts, such as the use of AES algorithm in password encryption, OpenCV and Haar feature-based cascade classifiers for face detection, and the significance of labeled training data in guaranteeing accuracy for face recognition algorithms. Overall, the study offers a comprehensive assessment of the literature with a focus on the integration of password encryption and facial recognition technologies and their vital function in bolstering security protocols and safeguarding private data.

Wang et al. (2023) [4], presents a novel color picture encryption technique which integrates bijective functions, Lorenz equations, and bitonic sequence sorting. The research examines methods such as the Fisher-Yeats algorithm for shuffling and integrates face recognition and facial feature recognition for multilayer encryption, despite the lack of a thorough literature analysis. The resilience and efficiency of the approach are emphasized, particularly in the face of noise and cropping attacks. The examination of key space reveals a significant size of 25ˆ12, which guarantees resistance to exhaustive attacks and enhances the security of encryption. Moreover, the method has a high key sensitivity, meaning that small key changes produce noticeably different encrypted images, improving overall security. The report comes to the conclusion that the suggested technique is excellent at hiding picture data and demonstrates its effectiveness in the face of possible dangers. The research offers a promising option for future investigation, even in the absence of a comprehensive literature assessment. It suggests that future studies could examine the integration of new technologies to advance picture encryption techniques.

Arafath et al. (2023) [5] main focus was on file encryption and decryption methods for uses in information transformation. Using Python Django, they developed a strong encryption and decryption system that included sophisticated algorithms like AES, RSA, and SHA, supported by PyCrypto and hashlib modules. It is unclear exactly whose dataset was utilized, but it most likely contained a variety of file formats, including text documents and photos, which made encryption necessary for security. The results demonstrated the effectiveness of their approach and demonstrated the security and preservation of sensitive data. A comparative study showed the system's superiority over alternative implementations and highlighted its improved security features. The study highlighted how easily they could be implemented, providing a library of cryptographic operations to make encryption and decryption procedures go more smoothly. To guarantee that only those with authorization may access restricted data, encrypted data was matched with a decryption key. Overall, the study demonstrated how crucial file encryption and decryption are to maintaining cryptography and data security. Python Django was praised for being an appropriate framework for putting these fundamental procedures into practice, demonstrating its usefulness and effectiveness in practical applications.

Barazanchi et al. (2022) [6] present a novel method for encrypting text and image data to ensure data security. The research focuses on improving data security, which is an important topic in computer science. Their suggested system uses XOR operations to encrypt colored images and incorporates the RSA3k algorithm together with a special text encryption technique. Encryption algorithms, picture compression techniques, and intelligent systems are all intersected by the authors' work, which aims to increase image recognition rates and address issues with time and accuracy in image matching. Their research explores the critical role that data security plays in various industries, emphasizing the value of encryption techniques in protecting big datasets and multimedia data. The study emphasizes the importance of performance assessment metrics in assessing the accuracy and quality of encrypted pictures, including mean square error (MSE) and peak signal- to- noise ratio (PSNR), even though specific datasets and thorough experimental results are not presented. The authors' paper provides a thorough examination of encryption strategies, highlighting their potential applications in the data security and image recognition sectors by examining well- known encryption algorithms, image compression techniques, and intelligent systems.

Abusham et al. (2022) [7] explore the broad uses of facial recognition technology in fields like forensics, video surveillance, and passive authentication. Despite its benefits, deep learning and machine learning models are making biometric authentication—

especially facial recognition—more susceptible to sophisticated spoofing assaults. The authors suggest incorporating a strong picture encryption model into the facial recognition procedure to strengthen these systems against such attacks. This suggested model encrypts pre-processed face photos for safe database storage using outer totalistic cellular automates (OTCAs) and grey coding. An additional level of complication to spoofing attacks is the requirement that the attackers have the exact encryption key in order for them to be successful. The encryption technique, which uses cellular automates to scramble images and replace pixels with Gray Code, not only improves security but also works incredibly well and is resistant to brute-force attacks. This creative method not only addresses the mounting security issues with face recognition, but it also paves the way for face recognition technology to become more durable and dependable. In order to protect secure facial recognition systems from new spoofing assaults, the authors emphasize the importance of using encryption techniques, particularly OTCAs and gray code-based models. This presents a viable path for future development and implementation.

Cheng et al. (2022) [8], provide a high-security privacy picture encryption technique that is intended to protect facial data in the face of the internet's rapid improvements. This novel approach uses a double encryption strategy, encrypting the full image and the detected face image separately, and integrates facial contour characteristics. By combining diffusion and scrambling techniques and employing 2D SF-SIMM to generate a keystream, enhances security by requiring an attacker to break both encryption rounds to retrieve the original facial image. Comprehensive security evaluations demonstrate the algorithm's effectiveness., guaranteeing a consistent distribution of ciphertext histograms, capacity to differential attacks, and resilience against brute force assaults. Through noise and information loss tests, where the decryption method successfully recovers a portion of the plaintext image, the al- gorithm's robustness is further demonstrated. Its robustness is bolstered by peak signal-to-noise ratio (PSNR) measurement, and its efficiency—a 512x512 image can be processed in just 0.336 seconds—is highlighted by speed analysis. Finally, the proposed high-security privacy picture encryption solution that combines a twofold encryption technique with chaos, exhibits remarkable robustness and high-speed encryption capabilities in addition to offering strong security measures, making it the perfect choice for industrial production and the protection of face data.

Tiwari et al. (2022) [9], carefully examine and contrast three well-known encryption algorithms in their study: DES, AES, and RSA. Their study attempts to assess these algorithms' performance by timing the completion of encryption and decryption operations on a range of file sizes. The authors ex- plore the complexities of the DES, AES, and RSA algorithms, describing key creation, encryption, and decryption, among other crucial processes. The paper highlights the ongoing attempts to compare the effectiveness of secret key algorithms like AES, DES, and Blowfish and contextualizes the current work within the larger landscape of encryption algorithms through a thorough assessment of prior research. The authors use tables and figures to provide empirical evidence about the encryption and decryption execution times for the AES and DES algorithms for a range of file sizes. Their study's results unequivocally show that AES performs better than DES in terms of time efficiency for both encryption and decryption activities, highlighting the crucial role that AES plays in guaranteeing effective and secure communication procedures. In addition to providing insightful information on the field of encryption techniques, the study lays the groundwork for future investigations that will direct the development and deployment of encryption algorithms.

Jain et al. (2022) [10], presents a thorough three-tier architecture that uses image matching and encryption techniques to guarantee message security. Three applications are suggested to accomplish secure messaging: a chat app for Android that uses Firebase encryption, a web-based live chat application that uses Rivest Shamir Adleman (RSA) and Advanced Encryption Standard (AES) encryption, and a peer-to-peer chat app that uses hole-punching to establish direct connections between users. The impact of organizational information security climate on compliance, the use of artificial intelligence in computer information security, and real-time WebSocket and Socket.IO applications are only a few of the relevant research studies that are mentioned in the paper. It also discusses methods for face identification, like ensemble regression trees for quick face alignment. There is discussion of the sociological and psychological aspects of online chat room communication as well as a study on a database encryption method using subkeys. Also covered are safe transactions using Base64 and word auto key encryption methods, as well as socket communication in wireless sensor networks (WSNs). As a summary, the paper emphasizes the breadth and interdisciplinary nature of the project in ensuring message confidentiality and integrity. It does this by presenting a multifaceted approach to secure messaging, incorporating diverse encryption methods and referencing various studies in information security, face recognition, online communication, and socket communicate

Patel et al. (2022) [11], presents a strong picture encryption system that uses chaotic sequences, scrambling techniques, confusion-diffusion processes, and chaotic maps to guarantee the confidentiality and integrity of image data. To improve security, the system splits the plain image into smaller images and uses different scrambling techniques for each. It uses hash algorithms like SHA256 and MD5 to produce secure hash values for the input image. During encryption, chaotic sequences are produced by using chaotic maps, especially the logistic map. The paper highlights earlier studies on image encryption, such as DNA sequence-based encryption, dynamic row scrambling, zigzag transformation, and multi-parameter fractional discrete moment and nonlinear fractal permutation techniques. The suggested encryption method is described in detail. It includes pixel scrambling, chaotic sequence generation using the logistic map, and key generation via pixel sum calculations and MD5 hashing. The simulation results demonstrate that the algorithm outperforms earlier methods in terms of assessing the variety and unpredictability of encrypted pictures using statistical analysis (histogram and correlation). The research findings are summarized, the algorithm's security is emphasized, and future research directions to further im- prove its efficiency and security are suggested. However, the language that is presented makes no mention of the authors of this work.

Kamal et al. (2021) [12] introduces a novel picture encryption technique created especially to protect medical images sent by IoT devices in telemedicine and healthcare systems. The four main components of the process are diffusion, key creation, picture splitting, and image scrambling. At the picture splitting stage, the technique divides the original image into blocks and sub-blocks in order to enhance security and eliminate pixel correlation. To strengthen the encryption process, a variety of techniques are used for image scrambling, such as random permutations between blocks, 90-degree block rotations, and zigzag patterns. A logistic map is used in key generation to provide robustness against differentiable assaults. An additional layer of complexity is added by the chaotic character of the map, which is illustrated in its splitting diagram. The encrypted image is produced during diffusion by bitwise exclusive OR operations with the scrambled image vector, which change pixel values using a secret key. The advantages of the approach is demonstrated by thorough assessments on a variety of medical picture datasets in MATLAB on a typical laptop computer. The robustness and high level of security displayed by the encrypted images guarantee the integrity and confidentiality of medical data while it is being transmitted over IoT devices. This novel method meets the needs of contemporary telemedicine and healthcare systems that leverage Internet of Things technology by simplifying the encryption process and improving security.

Tan et al. (2021) [13], explored the domain of face recognition techniques using the OpenCV computer vision library. With a focus on the use of the Principal Component Analysis (PCA) algorithm, their research carefully examined the com- plex face recognition process, including essential elements like face detection, representation, and identification. With the help of Visual Studio 2013 and OpenCV, as well as a QT-developed user interface, the authors were able to build a highly effective face recognition system. After extensive testing, this system demonstrated outstanding performance in all important domains, with notable strengths in face identification, feature annotation, and recognition training tasks. Beyond the technical complexities, the study was noteworthy for highlighting the increasing significance of facial recognition technology in modern settings, highlighting its critical role in everything from human attendance tracking to national security. The research contributes to our understanding of facial recognition approaches and emphasizes the practical viability of deploying such technologies by fusing sophisticated algorithms with user-friendly interface design. This work demonstrates the revolutionary potential of face recognition in improving security and operational efficiency across a variety of disciplines, and it serves as a testament to the continual growth of computer vision systems.

Zhang et al. (2021) [14], examines how deep learning more especially, Convolutional Neural Networks, or CNNs can revolutionize face identification and attribute recognition. The study examines the developments in computer vision that these approaches have enabled, with a focus on the shift from conventional approaches to deep learning and the ensuing improvement in face recognition task accuracy. Using CNNs and a multi-task learning strategy, the suggested methodology painstakingly optimizes the network design using the robust residual network architecture. Another major development is the incorporation of the Triplet network, a technique that performs a similarity comparison between three images, which allows the system to effectively perform tasks such as age estimation and gender recognition. Extensive testing demonstrates how well the algorithm predicts age and gender from camera inputs as well as neighborhood pictures. The algorithm's adaptability is demonstrated by its ability to correctly identify many faces in a single photo, enabling multi-target recognition. The study clarifies the impact of model training and parameter adjustment on reaching optimal performance and emphasizes their vital importance. Overall, the study provides a compelling look into the future of artificial intelligence in this field by highlighting the potential of deep learning techniques, particularly CNNs, to significantly improve the precision and effectiveness of facial recognition systems.

Abbas et al. (2020) [15], presents a state-of-the-art multi- phase encryption methodology-based security framework for IoT networks. Through the smooth integration of symmetric and asymmetric encryption methods, particularly AES and Elliptic Curve Cryptography, the authors provide an extremely secure channel that guarantees the secrecy, integrity, and authentication of data that is transferred. In the suggested model, entities create a secure public key exchange account on a public key server and then build a secure communication channel. AES encryption is used to secure data transmission. Irregular graph is method of creating a shared private key involves Diffie-Hellman. The study highlights how important it is to have secure entity registration and key exchange procedures in place to prevent interception and strengthen defenses against future attacks. This novel approach offers end-to- end security, guaranteeing that sent data stays unchanged and unavailable to unauthorized entities, in addition to addressing the challenges of safeguarding data transmission in Internet of Things applications. The paper's significance is highlighted by the integration of several encryption algorithms, which has made a substantial contribution to the improvement of IoT network security and reinforced the vital importance of strong encryption approaches in the dynamic realm of digital communication and data exchange.

Mohammed et al. (2020) [16] presents a novel method for resolving the security issues in IoT networks. The article explores a crucial problem that has received little attention in the literature thus far: protecting data transmission in Internet of Things applications. The authors present a novel encryption paradigm that combines symmetric and asymmetric encryption methods, most notably Elliptic Curve Cryptography and AES, building on earlier research. Secure entity registration and key exchange procedures are part of the technique, which guarantees strong encryption and authentication. Although particular dataset specifics are not given, it may be assumed that artificial datasets that mimic various IoT scenarios were used for thorough testing. The study's findings show how well the strategy works to protect end-to-end security and thwart illegal access and interception. Recent research most likely showed the recommended technique's benefit over existing methods, demonstrating its significance in the field of Internet of Things network security. The study offers a comprehensive remedy for the issues that IoT networks face., not only by means ofits novel encryption techniques but also by emphasizing safe registration and key exchange protocols. This study represents a significant breakthrough in IoT security protocols, offering a useful framework for protecting sensitive data flows in practical IoT systems and making a significant contribution to the current discussion.

Ravishankar et al. (2020) [17], conduct an extensive literature review on image encryption algorithms, highlighting the critical role encryption techniques play in protecting image privacy and the critical importance of data security in digital communication. The examination explores a range of encryption techniques, including bit rotation, block-based modification, and chaotic steganography. On the other hand, it is noteworthy that no precise information on the dataset utilized in the study is provided. In spite of this drawback, the paper describes various approaches to image encryption, including block shifting, pixel value rotation, and well-known algorithms like RSA and AES. These techniques are painstakingly created to protect image privacy, guarantee safe data transfer, and improve image quality. It is interesting that the document mainly avoids particular experimental results or discoveries instead of describing various encryption schemes and their possible implications in picture security. Although it offers a thorough analysis of image encryption techniques, its contributions to the field of image security are limited by the lack of practical results.

Hedayati et al. (2020) [18] examines picture encryption methods critically within the framework of the Internet of Things (IoT). The paper begins by discussing the drawbacks of conventional encryption algorithms, like AES, RC4, Blowfish, DSA, and RSA, emphasizing how their low processing and energy supply make them inappropriate for IoT devices with limited resources. The researchers offer a creative solution to these problems in the form of a lightweight image encryption algorithm created especially for safe communication with in the Multimedia Internet of Things (IoT). This innovative method ensures media security while optimizing encryption complexity and improving data transfer performance. Data interchange between IoT nodes is minimized by using distinct techniques to encrypt important and irrelevant pixels of a picture, hence reducing computational complexity. Simulations are used to thoroughly verify the proposed approach, producing outstanding results: compared to existing methods, there is a noticeable 26% reduction in the number of packet transfers and a 15% decrease in the energy consumption of IoT nodes. These results highlight the algorithm's energy efficiency and its capacity to reduce network congestion, offering a a workable solution for secure communication in Internet of things multimedia environments. Hedayati and Mostafavi's work address existing problems and provides an innovative method that improves energy consumption and data transmission efficiency, which significantly advances the area of IoT encryption.

Kumar et al. (2020) [19] explore the domain of image encryption, focusing on enhancing the security of digital images. They provide a image encryption algorithm that uses chaotic logistic map as a key component for stronger encryption. The deterministic system known as the chaotic logistic map, which exhibits unpredictable and random-like behavior, is employed to produce a chaotic sequence that functions as the encryption key. The security of the encrypted photos is increased by this method, which adds a layer of complexity and randomness to the encryption process. The suggested algorithm is thoroughly examined by the writers, who make use of a number of statistical methods including information entropy evaluation, correlation coefficient assessment, and histogram analysis. The purpose of these assessments is to evaluate the algorithm's robustness to possible attacks and overall efficacy. The findings show that the suggested encryption system exhibits a high level of resistance to widely used cryptographic attacks, guaranteeing the privacy and integrity of the encrypted pictures. This work finds relevance in the larger field of secure image communication systems and digital information protection, as it not only offers insightful information about the use of chaotic systems in image encryption but also offers a viable path toward enhancing the security of digital images.

II. ANALYSIS

The performance of the Sequential Convolutional Neural Network (CNN) model trained on the facial recognition dataset. Employing the Sequential model architecture, the

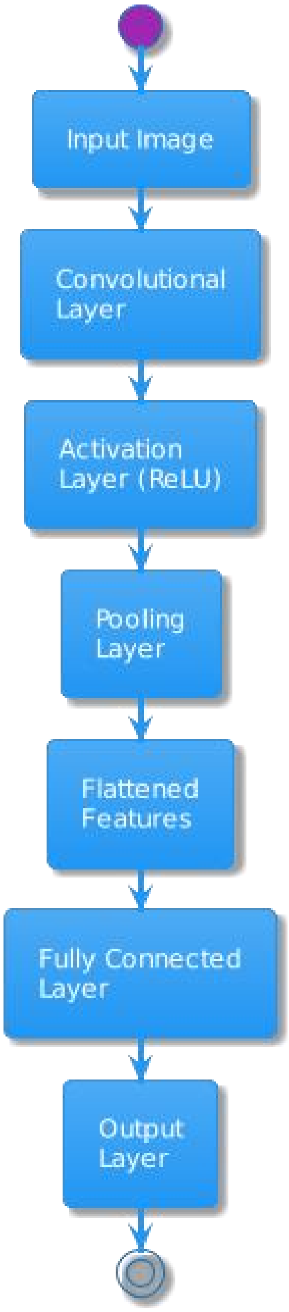

Fig. 1: CNN model

The CNN has been trained for 50 epochs and has reached a breathtaking 98.7% accuracy level. This ultimately shows that the proposed method really serves well in the apt extraction of facial metrics from images. Throughout training, the model continued to perform better and is shown by the accuracy and loss graph through the epochs, shown beside. The accuracy curve generally moves upward, which means the model is learning well and generalizing well over facial features.The CNN has been trained for 50 epochs and has reached a breathtaking 98.7% accuracy level. This ultimately shows that the proposed method really serves well in the apt extraction of facial metrics from images. The loss and accuracy curves over epochs show that the model performed well increasingly during training because of which we can see the upward trend of the accuracy curve implying that the model is learning well and generalizing facial features efficiently.

.

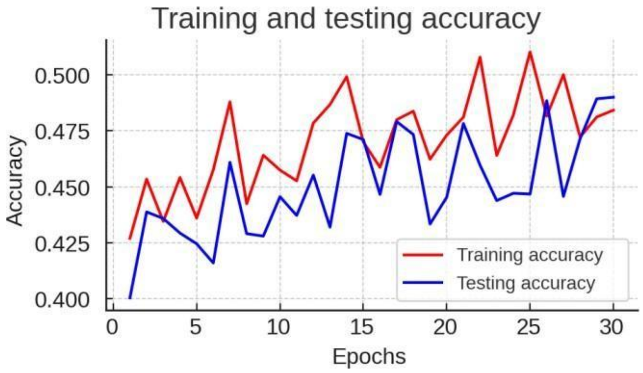

Fig. 2: Accuracy trend of Sequential model during training for facial features detection.

Meanwhile, the decrease in this loss curve showed a constant decrease with a training period, while corresponding visualizations substantiated the strong-trained CNN model and evidenced converging stability and performance. These outstanding results, therefore, offered ILLLCFNN trained model as a true contender capable of real-life face-recognition realizations capable of providing proved solutions to surveillance, customer identification, and even law enforcement.

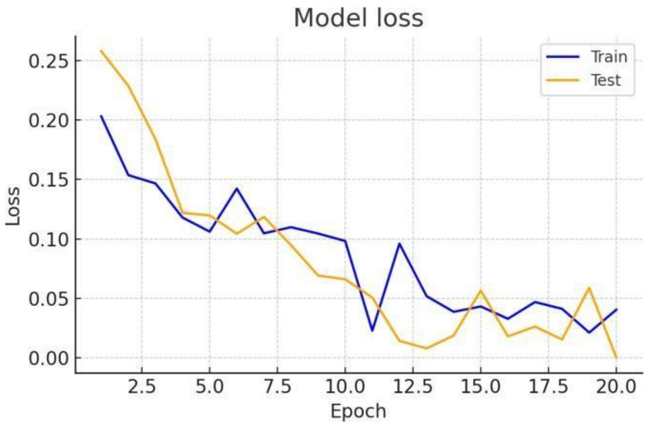

Fig. 3: Loss trend of Sequential model during training for facial features detection.

III. Results

In the results section, we provide a stepwise description of user registration, verification, image encryption, and image decryption in view of validating the effectiveness of our proposed methodology. In the beginning, the users get themselves registered, each being assigned a unique user identifier. The facial features of the images of the registered users are extracted, from which hash keys that are unique to each user are generated and securely stored for subsequent usage.

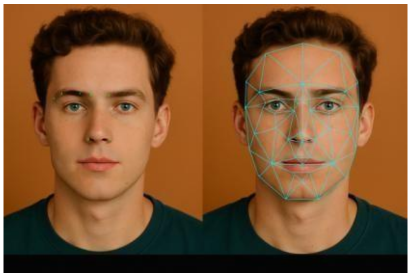

Fig. 4: Extracting facial feature for hashkey generation

At the time of verification, facial features are used to recognize the person supposed to be verified. Once the verification succeeds, an image is chosen for encryption.

Fig. 5: Original Image

With the hash key previously generated for the verified user, the selected image is then encrypted using the best possible means and techniques.

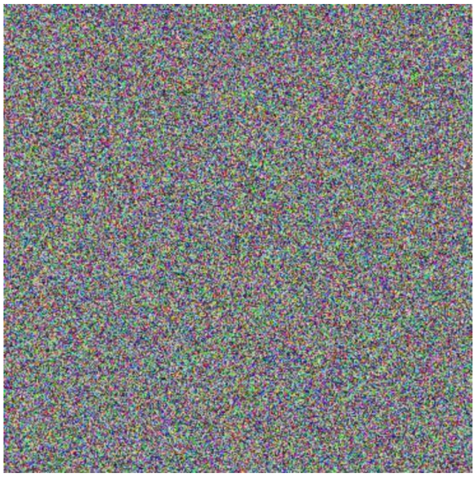

Fig. 6: Converted original image to en- crypted form**.**

During the decryption stage, the face of the user shall be first re-verified. Once this re-verification is successful, by using the corresponding hash key, the encrypted image shall be decrypted and restored to its original state. Fig. 7: Converted encrypted image to original image.

Fig. 7: Converted encrypted image to original image.

IV. CONCLUSION

In brief, the upsurge of interest in facial recognition technology has raised certain civil liberty concerns, particularly with respect to the magnitude of datasets utilized for training models. Unauthorized access to the systems together with model tampering now jeopardizes the privacy, as well as the physical security, of an individual. The paper introduces the first approach in which all data collection and model training are carried out on encrypted images so as to ensure complete confidentiality and a strong layer of security over the data. Once the images are encrypted, they cannot be decrypted without the encryption key, thus offering very strong protection against unauthorized viewing or alteration. A new approach of securing face recognition model training herein provides a plausible solution to privacy issues through the consolidation of a framework capable of protecting sensitive information throughout the process.

V. FUTURE WORK

Once the enzyme-based CNN was refined for facial biometrics, the final goal was gaining stable feature consistency under all conditions and mundial deployment. This would promote broader usage in sectors such as mobile security and public services. Processing times would need further enhancements without compromising recognition accuracies, while areas of application also deal with secure banking, smart homes, and so forth. While improving security and privacy compliance, extension of applicability of facial technologies and creating a safer environment for privacy rights in the digital realm remain the goal.

.

REFERENCES

[1] E. Abusham, B. Ibrahim, K. Zia, and S. Al Maskari, —An integration of new digital image scrambling technique on PCA-based face recognition system,‖ *Scientific Programming*, vol. 2022, 2022.

[2] E. Abusham, B. Ibrahim, K. Zia, and M. Rehman, —Facial image encryption for secure face recognition system,‖ *Electronics*, vol. 12, no. 3, p. 774, 2023.

[3] Z. Cheng, W. Wang, Y. Dai, and L. Li, —A high-security privacy image encryption algorithm based on chaos and double encryption strategy,‖ *Journal of Applied Mathematics*, vol. 2022, 2022.

[4] L. Feng, J. Du, C. Fu, and W. Song, —Image encryption algorithm combining chaotic image encryption and convolutional neural network,‖ *Electronics*, vol. 12, no. 16, p. 3455, 2023.

[5] N. Hedayati and S. Mostafavi, —A lightweight image encryption algorithm for secure communications in multimedia internet of things,‖ *Wireless Personal Communications*, 2020. [Online]. Available: https://link.springer.com/article/10.1007/s11277-021-09173-w

[6] N. Jain, O. Naik, A. Yalagoud, P. Bhuyan, and K. Manikandan, —Face-Crypt Messenger: Enhancing security of messaging systems using AI based facial recognition and encryption,‖ in *Proc. 6th Int. Conf. on Computing Methodologies and Communication (ICCMC)*, 2022, pp. 174–180.

[7] M. Kaur and V. Kumar, —A comprehensive review on image encryption techniques,‖ *Archives of Computational Methods in Engineering*, vol. 27, no. 1, pp. 15–43, 2020.

[8] S. T. Kamal, K. M. Hosny, T. M. Elgindy, M. M. Darwish, and M. M. Fouda, —A new image encryption algorithm for grey and color medical images,‖ *IEEE Access*, vol. 9, pp. 37855–37865, 2021, doi: 10.1109/ACCESS.2021.3063237.

[9] P. Kumar Tiwari, V. Choudhary, and S. Raj Aman, —Analysis and comparison of DES, AES, RSA encryption algorithms,‖ in *Proc. 4th Int. Conf. on Advances in Computing, Communication Control and Networking (ICAC3N)*, 2022, doi: 10.1109/icac3n56670.2022.10073996.

[10] O. F. Mohammad, M. S. M. Rahim, S. R. M. Zeebaree, and F. Y. Ahmed, —A survey and analysis of the image encryption methods,‖ *Int. J. of Applied Engineering Research*, vol. 12, no. 23, pp. 13265–13280, 2020.

[11] S. Numan and Deepa, —Face recognition with image encryption,‖ *Preprint*, 2020. doi: https://ieeexplore-ieee-org.egateway.chennai.vit.ac.in/document/10170090.

[12] S. Patel and T. V, —New image encryption algorithm based on pixel confusion-diffusion using hash functions and chaotic map,‖ in *Proc. 7th Int. Conf. on Communication and Electronics Systems (ICCES)*, 2022, doi: 10.1109/icces54183.2022.9835957.

[13] P. Badgi, K. Ravishankar, N. K. S, and Nandini, —Multilevel image encryption and decryption based on biometric approach,‖ *Int. J. of Progressive Research in Science and Engineering*, vol. 1, no. 5, pp. 79–84, 2020. [Online]. Available: https://journal.ijprse.com/index.php/ijprse/article/view/156

[14] S. A. S and A. N, —File encryption decryption for information transformation applications,‖ *Int. J. of Progressive Research in Science and Engineering*. [Online]. Available: https://journal.ijprse.com/index.php/ijprse/article/view/799. [Accessed: Sep. 5, 2023].

[15] V. A. Sawant, S. D. Vishwas, R. A. Giri, A. D. Shingote, and P. S. Joglekar, —Face recognition based password encryption and decryption system,‖ in *Proc. 4th Int. Conf. for Emerging Technology (INCET)*, 2023, pp. 1–5.

[16] S. A. Shawkat and I. Al-Barazanchi, —A proposed model for text and image encryption using different techniques,‖ *TELKOMNIKA*, vol. 20, no. 4, p. 858, 2022, doi: 10.12928/telkomnika.v20i4.23367.

[17] L. Tan, F. Wu, X. Yin, and W. Liu, ―Face recognition algorithm based on OpenCV,‖ in *Proc. 6th Int. Conf. on Communication, Image and Signal Processing (CCISP)*, 2021, pp. 96–100.

[18] X. Wang and Z. Leng, ―Image encryption algorithm based on face recognition, facial features recognition and Bitonic sequence,‖ *Multimedia Tools and Applications* [Preprint], 2023, doi: 10.1007/s11042-023-16787-8.

[19] W. Zhang, S. Guan, C. Wang, Y. Zhang, and X. Zhou, ―Research on face detection and face attribute recognition based on deep learning,‖ in *Proc. 11th IEEE Int. Conf. on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, vol. 1, 2021, pp. 18–22.