ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25mar1119

Cancelable Face Recognition using Deep Steganography

[1]S. Lokesh; [2]V. Lokeshwaran; [3]R. Muthu Kumar; [4]M. Priyadharshini

[4]Guide
SRM Valliammai Engineering College
Kanchipuram, Tamil Nadu

Publication Date: 2025/03/29

Abstract: While the dawn of digital privacy fears strikes hard at the very thread of our existence, biometrics, one of the traditional systems, is at risk of invasion through privacy breaches and identity theft. This is because cancellable biometric systems promise through revocation and reissuance of biometric templates. Based on this opportunity, the present work proposes a novel approach in cancellable face recognition through deep steganography such that biometric data is embedded in digital images to protect user privacy while maintaining the highest possible recognition accuracy. The approach utilizes deep learning models to design effective steganographic encodings of facial features that will then be securely embedded into innocuous images. In any given scenario, the embedded features can be extracted and used for a face recognition, thereby not leaking the original biometric data. The steganographic process is reversible, so the original face template can be revoked and replaced with a new one if compromised. We test the proposed system on publicly available face datasets and check the recognition accuracy, steganographic robustness, and cancelability of the proposed method. The results show that the deep steganography-based approach obtains high recognition accuracy to compare with traditional face recognition systems but also provides an extra layer of security by having the cancelability. This is highly potent in improving the privacy and security of biometric systems.

Keywords: *Cancellable Biometric Systems, Face Recognition, Deep Steganography, Privacy, Identity Theft, Deep Learning, Biometric Template Revocation.*

How to Cite: S. Lokesh ; V. Lokeshwaran ; R. Muthu Kumar; M. Priyadharshini (2025) Cancelable Face Recognition using Deep Steganography. *International Journal of Innovative Science and Research Technology*, 10(3), 1469-1474. https://doi.org/10.38124/ijisrt/25mar1119

I. INTRODUCTION

In the current digital age, privacy concerns are a significant challenge, especially in the context of biometric systems. Among various biometric modalities, face recognition has gained considerable attention due to its non-intrusive nature and high [1] recognition accuracy. However, traditional face recognition systems raise significant concerns about privacy and security. Once biometric templates, such as facial features, are stored in a system, they are vulnerable to identity theft, data breaches, and misuse. Unlike passwords or PINs, biometric data cannot be changed or reset once compromised, making it a prime target for malicious actors. Cancellable biometric systems have emerged as a promising solution to address these issues. By enabling the revocation and reissuance [2] of biometric templates, cancellable systems provide an added layer of security. If a biometric template is compromised, it can be replaced with a new one without requiring the user to provide new biometric data. This flexibility mitigates the risks associated with identity theft, making cancellable biometrics an attractive option for privacy-conscious applications.

This work proposes a novel approach to cancellable face recognition [3] using deep steganography. Steganography, the practice of concealing information within other data, offers a way to protect sensitive biometric information by embedding it within innocuous images. Deep learning techniques are employed to enhance the robustness and effectiveness of the steganographic process, ensuring that the embedded facial features remain secure while still being usable for recognition tasks. By leveraging deep neural networks, robust encodings of facial features are created and embedded within digital images in a way that preserves both privacy and recognition accuracy.

The key innovation of this approach lies in the reversibility of the steganographic process. If a face template is compromised [4], it can be revoked by simply replacing the innocuous image containing the encoded biometric data. A new face template can then be generated, embedded in another image, and used for future recognition

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25mar1119

tasks. This cancelability feature adds an extra layer of privacy, ensuring that even if the embedded data is exposed, it does not lead to permanent identity theft.

The proposed system is evaluated on publicly available face datasets to assess its performance. Several metrics are used, including recognition accuracy, steganographic robustness, and the ability to revoke and replace compromised [5] biometric templates. The results of the evaluation demonstrate that the proposed deep steganography-based method achieves recognition accuracy comparable to traditional face recognition systems. Moreover, it provides an additional layer of security through cancelability, making it a viable solution for privacy-sensitive applications such as secure access control and authentication systems.

In summary, this work presents a new approach to face recognition that not only maintains high recognition accuracy but also addresses critical privacy and security concerns. By integrating deep learning-based steganography with cancellable biometric templates, the proposed system offers a promising solution for safeguarding sensitive biometric data while ensuring that it can be securely updated if compromised. The outcome of this research has the potential to improve the adoption of biometric systems in privacy-conscious environments, where user confidentiality and data protection are paramount.

This work is organized Section II as reviews the literature survey. Section III outlines the methodology, detailing its features and functionality. Results and discussion are found in Section IV, where the effectiveness of the system is analyzed. Finally, Section V concludes with key findings along with future implications.

II. LITERATURE SURVEY

The steganography features significantly in protecting confidential information, especially in biometric systems, like face recognition. New approaches, such as coverless steganography and reversible LSB techniques, enhance the sophistication of data hiding and security. Clean label backdoor attacks and hybrid mapping image synthesis frameworks have become lately necessary for the secure training of deep learning models for face recognition. Hence, this survey covers such cutting-edge approaches that have significantly made the face recognition technology more robust and private.

A diffusion model-based coverless steganography framework is proposed to enhance the privacy protection of face recognition images. The proposed [5] method includes feature extraction, mask generation, and utilization of deterministic Denoising Diffusion Implicit Model, and then evaluation is conducted using high-quality steganographic images. The method obtained an over-96% recognition accuracy, and it was resistant to detection, making such sensitive face images more secure.

Comprehensive Review of Eigenface-based face detection based on Principal [6] Component Analysis. The work reviews the issues on the approach to different mechanisms on detection with regards to benchmark datasets. It addresses the pitfalls of the current systems to lighting conditions and occlusions-a research direction for future work on Eigenface-based face detection systems.

A clean label backdoor attack method for deep learning-based face recognition [7] models is proposed focusing on scalability and effectiveness, which leads to the discovery of physical triggers in poisoned samples by accessory injection and optimization-based feature transfer techniques. These can overcome limitations and render it successful with high success rates on unseen samples while maintaining the classification accuracy.

This work discusses the advancements of reversible LSB steganography with [8] a focus on security and confidentiality in communication. In medical imaging and satellite applications where the integrity of stego-image should be maintained, reversibility is an absolute necessity to restrict access to unauthorized persons. It envisages the importance of secured steganography that adheres to Kerckhoff's principle for the sake of safety of sensitive information.

By proposing the design of a hybrid image synthesis mapping framework for steganography without embedding, which addresses [9] the problem of current SWE techniques. It works by combining synthesis and mapping modules; then the technique allows for the hiding of secret messages using less image distortion along with higher payload capacity. We conducted extensive experiments and presented it clearly in comparison to the existing SWE techniques in terms of efficiency and accuracy.

A coverless steganography technique for face recognition images is proposed [10] with an intention to improve the diffusion model, so as to result in better privacy protection. Here, it uses the Denoising Diffusion Implicit Model as a deterministic one to extract facial features, produces masks, and then creates high-quality steganographic images. The proposed approach got the ability to achieve recognition accuracies above 96% along with resistance to the detection method to further improve security over sensitive face images.

An elaborate review of face detection by Eigenfaces, based on Principal Component Analysis [11] frames the face recognition system and approaches. Several eigenface-based face detection methods have been reviewed critically, as have applications and relevance of benchmarking datasets. Sensitivity to lighting variations as well as occlusions in images poses challenges with Eigenfaces face detection. These provide insights on future prospects of technologies based on Eigenface in face detection.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25mar1119

A clean-label backdoor attack technique tailored to the scalable and effective deep learning-based face recognition models is proposed [13] using the accessory injection technique combined with optimization-based feature transfer. The technique will focus on generating poisoned samples containing physical triggers, overcoming the limitations of the current methods which are increasingly becoming obsolete due to the effects of erroneous classification accuracies on unseen samples as well as attack success rates.

This work outlines reversible Least Significant Bit (LSB) steganography that has proved to have considerable consideration in security [14] and confidentiality communication. Reversible algorithms have proven useful in data integrity applications, including medical imaging and satellite communications. The study emphasizes the importance of secure steganography that ensures not only confidentiality but also obeys principles of preventing access to information from unauthorized people.

A hybrid framework approach called SWE is proposed here, which integrates [15] synthesis and mapping techniques to overcome the two problems of current SWE methods. Here, the synthesized image provides the message hiding and a mapped image is used to correct the compression error in extractions, so this hybrid approach has better payload capacity and efficiency compared with other SWE approaches.

Here comes a method for secure face recognition through diffusion-based coverless steganography, the security technique that protects privacy without distortion to the original image. The method [16] is to use a conditional diffusion model with Denoising Diffusion Implicit Model for high-quality steganographic image generation. The experiments show how this approach will be effective in hindered steganalytic attack for robust privacy and ensures the accuracy of face recognition to more than 96% without compromise of the hidden information.

The problem of Principal Component Analysis is well highlighted along with its strength [17] and weakness in facial detection by analyzing the face recognition techniques based on Eigenfaces. A wide range of strategies and methodologies have been explored in the Eigenface-based detection strategy, which also applies to the evaluation dataset. Based on these, it has also been shown that the technique possesses limitations such as effects of lighting and occlusions and improvement in such areas has been suggested for more effective use in real-world applications.

By devising a novel clean label backdoor attack technique for deep learning-based [18] face recognition models, which scales well across various applications. The attack relies on physical triggers, with optimization-based feature transfer and accessory injection for poisoned data construction. Our attacks achieve strong success rates in unseen samples while imposing minimal effects on model accuracy and evading traditional defenses.

Reversible Least Significant Bit (LSB) steganography is exploited to improve security, hiding sensitive data in digital images. The approach [19] of the study is based on the embedding of data with such an arrangement that the integrity of the original image is not affected by safe placement of the hidden data, particularly in data recovery applications like in the case of medical imaging. According to Kerckhoff's principle, the key is designed to rely completely on the secrecy of the used key instead of relying on the concealing algorithm.

This work proposes [20] an image synthesis-mapping framework called SWE to challenge the low payload capacity and incomplete message recovery of steganography without embedding. This hybrid combines synthesis-based techniques with mapping-based methods for hiding secret messages with minimal image distortion. Efficiency improvement of this framework reduces the number of required images needed to hide secret messages and outperforms traditional SWE methods to attain a better overall performance in terms of payload capacity and accuracy.

III. METHODOLOGY

This work centers its methodology on developing a cancellable face recognition system using deep steganography to enhance both privacy and security. Data preprocessing, deep models of learning, and steganographic encoding will be put together in a way that securely embeds biometric information into innocuous images. Biometric template revocation and replacement capabilities ensure very high recognition accuracy while maintaining high user privacy. Moreover, RNNs are used to efficiently classify the features embedded. It is a reliable solution for such privacy-aware biometric applications.

A. Data Collection

Acquisition of face images from publicly available datasets will be used. Such datasets would encompass images of faces belonging to a large number of people. It would help achieve variability, both in age and ethnicity and even in gender, with facial images. This allows one to build a robust set for training and testing to get good results in training the deep learning models and even while evaluating the performance of the system.

B. Preprocessing Techniques

Normalization and feature extraction techniques are used for uniformity in all face images. The images are resized and pixel values normalized over some given range so that uniform data goes to the model. One feature that usually reduces the dimension of a facial image but captures the informative features in the face required for recognition is achieved via techniques such as Convolutional Neural Networks (CNNs) or Principal Component Analysis (PCA). Besides, face segmentation methods such as histogram equalization or edge detection are applied to isolate primary facial features like eyes, nose, and mouth. This process will

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25mar1119

leave only the most pertinent facial areas to be used in the identification process, thus improving accuracy.

C. Deep Steganography

This technique utilizes deep steganography; the facial features obtained are embedded into random or seemingly innocuous images through deep learning models. A neural network is trained to create steganographic encoding to conceal the biometric information within the image. This process helps to ensure that the image-embedded maintains an appearance similar to the original image and ensures the risk of detection at its minimum level while still maintaining the privacy of the user. The biometric data embedded in the image are not directly accessible, but only through a specific decoding process can be retrieved from the image. It not only ensures the privacy of the user but also revokes and re-issues the biometric templates if needed.

D. Classification with RNN

RNNs are used in embedded facial feature classification. Since the characteristics of the data are sequential in nature, RNNs are well-suited to sequential data and can capture the temporal dependencies that may be present in the embedded features. RNN is trained to recognize patterns in the steganographically embedded features and match them to templates in the database. The classification ensures that the hidden presence of biometric data in the image does not jeopardize the ability of the system to identify the people embedded based on the features within it. The RNNs will therefore increase recognition accuracy and robustness so that the system functions as intended, regardless of the steganographic encoding.

E. Evaluation

This proposed system will be tested against publicly available face datasets for recognition accuracy, steganographic robustness, and cancelability. The recognition accuracy will be assessed by comparing the performance of the system with traditional face recognition methods. Moreover, another method to test for steganographic robustness is the ability of the system to extract embedded features after a set of transformations or attacks has been carried out on the image. Finally, cancelability is simulated by revoking and replacing biometric templates, in order to verify if the system manages compromised data properly.

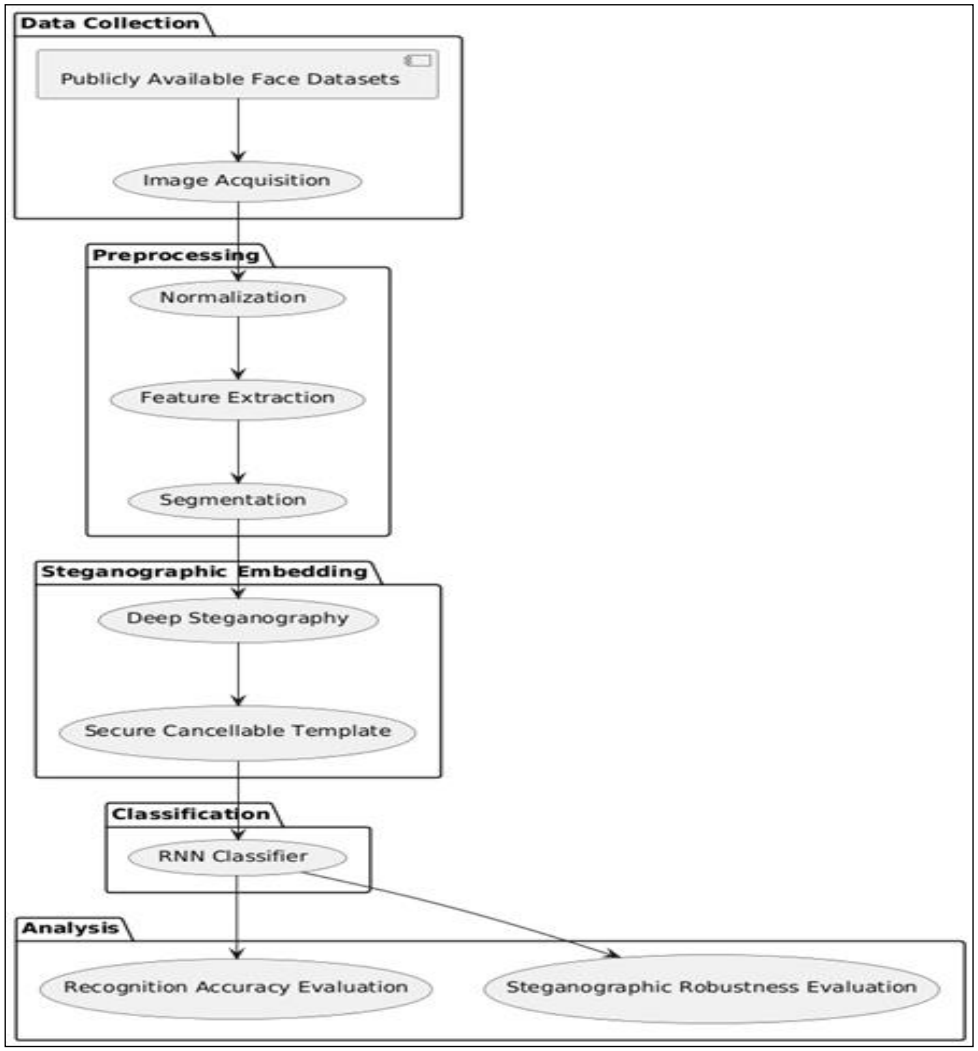

Fig. 1: Architecture Diagram

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25mar1119

IV. RESULT AND DISCUSSION

This deep steganographic cancellable face recognition system is tested using multiple publicly available face datasets in their testing. The recognition accuracy of this system matched the traditional face recognition techniques while steganographic encoding added additional complexity to the deep learning models used for feature extraction and embedding. The results obtained by the experiment demonstrated that this system detected persons with almost negligible loss in accuracy despite biometric data embedding in innocuous images.

For the steganographic robustness, this system performed really well. The features even proved resistant to several transformations, including compression and cropping noises. The experiments demonstrated that the biometric information embedded was indeed conserved and that the encoding still appeared to be a part of an original image, but it can be modified using steganographic encoding. And with this modification, it still is able to appropriately extract facial features and match them up with the respective templates; hence, its deep-learning-embedding integrity is proved.

The cancelability property may be tested through simulating revocation and issuance of biometric templates. If the template is compromised, then it allowed the replacing of the original biometric data with a new one. The processes were efficient and secure enough not to expose any of the sensitive information during the revocation and replacement stages. This capability to update biometric templates in a way that keeps the original data confidential greatly enhances the privacy and security of the system.

This experiment results add that even classification performance of RNNs shows a need to be included in the system's effectiveness. RNNs were most suitable for capturing sequential dependencies, therefore, were able to process embedded features with high accuracy in classification. This helps the system because even with the inclusion of another layer of steganography, the features are sure to match up to the right individual in the database.

In summary, the deep steganography-based approach holds strong promise for privacy-preserving face recognition. The system provides high recognition accuracy with robust encoding of the steganography scheme and cancelability, thus being a very valuable option for privacy conscious applications. It seems that such an approach could apply higher security levels without losing performance compared with traditional biometric systems, so it would be a kind of relevant contribution in the field of secure and privacy preserving biometric authentication.

V. CONCLUSION

In conclusion, the research under discussion discusses a novel approach toward cancellable face recognition using deep steganography that responds to major concerns of privacy and security in the biometric system. The proposed method embeds facial features with deep learning techniques within innocuous images in such a way as to keep the biometric data hidden while leading to a high amount of recognition accuracy. After thorough testing of the system on publicly available datasets, it demonstrated similar performance to the traditional face recognition systems, but with accurate identification and privacy friendliness.

Additionally, it showed strong aspects of steganographic robustness, where the features embedded inside remained quite resistant over various requirements of transformation such as compression on images, cropping, and noise addition. This robustness is well important in real applications. As images are updated during storage or transmission, the system also provides an additional layer of security with the possibility of revoking and replacing compromised biometric templates, which can be done in a way that maintains privacy since updating of the biometric data is permitted but in such a manner that the original information will not be exposed. This capability is very necessary with the identity theft prevention systems, wherein confidentiality demands have to be anchored in protecting very sensitive data.

The usage of RNNs in feature classification further enhanced the system, whereby the hidden biometric information was correctly matched against templates stored in its repository. RNN's sequential information processing capability allows it to identify hidden features, even when encoded by steganographic procedures that would otherwise conceal clear identifications.

The solution presents a promising avenue for improvements towards bettering the privacy and security of face recognition systems. The proposed approach integrates deep steganography with advanced machine learning techniques; its performance is therefore as high as that of traditional biometric systems, but it brings important improvements in terms of data protection. This makes the proposal relevant for privacy-sensitive applications where user data security becomes the utmost factor. Results achieved indicate that the proposed system is capable of being a strong alternative to the commonly used face recognition systems in secure biometric authentication and shall expand the horizon for further development.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25mar1119

REFERENCES

[1]. N. Li et al., "Chinese Face Dataset for Face Recognition in an Uncontrolled Classroom Environment," in IEEE Access, vol. 11, pp. 86963-86976, 2023, doi: 10.1109/ACCESS.2023.3302919.

[2]. Z. Huang, J. Zhang and H. Shan, "When Age-Invariant Face Recognition Meets Face Age Synthesis: A Multi-Task Learning Framework and a New Benchmark," in IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 45, no. 6, pp. 7917-7932, 1 June 2023, doi: 10.1109/TPAMI.2022.3217882.

[3]. P. C. Neto, J. R. Pinto, F. Boutros, N. Damer, A. F. Sequeira and J. S. Cardoso, "Beyond Masks: On the Generalization of Masked Face Recognition Models to Occluded Face Recognition," in IEEE Access, vol. 10, pp. 86222-86233, 2022, doi: 10.1109/ACCESS.2022.3199014.

[4]. S. Malakar, W. Chiracharit and K. Chamnongthai, "Masked Face Recognition With Generated Occluded Part Using Image Augmentation and CNN Maintaining Face Identity," in IEEE Access, vol. 12, pp. 126356-126375, 2024, doi: 10.1109/ACCESS.2024.3446652.

[5]. P. Terhörst, M. Huber, N. Damer, F. Kirchbuchner, K. Raja and A. Kuijper, "Pixel-Level Face Image Quality Assessment for Explainable Face Recognition," in IEEE Transactions on Biometrics, Behavior, and Identity Science, vol. 5, no. 2, pp. 288-297, April 2023, doi: 10.1109/TBIOM.2023.3263186.

[6]. Y. Guo and Z. Liu, "Coverless Steganography for Face Recognition Based on Diffusion Model," in IEEE Access, vol. 12, pp. 148770-148782, 2024, doi: 10.1109/ACCESS.2024.3477469.

[7]. H. -T. Ho, L. Vuong Nguyen, T. Huong Thi Le and O. -J. Lee, "Face Detection Using Eigenfaces: A Comprehensive Review," in IEEE Access, vol. 12, pp. 118406-118426, 2024, doi: 10.1109/ACCESS.2024.3435964.

[8]. T. -H. Kim, S. -H. Choi and Y. -H. Choi, "Instance-Agnostic and Practical Clean Label Backdoor Attack Method for Deep Learning Based Face Recognition Models," in IEEE Access, vol. 11, pp. 144040-144050, 2023, doi: 10.1109/ACCESS.2023.3342922.

[9]. K. Farhan Rafat and S. Muhammad Sajjad, "Advancing Reversible LSB Steganography: Addressing Imperfections and Embracing Pioneering Techniques for Enhanced Security," in IEEE Access, vol. 12, pp. 143434-143457, 2024, doi: 10.1109/ACCESS.2024.3468988.

[10]. R. Huang, C. Lian, Z. Dai, Z. Li and Z. Ma, "A Novel Hybrid Image Synthesis-Mapping Framework for Steganography Without Embedding," in IEEE Access, vol. 11, pp. 113176-113188, 2023, doi: 10.1109/ACCESS.2023.3324050.

[11]. M. Zhang, R. Liu, D. Deguchi and H. Murase, "Masked Face Recognition With Mask Transfer and Self-Attention Under the COVID-19 Pandemic," in IEEE Access, vol. 10, pp. 20527-20538, 2022, doi: 10.1109/ACCESS.2022.3150345.

[12]. H. O. Shahreza and S. Marcel, "Comprehensive Vulnerability Evaluation of Face Recognition Systems to Template Inversion Attacks via 3D Face Reconstruction," in IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 45, no. 12, pp. 14248-14265, Dec. 2023, doi: 10.1109/TPAMI.2023.3312123.

[13]. H. H. Nguyen, S. Marcel, J. Yamagishi and I. Echizen, "Master Face Attacks on Face Recognition Systems," in IEEE Transactions on Biometrics, Behavior, and Identity Science, vol. 4, no. 3, pp. 398-411, July 2022, doi: 10.1109/TBIOM.2022.3166206.

[14]. H. -B. Kim, N. Choi, H. -J. Kwon and H. Kim, "Surveillance System for Real-Time High-Precision Recognition of Criminal Faces From Wild Videos," in IEEE Access, vol. 11, pp. 56066-56082, 2023, doi: 10.1109/ACCESS.2023.3282451.

[15]. Y. Martínez-Díaz, H. Méndez-Vázquez, L. S. Luevano, M. Nicolás-Díaz, L. Chang and M. González-Mendoza, "Towards Accurate and Lightweight Masked Face Recognition: An Experimental Evaluation," in IEEE Access, vol. 10, pp. 7341-7353, 2022, doi: 10.1109/ACCESS.2021.3135255.

[16]. L. Laishram, J. T. Lee and S. K. Jung, "Face De-Identification Using Face Caricature," in IEEE Access, vol. 12, pp. 19344-19354, 2024, doi: 10.1109/ACCESS.2024.3356550.

[17]. L. Ambardi, S. Hong and I. K. Park, "SegTex: A Large Scale Synthetic Face Dataset for Face Recognition," in IEEE Access, vol. 11, pp. 131939-131949, 2023, doi: 10.1109/ACCESS.2023.3336405.

[18]. D. Wanyonyi and T. Celik, "Open-Source Face Recognition Frameworks: A Review of the Landscape," in IEEE Access, vol. 10, pp. 50601-50623, 2022, doi: 10.1109/ACCESS.2022.3170037.

[19]. J. P. Perez and C. A. Perez, "Face Patches Designed Through Neuroevolution for Face Recognition With Large Pose Variation," in IEEE Access, vol. 11, pp. 72861-72873, 2023, doi: 10.1109/ACCESS.2023.3295330.

[20]. C. Galea, "Comments on “Domain Alignment Embedding Network for Sketch Face Recognition”," in IEEE Access, vol. 10, pp. 71030-71034, 2022, doi: 10.1109/ACCESS.2022.3188796.