

Suspect Detection in Real Time using Generative AI Generated Dataset

Modesh Khandelwal¹ and Eswaran Parthsarthy²

¹⁻²Dept. of Electronics and Communications, SRM Institute of Science and Technology, Kattankulathur, Kanchipuram, Tamil Nadu, India

Email: mk1910@srmist.edu.in, eawaranp@srmist.edu.in

Abstract—Real-time suspect detection presents a formidable challenge for AI and ML methods due to the need for extensive image data. This work proposes a solution using Generative AI algorithms like GAN, StyleGAN, and TGAN to create a diverse high-definition test dataset from a single suspect image. Through feature-guided face manipulation, the algorithms generate realistic facial expressions and scenarios, expanding the dataset without requiring numerous unique images. Subsequently, the augmented dataset trains a Face Detection model, which analyses live video streams to identify suspects. Upon detection, the system triggers real-time alerts for swift intervention. By leveraging Generative AI for dataset augmentation and training robust Face Detection models, the project aims to improve suspect detection accuracy and efficiency in real-world settings, bolstering public safety measures.

Index Terms— Generative Adversarial Network, StyleGAN, TGAN, Generative AI, Suspect Detection, Face Detection.

I. INTRODUCTION

In contemporary law enforcement and public safety endeavors, the swift and accurate identification of suspects remains a vital component in upholding societal security and curbing criminal activities. However, traditional approaches to suspect identification encounter significant obstacles, especially when suspects deliberately alter their appearances or employ tactics to evade detection. Overcoming these challenges requires integrating cutting-edge technologies into existing surveillance frameworks. Recent advancements in generative artificial intelligence (AI) algorithms, when combined with real-time surveillance systems, represent a paradigm shift in enhancing the effectiveness of criminal identification processes. [1][8]

This paper explores the integration of generative AI algorithms with closed-circuit television (CCTV) cameras to enable real-time suspect detection by generating diverse facial representations. By leveraging generative models like generative adversarial networks (GANs) or variational autoencoders (VAEs), law enforcement agencies can dynamically create varied depictions of suspects' faces, even with limited or fragmented information. [5]

The real-time generation of diverse facial representations significantly enhances the effectiveness of CCTV surveillance by enabling adaptive responses to evolving scenarios and suspect descriptions. [10] Traditional static image databases often fall short in capturing the full range of potential appearances, limiting the efficacy of suspect identification. Generative AI algorithms overcome this limitation by continuously refining facial representations based on incoming video streams, ensuring comprehensive coverage and heightened accuracy in suspect detection. [3]

Furthermore, the fusion of generative AI with real-time CCTV surveillance enhances the adaptability and scalability of law enforcement operations. The ability to generate diverse facial representations of suspects in real-time empowers investigators to navigate dynamic and evolving situations adeptly, thereby improving response times and overall operational efficiency. [10]

However, despite the potential benefits of enhanced criminal identification capabilities, profound ethical and privacy considerations arise. The deployment of real-time surveillance combined with generative AI raises concerns regarding individual privacy rights, potential biases in suspect identification, and the responsible handling of sensitive data. Upholding ethical standards, ensuring transparency, and implementing robust safeguards are essential for law enforcement agencies to mitigate risks and protect civil liberties.

In conclusion, the amalgamation of generative AI algorithms for generating diverse facial representations with real-time CCTV surveillance represents a significant advancement in criminal identification and law enforcement. Leveraging these technologies equips law enforcement agencies with the tools to enhance their capacity for detecting, tracking, and apprehending suspects in real-time scenarios. This advancement not only strengthens public safety efforts but also contributes to the pursuit of justice while upholding ethical principles and respecting individual rights. [6]

This survey provides a comprehensive analysis of manipulated face image generation and detection techniques, focusing on deepfake technology and emerging methods. It explores key manipulation groups, including attributes manipulation, facial re-enactment, face swapping, and face synthesis, while highlighting advancements and detection strategies. By addressing existing challenges and proposing future research directions, the survey aims to advance understanding and combat the misuse of deepfake technology, contributing to enhanced detection and prevention measures in the face of emerging threats. [1]

This paper implements criminal face verification using a Deep Learning Algorithm, specifically a pretrained Convolutional Neural Network (CNN) known as Densenet. Through meticulous training and testing using Image Processing techniques, the proposed method achieves high accuracy in face recognition with minimal computational overhead. Leveraging Densenet for face classification, the system demonstrates efficient detection of multiple faces, offering potential applications in citizen identification systems like Aadhaar, with future prospects for distinguishing between residents and non-residents, aiding in criminal investigations. [2]

The article highlights the limitations of sketches produced by human artists for suspect identification, stressing inaccuracies due to both artistic error and witness misdescription. It introduces Generative Adversarial Networks (GANs) as a solution to generate images corresponding to specific classes, with StyleGAN utilized to overcome the challenge of generating high-resolution images. Further enhancement is achieved through Temporal-Lateral GAN (TL-GAN), offering precise alteration of generated images to closely match suspect descriptions. The review underscores the significance of this approach in reducing misidentification rates and subsequent crime. [3]

The article aims to streamline criminal recognition for law enforcement. Here, the author utilizes Generative Adversarial Networks (GANs) to generate hyper-realistic facial images from sketches and visual attributes, followed by facial identification using the HOG Face recognition algorithm. By employing context-based GANs, aiming to expedite the identification process, ultimately reducing sketching and recognition times for the police department. [4]

This article utilizes Conditional Generative Adversarial Networks (C-GANs) to automatically generate 2-D facial images based on user-defined attributes like gender, hair color, and facial features. By integrating a face matching feature with criminal databases, it enables quick suspect identification. Trained on a large dataset and evaluated for performance, the system offers real-time facial previews, aiding in the creation of realistic facial images with potential applications in forensic investigations. [5]

While previous methods rely on a 2D image generation model, our study takes a different approach by utilizing 3D Morphable Models for generating images in 3D modelling. The objective is to create test data that accurately represents three-dimensional aspects. Subsequently, we aim to leverage this data to implement real-time suspect detection using surveillance cameras. This shift to 3D modelling allows for more accurate and detailed representation of facial features, enhancing the effectiveness of suspect detection in various scenarios.

II. ALGORITHM AND METHODOLOGY

A. Algorithms

This project employs Histogram of Oriented Gradients (HOG) and 3D Morphable Face Models to extract features from input images of suspects. Variants of Generative Adversarial Networks (GANs), including Temporal Generative Adversarial Network (TGAN) and StyleGAN, are utilized to generate suspect faces for the

test dataset of the detection module, applying specified filters. Finally, Convolutional Neural Networks (CNNs) are employed to detect suspects in real-time, using the dataset generated by GAN algorithms. The integration of these techniques facilitates accurate and efficient suspect detection, leveraging advanced feature extraction and generation methods provided by HOG, 3DMM, and GANs, combined with the robust detection capabilities of CNNs.

B. Methodology

The entire work in this paper is divided into two parts: a. Generator Module and b. Detector Module. The block diagram of the complete process is as below:

a. Generator Module

The aim of this study is to achieve precise suspect detection using a minimal dataset for training the detection module. One image of the suspect serves as input, and with Generative Adversarial Network (GAN) algorithms like TGAN (Temporal GAN) and StyleGAN, a test database is generated. Initially, the input image is converted into grayscale, forming the foundation for further processing.

A complex facial analysis pipeline, incorporating techniques like Histogram of Oriented Gradients (HOG), is then applied to identify and analyze facial shapes and features.

This entails detecting key facial landmarks and capturing intricate facial details and patterns. Utilizing sophisticated algorithms like shape predictors and discriminators, the system meticulously extracts and defines facial features to gain a thorough understanding of the subject's facial characteristics.

Continuing the process, we utilize facial landmarks extracted by the Histogram of Oriented Gradients (HOG) discriminator, which are then inputted into the Expression Oriented Systems (EOS) framework. Within EOS, these landmarks are pivotal for crafting detailed 3D Morphable Face Models (3DMMs) of the input image, capturing intricate facial geometry nuances.

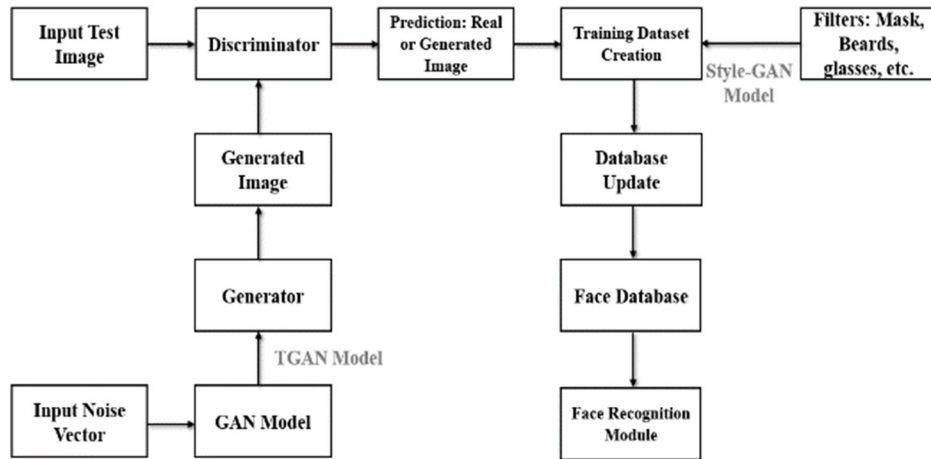


Figure 1. Block Diagram of Image Reconstruction Module

Simultaneously, inputs from HOG and EOS are channeled into the Temporal Generative Adversarial Network (TGAN) algorithm, known for its ability to produce temporally coherent sequences. TGAN synthesizes images relevant to project goals, evaluated by a discriminator to differentiate between real and synthetic images. This iterative refinement process sharpens the discriminator's ability to discern genuine from fabricated imagery, contributing to an extensive training dataset, ultimately improving TGAN's image generation capabilities.

By integrating TGAN with HOG and EOS, the project fortifies facial analysis techniques, enhancing accuracy and reliability across various fields reliant on precise facial data analysis.

In parallel, results from HOG and 3DMMs are fed into the StyleGAN generator, incorporating various masks and filters. StyleGAN, recognized for generating high-resolution, diverse images, produces a range of outputs, evaluated by a predictor to discern specific attributes. These images enrich the training dataset, enabling the model to adapt to a broader spectrum of facial features and variations.

Integrating StyleGAN augments the dataset with realistic facial images, refining predictive models and advancing facial recognition and analysis techniques for real-time suspect detection applications.

b. Recognition Module

The Face Recognition Module operates on Convolutional Neural Network (CNN) architecture, prized for its adeptness in discerning intricate patterns from image data. Utilizing datasets from TGAN and StyleGAN, the module endeavors to identify facial features in synthesized images, leveraging CNN's capacity to extract nuanced facial representations.

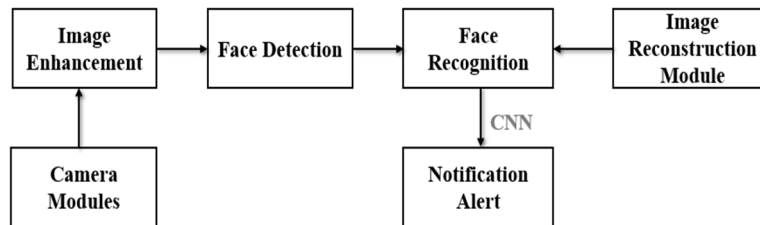


Figure 2. Block Diagram of Face Recognition Module

During testing, the module's efficacy is gauged through exposure to diverse inputs, encompassing synthesized and real-world images sourced online. Additionally, genuine images of individuals represented in the dataset are included. This comprehensive evaluation ensures the module's ability to differentiate between synthetic and genuine facial representations, enhancing its adaptability and reliability in practical settings.

Incorporating real-world images alongside synthesized ones enriches the testing dataset, enabling the module to generalize across a spectrum of facial attributes. By subjecting the module to varied inputs, the project aims to validate and enhance its performance across diverse scenarios and environments.

III. RESULTS AND DISCUSSIONS

The transformation of the input image into a grayscale representation initiates the facial analysis pipeline, which incorporates techniques like Histogram of Oriented Gradients (HOG) to detect and analyse facial shapes and features.



Figure 3. Input Image of Suspect Figure 4. Facial landmarks (HOG)

This process entails identifying facial landmarks and extracting intricate details to characterize the overall facial structure. Leveraging advanced algorithms, including shape and feature predictors, the system meticulously extracts and characterizes facial features, aiming to provide a comprehensive understanding of the subject's facial attributes.

Facial landmarks obtained from the HOG discriminator are employed in the EOS framework to create detailed 3D Morphable Face Models (3DMMs) from the input image. These models, which capture intricate facial geometry, lay the groundwork for subsequent stages of facial analysis and synthesis. Utilizing the EOS framework enables a broad range of facial analysis tasks, such as expression recognition, pose estimation, and texture mapping, enhancing the accuracy and depth of facial analysis. Integrating landmark-based modelling with the EOS framework enhances the system's capability to analyse and synthesize facial data, fostering progress in facial recognition and analysis techniques.

The outcomes from HOG and 3DMMs were integrated into both the Temporal Generative Adversarial Network (TGAN) algorithm and the StyleGAN generator to create training images with diverse masks and filters.

TGAN, known for its capability to generate temporally coherent sequences, was employed to generate images, subsequently evaluated by a discriminator within the GAN framework to differentiate real from synthetic ones. Incorporating TGAN-generated images into the training data refined the discriminator's ability to distinguish between authentic and synthetic imagery, enriching the training dataset. Meanwhile, StyleGAN processed these inputs to generate a variety of outputs, evaluated by a predictor to identify specific attributes from the generated

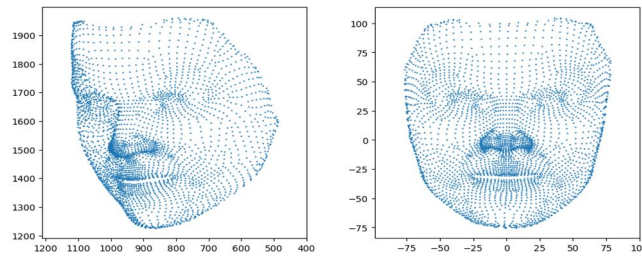


Figure 5. (a) 3DMM Side view (b) 3DMM Frontal View

images. This iterative process enhanced the dataset's comprehensiveness and diversity, allowing the model to learn and adapt to a wider range of facial features and variations.

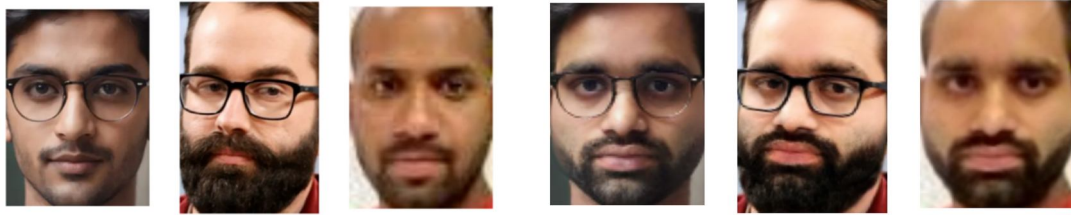


Figure 6. Random images to be used as Filters

Figure 7. Generated Images of Suspect

IV. CONCLUSION

In essence, this study seeks to enhance the accuracy of suspect detection despite limited training image datasets. Leveraging Generative Adversarial Network (GAN) methodologies like TGAN and StyleGAN, the investigation expands the test dataset comprehensively. Integrating Histogram of Oriented Gradients (HOG) with Expression Oriented Systems (EOS) enables the creation of intricate 3D Morphable Face Models (3DMMs), thus augmenting facial analysis capabilities. TGAN produces temporally coherent images, further refined by StyleGAN to high resolutions. The Face Recognition Module, built upon Convolutional Neural Network (CNN) architecture, adeptly discerns facial features, verified across diverse testing contexts encompassing synthetic and real-world imagery. This iterative strategy ensures the system's robustness and adaptability, advancing facial recognition methodologies for real-time suspect detection applications.

Subsequently future research endeavors will focus on expanding and diversifying the filter repertoire utilized in constructing the training dataset to ensure comprehensive representation of facial attributes and features for improved accuracy. Additionally, efforts will be directed towards developing a graphical user interface (GUI) to enhance the prototype's usability with any input image, along with optimizing hardware infrastructure to enable real-time suspect detection, thus bolstering the system's efficiency and efficacy for practical deployment in identifying suspects in real-world scenarios.

ACKNOWLEDGMENT

I would like to express my deepest gratitude to my guide, Dr.P. ESWARAN his valuable guidance, consistent encouragement, personal caring, timely help and providing me with an excellent atmosphere for doing research. All through the work, in spite of his busy schedule, he has extended cheerful and cordial support to me for completing this research work.

REFERENCES

- [1] Minh Dang and Tan N. Nguyen, "Digital Face Manipulation Creation and Detection: A Systematic Review", *Electronics* 2023, 12, 3407.
- [2] R. K. R, S. S. A, R. H. B, R. K and C. S, "Identification of Criminal and Non-Criminal Face Using Deep Learning and Image Processing," 2021 International Conference on System, Computation, Automation and Networking (ICSCAN), Puducherry, India, 2021, pp. 1-4.
- [3] H. J. Jalan, G. Maurya, C. Corda, S. Dsouza and D. Panchal, "Suspect Face Generation," 2020 3rd International Conference on Communication System, Computing and IT Applications (CSCITA), Mumbai, India, 2020, pp. 73-78.

- [4] Karve, A., Balasubramanian, M., Chaudhari, K., Mane, S.B. (2020). Automated Criminal Identification System Using Face Generation. In: Pandian, A., Ntalianis, K., Palanisamy, R. (eds) Intelligent Computing, Information and Control Systems. ICICCS 2019. Advances in Intelligent Systems and Computing, vol 1039. Springer, Cham.
- [5] Bhajaj, P., Panchal, P., Patel, N., Shinde, R., Gawade, A. (2022). FIGSI—Facial Image Generation for Suspect Identification. In: Shakya, S., Du, KL., Haoxiang, W. (eds) Proceedings of Second International Conference on Sustainable Expert Systems . Lecture Notes in Networks and Systems, vol 351. Springer, Singapore.
- [6] Mileva, M., Burton, A.M. Face search in CCTV surveillance. Cogn. Research 4, 37 (2019). <https://doi.org/10.1186/s41235-019-0193-0>
- [7] Ian J. Goodfellow, Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron Courville, Yoshua Bengio, “Generative Adversarial Networks”, <https://doi.org/10.48550/arXiv.1406.2661>
- [8] Tero Karras, Samuli Laine and Timo Aila, “ A Style-Based Generator Architecture for Generative Adversarial Networks”, <https://doi.org/10.48550/arXiv.1812.04948>
- [9] S. Masaki and M. Eiichi “Temporal Generative Adversarial Nets” (2016), <https://arxiv.org/pdf/1611.06624v1>
- [10] K. Sivanagireddy, S. Jagadeesh & A. Narmada, “Identification of criminal & non-criminal faces using deep learning and optimization of image processing (2023)”, <https://doi.org/10.1007/s11042-023-17471-7>.
- [11] Yang, S., Zhang, JT., Lin, CW., Hsu, CC. (2022). GAN-Based Criminal Suspect Face Generator. In: Hsieh, SY., Hung, LJ., Klasing, R., Lee, CW., Peng, SL. (eds) New Trends in Computer Technologies and Applications. ICS 2022. Communications in Computer and Information Science, vol 1723. Springer, Singapore.