ISSN No:-2456-2165

Criminal Face Recognition Using GAN

Anitta George
Dept. of Computer Science
Sahrdaya College of Engineering and Technology Thrissur, India

Krishnendu K A
Dept. of Computer Science
Sahrdaya College of Engineering and Technology Thrissur, India

Anusree K
Assistant prof.
(Dept. of Computer Science)
Sahrdaya College of Engineering and Technology Thrissur, India

Adira Suresh Nair
Dept. of Computer Science
Sahrdaya College of Engineering and Technology Thrissur, India

Hari Shree
Dept. of Computer Science
Sahrdaya College of Engineering and Technology Thrissur, India

Abstract:- Forensics and security at present often use low technological resources. Security measures often fail to update with the upcoming technology. This project is based on implementing an automatic face recognition of criminals or specific targets using machine-learning approach. Given a set of features to a Generative Adversarial Network(GAN), the algorithm generates an image of the target with the specified feature set. The input to the machine can either be a given set of features or a set of portraits varying from frontals to side profiles from which these features can be extracted. The accuracy of the system is directly proportional to the number of epochs trained in the network. The generated output image can vary from primitive, low resolution images to high quality images where features are more recognizable. This is then compared with a predefined database of existing people. Thus, the target can immediately be recognized with the generation of an artificial image with the given biometric feature set, which will be again compared by a discriminator network to check the true identity of the target.

I. INTRODUCTION

The promise of deep learning is to discover rich, hierarchical models that represent probability distributions over the kinds of data encountered in artificial intelligence applications, such as natural images, audio waveforms containing speech, and symbols in natural language corpora. So far, the most striking successes in deep learning have involved discriminative models, usually those that map a high-dimensional, rich sensory input to a class label. These striking successes have primarily been based on the backpropagation and dropout algorithms, using piecewise linear units which have a particularly well-behaved gradient. Deep generative models have had less of an impact, due to the difficulty of approximating many intractable probabilistic computations that arise in maximum likelihood estimation and related strategies, and due to difficulty of leveraging the benefits of piecewise linear units in the generative context. A new generative model estimation procedure is proposed that side-steps these difficulties. In the proposed adversarial nets framework, the generative model is pitted against an adversary: a discriminative model that learns to determine whether a sample is from the model distribution or the data distribution. The generative model can be thought of as analogous to a team of counterfeiters, trying to produce fake currency and use it without detection, while the discriminative model is analogous to the police, trying to detect the counterfeit currency. Competition in this game drives both teams to improve their methods until the counterfeits are indistinguishable from the genuine articles. This framework can yield specific training algorithms for many kinds of model and optimization algorithms. The special case when the generative model generates samples by passing random noise through a multilayer perceptron, and the discriminative model is also a multilayer perceptron is explored. This special case is referred to as adversarial nets. In this case, training is performed on both models using only the highly successful backpropagation and dropout algorithms and samples from the generative model using only forward propagation. No approximate inference or Markov chains are necessary.

II. DRAWBACKS OF EXISTING SYSTEM

- Human-made sketches may be ambiguous and unclear.
- The primitive sketches of a target may be black and white or monochrome. Features which are colour dependent will not be significant.
- Some features can be changed by culprit/target. E.g. hair colour, hairstyle, etc.
- Face recognition by humans takes more time if the target face has to find a match without a database.

III. METHOD

The proposed method presents a detailed deep learning-based model for face identification and detection. We are proposing this method specifically for criminal identification. An image of the person, who you want to identify is given as the input to the machine or generative network. This image may be uploaded by the investigating crew through an android application which can be installed into their mobile phones.

Our goal is to determine the target's identity by utilizing the visual clues obtained via the camera. The input image is fed into the Generative Adversarial Network (GAN) via android app. The image is taken into the generator first after preprocessing, the image features that

ISSN No:-2456-2165

are visible are stored as a feature set f(x) for the input image x. The features set is used to generate labels of the same target with slightly different features. This would describe the target that they changed their appearance at present and made variations such as change of hair colour, eye colour, etc. Generative Adversarial Networks are powerful enough to identify the target even in their best disguise since their facial features remain the same.

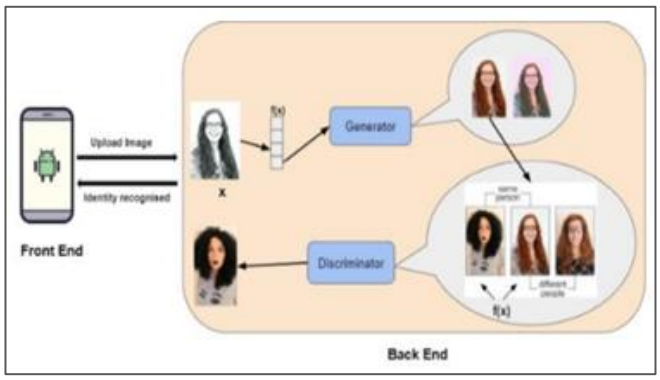

Fig 1:- Working of a GAN network

The generator module of the GAN network takes the features of an image as an input and produces a set of labels for each face found. This output image is fed into the discriminator module of the same network. It is the responsibility of the discriminator to take the generator's output and check if the features of the given target match with any of the ones in the database. If there is a match, the image will be invalidated and the identity of the target will be returned. Thus the network will extract as many visible features possible from the images x= 1 to n, and combine all features to produce the superset of features f(x). The identity of the target together with their original image is returned as the output through android app. The generator has two other submodules called encoder and decoder. The encoder takes in an image as input and extracts as many features from the position of the target. It then consolidates all features from n images given into the GAN network as f(x). The decoder of the GAN generator network takes this feature set and restores the image of the target with different poses denoted by different and unique pose-codes. This image result is then fed to the discriminator and the value is generated if the target is a real person. Also, the value is generated stating the identity of the person on the training database. The generator and the discriminator were first introduced as multiple neural networks but over time, it was found that the number of weights introduced in every layer of the multiple neural networks were infeasible with the increase of the number of pixels as the resolution if the training dataset images increased.

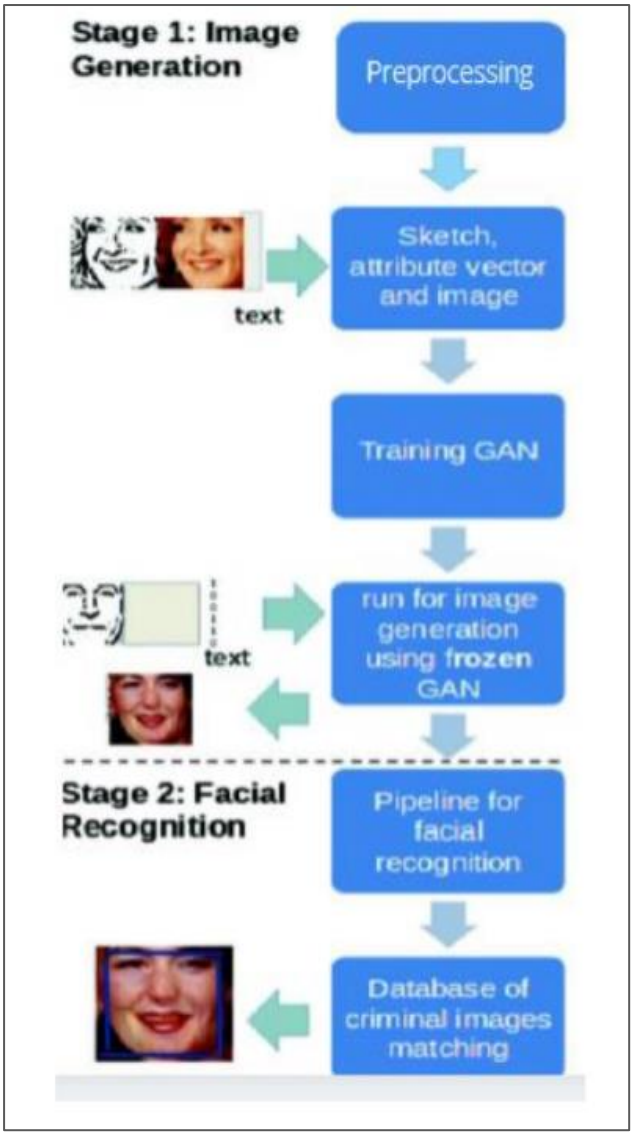

Fig 2:- System Architecture

The images are first preprocessed. They are aligned and the appropriate resolution is set to train them to the machine. Images are then vectorised. Their attributes that are distinguishable are stored as features into a feature set. The features are then given as input to the training GAN for further training procedure. The images that this machine works with would be the normal and practical resolution that would be clear enough to distinguish features and identify human faces.

ISSN No:-2456-2165

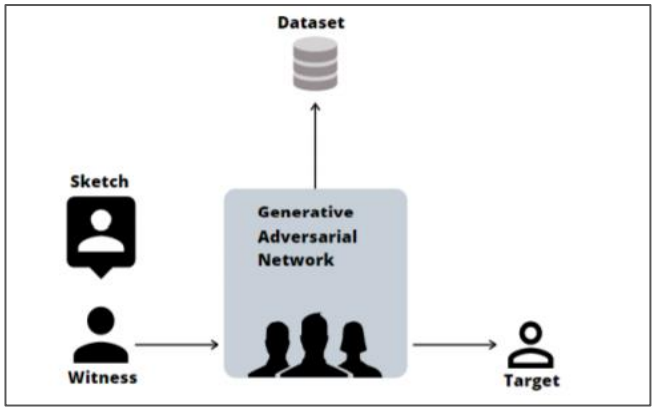

Fig 3:- Use Case Diagram

The advantages are:
- Easy recognition
- Accommodates ambiguous input faces
- Efficient with increased use
- Fast and accurate results
- Scope for broader applications

IV. RESULTS

Generative Adversarial Networks are used to identify targets or criminals even with slightly different facial features, including hair colour, eye colour, facial hair structure, etc. Thus, even when the target can disguise themselves, they are identified using the adversarial technique of machine learning. Generators can generate more realistically fake images with slightly tuned features which the discriminator will extract features from and can further generate the corresponding identity code of the target from the database. Thus face recognition is carried out successfully.

V. CONCLUSION

A system that can recover undisguised faces could be helpful for criminal investigation. In particular, witnesses should be able to make use of these processed images to identify the criminals among a series of ID photos, which typically include no disguise or in person among a number of held suspects. People utilizing online dating apps could also utilize the system to reverse the real person behind the facial disguise, a feature that many find useful. This project is built on current work related to GAN-based style transform methods that are commonly employed for applying facial disguise. There have been significant improvements in machine capability to identify and verify human faces over the past few years. Device makers are already taking advantage of such development by equipping their latest phones and tablets with AI co-processor and powerful image processing algorithms. However, the recent trend has mostly focused on making facial identification and verification invariant to facial features. These works certainly help machines recognize human faces. However, most humans are interested in seeing people in the natural state without any facial disguise.

ACKNOWLEDGEMENT

We would like to express our immense gratitude and profound thanks to all those who helped us to make this project a great success. We express our gratitude to the almighty God for all the blessings endowed on us. We express my thanks to our Executive Director REV.FR. GEORGE PAREMAN, Director DR.ELIZABETH ELIAS, Principal DR. NIXON KURUVILA for providing us with such a great opportunity. We are thankful for the help and appreciation we received from the head of the department DR. RAJESWARI M, project coordinators MS. DEEPA DEVASSY, MS. ANLY ANTONY and MR. WILLSON JOSEPH We would also extend my deep sense of gratitude to our project guide MS. ANUSREE K for her guidance and advice. We would like to express our gratitude towards my parents for their timely cooperation and encouragement. Every project is successful due to the effort of many people. Our thanks and appreciation go to all our peers who have given us their valuable advice and support and pushed us into successfully completing this project.

REFERENCES

[1]. **D. J. Robertson, R. S. Kramer, and A. M. Burton**, ``Fraudulent ID using face morphs: Experiments on human and automatic recognition," PLoS ONE, vol. 12, no. 3, 2017, Art. no. e0173319.

[2]. **J. Zhao, L. Xiong, P. K. Jayashree, J. Li, F. Zhao, Z. Wang, P. S. Pranata, P. S. Shen, S. Yan, and J. Feng.** Dual-agent gans for photorealistic and Identity preserving profile face synthesis. In NIPS, 2017.

[3]. **Karras, Tero**, et al. "Progressive growing of GANS for improved quality, Stability, and variation," arXiv preprint arXiv:1710.10196, 2017.

[4]. **T. Salimans, I. Goodfellow, W. Zaremba, V. Cheung, A. Radford, and X.Chen**, "Improved Techniques for Training GANs," in Advances In Neural Information Processing Systems, 2016, pp. 2234–2242.

[5]. **X. Yu and F. Porikli**, "Ultra-resolving face images by discriminative generative networks," in Proc. European Conf. Comput. Vis. Springer, 2016, pp. 318–333.

[6]. **C. Peng, X. Gao, N. Wang, and J. Li**, ``Face recognition from multiple stylistic sketches: Scenarios, datasets, and evaluation," Pattern Recognit., vol. 84, pp. 262272, Dec. 2018.

[7]. **M. S. Sarfraz and R. Stiefelhagen**, "Deep perceptual mapping for cross modal face recognition," International Journal of Computer Vision, vol. 122, no. 3, pp. 426–438, May 2017.

[8]. **I. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair**, A. Courville, and Y. Bengio, "Generative adversarial nets," in Advances in neural information processing systems, 2014, pp. 2672– 26.