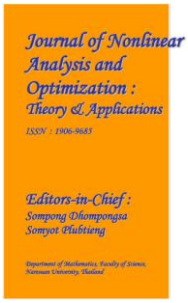
Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 15, Issue. 1, No.12 : 2024
ISSN : **1906-9685**



AI SIMULATED FAUX IMAGE DETECTION SYSTEM USING DEEP LEARNING

Dr. V. Shanmukha Rao Department of Information Technology, Andhra Loyola Institute of Engineering And Technology, Vijayawada, Andhra Pradesh, India Shanmukharao.v@gmail.com
B. Sai Charan Teja Department of Information Technology, Andhra Loyola Institute of Engineering And Technology, Vijayawada, Andhra Pradesh, India billasaicharantej677@gmail.com
L. Yaswanth Sai Department of Information Technology, Andhra Loyola Institute of Engineering And Technology, Vijayawada, Andhra Pradesh, India yaswanthsailinga@gmail.com
A. Bindu Department of Information Technology, Andhra Loyola Institute of Engineering And Technology, Vijayawada, Andhra Pradesh, India ambatibindu85341@gmail.com
D. Rama Krishna Department of Information Technology,Andhra Loyola Institute of Engineering And Technology, Vijayawada, Andhra Pradesh, India dokkuramakrishna2002@gmail.com

ABSTRACT –
Although biometric technology is essential for identifying people, thieves are always evolving to avoid being caught. We are using a state-of-the-art method called Deep Texture Features extraction from photos to tackle this problem. Building a Convolutional Neural Network (CNN) is our method for efficiently utilizing this technology. Known as LBPNET, this CNN-based model emphasizes the use of the Local Binary Pattern (LBP) methodology for feature extraction, making it stand out as a cutting-edge approach in the industry. To counter the spread of fake face photos in identification systems, we train the machine learning model to understand LBP descriptors taken from images. Our technique promises to improve the accuracy and dependability of facial recognition systems by integrating CNN technology with LBP descriptors, hence reducing the risk associated with fraudulent modifications to physical and psychological traits.

KEYWORDS:
Deep textures, CNN, NLBPNet, LBPNet, LBP descriptor images.

I. INTRODUCTION

These days, it is common practice to use deep learning-based generative models, like the Generative Adversarial Network (GAN), to partially or fully synthesize lifelike images and movies. Significantly, GAN research progress, as demonstrated by models such as Big GAN and Progressive Growing GANs (PGGAN), has enabled the production of remarkably lifelike material that defies human perception of authenticity in constrained time frames. Although the main purpose of generative applications is image translation, there are serious concerns associated with their misuse on social media sites. For example, Cycle GANs are used to create facial images in explicit content, and GANs can produce movies with public figure facial content that could cause disruptions in society, politics, and business.

Our research builds on earlier works, addressing these issues with a focus on practical and economical solutions. Two general techniques are used in conventional image forgery detection methods: active and passive. Without compromising the visual integrity of the original images, active schemes incorporate outside signals, such as watermarks, into them. These watermarks are extracted from target photos to help detect manipulation. Nevertheless, active forgery detection is useless in GAN-generated content since there is no visible "source image".

Passive forgery detection, on the other hand, is based on inherent statistical data found in source photos and has a high consistency across different images. This approach, however, fails to detect GAN-generated phony images since they are derived from low-dimensional random vectors while

remaining consistent with actual images. While GAN-generated images are unmodified from their source, they provide major problems to existing forgery detection methods.

Furthermore, face recognition systems are vulnerable to a variety of attack vectors, such as printed photos, presented images or videos, plastic surgery, sketching, makeup, 3D masks, and synthetic media generated by computer graphics. Addressing this vulnerability requires investigating Presentation Attack Detection (PAD) solutions designed for such systems.

II. LITERATURE REVIEW

In recent years, researchers have made tremendous progress in the construction of Generative Adversarial Networks (GANs), a type of deep learning model used for image generation. Three significant contributions to this topic are addressed below:

1. Progressive Growth of GANs (PGGAN).

Karras et al. (2017)[1] presented a new GAN training methodology called Progressive Growing of GANs. This method involves gradually raising the resolution of both the generator and the discriminator during training, beginning with a low resolution and adding new layers to capture finer information. Progressive development accelerates training and improves stability, producing high-quality images like CelebA at 1024^2 resolution. Furthermore, the authors proposed approaches for increasing the variety in generated images, resulting in a record inception score in unsupervised CIFAR10. Implementation details were supplied to alleviate unhealthy competition between the generator and discriminator, as well as a new criterion for evaluating GAN performance.

2. Large-Scale GAN Training.

Brock et al. (2018)[2] tackled the difficulty of generating high-resolution, diverse samples from complicated datasets such as ImageNet by training GANs on an unprecedented scale. They found instabilities related with large-scale training and implemented orthogonal regularization in the generator. This regularization technique enabled precise control over the trade-off between sample fidelity and variety, resulting in cutting-edge performance in class conditional picture synthesis.

3. Unpaired Image-to-Image Translation

Zhu et al. (2017)[3] proposed an unpaired image-to-image translation method based on Cycle-Consistent Adversarial Networks. Unlike previous methods that rely on paired training data, this methodology learns to translate images from one domain to another without the need of paired instances. Using adversarial loss, the model learns a mapping between domains, guaranteeing that the distribution of translated images is identical to the target domain.

Challenges and Risks of Image Synthesis

The rise of superior picture synthesis techniques, assisted by advances in artificial intelligence (AI), has generated worries about their potential misuse. A significant example is the emergence of "deepfakes," which are realistic fake videos made with AI algorithms. These tools, which were formerly restricted to professionals, have since become available to everyone with a powerful computer and GPU. While deepfakes have the ability to delight, they also pose major concerns, particularly in the field of non-consensual pornography. The simplicity with which fraudulent videos can be created raises ethical and legal considerations, emphasizing the importance of effective detection and mitigation techniques to prevent their negative impacts on individuals and society.

III EXISTING SYSTEM

Biometric systems play an important part in identity recognition today, but criminals cleverly change their physical and behavioral characteristics to fool these systems. To address this issue, we are applying a revolutionary approach called as Deep Texture Features extraction from images, in conjunction with Convolutional Neural Networks (CNNs) for machine learning model training. This approach, also known as LBPNet or NLBPNet, depends largely on Local Binary Patterns (LBPs) for feature extraction.

Disadvantages Of Existing System:

1] Limited to Surface Anomalies: Conventional methods are largely concerned with finding surface-level anomalies or discrepancies in photographs. However, advanced deep fake algorithms can provide

highly convincing results that are difficult to distinguish from legitimate content, making simple anomaly detection systems worthless.

2] Manual Inspection Requirement: Many current techniques require manual inspection or human interaction to detect potential manipulation indicators. This manual approach is time-consuming and inefficient, especially when dealing with massive amounts of content, such as on platforms where deep fakes grow quickly.

3] Vulnerability to Advancements in Deep Fake Technology: As techniques for creating deep fakes improve, traditional detection systems may become less reliable. Deep fake producers are constantly refining their algorithms to create increasingly realistic forgeries that defy detection by traditional methods, stressing the need for ongoing innovation in detection techniques.

4] Risk of False Positives and False Negatives: Traditional approaches may produce false positives, wrongly classifying genuine information as deep fakes, or false negatives, failing to detect actual deep fakes. Striking a balance between these two sorts of errors necessitates careful calibration of detection systems.

By recognizing these flaws and implementing modern techniques like as Deep Texture Features extraction and CNNs, we hope to improve the robustness and efficacy of biometric systems against emerging threats posed by sophisticated manipulation techniques.

IV. PROPOSED SYSTEM

In this work, we are creating an LBP-Based Machine Learning Convolution Neural Network dubbed LBPNET to detect false face photos. We will first extract LBP from images and then train LBP descriptor images using a Convolution Neural Network to create a training model. Whenever we upload a new test image, it is applied to the training model to determine whether it contains a fake image or not.

1. Deep Texture Features Extraction from Photos:

It involves analyzing photos to extract precise information like texture and structure that may not be visible to the human eye. This technique improves the accuracy of image-related tasks by allowing algorithms to better recognize and distinguish between objects or elements in images. In biometric systems, it helps to recognize individuals by recording distinctive facial traits and patterns, enhancing accuracy even in the face of attempts to trick the system through changes in look or behaviour.

2. Convolutional Neural Network (CNN):

A Convolutional Neural Network (CNN) is an artificial neural network modeled after the structure and function of the human visual cortex. It is made up of several layers of interconnected nodes, each of which performs a specific action on the input data, such as photographs. CNNs are very useful for image recognition, classification, and processing because they can automatically learn and extract features from raw pixel data. CNNs use convolutional filters, pooling layers, and fully connected layers to efficiently collect hierarchical representations of visual information, allowing them to recognize patterns, objects, and complex structures inside images. In the context of the presented information, CNNs play an important role in assessing deep texture features extracted from images, allowing for the discovery of subtle patterns and traits that aid in identifying genuine and counterfeit content in biometric systems.

3. Local Binary Pattern (LBP) Methodology:

The Local Binary Pattern (LBP) methodology is a basic but effective texture description tool in image analysis. It works by comparing each pixel in an image to its neighbours and recording the findings as binary patterns. These patterns capture local texture information, such as edges, corners, and texture changes, which are required for object recognition and classification in photos. LBP has aided in a variety of applications, including face recognition, texture classification, and image retrieval, because to its computational efficiency and resistance to changes in illumination and noise. LBP has made important contributions to image processing accuracy and performance by extracting discrete texture features.

4. Generative Adversarial Networks (GANs):

Generative Adversarial Networks are a form of artificial intelligence model made up of two neural networks, the generator and the discriminator, that are trained concurrently in a competitive

environment. The generator generates synthetic data, such as images or text, while the discriminator learns to distinguish between genuine and fraudulent data. Through this adversarial process, GANs can produce very realistic material that is indistinguishable from real data. GANs have transformed many fields by allowing for the development of lifelike images, videos, and text, accelerating progress in areas such as image synthesis, data augmentation, and creative content generation. They have also aided research into image-to-image translation, style transfer, and data production for machine learning tasks, resulting in important advances in artificial intelligence and computer vision.

5. Presentation Attack Detection (PAD):

Presentation Attack Detection (PAD) is the process of detecting efforts to trick biometric systems, specifically face recognition, using a variety of methods such as printed photos, presented images or videos, masks, or other synthetic media. PAD algorithms use subtle cues and features to distinguish between genuine and fraudulent presentation attempts, improving the security and reliability of biometric identification systems. PAD helps prevent unauthorized access and safeguards against identity fraud in a variety of applications, including secure access control and digital identity verification.

Advantages Of Proposed System:

1. Robust Feature Extraction: LBP efficiently captures local patterns in images, ensuring that key features are encoded for accurate anomaly identification.

2. Automatic Learning: LBPNets and CNNs automatically learn discriminative features, reducing the need for human feature creation and detecting subtle manipulations.

3. Hierarchical Representation: CNNs use hierarchical feature extraction to capture patterns at different levels of abstraction in order to detect complex manipulations.

4. Threat Adaptability: LBPNet and CNNs respond to growing deep fake characteristics, guaranteeing that they remain effective against emerging manipulation tactics.

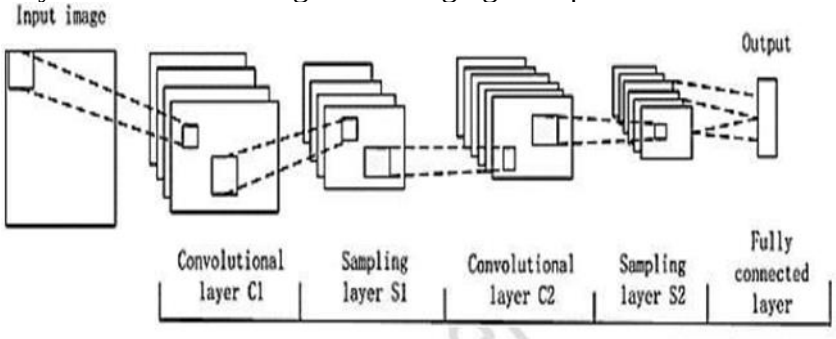


Fig 1: System Architecture

V. IMPLEMENTATION

Modules:

- Generate NLBPNet Train & Test Model:
- Upload Test Image
- Classify Picture in Image

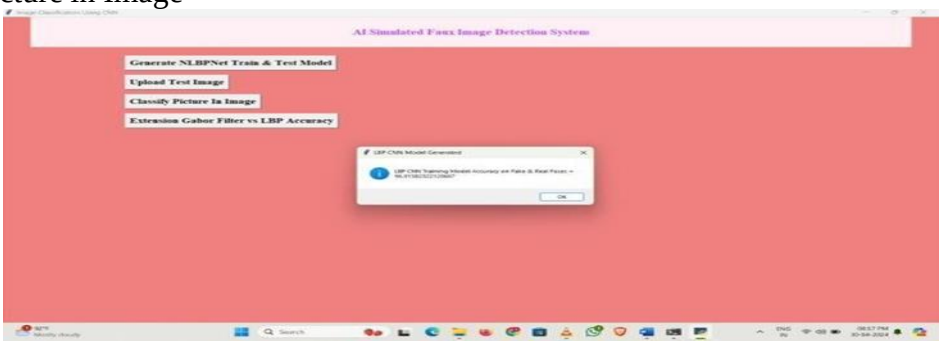


Fig 2: Implemented Model

In above screen (Fig-2) we can see CNN LBPNET model generated. Now click on 'Upload Test Image' button to uploadtest image.

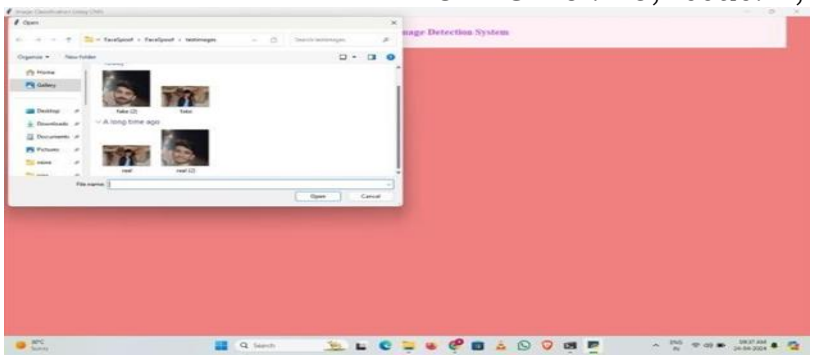


Fig 3: Uploading Image to the Model

In above screen (Fig-3) we can see two faces are there from same person but in different appearances. To simplify things, we assigned the image names false and real to see if the application could detect them. In the above screen (Fig-3), I am uploading a fake image and then clicking the 'Classify Picture in Image' button to achieve the following result.

Fig 4.1: Results of a faux image

In above screen (fig-4.1) application display message on image as it contains faux face and it is also displaying LBP format ofthe image.

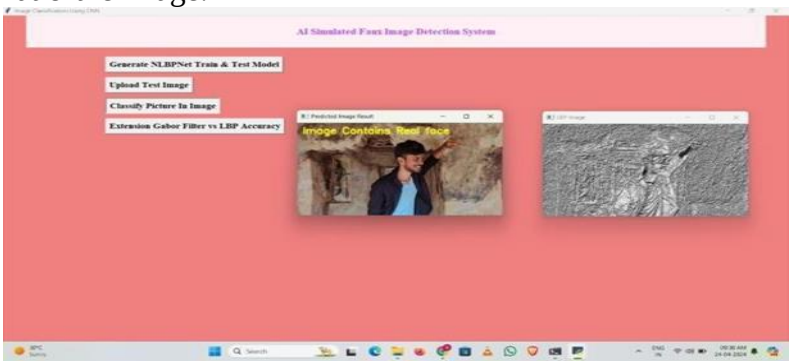


Fig 4.2 Results of a Real image

In above screen (Fig-4.2) , application display message on image as it contains Real face.

VI. CONCLUSION

Finally, that we provide the LBP-based Convolutional Neural Network, LBPNET, which is specifically intended for recognizing counterfeit faces. By extracting LBP features from images and training them using a CNN, we create a robust model that can distinguish between real and AI-manipulated images. This hybrid integration of CNN and LBPNET shows promising results in effectively identifying fake photos, ensuring the dependability of image authenticity assessments in a variety of applications.

VII. REFERENCES

1. T. Karras, T. Aila, S. Laine, and J. Lehtinen, "Progressive growing of gans for improved quality, stability, and variation," arXiv preprint arXiv: 1701.07873, 2017.
2. A. Brock, J. Donahue, and P. Belongie, "Large scale gan training for high fidelity and diverse image synthesis," arXiv preprint arXiv: 1809.11096, 2018.
3. J.-Y. Zhu, T. Park, C. Isola, and Jun-Yan Zhu, "Cycle-consistent adversarial networks," in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 2224-2232, 2017.

4. A. Alahmadi, M. Hussain, H. Aboalsamh, G. Muhammad, G. Bebis, and H. Mathkour," Passive detection of image forgery using DCT and local binary pattern", Signal, Image and Video Processing, vol. 11, no. 1, pp. 81–88, 2016.
5. S. Walia, and K. Kumar," An eagle-eye view of recent digital image forgery detection methods", BhattacharyyaP., Sastry H., Marriboyina V., Sharma R. (eds) Smart and Innovative Trends in Next Generation Computing Technologies (NGCT), Communications in Computer and Information Science, vol 828. Springer, Singapore, 2017.
6. M. Hussain, S.Q. Saleh, H. Aboalsamh, G. Muhammad, and G. Bebis," Comparison between WLD and LBP descriptors for non-intrusive image forgery detection", IEEE International Symposium on Innovations in Intelligent Systems and Applications (INISTA), pp. 197–204, 2014.
7. G. Muhammad, M. Al-Hammadi, M. Hussain, G. Bebis," Image forgery detection using steerable pyramid transform and local binary pattern", Machine Vision and Application, vol. 25, no. 4, pp. 985–995, 2014.
8. C.S. Prakash, A. Kumar, S. Maheshkar, V. Maheshkar," An integrated method of copy-move and splicing for image forgery detection", Multimedia Tools and Applications, vol. 77, no. 20, pp. 26939–26963, 2018.
9. 1. Ren, X. Jiang, and 1. Yuan," Noise-resistant local binary pattern with an embedded errorcorrection mechanism", IEEE Transactions on image Processing, vol. 22, no. 10, pp. 4049-4060,2013.
10. J. Dong, W. Wang, and T. Tan." Casia image tampering detection evaluation database", Signal and InformationProcessing (ChinaSIP), IEEE China Summit & International Conference on, pages 422–426. IEEE, 2013.
11. D.S. Vidyadharan, and S.M. Thampi," Digital image forgery detection using compact multitexture representation", Journal of Intelligent & Fuzzy Systems, vol. 32, no. 4, pp. 3177–3188, 2017.