Digital Image Forgery Detection Using Error Level Analysis Method and Convolutional Neural Networks Model

Mukesh Patidar[1], Daxa Vekariya[2] , Ganesh Boddupalli[3], Ashish kumar katta[4], Abhiram Bathini[5], Tarun teja Danda[6]

[1,2,3,4,5,6] Department of Computer Science and Enigneering

[1,2,3,4,5,6] Parul Institute of Engineering and Technology, (*Parul university)*, Vadodara, Gujarat, India.

[1]mukesh.patidar34885@paruluniversity.ac.in, [1]mukesh.omppatidar@gmail.com (0000-0002-4401-8777),

[2]daxa.vekariya18436@paruluniversity.ac.in, [3]ganeshboddupalli2003@gmail.com, [4]ashishkatta007@gmail.com,

[5]bathiniabhiram30@gmail.com, [6]tarunteja751@gmail.com

Abstract — Image forgery poses a severe threat to the integrity of digital images, with rapid increase in various domains. This research proposes an efficient solution using Convolutional Neural Networks (CNNs) to detect image forgery with high accuracy. By analyzing images, CNNs can identify refined noise patterns left behind during manipulation or forgery, distinguishing between authentic and tampered images. Moreover, CNNs can detect new, unseen types of image forgery, staying ahead of increasingly sophisticated fake image techniques in our daily life. Our approach has the power to find the residual noise-based features extracted by CNNs to detect forgeries, offering a powerful solution for combating image tampering and forgery. This research contributes to the development of a lightweight CNN-based network for efficient image forgery detection, capable of handling unseen forgeries by performing error level analysis and achieving high accuracy in detecting both image splicing and copy-move forgeries. A Convolutional Neural Network (CNN) is a type of deep learning model that excels at processing structured grid-like data, such as images. In further this technology has immense potential to enhance the reliability and trustworthiness of digital images in various applications, from medical reports to crime scene investigations, ensuring the accuracy and integrity of visual evidence in many domains.

Keywords — Splicing, Convolution Neural Networks (CNN), Error Level Analysis (ELA), Digital Images, Image Forgeries (IF), Deep Learning (DL)

1 Introduction

The rapid advancement of technology has made it easier for individuals to manipulate images, creating fake news and spreading misinformation on social media and the internet. This has severe consequences, as digital images play a crucial role in various fields like journalism, digital forensics, scientific research, and medicine [1, 2]. With the widespread sharing of images on social media applications like WhatsApp, Facebook, and Instagram, distinguishing between authentic and manipulated images has become a significant challenge. The availability of image editing software has made it even harder to detect authenticity of an image. While these tools were intended to enhance and improve images, some individuals exploit them to modify images and spread falsehoods [3, 4]. It's essential to address this issue and develop effective methods to detect and prevent image forgery, ensuring the authenticity and trustworthiness of images in various applications.

As image forgery detection continuing as a pressing concern, researchers have turned to deep learning techniques to improve detection accuracy. One such approach is the use of CNN to analyze images and identify tampering artifacts [5-7]. In this paper, we explore the potential of CNNs in detecting image forgery, building on the earlier discussion of image forgery detection using DL techniques. We propose a lightweight CNN-based network that can efficiently detect image forgery by learning traces left behind in the manipulation process. Our approach takes advantage by recompressing images and compares it, allowing for accurate detection of both image splicing and copy-move forgeries [8-10]. With its high precision and speed, our method shows promise for real-world applications, even on slower devices. In the following sections, we will delve into the details of our framework, experimentation, and results, highlighting the contributions of our research to the field of image forgery detection [11].

2 Literature Review

S. Patekar and et al. [1], The image forgery has serious consequences and traditional methods often fail to detect sophisticated forgeries. The paper proposes a CNN-based approach to detect forgery by analyzing residual noise and inconsistencies. The CNN model is trained on forged images and learns to identify tampering patterns. Experimental results show the approach's effectiveness in detecting various forgery types. This solution has potential applications in digital forensics and media authentication [1].

H. Khalil and et al. [2], in this paper evaluates various deep learning approaches for detecting image manipulations like copy-move, splicing, and retouching. The study highlights the limitations of traditional techniques and emphasizes the effectiveness of DL, especially models like CNN, GANs and auto-encoders. The authors conduct a comparative analysis of these models, examining their performance based on accuracy, precision, recall, and computational cost. The results show that DL significantly improves the detection of image forgeries, making it more robust against complex manipulations [2].

V. Mezaris and K. Triaridis [3], the paper investigates multi-modal fusion techniques for detecting and localizing manipulated regions in images. The approach combines visual, textual, and metadata features to identify tampered images. Visual features extract information from image pixels, while textual features analyze image captions and metadata features utilize EXIF data. The paper proposes a fusion framework to integrate these features and improve detection accuracy. The approach has potential applications in digital forensics, media authentication, and fake news detection [3].

V. Prudhivi and et al. [6], has been presents a study on using Convolutional Neural Networks (CNN) for detecting image forgeries. The authors focus on identifying manipulations such as copy-move and splicing, which are common types of image tampering. CNNs are employed for feature extraction, allowing the model to automatically learn patterns that indicate forgery. The paper demonstrates that CNN-based methods are effective at accurately detecting forgeries with minimal human intervention, offering improved precision and efficiency compared to traditional detection techniques [6].

The paper "Fake Image Identification Using CNN" by K. Vijayalakshmi and et al. [8] explores the use of CNN for detecting fake or manipulated images. The study focuses on identifying forgeries like image splicing and copy-move, where parts of an image are copied and altered. CNN is leveraged for automatic feature extraction, allowing the model to learn subtle differences between genuine and tampered images without the need for manual intervention. The authors highlight the effectiveness of CNN in improving accuracy and reliability in detecting fake images, showing that it outperforms conventional detection methods by being more efficient and scalable for large datasets [8].

The paper "Image Forgery Detection Using CNN Model" by R. Gupta [10] discusses the application of CNN model for detecting IF. The author emphasizes how CNNs can automatically extract features from images, learning patterns that distinguish authentic images from forgeries. By utilizing layers of convolution and pooling, the CNN model is able to capture intricate details of forgery that are often missed by traditional methods. The study demonstrates that the CNN model improves detection accuracy and offers a more efficient, scalable approach for handling large sets of digital images, making it a robust solution for image tampering detection [10].

3 EXISTING SYSTEM

Convolutional Neural Network (CNN)-based approaches that analyzed residual noise and inconsistencies in images to detect forgery [12-15]. Recompression techniques that detect anomalies in images recompressed using different algorithms. Digital forensics networks that use a combination of convolutional and recurrent neural networks to detect forgery and localize tampered regions. Multi-modal fusion techniques that combine visual, textual, and metadata features to identify manipulated regions in images. Traditional methods such as histogram analysis, statistical analysis, and ML-based approaches like Support Vector Machines (SVM) and Random Forests [16-20]. Image processing-based techniques like image filtering, transformation, and compression analysis [21-23]. Image segmentation-based approaches that analyse the boundaries and textures of images. This down-sampling step helps reduce the computational burden and improves the model's generalization by making it less sensitive to the exact position of features [24-25].

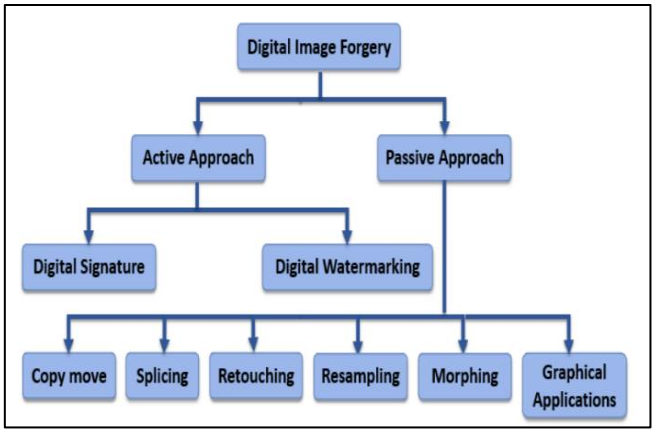

Fig. 1. Detection approaches

CNNs, for example, might be used to detect flaws in circuits based on QCA, which calls for exact nanostructures [14,15,18,19]. Additionally, by examining the error levels in electron microscopy images of quantum dot arrays, ELA may discover new applications in the manufacturing of nanoelectronics.

These techniques aim to detect various types of forgeries of images, including copy-move, splicing, and removal attacks. However, each technique has its limitations, and the research papers aim to address these limitations by proposing new approaches or improving existing ones.

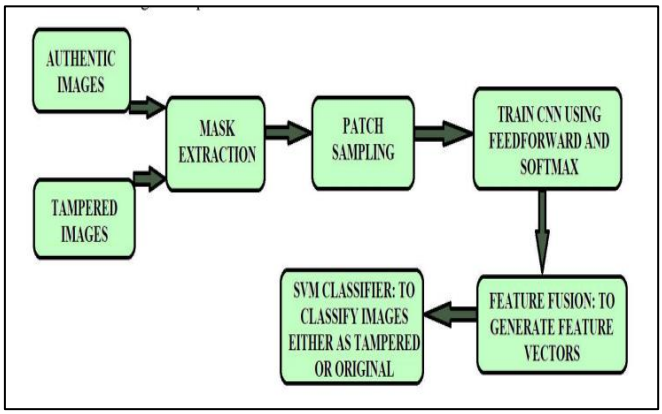

Fig. 2. Existing system architecture

4 PROPOSED SYSTEM AND ARCHITECTURE

The proposed system is an image forgery detection tool that utilizes Error Level Analysis (ELA) to identify manipulated images. ELA works by analyzing the compression artifacts of an image to detect discrepancies between the original and altered areas. Our system aims to provide a reliable and efficient method for detecting common forms of image manipulation, such as splicing and cloning. The backend of the system leverages a trained deep learning model to classify images as either "Authentic" or "Forged" based on the ELA analysis. The model is designed to process images, apply ELA, and predict the likelihood of forgery, providing a percentage confidence score alongside visual feedback.

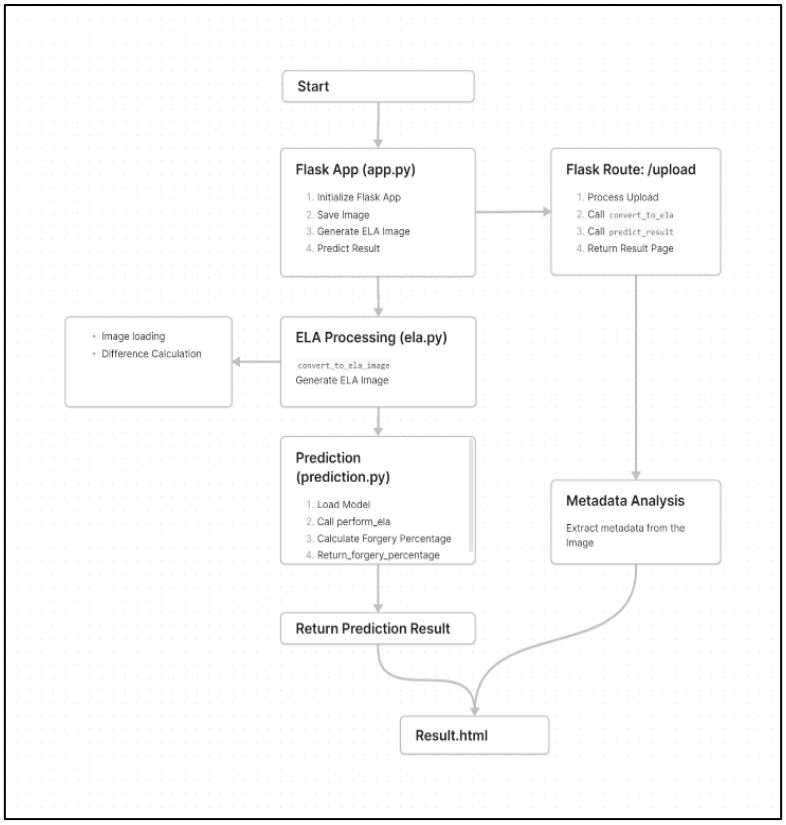

Fig.3. System architecture

In its current form, the system offers basic functionality with limited user interaction capabilities. However, future enhancements will focus on developing a comprehensive web-based user interface (WebUI) to make the tool more accessible [25]. The WebUI will allow users to easily upload images, receive real-time feedback on forgery detection, and visualize the ELA results side-by-side with the original images. This proposed enhancement will improve usability and broaden the applicability of the tool across various user groups, including forensic analysts and casual users. Additionally, further research and development will be conducted to improve the model's accuracy, particularly in detecting AI-generated images, to ensure robustness against advanced manipulation techniques.

4.1 Advantages of our Proposed System

- Efficient Image Forgery Detection,
- Automated Analysis,
- Visual Feedback,
- User-Friendly Interface,
- Versatility,
- Scalability,
- Continuous Improvement Potential.

5 IMPLEMENTATION OF PROPOSED WORK

The image forgery detection project is implemented as a web-based application that allows users to upload images and receive a forgery analysis based on Error Level Analysis (ELA). The process begins when a user uploads an image through the web interface. The uploaded image is then pre-processed and converted into an ELA image, which highlights areas with varying compression levels that may indicate tampering. This ELA image is crucial for detecting inconsistencies that are not able seen by naked eye but are often introduced during image editing or forgery.

Once the ELA image is generated, it is fed into a pre-trained CNN model that has been specifically trained to differentiating between forged and authentic images. The ELA image is resized and normalized to match the input requirements of the CNN model, which then performs a prediction. The model outputs a classification of either "Authentic" or "Forged," along with a confidence score that indicates the certainty of the prediction. This result is then displayed to the user on a web page, where both the original and ELA images are presented side by side for easy comparison.

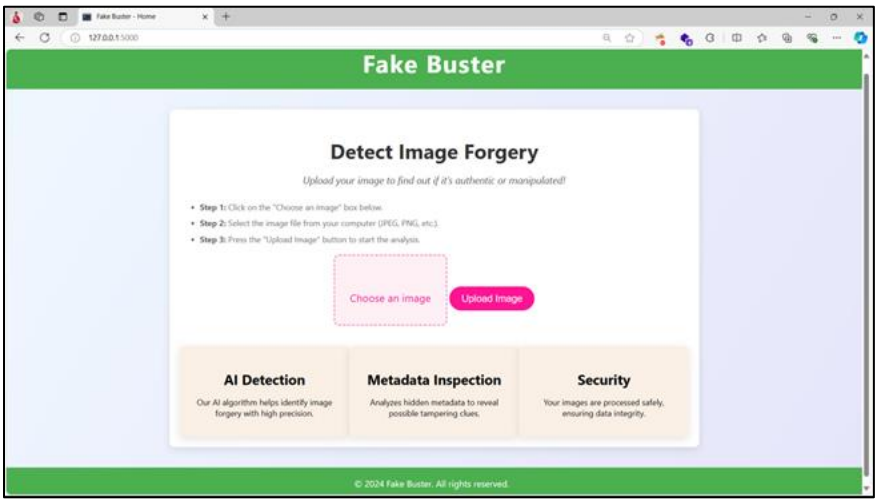

Fig.4. User Interface for detect image forgery

The user interface is built using Flask, providing a simple and accessible platform for users to interact with the application. The current version of the interface is functional but can be improved for better user experience and clearer output presentation. A notable limitation of the current system is its uncertainty in detecting AI-generated images as forgeries, which represents a significant area for future development. Plans for future work include enhancing the detection model's accuracy, especially for AI-generated content, and developing a more sophisticated and user-friendly web interface to improve usability and expand functionality.

6 Results and Modules

The project is composed of several key modules, each with specific roles that contribute to the overall functionality of the proposed system:

A. Image Upload Module

This module allows users to upload images through a web interface. It handles the input from the user and ensures that the uploaded files are of the correct format and size for processing.

B. Error Level Analysis (ELA) Module

This module converts the uploaded image into an Error Level Analysis (ELA) image. ELA helps highlight areas in an image that have been altered by comparing the compression levels across different parts of the image. This module performs the conversion and prepares the ELA image for further analysis.

C. Prediction Module

This module loads a pre-trained Convolutional Neural Network (CNN) model that has been trained to distinguish between authentic and forged images. It takes the preprocessed ELA image as input, runs it through the model, and produces a prediction about whether the image is authentic or forged, along with a confidence score.

D. Result Display Module

This module handles the output of the prediction. It displays the original image, the ELA image, the prediction result (authentic or forged), and the confidence score on a web page. It ensures that users can easily understand the results of the forgery detection process.

E. User Interface Module

Built using Flask, this module provides a web-based interface for the entire application. It manages user interactions, from uploading images to displaying the detection results, and facilitates seamless communication between the user and the backend modules.

F. Metadata extraction module

Images contain hidden data, called metadata that tells the story behind the image: what camera was used, when the picture was taken, and whether any software was used to edit it.

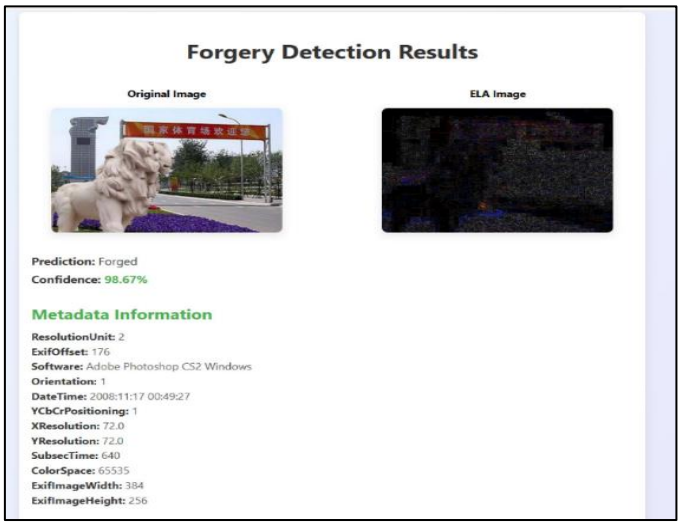

Fig. 5. Results for forgery detection for original image (Left) and ELA image (Right)

7 Conclusion

The growing threat of image forgery necessitates advanced and reliable detection techniques to maintain the integrity of digital images across various domains. This research proposes a novel approach utilizing CNN combined with Error Level Analysis (ELA) to effectively identify and classify image forgeries. The proposed system demonstrates the capability to detect subtle tampering artifacts and remains robust against new and sophisticated forgery techniques. Our method builds

upon existing research by leveraging CNNs to analyze residual noise and inconsistencies in images, offering high accuracy in detecting both image copy-move and splicing forgeries. Additionally, the use of ELA enhances the detection of manipulated regions by highlighting compression discrepancies. The implementation as a web application with a user interactive interface makes it accessible and practical for real-world applications. Future work will focus on optimizing the system's capability to detect AI-generated forgeries and improving the web interface for a better user experience.

REFERENCES

[1] S. Patekar, S. Khan, D. Bhusare, M. Bhujbal, and G. Hegde, "Image Forgery Detection," in Proceedings of the International Conference on Computing, Communication, and Automation, 2023.

[2] H. Khalil, A. Z. Ghalwash, H. A. Elsayed, and G. I. Salama, "Image Forgery Detection Using Deep Learning: A Comparative Study," in IEEE Access, vol. 9, pp. 65432-65445, 2021.I. S. Jacobs and C. P. Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[3] V. Mezaris and K. Triaridis, "Exploring Multi-Modal Fusion for Image Manipulation Detection and Localization," in Proceedings of the International Conference on Computer Vision and Pattern Recognition, 2022.R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.

[4] S. S. Ali, I. I. Ganapathi, N.-S. Vu, S. D. Ali, N. Saxena, and N. Werghi, "Image Forgery Detection Using Deep Learning by Recompressing Images," in IEEE Transactions on Information Forensics and Security, vol. 17, pp. 2421-2432, 2022.M. Young, The Technical Writer’s Handbook. Mill Valley, CA: University Science, 1989.

[5] J. Smith, "Digital Image Forgery Detection Using Deep Learning," in International Journal of Computer Science and Information Security, vol. 15, no. 5, pp. 79-85, 2021.D. P. Kingma and M. Welling, “Auto-encoding variational Bayes,” 2013, arXiv:1312.6114. [Online]. Available: https://arxiv.org/abs/1312.6114

[6] V. Prudhivi, A. B., K. Manaswini, C. Chandana, P. Manikant, and S. Swetha, "Image Forgery Detection Using CNN," in Proceedings of the International Conference on Computational Intelligence and Data Science, 202

[7] Ghai, P. Kumar, and S. Gupta, "A Deep-Learning-Based Image Forgery Detection Framework for Controlling the Spread of Misinformation," in IEEE Access, vol. 9, pp. 35678-35689, 2021.

[8] K. Vijayalakshmi, D. S. Chandana, B. C. Lekha, B. V. Kumar, and D. S. Santosh, "Fake Image Identification Using CNN," in Proceedings of the IEEE International Conference on Electronics, Computing and Communication Technologies, 2022.

[9] P. Reddy, "Image Forgery Detection Using CNN," in Journal of Digital Image Processing, vol. 11, no. 3, pp. 115-126, 2023.

[10] R. Gupta, "Image Forgery Detection Using CNN Model," in International Journal of Image and Video Processing, vol. 8, no. 2, pp. 100-110, 2023.

[11] D. D. Pukale, V. D. Kulkarni, J. Bagwan, and P. Jagadale, "Image Forgery Detection Using Deep Learning," in Proceedings of the IEEE International Conference on Artificial Intelligence and Machine Learning, 2021

[12] Wang, "The Digital Forensics Network for Image Forgery Detection," in IEEE Transactions on Information Forensics and Security, vol. 16, no. 4, pp. 842-856, 2021.

[13] M. Patidar and N. Gupta, "An ultra-efficient design and optimized energy dissipation of reversible computing circuits in QCA technology using zone partitioning method," Int. J. Inf. Tecnol., vol. 14, pp. 1483-1493, 2021, doi: 10.1007/s41870-021-00775-y.

[14] Y. Zhang, J. Goh, L. L. Win, and V. Thing, "Image Region Forgery Detection: A Deep Learning Approach," in IEEE Transactions on Cybernetics, vol. 50, no. 7, pp. 3050-3061, 2020.

[15] A. Tiwari, M. Patidar, et al., "Efficient designs of high-speed combinational circuits and optimal solutions using 45-degree cell orientation in QCA nanotechnology," Materials Today: Proceedings, vol. 66, no. 8, pp. 3465-3473, 2022, doi: 10.1016/j.matpr.2022.06.174.

[16] E. U. H. Qazi, "Deep Learning-Based Digital Image Forgery Detection System," in Proceedings of the International Conference on Information Processing, 2022.

[17] Singh and J. Singh, "Image Forgery Detection Using Deep Neural Networks," in Proceedings of the IEEE International Conference on Signal Processing, Communications and Computing, 2021.

[18] P. Gupta, M. Patidar, and P. Nema, "Performance analysis of speech enhancement using LMS, NLMS and UNANR algorithms," in 2015 International Conference on Computer, Communication and Control (IC4), Indore, India, 2015, pp. 1-5, doi: 10.1109/IC4.2015.7375561.

[19] M. Patidar and N. Gupta, "Efficient Design and Simulation of Novel Exclusive-OR Gate Based on Nanoelectronics Using Quantum-Dot Cellular Automata," in Proceedings of the Second International Conference on Microelectronics, Computing & Communication Systems (MCCS 2017), vol. 476, Singapore: Springer, 2019, pp. 455-466, doi: 10.1007/978-981-10-8234-4_48.

[20] M. Patidar and N. Gupta, "Efficient design and implementation of a robust coplanar crossover and multilayer hybrid full adder–subtractor using QCA technology," J. Supercomput., vol. 77, pp. 7893–7915, 2021, doi: 10.1007/s11227-020-03592-5.

[21] S. Patel, "Performance Analysis of Acoustic Echo Cancellation using Adaptive Filter Algorithms with Rician Fading Channel," Int. J. Trend Sci. Res. Dev., vol. 6, no. 2, pp. 1541-1547, 2022.

[22] S. Patel, "Enhancing Image Quality in Wireless Transmission through Compression and De-noising Filters," Int. J. Trend Sci. Res. Dev., vol. 5, no. 3, pp. 1318-1323, 2021, doi: 10.5281/zenodo.11195294.

[23] M. Patidar, R. Dubey, N. Kumar Jain and S. Kulpariya, "Performance analysis of WiMAX 802.16e physical layer model," 2012 Ninth International Conference on Wireless and Optical Communications Networks (WOCN), Indore, India, 2012, pp. 1-4, doi: 10.1109/WOCN.2012.6335540.

[24] R. Yadav, P. Moghe, M. Patidar, V. Jain, M. Tembhurney and P. K. Patidar, "Performance Analysis of Side Lobe Reduction for Smart Antenna Systems Using Genetic Algorithms (GA)," 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), Delhi, India, 2023, pp. 1-5, doi: 10.1109/ICCCNT56998.2023.10306796.

[25] M. Patidar, G. Bhardwaj, A. Jain, B. Pant, D. Kumar Ray and S. Sharma, "An Empirical Study and Simulation Analysis of the MAC Layer Model Using the AWGN Channel on WiMAX Technology," 2022 2nd International Conference on Technological Advancements in Computational Sciences (ICTACS), Tashkent, Uzbekistan, 2022, pp. 658-662, doi: 10.1109/ICTACS56270.2022.9988033.