IJARETY

International Journal of Advanced Research in Education and TechnologY (IJARETY)

Volume 11, Issue 3, May-June 2024

Impact Factor: 7.394

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 7.394| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 11, Issue 3, May-June 2024 ||

DOI:10.15680/IJARETY.2024.1103029

Image Immunizer an Image Tamper Resilient Multi Task Learning Scheme for Image Lossless Auto-Recovery

Prethi M, Dr. K. Pooranapriya, Dr. C. Gomathi

PG Scholar, Department of Master of Computer Applications, Vidyaa Vikas College of Technology, Tirucengode, Tamil Nadu, India

Professor, Department of Electronics and Communication Engineering, Vidyaa Vikas College of Technology, Tirucengode, Tamil Nadu, India

Professor, Department of Master of Computer Applications, Vidyaa Vikas College of Technology, Tirucengode, Tamil Nadu, India

ABSTRACT: Image tampering attacks involve the unauthorized or deceptive alteration of digital images, often for the purpose of misrepresenting their content or context. To address these challenges and combat image tampering, research on image tamper localization has garnered extensive attention. In this context, this project introduces an enhanced scheme known as Image Immunizer for image tampering resistance and lossless auto – recovery using Vaccinator and Invertible Neural Network a Deep Leaning Approach. This proposed technique achieves promising results in real-world tests where experiments show accurate tamper localization as well as high-fidelity content recovery.

I. INTRODUCTION

Social networking refers to using internet-based social media sites to stay connected with friends, family, colleagues, or customers. Social networking can have a social purpose, a business purpose, or both through sites like Facebook, Twitter, Instagram, and Pinterest. Social networking is also a significant opportunity for marketers seeking to engage customers. However, it also raises privacy concerns, such as oversharing personal information and loopholes in privacy settings. Adding strangers as friends can lead to security risks, and even closed groups may not guarantee privacy. Additionally, frequent social media usage can lead to inadvertent sharing of sensitive information and compromise privacy, as security agencies may access posted content.

Scope of The Project

The Image Immunizer Middleware for Online Social Networks using Invertible Neural Network is a robust solution designed to fortify image security on social media platforms. Through modules like Cyber Vaccinator and Vaccine Validator, the system ensures the integrity of shared images, incorporating imperceptible perturbations for enhanced security. The forward pass, backward pass, and adversarial simulation techniques enable tamper detection, image self-recovery, and resilience against potential threats like deepfakes. Performance metrics, including PSNR, and OSN-specific metrics evaluate the effectiveness of immunization processes. Seamlessly integrating with existing OSN architectures, the middleware provides a user-friendly and comprehensive defense against image-based attacks.

II.LITERATURE SURVEY

Title: Content Authentication and Tampered Localization Using Ring Partition and CSLBP-Based Image Hashing
Author: Abdul Shaik , Ram Karsh
Year: 2023
Reference Link: https://ieeexplore.ieee.org/document/10311570
Objective:
The objective of the study is to propose a perceptual image hashing technique using ring partition and CSLBP (Circular Symmetric Local Binary Pattern). The proposed method aims to provide stability, rotation invariance, and better performance in terms of robustness and discrimination compared to existing approaches.

Methodology:
The methodology involves converting the input image to a standardized form and extracting ring-based statistical features using Circular Symmetric Local Binary Pattern (CSLBP). Crucially, the chosen ring partition technique ensures feature stability and rotation invariance. The algorithm strategically combines ring partition and CSLBP to create a robust image hashing method resistant to geometric operations like rotation. Experimental results demonstrate superior performance in robustness and tamper localization, though a limitation is noted in the dependency on hash length reduction for improvement.

Algorithm/Techniques:
The employs ring partition and Circular Symmetric Local Binary Pattern (CSLBP) for perceptual image hashing. Ring partition preserves feature stability during image rotation, and CSLBP extracts circular symmetric local binary patterns. This combined approach establishes a robust hashing method resistant to geometric operations, particularly rotation. Experimental results highlight its superior performance in robustness and tamper localization, while a limitation involves the necessity of hash length reduction for potential improvement.

Merits:
Better Performance the results indicate that the proposed hashing method offers better performance in terms of robustness and discrimination compared to other existing approaches. Small Tampering Area Localization the method is sensitive to changes in visual information, allowing for the detection and localization of small tampering areas.

Demerits:
Hash Length Limitation: The major limitation of the proposed method is the need to reduce the hash length for improvement. This suggests a potential trade-off between hash length and performance.

III.PROPOSED SYSTEM

The proposed system comprises several key modules and functionalities to achieve this objective:

- **Cyber Vaccinator Module**
  The core module involves pre-processing, mid-processing, and post-processing steps. Landmark detection algorithms are utilized to create binary masks, distinguishing object contours in images shared on OSN.
- **Vaccine Validator**
  It distinguishes between vaccinated (secured) and unvaccinated (potentially tampered) media shared on the platform.
- **Forward Pass - Tamper Detection and Localization:**
  The forward pass involves transforming the original image and its associated metadata into an immunized version using INN.
- **Backward Pass - Image Self-Recovery**
  In the backward pass of the INN, the hidden perturbation is transformed into information, facilitating the recovery of the original image and its associated metadata.
- **Adversarial Simulation for OSN:**
  The system incorporates an adversarial simulation strategy during training, tailored for OSN scenarios. This exposes the network to potential threats specific to social media, including image-based attacks such as deepfakes and contextually relevant manipulations.
- **Integration with OSN Architecture:**
  The middleware is designed to seamlessly integrate with existing OSN architectures, ensuring compatibility and easy adoption within popular social media platforms. This integration facilitates widespread use and adoption by OSN users.

ADVANTAGES

- Accurate tamper detection fortifies shared images against potential threats.
- Preserves original image quality during the recovery process.
- Prepares the system for OSN-specific threats, including deepfake attempts.
- Tamper Resilience: Enhances resistance against unauthorized alterations.
- Ensures recovery without loss of original image information.

DOI:10.15680/IJARETY.2024.1103029

IV.MODULES

1. Social Networking Web App

The User Profile module fosters personalization, allowing users to create and customize profiles with responsive design elements.. Direct communication is enhanced through the Messaging and Chat module, offering real-time messaging, multimedia file sharing, and group chat functionalities. Admin Panel module centralizes control and management.

2. End User Interface

The End User Interface module provides a seamless and intuitive experience for social network users, encompassing essential functionalities such as registration, login, social connections, image sharing, download, and interaction with shared content. The module also includes features for applying digital attacks to images, sharing tampered content, and receiving notifications.

3. Adversarial: Training Against Threats

The system employs adversarial simulation, leveraging the capabilities of the Invertible Neural Network, to fortify its resilience against potential threats. The Invertible Neural Network, is well-prepared to detect and counteract a diverse array of potential attacks, thereby enhancing its robustness in maintaining the integrity of the digital landscape.

4. Image Immunizer Middleware

The Image Immunizer Middleware is a crucial component within a system designed to enhance the security and integrity of digital images. This middleware employs Invertible Neural Network (INN) to fortify images against malicious tampering, ensuring their authenticity and preventing unauthorized modifications.

4.1. Cyber Vaccinator:

Within the Cyber Vaccinator framework, the utilization of an Invertible Neural Network (INN) enhances the system's ability to preserve media authenticity through a sequence of pre-processing, mid-processing, and post-processing steps.

4.2. Vaccine Validator:

Integrated into the system is the Vaccine Validator, a critical component designed to discern between vaccinated and unvaccinated media.

4.3. Forward Pass with Tamper Detection and Localization:

In the face of an attacked image, a localizer comes into play, determining tampered areas by predicting the tamper mask and attack.

4.4. Backward Pass for Image Self-Recovery:

In the backward pass, the hidden perturbation, transformed by the Invertible Neural Network, is converted into information.

5. Objective Loss Function

The loss function measures the error or difference between the predicted output of a model and the actual target values.

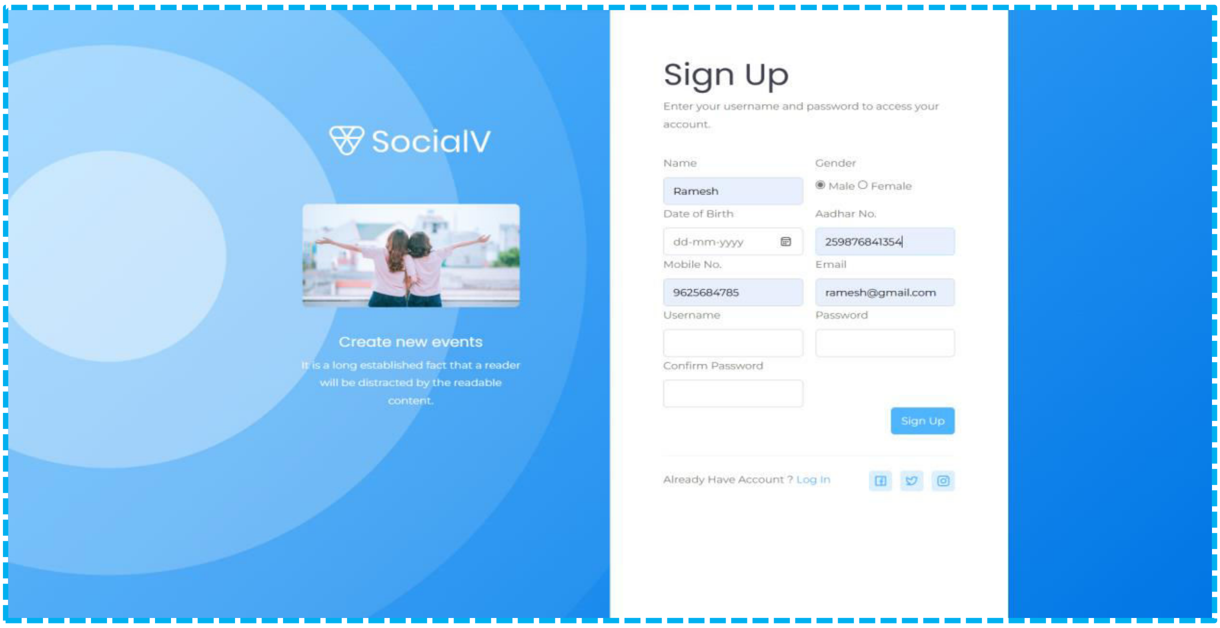
Run Length Encoding

Lossless image recovery using Run-Length Encoding (RLE) is a technique that focuses on preserving the original image data while achieving efficient image recovery.

6. Notification

The Notification Module serves as a vital component in keeping users informed and empowered when it comes to shared vaccinated images on other social networks. Specifically, when a user downloads and shares a vaccinated image without any attack, the Image Immunizer detects the shared image and triggers an email notification to the user.

V. EXPERIMENT AND RESULTS



Sign Up

Enter your username and password to access your account.

Name: Ramesh

Gender: ● Male ○ Female

Date of Birth: dd-mm-yyyy

Aadhar No.: 259876841354

Mobile No.: 9625684785

Email: ramesh@gmail.com

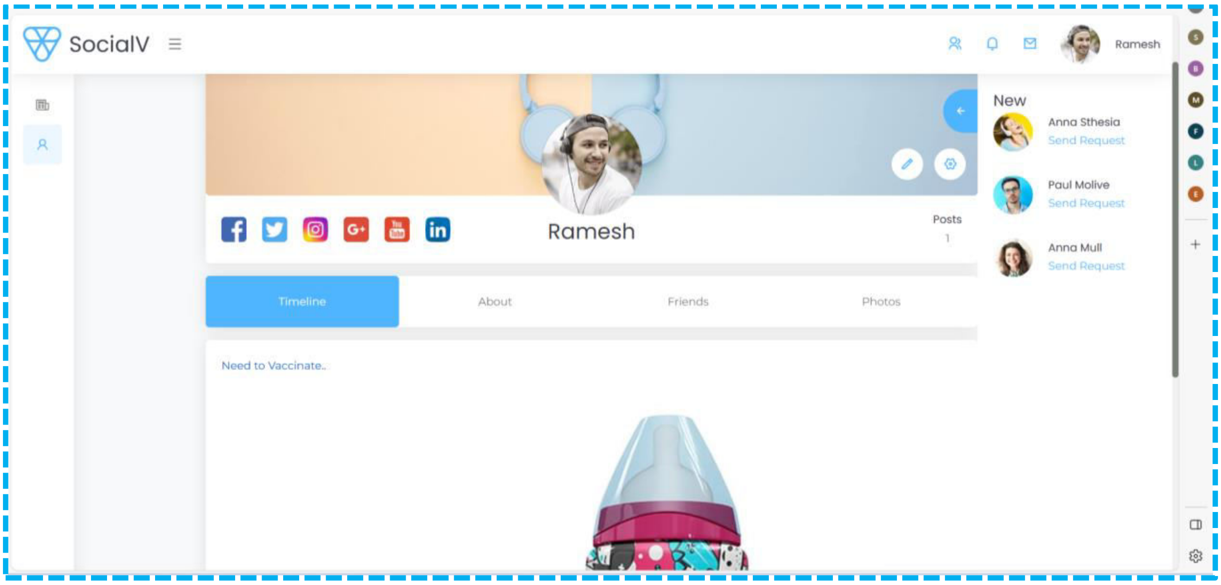
Username:

Password:

Confirm Password:

SocialV
Create new events
It is a long established fact that a reader will be distracted by the readable content.
Sign Up
Already Have Account ? Log In

Figure 1: Socio 1 login page



Ramesh

Posts 1

Need to Vaccinate..

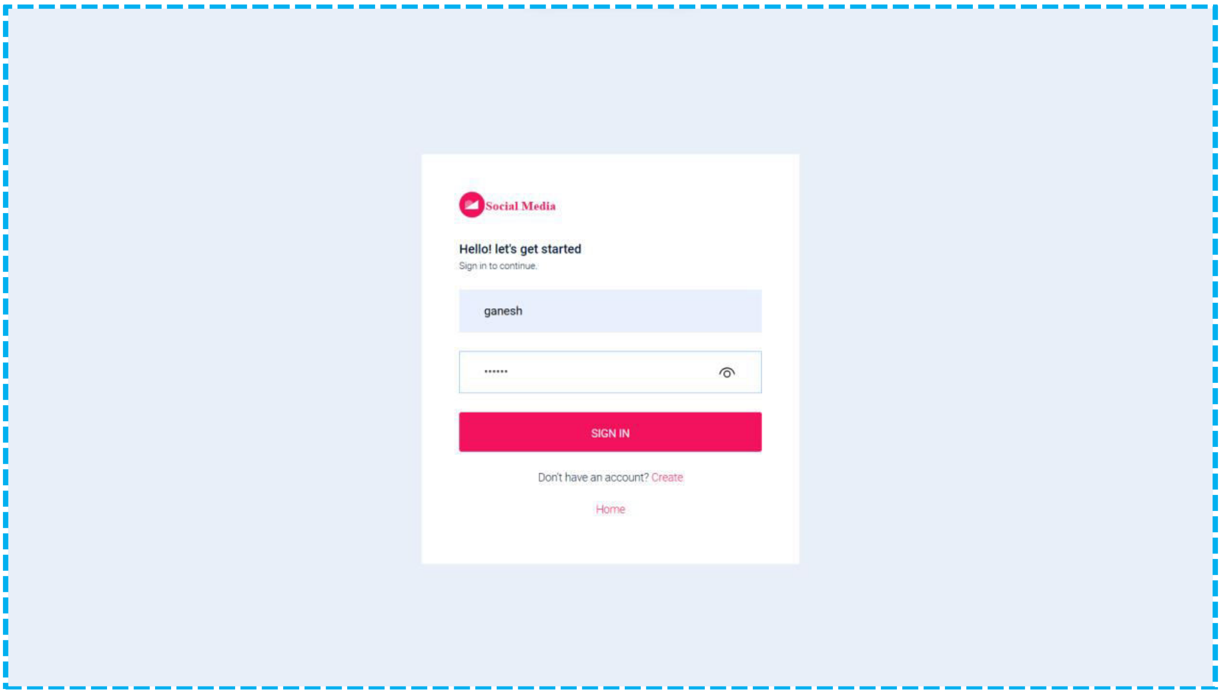
New

Anna Sthesia — Send Request

Paul Molive — Send Request

Anna Mull — Send Request

Figure 2: User s1 upload image



Social Media

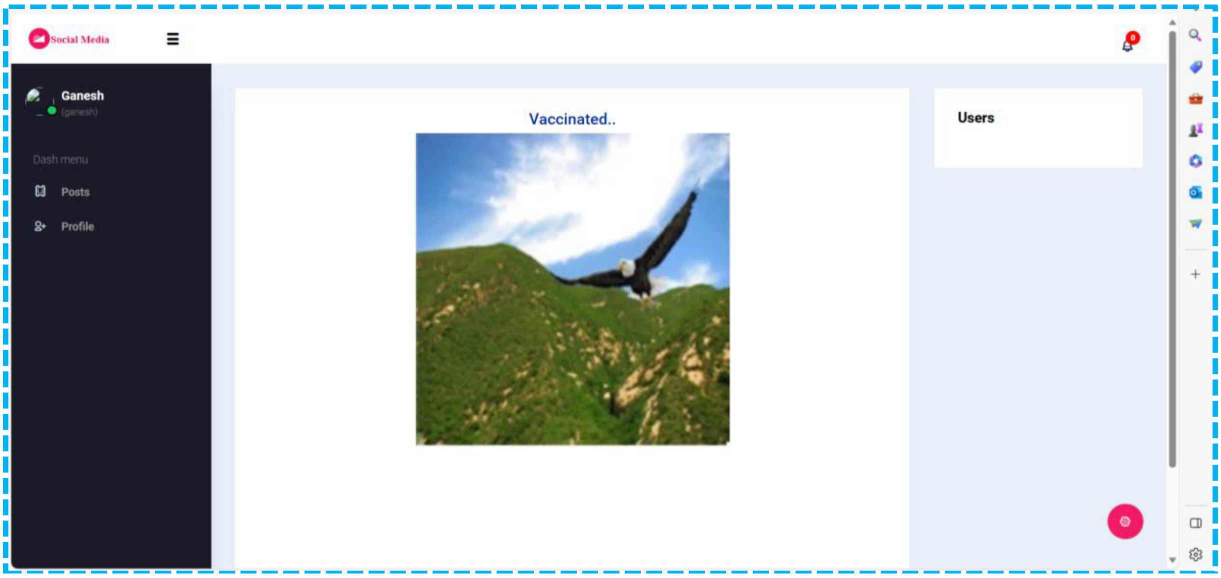
Hello! let's get started

Sign in to continue.

ganesh

••••••

Figure 4: Soci 2 login page



Vaccinated..

Figure 5: Soio 2 upload same image with attack

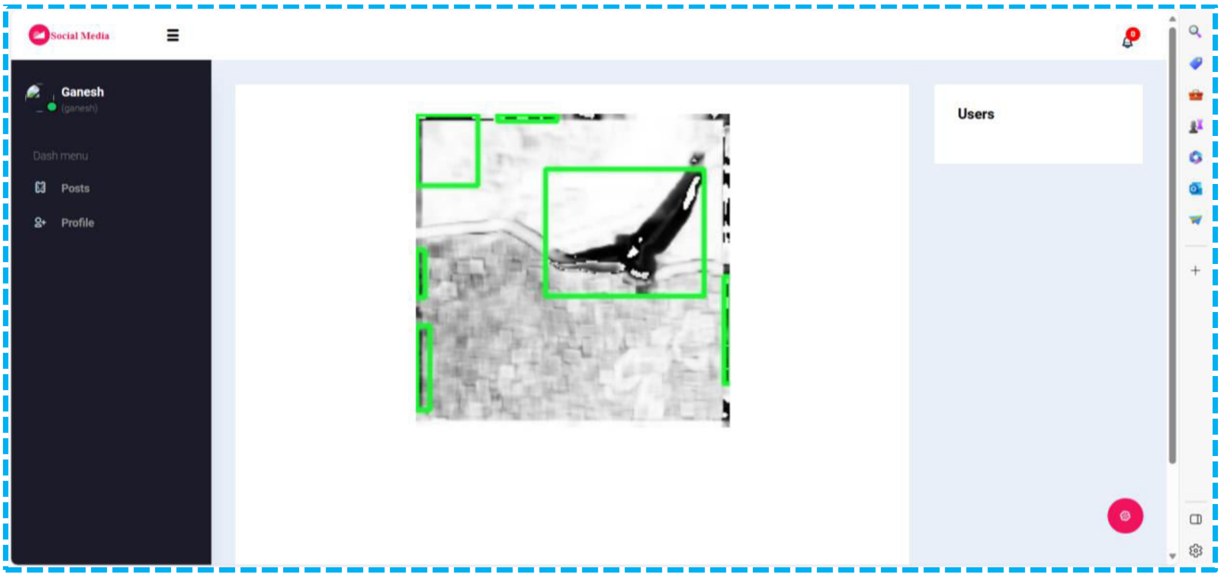


Figure 6: Attack is identified & leared

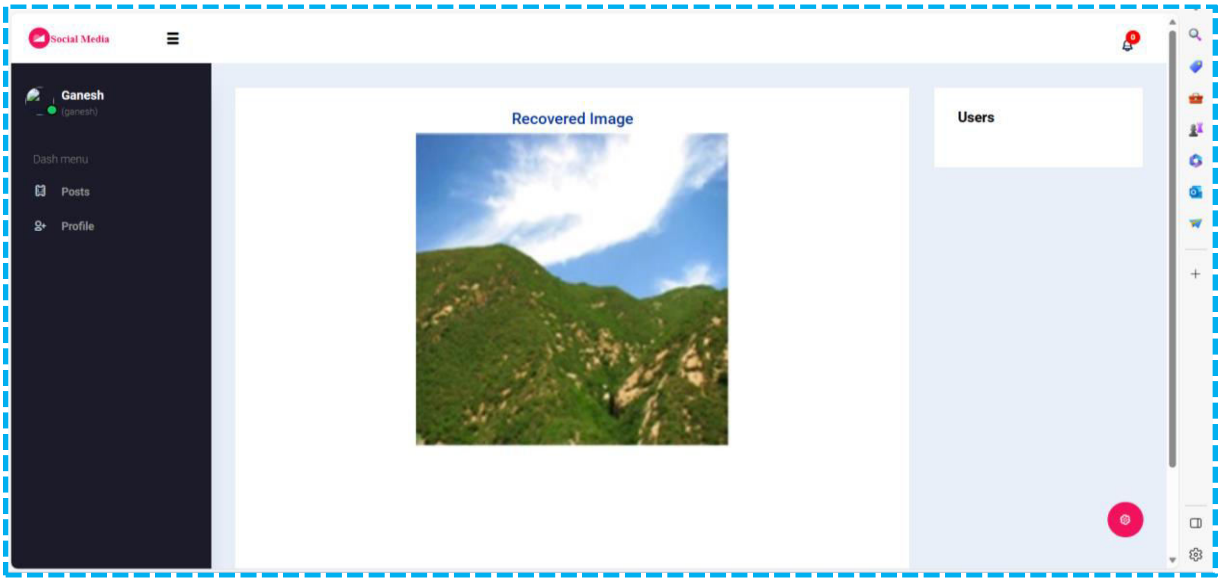


Figure 7: Recovered image

VI. CONCLUSION

In conclusion, the project Image Immunizer Middleware for Online Social Networks offers a cutting-edge solution to combat the growing threat of digital image attacks. Invertible Neural Network technology and incorporating adversarial simulation, the system provides a formidable defence, securing the authenticity and integrity of images shared on social networking platforms. Adversarial simulation during training further strengthens the system, exposing it to a spectrum of potential threats, including both malicious and benign attacks.

REFERENCES

1. C. Dong, X. Chen, R. Hu, J. Cao and X. Li, "MVSS-Net: Multi-view multi-scale supervised networks for image manipulation detection", IEEE Trans. Pattern Anal. Mach. Intell., vol. 45, no. 3, pp. 3539-3553, Mar. 2023.
2. X. Liang, Z. Tang, X. Zhang, M. Yu and X. Zhang, "Robust hashing with local tangent space alignment for image copy detection", IEEE Trans. Depend. Sec. Comput., Aug. 2023.

3. X. Liang, Z. Tang, Z. Huang, X. Zhang and S. Zhang, "Efficient hashing method using 2D–2D PCA for image copy detection", IEEE Trans. Knowl. Data Eng., vol. 35, no. 4, pp. 3765-3778, Apr. 2023.
4. X. Lin et al., "Image manipulation detection by multiple tampering traces and edge artifact enhancement", Pattern Recognit., vol. 133, Jan. 2023.
5. Z. Zhang, Y. Qian, Y. Zhao, L. Zhu and J. Wang, "Noise and edge based dual branch image manipulation detection", arXiv:2207.00724, 2022.
6. X. Liu, Y. Liu, J. Chen and X. Liu, "PSCC-Net: Progressive spatio-channel correlation network for image manipulation detection and localization", IEEE Trans. Circuits Syst. Video Technol., vol. 32, no. 11, pp. 7505-7517, Nov. 2022.

IJARETY

International Journal of Advanced Research in Education and Technology

ISSN: 2394-2975 Impact Factor: 7.394

www.ijarety.in editor.ijarety@gmail.com