www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 04, Issue 05, May 2024, pp: 511-516

e-ISSN : 2583-1062

Impact Factor: 5.725

VACCINATOR IMAGE FOR TAMPER-RESILIENTAND LOSSLESS AUTO-RECOVERY

Rajkumar A^{1}, Santhakumar G K^{2}, Boopathi R^{3}, Zakir Hussain R^{4}, Arasai P^{5}

^{1,2,3,4,5}Tichy Engimeering College, Trichy,Tamilnadu, India.

ABSTRACT

Digital images are susceptible to a range of vulnerabilities and threats that can compromise security and privacy in online social networking sites. 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. Image Processing and Machine Learning techniques have bolstered image forgery detection, primarily focusing on noise-level manipulation detection.

In this context, this project introduces an enhanced scheme known as Image Immunizer for image tampering resistance and lossless auto – recovery using Vaccinator and INN a Deep Leaning Approach. Multitask learning is used to train the network, encompassing four key modules apply vaccine to the uploaded image, ensuring consistency between the immunized and original images, classifying tampered pixels, and encouraging image self-recovery to closely resemble the original image.

In the backward pass with Run-Length Encoding, facilitating the recovery of the original, lossless image and its edge map, ensuring image integrity and authenticity. This proposed technique achieves promising results in real-world tests where experiments show accurate tamper localization as well as high-fidelity content recovery

1. 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.

Facebook remains the largest and most popular social network, with 2 billion people using the platform daily, as of Feb 1, 2023.1 Other popular platforms in the U.S. are Instagram, Twitter, WhatsApp, TikTok, and Pinterest. With the broad spectrum of websites, apps and services that exist online, there is no single exact definition of a social network. Generally, though, social networks have a few common attributes that set them apart.

A social network will focus on user-generated content. Users primarily view and interact with content made by other users. They are encouraged to post text, status updates or pictures for viewing by others. Social networks allow the user or organization to create a profile. The profile contains information about the person and a centralized page with the content posted by them.

Purpose of Social networking

Social networking fulfils the following four main objectives:

Sharing:

Friends or family members who are geographically dispersed can connect remotely and share information, updates, photos and videos. Social networking also enables individuals to meet other people with similar interests or to expand their current social networks.

Learning:

Social networks serve as great learning platforms. Consumers can instantly receive breaking news, get updates regarding friends and family, or learn about what's happening in their community.

Interacting:

Social networking enhances user interactions by breaking the barriers of time and distance. With cloud-based video communication technologies such as WhatsApp or Instagram Live, people can talk face to face with anyone in the world.

Marketing:

Companies may tap into social networking services to enhance brand awareness with the platform's users, improve customer retention and conversion rates, and promote brand and voice identity.

2. LITERATURE REVIEW

In[1]Enhanced Tamper Detection Algorithm using YOLOv5s with CBAM Attention and EIOU Loss,Author: Zhen Liu , Year: 2023.

Problem:

Traditional tamper detection models often struggle with unknown tampering modes, resulting in suboptimal performance. Specifically, the extraction of features from tampered regions is challenging when relying on hand-defined features, especially in complex scenarios.

[2] Content Authentication and Tampered Localization Using Ring Partition and CSLBP-Based Image Hashing Author: Abdul Shaik ; Ram Karsh Year: 2023 Problem The problem addressed in this paper is content authentication and tampered localization in digital images.

The goal is to develop a robust image hashing method that can resist geometric operations, including rotation, and effectively detect and localize small tampering areas.

3. METHODOLOGY

EXISTING SYSTEM

Digital Forensics Techniques

Digital forensics involves the examination of digital evidence to identify and analyse patterns of forgery. This may include analysing metadata, compression artefacts, and other forensic traces within the image.

Signature-Based Approaches

Signature-based methods use known patterns or signatures of forgery to identify manipulated images. These signatures may include noise patterns, repeated patterns, or specific features associated with common tampering techniques.

Watermarking

Watermarking involves embedding invisible or visible marks within an image to identify its origin or ownership. Watermarks can help in tracking and verifying the authenticity of images.

Image Hashing

Image hashing involves generating a unique hash or fingerprint for an image. Any alterations to the image, even minor ones, result in a significant change in the hash value, allowing for the detection of forgery.

4. DISADVANTAGES

1. Traditional methods may struggle with subtle manipulations, impacting detection precision.
2. Face challenges in detecting sophisticated deep fake content.
3. Computational complexity, hindering real-time implementation.
4. Vulnerability to sophisticated steganography methods.
5. Occurrence of false positives/negatives affecting detection accuracy.
6. Challenges in generalizing across diverse image types.
7. Absence of automatic or self-recovery mechanisms, requiring manual intervention for content restoration.

4.1 PROPOSED SYSTEM

The Image Immunizer Middleware for Online Social Networks (OSN) using Invertible Neural Network (INN) is designed to enhance the security and integrity of images shared on social media platforms. The proposed system comprises several key modules and functionalities to achieve objective.

Social Networking Web App

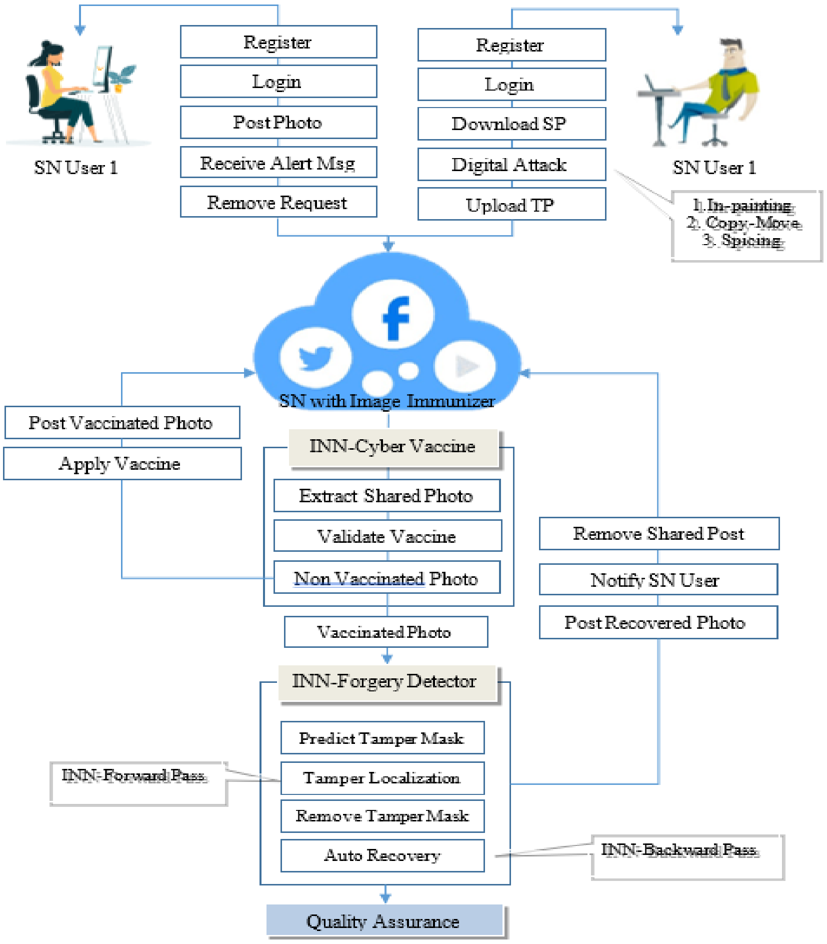
The social networking web app is meticulously crafted using Python, Flask, MySQL, Bootstrap, and Wampserver 2i to deliver a secure, responsive, and feature-rich user experience.

The User Authentication module guarantees secure access, employing features such as user registration, login, password hashing, and two-factor authentication.

The User Profile module fosters personalization, allowing users to create and customize profiles with responsive design elements.

The heart of the platform lies in the Media Sharing module, where users can seamlessly upload and share images, creating a dynamic and visually appealing environment. Connection Management facilitates user interactions, incorporating friend requests, group creation, and an effective notification system.

5. SYSTEM ARCHITECTURE



6. 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.

Through process involving the Cyber Vaccinator Module, the system adeptly pre-processes, vaccinates, and post-processes images, introducing imperceptible perturbations to fortify them against potential tampering. The Vaccine Validator ensures a vigilant distinction between vaccinated and unvaccinated media, enhancing the overall security posture.

The Forward Pass, employing INN, and the subsequent Backward Pass for image self-recovery collectively contribute to the identification and restoration of tampered areas. This dynamic approach ensures that the recovered image closely aligns with the original, reinforcing the reliability of shared media.

Adversarial simulation during training further strengthens the system, exposing it to a spectrum of potential threats, including both malicious and benign attacks. This proactive strategy equips the network to discern and counteract diverse forms of manipulation, enhancing its resilience.

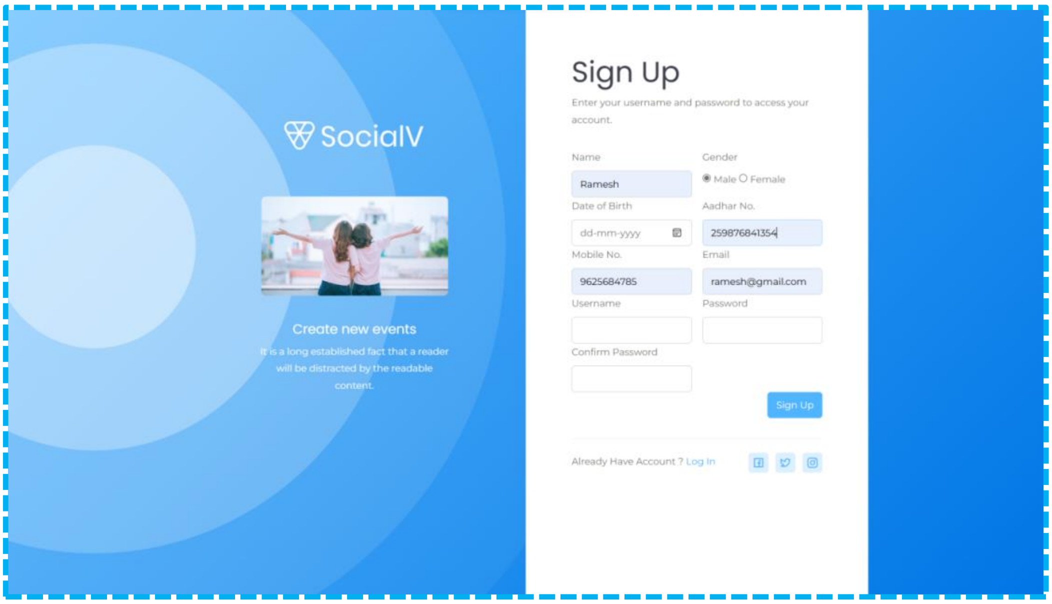
The middleware's seamless integration with existing OSN architectures not only ensures compatibility but also facilitates widespread adoption across popular social media platforms.

7. FUTURE WORK

The Future enhancements for the Image Immunizer Middleware for Online Social Networks using Invertible Neural Network (INN) aim to strengthen its capabilities and adapt to evolving technology. Integrating blockchain technology can enhance transparency in image transactions, ensuring a tamper-evident record.

The middleware's expansion to multimodal content analysis, including videos and audio, provides a more comprehensive defence against digital manipulation within OSN. These advancements reflect a commitment to robust security and holistic content integrity.

8. SCREEN SHOT



SocialV
Create new events
It is a long established fact that a reader will be distracted by the readable content.

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:

Sign Up
Already Have Account ? Log In

END USER INTERFACE

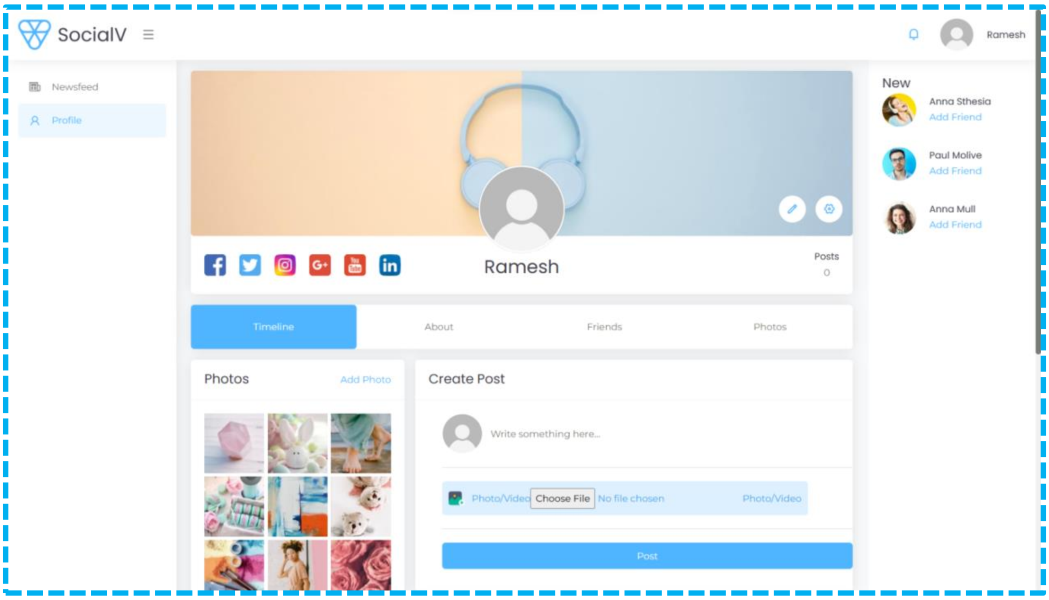
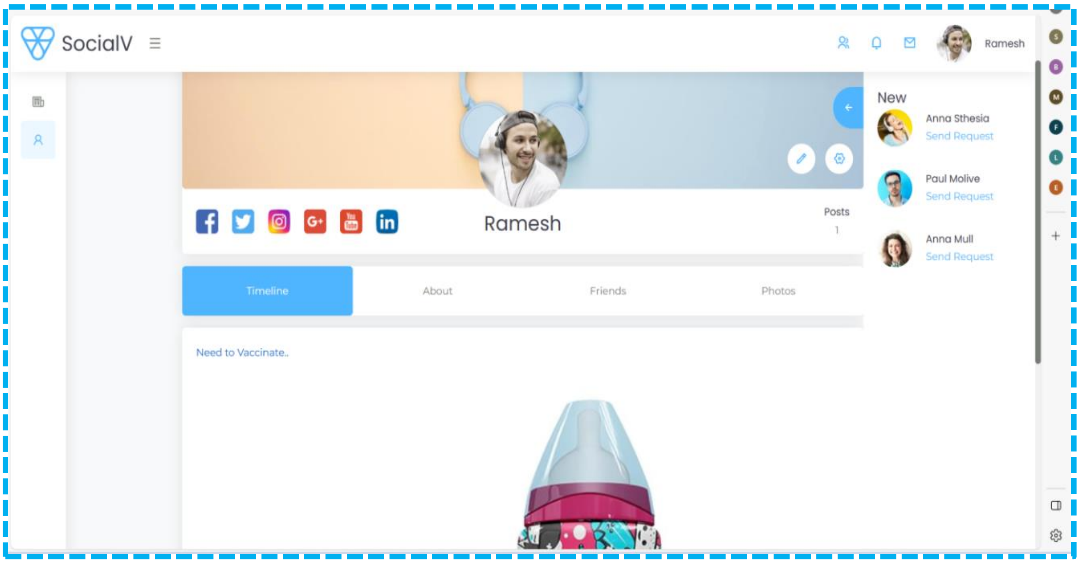
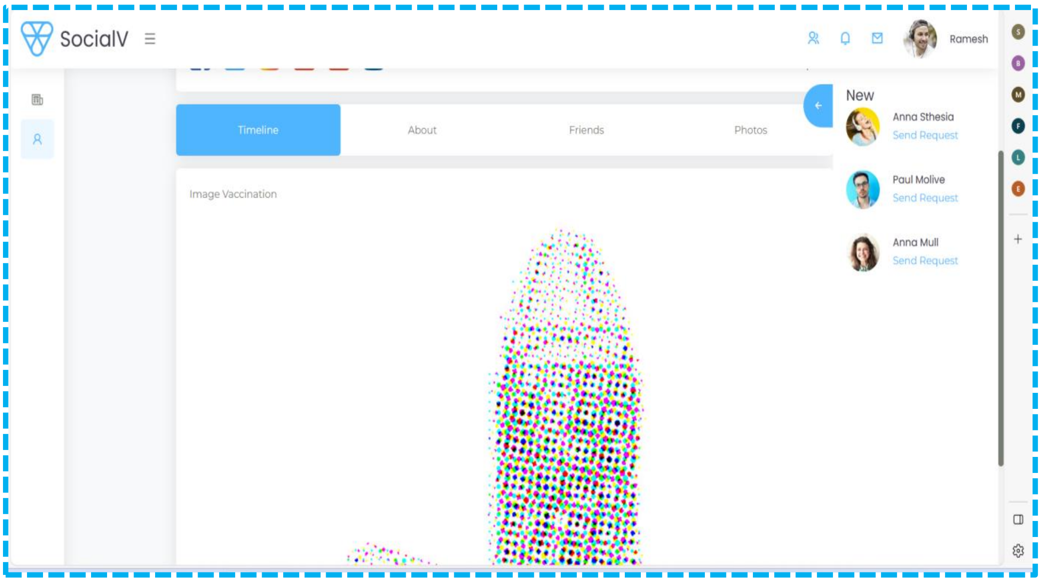


IMAGE IMMUNIZER MIDDLEWARE

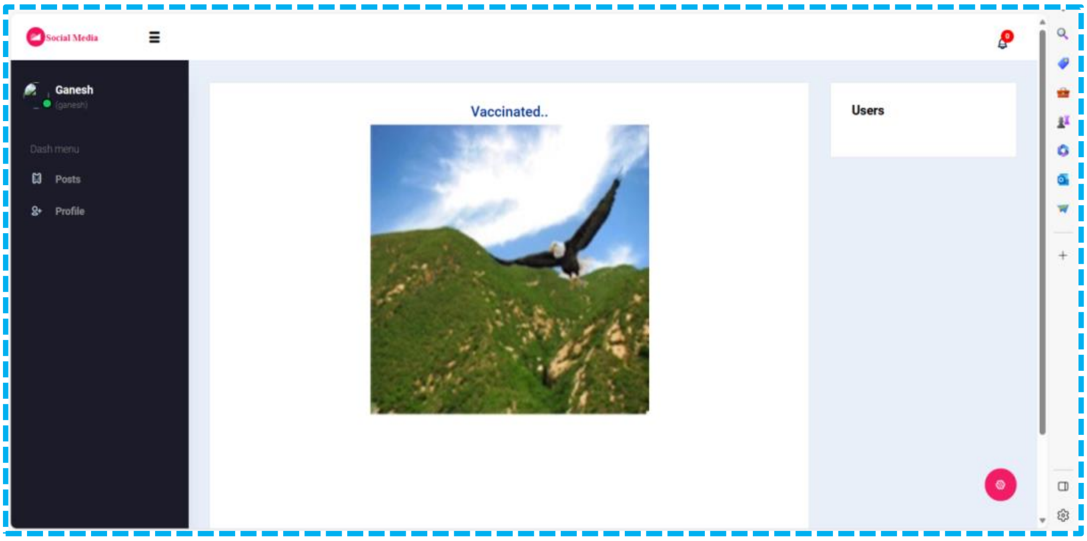


Need to Vaccinate..

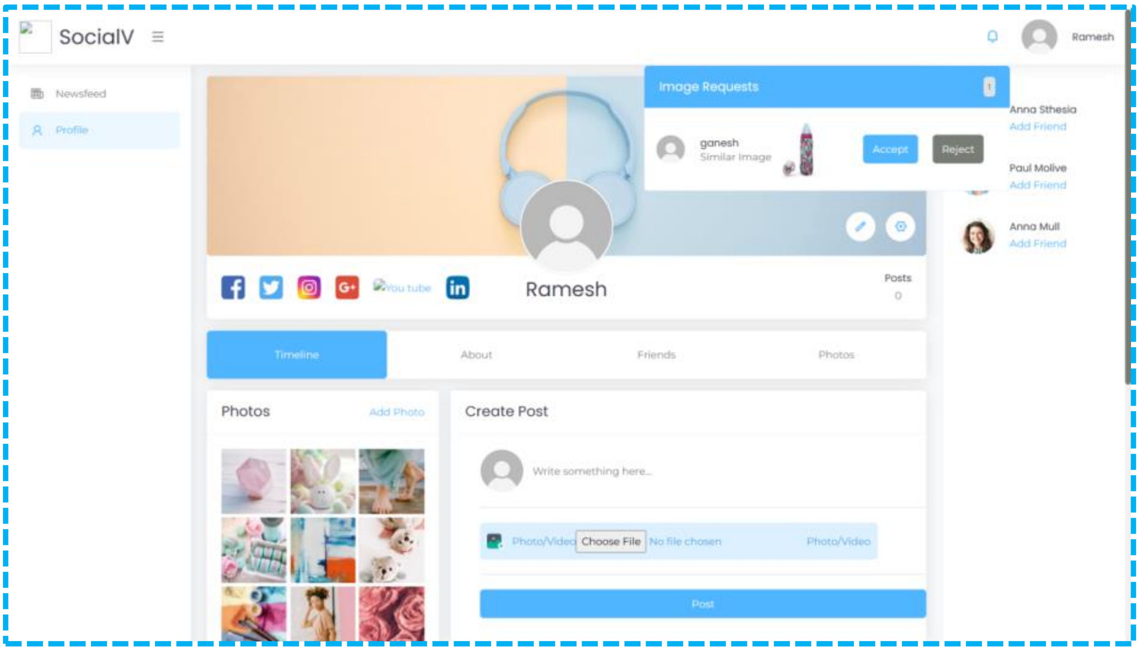
CYBER VACCINATOR



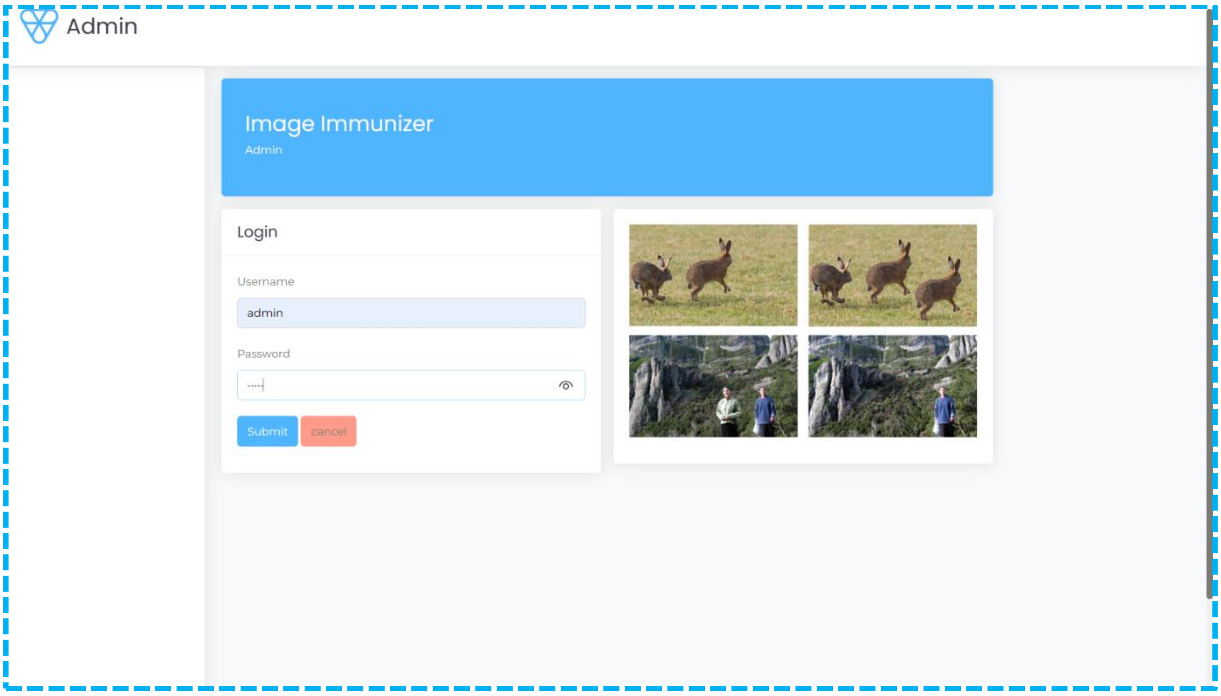
VACCINE VALIDATOR



NOTIFICATION



IMMUNIZER LOGIN



9. REFERENCES

[1] Chen .B, Tan .W, Coatrieux.Y, Zheng.Y and ShiY.Q, (2021)"A serial image copy-move forgery localization scheme with source/target distinguishment", IEEE Trans. Multimedia, vol. 23, pp. 3506-3517.

[2] Dong. C, Chen. X, Hu .R, Cao. J and Li. X,(2023) "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.

[3] Guan et al. H, (2019)"MFC datasets: Large-scale benchmark datasets for media forensic challenge evaluation", Proc. IEEE Winter Appl. Comput. Vis. Workshops (WACVW), pp. 63-72.

[4] Li .F, Pei .Z, Zhang .X and Qin .C,(2022) "Image manipulation localization using multi-scale feature fusion and adaptive edge supervision", IEEE Trans. Multimedia, pp. 1-15.

[5] Liang .X, Tang .Z, Huang .Z, Zhang .X and Zhang .S,(2023) "Efficient hashing method using 2D–2D PCA for image copy detection", IEEE Trans. Knowl. Data Eng., vol. 35, no. 4, pp. 3765-3778.

[6] Lin et al .X,(2023) "Image manipulation detection by multiple tampering traces and edge artifact enhancement", Pattern Recognit., vol. 133.

[7] Wu .H, Zhou .J, Tian .J and Liu .J, (2022)"Robust image forgery detection over online social network shared images", Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR), pp. 13430-13439.

[8] Wang et al .J,(2022) "ObjectFormer for image manipulation detection and localization", Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit., pp. 2354-2363.

[9] Xu .K, Sun Tand Jiang.X,(2020) "Video anomaly detection and localization based on an adaptive intra-frame classification network", IEEE Trans. Multimedia, vol. 22, pp. 394-406.

[10] [10] Zhang .Z,Qian .Y, Zhao .Y, Zhu .L and Wang .L,(2022) "Noise and edge based dual branch image manipulation detection", arXiv:2207.00724.

[11] Zhuang . P, Li .H, Tan.S, Li .B and Huang.B,(2021) "Image Tampering Localization Using a Dense Fully Convolutional Network", IEEE Trans. Inf. Forensics Secur, vol. 16, pp. 2986-2999.