IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 7, May 2024

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

Mohanapriya. E[1] and Dr. Krithika. D. R.[2]
PG Student, Department of Computer Applications[1]
Assistant Professor, Department of Computer Applications[2]
Vels Institute of Science Technology and Advanced Studies, Pallavaram, Chennai, India
22304224@vistas.ac.in and krithikabanu@gmail.com

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. Once the images are manipulated, it is hard for current techniques to reproduce the original contents. 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. Furthermore, these techniques are often less effective on compressed or low-resolution images and lack self-recovery capabilities, making it challenging to reproduce original content once images have been manipulated.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. 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. During the forward pass, both the original image and its corresponding edge map undergo transformation, resulting in the creation of an immunized version.Upon receiving an attacked image, a localizer identifies tampered areas by predicting a tamper mask. In the backward pass with Run-Length Encoding, hidden perturbations are transformed into information, 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*.

Keywords: OSN, Forward Pass, Run length encoding, Tamper, Localization.

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.

One problem with photo sharing privacy and security issues on social networking websites is the potential for unauthorized access to user's personal information and images. This can happen in a variety of ways, such as through hacking or data breaches, or through the misuse of data by third-party apps or advertisers. Digital image attacks encompass a range of techniques aimed at manipulating visual content, posing substantial threats to the authenticity and trustworthiness of images shared on social networking websites. Copy-move attacks involve duplicating and relocating specific portions within the same image, creating deceptive duplicates that appear unique. Splicing, another prevalent technique, combines elements from different images to fabricate composite visuals, often with the intent of inserting objects or people into misleading contexts. In-painting attacks focus on concealing or removing specific regions within an image, seamlessly filling the gaps to make alterations less conspicuous. The Image Immunizer Middleware for

DOI: 10.48175/IJARSCT-18606

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

The paper discussed about the enhanced fused tampering traces using the proposed edge artifacts enhancement modules and edge supervision strategy to discover subtle edge artifacts hidden in images. Thus,EMT-Net can prevent the risks of losing slight visual clues against well-designed post-processing methods. The proposed method can detect manipulated regions and outperform state-of-the-art approaches under comprehensive quantitative metrics and visual qualities [1]. The paper proposed about to fight against the OSN-shared forgeries, a robust training scheme is proposed. Firstly, we design a baseline detector, then analysis the noise as, predictable noise and unseen noise. The former simulates the noise introduced by the disclosed (known) operations of OSNs, while the latter is designed to not only complete the previous one, but also take into account the defects of the detector itself. We further improve the robustness of the image forgery detector[2]. The paper addresses about the existing work usually trains a detection model by fusing the features from diverse data streams. High feature redundancy may cause a large number of false detections for tampered region. To address this, first deep convolutional neural networks are utilized to extract multi-scale feature sets from the RGB streams. We then design a semantic refined bi-directional feature integration module to fully fuse multi-scale adjacent features and significantly enhance feature representation. Finally, a deep semantic residual decoder is sequentially re-constructed by spreading deep semantic information into each decoding stage [3].In this paper, we propose Object Former to detect and localize image manipulations. To capture subtle manipulation traces that are no longer visible in the RGB domain, we extract high-frequency features of the images and combine them with RGB features as multimodal patch embeddings. Additionally, we use a set of learnable object prototypes as mid-level representations to model the object-level consistencies among different regions, which are further used to refine patch embeddings to capture the patch-level consistencies. We conduct extensive experiments on various datasets and the results verify the effectiveness of the proposed method, outperforming state-of-the-art tampering detection and localization methods [4]. This paper we address both aspects by multi-view feature learning and multi-scale supervision. By exploiting noise distribution and boundary artifact surrounding tampered regions, the former aims to learn semantic-agnostic and thus more generalizable features. The latter allows us to learn from authentic images which are nontrivial to be taken into account by current semantic segmentation network-based methods. Our thoughts are realized by a new network which we term MVSS-Net. Extensive experiments on five benchmark sets justify the viability of MVSS-Net for both pixel-level and image-level manipulation detection [5].In this paper to solve the problem of the false matching and low robustness in detecting copy-move forgeries. we first, establish a Gaussian scale space; second, extract the orientated FAST key points and the ORB features in each scale space; thirdly, revert the coordinates of the orientated FAST key points to the original image and match the ORB features between every two different key points using the hamming distance; finally, remove the false matched key points using the RANSAC algorithm and then detect the resulting copy-move regions. This result is effective for geometric transformation, and exhibits high robustness even when an image is distorted by Gaussian blur, Gaussian white noise and JPEG recompression; the new algorithm even has great detection on the type of hiding object forgery [6].

III. METHODOLOGY

In this section, we provide a detailed discussion about the proposed approach to vaccinate the image and auto recovery of morphed image. 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 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. The mid-processing step generates a raw output by combining the image and mask, while the post-processing step replaces the object region in the raw output with that of the original image. Imperceptible perturbations are introduced to the non-object region, ensuring visual consistency while embedding crucial information.

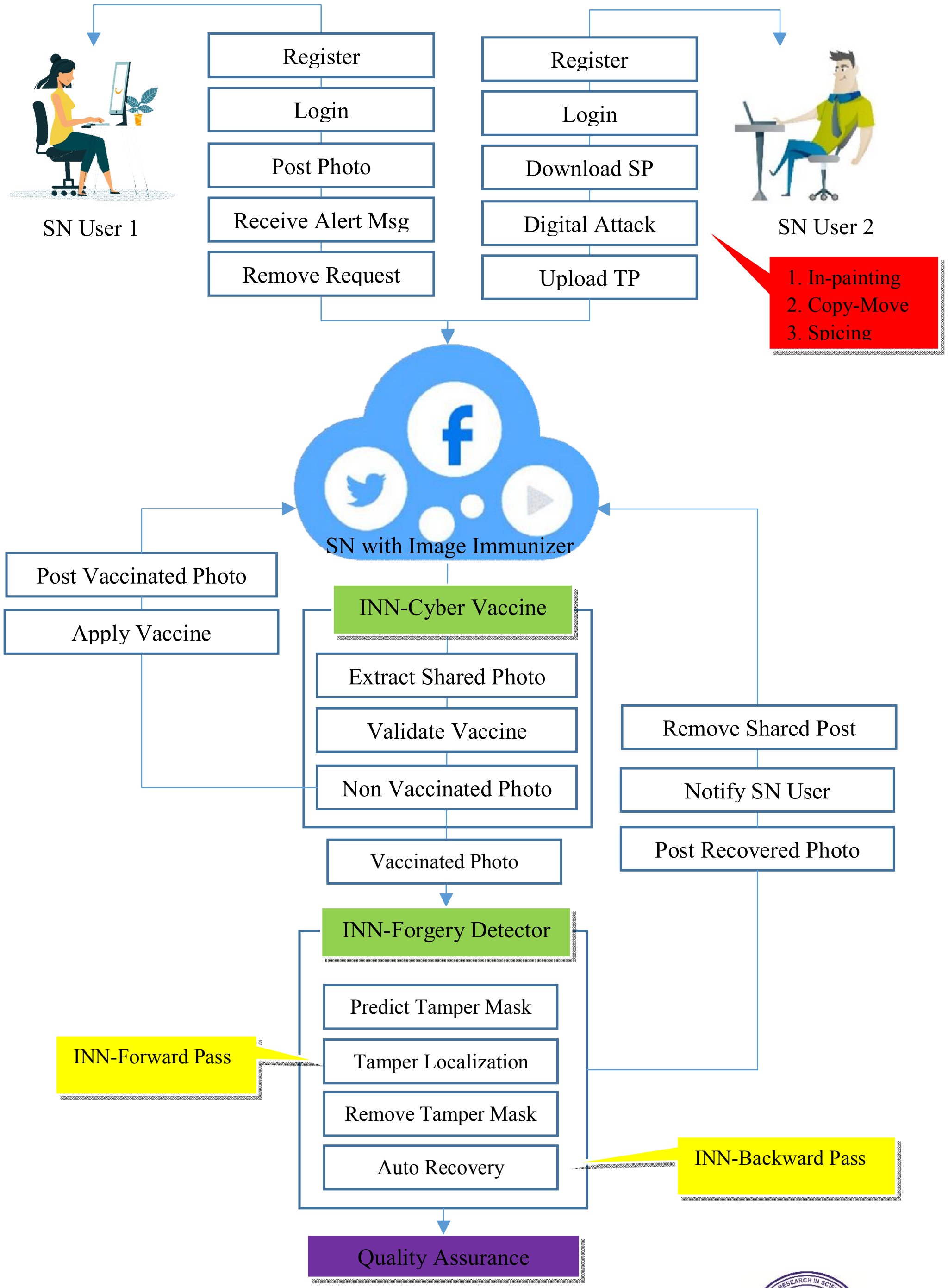


Fig. Methodology

Vaccine Validator

The system includes a Vaccine Validator module specific to OSN. It distinguishes between vaccinated (secured) and unvaccinated (potentially tampered) media shared on the platform. This component ensures the validation of image integrity, preventing the dissemination of potentially manipulated content. An adversary is integrated to simulate potential threats, including deepfake attempts within the social network context.

Forward Pass

Tamper Detection and Localization:

The forward pass involves transforming the original image and its associated metadata into an immunized version using INN. In case of an attacked image, a localizer is employed to determine tampered areas by predicting the tamper mask and type of attack. This step is crucial for identifying and localizing potential manipulations within the social network environment.

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.

Performance Metrics and OSN-Specific Metrics:

The proposed system incorporates performance metrics such as Peak Signal-to-Noise Ratio (PSNR) for image quality assessment. Additionally, OSN-specific metrics, such as context preservation and social relevance, are considered to evaluate the effectiveness of the immunization and recovery processes within the social network environment.

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.

IV. EXPERIMENTAL RESULTS

Here we auto recover a morphed image, for the safety of the user. In this proposed methodology first if a person downloads an image of any person through their social media post and do some editing and morph their photos and try to post in social media the proposed stops it and auto recovers the image. If the original user posts an image, it vaccinates the image and if some other tries to morph the vaccinated image and post it the image undergo tamper localization. It undergoes forward pass and run length algorithm. So, the image is auto recovered.

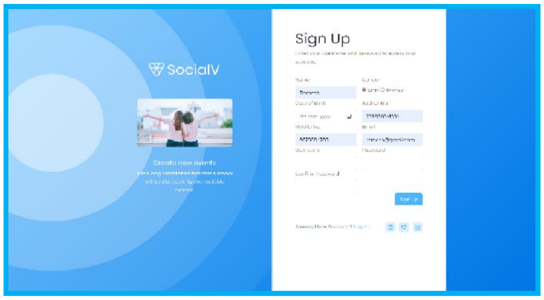


Fig.1 Signup

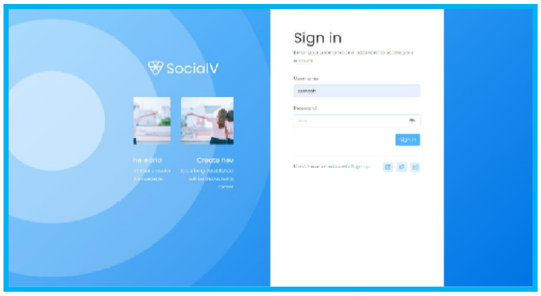
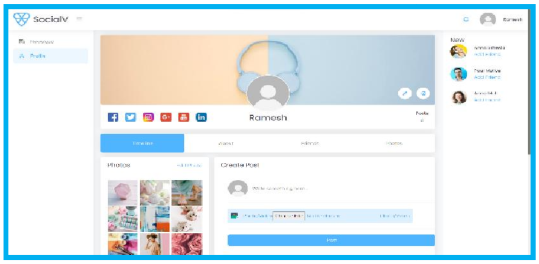


Fig.2signin

Fig.1 &2 : USER1 SIGN UP/SIGN IN:

DOI: 10.48175/IJARSCT-18606

Description: In this fig1&2 we need to enter the user details to sign in/up.



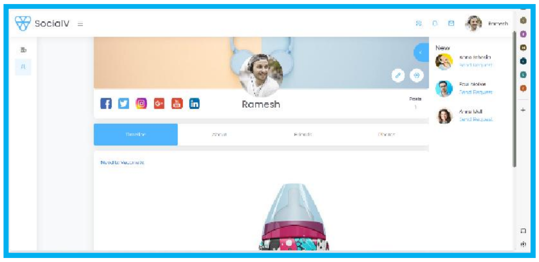


Fig.3User Shares Image Fig.4 OSN

Fig.3 and 4: User Shares Image on OSN

Description: A user shares an image on an Online Social Network (OSN) platform.

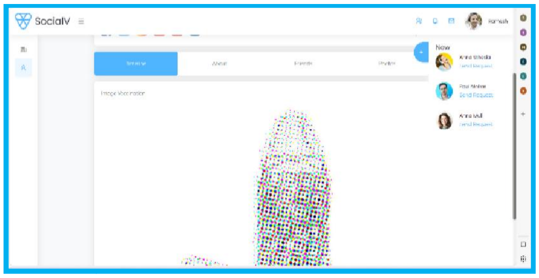


Fig.5 Cyber Vaccinator

Fig.5: Cyber Vaccinator Module:

Description: The image goes through the Cyber Vaccinator Module: Pre-processing, Mid-processing, post-processing.

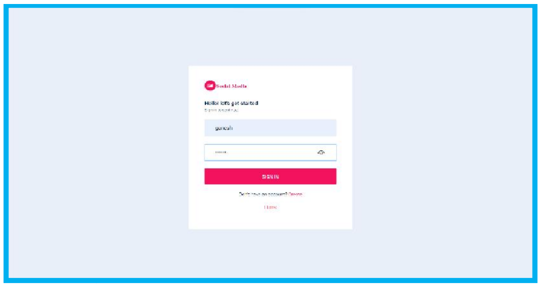


Fig.6 User Login

Fig.6: User 2 logins

Description: user 2 logins and tries to do some malicious work

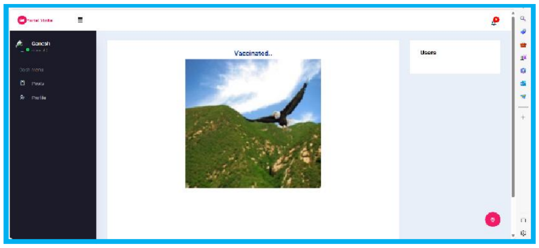


Fig.7 Vaccine Validator

Fig.7: Vaccine Validator

Description: Determines if the image is vaccinated (secured) or unvaccinated (potentially tampered).

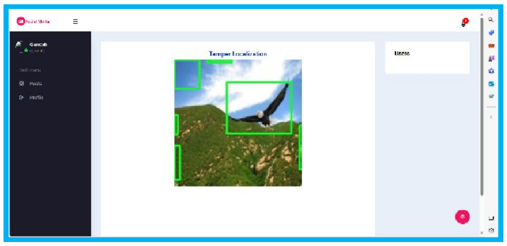


Fig.8 Tamper1

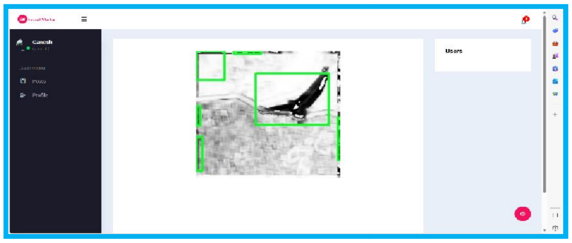


Fig.9Tamper2

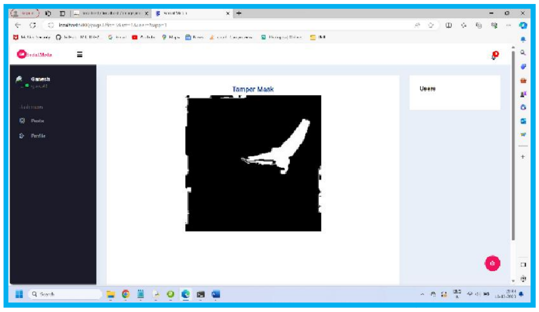


Fig.10Tamper3

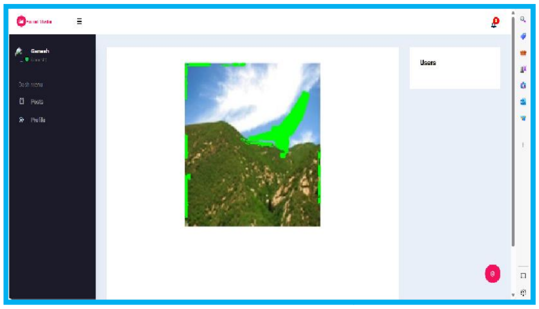


Fig.11Tamper3

Fig.8,9,10,11: Forward Pass - Tamper Detection and Localization.

Description: A localizer is employed to determine tampered areas by predicting the tamper mask and type of attack.

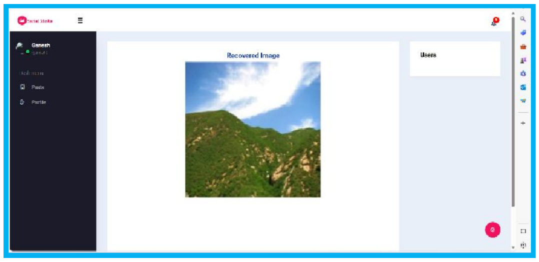


Fig.12 Tampered areas

Fig.12: Backward Pass - Image Self-Recovery

Description: Recovers the original image and encourages image self-recovery.

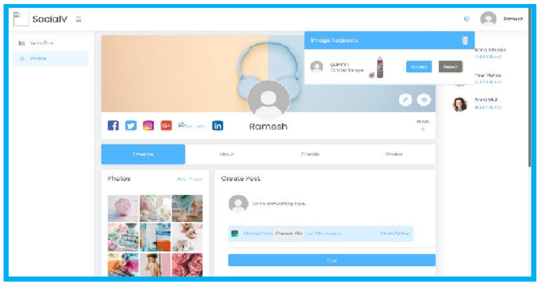


Fig.13Backward Pass

Fig 13: Notification to User:

Description: If vaccinated image being shared, the system triggers a notification to the user 1, ensuring awareness of the shared image's status.

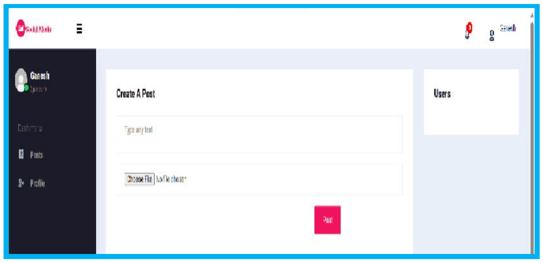


Fig.14 Notification to User

Fig.14: User 1 decline

Description: If user 1 decline it is not posted in user 2 page

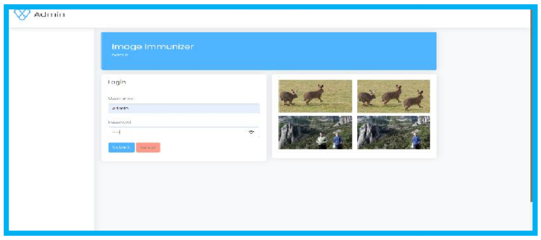


Fig.15 Admin

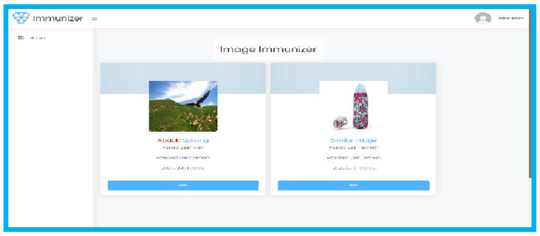


Fig.16 image

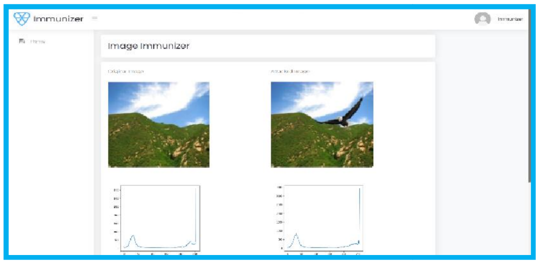


Fig.17 image1

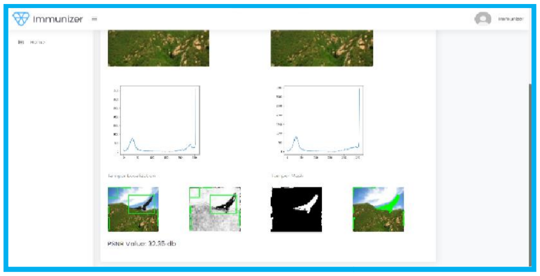


Fig.18 image2

Fig.15,16,17,18: Performance Metrics and OSN-Specific Metrics:

Description: Incorporates performance metrics such as Peak Signal-to-Noise Ratio (PSNR) for image quality assessment. It gives information on the attacked user, posted user and the type of attack.

V. 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 defense, 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. Additionally, the system's ability to notify users about the status of shared images and its capability to restore tampered images contribute significantly to fostering a secure and trustworthy social media landscape. This project represents a state-of-the-art

DOI: 10.48175/IJARSCT-18606

solution, combining advanced technologies and thoughtful design to safeguard the digital integrity of shared images in the dynamic realm of online social networks.

REFERENCES

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

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

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

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

[5]. X. R. Chen, C. B. Dong, J. Q. Ji, J. Cao and X. R. Li, "Image manipulation detection by multi-view multi-scale supervision", *Proc. IEEE Int. Conf. Comput. Vis.*, pp. 14165-14173, 2021.

[6]. Y. Zhu, X. Shen and H. Chen, "Copy-move forgery detection based on scaled ORB", *Multimedia Tools Appl.*, vol. 75, pp. 3221-3233, 2016.

DOI: 10.48175/IJARSCT-18606