e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 7, July 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.521

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707202 |

Image Immunizer an Image Tamper Resilient for Image Lossless Auto-Recovery

Mr.D.Prabhakaran., MCA., P.Mugilan., MCA

Assistant Professor, Master of Computer Applications, Gnanamani College of Technology, Namakkal,

Tamil Nadu, India

PG Student, Master of Computer Applications, Gnanamani College of Technology, Namakkal, Tamil Nadu, 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. 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. Upon receiving an attacked image, a localizer identifies tampered areas by predicting a tamper mask.

KEYWORDS: ImageVaccinator,Image tampering, Deep Leaning, tamper localization, Image Immunizer

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. 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.. A social network focuses on the connections and relationships between individuals. Social media is more focused on an individual sharing with a large audience. In this case, media is used in the same sense as in mass media. Most social networks can also be used as social media sites.

II.RELATED WORKS

- 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 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.Image processing techniques, including error level analysis (ELA) and noise analysis, are used to identify inconsistencies in pixel values or compression artefact that may suggest tampering.Steganalysis techniques focus on detecting hidden information within images. This includes identifying alterations made through steganography, where additional information is concealed within the image.Description: Some systems use block chain technology to timestamp and authenticate images. This ensures that the image's origin and content remain unchanged over time, providing a form of tamper-proofing. Traditional methods may struggle with subtle manipulations, impacting detection precision.
- Face challenges in detecting sophisticated deepfake content.
- Computational complexity, hindering real-time implementation.
- Vulnerability to sophisticated steganography methods.
- Occurrence of false positives/negatives affecting detection accuracy.
- Challenges in generalizing across diverse image types.
- Absence of automatic or self-recovery mechanisms, requiring manual intervention for content restoration.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707202 |

III.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 this objective.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.

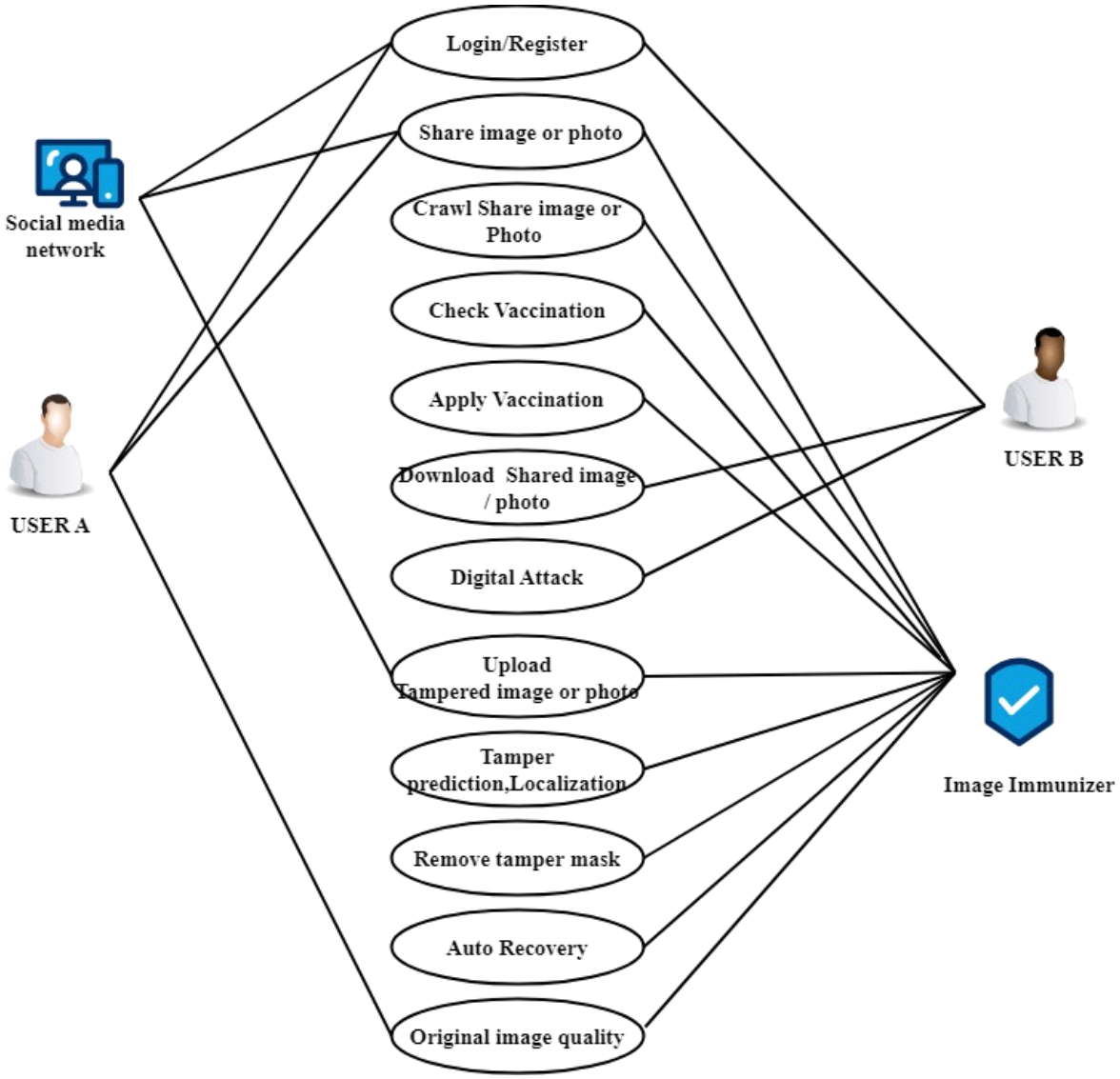

Figure- 1 System Architecture

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.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707202 |

IV. RESULT & DISCUSSION

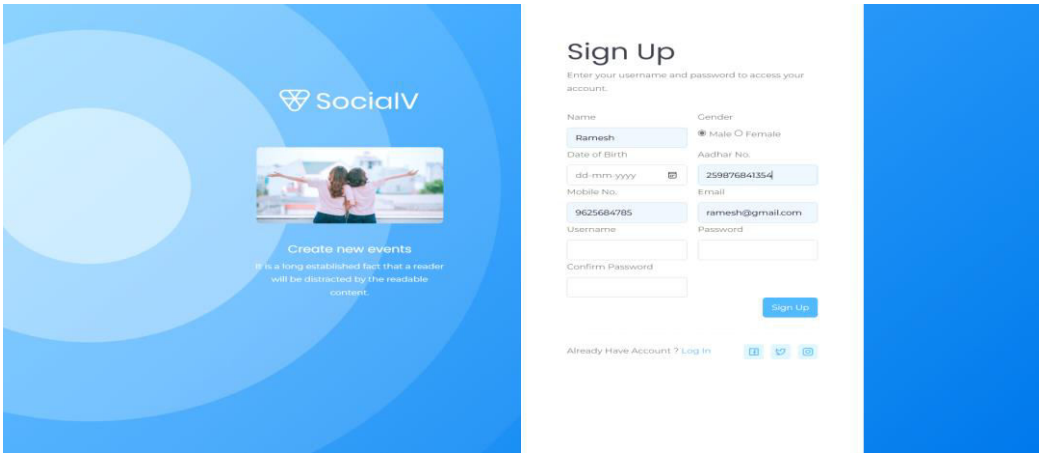

Figure- 2 login page

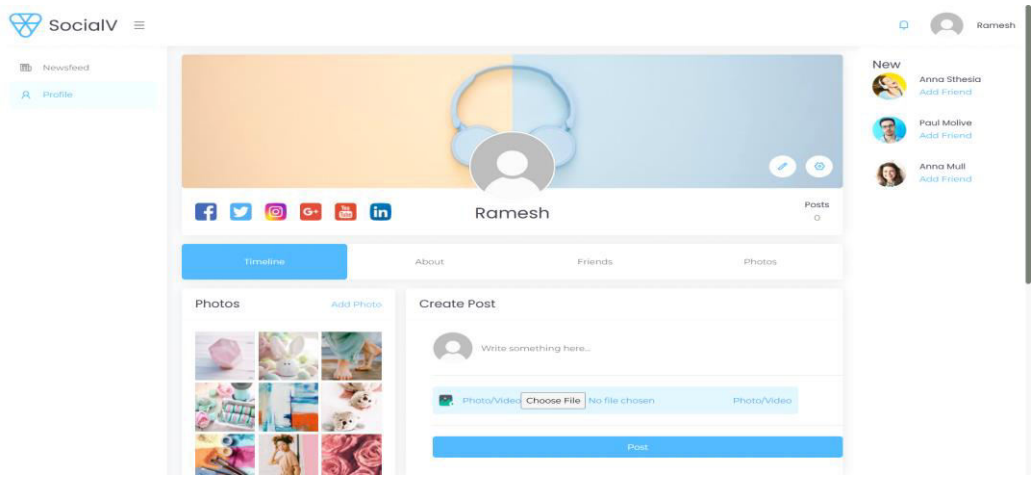

Figure 3:profile

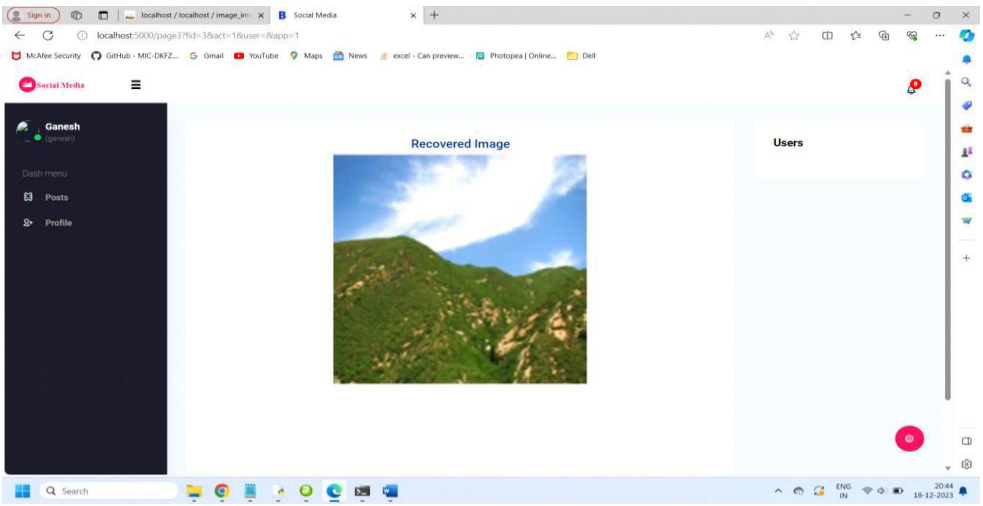

Figure 4: recoverd image

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707202 |

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 defence, securing the authenticity and integrity of images shared on social networking platforms. Through process involving the Cyber Vaccinator Module, the system adeptly prepossesses, 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.

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.
7. 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.
8. 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.
9. J. Wang et al., "ObjectFormer for image manipulation detection and localization", Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit., pp. 2354-2363, 2022.
10. 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.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com