Recognizing, Analysing, and recovering digitally Altered Image and Replacing with Original Image

Mrs.S.Hemaswathi,M.E.,(Ph.D.,)[1], Vasanth K[2], Manoj Kumar S[3], Senthil Murugan S[4]
[1, 2, 3, 4]Dept of Computer Science and Engineering
[1, 2, 3, 4]Kamaraj College of Engineering and Technology, Virudhunagar.

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 vaccine, research on image tamper localization has garnered extensive attention. Image Processing and Deep 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 Vaccinator 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. 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.*

Keywords- Image Vaccine ,Tamper Localization, Lossless Auto-Recovery, Invertible Neural Network(INN),Tamper Mask .

I. INTRODUCTION

The pervasive nature of photo sharing on social networking platforms has ushered in a myriad of concerns regarding user privacy and data security. Paramount among these issues is the persistent risk of unauthorized access to user's personal information and images. The vulnerabilities leading to such breaches may arise from malicious activities, including hacking incidents or unauthorized data exploitation by third-party applications and advertisers.

Furthermore, the absence of robust controls over shared content raises apprehensions, as even ostensibly private accounts may inadvertently expose photos through the actions of trusted connections or inadequacies in platform privacy configurations. The omnipresence of online harassment and cyberbullying compounds these challenges, capitalizing on the seamless sharing of personal information and images. The far-reaching consequences, spanning mental health implications to the extreme spectre of physical harm, underscore the imperative for comprehensive solutions.

The intricacies of these privacy and security challenges extend beyond unauthorized access, encompassing nuanced issues such as user awareness of privacy settings and the potential commercial exploitation of user data by social networking platforms. Additionally, the emergence of sophisticated digital image attacks, including Copy-Move, Splicing, and In-Painting techniques, poses threats to the integrity and credibility of shared visual content, thereby engendering misinformation and privacy breaches & it's tamper mask are deceted in modified image. 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.

II. IDENTIFY, RESEARCH AND COLLECT IDEA

In recent times, there has been a growing interest in the topic of digital image manipulation, leading to an increase in research aimed at detecting and preventing image tampering. Scholars have delved into various methods, merging conventional techniques with state-of-the-art deep learning approaches. Our project, entitled "Recognizing, Analysing, and Recovering Digitally Altered Images: Enhancing Image Security in Online Social Networks," is motivated by these advancements and seeks to formulate a

comprehensive solution to protect images shared on social platforms from manipulation.

Drawing inspiration from the studies conducted by Marra et al. [3] and Afchar et al. [4], which showcased the efficacy of traditional image processing techniques in identifying manipulated images, we integrate similar methods into our framework. By utilizing these techniques, we bolster our system's capability to detect subtle inconsistencies and artifacts in digital images, which are essential for recognizing potential manipulations.

Additionally, we glean insights from the progress made in deep learning approaches, such as Capsule-forensics [6] and LSTM-based architectures [7], to construct a robust detection system. By comprehending the hierarchical structures within images and employing recurrent neural networks, our framework becomes proficient in distinguishing between genuine and manipulated content, thereby enhancing its overall performance in detecting various forms of image manipulations.

Inspired by the research conducted by Tramèr et al. [11] on ensemble adversarial training, we integrate similar strategies to fortify the resilience of our framework against adversarial attacks. This ensures that our system remains effective even when confronted with sophisticated manipulation attempts.

Furthermore, we explore innovative techniques to enhance image authenticity and integrity, drawing inspiration from recent advancements in deep learning for image manipulation. By leveraging these techniques, our framework can produce lifelike facial animations and expressions, thereby mitigating the risk of image tampering.

To enhance the ability of our framework to generalize across facial analysis tasks, we incorporate insights from representation learning approaches, specifically rotation-based augmentation [19]. This integration enables our system to acquire more resilient representations of facial images, thereby improving its overall performance in detecting image manipulations.

In summary, the research paper titled "Recognizing, Analysing, and Recovering Digitally Altered Images" employs a combination of image processing techniques and advanced deep learning approaches. The objective is to develop a comprehensive solution that enhances image security in online social networks. By leveraging insights from previous studies, our aim is to establish a robust and effective defence mechanism against image manipulation, thereby ensuring the integrity of images shared on social media platforms.

III. PROPOSED SOLUTIONS

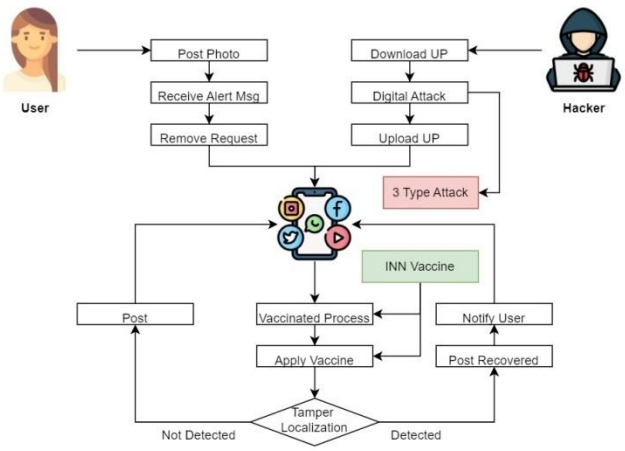

Figure 1 System Model

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.

- 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.

- 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. Image self-recovery is encouraged to ensure that the recovered image closely resembles the original, maintaining visual and contextual consistency within the OSN context.

- 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. RESULT

Figure 2 Result

V. CONCLUSION

In conclusion, the Image Immunizer project stands as a sophisticated solution against digital image forgery in social networks. Leveraging the power of Invertible Neural Networks and adversarial simulation, the system effectively guards the authenticity and integrity of images. The Cyber Vaccinator Module plays a pivotal role, processing images to embed subtle perturbations that shield them from tampering. The Vaccine Validator further fortifies security by discerning between secured and unsecured media. Crucially, the systems detect tampering, while the enables self-recovery of images, ensuring they retain their original quality. This dual process not only maintains the reliability of media but also the trust of users in the platform. Training with adversarial simulation arms the system against a wide array of threats, enhancing its ability to adapt and respond to different attack vectors. Seamless integration with existing Online Social Network architectures promises easy adoption, and features like user notifications and tamper restoration contribute to a safer social media space. Altogether, the Image Immunizer embodies a state-of-the-art approach, merging cutting-edge tech with user-centric design to uphold the digital integrity of images shared across social networks.

REFERENCES

[1] .S.Greengard,‘‘Willdeepfakesdodeepdamage?’’Commun. ACM,vol.63, no. 1, pp. 17–19, Dec. 2019.

[2] Y. Mirsky and W. Lee, ‘‘The creation and detection of deepfakes: A survey,’’ ACM Comput. Surv., vol. 54, no. 1, pp. 1–41, 2021.

[3] F. Marra, D. Gragnaniello, D. Cozzolino, and L. Verdoliva, ‘‘Detection of GAN-generated fake images over social networks,’’ in Proc. IEEE Conf.MultimediaInf.Process.Retr.(MIPR),Miami,FL,USA ,Apr.2018, pp. 384–389.

[4] D.Afchar,V.Nozick,J.Yamagishi,andI.Echizen,‘‘MesoNet :Acompact facial video forgery detection network,’’ in Proc. IEEE Int.Workshop Inf. Forensics Secur. (WIFS), Hong Kong, Dec. 2018, pp. 1–7.

[5] Y. Li, M.-C. Chang, and S. Lyu, ‘‘In ictu oculi: Exposing AI created fake videos by detecting eye blinking,’’ in Proc. IEEE Int. Workshop Inf. Forensics Secur. (WIFS), Hong Kong, Dec. 2018, pp. 1–7.

[6] H. H. Nguyen, J. Yamagishi, and I. Echizen, ‘‘Capsule-forensics: Using capsule networks to detect forged images and videos,’’ in Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP), Brighton, U.K., May 2019, pp. 2307–2311.

[7] J. H. Bappy, A. K. Roy-Chowdhury, J. Bunk, L. Nataraj, and B. S. Manjunath, ‘‘Exploiting spatial structure for localizing manipulated image regions,’’ in Proc. IEEE Int. Conf. Comput. Vis. (ICCV), Venice, Italy, Oct. 2017, pp. 4980–4989.

[8] P. Zhou, X. Han, V. I. Morariu, and L. S. Davis, ‘‘Learning rich features for image manipulation detection,’’ in Proc. IEEE/CVFConf. Comput. Vis. Pattern Recognit., Salt Lake City, UT, USA, Jun. 2018, pp. 1053–1061.

[9] J. H. Bappy, C. Simons, L. Nataraj, B. S. Manjunath, and A. K. Roy-Chowdhury,‘‘HybridLSTMandencoder–decoder architecture for detection of image forgeries,’’ IEEE Trans. Image Process., vol. 28, no. 7, pp. 3286–3300, Jul. 2019.

[10] H.H.Nguyen,F.Fang,J.Yamagishi,andI.Echizen,‘‘Multi-tasklearning for detecting and segmenting manipulated facial images and videos,’’ in Proc. IEEE 10th Int. Conf. Biometrics Theory, Appl. Syst. (BTAS), Tampa, FL, USA, Sep. 2019, pp. 1–8.

[11] Madry, A. Makelov, L. Schmidt, D. Tsipras, and A. Vladu, ‘‘Towards deep learning models resistant to adversarial attacks,’’ in Proc. Int. Conf. Learn. Represent. (ICLR), Vancouver, BC, Canada, 2018, pp. 1–23.

[12] F. Tramèr, A. Kurakin, N. Papernot, I. J. Goodfellow, D. Boneh, and P.D.McDaniel, ‘‘Ensemble adversarial training: Attacks and defenses,’’ in Proc. Int. Conf. Learn. Represent. (ICLR), Vancouver, BC, Canada, 2018, pp. 1–20.

[13] F.Tramèr and D.Boneh, ‘‘Adversarial training and robustness for multiple perturbations,’’ in Proc. Int. Conf. Neural Inf. Process. Syst. (NIPS), Vancouver, BC, Canada, 2019, pp. 5866–5876.

[14] J. Thies, M. Zollhöfer, M. Nießner, L. Valgaerts, M. Stamminger, and C. Theobalt,‘‘Real-time expression transfer for facial reenactment,’’ACM Trans. Graph., vol. 34, no. 6, pp. 1–14, Nov. 2015.

[15] H. Kim, P. Garrido, A. Tewari, W. Xu, J. Thies, M. Niessner, P. Pérez, C. Richardt, M. Zollhöfer, and C. Theobalt, ‘‘Deep video portraits,’’ ACM Trans. Graph., vol. 37, no. 4, pp. 1–14, Aug. 2018.

[16] J. Thies, M. Zollhöfer, M. Stamminger, C. Theobalt, and M. Nießner, ‘‘Face2Face: Real-time face capture and reenactment of RGB videos,’’ Commun. ACM, vol. 62, no. 1, pp. 96–104, 2018.

[17] D. Kononenko, Y. Ganin, D. Sungatullina, and V. Lempitsky, ‘‘Photorealistic monocular gaze redirection using machine learning,’’ IEEE Trans. Pattern Anal. Mach. Intell., vol. 40, no. 11, pp. 2696–2710, Nov. 2018.

[18] Y. Yu, G. Liu, and J.-M. Odobez, ‘‘Improving few-shot user-specific gaze adaptation via gaze redirection synthesis,’’ in Proc. IEEE/CVF Conf. Comput.Vis.PatternRecognit.(CVPR),LongBeach,CA,USA,Jun.2019, pp. 11929–11938.

[19] Y. Ganin, D. Kononenko, D. Sungatullina, and V. Lempitsky, ‘‘DeepWarp: Photorealistic image resynthesis for gaze manipulation,’’ in Proc. Eur. Conf. Comput. Vis. (ECCV), Amsterdam, The Netherlands, 2016, pp. 311–326.

[20] L. Tran, X. Yin, and X. Liu, ‘‘Representation learning by rotating your faces,’’ IEEE Trans. Pattern Anal. Mach. Intell., vol. 41, no. 12, pp. 3007–3021, Dec. 2019.