IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

IMAGE VACCINATOR AN IMAGE TAMPER RESILIENT AND LOSSESLESS AUTO-RECOVERY USING INVERTIBLE NEURAL NETWORK

[1]T.Sukanya, [2]C.Sanjaykumar, [3]G.Sudhir, [4]P.Ugabharathi

[1]Assistant Professor, [2,3,4]Student
[1]Computer Science and Engineering,
[1]Sri Ramakrishna College Of Engineering, Perambalur, 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. 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.

IndexTerms **-** Invertible Neural Networks, Online social networks (OSN), Cyber Vaccinator, Tamper Detection, Image Self-Recovery**.**

I. INTRODUCTION

INTRODUCTION

Managing 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 throughsites like Facebook, Twitter, Instagram, and Pinterest. Facebook remains the largest and most popular social network, with. are Instagram, Twitter, WhatsApp, TikTok, and Pinterest. With the broad spectrum of 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. The profile contains information about the person and a centralized page with the content posted by them. They allow the users to find other users and form webs of relationships. Often an algorithm will recommend other users and social media A social network focuses on the connections and relationships between individuals. Social media is more focused on an individual sharing with a large audience.

METHOD OF LEARNING

3.1 DIGITAL FORENSICS TECHNIQUES :

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

3.2 Signature-Based Approaches :

Authorization 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.

3.3 Block chain for Image Authentication :

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. 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.

RESEARCH METHODOLOGY

Face Social Networking Web App

Social networking web application is fully developed using Python, Flask and MySQL. Bootstrap and Wampserver 2i provide users with a secure, responsive and complete experience. This user authentication module guarantees secure access, employing features such as user registration, login, password hashing, and two-factor authentication. 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.

End User Interface

Login : Enables users to log into their accounts using valid credentials. A secure authentication process grants access to the user`s personalized space within the social network.Apply Digital Attack on Shared Image : Users can experiment with various tampering techniques, enhancing their understanding of potential threats.Share Tampered Image or Photo to Other Social Networks : This feature extends the reach of tampered content beyond the immediate social network, showcasing the potential impact of digital attacks.Receive Notifications : Notifies users of relevant activities, such as new friend requests, shared content, or interactions with their posts.

Image Immunizer Middleware

Cyber Vaccinator : 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.Vaccine Validator : Integrated into the system is the Vaccine Validator, a critical component designed to discern between vaccinated and unvaccinated media. This validator plays a pivotal role in safeguarding the authenticity of digital content.
Forward Pass with Tamper Detection and Localization : The forward pass incorporates an Invertible Neural Network to transform an original image and its edge map into an immunized version. In the face of an attacked image, a localizer comes into play, determining tampered areas by predicting the tamper mask and attack.

Backward Pass for Image Self-Recovery : In the backward pass, the hidden perturbation, transformed by the Invertible Neural Network, is converted into information. This transformative process serves the dual purpose of recovering the original image and its edge map while fostering image self-recovery. By encouraging the recovered image to closely resemble the original, this module ensures a seamless restoration process.

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. Run-Length Encoding (RLE) can be a valuable tool in achieving this, ensuring that the original image is restored.

PSNR : The Peak Signal-to-Noise Ratio (PSNR) is a metric used to quantitatively assess the quality of an image reconstruction or recovery compared to the original image.

Social Media Privacy: The Friend Loophole

While it may seem harmless to add people you don't know on social media, this can open you up to various privacy issues. For example, scammers may use fake accounts for spear-phishing campaigns. By adding a person on a platform such as Facebook, they can glean information that will make scam emails more convincing.

Another way it can compromise your security is when apps are able to access your information through a friend's account. This is what made the Cambridge Analytica scandal so shocking. Most people whose information was harvested didn't even take the quiz that was used to mine data.Rather, the Facebook quiz used a loophole to access the information of all the friends of people who took the quiz. While Facebook has tightened up privacy on the network in this regard, the various ways friends can compromise our privacy is still very much a concern.

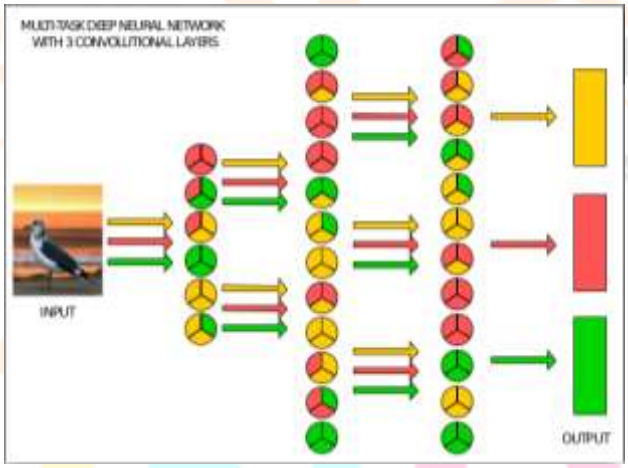
IV. DEEP LEARNING

Deep learning is a method in artificial intelligence (AI) that teaches computers to process data in a way that is inspired by the human brain. Deep learning models can recognize complex patterns in pictures, text, sounds, and other data to produce accurate insights and predictions. Deep learning models are computer files that data scientists have trained to perform tasks using an algorithm or a predefined set of steps. Businesses use deep learning models to analyse data and make predictions in various applications. Computer vision is the computer's ability to extract information and insights from images and videos. Computers can use deep learning techniques to comprehend images in the same way that humans do. Deep learning networks learn by discovering complex structures in the information you feed them. During data processing, artificial neural networks classify the data.

Deep learning algorithms are neural networks that are modelled after the human brain. For example, a human brain contains millions of interconnected neurons that work together to learn and process information. Similarly, deep learning neural networks, or artificial neural networks, are made of many layers of artificial neurons that work together inside the computer.
Artificial neurons are software modules called nodes, which use mathematical calculations to process data. Artificial neural networks are deep learning algorithms that use these nodes to solve complex problems.

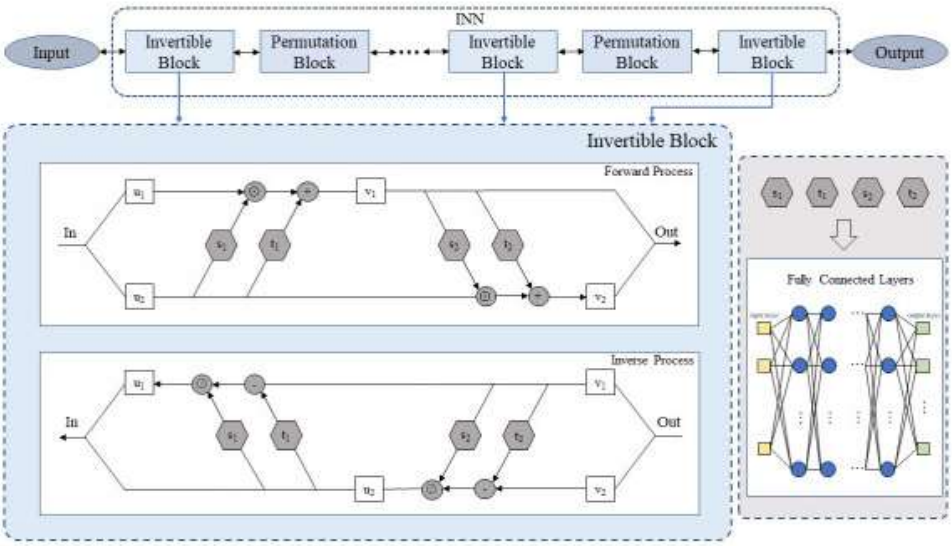
4.1 Multi Task Learning

Multi-task learning (MTL), including learning services, is emerging as a pivotal concept in the rapidly evolving landscape of artificial intelligence. Multi-task learning (MTL) involves training a model to perform multiple tasks concurrently in machine learning. In deep learning, MTL pertains to instructing a neural network to undertake several tasks, achieved by distributing certain network layers and parameters across these tasks.



4.2 Invertible Neural Network

Invertible neural network (INN) is a promising tool for inverse design optimization. While generating forward predictions from given inputs to the system response, INN enables the inverse process without much extra cost. The inverse process of INN predicts the possible input parameters for the specified system response qualitatively. For the purpose of design space exploration and reasoning for critical engineering systems, accurate predictions from the inverse process are required. Moreover, INN predictions lack effective uncertainty quantification for regression tasks, which increases the challenges of decision making. A new loss function is formulated to guide the training process with enhancement in the inverse process accuracy. INN is a bidirectional mapping network based on affine coupling blocks, considered as an excellent approach for solving inverse problems. The forward process of an INN predicts the output from the input while the inverse process derives the distribution of the input parameters. The key information of its inverse process is captured by the latent variables. INN shines not only in the field of computer vision, but also has distinctive achievements in the field of inverse design.



The forward process of the standard INN only gives the prediction result without presenting uncertainty. Moreover, its inverse process is usually acquired in a qualitative manner and not accurate enough for design purposes. To address this issue, we propose the P-INN with integrated epistemic uncertainty and aleatoric uncertainty. In this way, the outcome of the forward process carries uncertainty, while the posterior distribution of the inverse process incorporates epistemic uncertainty.

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. Run-Length Encoding (RLE) can be a valuable tool in achieving this, ensuring that the original image is restored without loss of information after tampering has been detected and addressed. Subsequent to tamper removal, the image is subjected to RLE compression. Runs of consecutive identical pixel values are encoded to represent sequences more efficiently. The integration of tamper detection, removal, and lossless recovery using RLE enhances the overall resilience of the system against malicious manipulations.

PSNR

It measures the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the quality of the signal.

PSNR Calculation

PSNR is calculated using the formula: PSNR = 10 * log10((MAX^2) / MSE), where MAX is the maximum possible pixel value (255 for an 8-bit image), and MSE is the Mean Squared Error between the original and recovered images.

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. 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 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. 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.

[2] B. Chen, W. Tan, G. Coatrieux, Y. Zheng and Y.-Q. Shi, "A serial image copy-move forgery localization scheme with source/target distinguishment & quot;, IEEE Trans. Multimedia, vol. 23, pp. 3506- 3517, 2021.

[3] 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.

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

[5] D.-Y. Huang, C.-N. Huang, W.-C. Hu and C.-H. Chou, "Robustness of copy-move forgery detection under high

JPEG compression artifacts", Multimedia Tools Appl., vol. 76, no. 1, pp. 1509-1530, 2017.

[6] X. Hu, Z. Zhang, Z. Jiang, S. Chaudhuri, Z. Yang and R. Nevatia, "SPAN: Spatial pyramid attention network for image manipulation localization", Proc. Eur. Conf. Comput. Vis. (ECCV), pp. 312-328, Aug. 2020.

[7] 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.

[8] 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.

[9] H. Li and J. Huang, "Localization of deep inpainting using high-pass fully convolutional network", Proc. IEEE/CVF Int. Conf. Comput. Vis. (ICCV), pp. 8300- 8309, Oct. 2019.

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

[11] 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.

[12] 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.

[13] A. Novozámský, B. Mahdian and S. Saic, "IMD2020: A large-scale annotated dataset tailored for detecting manipulated images", Proc. IEEE Winter Appl. Comput. Vis. Workshops (WACVW), pp. 71- 80, Mar. 2020.

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

[15] Y. Wu, W. Abd-Almageed and P. Natarajan, "BusterNet: Detecting copy-move image forgery with source/target localization", Proc. Eur. Conf. Comput. Vis., pp. 168-184, 2018.

[16] 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.

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

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

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

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