iJETRM
International Journal of Engineering Technology Research & Management

IMAGE FORTIFY: RESILIENT MULTI-TASK LEARNING FOR SECURE AND SEAMLESS IMAGE RESTORATION

Mrs. Rekha. P [1]
Assistant Professor, Sri Muthukumaran Institution of Technology, Mangadu, Chennai
Mrs. Rajashree. G [2]
PG Student, II MCA, Sri Muthukumaran Institution of Technology, Mangadu, Chennai

ABSTRACT:
Digital images shared on social networks are vulnerable to security and privacy threats, especially from tampering attacks aimed at altering their content. Traditional detection methods often struggle with compressed or low-resolution images and lack self-recovery capabilities. This project introduces an Image Protector utilizing a novel approach combining a Vaccinator and an Invertible Neural Network. It employs multi-task learning across four modules: image vaccination, consistency maintenance, tampered pixel classification, and self-recovery. During the forward pass, an immunized image and edge map are generated, while the backward pass utilizes Run-Length Encoding to restore the original image, ensuring integrity and authenticity. Real-world tests demonstrate effective tamper localization and content recovery.

Keywords:
Digital images, social networks, Security threats, Privacy threats, Tampering attacks, Traditional detection methods, Compressed images

INTRODUCTION

Social networking involves using internet-based platforms such as Facebook, Twitter, Instagram, and Pinterest to maintain connections with friends, family, colleagues, or customers. These platforms serve both social and business purposes and provide significant opportunities for marketers. Facebook, boasting 2 billion daily users, stands as the largest social network. Other popular platforms include Instagram, Twitter, WhatsApp, TikTok, and Pinterest. Social networks are characterized by user-generated content, profile creation, and the establishment of lasting connections through features like friending or following. While social networks focus on individual connections, social media emphasizes sharing content with a broader audience. Most social networks also function as social media sites..

OBJECTIVES

- To effectively train the network and enhance its resilience against real-world
- threats.
- To develop the Cyber Vaccinator for Image Immunization.
- To implement the Vaccine Validator for Media Distinction.
- To establish binary masks for object contours.
- To design Forward Pass for Tamper Detection.
- To develop a Localizer for Tampered Area Detection.
- To create Backward Pass for Image Self-Recovery.
- To simulate Adversarial Attacks for Effective Network Training.
- To encourage Image Self-Recovery Mechanisms.
- To achieve Proactive Image Immunization and Restoration.

LITERATURE REVIEW

Authors	Title	Techniques Used	Advantages	Disadvantages
Dong et al.	MVSS-Net for enhanced detection accuracy	Deep learning, neural networks	Comprehensive Coverage of Recent Advances	Lack of Critique on Methodologies
Liang et al.	Robust hashing techniques for image copy detection	Hashing algorithms	Clear Identification of Key Researchers	Limited Detail on Implementation
Lin et al.	Method for identifying subtle manipulation cues	Image processing, feature extraction	Highlights Diverse Methodologies	Scope Limited to Specific Algorithms
Zhang et al.	Dual-branch approach for improved detection robustness	Dual-branch neural networks	Mentions Practical Resources	Potential Publication Bias
Liu et al., Wu et al., Lin et al.	Novel network architectures for precise manipulation localization	Various neural network architectures	Provides Insight into Methodological Approaches	Missing Comparative Analysis
Wang et al.	Object Former	Object detection, computer vision	Advances state-of-the-art in object detection	Implementation complexity may be high
Chen et al.	Multi-view multi-scale supervision	Multi-view learning, deep learning	Enhanced learning from multiple perspectives	Requires significant computational resources
Matthes	"Python Crash Course"	Python programming	Easy-to-follow introduction to Python	Focuses primarily on basics, may not cover advanced topics in depth
Sweigart	"Automate the Boring Stuff with Python"	Web scraping, Automating GUI Applications	Simplifies automation tasks with practical examples	Limited coverage of advanced Python topics

METHODS AND MATERIALS

- **Techniques Used**: This column outlines the primary techniques or methodologies employed in each referenced work, such as deep learning, hashing algorithms, image processing, etc.
- **Advantages**: Summarizes the strengths or positive aspects of the literature review based on the authors and their titles.
- **Disadvantages**: Highlights the limitations or potential drawbacks associated with the literature review, offering a critical perspective on the discussed research.

This format provides a comprehensive overview, integrating information on techniques used along with advantages and disadvantages, which can aid in understanding the context and impact of each referenced work in image manipulation detection.

Recent advancements in image manipulation detection have catalyzed significant developments in algorithms and methodologies [1]. Noteworthy contributions include Dong et al.'s MVSS-Net, which enhances detection accuracy, Liang et al.'s robust hashing techniques for image copy detection [2][3], and Lin et al.'s method for identifying subtle manipulation cues [4]. Zhang et al. improved detection robustness with a dual-branch approach [5], while Liu et al., Wu et al., and Lin et al. introduced novel network architectures for precise manipulation localization [6][7][8]. Wang et al.'s Object Former and Chen et al.'s multi-view multi-scale supervision have further advanced the field. Additionally, practical resources such as Matthes' "Python Crash Course" and Sweigart's "Automate the Boring Stuff with Python" support real-world algorithm implementation.

Technical Description of components

Table Name: SN1_user1					
S.No	Field	Data Type	Field size	Constraint	Description
9	id	int	11	Primary Key	User id
2	Name	varchar	20	Null	User Name
3	Gender	Varchar	10	Null	User Gender
4	Dob	Varchar	40	Null	User dob
5	mobile	Big int	20	Foreign Key	User Mobile
6	email	Varchar	20	Null	User Email
7	adhaar	Varchar	11	Null	User aadhar
8	Username	Varchar	20	Null	Post username
9	password	varchar	20	Null	Post password
10	Date_time	Time_stamp	Time_stamp	Null	Post Date time

KEY COMPONENTS OF MULTI-TASK LEARNING (MTL)

- **Hard parameter sharing**: Shares hidden layers across tasks while maintaining task-specific output layers, which helps mitigate overfitting.
- **Soft parameter sharing**: Each task-specific model retains its own weights and biases, but these are regularized to encourage similarity across tasks, ensuring a balance between specialization and generalization.
- **Task clustering**: Groups similar tasks together to enhance knowledge transfer between related tasks, leveraging similarities for improved learning efficiency.
- **Shared layers**: Allows models to learn shared representations of data, fostering synergy between tasks and reducing redundancy in learned features.

- **Loss functions**: Customized for each task, accommodating varying task importance and optimizing performance accordingly.
- **Feature extraction**: Identifies task-specific features as well as shared patterns within the data, facilitating effective knowledge transfer across tasks.

SYSTEM SPECIFICATION

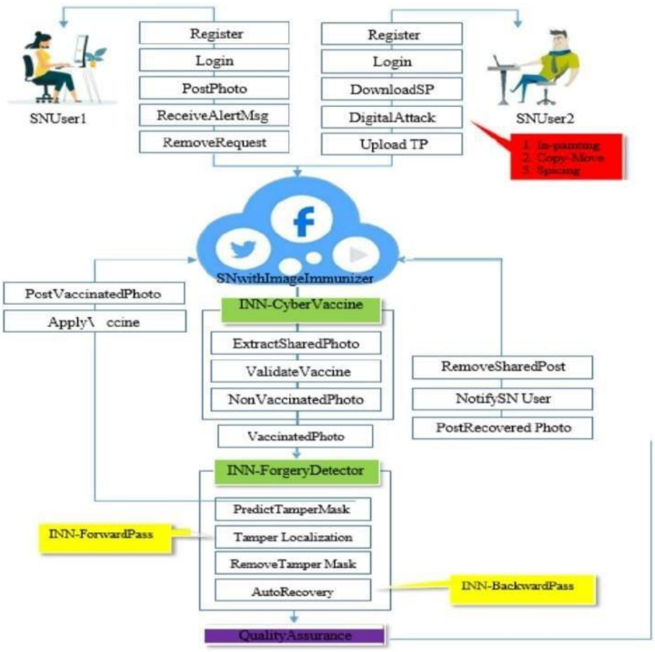
(6.1) Hardware Requirements

- **Processor:** Quad-core or higher for efficient parallel processing.
- **RAM:** 8 GB for seamless image processing and neural network tasks.
- **Storage:** 256 GB SSD for fast data access and storage.

(6.2) Software Requirements

- **Operating System:** Windows 10 or 11
- **Programming Language:** Python (version 3.6 or higher)
- **Neural Network Framework:** TensorFlow or PyTorch
- **Image Processing Libraries:** OpenCV and PIL (Pillow)
- **Web Framework:** Flask
- **Database Integration:** MySQL
- **IDE:** IDLE
- **Web Technologies:** HTML, CSS, and JavaScript

System architecture overview



RESULTS AND DISCUSSION

(8.1) SCREENSHOTS

Fig.8.1. Signup page

Social IV is the first app that is used to vaccinate the picture as Fig.5.1.1 Shows the login page and sign-up page as well.

Fig.8.2 : Login page

show the username and the password after the sign-up page used for the login page.

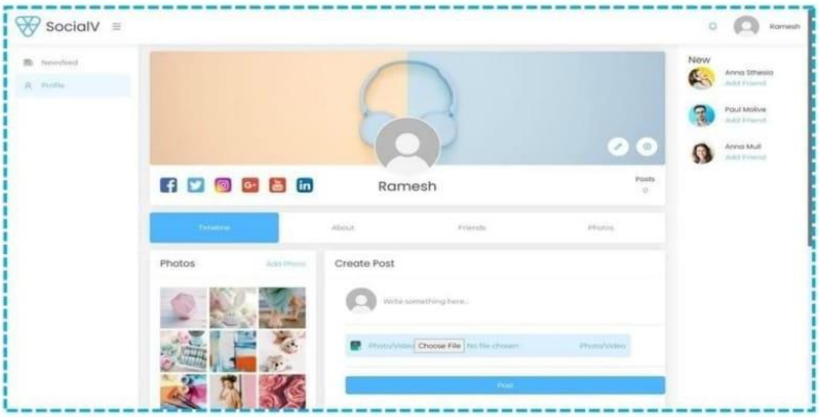
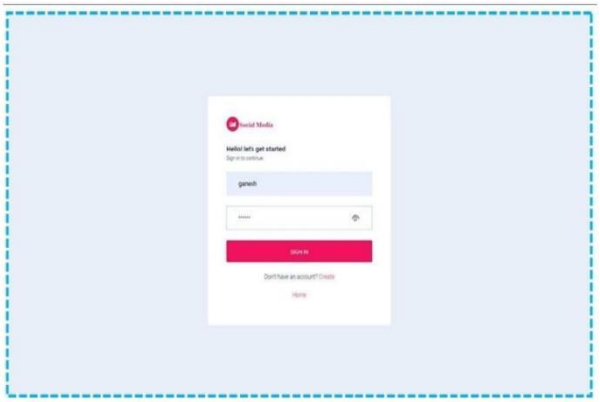


Fig. 8.3 : Image immunizer dashboard

This picture shows the front page of the profile which is where the picture is uploaded and gets vaccinated.



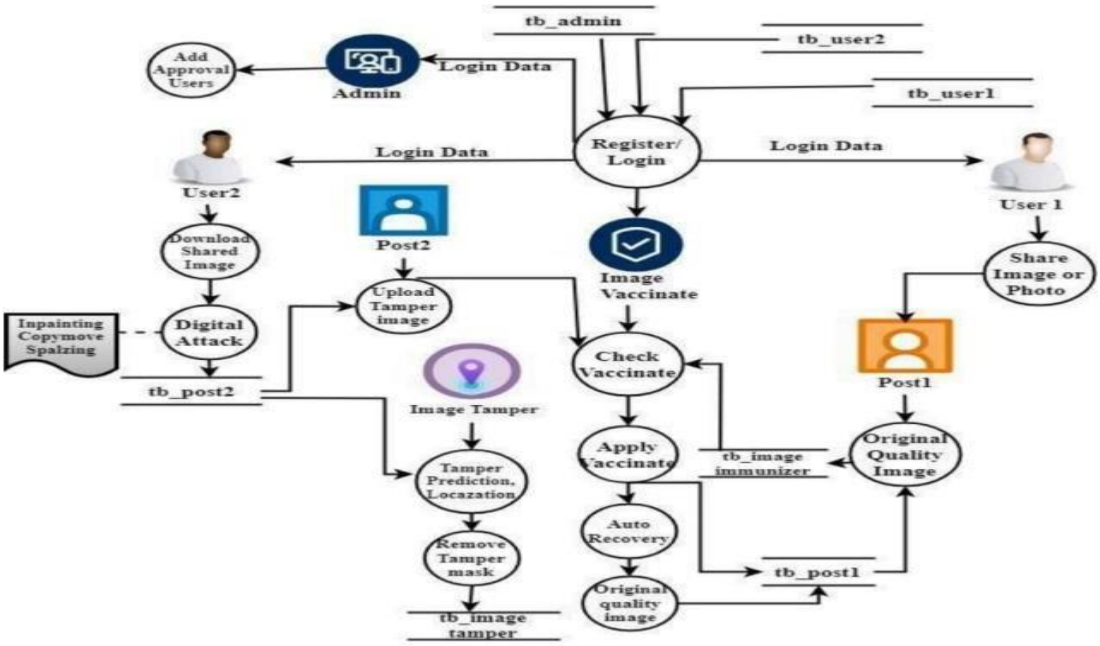
(8.4) Social media login page

ACKNOWLEDGEMENT

I also express my deep gratitude to my college "SRI MUTHUKUMARAN INSTITUTE OF TECHNOLOGY" and all the staff member of the department of Computer Applications for their warm support in all aspects. I owe my earnest gratitude to the project co-ordinator Dr. E.PANDIAN, Head of the Department of M.C.A and to the project guide Mrs. REKHA.P assistant Professor, Department of M.C.A.We express our heartiest thanks to all other teaching and non-teaching staff those who have helped us in one way.would like to thank our parents and staff.

Invertible Neural Network:

Invertible Neural Networks (INNs) are potent tools for inverse design optimization, enabling both forward and inverse predictions at minimal additional cost. While the forward process predicts outputs from inputs, the inverse process determines potential input parameters for a given system response. INNs utilize affine coupling blocks and are adept at solving inverse problems; however, they currently encounter challenges in accurately quantifying uncertainty, particularly for regression tasks. The advancement of new loss functions aims to bolster the accuracy of the inverse process. INNs leverage latent variables to capture critical information and find applications in fields like computer vision and inverse design. Despite their utility, standard INN implementations typically provide prediction results without uncertainty estimation.



CONCLUSION

In conclusion, the project "Image Immunizer Middleware for Online Social Networks" presents an innovative solution to combat digital image attacks effectively. By leveraging Invertible Neural Networks and adversarial simulation, the system ensures the authenticity and integrity of images shared on social platforms. The Cyber Vaccinator Module processes images by applying imperceptible perturbations during vaccination, thereby safeguarding them against tampering. The Vaccine Validator distinguishes vaccinated media to enhance security measures. Through its Forward and Backward Passes, the system identifies and restores tampered areas, ensuring the recovered images align closely with their originals. Adversarial training further bolsters resilience against a wide range of attacks.

This middleware seamlessly integrates with social media platforms, providing users with real-time notifications regarding image status and offering the capability to restore tampered images. Ultimately, it aims to establish a secure and trustworthy environment within social media networks.

FUTURE ENHANCEMENT

Future enhancements for the Image Immunizer Middleware for Online Social Networks using Invertible Neural Networks (INN) aim to bolster its capabilities and adapt to evolving technology. Integrating blockchain technology can enhance transparency in image transactions, ensuring tamper-evident records throughout the lifecycle of shared images. Expanding the middleware to include multimodal content analysis, such as videos and audio, will provide a more comprehensive defense against digital manipulation within Online Social Networks (OSNs). These advancements underscore our commitment to robust security and holistic content protection.

REFERENCES

[1] Carducci, C. G. C., Monti, A., Schraven, M. H., Schumacher, M., & Mueller, D. (2019). Enabling ESP32-based IoT Applications in Building Automation Systems. 2019 II Workshop on Metrology for Industry 4.0.

[2] M.H. Schraven, C. Guarnieri Calo' Carducci, M.A. Baranski, D. Mueller, A. Monti, "Designing a Development Board for Research on IoT Applications in Building Automation Systems," 36th International Symposium on Automation and Robotics in Construction (ISARC 2019), Banff, Canada, 2019, in press.

[3] ESP32 Overview by Espressif Systems (Shanghai) Co., Ltd. [Online]. Available: https://www.espressif.com/en/products/hardware/esp32/overview

[4] Guide to Open Protocols in Building Automation, Schneider Electric, 2015. [Online]. Available: https://download.schneiderelectric.com/files?penDocType=Brochure&pFileName=SE+Protocols+Guide.pdf

[5] A. Maier, A. Sharp and Y. Vagapov, "Comparative analysis and practical implementation of the ESP32 microcontroller module for the Internet of Things," 2017 Internet Technologies and Applications (ITA), Wrexham, 2017, pp. 143-148.

[6] D. Ghosh, A. Agrawal, N. Prakash and P. Goyal, "Smart Saline Level Monitoring System Using ESP32 And MQTT-S," 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom), Ostrava, 2018, pp. 1-5.

[7] Rai, P., & Rehman, M. (2019). ESP32 Based Smart Surveillance System. 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET).

[8] Pahuja, R. and Kumar, N., 2014. Android Mobile Phone Controlled Bluetooth Robot Using 8051 Microcontroller. International Journal of Scientific Engineering and Research, 2(7), pp. 14-17.

[9] Singh, P., Sharma, D. and Agrawal, S., 2011. A Modern Study of Bluetooth Wireless Technology. Dept. of Computer Sci. & Eng. Raipur, (Chhattisgarh).

[10] Chinmayi, R., Jayam, Y. K., Tunuguntla, V., Dammuru, J. V., Nadella, H., Anudeep Dulla, S. S. K., … Nair, J. G. (2018). Obstacle Detection and Avoidance Robot. 2018 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC).

[11] Arvind Kumar Saini, Garima Sharma, Kamal Kishor Choure, "BluBO: Bluetooth Controlled Robot," International Journal of Science and Research (IJSR) National Conference on Knowledge, Innovation in Technology and

Engineering (NCKITE), 10-11 April 2015, pp. 325-328.

[12] Singh, A., Gupta, T., & Korde, M. (2017). Bluetooth-controlled spy robot. 2017 International Conference on Information, Communication, Instrumentation and Control (ICICIC).

[13] Hossai, M. R. T., Shahjalal, M. A., & Nuri, N. F. (2017). Design of an IoT-based autonomous vehicle with the aid of computer vision. 2017 International Conference on Electrical, Computer and Communication Engineering (ECCE).

[14] Bairy A. (2022). Modeling Explanations in Autonomous Vehicles. In: ter Beek, M.H., Monahan, R. (eds) Integrated Formal Methods. IFM 2022. Lecture Notes in Computer Science, vol 13274. Springer, Cham.

[15] Aiman Ansari, Yakub Ansari, Saquib Gadkari, Aarti Goku: Android App Based Robot; Aiman Ansari et al., (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (2), 2015, 1598-1600.

[16] Singh, P., Sharma, D. and Agrawal, S., 2011. A Modern Study of Bluetooth Wireless Technology. Dept. of Computer Sci. & Eng. Raipur, (Chhattisgarh).

[17] Sairam, K.V.S.S.S.S., Gunasekaran, N. and Redd, S.R., 2002. Bluetooth is wireless communication. IEEE Communications Magazine, 40(6), pp. 90-96.

[18] Madhav, A.V.S., Tyagi, A.K. (2023). Explainable Artificial Intelligence (XAI): Connecting Artificial Decision-Making and Human Trust in Autonomous Vehicles. In: Singh, P.K., Wierzchoń, S.T., Tanwar, S., Rodrigues, J.J.P., Ganzha, M. (eds). Proceedings of Third International Conference on Computing, Communications, and Cyber-Security Lecture Notes in Networks and Systems. Springer, Singapore.

[19] Li Q, Wang Z, Wang W, Yuan Q. Understanding Driver Preferences for Secondary Tasks in Highly Autonomous Vehicles. In: Long S, Dhillon BS, editors. Man-Machine-Environment System Engineering. MMESE 2022. Lecture Notes in Electrical Engineering, vol. 941. Singapore: Springer; 2023.

[20] Kolb, A., Barth, E., & Koch, R. (2008). ToF-sensors: New dimensions for realism and interactivity. 2008 IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops. doi: 10.1109/cvprw.2008.4563159.

[21] Monika Jain, Aditi, Ashwani Lohiya, Mohammad Fahad Khan: Wireless gesture control robot; International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Issue 10, December 2012 Viraj Mali, Ankit Gorasia, Meghana Patil, Prof. P.S.Wawage Department of Information Technology, Vishwakarma Institute of Information Technology, Pune.

[22] Prof. Horacio Espinosa: Robotic Control with Bluetooth Wireless Communication; Northwestern University.