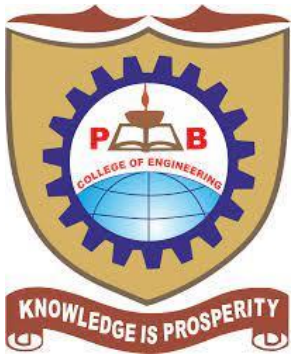


P. B. College of Engineering
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

Department of computer Science and engineering

Identifying forgery detection

Team Members:
Kanmani S - 211320104005
Sowmiya -211320104009

Batch No:
Date :

Supervised By,
Muthamizh

Abstract

- Today, people frequently interact with their families, friends, and colleagues through online social networks (OSN).People enjoy posting and sharing their photos in online communities, blogs, and content sharing sites.

- The problem addressed in this project is the susceptibility of digital images to tampering, which compromises security and privacy. Traditional image forgery detection methods face challenges in reproducing original content after manipulation.

- This project introduces an advanced Image Immunization System leveraging Invertible Neural Networks.

- The system, comprising the Cyber Vaccinator, Vaccine Validator, Forward Pass for Tamper Detection, and Backward Pass for Image Self-Recovery, aims to proactively immunize images against various attacks.

- Run-Length Encoding in the backward pass to transform hidden perturbations into information, facilitating lossless recovery of the authentic image.

Objective

Aim

The aim of the project is to develop an Image Immunization System using an Invertible Neural Network. The system aims to proactively immunize images against malicious attacks while enabling self-recovery in the event of tampering.

Objective

- To develop the Image Immunizer framework with Invertible Neural Networks.
- To Develop the Cyber Vaccinator for Image Immunization.
- To Implement the Vaccine Validator for Media Distinction.
- To implement a robust pixel classification module for accurate tamper localization.
- To integrate features promoting self-recovery for immunized images.
- To implement Run-Length Encoding for lossless perturbation transformation.
- To evaluate the accuracy of tamper localization achieved by Image Immunizer.

Existing System

- **Watermarking Techniques:**

Embedding watermarks in images to detect tampering by analyzing alterations in the watermark pattern.

- **Digital Signatures:**

Using cryptographic techniques to add a digital signature to images, ensuring integrity and authenticity.

- **Copy-Move Detection:**

Identifying duplicated or manipulated regions within an image by detecting identical patterns.

- **Forensic Hashing:**

Generating cryptographic hash values for images to verify their integrity and detect tampering.

Existing System

Steganalysis Techniques:
Analyzing hidden information or data embedded within images to detect tampering or alterations.

Image Forensics using Machine Learning:
Employing machine learning algorithms to analyze patterns, features, and inconsistencies indicative of tampering.

Biometric-Based Authentication:
Incorporating biometric features within images for authentication, making tampering more challenging without affecting the biometric data.

Image Phylogeny:
Examining the evolutionary relationships between images to identify common ancestry and potential tampering.

Disadvantages

- Limited robustness against advanced tampering techniques.
- Sensitivity to image compression leading to potential false alerts.
- 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.

Proposed System

The proposed system, "Image Immunizer," is designed to enhance image tamper resilience and facilitate lossless auto-recovery.

Cyber Vaccine: Vaccinator for inducing immunity for recovering image content

Invertible Neural Networks (INN): Core architecture facilitating reversible transformations for lossless recovery.

Multitask Learning Framework: Utilizes multitask learning to train the network for simultaneous tasks.

- Ensuring Consistency between Immunized and Original Images.
- Classifying Tampered Pixels.
- Encouraging Image Self-Recovery.

Proposed System

Forward Pass with Tamper Localization:

Localizer identifies tampered areas by predicting a tamper mask.

Backward Pass with Run-Length Encoding:

Hidden perturbations transformed into information during the backward pass.

Facilitates the recovery of the original, lossless image and its edge map.

Advantages

- Tamper Resilience: Enhances resistance against unauthorized alterations.
- Ensures recovery without loss of original image information.
- Improves the security of digital images against tampering threats.
- Applicable across domains such as forensics and digital communication.
- Maintains the authenticity of recovered images.
- Effectively addresses challenges posed by compressed or low-resolution images.

Software Requirements

- **Server Side** : Python 3.7.4(64-bit) or (32-bit)
- **Client Side** : HTML, CSS, Bootstrap
- **IDE** : Flask 1.1.1
- **Back end** : MySQL 5.
- **Server** : Wampserver 2i
- **Blockchain** : TensorFlow, Keras, Pandas, Sickit Learn, Matplotlib

literature survey

1) **“Learning to Immunize Images for Tamper Localization and Self-Recovery”**

- Presents Imuge+, an enhanced scheme for image immunization.
- Utilizes an invertible neural network for joint learning of immunization and recovery.

2) **“A Review of Reversible Medical Image Watermarking Scheme with Tamper Localization and Recovery Capability”**

- Reviews reversible medical image watermarking schemes with tamper localization and recovery capabilities.

3) **“Proposing an Enhanced Tamper Detection Algorithm Using YOLOv5s with CBAM Attention and EIOU Loss”**

- Focuses on improving feature extraction for unknown tampering modes.
- Integrates CBAM attention into YOLOv5s Neck layer.
- Achieves accuracy improvement over benchmarks.

literature survey

4) **“Image Immunization: A Technology for Protecting Images”**

- Discusses the concept of image immunization.
- Introduces techniques for applying vaccines to images and encouraging self-recovery.

5) **“Imuge+: Enhanced Image Immunization for Tamper Localization and Recovery”**

- Investigates the relationship between image immunization and self-recovery.
- Utilizes an invertible neural network for joint learning.

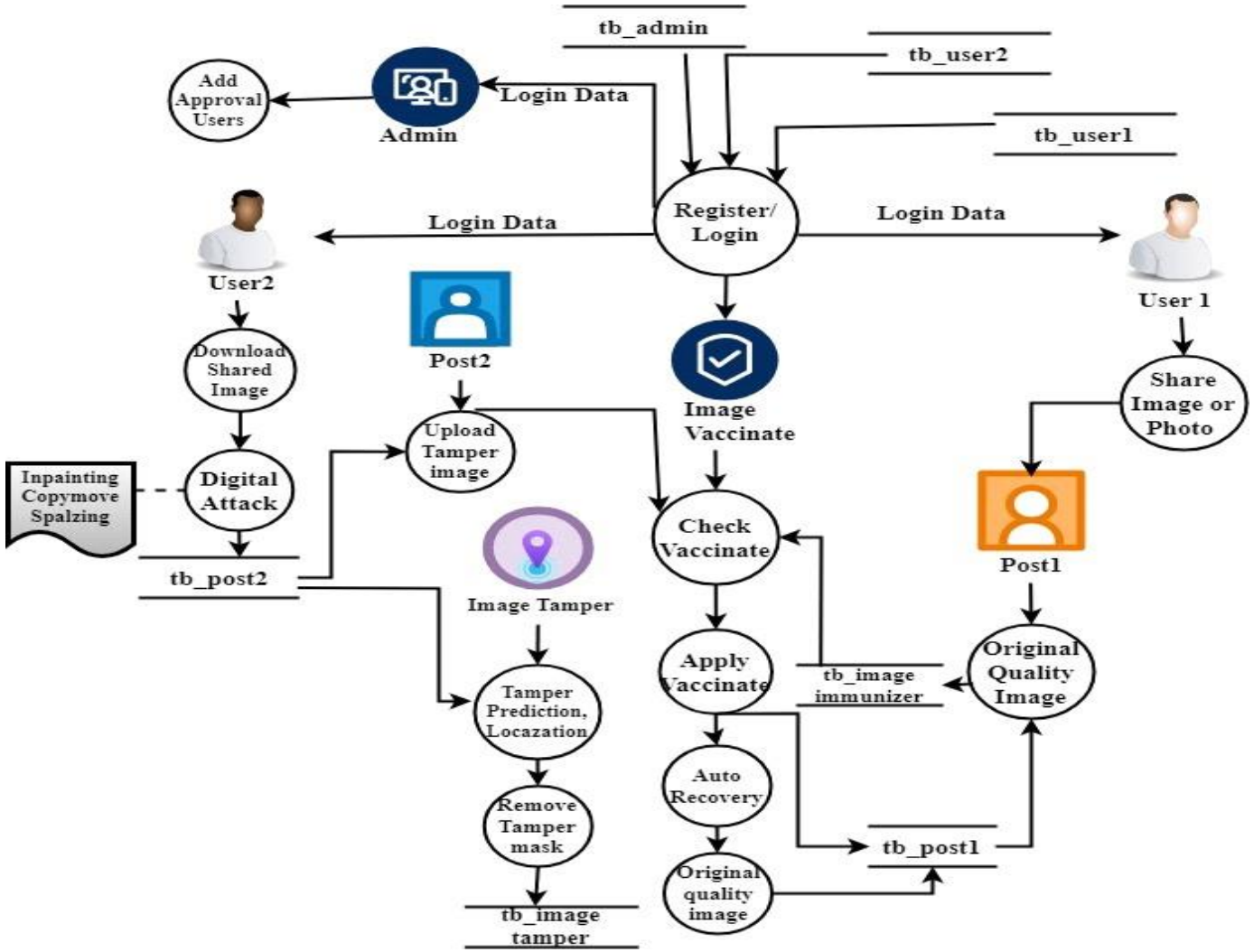
6) **“Image Immunization: Protecting Images by Introducing Trivial Perturbations”**

- Proposes Imuge, a technology for protecting images.
- Discusses the immune nature of tampered images.

literature survey

7) **Proposing an enhanced tamper detection algorithm using YOLOv5s with CBAM Attention and EIOU Loss**. The focus is on improving feature extraction for unknown tampering modes. Methodology involves integrating CBAM attention into YOLOv5s Neck layer and optimizing boundary frame loss with EIOU Loss. Achieves 1.57% average accuracy improvement over benchmarks, outperforming traditional methods. Lacks detailed dataset information and thorough explanation of techniques. Nonetheless, shows promise in robust tamper detection.

Block Diagram



Modules

a) The social networking web app is meticulously crafted using Python, Flask, MySQL, Bootstrap, and Wampserver 2i to deliver a secure, responsive, and feature-rich user experience. The User Authentication module guarantees secure access, employing features such as user registration, login, password hashing, and two-factor authentication. The User Profile module fosters personalization, allowing users to create and customize profiles with responsive design elements.

b) End User Interface: The End User Interface module provides a seamless and intuitive experience for social network users, encompassing essential functionalities such as registration, login, social connections, image sharing, download, and interaction with shared content. The module also includes features for applying digital attacks to images, sharing tampered content, and receiving notifications.

c) Adversarial Simulation: Training Against Threats The system employs adversarial simulation, leveraging the capabilities of the Invertible Neural Network, to fortify its resilience against potential threats. Three malicious attacks - copy-move, splicing, and benign attacks like rescaling and blurring - are simulated during the training process. The Invertible Neural Network, is well-prepared to detect and counteract a diverse array of potential attacks, thereby enhancing its robustness in maintaining the integrity of the digital landscape.

d) Image Immunizer Middleware: The Image Immunizer Middleware is a crucial component within a system designed to enhance the security and integrity of digital images. This middleware employs Cyber Vaccinator Framework to discern between vaccinated and unvaccinated, if unvaccinated means transform an original image to its edge map into an immunized version. Invertible Neural Network (INN) employs Forward pass to determine tampered areas by predicting the tamper mask and type of attack. Backward pass the recovery of the original image and its associated metadata. The module operates in real-time, seamlessly integrating into the image processing pipeline

e) Objective Loss Function: 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.

f) Notification: The Notification Module serves as a vital component in keeping users informed and empowered when it comes to shared vaccinated images on other social networks. Specifically, when a user downloads and shares a vaccinated image without any attack, the Image Immunizer detects the shared image and triggers an email notification to the user. The email prompts the user to make a decision regarding the shared imag

METHODOLOGY

A. **Deeps 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 are computer files that data scientists have trained to perform tasks.

B. **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.

C. **Hard Parameter Sharing**: This component involves sharing the hidden layers of a neural network while keeping task-specific output layers. It reduces overfitting by sharing layers across similar jobs.

D. **Soft Parameter Sharing**: Each model has its own set of weights and biases, and the spacing of these parameters in the model is regulated so that the parameters are homogeneous and representative of all applications.

E. **Task Clustering**: MTL uses task clustering to group tasks. This guarantees that AI models learn from tasks with similar characteristics, resulting in improved knowledge transfer

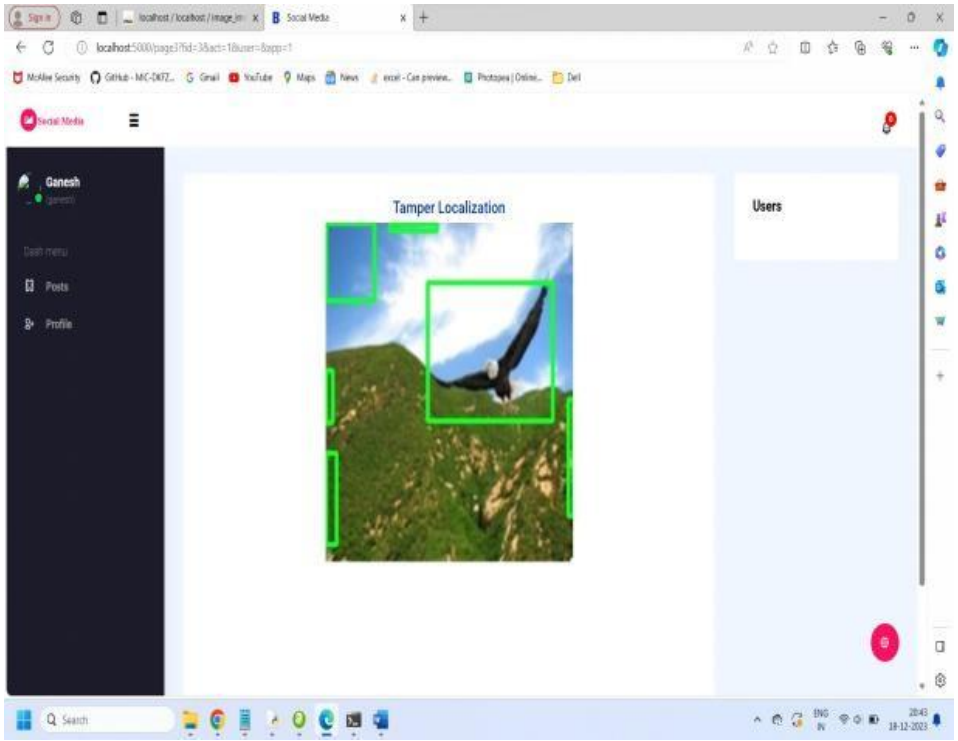
Methodology

F. **Shared Layers**: AI systems with shared layers enable models to learn shared representations across tasks. These shared layers promote learning synergy and eliminate redundancy.

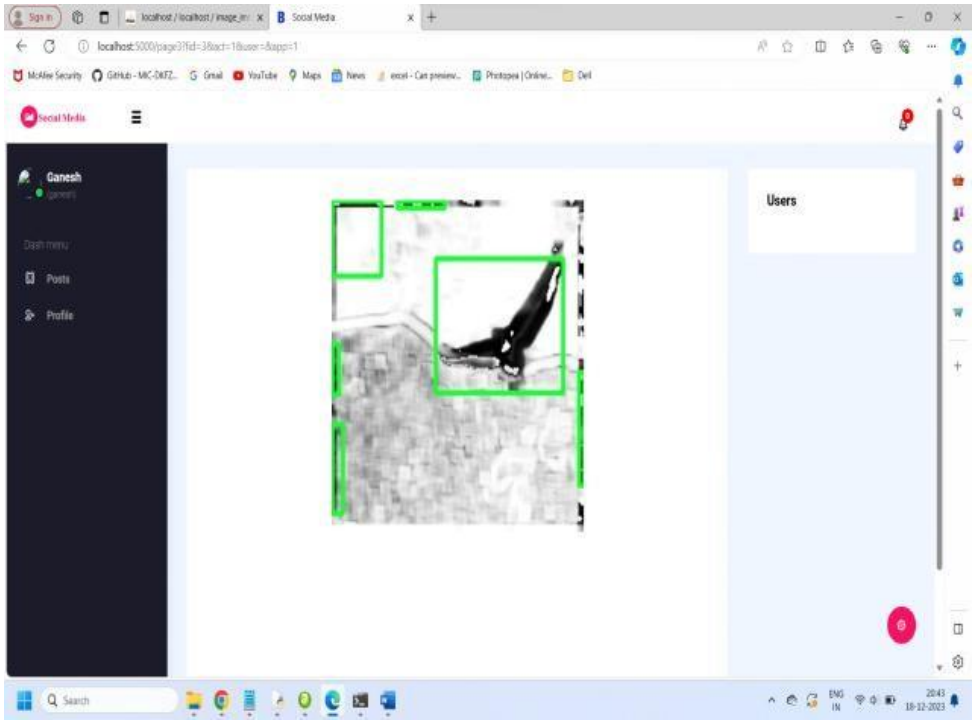
G. **Loss Functions**: MTL models can assign varied levels of importance to different activities thanks to tailored loss functions for each activity. This adaptability helps with performance enhancement in tasks of varying complexity.

H. **Feature Extraction**: MTL uses feature extraction techniques to help AI models find task-specific and shared elements in data. This encourages efficient knowledge transfer.

Result



Picture



Tampered layer

conclusion

The Image Immunizer Middleware is an advanced solution designed to combat digital image attacks on social networking platforms. Key features include:

- **Invertible Neural Network** (INN) technology for robust defense.
- Adversarial simulation during training to enhance resilience.
- **Cyber Vaccinator Module** for pre-processing, vaccination, and post-processing of images.
- **Vaccine Validator** to distinguish vaccinated and unvaccinated media.
- **Forward and Backward Pass** for image self-recovery.
- Seamless integration with existing OSN architectures.
- Real-time status notifications and tampered image restoration.

This state-of-the-art project ensures the integrity of shared images in the dynamic realm of online social networks.

References

1. X. Liang, Z. Tang, Z. Li, M. Yu, H. Zhang and X. Zhang, "Robust hashing via global and local invariant features for image copy detection", ACM Trans. Multimedia Comput. Commun. Appl., vol. 20, no. 1, pp. 1-22, Jan. 2024.

2. 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.

3. A. S. Shaik, R. K. Karsh, M. Suresh and V. K. Gunjan, "LWT-DCT based image hashing for tampering localization via blind geometric correction" in ICDSMLA 2020, Singapore:Springer, vol. 783, 2022.

4. Y. Chen, L. Liu, V. Phonevilay, K. Gu, R. Xia, J. Xie, et al., "Image super-resolution reconstruction based on feature map attention mechanism", Appl. Intell., vol. 51, no. 7, pp. 4367-4380, Jul. 2021.

5. B. Bolourian Haghighi, A. H. Taherinia and R. Monsefi, "An effective semi-fragile watermarking method for image authentication based on lifting wavelet transform and feed-forward neural network", Cognitive Computation, vol. 12, no. 4, pp. 863-890, 2020.