INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 05, May 2024, pp: 1858-1866

e-ISSN : 2583-1062

Impact Factor: 5.725

IMAGE IMMUNIZER - AN IMAGE TAMPER RESILIENT MULTI TASK LEARNING SCHEME FOR IMAGE LOSSES LESS AUTO-RECOVERY

Prithviraj V[1], Pranav Praven CV[2], Gowtham Dev[3], Jeyaram Kr[4], K Aishwariya Vidya[5]

[1,2,3,4,5]Adithya institute of technology, 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.

Keywords: Image immunizer, Deep Learning, Neural Network.

1 INTRODUCTION

1.1 OVERVIEW

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.

Fig. 1 : Social media apps

With the broad spectrum (fig.1.1.1) of websites, apps and services that exist online, there is no single exact definition of a social network. 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. They are encouraged to post text, status updates or pictures for viewing by others. Social networks allow the user or organization to create a profile. The profile contains information about the person and a centralized page with the content posted by them. Their profile may be associated with their real name. A social network has a way to form a lasting connection with other users. These connections are commonly called friending or following the other user. They allow the users to find other users and form webs of relationships. Often an algorithm will recommend other users and organizations they may want to form a connection with. Although often used interchangeably, social network is different than social media. A social network focuses on the connections and relationships between individuals. Social media is morefocused 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.

1.2 PROBLEM STATEMENT

One problem with photo sharing privacy and security issues on social networking websites is the potential for unauthorized access to user's personal information and images. This can happen in a variety of ways, such as through hacking or data breaches, or through the misuse of data by third-party apps or advertisers. Another issue is the lack of control that users have over their own content once it is posted online. Even if a user sets their account to private, their photos may still be accessible to othersif someone they have granted access to their account shares the photos or if the platform's privacy settings are not sufficient. There is also the risk of online harassment and cyber bullying, which can be facilitated by the sharing of photos and personal information on social media. This can have serious consequences for individuals' mental health and well-being, and can even lead to physical harm in extreme cases. Finally, social media platforms may also use facial recognition technology to automatically tag users in photos, which raises concerns about privacy and the potential form is use of this technology.

Photo sharing privacy and security issues in social networking websites can arise due to a varietyof reasons. Some of the common problems include: Social networking websites may have vulnerabilities that allow hackers to access private photos without authorization. This can compromise the privacy of the users and lead to identity theft or other malicious activities. User’s may not be aware of the privacy settings available on the social networking website, or they may not be using them effectively. This can result in unintentional sharing of personal photos with a wider audience than intended. Social networking websites may collect and use user data, including photos, for advertising purposes or other commercial activities. This can be a privacy concern for users who are not aware of how their data is being used. Social networking websites may have users who share inappropriate or offensive content, including photos. This can create a hostile environment for other users and can also be a security risk if the content is malicious. Digital image attacks encompass a range of techniques aimed at manipulating visual content, posing substantial threats to the authenticity and trustworthiness of images shared on social networking websites. Copy-move attacks involve duplicating and relocating specific portions within the same image, creating deceptive duplicates that appear unique.

Splicing, another prevalent technique, combines elements from different images to fabricate composite visuals, often with the intent of inserting objects or people into misleading contexts. In- painting attacks focus on concealing or removing specific regions within an image, seamlessly filling the gaps to make alterations less conspicuous. These manipulative practices can lead to misinformation,false narratives, or privacy breaches. Overall, these issues highlight the need for social networking websites to prioritize the privacy and security of their users, and for users to be aware of the risks involved in sharing photos online. This project addresses the critical problem of securing shared photoson social networking platforms by developing advanced techniques for the detection and prevention of Copy-Move, Splicing, and In-Painting attacks, ensuring a safer and more trustworthy online image- sharing environment.

1.3 DEEP LEARNING

Deep learning is a method in artificial intelligence (AI) that teaches computers to process data ina 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.

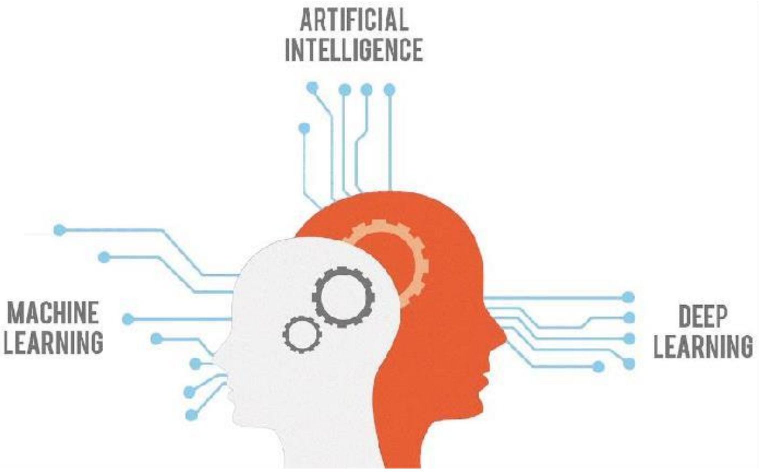


Fig.2 : Deep learning algorithm

Deep learning algorithms are neural networks that are modeled (figure no:1.3.1) 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.

1.4 Key components of multi-task learning

MTL forms the building blocks of synergy. The key components that enable this synergy are:

- **Hardparameter sharing**
  This component involves sharing the hidden layers of a neural network while keeping task- specific output layers. It reduces over fitting by sharing layers across similar jobs.
- **Softparameter 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.
- **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.
- **Shared layers**
  AI systems with shared layers enable models to learn shared representations across tasks. These shared layers promote learning synergy and eliminate redundancy.
- **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.
- **Feature extraction**
  MTL uses feature extraction techniques to help AI models find task-specific and shared elements in data. This encourages efficient knowledge transfer.

2 SYSTEM SPECIFICATION

2.1 HARDWARE REQUIREMENTS

Processor

Quad-core or higher processor for efficient parallel processing, capable of handling complex image transformations and neural network computations.

RAM

8 GB RAM to facilitate seamless image processing and provide ample memory for neural network training and inference tasks.

Storage

Solid State Drive with a minimum capacity of 256 GB for fast data access and storage of datasets, trainedmodels, and system files.

2.2 SOFTWARE REQUIREMENTS

- **Operating System:** Windows 10 or 11 (for Windows-specific development)
- **Programming Language:** Python(version3.6or higher)
- **Neural Network Framework:** TensorFlow or PyTorch
- **Image Processing Libraries:** OpenCV and PIL (Pillow)
- **Web Framework:** Flask for implementing a web-based user interface,
- **Database Integration:** MySQL for storing and retrieving relevant data.

Integrated Development Environment (IDE): IDLE

- **Web Technologies:** HTML, CSS, and JavaScript

3 IMAGE IMMUNIZER

3.1 SYSTEM ARCHITECTURE

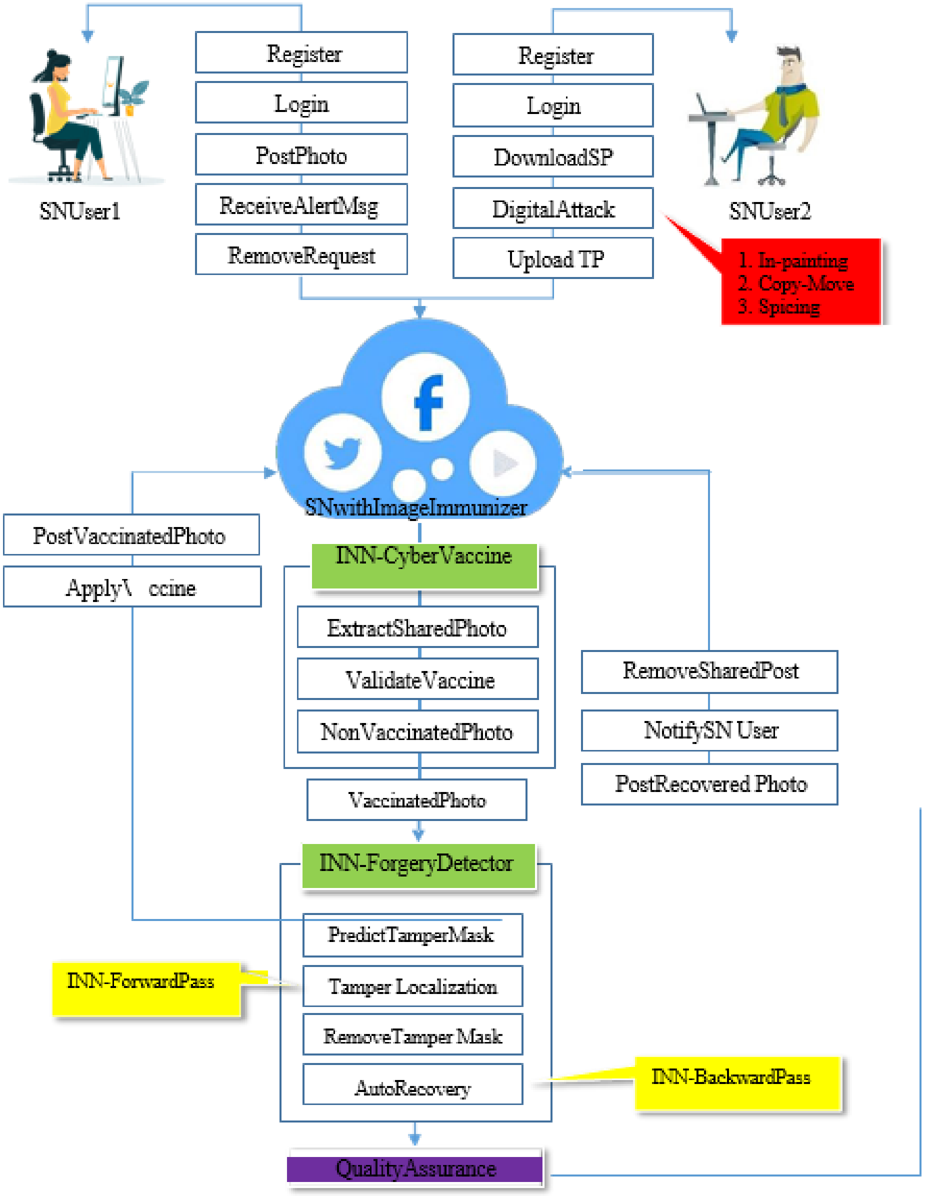
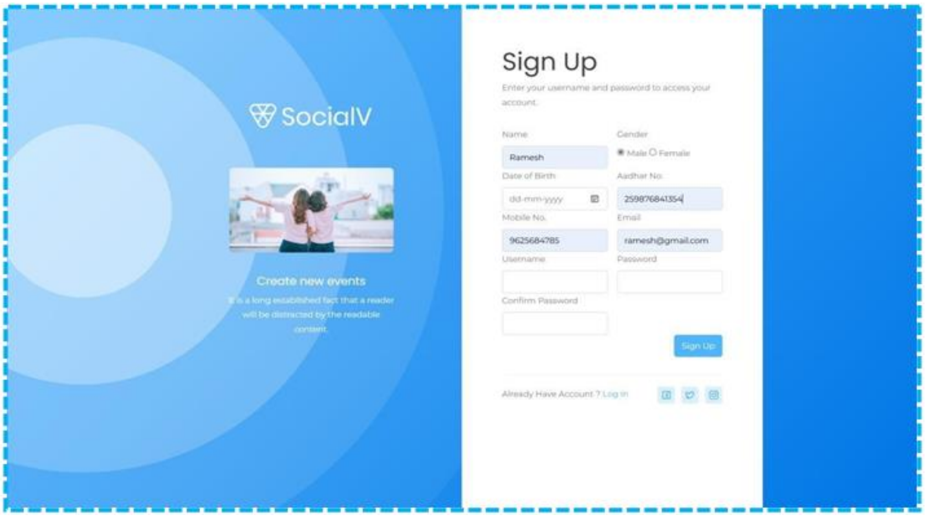


Fig.4.1.1: System architecture overview

Fig.4.1.1: System architecture overview

4 RESULTS AND DISCUSSION

4.1 SCREENSHOTS



Sign Up

Enter your username and password to access your account.

Name: Ramesh

Gender: ● Male ○ Female

Date of Birth: dd-mm-yyyy

Aadhar No: 259876841354

Mobile No.: 9625684785

Email: ramesh@gmail.com

Username:

Password:

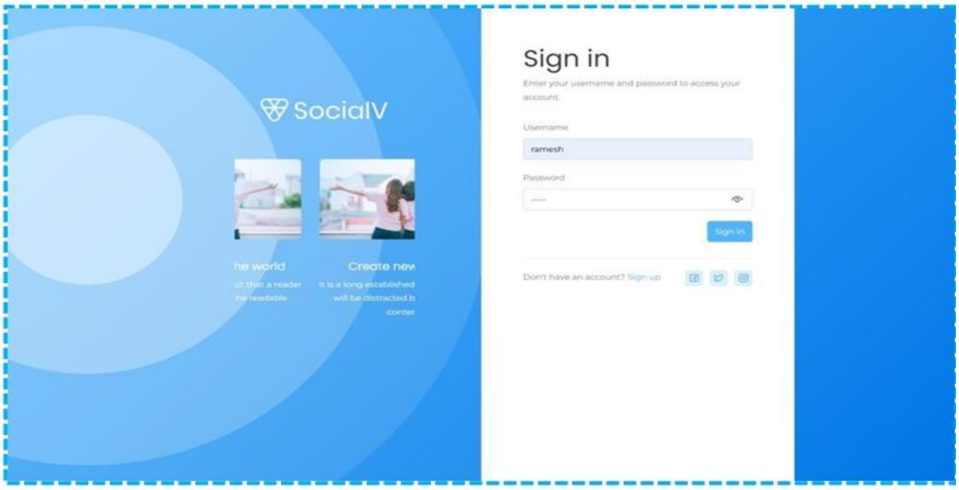
Confirm Password:

Already Have Account ? Log in

SocialV
Create new events
It is a long established fact that a reader will be distracted by the readable content.
Sign Up

Fig.4.1. Signup page

Social iv is the first app that is used to vaccinate the picture as Fig.5.1.1 Shows the login page andsign up page as well.



Sign in

Enter your username and password to access your account.

Username: ramesh

Password: ······

Don't have an account? Sign up

Fig.4.2 : Login page

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

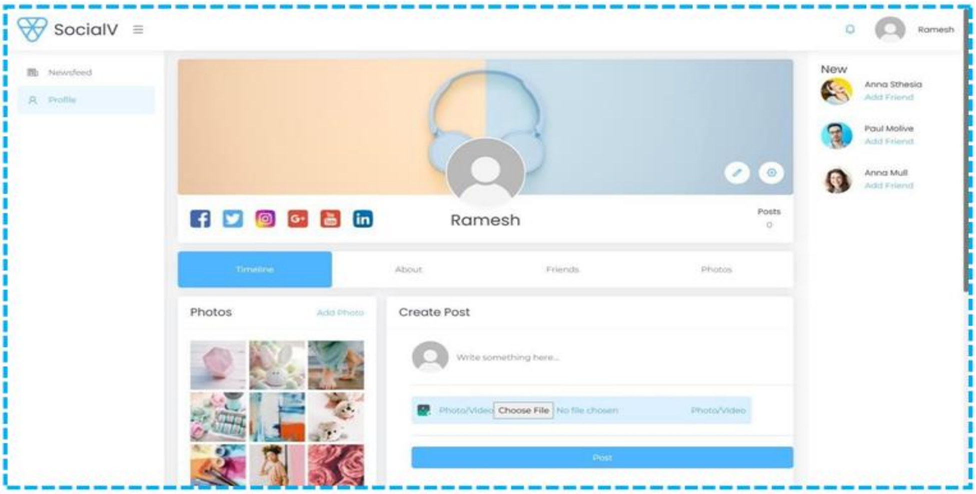
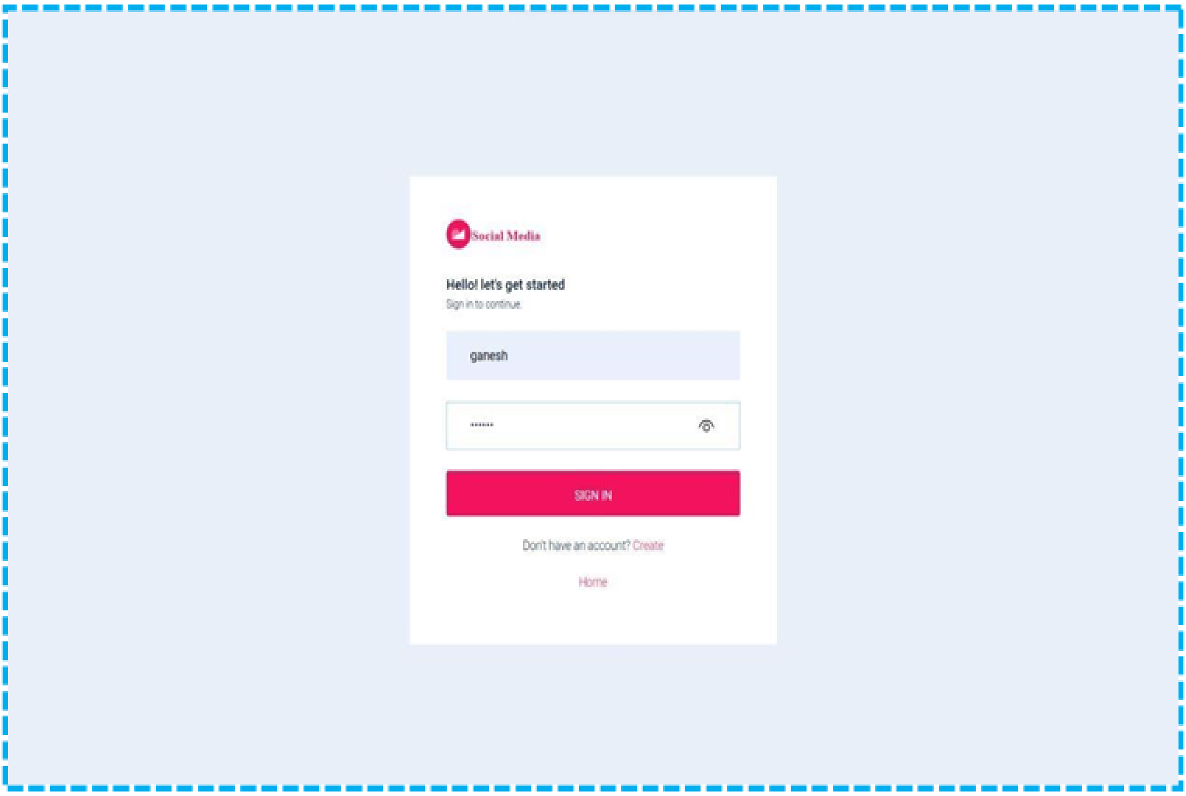


Fig. 4.3 : Image immunizer dashboard

This picture Fig.5.1.3 shows the front page of the profile that is where the picture is uploaded andgets vaccinated.



Social Media

Hello! let's get started

Sign in to continue.

ganesh

******

Don't have an account? Create

4.4 Social media login page

This is another app as same as a Social Iv , this is known as the Social Media app in the Fig. 5.1.4

5 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 pre-processes, 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 theoverall security posture.

The Forward Pass, employing INN, and the subsequent Backward Pass for imageself- recovery collectively contribute to the identification and restoration of tampered areas. This dynamicapproach 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.

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.

5.1 FUTURE ENHANCEMENT

The future enhancements for the Image Immunizer Middleware for Online Social Networks using Invertible Neural Network (INN) aim to strengthen its capabilities and adapt to evolving technology. Integrating block chain technology can enhance transparency in image transactions, ensuring a tamper- evident record.

The middleware's expansion to multimodal content analysis, including videos and audio, provides a more comprehensive defence against digital manipulation within OSN. These advancements reflect a commitment to robust security and holistic content integrity.

6 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 andS.Zhang ,"Efficient hashing method using 2D–2DPCA 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.ChenandX.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.Tianand, 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 adaptivedge supervision",IEEE Trans. Multimedia,pp.1-15,2022.

[9] J.Wangetal.,"Object Former 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.

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