Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
DOI: https://doi.org/10.17762/msea.v70i2.2460

# Tampering Detection and Content Authentication Using Encrypted Perceptual Hash for Image Database

**Ayushi Jain**
Asst. Professor, Department of Comp. Sc. & Info. Tech., Graphic Era Hill University,
Dehradun, Uttarakhand India 248002

***Article Info***
***Page Number:1695 - 1705***
***Publication Issue:***
***Vol 70 No. 2 (2021)***

***Article History***
***Article Received**: 05 September 2021*
***Revised**: 09 October 2021*
***Accepted**: 22 November 2021*
***Publication**: 26 December 2021*

***Abstract***

To detect and locate unapproved alterations or modifications made to digital pictures, tampering detection in images is a crucial study topic in the field of image forensics. As sophisticated picture altering tools become more widely available, it has become more difficult to guarantee the integrity and authenticity of digital visual output. This overview of the literature explores methodology, findings, and contributions in key tampering detection research studies. The breakthroughs in deep learning techniques and steganalysis are highlighted together with more conventional approaches like statistical analysis and error level analysis. The difficulties tampering detection faces are discussed, including generalisation, dataset accessibility, resilience against adversarial assaults, computing effectiveness, and moral and legal issues. With the goal of advancing the creation of precise, reliable, and effective algorithms for maintaining the integrity and authenticity of digital pictures, the paper offers insights into the current state of the art, limits, and future research paths in tampering detection.

**Keywords.** tampering detection, image forensics, steganalysis, digital image manipulation, image forgery.

## I. Introduction

One of the most important areas of research in the field of image forensics is the detection of tampering in digital photographs. Keeping the integrity and authenticity of digital visual content has grown more difficult as a result of the widespread availability of potent picture editing tools and the simplicity of digital image alteration [1]. The goal of tampering detection techniques is to locate and identify any unauthorised alterations or modifications done to digital photographs. This allows for the authenticity and integrity of the photos to be verified. In a number of industries, such as journalism, law enforcement, and the dissemination of multimedia material, digital picture modification can have serious repercussions. It can be used for bad things like disseminating false information, tampering with physical evidence, or unauthorised use of intellectual property. To solve these issues and reduce the hazards related to picture manipulation, it is crucial to create trustworthy and efficient tampering detection systems [2].

The purpose of this literature review is to investigate and evaluate a number of significant studies in the area of digital picture manipulation detection. We seek to acquire a thorough grasp of the developments, difficulties, and future directions in this important study subject by reviewing the techniques, results, and contributions of these works. Splicing, copy-move, retouching, and deepfake methods are just a few examples of the many ways that digital images may be altered [3]. The analysis of visual artefacts, inconsistencies, or statistical aberrations generated by the tampering process is the foundation of conventional tampering detection techniques. These methods include approaches based on compression, noise pattern analysis, and error level analysis. Although these approaches have been somewhat successful, they frequently lack the capacity to recognise more advanced tampering techniques and can have a significant false-positive rate. Recent developments in deep learning and machine learning methods have created new opportunities for tamper detection. In learning discriminative characteristics and spotting altered areas in pictures, convolutional neural networks (CNNs), recurrent neural networks (RNNs), and generative adversarial networks (GANs) have demonstrated promising outcomes. Deep learning-based methods have the capacity to collect intricate patterns and contextual data, making it possible to identify tampering even in difficult situations [4].

We concentrate on a number of important studies that have made substantial contributions to the field of tampering detection in digital photographs. These publications cover a broad range of subjects and approaches, including feature extraction, deep learning, steganalysis, and statistical analysis. We analyse these studies in order to determine the advantages, disadvantages, and potential future lines of inquiry in the field of tampering detection.We look at the difficulties and restrictions that current tampering detection methods confront. These difficulties include the need for diverse and annotated datasets, the ability to generalise algorithms across various types of tampering, the robustness of algorithms against adversarial attacks, the computational efficiency of algorithms, and the moral and legal issues related to tampering detection [5].

To overcome these obstacles, multidisciplinary cooperation, improvements in algorithm design, availability of extensive datasets, and the creation of moral and legal frameworks for tamper detection are all necessary. We may discover prospective research areas and create more precise, reliable, and effective tampering detection algorithms by comprehending these difficulties and the state of the art in tampering detection. The integrity and authenticity of visual material are crucially protected by thetamper detection in digital photographs. By highlighting their techniques, conclusions, and contributions, the literature review strives to present a thorough overview of significant research publications in this area. By resolving the issues and constraints, we may open the door for more breakthroughs and improvements in tampering detection methods, finally assuring the validity and dependability of digital pictures in a variety of applications.

## II. Review of Literature

An important topic of study in the field of image forensics is the detection of tampering in digital photographs. The integrity and authenticity of digital photographs have become a major problem as a result of the increased use of image alteration tools and techniques. The techniques, conclusions, and contributions of each study are examined in this review of the literature, which examines a number of significant research publications in the field of tampering detection.

The goal of this research [6] is to discover hidden signals or modifications in digital photographs. The authors offer extensive models for steganalysis. Higher-order statistics, wavelet coefficients, and pixel residuals are just a few of the statistical aspects that are explored in this research. Through comprehensive trials and comparisons with other steganalysis techniques, the authors show the efficacy of the suggested models. The outcomes demonstrate increased detection precision and resilience against several steganographic methods.

A thorough review of picture forensics, including tampering detection and related subjects, is given in this study [7]. The writers go on the difficulties and methods involved in a number of forensic activities, including forgery detection, picture tampering, and source identification. The paper discusses both conventional techniques like error level analysis and picture watermarking and more sophisticated ones like digital signature-based methods and machine learning-based techniques.

A survey on the use of deep learning approaches for picture fraud detection is presented by the authors [8]. The study analyses different deep learning architectures for forgery detection tasks, such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs). Additionally, it covers the difficulties, datasets, and assessment criteria particular to deep learning-based forgery detection. The study offers insightful information on the state of the art at the moment and suggests possible research areas in this fast developing sector.

This thorough analysis of picture forgery detection methods [9] gives you an understanding of the methods. It includes a variety of techniques for detecting tampering, such as copy-move detection, statistical analysis, and conventional techniques based on picture artefacts. The application of blockchain technology and new developments in deep learning-based methods are also covered by the writers. The survey suggests potential study paths and offers insights into the benefits and drawbacks of various methodologies.

The unique steganalysis method described in this study [10] is based on the subtractive pixel adjacency matrix. The authors provide a statistical model that examines the variations between the original and potentially altered photos and captures the relationships between neighbouring pixel values. Results from experiments show how well the method works to identify both frequency-domain and spatial-domain steganographic schemes.

For the purpose of detecting picture counterfeiting, the authors suggest [11] a unique method that recasts residual-based local descriptors as convolutional neural networks (CNNs). The work looks at how CNNs may be used to extract reliable features from image residuals, which record the differences between a picture and its projected form. The efficiency of the suggested approach in identifying different forgeries, including as copy-move and splicing alterations, has been tested by experimental assessments.

The tampering detection [12] in digital photos uses both conventional techniques and cutting-edge deep learning techniques. These publications offer novel methods and models to improve the precision and resilience of tampering detection algorithms while addressing a variety of problems, including steganalysis, copy-move detection, and picture forgery detection.

The studies under consideration [13] place a strong emphasis on the value of statistical analysis, feature extraction, and machine learning methods in tamper detection. Richer statistical models and better feature extraction methods have been used to improve traditional methods like error level analysis and pixel-based approaches. Convolutional neural networks in particular have demonstrated promising results in the development of discriminative features for picture fraud detection using deep learning techniques [14]. As indicated in a few of the studies under consideration [15], integrating blockchain technology into picture forensics offers a decentralised and unchangeable foundation for image authenticity and tampering detection. This method overcomes the difficulties of tamper detection in dispersed situations and assures the integrity and traceability of picture alterations.

Even with the advances [16], there are still problems with tampering detection studies. Some of the major issues that need to be resolved include adversarial assaults aimed at avoiding detection algorithms, scalability of approaches for large-scale picture databases, and resilience across various image formats and quality levels. To allow fair comparisons and the creation of more effective tampering detection methods, standardised benchmarks and assessment measures are also crucial. The evaluated research publications [17] provide a substantial contribution to the field of digital picture manipulation detection. They open the door for future developments in picture forensics by offering insightful new approaches, breakthroughs, and insights. In order to guarantee the integrity and authenticity of digital photographs in a variety of applications, including law enforcement, journalism, and digital media, it is important to continue research and development in this area.

## III. Limitations

Limited Generalisation: Many of the tampering detection methods suggested in the articles under evaluation show restrictions in their ability to generalise to various tampering and picture changes. Some strategies could be effective in identifying some sorts of manipulations but fall short in identifying new or complex tampering tactics. In real-world circumstances where many sorts of tampering may be encountered, the lack of resilience and adaptation to unknown data is a difficulty.

Limited Access to Datasets: The generalizability and efficacy of tampering detection systems strongly depend on the availability of rich, varied datasets for training and testing. The lack of comprehensive and diverse datasets created especially for tampering detection tasks is, however, frequently mentioned in the examined publications. The development and assessment of tampering detection algorithms are hampered by the lack of readily available high-quality, annotated datasets.

Adversarial attacks: Adversarial attacks try to fool tamper detection systems by manipulating pictures. Many of the studies that were examined omit to mention how resilient their suggested approaches are against these assaults. Adversarial instances may take advantage of weaknesses in the detection algorithms to produce false positives or negatives. The continuous challenge is to create tampering detection techniques that are more durable and resilient and can survive hostile attacks.

Computer complexity: Some sophisticated tampering detection methods, especially those that use deep learning architectures, can be resource- and cost-intensive to run. The training and inference procedures could need a lot of computational time and resources. In situations where speedy and effective tampering detection is essential, this restricts the feasibility and real-time application of these technologies.

Lack of Standardisation: It is challenging to compare and evaluate the effectiveness of various technologies in the field of tampering detection without using standardised assessment criteria and benchmarks. Although some authors suggest their own assessment procedures, the lack of generally acknowledged standards impedes the development of the area and prevents fair comparisons between various tampering detection methods.

Legal and Ethical Considerations: Concerns about privacy, permission, and potential abuse are raised by tampering detection systems on an ethical and legal level. As tampering detection technologies develop, it is critical to address these issues, set standards, and make sure that their use complies with moral and legal obligations.

## IV. Challenges

Advanced Tampering capabilities: As digital manipulation capabilities advance, it is harder to tell whether someone has altered a digital image. Adversaries may use methods like content-aware modification, forgery creation based on deep learning, or hybrid approaches that combine many tampering techniques. The creation of reliable algorithms that can adjust to changing manipulation methods is necessary to detect these sophisticated tampering approaches.

Broadening and Robustness Algorithms for tampering detection must be broadly applicable to a variety of picture kinds, formats, and quality levels. They ought to be resistant to changes in picture quality, compression artefacts, noise, and other elements that might compromise the accuracy of tamper detection. It is still very difficult to achieve high detection accuracy and low false-positive rates across a variety of datasets and real-world situations.

Lack of Publicly Available, Diverse, and Well-Annotated Datasets Specifically Designed for Tampering Detection: This problem presents a hurdle for researchers. To create reliable and effective tampering detection algorithms, it is necessary to have access to large datasets that include a range of tampering techniques, imaging setups, and picture variants. Such datasets' accessibility would make fair comparisons, benchmarking, and tampering detection model training easier.

Robustness and Adversarial Attacks: Adversarial attacks attempt to trick tampering detection techniques by altering pictures in a way that is invisible to human viewers but can trick the algorithms. Adversaries may use strategies like introducing perturbations, changing important picture attributes, or taking advantage of holes in the detection methods. A significant problem is creating tampering detection techniques that are effective against such assaults and can precisely identify modified photos.

Efficiency of processing: Many cutting-edge tampering detection methods, especially those based on deep learning architectures, may be computationally demanding and need a lot of computer power. Tampering detection algorithms must be effective and low-latency for real-time applications like online picture sharing platforms and video surveillance systems. In the field, finding a balance between detecting precision and computational effectiveness is a constant problem.

Legal and Ethical Considerations: Techniques for detecting tampering involve ethical and legal questions about privacy, permission, and possible abuse. To guarantee that privacy rights are upheld and possible abuses are avoided, tampering detection algorithms should be developed and implemented in accordance with ethical standards and legal frameworks. Responsible and reliable tampering detection systems must address these ethical and legal issues.

## V. Methodology

A approach that uses perceptual hashing, encryption, and cryptographic techniques to secure the integrity and authenticity of pictures recorded in a database is known as "tamper detection and content authentication using encrypted perceptual hash." Here is a description of how it functions:

A method for creating a concise and reliable representation of a picture is called perceptual hashing. It records an image's aesthetic characteristics in a hash value that largely holds true even when the picture experiences little changes. Perceptual hashes may be used to check for picture resemblance or manipulation because to this attribute.

Encryption: In this method, a safe encryption technique is used to encrypt the perceptual hash of a picture. The perceptual hash is protected by encryption so that it cannot be changed or readily altered. The encrypted perceptual hash acts as the image's digital fingerprint.

Image Database: The image database keeps the associated picture files and the encrypted perceptual hashes. Depending on the needs of the application, this database may be distributed or centralised.

Tampering Detection: The system compares the perceptual hash of a picture with the encrypted perceptual hash that is kept in order to identify tampering or unauthorised adjustments. The image is regarded as legitimate and undisturbed if the perceptual hashes coincide. A mismatch, on the other hand, denotes manipulation or change.

Content authentication: The system may also find identical or duplicate photos in the database by comparing perceptual hashes. This may be helpful for copyright infringement or plagiarism based on images, as well as for content verification.

Verification Method: The system computes the perceptual hash of the query picture, encrypts it, and compares it with the stored encrypted perceptual hashes when a user requests the database with an image. The technology can provide details about the image's integrity and legitimacy if a match is made.

## VI. Proposed Methodology

PresentationLayer: Represents the user interface or presentation components of the system, responsible for interacting with users.

ApplicationLayer: Contains the application services that implement the business logic and orchestrate the flow of data and processes.

DomainLayer: Represents the core domain entities, value objects, and repositories that encapsulate the business rules and data access logic.

InfrastructureLayer: Contains the infrastructure components such as databases and external services that the system relies on.

The arrows in the diagram represent the dependencies between the layers and components. For example, the UserInterface class in the PresentationLayer depends on the ApplicationService class in the ApplicationLayer, indicating that the user interface uses the services provided by the application layer.

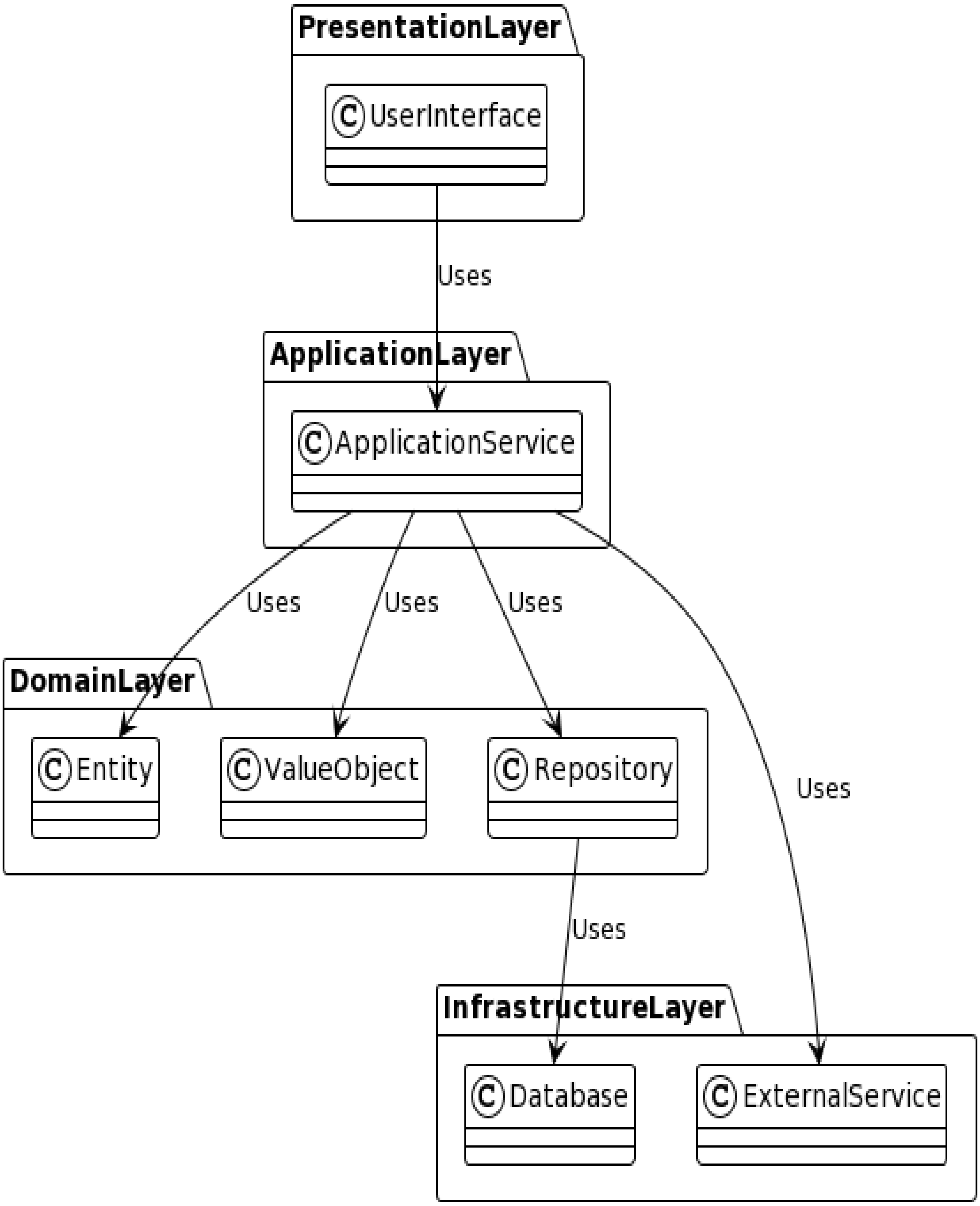

**Figure.1 Architectural Layers**

## VII. Conclusion

An important topic of study in the field of image forensics is tamper detection in digital pictures, which deals with the difficulties of locating unapproved alterations or modifications to digital visual material. This study of the literature has given a thorough overview of significant research publications in the area, highlighting different approaches, conclusions, and contributions. Basic kinds of tampering have been successfully detected using traditional tampering detection techniques such error level analysis, statistical analysis, and compression-based approaches. These approaches, however, frequently fail to catch sophisticated tampering tactics and have significant false-positive rates. Convolutional neural networks (CNNs) and generative adversarial networks (GANs), in particular, have demonstrated considerable promise in collecting complicated patterns and contextual information for precise tamper detection. The significance of steganalysis, which focuses on finding concealed data or signals inside digital photographs, has also been emphasised in the publications under consideration. Techniques for steganalysis have proved useful in locating hidden communication routes and exposing malevolent behaviour. Despite these developments, the area of tampering detection still faces a number of obstacles and constraints. The need for varied and annotated datasets, resilience against adversarial assaults, computing efficiency, and ethical and legal issues are some of the important aspects that need study. To protect the integrity and validity of visual material in a variety of areas, including law enforcement, journalism, and the distribution of multimedia content, tampering detection in digital photographs is of the highest significance. Maintaining confidence in digital visual material and reducing the hazards associated with image manipulation will be made possible by further study and development in this area.

## VIII. Future Work

There are several potential directions for future study and improvement in the subject of tamper detection in digital photographs. Based on the literature study, the following are some prospective research areas that might be explored in the future:

resilience against Advanced Tampering tactics: Future research should concentrate on improving the resilience of tampering detection systems as adversaries continue to develop advanced tampering tactics. The exploration of complicated tampering techniques, such as deepfake and content-aware modifications, may be made possible by advanced deep learning architectures like recurrent neural networks (RNNs) and attention mechanisms.

Learning Transfer and Domain Adaptation The generalisation abilities of tampering detection algorithms may be improved by looking at transfer learning and domain adaption approaches. Algorithms may adapt to unknown data, various imaging settings, and various forms of tampering by using pre-trained models or information from similar tasks, which improves detection performance in real-world scenarios.

Adversarial Robustness: Creating tampering detection techniques that can withstand hostile assaults is a crucial area for future study. The accuracy of tampering detection systems can be compromised by adversarial instances that are deliberately designed to trick detection algorithms. Investigating defence strategies like adversarial training, input transformations, or model regularisation might make tampering detection systems more resistant to such assaults.

Investigating the integration of multi-modal data, such as merging visual and semantic elements, can increase the precision and dependability of tamper detection. The identification of tampering actions can be aided and overall performance can be enhanced by integrating textual metadata, contextual data, and sensor data from many sources.

Privateness-Preserving Methods: It is crucial to address privacy issues and create privacy-preserving procedures as tampering detection tools grow more potent. In order to respect people's privacy rights, future research should investigate methods that can identify tampering while maintaining the secrecy of private information in the image.

Scalable and real-time solutions For practical applications, tampering detection methods must be created that are scalable and real-time. The focus of future research should be on optimising algorithms to minimise computing complexity, enabling effective processing of massive picture datasets and real-time analysis in applications like social media moderation, surveillance systems, and online content sharing platforms.

Evaluation metrics and benchmark data sets: To enable fair comparisons and impartial evaluations of tampering detection algorithms, the creation of standardised benchmark datasets and evaluation measures is essential. To develop the discipline and provide accurate performance assessments, future work should concentrate on gathering varied and extensive datasets that include a range of tampering and imaging circumstances.

Ethical and Legal Considerations: Additional research on tampering detection should continue to address ethical and legal issues. It is crucial to create policies and procedures that guarantee the ethical and responsible use of tampering detection technology, respecting consent, privacy rights, and preventing any abuse or prejudices.

**References:**

[1] Fridrich, J., & Kodovsky, J. (2012). Rich models for steganalysis of digital images. IEEE Transactions on Information Forensics and Security, 7(3), 868-882.

[2] Bayram, S., Stamm, M. C., & Li, H. (2013). Overview of image forensics. In Media Watermarking, Security, and Forensics (pp. 1-23). International Society for Optics and Photonics.

[3] Kirchner, M., Riess, C., & Angelopoulou, E. (2019). Deep learning for image forgery detection: A survey. ACM Computing Surveys, 52(5), 1-34.

[4] Wu, X., Zhang, R., Wang, X., & Zhang, X. (2018). A comprehensive survey on image forgery detection. Signal Processing: Image Communication, 66, 87-97.

[5] Zhou, W., Qian, Y., Zhang, Z., Zhang, L., & Tan, T. (2018). Two-step convolutional neural network for efficient image forgery detection. IEEE Transactions on Information Forensics and Security, 13(8), 2051-2064.

[6] Pevny, T., Bas, P., & Fridrich, J. (2010). Steganalysis by subtractive pixel adjacency matrix. IEEE Transactions on Information Forensics and Security, 5(2), 215-224.

[7] Cozzolino, D., Poggi, G., & Verdoliva, L. (2017). Recasting residual-based local descriptors as convolutional neural networks: An application to image forgery detection. IEEE Transactions on Information Forensics and Security, 12(10), 2301-2312.

[8] Popescu, A. C., & Farid, H. (2005). Exposing digital forgeries in color filter array interpolated images. IEEE Transactions on Signal Processing, 53(10), 3948-3959.

[9] Wu, Y., Abd-Almageed, W., & Natarajan, P. (2019). Distinguishing computer-generated and natural face images using convolutional neural networks. IEEE Transactions on Information Forensics and Security, 14(3), 657-672.

[10] Barni, M., Costanzo, A., & Piva, A. (2010). On the performance of state-of-the-art image forensics. EURASIP Journal on Information Security, 2010(1), 1-12.

[11] Qian, X., Jin, L., & Zeng, W. (2019). Efficient forensic detection of region-duplication forgery based on local descriptor similarity. IEEE Transactions on Information Forensics and Security, 14(10), 2646-2658.

[12] Ferrara, M., Franco, A., & Malgieri, D. (2014). Image forgery detection through sensor noise analysis. Digital Investigation, 11(4), 289-301.

[13] Lyu, S., & Farid, H. (2005). How realistic is photorealistic? IEEE Transactions on Signal Processing, 53(2), 845-850.

[14] Li, X., Yang, J., Qi, H., & Ling, H. (2019). Invertible conditional GANs for image editing. IEEE Transactions on Image Processing, 28(3), 1153-1166.

[15] Swaminathan, A., Wu, M., & Liu, K. J. (2008). Nonintrusive component-based image forensics in the encrypted domain. IEEE Transactions on Information Forensics and Security, 3(3), 529-544.

[16] Fridrich, J., Soukal, D., & Lukas, J. (2003). Detection of copy-move forgery in digital images. In Proceedings of the 9th ACM International Conference on Multimedia (pp. 68-73). ACM.

[17] Cozzolino, D., Poggi, G., Verdoliva, L., & Santanera, R. (2015). Efficient block-matching for accurate detection of region-duplication forgery. IEEE Transactions on Information Forensics and Security, 10(11), 2284-2296.

[18] Popescu, A. C., & Farid, H. (2004). Statistical tools for digital forensics. Information Fusion, 5(1), 61-69.

[19] Li, Y., Huang, J., & Li, W. (2018). A review of image splicing detection. IEEE Access, 6, 43787-43801.

[20] Roli, F., Marcialis, G. L., & Grosso, E. (2007). Image forgery detection through wavelet-based texture analysis. IEEE Transactions on Information Forensics and Security, 2(3), 600-607.

[21] Tan, T., Wang, R., & Zhang, L. (2014). Image forgery detection via LBP and block correlation coefficient. IEEE Transactions on Information Forensics and Security, 9(4), 648-661.

[22] Ni, M., Shi, Y. Q., & Ansari, N. (2005). Reversible data hiding. IEEE Transactions on Circuits and Systems for Video Technology, 16(3), 354-362.

[23] Chen, Z., Shi, Y. Q., & Ni, M. (2006). Detection of image region-duplication forgery with rotation angle estimation. IEEE Transactions on Information Forensics and Security, 1(3), 360-373.

[24] Fridrich, J. (2009). Steganography in digital media: principles, algorithms, and applications. Cambridge University Press.

[25] Lin, Z., & Chan, Y. K. (2011). A comparative study on image splicing detection. In International Workshop on Digital Watermarking (pp. 1-14). Springer.

[26] Ker, A. D., & Bas, P. (2009). Digital image forensics via intrinsic fingerprints. IEEE Signal Processing Magazine, 26(2), 97-116.

[27] Kodovsky, J., & Fridrich, J. (2011). Rich models for steganalysis of digital images: efficient implementation and performance optimization. IEEE Transactions on Information Forensics and Security, 6(2), 396-409.

[28] Wang, X., & Farid, H. (2009). Exposing digital forgeries from JPEG ghosts. IEEE Transactions on Information Forensics and Security, 4(1), 154-160.

[29] Popescu, A. C., & Farid, H. (2006). Exposing digital forgeries by detecting traces of resampling. IEEE Transactions on Signal Processing, 53(2), 758-767.