Review Article

ACCENTS Transactions on Image Processing and Computer Vision, Vol 8(23)
ISSN (Online): 2455-4707
http://dx.doi.org/10.19101/TIPCV.2022.823001

A review and analysis of digital image forensic techniques

Chaitanaya Singh[*] and M. Adil Hashmi
Madhyanchal professional University Bhopal, India

Received: 03-January-2022; Revised: 18-February-2022; Accepted: 20-February-2022

Abstract

In recent times, the popularity of digital photographs has increased due to their ability to convey more information than conventional image and text content. However, their easy accessibility has made ensuring their security a major concern. Therefore, serious problems can be quite challenging to minimize when testing and evaluating the validity of a study problem and identifying malevolent intruders. To address these challenges, various digital image forensics techniques have been proposed by numerous researchers to identify the forensics of an image and verify its content. The passive method and the active approach are the two most used techniques in digital forensics. In this paper, a digital image security forensics technique with different machine learning and deep learning classifiers was reviewed to demonstrate the effectiveness of the approach. The use of these techniques was explored to enhance the accuracy of digital image forensics.

Keywords

***Digital photographs, Image forensics, Security, Machine learning*.**

1.Introduction

Digital images have become an integral part of modern communication and are widely used in various fields, including social media, advertising, and journalism [1, 2]. However, with the increasing use of digital images, the issue of their security has become a major concern [3]. Digital images can be easily modified or manipulated, making it challenging to verify their authenticity and integrity. This has led to the development of digital image forensics techniques, which aim to detect and analyze the forgery in digital images [4, 5]. Passive digital image security forensics has gained prominence as a viable method owing to its efficacy and versatility among the different techniques [6–9]. The purpose of this paper is to give a concise overview of the latest developments in passive digital image security forensics, which encompasses its definition, classifications, and practical applications. The paper also highlights the importance of using advanced machine learning and deep learning algorithms to enhance the accuracy and efficiency of passive digital image forensics. The findings of this review paper can provide valuable insights for researchers and practitioners working in the field of digital image forensics.

The passive approach to digital image forensics can detect image forgeries by examining the inherent hints and identifying patterns that arise during the modification and creation of digital image content [10, 11]. This research paper aims to highlight the effectiveness of the passive forensic approach in managing image security and introduces its various applications in detecting digital image forgery. In recent times, digital images have become increasingly popular as they can convey more information compared to traditional image and text content.

Nonetheless, the simple accessibility of digital images has given rise to a notable security concern, posing a challenging problem to address. To tackle the issue of image forgery detection and image content authentication, numerous digital image forensics (DIF) methods have been proposed by developers and authors [12–15]. Digital forensics relies on two primary techniques: passive and active approaches [16]. The active forensic techniques require the identification and design of various types of fingerprints or watermarks for the image content, which are then embedded into the digital image. However, this technique necessitates watermarking all images before sharing, which is frequently unfeasible [17]. Consequently, passive approaches have gained more prominence in managing image security. By scrutinizing inherent hints and

[*] Author for correspondence

identifying patterns that occur during the creation and modification of the digital image, these approaches can detect image forgery [18–20].

The main objective of this paper is to provide an overview and critical analysis of the recent developments in the field of passive digital image security forensics, as discussed in various literatures.

This paper is organized as follows. Section 2 covers the literature review. Methodological discussion in section 3. Finally concluded in section 4.

2.Literature review

To store a digital image, there are multiple processing steps that must occur. The image is first captured using lenses that allow natural light to enter an imaging device. A color filter array (CFA) is applied to create a specific color pattern, with most cameras using the RGB system [21]. This filtered light is then converted to voltage and measured by photodetectors in the imaging area, which correspond to image pixels. Demosaicing and interpolation are then used to estimate missing color components [22]. Despite the introduction of imperfections during this process, these can be used to identify the source of the image and detect tampering [23].

Distortions can be introduced by the lens during image capture due to manufacturing and design processes. Two types of distortions are spherical aberration and chromatic aberration. Spherical aberration occurs when the camera lens does not focus on comprehending the color and various wavelengths correctly. Noise is another feature of digital camera acquisition. Photo response non-uniformity (PRNU) plays a crucial role in generating noise from the camera during image creation and modification [21]. Renewing PRNU for each captured image can help detect and address the noise problem quickly. It also includes copy-paste tampering as shown in *Figure 1*.

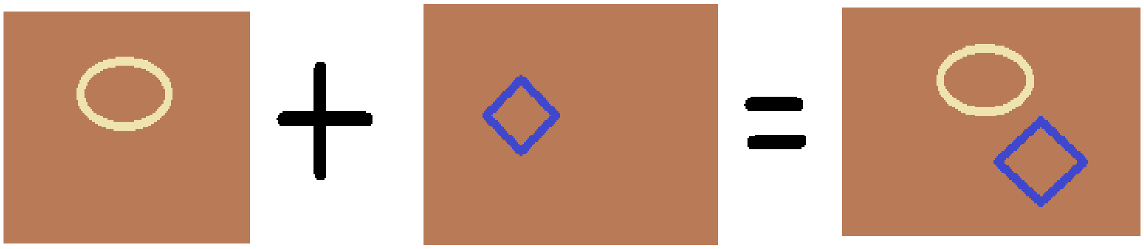

Figure 1 Tampering mechanism considering copy-paste tampering

The main purpose of utilizing lenses is to identify image forgery, which can be accomplished through various systems that capture both. A lens artifact called purple fringing aberration (PFA) has been introduced as a new method of successful extraction for this purpose. PFA's formal directions can be used as a distinctive fingerprint to detect any discrepancies in the image during the testing phase. An algorithm based on machine learning has shown improved performance in detecting both tampering and forgery [24].

Table 1 shows the outcome in terms of the analysis of the related work.

Table 1 Analysis of the related work

Reference	Result analysis
Kakkad et al., 2019[25]	The rapid progress in internet performance and speed has brought about a significant transformation in human society. Real-time storage and processing of multimedia data now depend heavily on cloud computing and its strategies. Given that images have become a major component in recent times, ensuring their security has become vital.
Karthika and Vidhya 2019[26] and Cha et al., 2018[27]	Ensuring system security has become a crucial concern in the present scenario, as failure to do so can lead to data breaches and misplacement. Various AI methods, are being employed to enhance image security.
Elkandoz et al., 2019[28]	The performance and speed improvements of the internet have significantly transformed human society. Cloud computing and its approach are essential for real-time, faster storage and processing of multimedia data. In modern times, images constitute the majority of this data, so ensuring security is crucial.
Karthika et al.,	In the current landscape, ensuring system security has become a critical priority. Otherwise, it can

Reference	Result analysis
2020[29]	result in data breaches and data loss. Nowadays, various AI techniques such as SVM, ANN, and IoT are being used to guarantee image security [30].
Babu et al., 2019[31]	The SVM and ANN classification techniques are highlighted in this study.
Shankar and Lakshmanaprabu, 2018[32]	In the current situation, digital image applications have been growing significantly compared to traditional methods. However, maintaining the security of digital images while sharing them through communication channels has become challenging. Therefore, people need to follow cryptography methods to ensure ongoing secure image communication.
Susanto et al., 2020[33]	Image encryption is a popular technique widely used for image security in recent times. In this research, the researcher proposed three encryption techniques, namely chaos-based encryption, shift-based encryption, and stream encryption.
Hasan et al., 2021[34]	The lightweight encryption technique of image security is highlighted in this study.
Arora et al., 2021[35]	The combination of image encryption and image security in a hybrid model has significantly improved digital security systems. This study provides researchers with a broader perspective on this topic.
Kumar et al., 2020[36]	This study sheds light on the importance of image security in various fields and comparative techniques. It helps researchers gather information on how image security is utilized in different contexts.

3.Discussion and analysis

The most widely used format for transporting and storing images is JPEG. This is because JPEG follows a long-established compression standard and can establish a distinct compression pattern for each image. By analyzing these patterns, it is feasible to reduce crucial forensic indicators that disclose the frequency of compression applied to an image and whether every area of the image has undergone an identical level of compression [37].

JPEG images undergo a non-overlapping division process as part of their normal compression process. The application of two-dimensional discrete cosine transformation (2D-DCT) transforms pixels to the image's frequency domain [21].

This paper provides a comprehensive analysis of passive digital image forensics. It also describes how passive approaches, with technological improvements, have developed a place in the modern world. Advances in this area have made it possible to overcome active approaches [38]. The study highlights the major aspects in the same direction [39]. The wider part of the paper has focused on these three traces, demonstrating that quality is maintained in the structure [40, 41].

The most preferred way of digital image forgery is copy-paste picture tampering, as discussed in this section. Lighting from the real environment does not effectively support an image, so artificial light is often used. This passive digital image forgery has used this lighting technique quite successfully, and they provided a detailed analysis of this advanced aspect of digital image forgery [42].

Figure 2 shows the overall analysis of the method used as covered in the literature.

4.Conclusion

Based on the preceding discussion, the lens may cause distortion that affects the captured image due to manufacturing and design processes. This distortion can take the form of spherical aberration or chromatic aberration. One-time distortion may occur if camera lenses do not focus on accurately capturing colour and different wavelengths. Noise is another challenge that arises when acquiring digital images. A key factor in the noise produced by the camera is PRNU, which can be identified and solved by renewing PRNU for each collected image. With the advancement of artificial intelligence technology, deep learning techniques have emerged as a promising solution in the field of digital forensics. Various deep learning techniques, such as deep residual networks, automatically learn features extracted from samples during training, reducing human involvement and minimizing human error. However, while deep-learning-based techniques show promise, they can also introduce issues in digital image forensics.

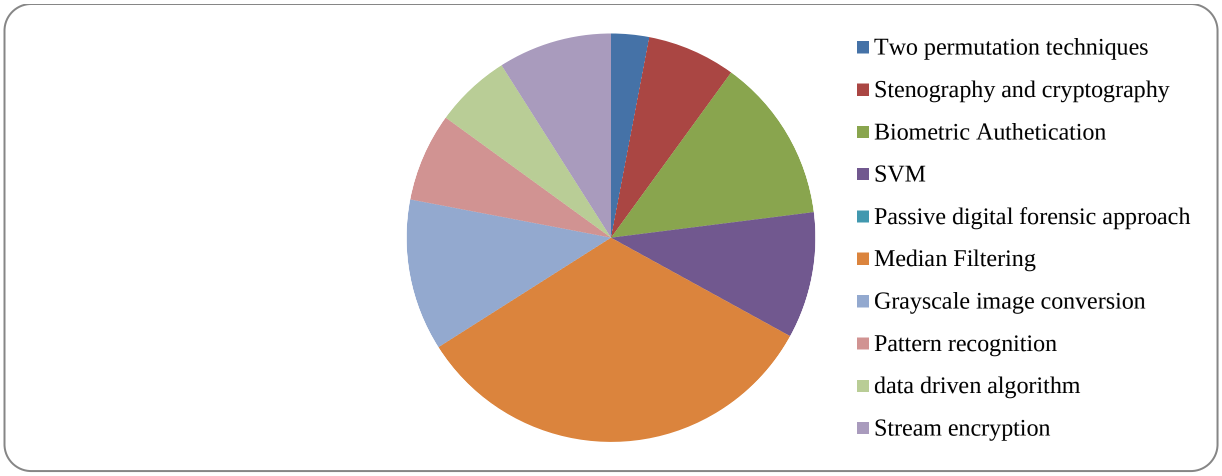

Figure 2 Forgery detection methodology used in this study

Acknowledgment

None.

Conflicts of interest

The authors have no conflicts of interest to declare.

References

[1] Zhang Y, Yan Y, Feng G. Feature compensation network based on non-uniform quantization of channels for digital image global manipulation forensics. Signal Processing: Image Communication. 2022; 107.

[2] El-Bendary MA, Faragallah OS, Nassar SS. An efficient hidden marking approach for forensic and contents verification of digital images. Multimedia Tools and Applications. 2023:1-32.

[3] Akbari Y, Al-maadeed S, Elharrouss O, Khelifi F, Lawgaly A, Bouridane A. Digital forensic analysis for source video identification: a survey. Forensic Science International: Digital Investigation. 2022.

[4] Liu K, Li J, Hussain Bukhari SS. Overview of image inpainting and forensic technology. Security and Communication Networks. 2022; 2022:1-27.

[5] Liu C. A proposal of digital image steganography and forensics based on the structure of file storage. In proceedings of the 11th international conference on computer engineering and networks 2022 (pp. 731-40). Springer Singapore.

[6] Akbari Y, Al-Maadeed S, Al-Maadeed N, Al-Ali A, Khelifi F, Lawgaly A. A new forensic video database for source smartphone identification: description and analysis. IEEE Access. 2022; 10:20080-91.

[7] Muhammad NA, Fatima R. Role of image processing in digital forensics and cybercrime detection. International Journal of Computational and Innovative Sciences. 2022; 1(1):1-4.

[8] Bernacki J, Scherer R. Digital forensics: a fast algorithm for a digital sensor identification. Journal of Information and Telecommunication. 2022; 6(4):399-419.

[9] Bansal D, Passi A. Image forgery detection and localization using block based and key-point based feature matching forensic investigation. Wireless Personal Communications. 2022:1-7.

[10] Khan AA, Shaikh AA, Laghari AA, Dootio MA, Rind MM, Awan SA. Digital forensics and cyber forensics investigation: security challenges, limitations, open issues, and future direction. International Journal of Electronic Security and Digital Forensics. 2022; 14(2):124-50.

[11] Sasubilli SM, Dubey AK, Kumar A. A computational and analytical approach for cloud computing security with user data management. In international conference on advances in computing and communication engineering 2020 (pp. 1-5). IEEE.

[12] Arava K, Paritala C, Shariff V, Praveen SP, Madhuri A. A generalized model for identifying fake digital images through the application of deep learning. In 3rd international conference on electronics and sustainable communication systems 2022 (pp. 1144-7). IEEE.

[13] Saleem M, Warsi MR, Islam S. Secure information processing for multimedia forensics using zero-trust security model for large scale data analytics in SaaS cloud computing environment. Journal of Information Security and Applications. 2023.

[14] Shahbazi Z, Byun YC. NLP-based digital forensic analysis for online social network based on system security. International Journal of Environmental Research and Public Health. 2022; 19(12).

[15] Zhu N, Liu Z. Recaptured image forensics based on local ternary count of high order prediction error. Signal Processing: Image Communication. 2022.

[16] Patil SS, Patidar K, Saxena G, Sharma N. A study and analysis of image security algorithms and the current challenges. ACCENTS Transactions on Image Processing and Computer Vision. 2021; 7(22): 1-6.

[17] Alyahya H, Ismail MM, Al-Salman A. Deep ensemble neural networks for recognizing isolated Arabic handwritten characters. ACCENTS Transactions on

Image Processing and Computer Vision. 2020; 6(21):68-79.

[18] Das D, Bose P, Ruaro N, Kruegel C, Vigna G. Understanding security issues in the NFT ecosystem. In proceedings of the ACM SIGSAC conference on computer and communications security 2022 (pp. 667-81).

[19] Rustad S, Syukur A, Andono PN. Inverted LSB image steganography using adaptive pattern to improve imperceptibility. Journal of King Saud University-Computer and Information Sciences. 2022; 34(6):3559-68.

[20] Prasanalakshmi B, Murugan K, Srinivasan K, Shridevi S, Shamsudheen S, Hu YC. Improved authentication and computation of medical data transmission in the secure IoT using hyperelliptic curve cryptography. The Journal of Supercomputing. 2022; 78(1):361-78.

[21] Lin X, Li JH, Wang SL, Cheng F, Huang XS. Recent advances in passive digital image security forensics: a brief review. Engineering. 2018; 4(1):29-39.

[22] Shuja SM, Khan RF, Shah MA, Khattak HA, Abbass A, Khan SU. On efficiency of scrambled image forensics service using support vector machine. In services–SERVICES 2019: 15th world congress, held as part of the services conference federation, SCF 2019, San Diego, CA, USA, , Proceedings 2019 (pp. 16-30). Springer International Publishing.

[23] Boato G, Dang-Nguyen DT, De Natale FG. Morphological filter detector for image forensics applications. IEEE Access. 2020; 8:13549-60.

[24] Aditya K, Grzonkowski S, Lekhac NA. Enabling trust in deep learning models: a digital forensics case study. In international conference on trust, security and privacy in computing and communications/12th international conference on big data science and engineering (TrustCom/BigDataSE) 2018 (pp. 1250-5). IEEE.

[25] Kakkad V, Patel M, Shah M. Biometric authentication and image encryption for image security in cloud framework. Multiscale and Multidisciplinary Modeling, Experiments and Design. 2019; 2:233-48.

[26] Karthika P, Vidhya SP. Image security performance analysis for SVM and ANN classification techniques. International Journal of Recent Technology and Engineering. 2019; 8(4S2):436-42.

[27] Cha S, Kang U, Choi E. The image forensics analysis of jpeg image manipulation (lightning talk). In international conference on software security and assurance (ICSSA) 2018 (pp. 82-5). IEEE.

[28] Elkandoz MT, Alexan W, Hussein HH. Double-layer image security scheme with aggregated mathematical sequences. In international conference on advanced communication technologies and networking (CommNet) 2019 (pp. 1-7). IEEE.

[29] Karthika P, Babu RG, Jayaram K. Biometric based on steganography image security in wireless sensor networks. Procedia Computer Science. 2020; 167:1291-9.

[30] Roy A, Dixit R, Naskar R, Chakraborty RS. Digital image forensics. Singapore: Springer; 2020.

[31] Babu RG, Karthika P, Elangovan K. Performance analysis for image security using SVM and ANN classification techniques. In 3rd international conference on electronics, communication and aerospace technology 2019 (pp. 460-5). IEEE.

[32] Shankar K, Lakshmanaprabu SK. Optimal key based homomorphic encryption for color image security aid of ant lion optimization algorithm. International Journal of Engineering & Technology. 2018; 7(9):22-7.

[33] Susanto A, Rachmawanto EH, Mulyono IU, Sari CA, Sarker MK, Sazal MR. Triple layer image security using bit-shift, chaos, and stream encryption. Bulletin of Electrical Engineering and Informatics. 2020; 9(3):980-7.

[34] Hasan MK, Islam S, Sulaiman R, Khan S, Hashim AH, Habib S, et al. Lightweight encryption technique to enhance medical image security on internet of medical things applications. IEEE Access. 2021; 9:47731-42.

[35] Arora H, Soni GK, Kushwaha RK, Prasoon P. Digital image security based on the hybrid model of image hiding and encryption. In 6th international conference on communication and electronics systems 2021 (pp. 1153-7). IEEE.

[36] Kumar M, Kumar S, Nagar H. Comparative analysis of different steganography technique for image or data security. International Journal of Advanced Science & Technology. 2020; 29(4): 11246-53.

[37] Barni M, Kallas K, Nowroozi E, Tondi B. On the transferability of adversarial examples against CNN-based image forensics. In international conference on acoustics, speech and signal processing (ICASSP) 2019 (pp. 8286-90). IEEE.

[38] Sun Y, Shen X, Liu C, Zhao Y. Recaptured image forensics algorithm based on image texture feature. International Journal of Pattern Recognition and Artificial Intelligence. 2020; 34(03).

[39] Yang P, Baracchi D, Ni R, Zhao Y, Argenti F, Piva A. A survey of deep learning-based source image forensics. Journal of Imaging. 2020; 6(3):1-24.

[40] Chen Y, Kang X, Wang ZJ, Zhang Q. Densely connected convolutional neural network for multi-purpose image forensics under anti-forensic attacks. In proceedings of the 6th ACM workshop on information hiding and multimedia security 2018 (pp. 91-6).

[41] Chen Q, Liao Q, Jiang ZL, Fang J, Yiu S, Xi G, et al. File fragment classification using grayscale image conversion and deep learning in digital forensics. In security and privacy workshops (SPW) 2018 (pp. 140-7). IEEE.

[42] Ferreira WD, Ferreira CB, da Cruz Júnior G, Soares F. A review of digital image forensics. Computers & Electrical Engineering. 2020.

Chaitanaya Singh is doing M.Tech in Computer Science and Engineering, Madhyanchal Professional University, Bhopal and B.Tech from RKDF College Bhopal (MP). His area of interest are data mining, machine learning and IOT.

Md Adil Hashmi is working as Assistant proffesor with the department of Computer Science and Engineering at Madhyanchal Proffessional University , Bhopal , India. He has completed his Bachelor of Engineering and Master of Technology in Computer Science Engineering from Rajeev Gandhi Technical University Bhopal (M.P). He has more than Five Publication in reputed general and conferences His reserch area in network and web security, etc.
Email:adilhashmi17@gmail.com