REVIEW PAPER

Evolving Paradigms in Digital Document Forgery Detection: From Heuristics to Multimodal

Deepika Dubey[1], Richa Rohatgi[2], Seema R. Pathak[1*]

[1]Department of Chemistry, Biochemistry and Forensic Science, Amity School of Applied Sciences, Amity University, Haryana, India
[2]LNJN NICFS, National Forensic Science University, Delhi Campus, Rohini, New Delhi, India
Corresponding Author: srpathak@ggn.amity.edu

Abstract
In this era of deepfakes, it is now easier than ever to alter the digital documents. With the concept of digitalization and rapid advancements in digital documents creation, processing and reproduction technology, the alteration of documents has become very easy to perfect. Traditionally, the main form of transmission and storage of information has been done in the form of paper documents. But nowadays, most of the documents are electronically formed for better storage and efficient processing. It has become very easy for a person to manipulate or alter any kind of digital document with the help of various easily available image processing software tools, and web-based applications. The world is still waiting for a universal method for detecting alteration in such documents. Several detection techniques and methodologies have been proposed by many scientists and researchers from various parts of the globe. This paper provides an overview of digital methods and techniques used in the detection and forensic analysis of the various kinds of digital forgery over the years.

Keywords: Deepfake, Digital Documents, Forensic Documents Examination, Digital Forensics, Digital Forgery

How to cite this article: Dubey D, Rohatgi R, Pathak SR. Evolving Paradigms in Digital Document Forgery Detection: From Heuristics to Multimodal. Int J Drug Deliv Technol. 2026;16(33s):226-235. DOI: 10.25258/ijddt.16.33s.28

Introduction

Document forgery has been an ever-growing problem for decades, but with the advancement of digital technology, it has taken on a new form.[1] Ensuring the authenticity of such records has become a big issue in today's digital era, when most records are digitally collected and paper-based documents are routinely converted from physical form to digital formats. Whether it is for legal, financial, intellectual, or personal interests, digital documents authenticity is fundamental. However, the same technology that makes it convenient to store, exchange, and retrieve data also creates new opportunities for tampering and forgeries, making the detection even more difficult.

It can be hard to work with scanned documents, especially ones that have been changed from paper to digital format. Forgeries in the past might involve changing written information like writing and/or pictures. But now, digital tools and technologies allow for even more complex changes that can be even harder to spot. Graphic editing software and image processing tools like Adobe Photoshop, CorelDraw, GIMP, and others make it easier than ever to change scanned documents in ways that look natural to the naked eye. Because of this, many types of fraud have been possible, from fake signatures and text changes to adding or removing whole parts of documents.[2] Forgeries like these can have very bad effects, so there is a growing need for reliable tools to find them. This is especially important in fields like law, banking, and education, where the legal and financial value of a document's integrity can be very high. Traditional methods of finding forgeries, such as eye inspection, ink examination, and forensic handwriting analysis, are still used, but they can't handle the complex details of current document copies used in new age forgeries. In response, experts and scientists have come up with more advanced methods that use digital forensics to make sure that documents are real and true.[3] Finding tiny hints that were left behind when the fake document was made is usually the first step in proving that a digital document is fake. These hints could include pixels that are not arranged normally, inks that are not the same colour on different parts of a paper, and scanners leaving behind patterns or noise that are not smooth.[4] As forgery tactics get better, it takes more complicated tools and methods to find these changes. Different methods, like image processing, hyperspectral imaging, and machine learning have been used by researchers to deal with different parts of document fraud where each method has its own benefit. Image processing methods can help find fakes, for instance, by looking at the structure of digital document pictures. They can spot problems down to the pixel level, like areas that have been copied or lighting and colours that don't match up, which are all signs of manipulation. Also, machine learning algorithms have made it easier to spot fakes by teaching models to find trends in papers and images that have been changed.[5] Additionally, deep learning models are now useful for finding fakes, especially when working with big data sets. These models make the discovery process faster and more reliable by letting automatic, scalable solutions work. It's very important that monitoring tools keep up with how complex forgeries are getting. Researchers are

*Author for Correspondence: srpathak@ggn.amity.edu

always coming up with new and better tools and strategies to keep up with these more advanced fake methods. Not only do these new technologies improve the accuracy of identification, they also make the process easier, which means that in real life, document authenticity can be checked faster, more effectively, and more efficiently.

This review aims to explore the timeline of these growing trends in detecting forgery in digital documents and documenting the evolution of forensic technologies throughout the time. It will focus on noteworthy research projects and discoveries to provide an overview of how the subject has advanced, highlighting key contributions that have constructed the contemporary environment. From this comprehensive review the readers will gain an in-depth understanding of both the historical context and the most recent developments, as well as insights into how forensic experts are addressing the increasing challenges of digital document manipulation.

Literature Review:

Forgery of digital documents has become a serious global issue, affecting businesses such as finance, academics, law, and government. The ease with which it has become effortless to manipulate the digital documents has resulted in issues such as identity theft, fraud, and the dissemination of misleading information. As we increasingly rely on digital documents for everyday business and transactions, ensuring their authenticity is important for maintaining trust and security. This review paper will look at how forgery detection technologies have evolved over the time, from old approaches to the most recent techniques such as machine learning, deep learning and neural networks. It will also highlight significant developments and examine the potential for future advancements in forgery detection.

Deringas (2001) discussed how graphic processing techniques can be misused and can produce digital documents that are unrecognisable and provided a case study demonstrating how to find evidence of forgery in a such digitally altered document by analysing and reconstructing the background region of the document.[6]

Cox et al. (2002) proposed the digital watermarking, an active forensic technology that embeds invisible information also known as a watermark, into media to preserve and authenticate it. The watermark is then extracted during the verification process to guarantee the media's validity. This method has been widely used to safeguard digital content.[7]

Shien and Yuan (2003) introduced digital signatures, which extract key features from the media and store them separately. Unlike watermarking, this technique does not alter the media but still allows for validation by comparing stored features with the current media state.[8]

Fridrich et al. (2003) developed an early method to detect copy-paste forgery by dividing an image into blocks and comparing them. They used two techniques: one that looked for exact matches between blocks, and another more flexible one that matched blocks based on mathematical transformations (DCT coefficients), even when parts of the image had been touched up. However, the method struggled with large areas of identical textures, making it less effective in those cases. [1]

Luo et al. (2006) created a method that divided the image into overlapping blocks and compared colour features to detect identical regions. They used colour information from both the RGB colour model and the YCbCr model. While this worked effectively in many circumstances, it struggled with photographs which has huge smooth sections or were severely deformed. The authors further proposed that human assistance will be required to manage such scenarios efficiently.[9]

Lukas et al. (2006) proposed a method for identifying forgeries in digital images based on sensor pattern noise, a unique noise fingerprint produced by imaging sensors in cameras and scanners. Their method detects discrepancies in noise patterns across image regions, indicating suspected tampering. This approach is particularly successful for identifying content alterations, especially those made to scanned documents, because it can highlight locations where content has been changed.[10]

Li et al. (2007) proposed a method for identifying duplicated regions in images, which is essential in identifying forgery in scanned documents. The authors processed images using the Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD), which allowed them to identify copied and pasted portions, a prevalent approach in image and scanned document forgeries. The method increased both accuracy and computing efficiency, making it appropriate for large-scale document processing. They also addressed challenges in detecting minor changes and alterations that may not be clearly observable using traditional approaches.[11]

Mahdian and Saic (2007) presented a method to identify the duplicated regions and proposed a technique that used overlapping blocks and blur invariants (features that remain unchanged even when the image is blurred). They employed principal component analysis to simplify the data and used the k-d tree to determine similarity. However, the biggest difficulty with the method they used was the long processing time—it took approximately 40 minutes to evaluate a moderately sized image, emphasising the need for speed improvements.. [4]

Farid (2009) provided an in-depth overview of methods and techniques for detecting digital image forgeries. The paper discussed both traditional methods and modern technologies, including tamper localization, feature-based analysis, and image processing techniques. It also covered topics such as identifying duplicated regions (copy-move forgery), splicing, and re-sampling to detect forgeries in scanned and digital documents. The work also focused on challenges in creating automated detection systems and the growing importance of forgery detection in legal and forensic contexts.[12]

Math and Tripathi (2010) discussed about the complexity of the digital forgery, challenges faced during investigation and methods to detect a digitally forged content. They majorly focussed on introduction and discussion on forgery research problems and

associated challenges in solving a forgery problem. Some of the major challenges discussed were Data provenance, ethical, legal, and institutional issues, Differentiating forgery and clarity modification, and Performance evaluation.[3]

Zhang et al. (2010) identified the forged regions by enforcing the planar homograph constraint, which accounts for variations in the appearance and position of objects depending on camera settings. To accurately outline the boundaries of the tampered regions, they used a graph cut segmentation method.[13]

Joshi et al. (2011) presented a case study describing the method of forgery detection in a machine-generated document and discussed about the challenges and future perspective of document forgery related to digitally forged documents.[14]

Christlein and Riess (2012) discussed about methods of evaluation of popular Copy-Move Forgery and various detection approaches. They analysed the detection performance on a per-image basis and on a per-pixel basis and studied the feature sets that exhibits the best robustness against various noise sources and down sampling, while reliably identifying the copied regions.[15]

Yao et al. (2011) developed a forgery detection method based on perspective geometry by analysing height ratios of objects in an image. Their approach assumed a reference plane where the objects were positioned, and any inconsistencies in these height ratios suggested possible tampering. However, the technique was limited in its ability to independently detect image splicing, highlighting the need for complementary algorithms to improve detection accuracy.[16]

Khan et al. (2013) proposed a method for detecting ink irregularities in scanned documents. The authors used hyperspectral imaging to examine the spectral features of ink, allowing them to identify small variations that would be invisible to the naked eye. This method was shown to be essential in identifying document alterations, such as forgery or tampering, because it revealed ink mismatches that occur when different writing implements or printing devices that were used. Their method improved the document authentication processes in forensic analysis.[17]

Morales et al. (2014) studied the use of hyperspectral analysis to detect various types of ink in handwritten documents. This approach allowed for the detection of small variations between inks that are not visible to the human eye, making it highly useful for identifying adjustments or forgeries in documents. By evaluating the spectral features of the ink, their method can efficiently distinguish between genuine and manipulated regions of a document, offering a non-destructive means of document authentication. This has significant implications for forensic document examination.[18]

Luo et al. (2015) used hyperspectral imaging for detection of forgeries that were limited to specific regions of a document. The authors devised a technique for identifying variations in inks and materials by analysing the spectral and spatial characteristics of document images. Their method proved to be a precise tool for detecting localised forgery by using hyperspectral analysis that can even detect small alterations that are not detectable to the human eye or conventional imaging techniques. The technique was especially helpful for identifying instances of document manipulation in official or legal documents.[19]

Mankar et al. (2015) reviewed a number of methods for detecting image forgeries, including pixel-based, partition-based, and SVM classifier. According to the authors, the multimedia authentication methods have been developed to ensure the integrity of material and stop picture forgeries.[20]

Sameria et al. (2015) researched about forensic examination of Offline Scanned Documents and Digital Images using the Digital Image Processing software MATLAB to determine the presence of alteration. They concluded that more research is needed into the analysis of alterations in offline scanned documents because there hasn't been much work done in this area.[21]

Iuliani et al. (2015) expanded on the concept of using height ratio measurements to identify forgeries in images. While their method effectively detected discrepancies in object sizes due to manipulation, they also acknowledged the challenges in detecting splicing forgeries solely with this approach. They suggested that integrating it with other detection techniques could enhance the overall effectiveness of forensic tools.[22]

Saini and Kaur (2016) studied about the forensic examination of computer-manipulated documents using image processing tools. They investigated alternations in system-generated documents, including those with printed and plain backgrounds. The documents were manipulated using image processing software applications such as Adobe Photoshop and Paint. The documents were examined for changes after being manipulated; encouraging results were obtained. The findings showed that several features were associated with image manipulation and could be easily detected using standard image processing software.[23]

Abramova and Bohme (2016) studied methods for detecting Copy–Move Forgeries in scanned text documents. They addressed the problem of detecting and localizing copy–move forgeries in images of scanned text documents with purpose of analysis to study how block-based detection of near-duplicates performs in application scenario.[24]

Asghar et al. (2017) reviewed methodology of Copy-move and splicing image forgery detection and localization. In this review paper, they presented an extensive literature review of the state-of-art techniques on copy-move and splicing forgeries, highlighted the limitations of these techniques, and discussed about the future direction in this area of research.[25]

Sadiku et al. (2017) in his research studied and discussed about digital forgery and its elements such as types of image forgeries, different types of approaches that can be taken to identify the forged images and the challenges associated with identification and analysis of forged images.[26]

Saini and Kaur (2018) described the efficient use of advanced image processing tools such as Adobe

Photoshop and MAT-LAB to identify alterations made to a digital document and demonstrated that simple software could improve the efficiency of digital fraud detection, and it is expected that such image processing software will be used by document examiners in their routine casework.[27]

Khan et al. (2019) studied a hybrid deep learning model that combines both spatial and spectral data for authenticating documents. Using hyperspectral imaging, they proposed convolutional architecture detected forgeries by analysing variations in ink and paper properties that are invisible to the naked eye. The method they used significantly improved the accuracy and reliability of forgery detection in scanned documents, especially in detecting precise alterations. The study emphasised the relevance of this approach for real-world applications such as document verification and forensics.[28]

Kumar et al. (2020) presented an end-to-end CNN model that can examine images that have been compressed, rotated, or resized in order to detect the copy-move forgeries. Using the hybrid datasets, their model's accuracy ranged from 93 to 95%.[29]

Al-Azrak et al. (2020) developed a new method for detection of forgery in images by combining trigonometric transforms with deep learning algorithms, with the goal of increasing the efficiency and accuracy of forgery detection, particularly for scanned documents. They tested their method using a sample size of 220 images (110 original and 110 modified). The findings revealed that combining transforms such as the Discrete Cosine Transform (DDCT) with the Discrete Wavelet Transform (DWT) and the Discrete Fourier Transform (DDFT) with DWT resulted in pristine accuracy (100%). However, particular approaches, such as the Discrete Sine Transform (DST) and DDFT, showed the lesser accuracy (about 60%). This work emphasised the potential of integrating mathematical transformations and deep learning for enhanced digital forensic investigation and efficient forgery detection model.[30]

James et al. (2020) studied a graph comparison approach by extracting the features of each character and evaluated algorithms of forgery detection on dataset constructed from real business documents.[31]

Khudhair et al. (2021) reviewed papers on copy-move image forgery published in reputed journals from 2017 to 2020 and focused on discussing various strategies related with fraud images to highlight on the latest tools used in the detection.[32]

Nath et al. (2021) proposed a blind image splicing detection technique using a deep convolutional residual network followed by an ANN classifier, which differentiates between real and altered images effectively.[33]

Kafali et al. (2021) presented a deep learning architecture aimed at enhancing the detection of copy-move forgeries in images. It introduced a nonlinear Volterra-based convolutional layer that combines linear and nonlinear pixel interactions to improve feature extraction. By integrating this into an Inception module, the RobusterNet effectively captured both low- and high-level features while maintaining localization accuracy. This model produced promising results, surpassing earlier used methods with only a slight increase in parameters.[34]

Al-Ameri et al. (2022) studied a new technique that employs spectral data analysis to detect forgeries in official documents. Their study examined the unique properties of ink and paper using graph-based approaches, which allowed for the detection of inconsistencies that would point to manipulation/forgery. The authors highlighted the effectiveness and efficiency of this network-based technique in enhancing the accuracy of forgery detection techniques. This approach resulted in a significant advancement in forensic document examination.[35]

Shinde et al. (2022) examined several image processing algorithms for document forgery detection that emphasized the need to counter evolving forgery methods. In order to suggest a new approach for upcoming forensic investigations targeted at enhancing detection accuracy, the authors studied and examined various forms of forgery detection techniques and then employed transform-based techniques and compared their efficacy.[5]

Mallick et al. (2022) used Convolutional Neural Networks (CNN) to identify splicing and copy-move forgeries. Using a dataset of 1000 pictures, they employed the VGG16 and VGG19 architectures, obtaining 72.9% accuracy with VGG19 and 71.6% accuracy with VGG16.[36]

Ali et al. (2022) suggested a technique that compares the differences between the original and recompressed images in order to identify forgeries using deep learning and image recompression. The validation accuracy of this approach was 92.23%.[37]

Rabah (2022) researched about analysis of scanned images & documents for checking its integrity and authenticity. The author proposed a technique to identify the origin of the scanned images & documents i.e., brand of the scanner, method through which it could be identified whether two images were acquired by same scanner or not and identified a few security mechanisms which could be used to detect the manipulated content in the scanned documents.[2]

Naglaa et al. (2023) proposed an approach that utilizes supervised deep learning to detect ink mismatches in hyperspectral document images. Using a dataset from the University of Western Australia, the model was tested with different ink mixtures of blue and black colours. The system achieved high accuracy, with 99.91% for blue ink and 97.51% for black ink, outperforming eleven previously published systems. This method's ability to identify ink mismatches and locate potential forgeries makes it a valuable tool for document forensics.[38]

Al-Ameri et al. (2023) suggested an unsupervised approach that uses graph theory and network science to identify fraudulent documents. The Laser-Induced Breakdown Spectroscopy (LIBS) technique was used to acquire the document spectrums. The improved Louvain algorithm, which performs well in four important tests,

was used for detection. The approach was computationally efficient and simple to execute, which benefits digital forensics. Other techniques were also used to test the resulting dataset in which the Updated-DBSCAN algorithm has shown better accuracy.[39]

Dubey et al. (2024) explored the challenges forensic investigators face in detecting forgery in digitally manipulated documents. They presented a real-life case where a contractor submitted a forged authorization certificate. Through visual and technical analysis, including file signature, metadata, and hash value comparison, the study identified key differences between the original and tampered documents. Their research emphasizes the importance of advanced forensic techniques to ensure document integrity in the digital age.[40]

Boonkrong (2024) addressed the need to verify the authenticity of digital academic documents, which are vulnerable to illegal modifications through editing software. He proposed a cryptographic hash function to detect alterations, focusing on data integrity. Experiments demonstrated that the system achieves 100% accuracy and a fast verification speed of 0.352 ms, outperforming conventional methods like digital signatures, CNN, and blockchain technologies. The cryptographic hash function offers an efficient solution for detecting forged academic documents.[41]

Riaz et al. (2025) proposed a dual-stream approach for detecting forged text in scanned documents by combining CNN and transformer architectures. It processes both RGB and DCT features to capture local artifacts like compression traces and global inconsistencies in document structure. They integrated a cross-attention fusion mechanism which uses these signals effectively. Tested on the DocTamper dataset, it delivers strong gains in precision, recall, and robustness, especially under heavy JPEG compression.[42]

Dubey et al. (2025) proposed a cross-modal AI framework for detecting forgeries in scanned documents by jointly analysing visual content, text, signatures, stamps, and layout. Using attention-based multimodal fusion and deep feature extraction, it identifies inconsistencies across document elements and localizes tampered regions. Experiments show improved accuracy, robustness to diverse forgery types, and near real-time performance, making it a strong candidate for reliable automated document authentication.[43]

Li et al. (2026) introduces DCLNet, a contrastive learning-based framework designed to detect and localize forgeries in document images where benign desensitization is also present. Built on a ConvNeXt encoder–decoder with global context attention, it learns multi-scale features while distinguishing subtle tampering from strong desensitization artifacts. A dedicated dataset is also proposed, with results showing improved accuracy, robustness to post-processing, and strong generalization.[44]

Table 1 provides an overview of research efforts focused on detection of digital forgery in images and documents. It also highlights the unique techniques each study employed and the specific type of forgery addressed, offering insights into the various methods developed to tackle forgery detection challenges.

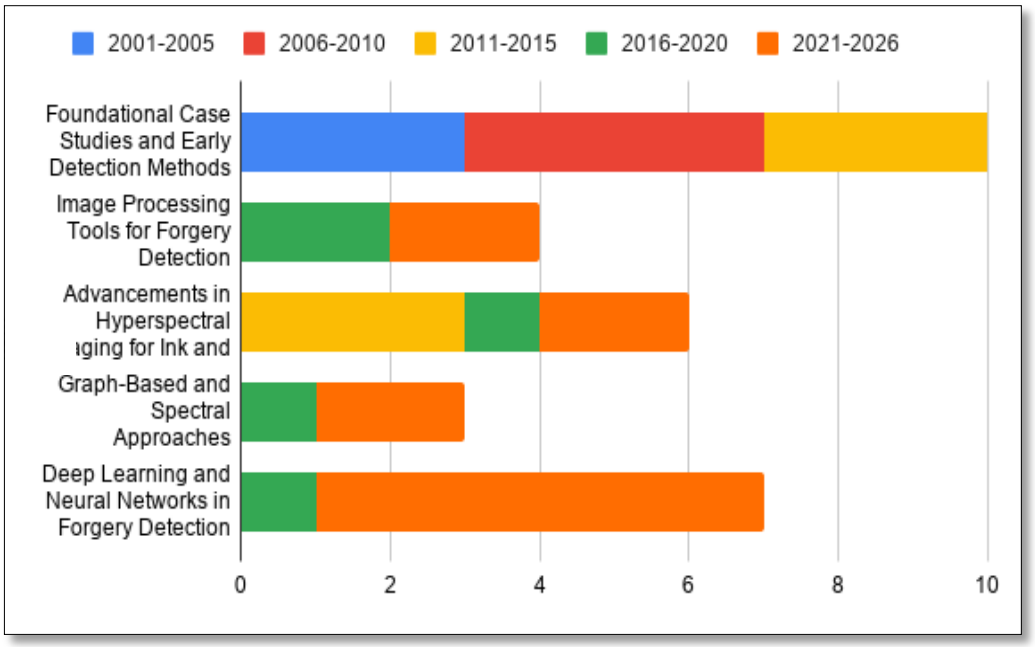
Table 1: Summary of research works on Digital Forgery (2001 to 2026)

Authors	Year of Publication	Method/Technique used to detect Forgery	Type of Forgery Detected
Deringas	2001	Digital manipulation detection	Copy-move forgery
Cox et al.	2002	Digital watermarking	Media content alteration
Shien and Yuan	2003	Digital signatures	Media content alteration
Fridrich et al.	2003	Block comparison with DCT coefficients	Copy-move forgery
Luo et al.	2006	Overlapping block colour feature analysis	Duplicate region detection
Lukas et al.	2006	Sensor pattern noise analysis	Media content alteration in scanned documents
Li et al.	2007	DWT and SVD for duplicated regions	Copy-move and splicing forgery
Mahdian and Saic	2007	Blur invariants and PCA	Copy-move forgery
Farid	2009	Overview of forensic techniques for image forgery detection	Copy-move forgery
Math and Tripathi	2010	Review of forgery challenges	General digital image forgery
Zhang et al.	2010	Planar homograph constraint	Media content alteration
Joshi et al.	2011	Case study on machine-generated docs	Media content alteration in scanned documents

Christlein and Riess	2012	Evaluation of copy-move detection	Copy-move forgery
Yao et al.	2011	Perspective geometry analysis	Height ratio inconsistencies in images
Khan et al.	2013	Hyperspectral ink analysis	Ink inconsistency detection in documents
Morales et al.	2014	Hyperspectral ink analysis	Ink inconsistency detection in documents
Luo et al.	2015	Hyperspectral analysis	Localized forgery in legal documents
Mankar et al.	2015	SVM classifier, pixel and partition-based	Copy-move and splicing forgery
Sameria et al.	2015	MATLAB-based image processing	Manipulated images (resize, rotate, compress)
Iuliani et al.	2015	Height ratio analysis	Size manipulation detection in images
Saini and Kaur	2016	Image processing tools	System-generated document forgery
Abramova and Bohme	2016	Copy-move detection in text documents	Media content alteration in scanned documents
Asghar et al.	2017	Review of copy-move and splicing detection	Copy-move and splicing forgery
Sadiku et al.	2017	Review of image forgery types	General digital image forgery
Saini and Kaur	2018	Adobe Photoshop and MATLAB tools	Copy-move forgery
Khan et al.	2019	Hybrid deep learning with hyperspectral imaging	Ink-based forgery
Kumar et al.	2020	CNN for copy-move forgery	Manipulated images (resize, rotate, compress)
Al-Azrak et al.	2020	Trigonometric transforms with deep learning	Media content alteration in scanned documents
James et al.	2020	Graph comparison for feature extraction	Copy-move and splicing forgery
Khudhair et al.	2021	Review of copy-move detection strategies	Image splicing detection
Nath et al.	2021	Deep convolutional network for splicing	Image splicing detection
Kafali et al.	2021	RobusterNet with nonlinear Volterra convolution	Copy-move forgery
Al-Ameri et al.	2022	Spectral data analysis with graph-based techniques	Copy-move and splicing forgery
Shinde et al.	2022	Review of image processing techniques	Copy-move forgery
Mallick et al.	2022	CNN with VGG16 and VGG19	Copy-move and splicing forgery
Ali et al.	2022	Deep learning with image recompression	Manipulated images (resize, rotate, compress)
Rabah	2022	Scanner origin identification & forgery detection	General digital image forgery in scanned documents
Naglaa et al.	2023	Supervised DL for ink mismatch in hyperspectral images	Ink inconsistency detection in documents
Al-Ameri et al.	2023	Unsupervised detection with network science	General digital image forgery

Dubey et al.	2024	Visual and technical analysis	Copy-move and splicing forgery
Boonkrong	2024	Cryptographic hash function	Academic document forgery
Riaz et al.	2025	Dual cross-stream fusion network combining CNN (local features) and transformer (global context) with RGB + DCT inputs and cross-attention fusion	Text manipulation, compression artifacts, structural inconsistencies in scanned documents
Dubey et al.	2025	Cross-modal AI framework using multimodal fusion (visual, text, signature, stamp, layout) with attention-based deep learning	Signature manipulation, stamp duplication, multi-layer document tampering
Li et al.	2026	DCLNet using ConvNeXt encoder–decoder, global context attention, and contrastive learning to separate tampering from desensitization	Tampering in presence of desensitization (privacy masking) and subtle pixel-level forgeries

The detection techniques above were further broadly categorized to visualize the most prevalent methods and types of forgery detected over the years. **Graph 1** illustrates the various types of forgeries prevalent over the years.



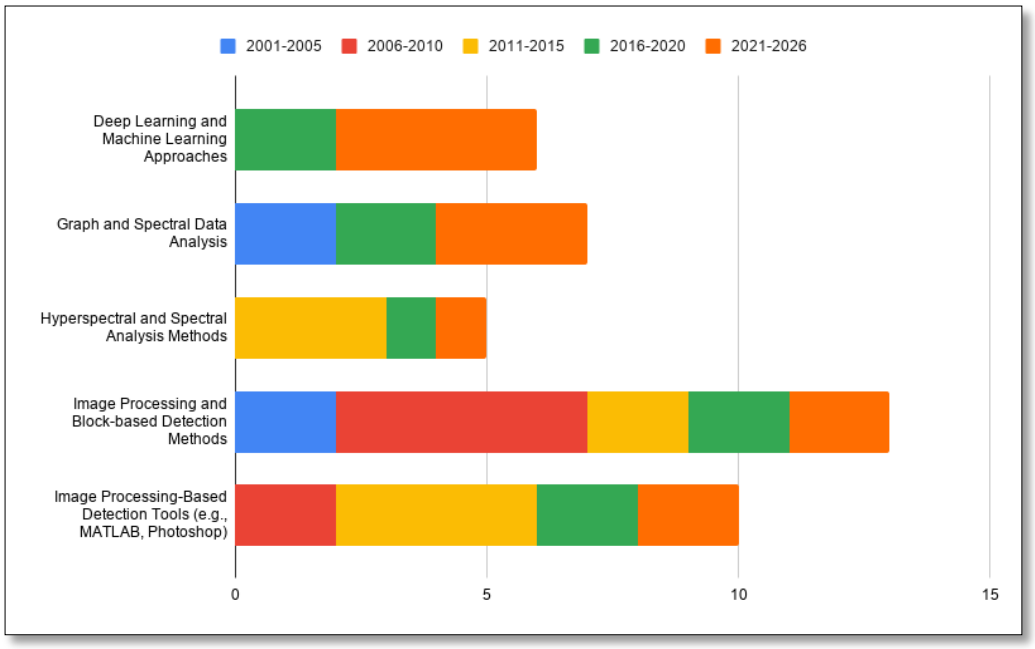
Graph 1: Common types of forgeries from the past 25 years

The reviewed studies can be broadly grouped into five categories based on the techniques used to detect various types of forgeries.

1. **Image processing based Detection Tools** includes tools and techniques such as MATLAB, Photoshop, Pixel-based analysis, etc.
2. **Image Processing and Block-based Detection** involve approaches using image blocks, feature comparison, or transforms to identify copy-move forgeries.
3. **Hyperspectral and Spectral Analysis** employ methods using hyperspectral imaging or ink spectral properties to detect document alterations.

4. **Graph and Spectral Data Analysis** include methods employing graph-based techniques, spectral data, and hashing for document integrity and authenticity mainly in scanned and printed documents.
5. **Deep Learning and Machine Learning** include approaches applying CNNs or hybrid models to detect forgery, especially in images and documents.

The below **Graph 2** illustrates the frequency of various tools, techniques, and methods employed to detect forgery in digital images and documents.



Graph 2: Forgery detection approaches from the past 25 years

Conclusion:

Based on the review of above studies it is evident that the development of forgery techniques in digital documents has progressed alongside the advancements in detection methods used to uncover these manipulations. Over the time, the forgery in digital documents has become even more sophisticated, employing various easily available digital tools and software that complicate the identification. Early detection methods mainly relied on basic techniques such as image processing methods, sensor pattern noise analysis and block-based detection methods. But as the manipulation methods evolved, so did the detection approaches, incorporating techniques like Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD). Recently, deep learning and neural networks have shown great improvement in forgery detection accuracy and efficiency, precisely identifying even minute alterations including copy-move forgeries. Forgery detection has advanced significantly with these changes from conventional approaches to the contemporary machine learning technology. Nevertheless, the growing complexity of manipulation methods still presents a challenge and emphasises the need of a thorough approach that will be able to accommodate several manipulations and technological developments. This review article offers information on such continuous problems and possible remedies for digital forgery, thereby supporting law enforcement, educational institutions, businesses, and law enforcement in effectively identifying bogus documentation.

References:

1. Fridrich, J., Soukal, D., & Lukáš, J. (2003). Detection of copy–move forgery in digital images. *Proceedings of the Digital Forensic Research Workshop*, 3(3), 55-58
2. Rabah, C.B. (2022) Analysis of scanned documents for integrity and authenticity checking. *HAL Open Science,* HAL Id: tel-03516239
3. Math, S. and Tripathi, R. C. (2010) Digital forgeries: Problems and challenges. *International Journal of Computer Applications*, vol. 5, no. 12, August 2010, pp. 9-12
4. Mahdian, B., & Saic, S. (2007). Detection of copy–move forgery using a method based on blur moment invariants. Forensic Science International, 171(2-3), 180-189.
5. Shinde, A., Patil, G., and Kumar, S. (2022) Document Image Forgery And Detection Methods Using Image Processing Techniques – A Review. *International Research Journal of Modernization in Engineering Technology and Science*, Volume:04/Issue:08/ , www.doi.org/10.56726/irjmets29313
6. Deringes, A. (2001), Traces of forgery in digitally manipulated documents. *Problems of Forensic Sciences*, vol. XLVI, 2001, 375–382

7. Cox, I. Matthew, M. J. & Jeffrey, B. A. (2002), Digital Watermarking, Morgan Kaufmann, San Mateo, CA
8. Shien, L.C. & Yuan Mark, L. H. (2003), Structural digital signature for image authentication: An incidental distortion resistant scheme, *IEEE Transactions on Multimedia*, vol. 5, no. 2, pp. 161-172
9. Luo, Jiwu Huang & Qiu 2006, 'Robust detection of region-duplication forgery in digital image', The 18th International Conference on Pattern Recognition (ICPR'06), pp. 746-749.
10. Lukáš, J., Fridrich, J., & Goljan, M. (2006), Detecting digital image forgeries using sensor pattern noise. *Proceedings of SPIE - The International Society for Optical Engineering*, 6072, 60720Y. https://doi.org/10.1117/12.659602
11. Li, G., Wu, Q., Tu, D., & Sun, S. (2007). A sorted neighbourhood approach for detecting duplicated regions in image forgeries based on DWT and SVD. *Proceedings of the 2007 IEEE International Conference on Multimedia and Expo*, 1750–1753. https://doi.org/10.1109/ICME.2007.4285025
12. Farid, H. (2009), Image forgery detection. *IEEE Signal Processing Magazine*, 26(2), 16–25. https://doi.org/10.1109/MSP.2008.931079
13. Zhang, W., Cao, Z., Qu, Y., Hou, Y., Zhao, H. & Zhang, C. (2010), Detecting and extracting the photo composites using planar homography and graph cut, *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 3, pp. 544-555
14. Joshi, M.C., Kumar, A. and Thakur, S. (2011) "Examination of a digitally manipulated – machine generated document. A case study elucidating the issue of such unwanted progenies of modern technology" *Problems of Forensic Sciences* 2011, vol. LXXXVI, 162–173, ISSN 1230-7483
15. Christlein, V., Riess, C., Jordan, J. and Riess, K. (2012) "An Evaluation of Popular Copy-Move Forgery Detection Approaches" *IEEE Transactions on Information Forensics and Security*, arXiv:1208.3665v2 [cs.CV] 26 Nov 2012
16. Yao, H., Wang, S., Zhao, Y. & Zhang, X. (2012), Detecting image forgery using perspective constraints, *IEEE Signal Processing Letters*, vol. 19, no. 3, pp. 123-126
17. Khan, Z., Shafait, F., & Mian, A. (2013). Hyperspectral imaging for ink mismatch detection. *Proceedings of the 2013 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, 10–16. https://doi.org/10.1109/CVPRW.2013.10
18. Morales, A., Ferrer, M. A., Diaz-Cabrera, M., Carmona, C., & Thomas, G. L. (2014). The use of hyperspectral analysis for ink identification in handwritten documents. *Proceedings of the International Carnahan Conference on Security Technology (ICCST)*, 1-5. https://doi.org/10.1109/CCST.2014.6987017
19. Luo, Z., Shafait, F., & Mian, A. (2015). Localized forgery detection in hyperspectral document images. *Proceedings of the International Conference on Document Analysis and Recognition (ICDAR)*, 496-500. https://doi.org/10.1109/ICDAR.2015.7333855
20. Mankar, S.K. and Gurjar, A.K. (2015) Image Forgery Types and Their Detection: A Review. *International Journal of Advanced Research in Computer Science and Software Engineering*, Volume 5, Issue 4, April 2015
21. Sameria, S., Saran, V. and Gupta, A.K. (2015) Analysis of offline scanned document and digital images for alteration through digital image processing. *International Journal of Social Relevance & Concern (IJSRC)*, ISSN-2347-9698, Volume 3 Issue 8, August 2015
22. Iuliani, M., Fabbri, G. & Piva, A. (2015), Image splicing detection based on general perspective constraints, *International Workshop on Information Forensics and Security*, (WIFS), pp. 1-6
23. Saini, K. and Kaur, S.P. (2016) Forensic examination of computer-manipulated documents using image processing techniques. *Egyptian Journal of Forensic Sciences*, Volume 6, Issue 3, September 2016, Pages 317-322
24. Abramova, S. and Böhme, R. (2016) Detecting copy–move forgeries in scanned text documents. *Electronic Imaging* 2016(8): 1–9
25. Asghar, K, Habib, Z. and Hussain, M. (2017) Copy-move and splicing image forgery detection and localization techniques: a review. *Australian Journal of Forensic Sciences*, vol. 49, no. 3, 2017, pp. 281-307
26. Sadiku, M.N.O., Musa1, S.M. and Nelatury, S.R. (2017) "Digital Forgery", *International Journal of Advances in Scientific Research and Engineering*, vol. 3, issue 4
27. Saini, K. and Kaur, S.P. (2018) "Examination of digitally manipulated documents using matlab 7.10.0 and adobe photoshop 7.0" *Problems of Forensic Sciences*, 2018, vol. 111, 31–44
28. Khan, M. J., Khurshid, K., & Shafait, F. (2019). A spatio-spectral hybrid convolutional architecture for hyperspectral document authentication. *Proceedings of the International Conference on Document Analysis and Recognition (ICDAR)*, 1097-1102. https://doi.org/10.1109/ICDAR.2019.00179
29. Sanjeev Kumar and Suneet K Gupta. (2020) A robust copy move forgery classification using end to end convolution neural network. *8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO)*, pages 253–258. IEEE, 2020
30. Al-Azrak, F. M., Ghazal, A. M., & Rihawi, W. (2020). An efficient method for image forgery detection based on trigonometric transforms and deep learning. *Multimedia Tools and Applications, 79*(47), 35137-35157. https://doi.org/10.1007/s11042-020-09195-0

31. James, H., Gupta, O. and Raviv, D. (2020) OCR Graph Features for Manipulation Detection in Documents. *Association for the Advancement of Artificial Intelligence*, arXiv:2009.05158v2 [cs.CV] 14 Sep 2020
32. Khudhair, Z.N., Mohamed, F. and Kadhim K.A. (2021) "A Review on Copy-Move Image Forgery Detection Techniques", *Journal of Physics: Conference Series*, 1892 (2021) 012010
33. Nath, S. and Naskar, R. (2021) Automated image splicing detection using deep cnn-learned features and ann-based classifer. *Signal, Image and Video Processing*, 15(7):1601–1608
34. Kafali, E., Vretos, N., Semertzidis, T., & Daras, P. (2021). RobusterNet: Improving copy-move forgery detection with Volterra-based convolutions. *Pattern Recognition Letters, 143*, 13-20. https://doi.org/10.1016/j.patrec.2021.01.003
35. Ali Al-Ameri, M., Ciylan, B., & Mahmood, B. (2022). Spectral data analysis for forgery detection in official documents: A network-based approach. *Electronics, 11*(23), 4036. https://doi.org/10.3390/electronics11234036
36. Mallick, D., Shaikh, M., Gulhane, A. and Maktum, T. (2022) Copy move and splicing image forgery detection using cnn. *ITM Web of Conferences*, volume 44, page 03052. EDP Sciences
37. Ali, S.S., Iyappan Ganapathi, I., Vu, N., Ali, S. D., Saxena, N. and Werghi. N. (2022) Image forgery detection using deep learning by recompressing images. *Electronics*, 11(3):403
38. Naglaa F. EL Abadya, Hala H. Zayeda,b, Mohamed Taha (2023) An efficient technique for detecting document forgery in hyperspectral document images. Alexandria Engineering Journal 85 (2023) 207–217
39. Al-Ameri, M.A.A.; Mahmood, B.; Ciylan, B.; Amged, A. Unsupervised Forgery Detection of Documents: A Network-Inspired Approach. *Electronics* **2023**, *12*, 1682. https://doi.org/10.3390/ electronics12071682
40. Dubey, D., Rohatgi, R., & Pathak, S. R. (2024) Unveiling Digital Document Manipulation: A Case Study in Forensic Examination. Indian Journal of Forensic Medicine and Toxicology/ Volume 18 No. 2, April-June 2024
41. Boonkrong, S. (2024) Design of an academic document forgery detection system. *Int. j. inf. tecnol.*, https://doi.org/10.1007/s41870-024-02006-6
42. Riaz, N., Agne, S., Dengel, A., & Ahmed, S. (2025). DocForgeNet: Dual cross-stream fusion network for robust forgery detection in scanned documents. In Document Analysis and Recognition – *ICDAR 2025: 19th International Conference*, Wuhan, China, September 16–21, 2025, Proceedings, Part IV (pp. 329–346). Springer. https://doi.org/10.1007/978-3-032-04627-7_19
43. Dubey, D., Rohatgi, R., & Pathak, S. R. (2025). Cross-modal AI-based system for detecting forgery in scanned documents. *Journal of Applied Bioanalysis, 11*(S6), 458–471. https://doi.org/10.53555/jab.v11si6.1815
44. Li, W., Li, B., Zheng, K., Li, S., & Li, H. (2026). Document image forgery detection and localization in desensitization scenarios. *Signal Processing, 238*, 110123. https://doi.org/10.1016/j.sigpro.2025.110123