Xournals

Academic Journal of Forensic Sciences

ISSN: 2581-4273 | Volume 07 | Issue 01 | April-2024

Digital Image Forgeries and their Detection Techniques – A Review

Manju[1]

Available online at: www.xournals.com

Received 3rd April 2024 | Revised 12th April 2024 | Accepted 25th April 2024

Abstract:

Currently, the world is moving towards digitalization extensively with which crime or forgery related to digital documents, images, and autographs also are growing with plenty of intelligence. Because of the vacuity of advanced result digital cameras, hi-tech and sophisticated personal computers, and powerful software and hardware tools within the image editing and manipulating field, it becomes conceivable for anyone to produce, alter, and modify the contents of a digital image and to violate its legitimacy. Fake and duplicate images are numerous times used to gain popularity in social media and journals. Numerous cases are noted regarding the defaming of businesses similar to political leaders by exploiting fake photos and videos. Digital image forensics aims at confirming the genuineness of images by sicking information about their past. Two important questions are addressed: The first one is the identification of the imaging device that captured that image, and the second one is, therefore, the identification of traces of forgeries. In this review paper, the author reviews the various image forgery detection techniques along with their results.

Keywords: *Digitalization, Video forgery, digital forensic, forgery, traces of forgery, DWT and SIFT optical flow, etc.*

Authors:

1. *Intern, Sherlock Institute of Forensic Science, Delhi, INDIA.*

Introduction

In today's digital landscape, images serve as potent communicative tools across various sectors, from journalism to medicine. However, the widespread use of digital imagery has opened the door to image forgery **(Sharma, 1990)** facilitated by advanced editing software and high-resolution cameras. This presents a pressing challenge to image authenticity and security. Digital forensics **(Sharma, 2017)** has emerged as a crucial field, offering techniques to authenticate images and detect manipulation. As technology evolves, ensuring the legitimacy of digital images becomes paramount. In response, researchers are continuously developing innovative methods to safeguard image integrity. Despite the convenience and versatility of digital imagery, the threat of forgery underscores the importance of robust security measures and vigilant verification processes. Addressing these challenges is essential to maintaining trust and reliability in the digital realm.

Digital image

Images are electronic representations of visual information in the form of pixels. Digital images are composed of pixels, tiny squares containing colour and brightness information. They are created by digital cameras, scanners, or software programs. Image files come in formats like JPEG, PNG, GIF, TIFF, and BMP, each with different compression, quality, and compatibility characteristics **(Sharma, 1990).**

Digital forensics

Digital forensics, also known as computer forensics, is the practice of collecting, analysing, and preserving electronic data to be used as evidence in criminal or civil investigations. It involves the use of specialized techniques and tools to extract data from digital devices, such as computers, smartphones, and other digital storage media **(Sharma, 2017).**

The process typically comprises numerous steps, including:

1. **Identification and seizure of digital devices:** Investigators must identify all relevant digital devices that may contain relevant data, and then seize them in a manner that preserves the integrity of the data.

2. **Preservation of evidence:** Investigators must ensure that the data on the seized devices is not altered or destroyed in any way during the investigation.

3. **Analysis of data:** Investigators must analyse the data on the seized devices to determine their relevance to the investigation and to extract any potential evidence.

4. **Presentation of findings:** Investigators must present their findings clearly and concisely so that are admissible in court.

Digital image forgery

Digital image forgery, also known as image manipulation, is the process of altering a digital image to create a new, falsified image and deceiving the viewer into believing that the image is authentic. This can involve adding, removing, or modifying elements within the image, and is typically done to deceive or mislead viewers. Image forgery suggests the manipulation of the digital image to hide some meaningful or helpful information about an image. There are numerous cases when it is tough to recognize the edited region from the original image. The identification of forged images is determined by the need for legitimacy and to preserve the integrity of the image.

Types of digital image forgery

There are several methods of digital image forgery, including:

1. **Copy-pasting:** This involves taking elements from one image and pasting them onto another, creating a new image that appears to be authentic. Usually duplicated areas are enlarged, contracted, or tilted to make forgery extra convincing, making it tougher to distinguish forgery images **(Katzenbeisser and Fabien, 2000)**.

2. **Image splicing:** This involves taking two or more images and merging them to create a new image that appears to be authentic. The splicing methodology is a sort of falsification process, conjointly referred to as image composition for the reason that it is the process of combining two or more images to create a single image **(Rosales-Roldan *et al.*, 2013).**

3. **Image retouching:** This involves altering the appearance of an image by adjusting its colour, contrast, or other visual attributes. Image retouching forgery is well-thought-out as a marginally harmful form of digital image. An original image doesn’t alter substantially however certain aspects of the original image have been reduced. The use of such type of techniques to manipulate the image for famous journals is most common.

4. Deepfakes: This involves using artificial intelligence and machine learning algorithms to create highly realistic fake images and videos.

Digital image forgery detection

The methods used to recognize the forensic changes made are acknowledged as forgery detection (FD) techniques. Image forgery detection techniques include analysing metadata, examining lighting/shadow inconsistencies, and using software tools to detect anomalies in pixel data. A study suggests identifying statistical artefacts in pixel value histograms as intrinsic fingerprints of forgery. Models of original and forged image histograms are compared to detect diagnostic features of pixel value mapping. Various methods in image forensics focus on recognizing tampered images, leveraging developments in the field. Recent developments in image forensics have given upliftment to numerous methods for the recognition of tampered images. Here are some Image forgery detection techniques. Here is a generalized scheme for image forgery identification:

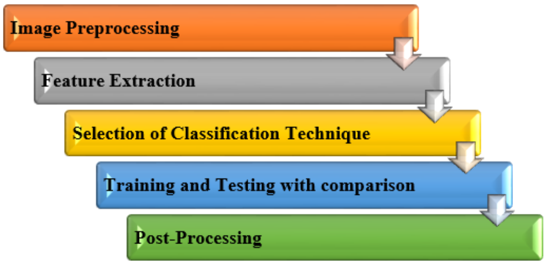
Image Preprocessing
Feature Extraction
Selection of Classification Technique
Training and Testing with comparison
Post-Processing

Figure No. 1: Generalized Schema for Image Forgery Identification

1. Image Pre-processing: The first step is to pre-process the image to make it suitable for further analysis. This can include tasks such as resizing, cropping, and noise reduction. Depending on the calculation, this step might be included in the algorithms being analysed at this point **(Makandar and Bhagirathi, 2015)**.

2. Feature Extraction: The following step is to extract features from the image. Features can be divided into two categories: global and local. While local features concentrate on particular areas of the image, global features take into account the complete picture. The choice of features for each class divides the picture set from other classes while remaining consistent for the chosen class in the interim **(Phkan and Borah, 2014)**.Some popular feature extraction techniques include Scale-Invariant Feature Transform (SIFT), Speeded Up Robust Feature (SURF), and Local Binary Pattern (LBP).

3. Selection of Classification Technique: the next step after feature extraction is to choose a classification method. The classifier will perform better because of the vast training data **(Munirah *et al.*, 2016; Sutthiwan *et al.*, 2010).** Some popular techniques for image forgery detection include Support Vector Machines (SVM), Artificial Neural Networks (ANN), Random Forests, and Decision Trees.

4. Training and Testing: In this step, the chosen classification system is trained using a dataset of real and altered photos. A second batch of real and altered photos is used to test the trained model. The sole goal of classification is to establish whether or not the image is original. For this, classifiers such as neural systems **(Lu and Huang, 2008)**, LDA (**Fang *et al.*, 2009),** and SVM (**Fu *et al.*, 2006)** are employed.

5. Post-Processing: The output from the classification model is post-processed in the last step. Tasks like thresholding, clustering, and post-classification filtering can fall under this category. Some forgeries may call for post-processing, including modifications like copy locale localization (**Gopi *et al.*, 2006; Christlein *et al.*, 2013)**

Types of Digital Image Forgery Detection Techniques

Active and passive forgery identification techniques are two broad categories of techniques used in digital image forgery detection.

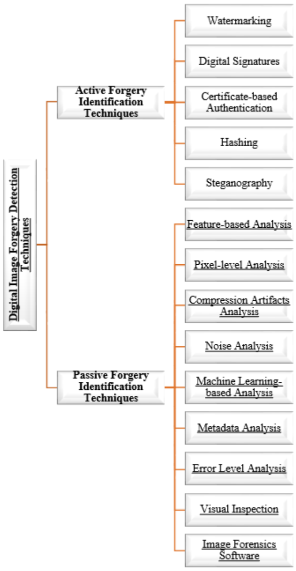
Digital Image Forgery Detection Techniques
Active Forgery Identification Techniques
Watermarking
Digital Signatures
Certificate-based Authentication
Hashing
Steganography
Passive Forgery Identification Techniques
Feature-based Analysis
Pixel-level Analysis
Compression Artifacts Analysis
Noise Analysis
Machine Learning-based Analysis
Metadata Analysis
Error Level Analysis
Visual Inspection
Image Forensics Software

Figure No. 2: Types of Digital Image Forgery Detection Techniques

1) Active Forgery Identification Techniques

Active forgery identification techniques involve adding information to the image to detect any modifications or alterations made to the image. this technique involves pre-removed or pre-implanted evidence. This technique involves identifying the source of an image, such as the camera or device used to capture it. This can help determine if an image has been tampered with or manipulated. Active forgery identification techniques (**Katzenbeisser and Petitcolas, 2000; Cox *et al.*, 2002)** involve the use of watermarking (**Lin and Chang, 1998; Lu and Liao, 2003),** digital signatures (**Shieh *et al.*, 2006; Chamlawi *et al.*, 2010)**and other methods to embed information into an image that can be used to identify the authenticity of the image. Here are some commonly used active forgery identification techniques:

- **Watermarking:** Watermarking is the process of embedding a hidden message or signal into an image. This message can be used to identify the owner of the image, track the distribution of the image, and detect any tampering or forgery. There are different types of watermarking techniques, including visible and invisible watermarking, and robust and fragile watermarking (**Rosales *et al.*, 2013)**

- **Digital Signatures:** Digital signatures are used to verify the authenticity of an image and ensure that it has not been tampered with. A digital signature is created using a private key and can only be verified using a public key. It's a mathematical technique proposed to solve the delinquency of tampering and impersonation in digital communications. This method is commonly used for the secure transmission of images.

- **Certificate-based Authentication:** Certificate-based authentication involves the use of a trusted third-party certificate authority to issue and verify digital certificates for images. These certificates are used to authenticate the origin and authenticity of the image.

- **Hashing:** Hashing is a technique used to generate a unique digital fingerprint of an image. The hash can be used to verify the integrity of the image and detect any tampering or forgery.

- **Steganography:** Steganography is the process of hiding information within an image. This technique can be used to embed a hidden message or signal into an image that can be used to identify the authenticity of the image.

It is important to note that active forgery identification techniques involve the modification of the original image, and therefore can potentially affect the quality and visual appearance of the image. Additionally, active forgery identification techniques may not be effective for detecting forgeries that involve the manipulation of the image at a pixel level.

2) Passive Forgery Detection Techniques

- Passive methods, conjointly called blind methods, simply use the picture itself for its authentication examination (**Ng *et al.*, 2006; Luo *et al.*, 2007; Farid *et al.*, 2006)**. Passive forgery detection techniques involve analysing the image itself, without modifying it, to detect signs of forgery. This methodology assumes that although there may be no visual clues of interference in the image. However, meddling might disturb the underlying statistics property because of the Noise inconsistency (**Mahdian and Saic, 2009),** Blurring of the image (**Cao *et al.*, 2007),** Image sharpening (**Zhao *et al.*, 2009),** Forgery through copy-move (**Peng *et al.*, 2011)** and Image in painting (**Zhao *et al.*, 2013),** etc. passive methodology comprises of image retouching image splicing, and copy-move tempering. Here are some commonly used passive forgery detection techniques:

- **Noise Analysis:** Image noise is a type of random variation that occurs in the brightness or colour of pixels in an image. Noise analysis techniques involve analysing the noise pattern in an image to detect any inconsistencies or anomalies that may indicate tampering or forgery.

- **Compression Artifacts Analysis:** Compression artifacts are introduced when an image is compressed using lossy compression techniques such as JPEG. These artifacts can be analysed to detect any inconsistencies or anomalies that may indicate tampering or forgery.

- **Pixel-level Analysis:** Pixel-level analysis involves analysing the individual pixels in an image to detect any inconsistencies or anomalies that may indicate tampering or forgery. This can include tasks such as analysing the colour distribution of pixels, detecting duplicated or cloned regions of an image, and detecting any splicing or merging of different images.
- **Feature-based Analysis:** Feature-based analysis involves analysing specific features of an image, such as edges, corners, or texture, to detect any

inconsistencies or anomalies that may indicate tampering or forgery. This can include tasks such as detecting any inconsistencies in the lighting or shadow patterns in an image.

- **Machine Learning-based Analysis:** Machine learning-based analysis involves training a classification model on a dataset of genuine and tampered images. The trained model can then be used to detect any inconsistencies or anomalies in an image that may indicate tampering or forgery.

- **Error level analysis:** This technique involves analysing the compression artifacts in an image to determine if it has been manipulated. When an image is compressed, the image quality is reduced, and compression artifacts are introduced. These artifacts can reveal if an image has been manipulated.

- **Metadata analysis:** Image metadata contains information about the camera or device used to capture the image, including the date and time of capture, camera settings, and GPS location. Analysing metadata can help determine if an image has been altered or manipulated.

- **Visual inspection:** A trained forensic examiner can visually inspect an image to detect signs of manipulation, such as inconsistencies in lighting, shadows, and reflections.

- **Image forensics software:** There are several software tools available that use sophisticated algorithms to analyse images for signs of manipulation, including copy-pasting, splicing, and retouching.

It is important to note that the success of passive forgery detection techniques depends on the quality of the image and the specific type of forgery being detected. Different techniques may be more effective for detecting different types of forgeries, and a combination of techniques may be necessary to achieve high accuracy.

I. Copy-Move Forgery Detection Techniques

Copy-move forgery is a sort of image forgery in which a component of an image is copied and pasted to another area of the same image to duplicate the content. The duplicated image is acquired from a closely related image, making it extremely difficult to spot this kind of fabrication (**Ardizzone *et al.*, 2010; Soloria *et al.*, 2011)** Some methods that are frequently used to spot copy-move fraud include the following:

1. **Block-based matching:** This technique divides the image into small blocks and compares them to find similar blocks. If two or more blocks have a high degree of similarity, then they are considered to be copied from each other.

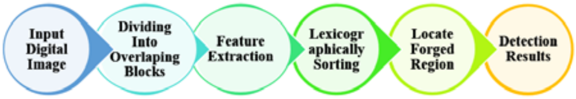

Figure No. 3: The basic approach of block matching techniques for copy-move image forgery identification.

2. **Key point-based matching:** This technique identifies key points in the image and matches them to find the duplicated regions. The key points are usually detected using techniques such as SIFT, SURF, or ORB.

3. **Phase correlation:** This technique involves calculating the Fourier transform of the image to obtain the phase correlation between different regions. If two regions have a high degree of phase correlation, then they are considered to be copied from each other.

4. **DCT-based method:** This technique converts the image into its Discrete Cosine Transform (DCT) domain and identifies similar DCT coefficients in different regions of the image (**Soloria *et al.*, 2011).**

5. **Grid-based method:** This technique divides the image into grids of different sizes and compares the histograms of the grids to find similar regions.

6. **Deep learning-based method:** This technique uses convolutional neural networks (CNNs) to automatically learn the features that distinguish between genuine and tampered images. The CNN can be trained on a large dataset of genuine and tampered images to identify copied regions.

7. **The brute force approach:** This technique relies on autocorrelation and exhaustive search. A picture is used to assess matching segments with circularly shifted versions during a thorough search. Due to the sheer volume of comparisons, it does, its computational unpredictability is considerable. The location change is determined by autocorrelation.

II. Image splicing forgery detection

Image Splicing includes the convergence of at least two pictures to create a fake image. If the pictures with contrasting foundations are combined then it turns out to be extremely hard to make the borders and boundaries incoherent (**Moghaddasi *et al.*, 2014; Ibrahim *et al.*, 2015).** Here are some commonly used techniques for Image splicing forgery detection

1) Inconsistency Analysis: This technique analyses the inconsistencies in colour, texture, and lighting between different regions of the image to identify potential splices. It compares the statistical properties of the regions, such as mean and variance, to identify significant differences that may indicate splicing.

2) Compression Artifacts: When an image is spliced together, the compressed image may have different artifacts in different regions. This technique analyses the compression artifacts, such as blocking and ringing, to identify potential splices. The artifacts in the different regions of the image are compared to identify inconsistencies.

3) Correlation Analysis: This technique analyses the correlation between different regions of the image to identify potential splices. If two regions of an image have been spliced together, the correlation between them may be lower than expected. Correlation analysis can be performed in both the spatial and frequency domains.

4) Texture Analysis: This technique analyses the texture properties of different regions of the image to identify potential splices. If two regions of an image have been spliced together, the texture properties may be significantly different. Texture analysis can be performed using features such as Local Binary Patterns (LBP) and Gabor filters.

5) Deep Learning: Deep learning techniques can be used to learn features and patterns of spliced images from a large dataset. A convolutional neural network (CNN) can be trained on a dataset of spliced and authentic images to detect splices in new images. This technique can be effective in detecting sophisticated splicing techniques but requires a large dataset for training.

III. Image Retouching Forgery Detection

Image retouching forgery detection techniques are used to identify if an image has been manipulated or altered in any way. Several techniques can be used for this purpose, including:

1. Image Metadata Analysis: Image metadata is information stored in an image file that includes details such as the camera model, date and time of capture, and location. This information can be used to verify the authenticity of an image.

2. Error Level Analysis (ELA): ELA is a technique that highlights the areas of an image that have been altered by calculating the difference in error levels between the original and compressed versions of the image.

3. Image Forensics: Image forensics is a technique that uses statistical methods to analyse the patterns of an image to determine if it has been manipulated. This technique can be used to detect image tampering such as cloning, retouching, and compositing.

4. Edge Detection: Edge detection techniques can be used to detect the boundaries between different regions in an image. If an image has been manipulated, the edges in the altered regions may not match those in the original regions.

5. Fourier Analysis: Fourier analysis is a mathematical technique that can be used to analyse the frequency components of an image. This technique can be used to detect any irregularities in the image that may indicate manipulation.

6. Machine Learning: Machine learning techniques can be used to train algorithms to detect specific types of image manipulation. This technique involves analysing a large dataset of manipulated and non-manipulated images to identify patterns that can be used to detect manipulation.

IV. Deep Fakes Forgery Detection

Deep fake forgery detection techniques are used to identify when an image or video has been manipulated using deep learning techniques to create a fake representation of a person or event. Here are some commonly used techniques:

1. Face Detection and Recognition: This technique uses face detection and recognition algorithms to identify the presence of a manipulated face in an image or video. The algorithms compare the manipulated face to a database of known faces to determine if the face is authentic or fake.

2. Lip Sync Analysis: When a video has been manipulated to create a deep fake, the audio may not match the movement of the lips in the video. Lip sync analysis uses machine learning algorithms to identify inconsistencies between the audio and visual components of the video.

3. GAN-based Detection: Generative Adversarial Networks (GANs) are commonly used to create deep fakes. GAN-based detection techniques use similar networks to detect the presence of a deep fake. The network is trained on a dataset of real and fake images to identify the features that distinguish between the two.

4. Motion and Style Analysis: Deep fakes may exhibit unnatural motion and style characteristics that differ from authentic videos. This technique analyses the motion and style properties of the video to identify potential deep fakes. It uses machine learning algorithms to identify inconsistencies between the manipulated video and authentic videos.

5. Metadata Analysis: When a deep fake is created, metadata such as the creation date, software used, and location may differ from the metadata of the original image or video. Metadata analysis compares the metadata of the manipulated image or video to the metadata of the original to identify potential deep fakes.

V. Image Forgery Detection Using Jpeg Artifacts

Most digital cameras export JPEG document format. Manipulation of image content and cropping are the attacks that can be performed on JPEG images JPEG compression is a lossy compression technique used to reduce the file size of images. When an image is compressed using JPEG, it introduces certain artefacts that can be used to detect image forgery. Here is a general overview of how JPEG artifacts can be used for image forgery detection techniques:

1. **JPEG Compression:** The first step is to compress the image using JPEG. The compression level and quality factor should be selected to produce a high-quality image with enough artifacts for detection.

2. **Extraction of Artifacts:** The next step is to extract the artifacts from the compressed image. JPEG artifacts are introduced due to quantization, DCT, and Huffman coding. Artifacts such as blocking, ringing, and blurring can be extracted from the image.

3. **Feature Extraction:** After artifact extraction, features are extracted from the image. These features can be either handcrafted or learned using deep learning techniques. Handcrafted features include statistical features such as mean, variance, and entropy, while deep learning features can be learned from a convolutional neural network (CNN).

4. **Training and Testing:** The features extracted from the compressed images are used to train a classification model, such as SVM or Random Forest. The trained model is then tested on a new set of images to detect forgery.

5. Post-Processing: The final step is to post-process the output of the classification model to refine the results. This can include tasks such as thresholding, clustering, and post-classification filtering.

It is important to note that the success of JPEG artifact-based forgery detection depends on the quality of the compressed image and the selection of appropriate features. Additionally, JPEG artifact-based forgery detection is limited to detecting forgeries that involve JPEG compression and may not be effective for other types of forgeries. Double JPEG compression detection, DCT coefficient analysis, and quantization noise analysis are effective for detecting copy-move forgeries that involve JPEG recompression but may have limitations in handling low-quality JPEG images or legitimate JPEG compression. JPEG ghost detection is effective for detecting region duplication with different compression levels but may also produce false positives in legitimate JPEG compression. Computational efficiency and performance accuracy should also be taken into consideration when selecting the appropriate technique for a specific application.

Conclusions

In this paper, I have examined several researchers' research on digital image forgery detection methods. This study presented some of the strategies and contrasted them according to their benefits and drawbacks. Every author examined various issues and methodologies, but I've discovered that these methodologies are used with photos. The research can only be expanded to include audio and video. Currently, no method can distinguish between deliberate forgeries and simple retouching, such as artistic manipulation. The most difficult task is to create a unified algorithm that can recognize every kind of forgery. It is significant to highlight that no single technique is ideal for identifying all varieties of copy-move forgery, and better results might be obtained by combining many distinct strategies. Key-point-based techniques can be more computationally expensive, but they are typically more reliable than block-based strategies.

List of Abbreviations:

1. **DWT-** Discrete Wavelet Transform
2. **SIFT-** Scale Invariant Features Transform
3. **JPEG-** Joint Photographic Experts Group
4. **SURF-** Speed Up Robust Features

References:

Ardizzone, E., A. Bruno, et al. "Copy-Move Forgery Detection via Texture Description." ACM Workshop on Multimedia in Forensics, Security, and Intelligence, 2010.

Cao, G., Y. Zhao, and R. Ni. "Edge-Based Blur Metric for Tamper Detection." Proceedings of the IEEE International Conference on Image Processing, 2007.

Chamlawi, R., A. Khan, and I. Usman. "Authentication and Recovery of Images Using Multiple Watermarks." Computers and Electrical Engineering, 2010.

Christlein, V., C. Riess, J. Jordan, and E. Angelopoulou. "An Evaluation of Popular Copy-Move Forgery Detection Approaches." IEEE Transactions on Information Forensics and Security, 2012.

Cox, I.J., M.L. Miller, et al. Digital Watermarking. Morgan Kaufmann, 2002.

Fang, Z., S. Wang, and X. Zhang. "Image Splicing Detection Using Camera Inconsistency." International Conference on Multimedia Information Networking and Security, 2009.

Farid, H. "A Survey of Image Forgery Detection." IEEE Signal Processing Magazine, 2006.

Fu, D., Y. Shi, and W. Su. "Detection of Image Splicing Based on Hilbert Huang Transform and Moments of Characteristic Functions with Wavelet Decomposition." International Workshop on Digital Watermarking, 2006.

Gopi, E., N. Lakshmanan, et al. "Digital Image Forgery Detection Using Artificial Neural Network and Autoregressive Coefficients." Canadian Conference on Electrical and Computer Engineering, 2006.

Ibrahim, R.W., Z. Moghaddasi, et al. Noor. "Fractional Differential Texture Descriptors Based on the Machado Entropy for Image Splicing Detection." International Journal of Computer Science Issues, 2015.

Katzenbeisser, S., and F.A. Petitcolas, editors. Information Hiding Techniques for Steganography and Digital Watermarking. Artech House, 2000.

Katzenbeisser, Stephan, and Fabien Petitolas. “Information Hiding Techniques for Steganography and Digital Watermaking.” EDPACS, vol. 28, no. 6, Dec. 2000.

Lin, C.Y., and S.F. Chang. "Generating Robust Digital Signature for Image/Video Authentication." Multimedia and Security Workshop at ACM Multimedia, 1998.

Lu, C.S., and H.Y. Mark Liao. "Structural Digital Signature for Image Authentication: An Incidental Distortion Resistant Scheme." IEEE Transactions on Multimedia, 2003.

Lu, W., W. S. un, and J.W. Huang. "Digital Image Forensics Using Statistical Features and Neural Network Classifiers." International Conference on Machine Learning and Cybernetics, 2008.

Luo, W., Z. Qu, F. Pan, and J. Huang. "A Survey of Passive Technology for Digital Image Forensics." Frontiers of Computer Science in China, 2007.

References:

Mahdian, B., and S. Saic. "Using Noise Inconsistencies for Blind Image Forensics." Image and Vision Computing, 2009.

Makandar, Aziz, and Bhagirathi Halalli. “Image Enhancement Techniques Using Highpass and Lowpass Filters.” International Journal of Computer Applications, vol. 109, no. 14, 16 Jan. 2015.

Moghaddasi, Z., H. A. Jalab, R. Noor, et al. "Improving RLRN Image Splicing Detection with the Use of PCA and Kernel PCA." The Scientific World Journal, 2014.

Munirah, M.Y., N. M. Nawi, et al. "A Comparative Analysis of Feature Selection Techniques for Classification Problems." ARPN Journal of Engineering and Applied Sciences, 2016.

Ng, T.T., S.F. Chang, C.Y. Lin, and Q. Sun. "Passive-Blind Image Forensics." Multimedia Security Technology for Digital Rights, 2006.

Peng, F., Y. Nie, and M. Long. "A Complete Passive Blind Image Copy-Move Forensics Scheme Based on Compound Statistics Features." International Journal of Forensic Science, 2011.

Phkan, A., and M. Borah. "A Survey Paper on the Feature Extraction Module of Offline Handwriting Character Recognition." International Journal of Computer Engineering and Applications, 2014.

Rosales, L., M. Cedillo, et al. "Watermarking Based Image Authentication with Recovery Capability Using Halftoning Technique." Signal Processing: Image Communication, 2013.

Rosales-Roldan, Luis, et al. “Watermarking-based Image Authentication with Recovery Capability Using Halftoning Technique.” Signal Processing. Image Communication, vol. 28, no. 1, Jan. 2013.

Sharma, B. R. Forensic Science in Criminal Investigation and Trials. 1990.

Sharma, B. R. Forensic Science in Criminal Investigation and Trials. 2017.

Shieh, J.M., D.C. Lou, and T. Ming Chang. "A Semi-Blind Digital Watermarking Scheme Based on Singular Value Decomposition." Computer Standards and Interfaces, 2006.

Soloria, B., and A.K. Nandi. "Automated Detection and Localization of Duplicated Regions Affected by Reflection, Rotation and Scaling in Image Forensics." International Journal of Signal Processing, 2011.

Sutthiwan, P., Y. Q. Shi, et al. "Rake Transform and Edge Statistics for Image Forgery Detection." IEEE International Conference on Multimedia, 2010.

Zhao, Y.Q., M. Liao, et al. "Tampered Region Detection of Imprinting JPEG Images." International Journal on Light and Electron Optics, 2013.

Zhao, Y.Q., N. R. Cao, and G. Ni. "Detection of Image Sharpening Based on Histogram Aberration and Ringing Artifacts." IEEE International Conference on Multimedia and Expo (ICME), 2009.