International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-3, February 2020

Forensic Science Research Summary for Forgery Detection of Digital Images

Monika, Dipali Bansal

Abstract: ***An important measure of proof collection, storage, and authentication in forensic sciences, which decide the safety and security of any system documents, which can be either portable document formats or scanned images. To gather evidence, or plan a forensic investigation digital images are secured with different modern methodologies. Digital image analysis includes image recovery and surveillance for image information improvement. The goal of forgery detection is to maximize the extraction of information from manipulated images, particularly noisy and post-processed images. Because digital image processing is becoming popular with many advantages in scientific and engineering applications, the forgery techniques are also growing at a rapid rate. Therefore, the main focus is on different types of forgery detection in digital image processing with the help of all transform techniques and comparing their best results for further improvement in order to generate a new approach for a future forensic science investigation.***

Keyword: Forensic Science, Digital Image Forensics Analysis, Forensic Investigation, Transform Techniques.

I. INTRODUCTION

Today images provide an effective and natural media of exchanging data between humans. Therefore, images play an important role in the day to day routine of a human being. But now a day everyone can record, store and share a lot of digital images. At the same time, the wide availability of software tools for editing images makes it extremely easy to manipulate the content of images or to generate new ones so that the possibility of altering images increases and current software enables us to create computer-processed images so that viewers are unable to distinguish themselves from photographic images showing background issues in the digital media field. Multimedia security is required to information hiding which involves security methods like steganography and watermarking for visible and invisible fingerprint, copyright protection with spatial domain and transform domain all are having different applications like copyright protection, data hiding, fingerprinting, tracing, authentication in both reversible and irreversible conditions all are applicable in many multimedia types like audio, text, video, 2D images, 3D model. It is also useful in applications like quality control systems, benchmark image processing techniques, image processing systems for optimization. Digital image quality will be degraded during compression, transmission, capturing, archiving, retrieving process [1].

Thus, it becomes impossible to trust the content of the images in the digital world. The authentication process involves two broad categories like personal steps as identification, authorization with different types involve password authentication, smart card authentication, and biometric authentication. Another category is based on content authentication involve methods like fragile watermarking (exact authentication) semi-fragile watermarking (selective authentication), digital signature, cryptography with key distribution as symmetric authentication, asymmetric authentication, and services as strict authentication, tamper localization, tamper recovery. So, there is a need for secure techniques that can be applied for authenticity purposes on very important information without degrading the image quality. The image size of tampered regions is also important parameter for the detection of forgery. When post-processing is applied then the result will be a low-quality factor that made difficult computations. Digital forensic is a collection of scientific methods for identification, analysis, interpretation, content authentication, classification, documentation from digital sources for the reconstruction of original information, which helps in forgery detection. It means who, what and why circumstances. Forensic science is very important for image investigation in which statistical binary patterns were analyzed using different transform techniques. Forensic image processing is a new approach to improving digital images from monitoring, closed-circuit TV and many more applications using computer programming tools. These schemes consist of digital filters that can suppress different types of noise like Gblur noise, Pepper noise, Salt noise, Gaussian White Noise, Motion Noise, Multiplicative Spectrum, Poisson, Filter Dilation, Filter Erosion, JEG transmission errors etc. in shadow-generated digital images and provide sharpening of images as well as optimizing histogram for extraction of features. In some image noise patterns will be based on the calibration of the value of the camera. Image information like color, shape, texture, faces, etc. helps to find out the spatial arrangement of image [2]. Every forgery leaves a trace that we tried to analyze effectively. Many Copy — move forgery methodologies are based on threshold calculation through the filtering process, patch matching process which involves forged regions of different sizes.

Revised Manuscript Received on February 06, 2020.
* Correspondence Author
Ms Monika*, PhD degree in ECE, MRIIRS FARIDABAD.
Dr Dipali Bansal, Director-IQAC and Associate Dean - Academics with MRIIRS, Faridabad, NCR, India.

Some times every pixel match processing is complex and time-consuming so that block-based image pixel comparison was done using Euclidean distance calculation tried to reduce the dimensions from RGB vectors of the whole image. Many authors used different transforms and symmetry techniques and multimedia analysis also based on blind forgery study. Non-blind forgery detection has a constraint on their application due to the costly process of the benchmark presented on their images. Different techniques suggested by previous authors have a general workflow that includes pre-processing, feature extraction, matching, visualization of features. Copy- move forgery includes some characteristics like quality degradation via different attacks on images. These different types of image attacks are implemented as filtering attacks of smoothing, sharpening, some normal attacks include noise addition, cropping, compression, vertex quantization, vertex addition, and deletion, some desynchronized attacks are rotation, scaling, translation, vertex recording, sampling, subdivision, and simplification. Some of the important features required for calculating parameters like Characteristic similarity index, gradient magnitude similarity variance, spectral residual similarity, hair similarity index, natural scene statistics, information fidelity criterion also known as visual information fidelity. Motivation comes from the detection of tampered events. [3]. But our main aim is to improve final score value for any kind of image evaluation is compared with existing state-of-art Copy- move forgery. Figure.1 presents a basic approach to forensic investigation. This paper presents a precise objective of analyzing all types of forgery detection that helps in summarizing various approaches adopted for rapid processing and reducing computational complexities. [4].

II. RELATED WORK

Many methods used by many researchers to locate and detect forgery regions such as Copy--move forgery through Discrete Cosine Transform (DCT), Fast Walsh-Hadamard Transform, Normalized Cross-Correlation (NCC) and Discrete Wavelet Transform (DWT), which reduces the complexity of time and its representations of dimensions.

Jayasankar [5] (2018) implemented an image quality assessment measurement for reliable, accurate results involved mean absolute mean-variance, Average square error, root mean square error, peak signal to noise ratio for color and grayscale images with impressive results of fidelity ratio compared with existing metrics without human visual system. Still has some limitations in various image processing systems like Satellite machine-generated imagery, binary images, geographical information systems.

Siddeq [6] (2017) proposed 2D image compression based one-dimension discrete cosine transform and output of this is applied through discrete sine transform for high-frequency components minimization through quantization and binary search algorithm for compressed quality ratio compared with others methods but still complex in image type of JPEG and JPEG2000 for best results.

Kamenicky *et al.* [7] (2016) presents different methods for forensic video and image analysis with their originality, improved image quality by reducing noise, unwanted blur and other possible artifacts that contribute to the criminal investigation. The authors ensure image analysis repetition, image processing functions such as image source and their verification, restoration using PIZZARO software. The authors presented real cases solved by the image processing expertise team of the Czech Academy of Science, Czech Republic Police's National Drug Headquarters and Investigation Service. But still there are some limitations in their study that it is difficult to verify credibility, origin, restore an image by removing unwanted artifacts with increasing data quality, it is not time-effective in terms of facilitating criminal work, it is necessary to use different methods to obtain stronger evidence. It represents PIZZARO-based forensic image implementation tool [8] which includes 1.) Image source determination: Source device assignment, LCD re-captured images detection, Quantization table implementation. 2). Verification of image content: Double JPEG compression, detection of interpolation, detection of movement of Copy-, the incoherence of noise Chromatic aberration. 3) Restoration of images: DE-noising, super-resolution, elimination of JPEG artifacts. Garfinkel [9] (2010) presented an efficient review of the investigative literature directions of digital forensic science for the next 10 years starting from 2010. Digital forensic is approximately 50 years old and initially required for email data recovery, data formatting, immediate deletion and identification, data remedy, software and hardware application, time-sharing, centralized computing facilities. For many investigations such as military analysis, government organization, and e-discovery, digital forensics is, therefore, a very important part. Digital forensic also helps to solve computer crime such as bank fraud, money laundering, and child exploitation. Previous DFRWS and CDESF begins together for digital evidence but is dispersed due to inadequate resources using HASS and CARVER support XML data file representation. The authors show different views on how new data representation concepts can make digital forensic more efficient, but only with the support of funding agencies that need to accept standards and procedures for testing and validating research products. Short-coming in their study is: the lack of incompatibility of training data-sets and format, the efficiency of the research process reduces day by day; unauthentic users cannot easily obtain forensic data for processing [10]. Forensic image analysis increases the speed with new technologies of processing forensic investigation. Authors also explore the principle of design such as transparency, privacy, and security with Van-Beek *et al.* [11] (2015) implementing it for a business perspective. With the help of the Hansen System, the author uses some forensic drivers to reduce the case lead time, maximum data coverage, and expert team analysis. Short-coming in their study is: Need to substitute Hansen System for the Xiraf System [12]. Authors tested various methodologies such as data descriptions, showing platform, feature selection, extraction of features, the color derived feature similarities for reliability purposes with the help of the region of interest curve showing true positive rate and false positive rate by

Talbot-Wright *et al.* [13] (2016) for different data types. For their fundamental uniqueness, Authors analyze traditional forensic information such as chromatography and digital images and perform scaling operations to enable more automated discovery of trends in the forensic case study with more powerful algorithms. Authors effectively present the practical application for the forensic intelligence process of generalized and transversal work such as deletion memory, problem profile, etc. Forensic research is an expansion of forensic science that helps in many policies and security content. Authors implemented a simple approach to exploring images that enable strong insights into domestic and regional scales of criminal organizations. The drawbacks in their study are: the threshold value found for descriptive statistics between 28% and 45% of the profile document, this can be strengthened with a good approach, the strength of the association between the origin rate and the sequence of repetitions. gives their relationship hypothesis for the week.

Warbhe *et al.* [14] (2016) presented a novel approach for image forgery detection using (NCC) Normalized Cross-Correlation, a tool for matching image recording features, tempering matching and pattern recognition. Authors use coarse forgery detection to find the highly correlated area where each uneven block acts as a template for NCC and fine-tuned detection to detect forged region. NCC helps to calculate the cross-correlation of each pixel and standardize that image by square root autocorrelation. The authors use the detection method based on a block-based approach. This helps to determine the similarities and non-similarities between + 1 and -1 of digital images. The limitations of this study are: the need for improved post-processing algorithms such as scaling, rotation, etc., the threshold value for block-size of 4 and block size of 20 is 0.98, which can be further improved by changing these two values. The authors successfully proposed a method to increase the efficiency of digital evidence detection investigation promptly presented by Hitchcock *et al.* [15] (2015) reducing block size for analysis in the forensic laboratory between regular and non-regular datasets. The authors successfully implemented an analysis of forgery detection. Authors represent digital field triage analysis through planning, evaluation, reporting, threshold, where the calculation is carried out through various phases such as user account, type of crime (internet activity, multimedia documents, installed software, emails), attached device, timely search, encryption one by one. The triage model of the digital field works in two ways i.e. DCFT (Digital Computer Field Triage) and DMFT (Digital Mobile Field Triage). Digital field triage members collect confirmation from RAM running on that TCU (Technological Crime Unit Examination) threshold machine. The limitations in their study are: time-consuming process between analyzing digital evidence and receiving the analytical report, Advanced training required for ram capture, basic acquisition, encoding capability detection on a live machine, need for experienced digital field triage members, need to review the DFT model's efficiency and efficiency.

Hashmi *et al.* [16] (2014) proposed an efficient and robust Copy--move image forgery detection method through the process of feature extraction techniques called DyWT (Dyadic Wavelet Transform) with SIFT (Scale Invariant Feature Transform), which helps to match large key points with the precision of 95 percent but with a combined effort of DyWT+SIFT. Experimental results show that precision was 88 percent with a false positive rate of 10 percent. Image forensics proofs that digital image authenticity can be easily detected and used as evidence for judgment purpose. The proposed novel methodology is based on the transformation of invariant scale features (SIFT) for Copy- move forgery occurrence and recovering by Irene Amerini *et al.* [17] (2011) also shows geometric transformation for highly reliable cloning. The main drawback is how to improve the investigation of cloning damage patch with highly uniform texture and how to extend the clustering phase by the process of image segmentation [18].

Warbhe *et al.* [19] (2016) proposed interpolation techniques to find JPEG (Joint Photographic Experts Group) artifacts using Nearest neighbor techniques of Bilinear and Bicubic methods. The experimental results of the author show better image quality results through the Bicubic Interpolated method compared with other techniques explained by George *et al.* [20] (2016). The proposed technique is simple to execute and can also be applied to compression techniques for single and double JPEG. JPEG Artifacts made it difficult to detect forgery and a challenging job. It also authenticates the quality of the various antiforensic images using different methods of calculating quality: MSE, PSNR, BRISQUE, and SSIM. The limitations in their study are: it leaves interpolation clues where it is possible to use random selection for every pixel, where interpolation methods can be used with random selection to obtain better image quality.

The authors use quality factor evaluators to test the different images, obtaining maximum effective results. Authors used BRISQUE: 31.641, Usc Sipi database for testing images by evaluators of spatial quality, MSE: 93.709, Usc Sipi database for Mean Square Error for test images, PSNR: 36.137, Peak signal to noise ratio for the testing images, SSIM: 0.9757 for the test images for structural similarity Index ratio. Digital image forensic investigation easily detects image manipulation such as histogram, gamma correction or equalization. The authors proposed an efficient and effective method to detect contrast enhancement using intrinsic fingerprints where noise is added before JPEG is compressed. The authors also tested many simulations to detect their designated image processing operations with the likelihood of detection and the likelihood of false alarm being only 7%, by Stamm and Liu [21] (2010). The major disadvantages of their studies are: different regions of interest curve additive noise detection can be improved by applying new techniques for contrast enhancement [22].JPEG Anti-Forensic Method: Good for identifying traces of JPEG image compression using discrete cosine transformation (DCT) domain with a reasonable loss of image quality and shows improved trade-off between JPEG forensic detectability and the visual quality of the images processed with different JPEG compression artifacts as suggested by Fan *et al.*

[23] (2014). the proposed process of JPEG forgery involves: blocking of DE based on TV, DCT histogram, and calibration of DE. To trace the processed image from the detection regions of multiple detectors that could be applied with different domains, while maintaining a high image quality under the evaluation of both PSNR and SSIM metrics. Authors proposed JPEG anti-forensic method to improve trade-off between forensic detectability and visual quality of the image, the main limitations of their studies are: To design the optimal techniques for detecting JPEG image forgery using multiple detectors and the non-convex SSIM metric, authors apply various image statistics in the DCT domain for a better restoration of the histogram to investigate the design and implementation of general anti-forensics, SSIM is non-convex, making it difficult to optimize.

Swaminathan *et al.* [24] (2008) proposed a new forensic analysis methodology implemented on indoor and outdoor post-operation of acquisition devices to verify the integrity of digital image forensics, which helps to calculate the Constrained Optimization inverse manipulation filter coefficients. In [25] JPEG compression was considered to be a quantization in the discrete cosine transformation (DCT) domain and statistical analysis. Estimated filter coefficients used to detect various post-camera processing operations, such as steganography embedding and watermarking. Any change of inconsistency in the estimated fingerprints of the camera provides clues to detect cut-paste tampering and to determine whether a camera, scanner or computer graphics software was used to create the image. Proposed methods, therefore, verify that the digital images are from direct camera output, the main limitations of their study are: the receiver operating characteristics for manipulating detection show an average accuracy of 62 % and 52 % at rates of 100 % and 78 % respectively, the average accuracy of identification is reduced to 91% [26].

Blocking artifacts in Skin Images can be generated by the JPEG algorithm which affects the visibility of the small skin marks and is very common to identify individuals in evidence images and JPEG-compressed child pornography. The proposed approach is knowledge-based (KB), which removes JPEG blocking artifacts and recovers skin features, The authors developed various algorithms: Markov-model-based algorithm is a faster one-pass algorithm to implement the inference, while block synthesis algorithm to handle the various cases where compressed blocks are not included in the training set. Tang *et al.* [27] (2011)**.** There is also an improvement in the visual quality of biometric features. The authors also designed a mechanism for indexing these algorithms to accelerate. The short-coming in their study is: Complexity is extremely high in the calculations of an iterative process for forward and reverses DCT. Compression testing of 500 images reduces the quality factor of 50, and the average compression ratio was only 72.55, another 262 compressed image test reduces the quality factor of 25, and the average compression ratio was only 126.93.

Visual Sensor Forensics: it helps handle patent infringements, authenticate sources of acquisition, protect rights of intellectual property, and identify manipulations of data. In the field of visual sensor techniques, the authors proposed a new methodology for forensic analysis to estimate algorithms for color filter array and color interpolations. The analysis examines the similarities between different technologies that various camera models use to identify potential infringement or licensing. The methodology proposed includes testing of objects, extraction of features, classification, testing, and validation. It's good for post-processing as well. The main limitation is the result shows only an average accuracy of 90% for the correct camera brand is effectively identified. Another is to investigate other important components within digital cameras such as raw sensor data and the white balanced provides useful information for various sensor characteristics Swaminathan *et al.* (2007) [28].

Bone Image Analysis: bone diseases related to the age of bone growth in bone biology. The authors present the use of the image processing system for rational knowledge in bone cross-section and micro-structural with reliable output based on quantitative measurements. The study represents the correlation between bone characteristics and bone growth associated with age. Experiments use knowledge-based techniques to show image clustering, channel extraction, region image mapping, boundary extraction, post-processing. The main problem is how to process conventional images Gherghel *et al.* [29] (2016). Forensic Medical Sciences: Virtual anthropology and radiographic imagery used in human skeletal forensic analysis. Proposed techniques provide a powerful non-invasive supplement or alternative to traditional forensic virtual anthropology and DVI applications. Forensic anthropology helps to access a large body of evidence that is not easily accessible through gross skeletal material that helps to investigate the bone's internal structure and explores facial recognition Franklin *et al.* [30] (2016).

Forensic DNA science: reviews forensic DNA development standards that support writing procedures to effectively perform testing by comparing and sharing data. This article provides a broad review of the activities, including the efforts of the White House National Science and Technology Council Subcommittee on Forensic Science and Partnership between the Department of Justice (DOJ) and the National Institute of Standards and Technology (NIST) to establish the National Forensic Science Commission and the Organization of Scientific Area Committees by Butler [31] (2015). The shortcomings in their study are: To improve academic education programs with pretty scholarship and fellowship contributions and to establish on-going legal education programs for law students, specialists and judges to improve death investigations by establishing a medical examination system with all legal medical autopsies or improved computer algorithm accuracy, supervised by a board-certified forensic pathologist, achieves national Automated Fingerprint Identification Systems (AFIS) interoperability of fingerprint data and work [32]. Sifting Collectors: Provide an AFF V3 sector-by-sector, bit-identical image of disk regions selected fully compatible with existing forensic tools and methods.

Authors proposed a new approach useful for the acquisition of digital forensic evidence and disk imaging for easy storage of large discs without sacrificing the many benefits of imagery. Grier and Richard [33] (2015) Results show the acceleration of 95%. The limitations of their studies are: Testing sifting collectors requires library expanding profiles, integration of sifting collectors applied with hardware and software analysis tools for post-collection image size reduction in forensic technologies such as disk duplicators. Li *et al.* [34] (2017) presented Image fusion: Mixing two images in one image by extracting key features from the image source. Multi-resolution techniques were proposed by authors to decompose an image and obtain information from coarse to fine scales. Cartridge image checking enables the image fusion technique to be multi-resolution. Major issues arise with the image check of the cartridge, enabling all required data information to be provided in [34].

Warbhe *et al.* [35] (2016). authors proposed a new approach for Copy-ing past detection using standardized cross-correlation image editing software programs that makes manipulation very easy like Copy-ing past, composing, splicing. Copy-paste forgery detection includes a block or key-point detection method. One of the transform approaches such as Discrete Cosine Transformer (DCT) is an effective approach to reducing the cost of detecting Copy-move forgery. The proposed work includes Fine-tuned Scale Tampering Detection (FSTD), Scaling Detection Percentage and Coarse Scale Tampering Detection (CSTD). The main limitations of their studies are: Rotation is not fully analyzed to detect accurate forged region. Blind Image Forensics is also known to Copy- move forgery and it includes scaled images, rotated images, translated images and cloned images with a new Auto Colour Correlogram approach for features extraction procedure that effectively detects multiple region duplication in the same image.

The proposed work includes noise filtering, transformation, auto color correlogram for extraction feature, matching forgery detection similarities, Malviya *et al.* [36] (2016). The result shows that accuracy is only 95.65 % with a false positive rate of 16 and a false negative rate of 32 by testing 400 images from the database [37].

According to the literature described above, the following Table.1 shows the literature survey on forensic image processing approaches with all their applications, limitations, techniques and extracted features, as well as Table2, represents a comparison of various algorithms for forgery detection, as well as Table3 provides a comparative study of various transformation techniques for best detection of forgery. Figure.2 represents approaches to digital image processing.

III. CONCLUSION

Copy- moving forgery detection tested by many methodologies for the extraction of features, segmentation, acquisition, histogram, transformation, etc. Therefore, the authentication of digital images is a very important area in the field of forensic research on image processing. With their comparative analysis of existing forgery detection algorithms, we presented an overview of different forgery detection algorithms.

Many existing methods face the problem involving human interpretation, larger modified regions with inconsistencies, camera model identification, compression artifact difficulties, high false-positive rate, expensive and lower quality factors, etc., some post-processing operations affected and produced lower accuracy in case of blurring of edges, additive noise, loss compression. Therefore, the main concern is about the security of digital content without degrading the quality and reducing the difficulties of distinguishing between innocent and malicious tampering with statistical features for different post-processing functions. We hope that this survey will help to identify new methodologies and ideas for future investigators working in the field of electronic forgery identification forensic investigation.

ACKNOWLEDGMENTS

I would like to thank my guide Dr. Dipali Bansal Professor and Head of ECE Department, MRIIRS Faridabad., for her guidance, innovative ideas, relentless support and encouragement towards the research. I would specifically like to thanks Dr. M. K. Soni Pro Vice-Chancellor, FET, MRIIRS, Faridabad for providing institutional facilities and support during the whole research.

Availability of Data and Material**:**
DATA SHARING DOES NOT APPLY TO THIS ARTICLE AS DURING THE CURRENT STUDY NO DATA SETS WERE GENERATED OR ANALYZED.
FUNDING:
FUNDING INFORMATION IS NOT APPLICABLE TO THE CURRENT STUDY.

Table1. Literature survey on Forensic Image Processing Approaches

Authors/Years	Approaches	Applications	Methodology	Limitations
Malviya *et al.* [36] (2016)	Auto Color Correlogram Approach	Feature Extraction, Calculation of True Positive Rate and False Positive Rate	Noise Filtering, Transformation.	Testing Can Be Improved with Large Set of Data Base.
Talbot-Wright *et al.* [13] (2016)	Data Descriptions, Script Platform, Feature Selection, Feature Extraction, Color Derived Feature Similarities	Generalized and Transversal Work Like Deletion Memory, Problem Profile, Etc. for Forensic Intelligence Process	Authenticity, Forged Region Detection, Stolen Banks, Reliability Maintained in ROC Curve Which Shows True Positive Rate and False Positive Rate for Different Data Types	To Test and Train Methods for Different Situations. Acquisition Difficulty in Database for Different Police Jurisdiction
Tang *et al.* [27] (2011)	Knowledge-Based (KB) Approach, Markov-Model-Based Algorithm, Faster One-Pass Algorithm, Block Synthesis Algorithm	Biometrics and Vein Pattern Recognitions Restoration Detection	Pigmented Skin Marks Skin Features DCT Calculations QDCT Coefficient	Difficult Analysis in Human Vision System (HSV)
Fan, W *et al.* [23] (2014)	Variation-Based DE blocking Approaches	Removing of JPEG Artifact, Double JPEG Compressed Artifacts	DCT Histogram	Optimization of SSIM is difficult
Hashmi *et al.* [16] (2014)	DYWT (Dyadic Wavelet Transform) with SIFT (Scale Invariant Feature Transform)	Correlation and Key Feature Detection, Transformation, Blind passive techniques	Digital Signature and Water Marking. Binary Pattern Recognitions, Key point Descriptor Identifications	Standard Database Requirement
Garfinkel *et al.* [9] (2010)	Summarizes the current Forensic Research	XML Data representation and processing for forensic investigation	Virtual Software and Approaches Live Acquisition, Multimedia Document Controls	To reduce the cost of Forensic Investigation with improved Image Quality
Van Beek *et al.* [11] (2015)	Xiraf System Approach	Forensic Drivers for Security, Safety, Networks, Software, and Openness on the Design	Reducing the Case Lead Time, Maximum Coverage of Data	Progress becomes slow by Xiraf System so need to replace by Hansen System
Amerini *et al.* [17] (2011)	Scale-Invariant Features Transform (SIFT)	Image Segmentations Splicing Attacks.	Image Source Identifications, Cluster Point Description, Blur Artifects. Geometric Transformations Statistical Measurements	FPR is 8% with the time 4.94 sec. Detection can be limited to Cloning operations.

Kamenick *et al.* [7] (2016)	Full Size and Central Size Image Approaches	Image Source Identification and their Verification, Restoration	Double JPEG Compression Interpolation Detection Copy-Moving Noise Detection Inconsistency Chromatic Aberration LCD Re-captured Noise Detection JPEG Artifacts Removal	By removing unwanted artifacts with Increasing Data Quality, it is difficult to verify credibility, origin, image restoration. In terms of automation, it is not time-effective can facilitate criminal work. Different methods are required to obtain stronger evidence.
Stamm and Liu.[21](2010)	Intrinsic Fingerprint,	Identification of forgery with MSE, PSNR, SD etc.	Histogram Equalization / Gamma Correction Contrast Enhancement	Reduction in False Alarm Probability
Warbhe *et al.* [14] (2016)	Nearest neighbor Bilinear and Bicubic Interpolation Antiforensic Techniques	Testing of Single and double JPEG compression.	Quantization and Blocking Artifacts, Statistical Measurements of JPEG Compressed Images	Shows Traces of Forgery
Warbhe *et al.* [19] (2016)	Pixel Based Forensic Techniques: Ncc Via Coarse Forgery and Detection, Fined Tuned Forgery Detection	Blind Image Forensic Investigation	Tempering matching, pattern recognition, threshold detection setting, easy image registration, less time consuming compared to lexicographic algorithms,	Not Performed Well for Some Operation Like Scaling, Rotations, Difficulty in Feature Matching Correlated Regions

Table 2. Comparison of various algorithms for Forgery Detection.

Authors	Extracted Features	Accuracy of Forgery Detection
Liu *et al.* [59] (2011b)	First and higher-order wavelet statistics	67%
Yu-Feng and Shih-Fu [91] (2010)	Geometry invariants for CRF estimation	70%
Ng *et al.* [69] (2004)	Incoherence results	71%
Dong *et al.* [45] (2008)	Edge detection and Run-length based statistical moments	77%
Avcibas *et al.* [8] (2004)	Czenakowski measure and angular correlation	80%
Fu *et al.* [48] (2006)	Moments of characteristics function using wavelet decomposition and Hilbert-Huang transform	81%
Kirchner *et al.* [56] (2010)	Subtractive pixel adjacency matrix and Streaking artifacts	81%
Khanna *et al.* [38] (2008)	Residual pattern noise	82%
Ng and Chang [59] (2004b)	wavelet transform and Natural image statistics from the power spectrum	83%
Luo *et al.* [44] (2007b)	Geometry-based features	84%
Chen *et al.* [15] (2007)	Wavelet characteristic by Statistical moments function	84%
Hsu and Chang [29] (2006)	Camera-based operations using geometry invariants	87%
Qing Zhong and Andrew [60] (2009)	Image quality metrics and cosine transform with DCT coefficients	87%
Zhang *et al.* [93,94] (2008a, 2008b)	Image quality metrics and moment features extracted through a multi-size block of discrete transform cosine	87%
Dirik *et al.* [20] (2007)	Chromatic aberration and Color filter array DE mosaicking	90%
Rocha *et al.* [66] (2006)	Statistical descriptions of the least significant bit occurrence using progressive randomization techniques	90%
Sankar *et al.* [71] (2009)	Color histogram patch statistics Moment-based method and texture interpolation method,	90%
Wang *et al.* [85] (2009)	Gary level matrix of Chroma components	91%
Luo *et al.* [45,44] (2007a, b)	Blocking artifact characteristics matrix	92%
Shi *et al.* [73] (2007a, b)	Markov transition probabilities and characteristic functions of wavelet subbands	92%
Sutthiwan *et al.* [76] (2009a)	JPEG 2-D array Image and pixel 2D array image and 2D histogram	93%
Sutthiwan *et al.* [75] (2009b)	Second-order statistics transition probabilities matrices using Markov process	94%
Cao *et al.* [12,13] (2010a, b)	MF statistical fingerprint and texture regions	
Wu *et al.* [87] (2011)	First-order or second-order disparity images	95%

Li *et al.* [90] (2015)	statistics of predicting error signals and features based on variance and kurtosis of second-order difference signals	96%
Stamm and Liu [21] (2010)	Image pixel value histogram	98%
Mahalakshmi *et al.* [66] (2012)	DA and AD DFT methods	99%
Bayram *et al.* [4, 10] (2005a, b)	Binary similarity measures	99%
Bayram *et al.* [44] (2007)	Binary similarity measures, Higher-order wavelet statistics, and Image quality Measures	100%
Gul *et al.* [49] (2010)	SVD based features	100%
Lint *et al.* [18] (2005)	Inverse camera responses	100%

Table 3: comparative techniques of forensic image approaches

Authors	Feature Extraction Techniques	Precision%	Recall %	Score%
Amerini *et al.* [17] (2011)	Scale invariant features transform (**SIFT**)	95	74	83.20
Hashmi *et al.* [16] (2014)	**DyWT +SIFT**	88	80	83.80
Siddeq et al. [6] (2017)	discrete cosine transforms (**DCT**)	78.69	100	88.07
Tang *et al.* [27] (2011)	knowledge-based **(KB)** approach	90.1	90	90.05
Warbhe *et al.* [14] (2016)	Speed Up Robust Features (**SURF)**	91.49	89.58	90.53
Warbhe *et al.* [19] (2016)	Normalized Cross Correlation (**NCC**)	94	90	91.95
Malviya *et al.* [36] (2016)	Auto Color Correlogram (**ACC**)	95.65	91.67	93.62

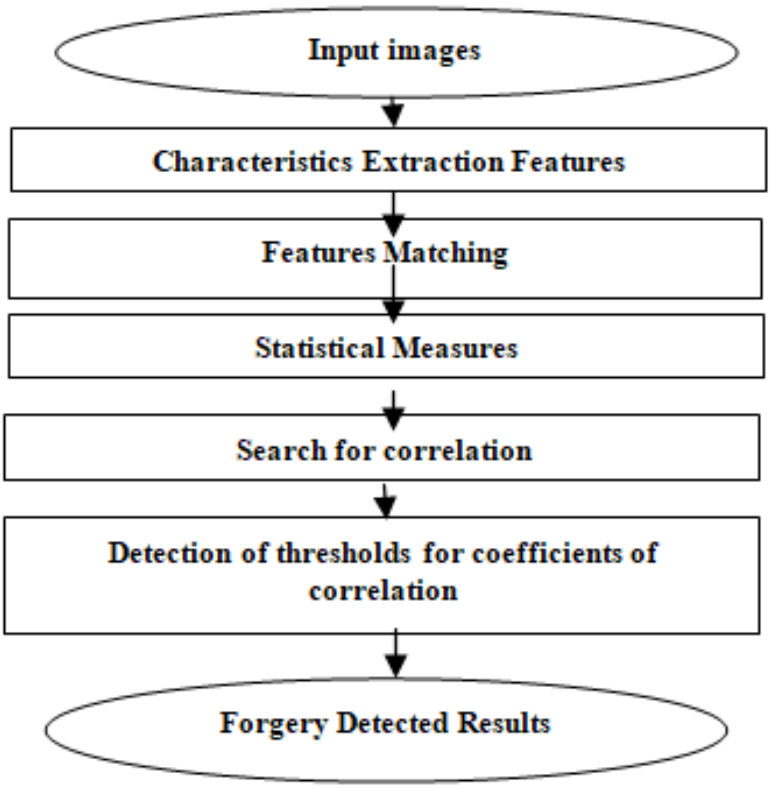

Figure 1. Digital Image Forgery Forensic Approaches

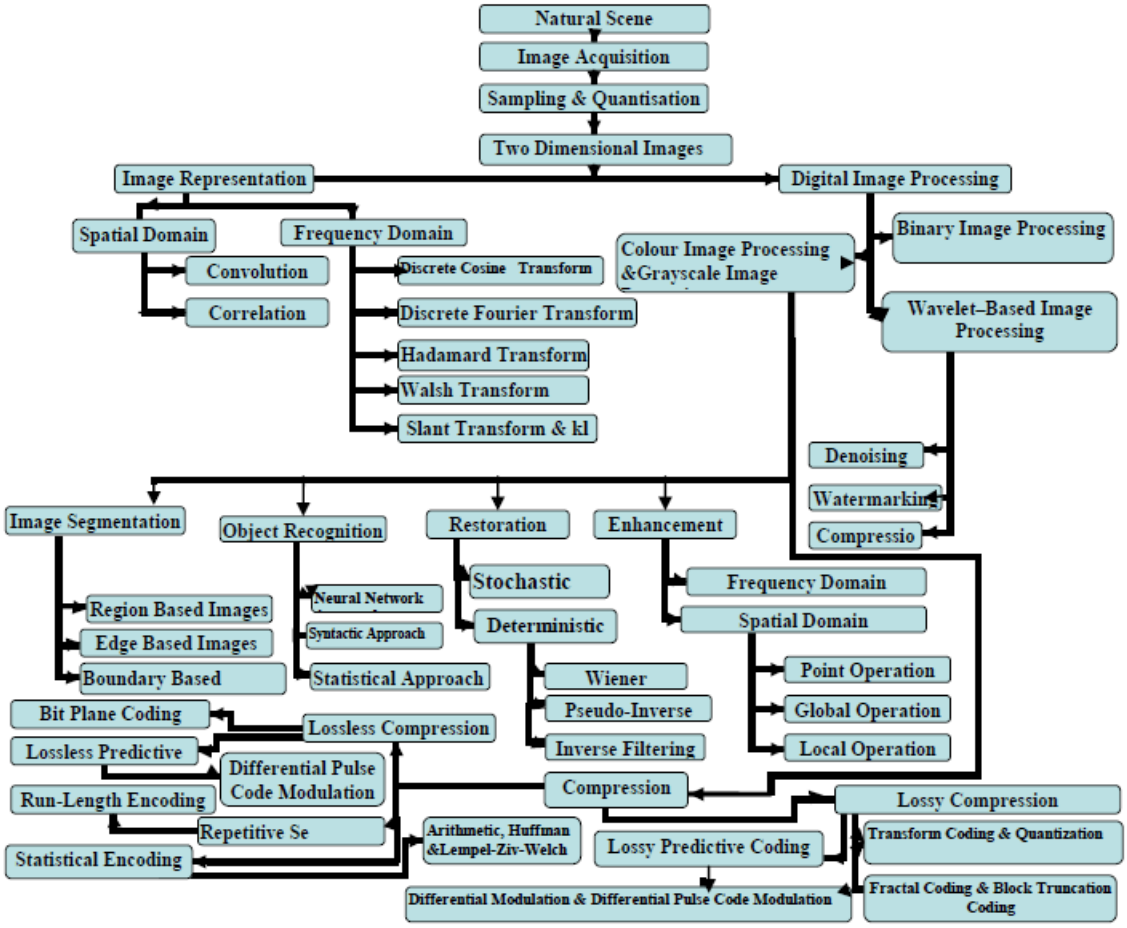

Figure 2. Digital Image Processing Approaches.

REFERENCES

1. Luo W, Qu Z, Pan F, Huang J,"A survey of passive technology for digital image forensics". Front Comput Sci China.1 (2). pp.166–179, 2007a.
2. Wang W, Dong J, Tan T. "Effective image splicing detection based on image chrom." IEEE International conference on image processing .pp. 1257–1260, 2009.
3. K. P. Chandar and T. S. Savithri, "3D Face Model Estimation based on Similarity Transform using Differential Evolution Optimization," *Procedia Comput. Sci.*, vol. 54, pp. 621–630, 2015.
4. Bayram S, Avcibas I, Sankur B, Memon N,"Image manipulation detection with binary similarity measures". Proc. of 13th European signal processing conference, vol. 1. pp. 752–757, 2005a.
5. U. Jayasankar, "A New Objective Image Quality Assessment Metric : For Color and Grayscale Images," *3D Res.*, 2018.
6. M. M. Siddeq and M. A. Rodrigues, "DCT and DST Based Image Compression for 3D Reconstruction," *3D Res.*, 2017.
7. Jan Kamenicky.et al. "Forensic analysis and restoration of image and video data "264, pp.153–166, 2016.
8. Avcibas I, Bayram S, Memon N, Ramkumar M, Sankur B, "A classifier design for detecting image manipulations". Proc. International conference on image processing (ICIP) pp. 2645–8, 2004.
9. S. L. Garfinkel, "Digital forensics research: The next 10 years," *Digit. Investig.*, vol. 7, no. SUPPL., 2010.
10. Bayram S, Sencar HT, Memon ND, Avcibas I,"Source camera identification based on CFA interpolation". Proc. International conference on image processing (ICIP). pp. 69–72, 2005b.
11. H. M. A. Van Beek, E. J. Van Eijk, R. B. Van Baar, M. Ugen, J. N. C. Bodde, and A. J. Siemelink, "Digital forensics as a service: Game on," *Digit. Investig.*, vol. 15, pp. 20–38, 2015.
12. Zhang Z, Yuan R, Jian P, Zhang H, Shan-Zhong. "A survey on passive-blind image forgery by doctor method detection." International conference on machine learning and cybernetics, vol. 6.pp. 3463–3467, 2008a.
13. B. Talbot-Wright, S. Baechler, M. Morelato, O. Ribaux, and C. Roux, "Image processing of false identity documents for forensic intelligence," *Forensic Sci. Int.*, vol. 263, pp. 67–73, 2016.
14. A. D. Warbhe, R. V. Dharaskar, and V. M. Thakare, "A Scaling Robust Copy--Paste Tampering Detection for Digital Image Forensics," *Procedia Comput. Sci.*, vol. 79, pp. 458–465, 2016.
15. B. Hitchcock, N. Le-khac, and M. Scanlon, "Tiered forensic methodology model for Digital Field Triage by non-digital evidence specialists," *Digit. Investig.*, vol. 16, pp. S75–S85, 2016.
16. M. F. Hashmi, V. Anand, and A. G. Keskar, "Copy--move Image Forgery Detection Using an Efficient and Robust Method Combining Un-Decimated Wavelet Transform and Scale Invariant Feature Transform," *AASRI Procedia*, vol. 9, no. Csp, pp. 84–91, 2014.
17. I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, "A SIFT-based forensic method for Copy--move attack detection and transformation recovery," *IEEE Trans. Inf. Forensics Secur.*, vol. 6, no. 3 PART 2, pp. 1099–1110, 2011.
18. Lint Z, Wang R, Tang X, Shum H,"Detecting doctored images using camera response normality and consistency" Proc. of IEEE Computer Society conference on computer vision and pattern recog-nition(CVPR'05), vol. 1. pp. 1087–1092. 2005.
19. A. D. Warbhe, R. V. Dharaskar, and V. M. Thakare, "A Survey on Keypoint Based Copy--paste Forgery Detection Techniques," *Phys. Procedia*, vol. 78, no. December 2015, pp. 61–67, 2016.
20. M. George, M. Thomas, and C. K. Jayda's, "A Methodology for Spatial Domain Image Compression Based on Hops Encoding," *Procedia Technol.*, vol. 25, no. Rarest, pp. 52–59, 2016.
21. M. C. Stamm and K. J. R. Liu, "Forensic detection of image manipulation using statistical intrinsic fingerprints," *IEEE Trans. Inf. Forensics Secur.*, vol. 5, no. 3, pp. 492–506, 2010.
22. V. S. Harichandran, D. Walnycky, I. Baggili, and F. Breitinger, "CuFA: A more formal definition for digital forensic artifacts," *Digit. Investig.*, vol. 18, pp. S125–S137, 2016.

23. W. Fan, K. Wang, F. Cayre, and Z. Xiong, "JPEG anti-forensics with improved tradeoff between forensic undetectability and image quality," *IEEE Trans. Inf. Forensics Secur.*, vol. 9, no. 8, pp. 1211–1226, 2014.
24. Swaminathan, A., Wu, M. and Liu, K.J.R., "Digital image forensics via intrinsic fingerprints." IEEE Transactions on Information Forensics and Security, 3(1), pp.101–117, 2008.
25. Swaminathan, A., Wu, M. and Liu, K.J.R., "Nonintrusive component forensics of visual sensors using output images." IEEE Transactions on Information Forensics and Security, 2(1), pp.91–105, 2007.
26. X. Chu, S. Member, Y. Chen, M. C. Stamm, and K. J. R. Liu, "Information Theoretical Limit of Operation Forensics," *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 4, pp. 774–788, 2016.
27. C. Tang, A. W. K. Kong, and N. Craft, "Using a knowledge-based approach to remove blocking artifacts in skin images for forensic analysis," *IEEE Trans. Inf. Forensics Secur.*, vol. 6, no. 3 PART 2, pp. 1038–1049, 2011.
28. Y. Li and J. Zhou, "Anti-Forensics of Lossy Predictive Image Compression," *IEEE Signal Process. Lett.*, vol. 22, no. 12, pp. 2219–2223, 2015.
29. S. Gherghel, R. M. Morgan, C. S. Blackman, K. Karu, and I. P. Parkin, "Analysis of transferred fragrance and its forensic implications," *Sci. Justice*, vol. 56, no. 6, pp. 413–420, 2016.
30. D. Franklin, L. Swift, and A. Flavel, "'Virtual anthropology' and radiographic imaging in the Forensic Medical Sciences," *Egypt. J. Forensic Sci.*, vol. 6, no. 2, pp. 31–43, 2016.
31. J. M. Butler, "U.S. initiatives to strengthen forensic science and international standards in forensic DNA.," *Forensic Sci. Int. Genet.*, vol. 18, no. January 2007, pp. 4–20, 2015.
32. Cao, H. and Kot, A.C,"Accurate detection of demosaicing regularity for digital image forensics". IEEE Transactions on Information Forensics and Security, 4(4), pp.899–910, 2009.
33. J. Grier and G. G. Richard, "Rapid forensic imaging of large disks with sifting collectors," *Digit. Investig.*, vol. 14, pp. S34–S44, 2015.
34. H. Li, W. Luo, X. Qiu, and J. Huang, "Image Forgery Localization via Integrating," vol. 6013, no. c, pp. 1–13, 2017.
35. A. D. Warbhe, R. V. Dharaskar, and V. M. Thakare, "Computationally Efficient Digital Image Forensic Method for Image Authentication," *Procedia Comput. Sci.*, vol. 78, no. December 2015, pp. 464–470, 2016.
36. A. V Malviya and S. A. Ladhake, "Pixel based Image Forensic Technique for Copy-move forgery detection using Auto Color Correlogram.," *Procedia - Procedia Comput. Sci.*, vol. 79, pp. 383–390, 2016.
37. R. Raj and N. Joseph, "Keypoint Extraction Using SURF Algorithm for CMFD," *Procedia Comput. Sci.*, vol. 93, no. September, pp. 375–381, 2016.
38. Cao G, Zhao Y, Ni R, Yu L, Tian H, "Forensic detection of median filtering in digital images. Proc". IEEE International conference on multimedia and Expo .pp. 89–94, 2010b.
39. Cao G, Zhao Y, Ni R. "Edge-based blur metric for tamper detection". J Inf Hiding Multimed Signal Process; 1(1) pp.20–27, 2010a.
40. Chen W, Shi Y, Su W,"Image splicing detection using 2-d phase congru- ency and statistical moments of characteristic function".Proc. of SPIE electronic imaging: security, steganography, and watermarking of multimedia contents, 2007.
41. D. Chauhan, D. Kasat, S. Jain, and V. Thakare, "Survey on Keypoint Based Copy--move Forgery Detection Methods on Image," *Procedia Comput. Sci.*, vol. 85, no. Cms, pp. 206–212, 2016.
42. D. Dietrich and F. Adelstein, "Archival science, digital forensics, and new media art," *Digit. Investig.*, vol. 14, no. S1, pp. S137–S145, 2015.
43. D. Gugelmann, F. Gasser, B. Ager, and V. Lenders, "Hviz: HTTP(S) traffic aggregation and visualization for network forensics," *Digit. Investig.*, vol. 12, no. S1, pp. S1–S11, 2015.
44. Dirik AE, Bayram S, Sencar HT, Memon N,"New features to identify computer generated images".Proc. IEEE International conference on image processing, vol. 4. pp. 433–439, 2007.
45. Dong J, Wang W, Tan T, Shi Y,"Run-length and edge statistics based approach for image splicing detection".Proc. digital water marking. 7th International workshop (IWDW). pp. 76–87, 2008.
46. E. R. Almeida, J. L. sPorsani, I. Catapano, G. Gennarelli, and F. Soldovieri, "Microwave Tomography-Enhanced GPR in Forensic Surveys: The Case Study of a Tropical Environment," *IEEE J. Sel. Top. Appl. Earth Obs. Remote Sens.*, vol. 9, no. 1, pp. 115–124, 2016.
47. F. M. M. Badr El Dine and M. M. El Shafei, "Sex determination using anthropometric measurements from multi-slice computed tomography of the 12th thoracic and the first lumbar vertebrae among adult Egyptians," *Egypt. J. Forensic Sci.*, vol. 5, no. 3, pp. 82–89, 2015.
48. Fu D, Shi Y, Su W, "Detection of image splicing based on Hilbert-Huang transform and moments of characteristic functions with wavelet decomposition". Proc. of International workshop on digital water-marking. pp. 177–187, 2006
49. [49] Gul G, Avcibas I, Kurugollu F,"SVD based image manipulation detection". International conference on image processing (ICIP). pp. 1765–1768, 2010.
50. H. K. Chethan and G. Hemantha Kumar, "Image dewarping and text extraction from mobile captured distinct documents," *Procedia Comput. Sci.*, vol. 2, pp. 330–337, 2010.
51. Hsu Y, Chang S. "Detecting image splicing using geometry invariants and camera characteristics consistency". Proc. IEEE International con- ference on multimedia and Expo (ICME). pp. 549–552, 2006.
52. I. Amerini, R. Becarelli, R. Caldelli, and M. Casini, "A feature-based forensic procedure for splicing forgeries detection," *Math. Probl. Eng.*, vol. 2015, pp. 1–7, 2015.
53. J. S. Arunalatha *et al.*, "FIVDL: Fingerprint Image Verification using Dictionary Learning," *Procedia Comput. Sci.*, vol. 54, pp. 482–490, 2015.
54. J. Stüttgen, S. Vömel, and M. Denzel, "Acquisition and analysis of compromised firmware using memory forensics," *Digit. Investig.*, vol. 12, no. S1, pp. S50–S60, 2015.
55. Khanna N, Chiu GT-C, Allebach JP, Delp EJ,"Forensic techniques for clas- sifying scanner, computer generated and digital camera images". In: Proc. IEEE International conference on acoustics, speech and signal processing. pp. 1653–1656, 2008.
56. Kirchner M, "Efficient estimation of CFA pattern configuration in digital camera images". Proc. SPIE conference on media forensics and security, vol. 7541. pp. 754-765, 2010.
57. L. Fongaro, D. M. Lin Ho, K. Kvaal, K. Mayer, and V. V. Rondinella, "Application of the angle measure technique as image texture analysis method for the identification of uranium ore concentrate samples: New perspective in nuclear forensics," *Talanta*, vol. 152, pp. 463–474, 2016.
58. L. Gómez-Miralles and J. Arnedo-Moreno, "Versatile iPad forensic acquisition using the Apple Camera Connection Kit," *Comput. Math. with Appl.*, vol. 63, no. 2, pp. 544–553, 2012.
59. Liu Q, Cao X, Deng C, Guo X,"Identifying image composites through shadow matte consistency". IEEE Trans Inf Forensics Security. 6(3) pp.1111–1122, 2011b.
60. Luo W, Qu Z, Huang J, Qiu G, "A novel method for detecting cropped and recompressed image block". Proc. IEEE International conference on acoustics, speech and signal processing, vol. 2.. pp. 217–220, 2007b.
61. M. C. Stamm and K. J. R. Liu, "Anti-forensics of digital image compression," *IEEE Trans. Inf. Forensics Secur.*, vol. 6, no. 3 PART 2, pp. 1050–1065, 2011.
62. M. George, M. Thomas, and C. K. Jayda's, "A Methodology for Spatial Domain Image Compression Based on Hops Encoding," *Procedia Technol.*, vol. 25, no. Rarest, pp. 52–59, 2016.
63. M. Guido, J. Butter, and J. Grover, "Rapid differential forensic imaging of mobile devices," *Digit. Investig.*, vol. 18, pp. S46–S54, 2016.
64. M. M. Patil, "Digital Image Alteration Detection using Advance Processing," vol. 116, no. 18, pp. 18–22, 2015.
65. M. R. Keyvanpour and F. Merrikh-Bayat, "Robust dynamic block-based image watermarking in DWT domain," *Procedia Comput. Sci.*, vol. 3, pp. 238–242, 2011.
66. Mahalakshmi DS, Vijayalakshmi K, Priyadharsini S,"Digital image forgery detection and estimation by exploring basic image manipulations". Digital Invest.8 (3–4) pp.215–225, 2012.
67. N. Kishore and B. Kapoor, "Faster File Imaging Framework for Digital Forensics," *Procedia Comput. Sci.*, vol. 49, pp. 74–81, 2015.
68. N. Singh, "A Novel Digital Image Steganalysis Approach for Investigation," vol. 47, no. 12, pp. 18–22, 2012.
69. Ng T, Chang S,"A model for image splicing" Proc. of IEEE International conference on image processing (ICIP). pp. 1169–1172. 2004.
70. Ng T, Chang S,"Classifying photographic and photorealistic computer graphic images using natural image statistics" ADVENT Technical Report, #220-2006-6. Columbia University. 2004b.
71. Qingzhong L, Andrew H,"A new approach for JPEG resize and image splicing detection". Proc. ACM multimedia and security workshop. pp. 43–48, 2009.

72. R. S. Oommen, M. Jayamohan, and S. Sruthy, "Using Fractal Dimension and Singular Values for Image Forgery Detection and Localization," *Procedia Technol.*, vol. 24, pp. 1452–1459, 2016.
73. R. Satta and A. Ciardulli, "Sensor pattern noise and image similarity for picture-to-identity linking," vol. 9, pp. 711–722, 2015.
74. R. Thanki and K. Borisagar, "Sparse Watermarking Technique for Improving Security of Biometric System," *Procedia Comput. Sci.*, vol. 70, pp. 251–258, 2015.
75. R. Vieira, C. Silva, M. Antunes, and A. Assis, "Information System for Automation of Counterfeited Documents Images Correlation," *Procedia - Procedia Comput. Sci.*, vol. 100, pp. 421–428, 2016.
76. Rocha A, "Goldenstein S. Is it fake or real?" Proc. XIX Brazilian symposium on computer graphics and image processing, 2006.
77. S. Dubey, "Image Forgery Detection based on Local Descriptors and Block-Matching using Clustering Technique," vol. 141, no. 10, pp. 11–15, 2016.
78. S. G. Mueller, L. M. Bateman, and K. D. Laxer, "Evidence for brainstem network disruption in temporal lobe epilepsy and sudden unexplained death in epilepsy," *NeuroImage Clin.*, vol. 5, pp. 208–216, 2014.
79. Sankar G, Zhao V, Yang Y-H.,"Feature based classification of computer graphics and real images". IEEE International conference on acoustics, speech and signal processing. pp. 1513–1516, 2009.
80. Sciences, B., "Studies in History and Philosophy of Biological and Biomedical Sciences. Medicine", 40, pp.1–3, 2009.
81. Shi Y, Chen C, Chen W. ".A natural image model approach to splicing detection". Proc. of ACM workshop on multimedia and security (ACM MMSEC07). pp. 51–62, 2007a.
82. Shi YQ, Chen W, Xuan G."Identifying computer graphics using HSV color model and statistical moments of characteristic functions."IEEE International conference on multimedia and Expo. pp. 1123–1126, 2007b.
83. Sutthiwan P, Cai X, Shi YQ, Zhang H, "Computer graphics classification based on Markov process model and boosting feature selection technique". IEEE International conference on image process- ing. pp. 2913–2916, 2009b.
84. Sutthiwan P, Ye J, Shi YQ. "An enhanced statistical approach to identifying photorealistic images."8th International workshop on digital watermarking. pp. 323–335, 2009a.
85. T. Thongkamwitoon, H. Muammar, and P. L. Dragotti, "An image recapture detection algorithm based on learning dictionaries of edge profiles," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 5, pp. 953–968, 2015.
86. T. Vidas, B. Kaplan, and M. Geiger, "OpenLV: Empowering investigators and first-responders in the digital forensics process," *Digit. Investig.*, vol. 11, pp. S45–S53, 2014.
87. V. K. Singh and R. C. Tripathi, "Fast Rotation Invariant Detection of Region Duplication Attacks even on Uniform Background Containing Digital Images," *Procedia Comput. Sci.*, vol. 54, pp. 772–780, 2015.
88. Worth, "A Picture's Worth, Digital Image Analysis and Forensics." Solutions, pp.1–31, 2007.
89. Wu R, Li X, Yang B, "Identifying computer generated graphics via histo- gram features. International conference on image processing ". pp. 1933–1936, 2011.
90. X. Kang, M. C. Stamm, A. Peng, and K. J. R. Liu, "Robust median filtering forensics using an autoregressive model," *IEEE Trans. Inf. Forensics Secur.*, vol. 8, no. 9, pp. 1456–1468, 2013.
91. Yu-Feng H, Shih-Fu C, "Camera response functions for image forensics: an automatic algorithm for splicing detection". IEEE Trans Inf Forensics Security5 (4):816–825, 2010.
92. Z. Yuan, X. Xie, J. Hu, and D. Yao, "An Efficient Method for Traffic Image Denoising," *Procedia - Soc. Behav. Sci.*, vol. 138, no. 0, pp. 439–445, 2014.
93. Zhang Z, Kang J, Ren Y,"An effective algorithm of image splicing detection". International conference on computer science and software engineering. pp. 1035–1039, 2008b.

AUTHORS PROFILE

Ms Monika, received her B. Tech degree in application of Electronics and Communication Engineering in 2007and M. Tech degree in ECE in 2011 both from MDU Rohtak, Haryana. From 2007 to 2019, she was an Assistant Professor in MRIIRS, Faridabad, NCR, India. She is currently working towards the PhD degree in ECE at MRIIRS FARIDABAD. Her research interest includes image processing, image forensics, Digital Logics.

Dr Dipali Bansal, is the Director-IQAC and Associate Dean - Academics with MRIIRS, Faridabad, NCR, India. Dr Bansal is a doctorate in Bio signal processing from Jamia Milia University, New Delhi. She has got a distinguished career in teaching and industry spanning 22 years and her research work has found prominent recognition and has been published in many national and international journals and conferences (80 papers). She has attended many International conferences abroad primarily at Washington D.C and Los Angeles USA and Italy (Florence). She is a Reviewer of many journals including the journal of Medical and Biological Engineering and Computing (Springer), Computers in Biology and Medicine, Elsevier Journal (Science Direct), and Journal of Circuits, Systems, and Signal Processing.