INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor : 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 01, January 2024, pp : 371-378

A REVIEW OF IMAGE FORENSICS IN DETECTING DIGITAL FORGERIES.

Sarvesh V [1], Shamanth S R[2], Mohammed Rafi[3]

[1,2,3]Computer Science and Engineering, University B. D. T. College of Engineering Hadadi Road, Davangere, Karnataka, India.

ABSTRACT

Digital image manipulation has become a major concern today, with increasing challenges surrounding its authenticity and integrity. Image forgery is a common practice that aims to manipulate images in such a way that they become indistinguishable from the original image, appearing genuine. The use of digital images has grown significantly in crime investigations, law evidence, and surveillance, making it necessary to ensure their trustworthiness. Digital image forensics (DIF) has become a crucial area of expertise as forensic experts also use digital images in their investigations. DIF focuses on verifying the authenticity and integrity of digital files. This paper presents a literature review of DIF, covering active and passive methods, as well as those based on deep learning. It provides an updated set of references synthesized in textual, tabular, and graphic form.

Keywords- Digital Image Forensics, Digital Image Processing, Computer Generated Image, Co-occurence Probability Matrix

1. INTRODUCTION

An image is a visual representation of an object, while a digital image is a binary representation of visual data. Digital images can be presented in the form of photographs, graphics or individual video frames. They are created or copied and stored in electronic form. However, forgery is an illegal means of manipulating images or documents without prior access. Tampering with images is done for various reasons, such as creating false evidence or earning money in an illegal way. Pictures convey ideas much better than words. With digital technology, many tools like Adobe Photoshop, GIMP, and Corel Paint Shop are used to process images. However, these tools pose a threat to the authenticity of digital images. Image forensics techniques rely on the assumption that every stage of image acquisition and processing holds some inherent statistics and leaves a particular trace. It is possible to infer the source of the image or determine whether it is authentic or tampered with by identifying the existence, lack, or inconsistency of forensic traces that are inherent to the image itself.

2. IMAGE FORENSICS

The field of image forensics involves using scientific techniques to determine if an image was captured by a specific device or if it has been manipulated in any way. This is done by analyzing the inherent statistics and traces left behind during the various stages of image acquisition and processing, from its raw form to compression, storage, and post-processing. By identifying the presence, absence, or inconsistency of these forensic traces, it is possible to determine the authenticity of an image. This is especially important in fields such as criminal and forensic investigation, intelligence systems, medical imaging, insurance claims, and journalism where digital images are often used as critical evidence.

3. DIGITAL IMAGE FORGERIES

Digital image forgery is a complex area of study that deals with the manipulation and tampering of digital images. It is a major concern for society as a whole and is described by Merriam-Webster as the "falsely and fraudulently changing a digital picture," an issue that has been present since 1840. Image forgery involves reproducing images with different parameter values, and the incidence of serious cases is increasing, which has alarmed law-and-order systems around the world. The availability of numerous image editing, enhancing, correction, modification, and recreation tools has made it easier for these criminal acts to occur. [4]

In 2010, British Petroleum (BP) faced criticism from the public due to the release of several images that were doctored to exaggerate the company's response to the Gulf of Mexico oil spill. These images were edited to give the impression that BP staff were working harder than they actually were, leading to public outrage.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 01, January 2024, pp : 371-378

e-ISSN : 2583-1062

Impact Factor : 5.725

Fig1. Pairs of the original image with the tampered image. [3]

In Figure 1, there are two sets of images - the original images in the first column and the tampered-with images in the second column. According to a spokesperson for the company, one of the images in the first row of Figure 1 showed two blank screens in the original picture. On the other hand, the second row of Figure 1 displayed a photograph taken inside a company helicopter that appeared to be flying off the coast. However, it was later discovered to be fake as several problems were identified by internet bloggers. These problems included a part of a control tower visible in the top left corner of the picture, the pilot holding a pre-flight checklist, and the control gauges showing the helicopter's door and ramp open, as well as its parking brake engaged.

To perform any operation, the necessary information or inputs are required. In image forgery procedures, the datasets used can be original images, falsified images, or artificially generated images. The distinction between these types of datasets will be explained in the following section.

4. DATA SETS

Acquiring a proper dataset is the foremost step in the deep-learning paradigm to ensure its efficacy, besides the use of different models and approaches. The dataset must match the problem context and include all the necessary acquiring and processing steps to predict the desired results. Developing a dataset is a time-consuming task that requires an in-depth understanding of the problem and context to collect relevant and compatible data. The dataset should have adequate and appropriate information to avoid issues such as overfitting and underfitting. Furthermore, using multiple datasets is crucial to obtain more reliable benchmarking of existing and new methods. In this section, we will introduce publicly available datasets for various image forensics categories, grouped according to their usage. [3]

A. Original Data

Datasets containing pure and unaltered image data are frequently used in the field of image forensics, particularly in manipulation detection studies. These datasets typically contain uncompressed image data, allowing researchers to recreate various manipulation operations and conduct experiments on a suitable and customized dataset. Some of these databases were initially created for the purpose of benchmarking camera identification techniques.

In contrast, Deepfakes, which refer to fake images generated by deep neural networks, have been trained using well-known datasets of human faces, such as the CelebA dataset. The CelebA dataset contains approximately 200,000 faces with various annotations originally designed for facial image analysis. One of the first datasets utilized for training and evaluating Generative Adversarial Network (GAN) models for face generation and editing is the CelebAHQ dataset, which is a collection of high-resolution face images derived from the CelebA dataset.

B. Falsified Data

The detection of splicing, which is a common image falsification technique where a part of an image is copied and pasted onto another image, is aided by several public datasets. The Columbia gray DVMM dataset and the Columbia color splicing dataset were the first public datasets available for splicing detection. The former comprises 1845 grayscale images, while the latter comprises 180 color spliced images, both with random-like splicing falsifications. CASIA V1 and V2 are two other popular splicing datasets that contain more realistic forgeries and post-processing operations on V2 to cover the traces of splicing. The Korus dataset, also known as the Realistic Tampered Dataset, contains 220 splicing and copy-move forgeries with realistic levels of tampering. The authors of this dataset included PRNU

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor : 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 01, January 2024, pp : 371-378

signatures and ground-truth maps. Other datasets have been created with a specific purpose, such as the VIPP dataset, which was created to evaluate the detection of double JPEG compression artifacts that may be present in splicing falsification.

However, the use of datasets specific for copy-move falsification is not common in deep-learning-based detection methods due to their relatively small size. Therefore, most research on deep-learning-based copy-move detection has created customized synthetic datasets derived from original image datasets that contain more samples.

C. Artificially Generated Data

Artificially generated data is becoming increasingly important in various fields, and it is essential to use datasets that contain realistic examples. These datasets typically include a combination of authentic images captured by a camera, as well as artificially generated images created using either conventional Computer-Generated Image (CGI) algorithms or more recent GAN architectures.

There are several datasets available for use, such as the Columbia dataset, which contains 1600 photorealistic computer graphics images. Afchar et al. created a dataset consisting of 5100 fake images generated from videos downloaded from the Internet. Rahmouni et al. created a dataset of CGIs taken from high-resolution video game screenshots, and there are also several online repositories for CGI that have been used as datasets for different detection approaches.

In recent years, Google, in collaboration with Jigsaw and Facebook, created a Deepfake dataset to contribute to relevant research. Facebook also created the DFDC dataset for the Deepfake detection challenge in 2019, which included 4113 Deepfake and 1131 original videos from 66 subjects of diverse origins who gave their consent for the data to be used. Finally, the DFD dataset contains 3068 Deepfake videos and 363 original ones from 28 individuals who consented to the data. It is important to note that when using artificially generated data, the datasets chosen should contain realistic examples to ensure accurate results.

5. IMAGE FORGING DETECTION

Image manipulation involves carrying out operations on an image with the aim of modifying it. Image forgery is a form of image manipulation that involves malicious intent and the manipulation of the entire image. On the other hand, image tampering is a type of image manipulation that involves the intentional modification of only parts of the image. Image generation is a technique used to create images that simulate real-world scenes, using computer software or algorithms. In steganography, the image is modified in a way that allows it to store secret information that is invisible to the human eye. Image watermarking involves altering an image by inserting a mark that serves as proof of authenticity.

There are two main categories of methods for detecting image forgery: active and passive techniques. Active techniques require prior knowledge of certain elements that were initially associated with the original image, such as watermarking or steganographic data. In contrast, passive techniques do not rely on any previous information about the original image to determine its authenticity. These techniques involve identifying typical image forgery operations, like spatial transformations (resizing, rotation, and stretching) or copy-move. You can see this classification illustrated in Figure 2. [2]

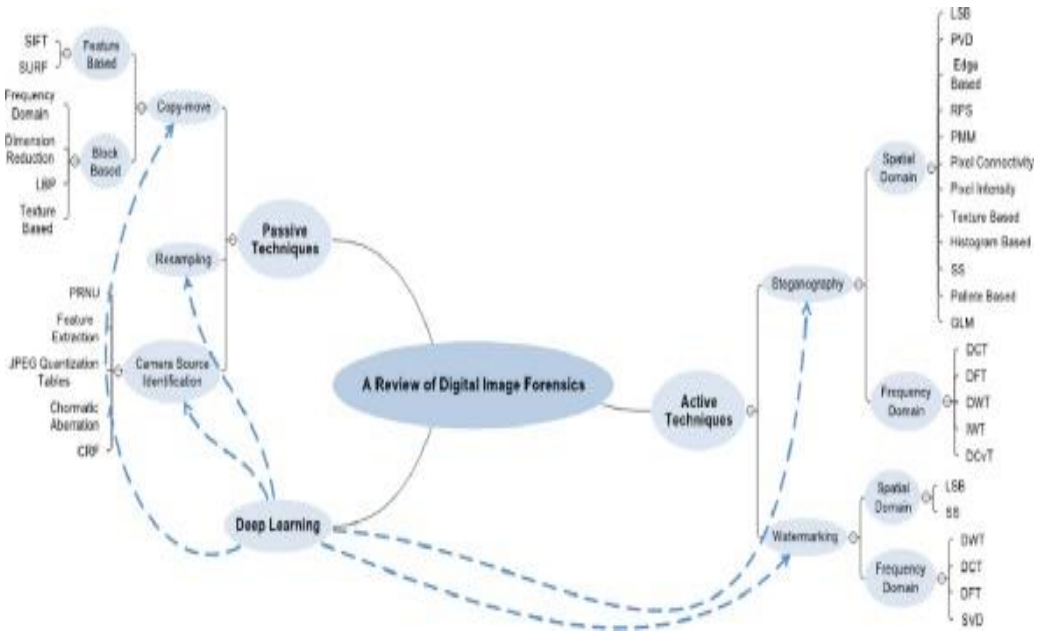


Fig2. Techniques for detecting digital image forgeries. [2]

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor : 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 01, January 2024, pp : 371-378

Active Techniques.

Active techniques involve the insertion of certain elements into an original image and thus require previous information about the image for authentication purposes. These techniques typically involve embedding watermarks into the image, which may or may not be visible to the human eye.

The active class of forgery detection uses two techniques: digital signature and digital watermarking. These approaches require some prior picture information, which could have been embedded in the image at the moment of capture, during image acquisition, or at a later point. In practice, photos created for forensic investigation, such as fingerprint photos, criminal photos, crime scene photos, and so on, are very unlikely to have a watermark or signature. As a result, active forgery detection techniques have proven to be very useful for forensic examination of digital images. These are not very useful for forensic investigation of digital images.

Digital Watermarking and Digital Signature are two basic methods used for Active Image Forgery Detection.

A. Digital Watermarking

In order to detect a watermark, one can apply the maximum length of the linear shift register sequence to the pixel data and then compute the sequence's spatial cross-correlation function along with the picture that has been watermarked. This information can be added or attached with dynamic picture validation that ensures a validation code at the time the image is produced or transferred. However, it is possible for fake image capturing or processing tools to alter this information. When a fake photograph resembling an original image is created using image editing tools, it either lacks this information or contains it. Ferrara have developed a new forensic tool based on the interpolation procedure that can be used to assess the original image and any forged portions.

During forgery detection, the conditional co-occurrence probability matrix (CCPM) is used for detecting third-order statistical features that can also be used to detect picture splicing.

- Li devised a new method for the detection of copy-move forgeries in which the circular blocks were extracted using the Local Binary Pattern (LBP).
- Hussain proposed a multiresolution Weber Local Descriptors (WLD) method for detecting picture forgeries based on chrominance component characteristics

In Digital Watermarking Forgeries, the Support Vector Machine (SVM) classifier and the WLD histogram components are used.

B. Digital Signature.

One of the most common ways to detect picture forgery or manipulation is through digital signatures. A Digital Signature is used to represent the validity of a digital document using a mathematical structure. This is an owner and application-specific utility that embeds authentic user and device information.

A digital signature is a unique code that is added to an image to validate it at the time of transfer or creation. The digital signature consists of a robust bit of the original image, which is taken using a 16*16 pixel block to divide the picture. To create random matrices of size N with elements evenly divided in the interval [0, 1], a secret key k is used. Each random matrix is then subjected to a low pass filter regularly to N random smooth patterns. By applying the signing procedure to a digital picture, the system generates a digital signature that ensures the authenticity of the image.

Some of the propositions proposed in the implementation of digital signature.

- Doke proposed a low-phase filter method for acquiring an X random pattern for each random matrix recurrently. Through the signing operation on the image, the model generates a digital signature.
- Ginesu presented a novel mutual image-based authentication framework. It is a challenge-response scheme that uses a visual password and image scrambling.

The software's application window is divided into k grids, each with h cells. Throughout the user must correctly identify images to pass the image/s selection procedure the k pass image/s chosen at random from the N JPEG images database.

6. PASSIVE TECHNIQUES

Passive techniques do not require any information about the original image, unlike active authentication methods. These techniques utilize the inherent information of images to analyze their content without the use of any previously inserted mark. The three notable passive techniques are source camera identification, copy-move, and resampling.

Picture forensics, which is also referred to as passive or blind image forensics, is a technique for identifying the authenticity and source of an image without relying on pre-extracted or pre-embedded data.

There are five methods involved in this process, which include Pixel-based detection, Format-based detection, physical-based detection, Camera-based detection, and Geometry-based detection.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 01, January 2024, pp : 371-378

Impact Factor : 5.725

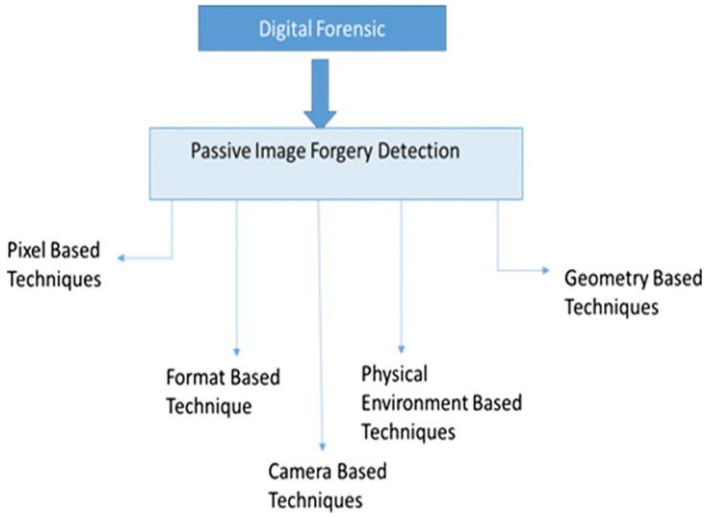


Fig3. Passive image forgery detection techniques.

Passive processes are given into shape with one or more images. The fake image thus produced, although looks authentic, contains intricate traces of inconsistencies, such as overlapping loss of information, distortions, and other artifact fingerprints as clues for Image Forensics.

The techniques used in the Passive approach to detect image forging are as follows besides their types:

A. Pixel Based Forgery Detection

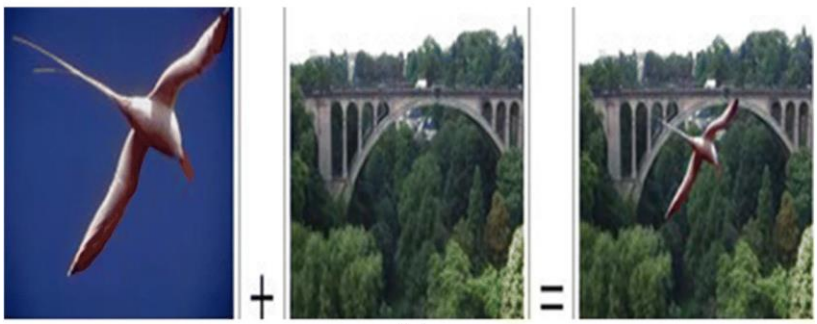
Pixel-based classification is a technique that operates on a pixel-by-pixel basis by utilizing the spectral information available for each individual pixel. This approach is often used to extract low-level features, where the image is classified based on its spectral information. However, this technique has some drawbacks as it can lead to class confusion, resulting in misclassification of pixels in the overlapping region. [1]

There are several types of pixel-based forgeries, including copy-move, image splicing, image resampling, and image retouching. These forgeries can have a significant impact on image analysis and may require advanced techniques to detect and prevent them.

B. Copy and move based methods.

It is one of the most common image tampering techniques, and it's also one of the most difficult to spot because the cloned image is taken from the same image. A section of an image is copied and pasted to another part of the same picture in Copy-Move image forgery.

(a)



(b)

Figure (a) and (b) show an example of class 1 and class 2 attacks.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 01, January 2024, pp : 371-378

Impact Factor : 5.725

Copy and move-based methods consist of two attacks: 1)class 1 copy-move forgery and 2)class 2 copy and creates a forgery.

The act of manipulating images for negative purposes is often achieved through a technique known as image editing. This involves using various tools, such as copy, move, duplicate, clone, image merging, and filters, to alter the original image message or conceal specific parts.

C. Image-retouching forgery detection methods

It is a very useful approach in magazines and photography in films. Although such modifications are to beautify the image and hence not counted for forging. But we are including it here as it includes changes/manipulations with the originality of the image. The image is upgraded to beautify it, and only particular parts are altered (like removing wrinkles) to produce the final shot.

(a) (b)

(A) Retouched image and (**B)** original image

D. Image splicing or photomontage forgery detection methods

Digital image alteration is a common practice, often involving image splicing or composition. This technique involves copying and pasting portions of an image from similar or different sources. By merging several images, the technique can transform and recreate an image. However, this process can lead to the loss, distortion, or damage of primary information from each image used in the splicing or composition process.

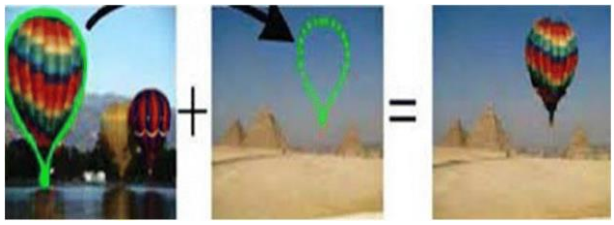


Fig: 4 Image splicing forgery

E. Image resampling forgery detection

The technique involves making geometric modifications such as stretching, flipping, skewing, rotating, scaling, etc. to specific sections of an image to create a visually appealing altered version. During the resampling process, the interpolation stage plays a critical role as it introduces significant statistical changes. When the image is resampled, it results in unique periodic correlations that can be utilized effectively.

Fig:5 Image resampling forgery.

F. Compression-based forgery detection

Detecting forgery in images can be challenging due to the manipulation of forged images for compression and other purposes. One of the most commonly used picture compression techniques is JPEG, or Joint Photographic Experts Group. However, forensics experts have developed methods that use some of the features of JPEG compression to detect tampering. These methods include JPEG quantization-based, double JPEG compression-based, multiple JPEG compression-based, and JPEG blocking-based approaches. Statistical correlation introduced by specific compression algorithms can be useful for identifying image counterfeiting. Huang has developed a technique for detecting double JPEG compression using a quantization matrix, while Kee has described a method that uses the camera signature of a JPEG image to determine whether or not a picture has been edited.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor : 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 01, January 2024, pp : 371-378

There are various methods in compression based forgery detection and those are listed in the following list:

1. JPEG quantisation method.
2. Double JPEG quantisation and JPEG blocking method.
3. -based forgery detection.
4. Chromatic aberration.
5. Color filter Array.
6. Source camera abbreation.
7. Sensor imperfection.

G. Physics based forgery detection.

Natural photographs are often taken in different lighting conditions, which can pose a challenge when editing them. When multiple images are used to create a forged image, the lighting of the forged area may differ from the original. To detect evidence of tampering, physics-based approaches utilize differences in light sources between certain objects in the scene. During the editing process, images are blended under various lighting conditions, making it difficult to match up the lighting state. However, the difference in illumination among the blended photos can be used to identify the tampered areas of image manipulation. [1]

Some of the methods in this forgery detection are listed below:

1. Light direction – 2D
2. Light direction – 3D

H. Geometric based forgery detection

Geometric constraints play a crucial role in detecting forgeries in systems that use perspective views. There are different techniques that fall under this category, such as intrinsic camera parameters-based techniques (including focal length, main point, aspect ratio, and skew), metric measurement-based techniques, and multiple view geometry-based techniques.

When an image is captured, the primary point, which is the intersection of the optical axis and the image plane, is usually located at the center of the image. However, if a small section of the image is moved or copied, or if multiple images are combined or spliced together, maintaining the correct perspective of the primary point becomes difficult. [1].

The various methods in this detection are given as follows:

1. Camera intrinsic parameters

2. Metric measurement.

3.Multi-view geometry.

Deep learning approaches.

Artificial neural networks, also known as neural networks (NNs), are algorithms designed for pattern recognition and classification of objects. They are based on a computing model inspired by the structure of neurons in the brain, with layers of interconnected neurons. NNs are among the most commonly used machine learning (ML) tools today. ML is a paradigm that enables artificial intelligence (AI) to learn directly from data instead of relying on specific programming. [2]

Limitations of existing deep-learning based approaches are:

Lack of optimal model of image forgery model

Many image forgery detection models suffer from cumbersome algorithms that are fitted with incorrect classifiers, leading to poor or faulty performance. The choice of dataset or its unavailability is another criterion where these models struggle. Ultimately, a faulty image forgery detection model can fail due to increased time consumption and expense. Additionally, the procedures in deep learning image forgery detection can vary greatly from one another, particularly in terms of pre-processing, training, and the human decision analytical phase.

Lack of accuracy of automated forgery prediction.

The identification and detection of complex forgeries, such as Deep Fakes, are still largely dependent on classifiers, even today. However, these classifiers often exhibit poor performance in such cases. Additionally, choosing the appropriate initiation mode and detection location (pixel/region) often becomes incompatible with one another during the analysis phase, making it difficult to achieve automation in this phase. As a result, human experts are required to intervene in the process in almost every case.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

Impact Factor : 5.725

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 01, January 2024, pp : 371-378

Lack of availability of deep-learning based good tools

According to research, the effectiveness of Deep Learning-Based Image Forgery Detection is limited to certain areas such as device detection, copy-moving detection, among others. Additionally, the accuracy of experimental results heavily relies on the selection and usage of datasets.

Lack of cost-effectiveness.

The high cost associated with implementing the mechanisms categorized in the study is primarily due to the need for classifiers, advanced training algorithms, and computational resources. In the field of Image Forensics, datasets are crucial for training and developing models. There are various types of datasets available for these analyses, including the UCID dataset, RAISE dataset, Vision Dataset, and others, which provide original information.

Modern Deep learning-based forgery detection techniques.

This section defines the most prevailing, demanding, and modern detection techniques used in the world nowadays in the field of forensic sciences. Joudar proposes a new optimization model for kernels redundancy reduction in CNN. Fernandes proposed that a particle swarm optimization-based algorithm could be used to search for the most effective convolutional neural networks.

Different types of techniques in Modern Deep learning based forgery detection are as follows:

- Deep Fakes:

  Deep fakes refer to images or videos in which an individual's face has been replaced with a computer-generated face that closely resembles another person. This technique is used to create convincing illusions that can be difficult to distinguish from reality.

- Anti-forensics.

  Anti-computer forensics, also known as counter-forensics, refer to the methods used for preventing forensic analysis. With the limitations of deep learning-based image forensics approaches, adversarial attacks have been developed to bypass the detection systems. Some of these techniques include Jacobian-based Saliency Map Attack (JSMA), Fast Gradient Sign Method (FGSM), and others.

- Image source location (or Location forensics approaches).

  Image source location based forensic approaches discusses into three categories. Camera artifacts based, Imaging property based and Sensor imperfection based source locations.

The types of location forensics approaches are:

a) Camera artifact based source location.

b) Sensor imperfection based source location.

c) Imaging property based source location.

7. CONCLUSION

In conclusion, digital image forensics is an important field that focuses on verifying the authenticity and integrity of digital files, particularly in the context of image forgery. With the increasing use of digital images in a variety of critical fields, it is essential to ensure their trustworthiness. This paper presented a literature review of DIF, covering active and passive methods, as well as those based on deep learning. The review provided an updated set of references synthesized in textual, tabular, and graphic form. As digital image manipulation becomes more widespread and sophisticated, it is crucial to continue research in this area to develop new techniques and tools for detecting and preventing image forgery.

8. REFERENCES

[1] Sharma, P., Kumar, M. & Sharma, H. Comprehensive analyses of image forgery detection methods from traditional to deep learning approaches: an evaluation. Multimed Tools Appl 82, 18117–18150 (2023).

[2] William D. Ferreira, Cristiane B.R. Ferreira, Gelson da Cruz Júnior, Fabrizzio Soares, “A review of digital image forensics” , Computers & Electrical Engineering, Volume 85, 2020.

[3] A Comprehensive Review of Deep Learning Based Methods for Image Forensics, by Ivan Castillo Camacho and Kai Wang, 2021. https://doi.org/10.3390/jimaging7040069

[4] S. Devi Mahalakshmi, K. Vijayalakshmi, S. Priyadharsini, “Digital image forgery detection and estimation by exploring basic image manipulations”, Digital Investigation, Volume 8, Issues 3–4, 2012.