A Survey on Digital Image Forensics: Metadata and Image forgeries

Renu Gopal Mani, Rahul Parthasarathy, Sivaraman Eswaran and Prasad Honnavalli

[a] *Centre for Information Security, Forensics and Cyber Resilience, PES University Bengaluru, India*

Abstract

In this modern day of digital media, the ease of image tampering is far from arduous. With growing advancements in editing software, the growth of crimes such as phishing, insurance fraud, cyberbullying, etc., goes unchecked and has cast appall amidst the cyber sectors of Crime divisions across the world. This calls for advancements in forensic tools to identify media tampering to prevent situations from escalating. In the following paper, we look at various forensic methods of identifying media tampering. These methods include multitudes of ways that media can be tampered with but we mainly focus on two aspects: i.e., metadata tampering and image forgery analysis. Metadata tampering constitutes analysing the metadata of an image to search for discrepancies in data between the original and altered images. It also constitutes an analysis of watermarks and other intentional changes done to the image metadata. Image forgery analysis comprises various methods of identifying media tampering, The ability to identify tampering done to the media can open doors for Crime Divisions to successfully prevent crimes and apprehend criminals that have taken part in such activities. This paper goes deep into the world of image analysis to give an understanding of how forensic methodologies can help such investigations. Various methodologies of metadata and image analysis including valuable information that can be extracted are discussed, followed by the different types of image modification techniques (or Image Forgery) one can come across, along with mentioning some methods that are used to evade detection - i.e., Counter Forensics. Several Machine Learning-based image forensics methods - From Error level Analysis of images to the study of individual pixels and extracting evidence of tampering and the use of other methods to detect any tampering in images especially when the tampered images are modified subsequently to make it difficult to detect any form of tampering. The paper also compares some of the well-known tools that aid image forensics. Finally, some case studies are presented where image forensics played a crucial role in the investigations, as well as some of the possible challenges faced are discussed.

Keywords 1

Digital Forensics, Image Forensics, Image Metadata,

1. Introduction

Digital Forensics is the preservation, identification, extraction, and documentation of computer evidence that can be produced in a court of law. It inculcates techniques to recover and analyse evidence found on digital media platforms like a computer, mobile phone, server, or network that are related to cybercrime [27]. Digital forensics is generally carried out in 5 major steps [28] –

WAC-2022: Workshop on Applied Computing, January 27 – 28, 2022, Chennai, India.
EMAIL: sivaraman.eswaran@gmail.com (Sivaraman Eswaran)
ORCID: 0000-0003-0858-148X (Sivaraman Eswaran)

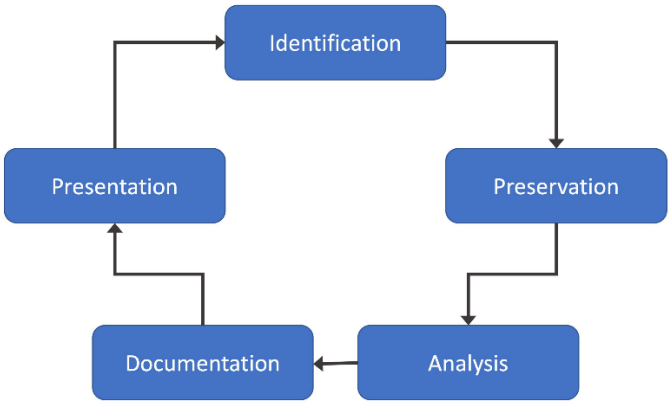


Figure 1: Major steps carried out in Digital forensics

1. Identification – Involves locating the evidence and location of storage.
2. Preservation – Involves isolating and securing the data, i.e., taking measures to prevent the evidence from being susceptible to tampering.
3. Analysis – Involves reconstruction of fragments of available data and charts out conclusions using the evidence discovered.
4. Documentation – Chart out all available data in an easy-to-read format to recreate the crime scene.
5. Presentation – Involves summarising and drawing out conclusions.

The flowchart in Fig.2 represents the classification of digital forensics into broad categories [29]

Overall, Digital Forensics branches out into multiple domains - Wireless Forensics, Database Forensics, Disk Forensics, Network Forensics, Email Forensics, Memory Forensics, Digital Image Forensics, Malware Forensics, etc.

Digital image forensics [1] is a category of Digital Forensics that targets the validation of the authenticity of images by rendering pre-existing information on the history of the image. The two main prominent issues addressed are: 1) the identification of the device responsible for capturing the image 2) the detection of traces of forgeries, i.e., image tampering.

Digital Image Forensics can be broadly classified into these formats [31]:

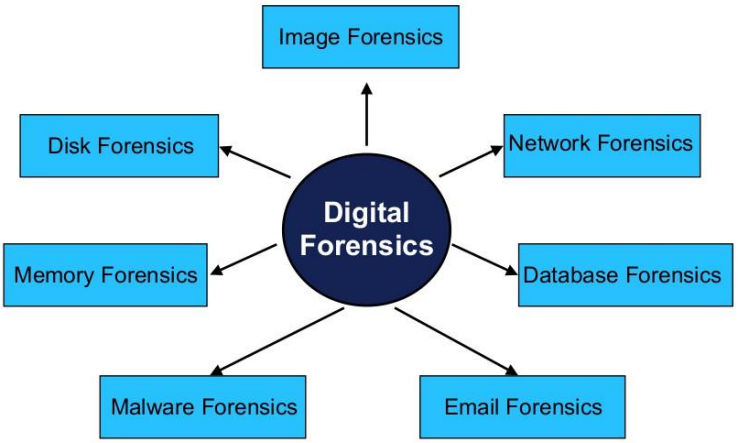


Figure 2: Classification of Digital Forensics

Active:
Active techniques can be further sub-categorized into the following:

- Watermarking. The types of available watermarks are

    - Fragile
    - Robust
    - Semi-Fragile
- Digital Signature

Passive:

Passive methods can be sub-categorized depending on what they focus on:

- Signal Based
- Scene Based

Image Forensics [32] techniques used in the investigations are of two types; Blind and non- blind. Blind techniques [33] of image investigation are used when the original copy of an image is unavailable while nonblind techniques are used when the principal investigator has access to the original document.

The detection of forgery is extremely easy if both the original image and the altered ones are available for parallel comparison. Alas, this is rarely the case and most cases involve only the altered image and thus it usually results in a blind investigation involving extraction of fingerprints that were generated during different instances of processing the image. Non-blinded approaches can be further classified as either intrusive or semi-intrusive. During intrusive analysis, the input and output results of each device component alongside varying parameters used during the process of image creation are readily available to the analyst. In semi-intrusive, the access to the source device is acquired by the analyst in the form of a black box.

Unfortunately, in this case, the analyst has access to neither the processing techniques nor the parameters.

2. Background

2.1. Active and Passive Image Forensics

The realm of Digital Image Forensics (DIF) is vast enough that we can sub-categorize it into two forms: Active and Passive [34]. Active methods intrude the process of image generation and the image is intentionally altered to leave behind easily identifiable trails. They mainly serve two distinguishable purposes, the first being the authentication of the image source and the second being the proof of image integrity. To achieve the first purpose, components such as digital signatures or watermarks that may or may not be encrypted are embedded into an image in a way that they can't be separated. These embeds retain their form no matter what processing or editing is done to the image. The watermark constitutes private data that is embedded into a digital signal via an unknown encryption key. The authentication of this watermark can be done by extracting it and putting it through a decryption process using the key. This method is predominantly used for the protection of images under Copyright laws. Other examples of Active techniques involve the addition of either fragile or semi-fragile watermarks to images. Fragile watermarks don't survive the image process phase. They get disfigured upon any hint of processing done to the image. The watermark from the acquired image is extracted and a parallel comparison with the original watermark is done. Any discrepancy shows that the image has been morphed.

Passive methods take into consideration the generation of an image, as read-only. They don't interfere in the generation phase. These methods can be widely divided into two sub-categories based on Signals and Scene based techniques. Signal based techniques rely heavily on traces inherently left behind by the process or fingerprints that were embedded in the duration of varying phases of image processing. Parallelly, Scene based techniques analyse both the scene and its semantics that are deployed and look for inconsistencies during the interaction of the operations and physical objects. Passive DIF molds the essentials of blind investigating methods with its principles. They analyse the entirety of an image and rigorously extract any available trace of data that they can associate to its

source to validate image integrity. Status quo doesn't provide cameras that implement cryptic or any form of watermarking algorithms. This results in the production of media with no regard for authenticity or integrity validation. Hence, the need for developing DIF tools with high efficacy rises. [7]

Figure 3 gives an overview of the subcategories of digital image forensics:

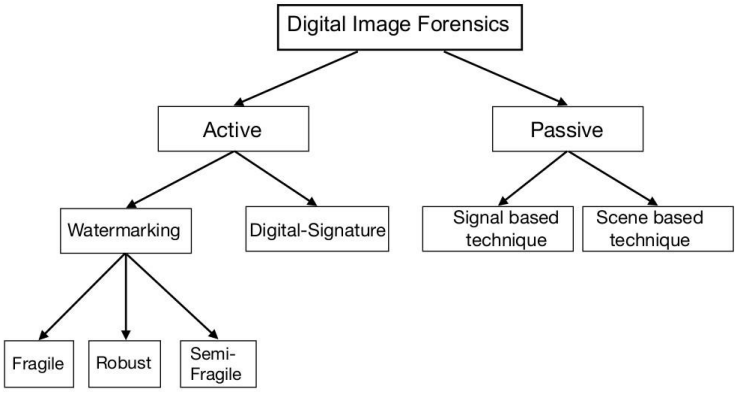


Figure 3: Subcategories of the Digital Image Forensics

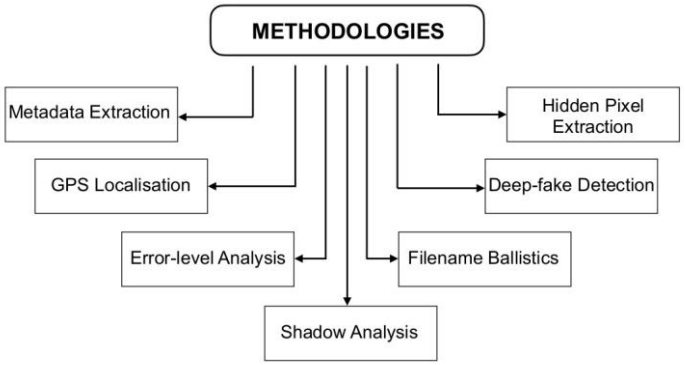


Figure 4: Common Methodologies

3. Methodologies

3.1. Metadata Extraction

Images have a lot of data. Even the process of taking an image leaves behind data. By analysing and comparing such data one can uncover hints to possible forgery. The process of acquiring the metadata is known as extraction [35]. There are multiple methods we can use to extract files containing the metadata of an image. Examples of files whose metadata we can analyse include files such as EXIF, IPTC, 8BIM, ICC, PLUS, and Dicom files [32]. Different forms of metadata such as XMP that predominantly deals with XML allow you to edit such data. Analysis of markers and different compression parameters in EXIF data is a method of authentication of digital media.

3.2. GPS Localization

Some aspects of metadata also store information such as the location of where the image was taken. The latitude and longitude of the place can be acquired from the image metadata [36]. An integration of this data with google maps gives way to easy location search. This method can be used to verify that the photograph was taken at the place it claims to have been photographed.

3.3. Error Level Analysis

A lot of devices use compression formats for the storage and transmission of images. Some of these compression formats offer lossy compression [38]. An example of this would be JPEG. ELA [37] deals with the analysis of such lousy compression formats. The image is transformed for noise analysis. If there is a discrepancy in the noise levels within the same image, it is grounds for the assumption that the image has been edited.

3.4. Shadow Analysis

Images capture a moment in time. This moment includes shadows left behind by objects. By observing the shadows in an image and analysing the accuracy of the existence of a shadow to an object, we could decipher if an image was edited or not, based on discrepancies in the shadows [39].

3.5. Filename Ballistics

Filename Ballistics [21] is a previously introduced concept, but with the advent of the digital age and a few additions, it has proved to be a reliable method to consistently guess the camera make and model of an image. There are some predefined standards for the design of camera file systems, but they are optional and are not universally adopted. In the most rudimentary sense, it can be described as a list of regular expressions where the filename of the image is checked for a match. For example, the image" DSCN8859.JPG" (along with other filename that matches the pattern "DSCN[0- ˆ 9]4˙JPG$")is not just from a Nikon camera but a Nikon Coolpix camera. The filename "DC0555L.JPG" is very specific – it is a large-size photo from a Kodak DC-40, DC-50, or DC-120 and "IMG005.jpg" identifies an LG smartphone running Android 2.2 (Froyo). A drawback with this method is that, since all camera filename formats are not unique, some companies/models can share the same naming system. [IMG 1234.JPG is a format used by some Canon cameras and by Apple mobile devices (iPhone, iPad, etc.)]. The previously mentioned issue is not a dealbreaker if it is possible to ensure that it does not belong to certain brands. This can also be extended to online services. A file downloaded from Facebook has a different filename than one downloaded from another website like Instagram. The underlying assumption of Filename ballistics is that the user does not rename his files. To observe the number of users who rename their files, a few statistics were analyzed. In a survey of 500 unique images, 78matched while for the remaining 22the file was renamed. The advantage is that almost everything happens entirely offline provided users have all the regular expressions. The entire process needs only the filename. If a potential person of interest is being investigated, it can be ensured that this method will not make the person of interest suspicious. Luckily, most of the time the files are not renamed.

3.6. Deepfake Detection

Deepfakes are advanced editing techniques where a person's face can be completely replaced by another and produce a realistic output. These synthetic media forms are tough to detect, and the need to identify them continually increases [40].

3.7. Hidden Pixel Extraction

Pixels are an important part of an image, nevertheless, an entity known as hidden pixels do exist in images that make use of jpeg cropping alongside transparency. Corresponding to their non-hidden versions, these hidden pixels also still constitute colour values. There are a plethora of colour managing approaches to deal with undisplayed areas. With an analysis of these approaches and their corresponding applications, it is possible to detect hints of editing [41].

4. Image Metadata - Information, Tampering, and Authentication

4.1. Metadata Tampering

Metadata can be broadly classified into 3 categories [42] –

1. Technical metadata - Most devices that employ image capturing capabilities generate and markdown information about themselves and the images they record. These data points usually illustrate the images' technical characteristics like ISO speed, size, and colour profile. Additionally, cameras can be configured to append ownership and descriptive information in a comment field on one of the fields of the metadata.
2. Descriptive metadata - The owner of an image can enter and implant a plethora of information on an image's content which encompasses fields like captions, titles, location, headlines, and many more. The fields are a part of the IPTC*-IIM schema and have been expanded into the IPTC Core and IPTC Extension metadata schemas. Efficient and descriptive metadata is imperative to locate image collection to find stored images.
3. Administrative metadata - The broader goal of this type of metadata is to help identify provenance information such as an image creator. PLUS* system has standardized fields such as specific restrictions on the image, model releases, contact information of the creator, etc.

Image metadata contain multiple formats depending on the type of data being stored, some of the prominent metadata types are listed in Fig.5 [8] –

Metadata Formats	
Exif	Contains technical information concerning camera settings and manufacturer information.
IPTC	Empowers the user to add user-defined metadata fields.
8BIM	Added by photoshop, dealing with graphic related fields.
ICC	Contains fields dealing with embedded colour profiles.
PLUS	Contains communication rights and ownership information.
Dicom	Contains fields dealing with niche image information
XMP	XMP is an XML based metadata format which provides a description on the contents of the file it is attached to. XMP allows the user to add custom parameters. While you can add custom metadata, few image databases like photoshop and bridge can detect them.

Figure 5: Metadata Formats

JPEG: JPEG is an extensively utilized method for lossy compression of digital images derived from discrete cosine transform [43]. Every JPEG file is initialized at the binary value of '0xFFD8' and terminates with a value '0xFFD9'. There exist multiple special binary locations ('0xFFXX') in JPEG that are called 'Markers' [44] that convey a special meaning. Some important markers are EOI (end of image), SOI (start of image), SOS (Start of Scan), APPn (Application-specific), baseline DCT, SOIf0 (Start Of Frame) [8].

Within JPEG, the Exif data is segregated into 5 main Information File Directory (IFDs) into which the metadata is organised as follows: Exif, Primary, Thumbnail, Interoperability, and GPS. A visual description is represented in Fig.4.1. [13]

JPEG Markers [45] range from the start of the image, i.e., binary value '0xFFD8' to the end of the image, i.e., binary value '0xFFD9'. Each segment has the same structure, the initial two bytes contain a tag to identify the type of segment, the trailing two bytes mark the size of the segment without taking

into consideration the bytes for the tag but including these two. For example, the initial two bytes '0xFFD8' represent the JPEG file signature, the bytes 3 & 4 are the segment tags, 0XFFE1, and the length of the segment is 0xEDF6 bytes, the remnant of the segments contains the data. Post the SOI markers, the first group of segments holds the metadata for the file. [8]

When considering metadata, the most important segment is the APPn. The APPn marker has 16 application segments allocated for metadata ranging from APP0 to APP15 (binary val- ues:0xFFE0 to 0xFFEFc). The purpose of each segment is represented using a signature that follows two bytes defining the segment size. Metadata readers are designed such that they skip over a segment if they do not recognise the signature. Out of the application segments, the most commonly used ones are APP0, APP1, APP2, APP13, APP14.

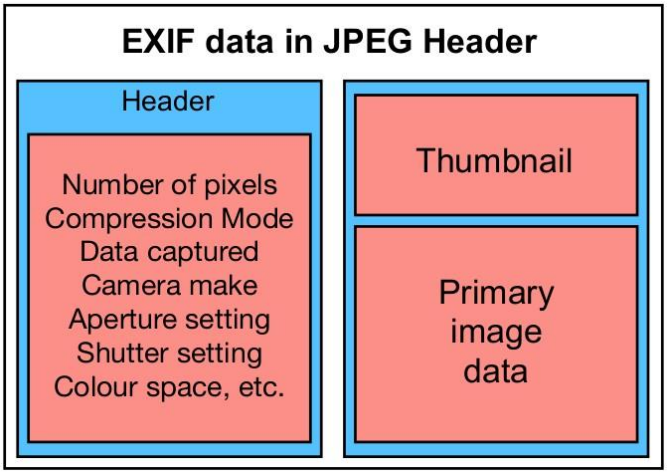


Figure 6: Exif data in JPEG Header

The table in Fig.7 [49] gives an overview of the application segments:

APP1 is followed by five other segments directly related to compression, namely: SOF0, SOS, DQT, DRI, and DHT. [9]

Huffman tables: Lossy compression of JPEG images can be handled by Huffman tables. These tables make use of Huffman coding and generate encoding schemes for individual characters completely based on the frequency generated by making use of tree structures. [11]

Quantization tables: Quantization tables are designed to filter out and discard high-frequency noise-like details and preserve the low-frequency information. The quantization table is designed to help the user determine the quality and degree of compression of the jpeg image. [12]

The relation between adobe and IPTC [45]: The formers flagship file management application, bridge, provides substantial support to IPTC across the available range of adobe applications like InDesign, acrobat, photoshop, and ImageReady with photoshop being the most commonly used application. GIMP is one of the most widely used open-sourced alternatives to photoshop although it offers limited IPTC and XMP editing facilities. [9]

Bridge [46]: Produced by Adobe, it is designed to function as a management application for images. Similar to the Windows explorer, a second APP1 is added to hold the XMP. For reasons that have yet to be determined, it also adds a segment that holds Photoshopstyle metadata (APP13) despite the image not having been edited on Photoshop, and the same information can be found, stored in the XMP segment.

Applications that aren't APP1, APP13, and APP14 are usually most likely to be written over. EXIF metadata [47]: This is stored within APP1 segments. Its presence can be determined by the EXIF Signature that can be seen immediately after the first couple of bytes. This signature contains the ASCII values of Exif followed by a couple of NULL values.

Application Segments	
APP0	This is a must for usage in JFIF information. It's predominantly used by applications for the purpose of compatibility with similar applications. The image doesn't appear immediately after processing via camera.
APP1	On creation and editing of a JPEG file, it typically has JFIF data embedded in the first segment (APP0) and EXIF data in the second segment (APP1). In actuality, they parallelly exist problem-free. XMP and EXIF both make use of this segment for metadata. Two of these segments exist if both XMP and EXIF. APP1 is followed by five other segments directly related to compression, namely: DQT, DRI, SOF0, DHT and SOS. [9]
APP2	Originally dedicated to FlashPix tags, this particular segment was introduced in 1996. Though outdated, some structural aspects still exist in the EXIF specification and can be encountered. Ex: Used by Photoshop for editing.
APP3	JPS Tag for Stereoscopic JPEG images
APP4	unassigned
APP5	unassigned
APP6	NITF Lossless profile
APP7	unassigned
APP8	unassigned
APP9	unassigned
APP10	Active Object (multimedia messages / captions)
APP11	HELIOS JPEG Resources (OPI Postscript)
APP12	Picture Info (older digicams), Photoshop Save for Web: Ducky
APP13	Adobe uses this for tagging in Photoshop
APP14	Adobe uses this to encode information into images concerning DCT filters.

Figure 7: JPEG Application Markers

4.1.1. Metadata Tags [9]:

1. IDF0 comprises a total of 231 tags that are displayed in their corresponding numerical order. The first 10 tags, i.e., (F0-F9) in IDF0, are implemented in both Exif and GPS tags as well. The plethora of available Exif tags can be observed in fig 8.
2. The number of GPS tags is well over 30. The Altitude, Latitude, and Longitude tags are omniscient. The other tags are device-dependent and hence vary.
3. Manufacturers mark their signatures by utilising different lengths for the initial string of bytes.
4. The general standard for considering the fingerprint of the jpeg image should be the hash value of the encoded image and not the metadata of the image as changes in the metadata do not affect the integrity of a file due to the actual data of the file not being modified.

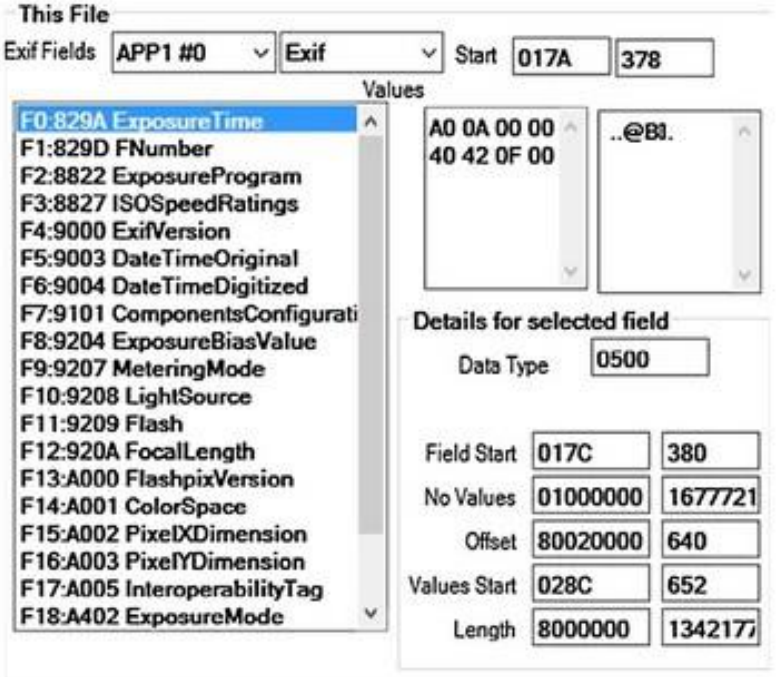


Figure 8: Tags in Exif Image File Directory [9]

Even though there is an abundance of free and paid tools to create, encrypt and decrypt metadata. There are very few tools that focus on establishing the integrity and authenticity of an image.

Metadata, image thumbnail, camera traces, compression signature, Huffman codec found in digital images provides a robust analysis that grants certainty and reliability of an image. When Image forgery is performed, the forger could conceal traces of tampering by altering the image further, followed by reforming the image using the appropriate EXIF format and all the necessary parameters such as image thumbnail, camera traces, compression signature, Huffman codec, etc. [9]

In [10], image authentication was proposed by creating a certificate that consists of a hash value (SHA 256) of the given image followed by a timestamp and a user detail. A generated certificate is then verified via a digital certificate issued by the Comodo certification authority. The drawback of this model is that the original file and the certificate are two different entities and can get separated during transmission, a malicious entity can modify the image and provide a new certificate without the knowledge of the user. Thus, it becomes imperative to insert the certification into the image.

Some of the most common parameters that are victim to tampering are XY resolution, Image width/length, make and camera model, exposure time, Data and time of the original and edited image, ISO speed rating, focal length, F.number, image size, interoperability index, shutter speed value, interoperability IFD pointer, aperture value, exposure bias value, thumbnail information, and max aperture value [8].

Windows unlike Mac OS and Linux enables us to edit multiple tags, some tags that can be edited are marked in "*" which can be seen in Fig.9

Figure 9: Modifiable tags in windows

Image tampering is composed of techniques that require foundational knowledge on image properties and high creativity.

4.1.2. Implementation of digital image authentication using forensic techniques:

Four steps are proposed in the implementation –

1. **Collection:**
    a) Documentation - Documentation encompasses the circumstances of the incident, the instrument concerned with the generation of the image, and the container device which accommodates the concerned image to be analysed.
    b) Saving and integrity verification - This involves generating 2 identical copies of the original image and generating hash values for all 3 images. The hash values of the copies are then verified with the original.

2. **Extraction of the image's technical features:**
    a) Format verification – The compression format of the image is verified by comparing the image headers with the corresponding detected format of the image. If the two do not match, the process is concluded.
    b) Feature extraction – On successful completion of the former step, the following is extracted:
        i. Camera traces – Footprints of the demosiacing, used to completion of pixels of the image on creation.
        ii. Image metadata
        iii. Compression signatures
        iv. Image thumbnail - Found at the header of the image file.

3. **Analysis of the image's technical features:**

a) Analysis of image metadata – It is imperative to verify if the digital image conserves the metadata at the time of capture, modifications made to an image may lead to loss of metadata generated during capture. Key metadata parameters include brand, orientation, compression by software, the orientation of the image thumbnail, model of the camera, date/time.
b) Analysis of image thumbnail - Encapsulates pixel-wise juxtaposition of the thumb- nail from the metadata file and the one post generation from the analysed image.
c) Analysis of camera traces – Involves verification of integrity and detects traces of tampering of an image without taking into consideration any pre-embedded and preextracted data. If the image exhibits traces of tampering, plausible inconsistencies can be found on the Y Plane, presuming that the color space used is YCrCb. Plane Y tends to endure a reduced loss of information in the case of Jpeg compression, and modifications can be detected.
d) Searching compression signatures – A compression signature is left behind in the header of the digital image post-editing.

4.1.3. Metadata tampering detection using Deep Learning [15]:

Development in Machine Learning techniques have led to the achievement of accurate prediction of meteorological information from images. Sun's altitude angle and parameters such as weather, humidity, and temperature can be utilized for detecting traces of tampering in images. Collation of meteorological attributes extracted from images and the adjoining attributes from weather databases at specified geographical conditions is performed.

The various resources that have been used comprise a large dataset called AMOS+M2, meta- data such as timestamps, GPS Location, etc, sun's altitude angle, other information based on the previously existing AMOS database and the Weather Underground Internet API. AMOS+M2 is trained to grasp various convolutional models for prediction. Several joint models based on multi-task learning, which perform prediction of all features concurrently are used.

The primary contributions of the paper considered here includes Analysis of meteorological data for images in comparison with metadata discrepancy, utilizing the advantage of multi-task learning on meteorological data and building a large dataset called AMOS+M2 consisting of more than 500,000 annotated outdoor images. The AMOS + M2 is trained to comprehend multiple convolutional prediction models where multiple joint models based on multi-task learning are used to carry out the prediction features simultaneously. The table (Fig.10) gives a gist of the datasets used.

Dataset	# of locations	# of images	Metadata	Meteorological information	Sun angle
Weather Image Dataset [13]	N/A	10K	N	weather	N
Multi-class Weather Image [16]	N/A	20K	N	weather	N
Glasner*et al.* [5]	10	6K	Y	temperature	N
Time of the Year Dataset [15]	10	23K	Y	temperature	N
AMOS+M2 (Ours)	638	500K	Y	weather, temperature, humidity	Y

Figure 10: Datasets used in [15]

Convolutional networks are used to predict the angle of the sun and its corresponding meteorological information. AlexNet is used to experiment with different loss functions owing to its high training speed and ResNet-50 to train the model for better accuracy.

4.1.4. Metadata Tampering involved:

1. The weather model produced the optimum results when the time was tampered with by about one or two months from the original since the other information only changed by short time frames. Incidentally, the temperature model achieves such a result when the tampering is done for around three to six months. The prediction of the sun's altitude angle performs

better the further away the tampering is done from the ground truth as the position of the sun constantly changes.

2. Detection of tampering on time - the weather model begets the best performance values in inconsistency detection when the duration taken into consideration lies between one to two months. The former is due to the small alterations in the sun's altitude, temperature, humidity, and angle. The model faces difficulties perceiving the differences in these properties.
3. The performance of the sun's altitude is directly proportional to the length of the tampering time as the angle of the sun at the same time of day differs largely by the number of months in between.
4. Detection of tampering on the location: The larger the tampered distance, the larger the performance of these models due to larger discrepancies in the meteorological features. However, in the particular instance, the model doesn't match its previous performances as the distance of 1000km is too minuscule to observe any changes in the sun angle.

4.2. Image Authentication from thumbnails [16]

Thumbnails are created via multitudes of operations including contrast adjustment, filtering as well as compression. Their respective model parameters estimate huge discrepancies based on the camera model and the software used for editing [48]. A thumbnail version of the original image is embedded into the image header. This thumbnail typically follows the 160X120 pixel resolution. Consider an image f(x,y). The thumbnail creation follows 6 steps: down-sample, pre-filter, crop, contrast and brightness adjustment, post-filter, and finally JPEG compression. If a discrepancy in the aspect ratio between the original image and the thumbnail can be observed, it means that either the image needs padding or cropping. Positive values imply that it requires padding whereas negative values imply cropping. Let's denote the cropped image as f'(x,y). The processing steps can be observed by the following:

$$t(x, y) = \alpha(Df'(x, y) * h1(x, y) * h2(x, y)) + \beta \quad (1)$$

t(x, y) is the thumbnail, h1(·) is the pre-filter, h2(·) is the post-filter, * is the convolution operator, and α and β are the multiplicative contrast and additive brightness adjustment terms. The model for thumbnail creation model can be observed in its entirety by 11 processing parameters. Of these 11 parameters, 2 are utilised for the thumbnail size, 1 for pre-filter, 2 for padding/cropping, 2 for brightness and contrast, and finally, 2 for post-filter.

5. Digital Image Processing

Digital image processing (DIP) deals with the manipulation of images, done through processing via an algorithm to generate new images that incorporate a part of the whole of the original image in tandem with modifications to meet business or entertainment goals. It involves altering the nature of an image to improve its pictorial representation for human interpretation or rendering it more suitable for autonomous machine perception. [3]

Improving pictorial information can include –

1. Enhancing the edges of an image to sharpen the appearance to make it more "crisp and cleaner", thereby increasing the aesthetics of the image as a whole. Figure 11 depicts an image before and after image sharpening.
2. Filtering "noise", i.e., the random errors in an image. Traditionally, there are 2 ways of filtering out noise – a) Linear model b) Non-linear model. The linear model is most popularly used due to higher speeds of processing but is limited due to the inability to preserve the edges of images, i.e., the discontinuous portions of the images are smeared out. Filters like Gaussian filter, mean

filter (edges are unpreserved), median filter (Edges are preserved), Wiener filter [4]. Figure 12 depicts the transitions in image quality from before and after noise removal.

3. Removing motion blur from an image; When an image is taken using a camera, the captured portion represents a period as opposed to a single instant in time. The exposure time of the camera lens remains so brief that it begets the falsity of an instantaneous moment. The blur results (Fig.13) from either an agile object or from prolonged exposure that is apparent on the image. [3]

(a) Original Image **(b) Sharpened Image**

Figure 11: Image Sharpening [3]

(a) Original Image **(b) De-noised Image**

Figure 12: Removing noise from an image [3]

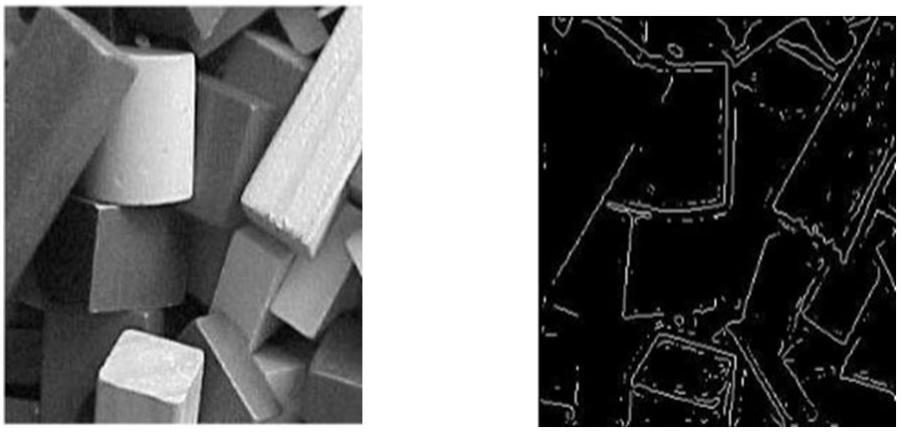
5.1. Rendering images for autonomous machine perception

1. Extracting the edges of an image; One application of this could be to leverage the measurements of the plethora of objects present in the image, provisioning the ability to compute the various segments of mensuration concerning the objects. Fig.14 depicts edge extraction of objects in an image.

2. Removing details from an image. During the extraction of parts, the remnants of the image become redundant. In Fig 15, image (a) is the original image of a buffalo, and image (20) is a blurred version that discards redundant details, i.e., the entire background of the buffalo. All the fine details of the image have been removed and the coarse structure of the image is retained.

(a) Original Image **(b) Blur-ridden Image**

Figure 13: Removing noise from an image [3]



(a) Original Image **(b) Edge-extracted Image**

Figure 14: Edge extraction from an image [3]

Image processing involves steps encompassing –

(a) Original Image **(b) Image with details removed**

Figure 15: Removing details of an image

1. Importing via image acquisition tools
2. Analysis and manipulation of the image
3. The output; either includes the altered image or a report based on the image analysis. These steps are spanned over the phases as seen in Fig.16

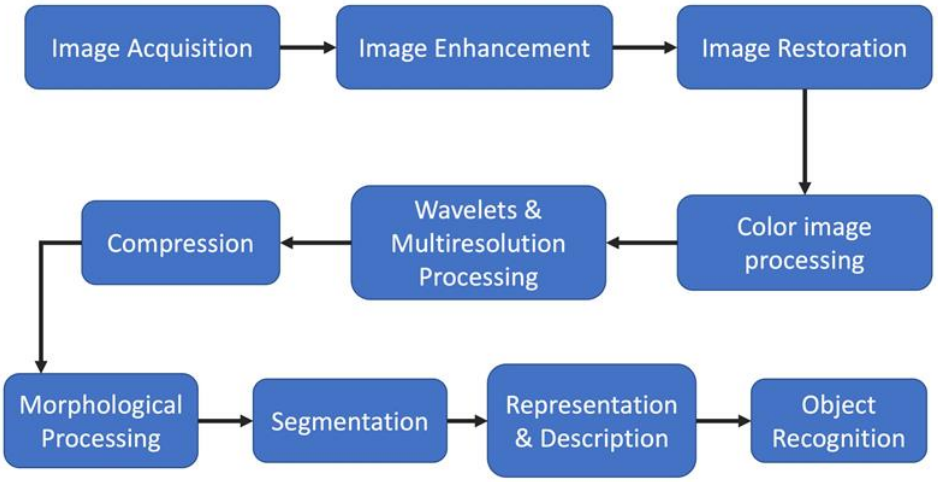


Figure 16: Phases of Image Processing

1. Image Acquisition – The image acquisition phase incorporates obtaining the concerned image in digital format along with minimal pre-processing like scaling.
2. Image enhancement – Enhancements are made to remove obscurity from images or to enhance features that are of interest within the image. This can include contrast, brightness, etc.
3. Image restoration – Image restoration also improves the appearance of an image but uses probabilistic or mathematical models of image degradation to do so.
4. Colour image processing – This phase concentrates on colour modeling and processing in the digital domain.
5. Wavelets and multiresolution processing – The various degrees of resolution within an image are represented by wavelets of which they form a core. Images are subdivided successively for pyramidal representation and data compression.
6. Compression - Compression consolidates the steps necessary to minimize the storage requirement to save an image or the bandwidth necessary for transmission.
7. Morphological processing - Morphological processing involves the tools required for the extraction of image components that are useful in the representation and description of the image.
8. Segmentation – Segmentation partitions the image into its constituent objects.
9. Representation and Description – This phase almost always follows segmentation. A chosen representation forms a part of a solution for transforming raw data into a suitable form for processing. Description involves extracting attributes that could be classified into the information of interest or for differentiating one class of objects from another.
10. Object recognition – Object recognition is a process that assigns a tag to an image based on its descriptors. [2]

Figure 17 depicts the DIP process flow.

All modification made to an image for malicious purposes can be associated with the following terms – Tampering, Manipulation, Forgery, Image forgery, and Image Generation [6].

Image manipulation refers to the process through which changes are introduced to an image with the help of software and other readily available tools and/or devices. There are many image manipulation

techniques, but they can all be broadly classified into two levels, pixel-level image manipulation, and content-level image manipulation.

Image Tampering refers to the process of introducing changes in an image either by removing, duplicating, or adding an object. Image tampering is a subset of image forgery. The figure below gives an overview of the relation between the various image modification techniques, as seen in Fig.18

6. Image Forgery

Image forgery refers to the manipulation of digital images to conceal some meaningful or useful information in the images to direct a viewer's attention towards misleading/falsified information. Manipulation is carried out employing photo editing tools like Photoshop and Gimp. Fig.19 uses the copy-move technique which is one of the most popular image forgery techniques, Fig.19a is the original image, and Fig.19b is the forged image. Through observation alone, it remains a conundrum to recognise Fig.19 as a forged image.

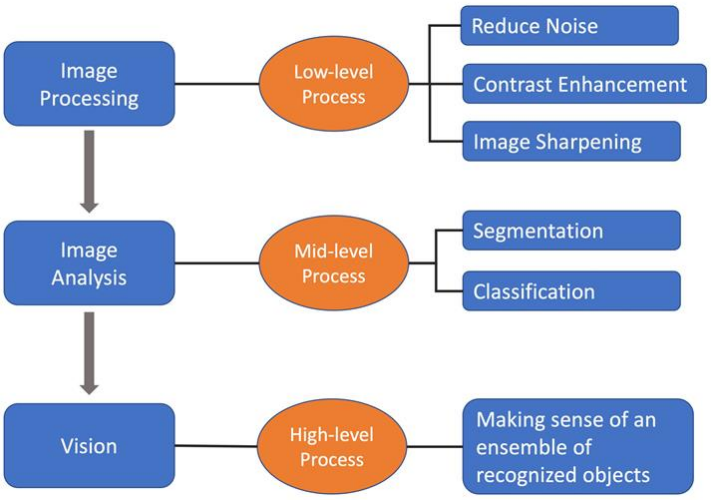


Figure 17: DIP Process flow [2]

Image tampering, cloning, and splicing are notable image forgery techniques that compromise the image authenticity and integrity. [5]

A famous example of image modification is the Kerry Fonda election photo controversy. In the 2004 presidential elections, an image of John Kerry and Jane Fonda speaking at an anti-Vietnam protest. The picture was later exposed as a politically motivated forgery to link Fonda, who was considered a traitor, to Kerry. Fig.20 contains the original images and the modified output. [6] Types of image tampering: The different types of image tampering techniques can be pre-dominantly grouped into the following three layers:

1. Acquisition-based Activities: A lot of data is left behind during the process of acquiring an image. In simpler terms, residual amounts of data can be obtained from every layer of acquisition of an image. This residual information ranges from anything pertaining to traces of CFA patterns or color interpolation filters. Other examples of remnant information include residual traces of noise such as PRNU left behind by camera sensors which is a default setting on most cameras. Silicet, two different devices would leave different information of the same image purely based on differences in acquisition steps. The analysis of these differences in data could potentially help with the identification of the acquisition device. As it could be seen in Fig.21. The following Fig.22 shows different CFA patterns
2. Coding-based Activities: Most modern-day devices generally use the JPEG compression format due to its high efficacy regarding storage and transmission. This piques interest in the

study of compression formats and their history. The fact that different imaging software makes use of varying compression parameters and implement different quantization tables is grounds to believe that the analytical study of quantization matrix inconsistencies can be instrumental in image forensics for forgery detection. A method of alignment distinguishing of DJPEG compression via identification of DCT coefficients of the original image was proposed by Ferret et al. The figure below (Fig.23) is an example of compression history that can be studied.

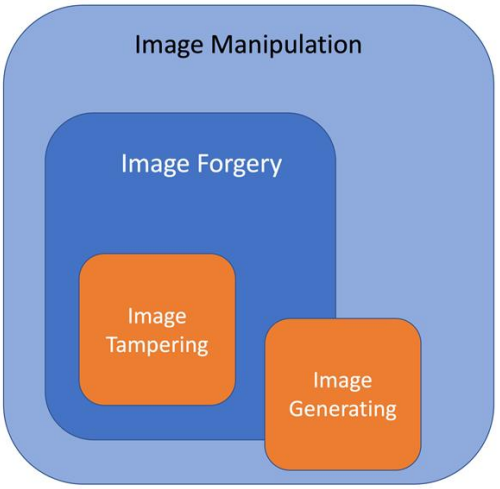


Figure 18: Relationship between different malicious image modification techniques

(a) Original Image

(b) Forged Image

Figure 19: Forged image example [5]

3. Editing based Activities: Digital footprints are also left behind when editing software is used to morph an image. Editing techniques such as geometric transformation which encompasses processes such as rotation or resizing have interpolation of pixels as a prerequisite to these tasks. The employment of these techniques results in trace amounts of detectable data on the said image due to interpolation values. Additionally, alteration of subparts of the image constituting changes in the saturation, lighting, contrast, etc also result in remnant data. Techniques involving median filters such as denoising or blending can be used to hide the data remnants of previous morphing attempts. Copy- move, erase-fill, and cut-paste are three major actions that can be leveraged on the image for graphic modifications, where, Copymove is more easily detectable through human visualisation than the latter two techniques due to repetitions being more perceptible to the human eye. To mask any form of tampering on images, a plethora of techniques such as hue moderation, blurring, resampling, JPEG compression, exposure manipulation, noise adding, palette tempering, etc. [6]

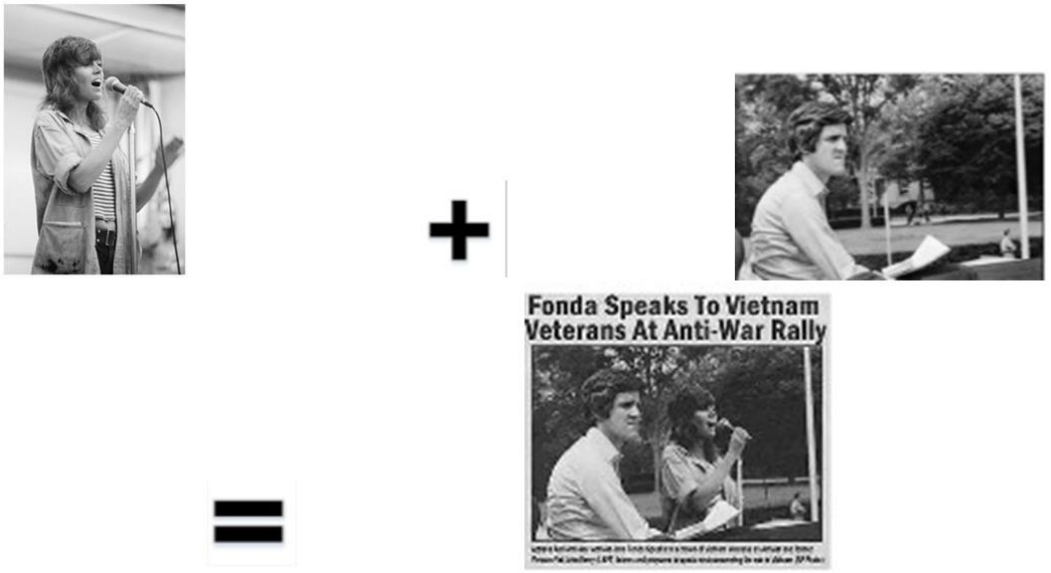


Figure 20: Kerry-Fonda election photo controversy

a) Copy-move tampering – The most commonly used image tampering technique where a part of the image is covered to add or remove data. Textured regions are utilised for copy-move tampering. Textured areas have identical colour, dynamic range, and noise variation properties, it remains undetectable to human vision.
b) Image splicing – Production of spliced images is done via bounding photographic images together.
c) Resize – Resizing incorporates geometric transformations used to minimize or maximize the size of an image either in part or completely. Technically the process involves interpolation of pixel values within local neighbourhoods.
d) Cropping - Cropping involves cutting off borders or resizing the canvas area of an image. Generally, cropping is used to remove border information.

Results on the median value of various datasets and interpolations

No CFA:	bilinear 1.58, bicubic 1.55, gradient 1.67, median 1.81
Ideal:	bilinear 1.16, bicubic 2.13, gradient 2.04, median 2.01
Canon EOS:	bilinear 2.00, bicubic 1.90, gradient 1.89, median 1.96
Nikon D50:	bilinear 1.73, bicubic 1.79, gradient 1.83, median 1.81
Nikon D7000:	bilinear 2.20, bicubic 2.06, gradient 1.72, median 1.89
Nikon D90:	bilinear 1.99, bicubic 1.92, gradient 1.66, median 1.92.

Figure 21: Various Device Information

e) Noising or blurring – When images are manipulated with the above techniques, the manipulation can be easily viewed due to a variety of features such as harsh colour change, improper backgrounds, etc. These are very obvious to the human eye and can easily be

detected, but these obvious features can be made inoperative by introducing traces of blur and background noise where the manipulation is visible. Fig.24 is a structural diagram of Image Forensics

7. ML – Based Image Forensics [17]

Machine learning is leveraged to comprehend various complex patterns from a set of features and enable classification, some ML* based techniques are listed below –

1. SVM-based image forensics – Support Vector Machine algorithm is highly preferred for classification tasks due to the accuracy of the outcomes. The paper mentions i) Remnants of mean, entropy, and variance left by DJPEG (Double JPEG compressed) images by using SVM classifier. ii)Derived statistics from the DCT histograms that are based on the FSD* to differentiate between single and double JPEG compressions. iii)Detection of copy-move or splicing using a technique that makes use of SVM classification of LBP* descriptors that are taken from the block DCT in chroma channels. SVMs are often used in the identification of camera models for multi-class classification that is based on high order features taken from the respective images or the PRNU noise pattern produced by the different camera models.

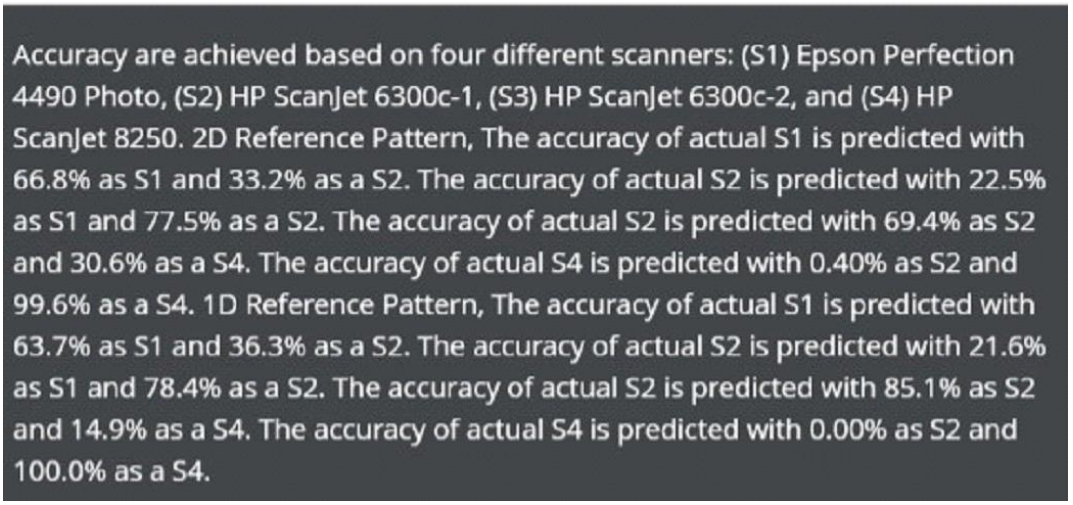


Figure 22: CFA Patterns

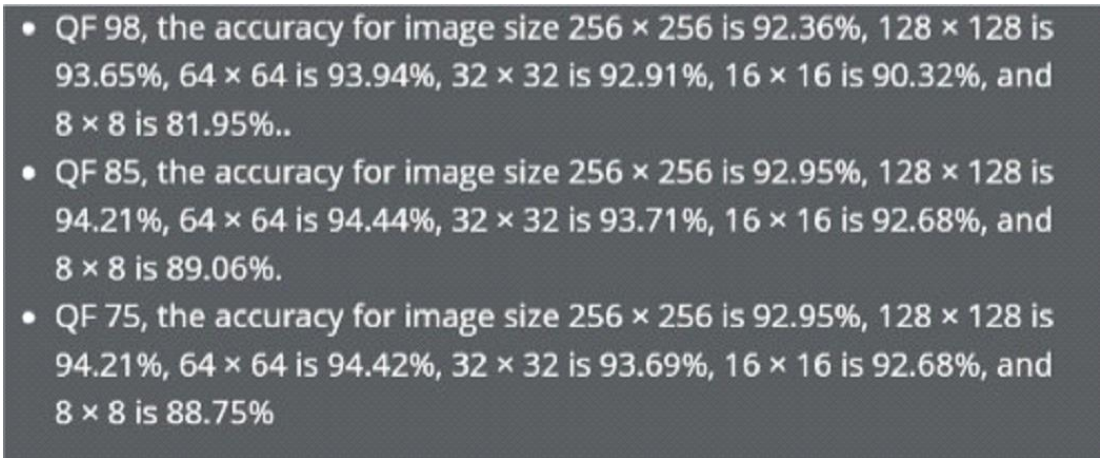


Figure 23: Compression Values

2. CNN-based image forensics - Both binary and multi-class Convolutional neural networks are implemented in operations like median filtering, blurring, and resizing. This approach was later extended by using each image to patch to distinguish between camera models. Although these

networks are not extensive with only three or four convolutional layers. The method of considering completely self-learned features, without forcing the initial layers, is useful for detection, as long as sufficient training data is available. 3) The primary task of image forensics is to deal with a plethora of algorithms based on analysing the statistics and recognising patterns. It's also dealing with the improvement of the computational capabilities in the ML methods, specifically in Deep Learning methods. These have shown effectiveness in multiple forensics competitions.

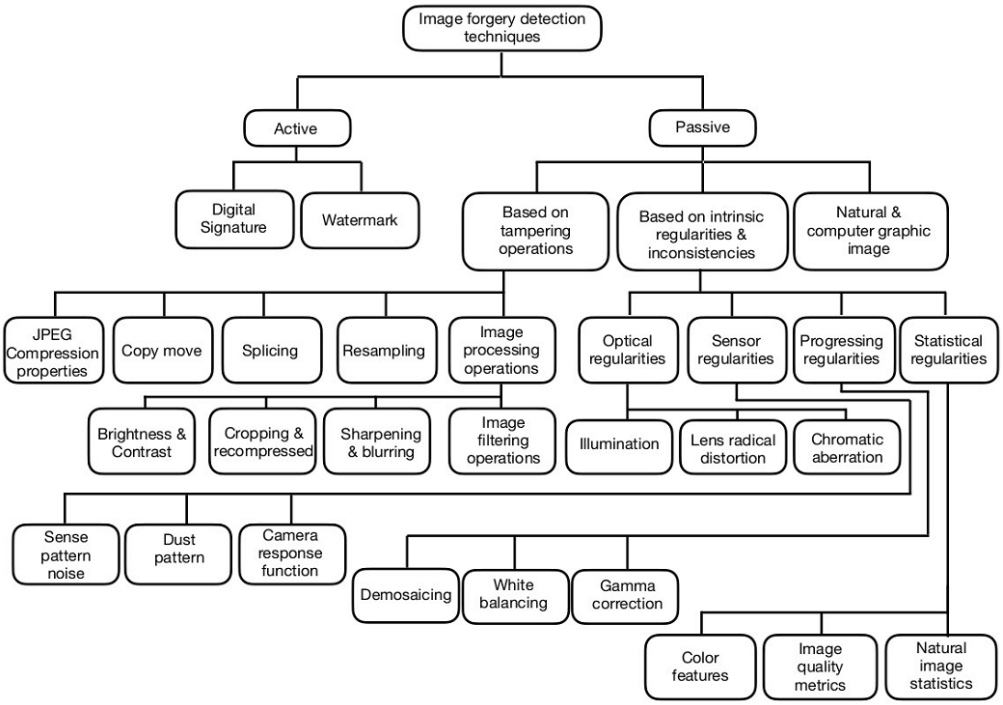


Figure 24: Image Forensics Structural Diagram

3. Counter Forensics: This term refers to all the proposed solutions towards bypassing analysis done via forensics.
   a) The addition of noise dithering decreases the gaps in the histograms of DCT coefficients. The blocking artifacts are hidden by the employment of a smooth operation done to hide JPEG compression traces. Dither is a noise that is intentionally applied to randomise the quantization error. This prevents patterns that appear on a large scale that include color banding in images.
   b) Dithering is a specialised method that results in the removal of gaps and picks in pixel histograms was proposed as a solution for concealing the traces of enhancement in the contrast of images. We can hide the remnants of resampling by perturbing the high image frequencies with noise while it's being resampled.
4. Adversarial inputs are introduced to a Machine Learning algorithm by an attacker to intentionally cause the model to make errors, they are analogous to optical illusions. Developments in Deep learning led to the creation of Generative adversarial networks (GANs) that has a higher success rate at deceiving forensics investigators and are referred to as ad versarial examples. Adversarial examples utilise perturbations on images to in turn cause the system to make false decisions. The perturbations can be extracted by estimating the input image's loss function, such as using the FGSM method. Both the JSMA and FGSM adversarial attacks can be employed to deceive the CNN camera model identification, due to this most Deep Learning models are vulnerable to adversarial attacks. Researchers have tried improving the DL algorithms by retraining the classifier with adversarial examples, but this still left the model vulnerable to powerful attacks.

8. Copy-Move Forgery Detection using Brute-Force Matching [22]

The active technique comprises real-time authentication of images via knowledge that is already known. These images are digitally watermarked, so by knowing this data beforehand, we can authenticate them by using the digital signature method.

The passive method is used when no previous information about the image is known. This type of detection is harder to recognise as no information is known beforehand. Within this method, we find various techniques of tamper detection based on the type of tampering done to the images i.e., retouching, splicing, and copy-move. This paper proposes two methods of copy-move detection, namely: Block-based and Keypoint-based.

Block-based method: the source of input is divided into two sets of blocks, namely, overlapping and non-overlapping. The forged regions are acquired by matching the above-mentioned blocks.

Keypoint-based method: The tamper is detected by looking for areas with high entropy (a.k.a key points) and extracting descriptors from these. This is a less complex method owing to its faster process and lesser calculations. This method is superior to block-based as it overcomes the shortcomings presented in the latter.

This method is divided into 4 main phases. The input consists of an image where copy-move forgery has been applied:

Phase 1: Adaptive Over-Segmentation

This phase identifies and segments the input image into one of the two blocks: non-overlapping and irregular. SLICO, a zero parameter version of SLIC* is used for the image segmentation process. The initial size of the super pixels is essential to get an accurate measure of the forgery region. We can acquire the initial size via a DWT. This process will be complete in 4 steps:

1. A four-level DWT is applied to the input. The low and high-frequency component's frequencies are obtained.
2. An estimate of the low-frequency distribution is taken.
3. We estimate the initial size S.
4. SLICO is applied. This adaptively segments the inputs and outputs the total number of IBs*

Phase 2: Block Feature Extraction

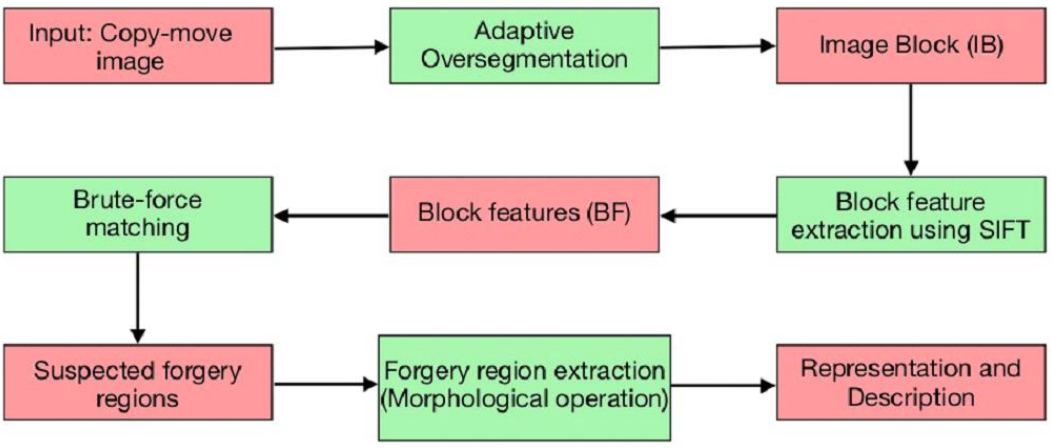


Figure 25: Method of detecting copy-move forgery

This phase focuses on extracting features from individual image blocks vis SIFT. The detection and explanation of local features are done by SIFT. Local features indicate the description of image patches

of single objects and also the representation of the image patch texture. This phase follows the following steps:

1. Find image key points
2. Draw miniature circles on the key point location
3. Compute descriptors from key points

Phase 3: Brute Force Matching

This involves the simplest matching of sub-strings. This requires two inputs consisting of a pattern (to search) and text (search from). The pattern is initially aligned with the text. Post this, each character is compared to the character on its right until a match or mismatch is detected. While the pattern has still not been found, the pattern is realigned by shifting its position to the right by 1 and the process repeats itself. This method makes use of 3 thresholds: TRp* and TRb*. Good feature points are identified when the TRp is higher and are compared to their corresponding image blocks via TRb once identified. This step yields the regions where forgery is suspected.

Phase 4: Forgery Region Extraction

This phase utilizes morphological close operation to detect more accurate regions of suspected forgery. These operations are dependent on the shape of the image. It requires 2 inputs: the original as well as the structuring kernel. The Kernel dictates the nature of the operation. The operation is essentially dilation accompanied by erosion. This is very useful in terms of filling gaps and upholding the shape of the region

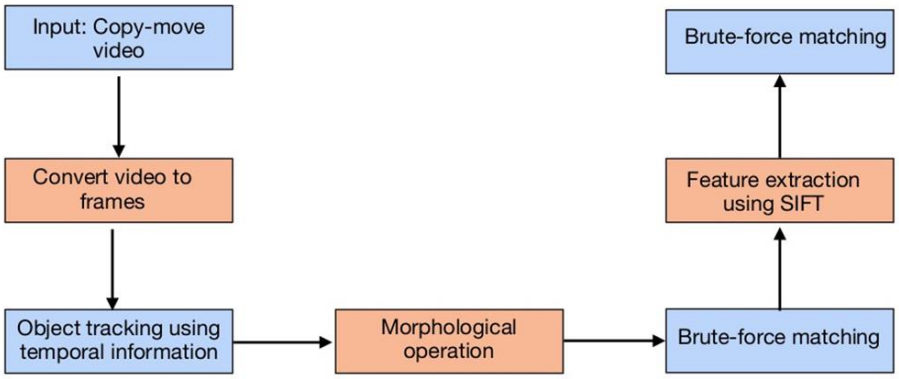


Figure 26: The process of Brute Force Matching

The model was implemented on Raspberry Pi3 using Python Language with OpenCV. Python version 2.7 and OpenCV version 3 are used. Window 7 is used as an operating system. OpenCV-Python is a library of Python bindings designed to solve computer vision problems. The libraries Numpy, Opencv2, Matplotlib, Pywt, and morphology are used for the implementation purpose. cite this part. Not edited the results of the experiment are shown in the below diagram (Fig.27):

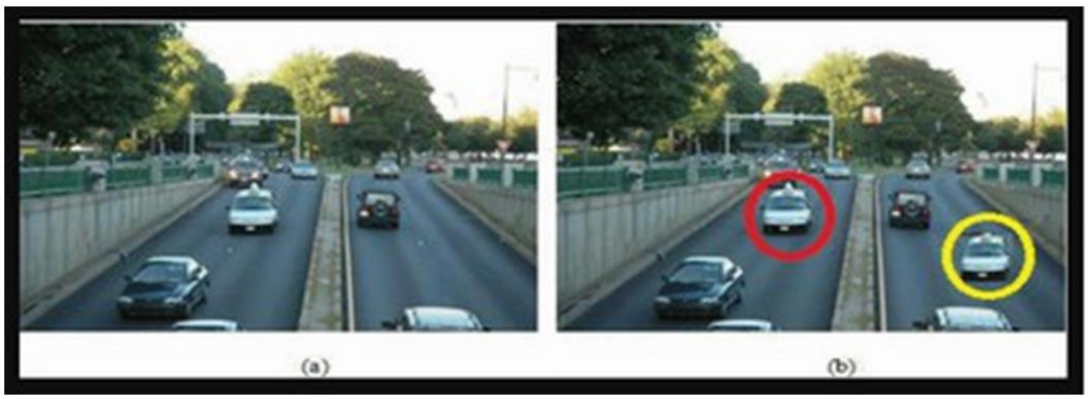


Figure 27: The results observed from the experiment

Conclusion: This method showed the advantage of low computational time and good performance. The non-overlapping method gave better detection results and went beyond the limitations set by the overlapped method.

9. Splicing Detection in Tampered Blur Images [20]

Splicing detection is the technique of extracting part of an image and embedding it on another image to render the appearance of an authentic image. Splicing detection turns into more of a challenge when the forged image is further processed, such as blurring the edges of the spliced portion, the addition of noise, resizing, rotation, etc.

One proposed way to detect splicing is by observing the inconsistencies of different properties of the image in different parts of the image. Differences in the blur around the spliced portion and the original image are one such example. This can be effective even when noise is added to the forged image.

Blurring can be categorised into motion blur, out of focus blur, and artificial blur:

1. Motion blur is caused when either the camera or the object is in motion
2. Out of focus blur is as the name implies - when the camera is out of focus
3. Artificial blur involves the addition of blur manually using editing tools on an image

When the spliced portion contains a blur of a variation different to that of the original image, the ease of detection augments in the presence of some kind of tampering, in this case, splicing, this is analogous to the detection of an anomaly that doesn't match the other parts of the tampered image. The blurring of an image is represented using the equation

$$G = I * K + N \qquad (2)$$

I=sharp image, K = blur kernel (represented using a 2d matrix), N = noise matrix, * = Convolution

Blur kernel for out-of-focus blur has values around 1 and around 0 for motion blur. Blur kernel distributions can be approximately depicted as a Gaussian distribution using the formula given below (Fig.28).

K − the estimated blur kernel
Γ − gamma function μ–mean
σ − standard deviation
γ(> 0) − shape parameter

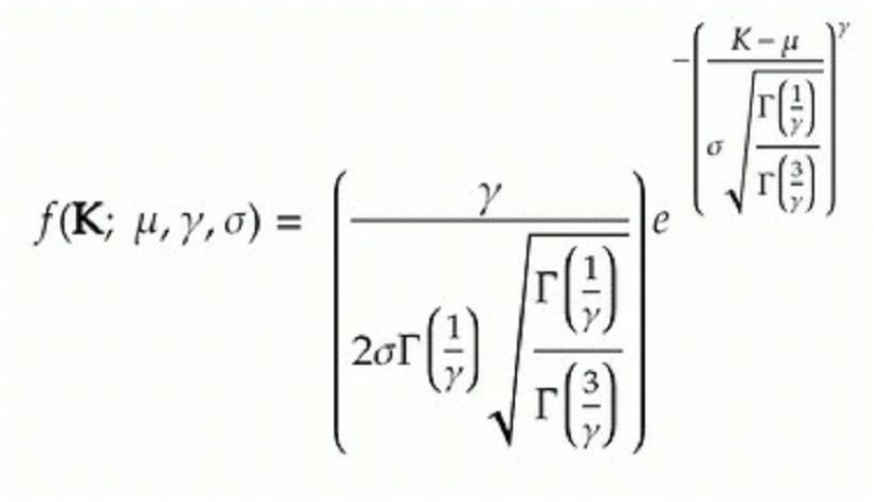
Motion and out-of-focus blur kernels have different characteristics which are used to differentiate between the two blurs in images. The standard deviation and shape parameter of the GCD of the blur kernels are important statistics that can be used for the classification of the blur types. There is a method proposed in which the image is divided into several blocks and the required characteristics are calculated for each block which is then compared to conclude the blur kernel.

10. Counter – Forensics [17]:

We can group all the attacks done in ML-based environments by i) influence ii) specificity and iii) security.

1. Influence: This can be further grouped into Causative and Explorative. In Causative, the training data is fed malicious data by the attacker. The learning parameters, in this case, are

changed because adversary data is fed into the model. In Explorative, malicious content is fed into the testing data and the training data is untouched. In this case, the attacker intends to either misclassify data by using adversarial examples or to obtain data from these models.



$$f(\mathbf{K};\ \mu, \gamma, \sigma) = \left(\frac{\gamma}{2\sigma\Gamma\left(\frac{1}{\gamma}\right)\sqrt{\frac{\Gamma\left(\frac{1}{\gamma}\right)}{\Gamma\left(\frac{3}{\gamma}\right)}}} \right) e^{-\left(\frac{K-\mu}{\sigma\sqrt{\frac{\Gamma\left(\frac{1}{\gamma}\right)}{\Gamma\left(\frac{3}{\gamma}\right)}}} \right)^{\gamma}}$$

Figure 28: Formula

2. Specificity: This can be grouped into Targeted or Indiscriminate. In targeted, the attacker tried to reduce the classifier's performance via deception of specific algorithms or sam- ples. In Indiscriminate, the attacker's final goal is more flexible. They target classes of algorithms instead of a specific algorithm.
3. Security violation: This can be grouped by Integrity and Availability. In Integrity, the attack intends on the misclassification of malicious data as normal. That is done by attempting to increase the number of false negatives errors during the classification of adversarial samples. In Availability, the attack intends on causing classification errors of any possible types that include both false positive and false negative errors.

10.1. Counter-forensic attack model:

1. Attacker's goal: The image is misclassified by making a trade-off with integrity by slightly distorting the image to cross a particular boundary of a decision to reduce the visual distortion while simultaneously increasing the loss function.
2. Perfect Knowledge:
   a) The most optimum attack would be a gradient-based attack that is based on descent solutions in situations where the detectors are more complex.
   b) Existing techniques generally get canceled by the rounding of pixels and render attacks useless when minuscule perturbations are applied to them.
   c) The primary challenge with most scenarios about perfect knowledge is that most counter forensics attacks are used within the feature domain. Controlling the distortion within this situation proves to be a hard task because the pixel and feature domains are non-invertible. To put it in general, an average strategy is deployed in two steps: The first being the minimization of the feature domain distortion and the second being the implementation of a new minimization within the pixel domain repetitively until a close desire attack is achieved.
3. Limited-Knowledge: Counter-forensic attacks are classified into 3 types. Namely: At- tacks on a surrogate detector, Laundering type attacks, and universal attacks. 4) Attacker's knowledge: i) An attacker can either possess Perfect knowledge or limited knowledge by observing what the attacker knows concerning features, classifier architecture, training data, decision functions, and the learning parameters. In the case of Perfect knowledge, the attacker possesses full

knowledge concerning the forensic algorithm. In the case of limited knowledge, the attacker only possesses bits of data regarding the algorithm.

10.2. Generative Adversarial Network (GAN) image forensics [18]

1. Unstable noise cues of low levels can be destroyed by the application of similar pre- processing to both real and fake images.
2. GANs are essentially generative models that actively learn about the data distribution with zero supervision. Presently, these are proven to be the most effective models when it comes to image generation and these images could reach high levels of quality to the point where even the regular human eyes cannot differentiate.
3. Deepfakes, a technology built on GAN can be used to seamlessly overlap and substitute an individual's face with a second individual's/animal's face.
4. To enhance the generalisation of Convolutional Neural Networks to the model, a novel approach to pre-processing, e.g., Gaussian blur and Gaussian noise is performed in the training phase.
5. The traditional forensic technique employs enhancement of high-frequency pixel noise and uses it to focus on low-level pixel statistics, whereas in [18], these low-level high- frequency noise is destroyed to force the forensic classifier to be more susceptible towards more intrinsic and meaningful features.
6. Generalization abilities of the most forensics models are ignored by most works. Their methods are usually just trained and tested on the same type of generated image. [18] mentions a paper that effectuates the activation of different regions within a latent vector for the real and fake classes using a new autoencoder-based architecture. A learning-based forensics detector is devised that accustoms itself to new domains while handling scenarios with a minimal availability of target domain fake examples during training.
7. The paper proposes a model based on image preprocessing to solve this problem. The use of an image pre-processing step during training is what differentiates this model from other GAN forensics works. Here, the motive is to destroy all existing low-level unstable artifacts. Within the GAN images, thus imposing the forensics discriminator to concentrate on more inherent forensic clues. The proposed method introduces a pre- processing step by employing smoothing filters or noise by deliberately depressing or destroying these low-level high-frequency clues. By performing the above, the forensic classifier is forced to imbibe intrinsic features that have better generalization ability by improving the low-level similarity between real and fake images.
8. By using the proposed model, there is an improvement in the TNR by close to 10an overall improvement in the ACC as well thus showing that. And this can show that the method of preprocessing operation is effective for improving generalization ability on unseen generated images.

10.3. Detection of GAN-generated Images of social media [19]

A multitude of papers, in general, proposes to detect tampering of images using statistics elicited from their wavelet decomposition, whereas the main focus is image-to-image translation, a process-driven towards the modification of the target attributes by translation of one possible representation of a scene into another one. The challenge with social media websites is the routine compression performed on image uploading which impairs the performance of most forgery detectors. The following detectors are considered – Gan discriminator, Steganalysis fea- tures, an Ad-Hoc CNN(Cozzolino2017), a constrained CNN(Bayar2016), a network comprising of 2 convolutional layers of 32 and 64 layers (Rahmouni2017), DenseNet, InceptionNet v3, and XceptionNet. A subsection of the ImageNet dataset with 10 different categories of images was utilised with each category containing real and fake images.

A total of 3 scenarios are considered, 1) The original uncompressed dataset, 2) Twitter-like compressed images with training mismatch, 3) Twitter-Like compressed images.

Scenario-1: The original uncompressed dataset in this scenario, all detectors are trained and tested on the various categories of images and the accuracy of manipulation detection is com- puted. The results can be seen in figure m1. Among all, the highest average accuracy was obtained by the Cozzolino2017(Ad-HocCNN) model. It provides accurate predictions for all manipulations except winter2summer. Among the deep networks, XceptionNet provides the best results. Figure m1, also reports the average classification accuracy of each manipulation in the last row, this directs us to the most challenging cases being winter2summer and map2stat, while the most easily detected were horse2zebra and some painting style transfer.

Scenario-2: Twitter-like compressed images with training mismatch While the results from the former experiment, i.e, the case when we have direct access to the user's raw edited im- age, this is not the case in the real world. In the real world, images will most likely be taken from social media where the user will post them, to reach as many people as possible. Social media poses a unique challenge because of the automatic image compressions. Their image compressions generally ruin the minute patterns which form the basis for most classifiers. Hence, leading to poorer performances. Deep neural networks were more resilient than shallow neural networks. XceptionNet, in particular, had an accuracy of 87.17%. Just around 7%worse than the previous case. This proves that the deeper neural networks learn more from an im- age, that is, they do not rely on micropatterns only but also other compression surviving features.

Scenario-3: Twitter-Like compressed images the last case assumes the worst-case scenario, with a mismatch between the test and training set. Training the detectors on compressed images directly posits forward a better likelihood of detection of fake images on social media. Steganalysis and Cozzolino2017(Ad-Hoc CNN) have good performance metrics though falls 10when compared to the uncompressed scenario due to loss of information beneficial to spotting fakes as an account of lossy compression. XceptioNet provides the best performance with an accuracy of 89.03%.

11. Tools

a) Autopsy

Autopsy is a tool designed for hard drive investigation implementing features like keyword search, malicious file detection, timeline analysis, email analysis, registry analysis, EXIF analysis, multi-user cases and many more.

b) FotoForensics

FotoForensics utilises a complex algorithm to decode any photoshopped or manipulated pictures. It makes use of Error Level Analysis to identify the regions of an image that have varied compression levels. When considering JPEG images, the entirety of the image exists roughly at the same error level. If any portion of the image it found to be at a different error level, then we could point towards a modification.

c) JPEGSnoop

JPEGSnoop can help you detect various settings that are used in digital cameras when taking photos (EXIF metadata, IPTC). JPEGSnoop reports what digital cameras or software may have been used to create that image.

d) Ghiro

The following features are provided by the tool:

- GPS Localisation

- Thumbnail Extraction
- MIME Information
- Metadata Extraction
- Error Level Analysis
- Hash Matching
- Signature Engine

A web interface can be used to access all features of Ghiro. Ghiro makes the provision to upload a bunch of images, navigate reports, acquire a quick or in-depth understanding of image analysis. You can collate images into cases, find any type of analysis data, acquire photos around a particular GPS location, administer users and view all images present in the system.

e) Exiftool

ExifTool is a free and open-source software. It is used to modify an image, PDF, audio, and video metadata. It is platform-independent and readily acquirable as a command-line application and a Perl library. We can find this tool incorporated into different digital workflows while supporting different metadata types like EXIF, JFIF, ICC Profile, IPTC, ID3, XMP, FlashPix, Photoshop IRB, GeoTIFF, and AFCP, along with the manufacturerspecific metadata formats of different digital cameras.

f) Forensically

The tools' functionalities comprise noise analysis, error level analysis, magnifying functions, level sweep, clone detection, and many more.

g) Amped Authenticate

Amped authenticate takes the number one spot among forensics software for introducing the processing history of a digital image. It contains a suite of highly capable tools to pinpoint if an image remains unaltered. If an image is original and unaltered, an original created by a device or a manipulated image made via editing software, making its authenticity as evidence in court questionable. Various intelligence agencies and digital forensics experts worldwide make use of Amped Authenticate.

h) FFmpeg

FFmpeg is a free and open-source software project made up of an expansive suite of pro- grams and libraries designed to handle video, audio, other multimedia files, and streams. The FFmpeg program is itself located at its core and designed for command-line-based pro- cessing of audio and video files. It is extensively utilised in video scaling, transcoding, video post-production effects, compliance standards (SMPTE, ITU), and basic editing (trimming and concatenation).

i) Four match

A photoshop extension provisions the necessary evidence that ensues proof as to weather a JPEG file has been modified at any point from the time of creation.

j) Exiv2

Exiv2 is a Cross-platform C++ library and a command-line utility for managing image metadata. It provides easily accessible read and write functionalities to XMP, Exif, and IPTC metadata, as well as the ICC Profile embedded in the digital images. Fig.29 and Fig.30 display the comparative study of various forensic tools.

12. Case Studies

a) CASE 1 [23]

a) Background: This case involves an NRI residing in Dubai who fell victim to the accused who was posing as a young girl living in Kolkata, the accused used many such emails to start an email conversation with the victim. Along came the demands for money and gifts to which the victim complied expecting sexual 'favours' in return. The victim stopped the conversation as he received no such favours from the many 'girls' he was sending money and gifts to. When the accused stopped getting money and the gifts, he resorted to blackmailing the NRI and threatened to use their email conversations as proof if need be. The accused even blamed the NRI for being responsible for the suicide of one of the so-called 'girls'. The accused also forged several documents from CBI, High Court, etc. to intimidate the victim. This worked as the victim lived in fear of being arrested for being responsible for the death of a young girl. The accused extorted a sum of 12.5 million Rupees from the victim over sometime, all this took on the victim to the point that he considered committing suicide.

	Autopsy	FotoForensics	JPEGSnoop	Ghiro	Exiftool	Amped Authenticate	FFmpeg	Exiv2
Release Date	March 2001	August 2007	June 2017	2013	November 2003	2008	December 2000	2018
Main function	Autopsy is a graphical interface to the command line digital investigation analysis tools in The Sleuth Kit. Together, they can analyze Windows and UNIX disks and file systems (NTFS, FAT, UFS1/2, Ext2/3).	FotoForensics permits users to upload an image by specifying a URL. However, sometimes users upload URLs that point to web pages that contains images, rather than the direct URL to the image. When this happens, FotoForensics tries to automatically identify the primary image on the page.	PEGsnoop is a free Windows application that examines and decodes the inner details of JPEG, MotionJPEG AVI and Photoshop files. It can also be used to analyze the source of an image to test its authenticity.	Ghiro is a fully automated tool designed to run forensics analysis over a massive amount of images, just using an user friendly and fancy web application.	ExifTool is a free and open-source software program for reading, writing, and manipulating image, audio, video, and PDF metadata. It is platform independent, available as both a Perl library (Image::ExifTool) and command-line application	Amped Authenticate provides a suite of powerful tools to determine whether an image is an unaltered original, an original generated by a specific device, or the result of manipulation using a photo editing software, making its admissibility as evidence questionable.	FFmpeg is the leading multimedia framework, able to decode, encode, transcode, mux, demux, stream, filter and play pretty much anything that humans and machines have created. It supports the most obscure ancient formats up to the cutting edge.	Exiv2 is a Cross-platform C++ library and a command line utility to manage image metadata. It provides fast and easy read and write access to the Exif, IPTC and XMP metadata and the ICC Profile embedded within digital images in various formats.
Language	Version 2 of Autopsy is written in Perl. Autopsy 3.0 is written in Java using the NetBeans platform.	Perl	C++	Python	Perl	C++	C	C++
Platforms they run on	Linux,Mac OS X,Open & FreeBSD,Solaris, Cygwin	Fotoforensics is a web-based system. It works best with HTML5 and CSS3. This includes most up-to-date web browsers.	JpegSnoop works on most of the common platforms like Linux,Mac OS, Windows etc.	Ghiro requires users to import in virtualization software (like VirtualBox or VMWare) and configure the networking.	Exiftool works on most of the platforms such as Windows, macOS, Linux	It works on most of the common platforms like Linux,Mac OS, Windows etc.	x86, ARM, PowerPC, MIPS, DEC Alpha, Blackfin, AVR32, SH-4, and SPARC; may be compiled for other desktop computers	Exiv2 is supported on Linux, macOS, Cygwin, MinGW/ msys2 and Microsoft Visual Studio.

Figure 29: Comparative study of various forensic tools

b) Investigation: The victim approached the police with all the email conversations but since all of them had masked headers, they weren't of much help. None of the emails could be traced back to Kolkata as the accused claimed. However, some of the emails could be traced back to the office of a large cement company, where the police raided and seized several electronic items which were concluded to be the source of the different emails with the help of digital forensics.

	Autopsy	FotoForensics	JPEGSnoop	Ghiro	Exiftool	Amped Authenticate	FFmpeg	Exiv2
Latest release	4.18.0	8.1	1.8.0	0.2.1	12.16	v2021 Build 19348	4.3.2	0.27.3
File Type	Autopsy analyzes major file systems (NTFS, FAT, ExFAT, HFS+, Ext2/Ext3/Ext4, YAFFS2) by hashing all files, unpacking standard archives (ZIP, JAR etc.), extracting any EXIF values and putting keywords in an index.	FotoForensics only evaluates pictures. The picture must be a JPEG, PNG, or WebP.	JPEGsnoop will open and attempt to decode any file that contains an embedded JPEG image such as .JPG , .THM, .AVI , .DNG , .PSD, . CRW, .CR2, .NEF, . ORF, .PEF , .MOV , .PDF.	Windows bitmap .bmp, Raw Canon .cr2, Raw Canon .crw, Encapsulated PostScript .eps, Graphics Interchange Format .gif, JPEG File Interchange Format .jpg or .jpeg, Raw Minolta .mrw, Raw Olympus .orf, Portable Network Graphics .png, Raw Photoshop .psd, Raw Fujifilm .raf, Raw Panasonic .rw2, Raw TARGA .tga, Tagged Image File Format .tiff.	supports many types of metadata including Exif, IPTC, XMP, JFIF, GeoTIFF, ICC Profile, Photoshop IRB, FlashPix, AFCP and ID3, as well as the manufacturer-specific metadata formats of many digital cameras.	Amped Authenticate provides a very user-friendly interface that allows to open an image in the most common formats (JPEG, HEIF, PNG, TIFF, BMP, etc.)	FFmpeg supports AIFF, ASF, AVI and also input from AviSynth, BFI, CAF ,FLV, GIF, GXF, General eXchange Format, SMPTE 360M.	Exiv2 can now read TIFF images and a number of TIFF-based RAW image formats, including Nikon NEF, Canon CR2, Pentax PEF, Sony SR2, Adobe DNG and Minolta MRW formats.
Cost	Free	Free	Free	Paid	Free	Free	Free	Free

Figure 30: Comparative study of various forensic tools

b) CASE 2 [23]

a) Background: The victim received several obscene emails with morphed photographs of herself, the suspect claimed to have put these photos on a popular website and threatened to leak these photos on several pornographic websites.

b) Investigation: The IP which was used to upload these obscene morphed photos to the website was traced back to a company in Delhi. All the Terminals were thoroughly checked for any cookies and records, one such terminal seemed to have one of the morphed photographs, and after forensic analysis using disc imaging and analysis tools which provided necessary files for the case, the perpetrator was found to be an ex-colleague of the victim.

c) C. CASE 3 [24]

a) Background: An Uzbekistan citizen was arrested in the Kalkaji area of Delhi by the Delhi police for committing crimes such as impersonation and forgery of documents. The accused was identified to be Shodiyor Zokirov who was from Tashkent, Uzbek- istan. The Delhi police claimed that the man was masquerading as an Indian with the name Mahesh Singh, but when questioned, he wasn't able to communicate in Hindi or English, with the aid of google translator the police were able to uncover the nationality of the accused. The police found several debit and credit cards in his possession each having different names or originating from different banks. On being questioned, the man was not able to provide any satisfactory explanation for the same.

b) Investigation: The accused tried to deceive the police by providing a fake aadhar card in the identity of Mahesh Singh. An Uzbekistan Airways ticket, cash worth about Rs.23,500, and a mobile phone were found along with numerous credit and debit cards with false identities. After further questioning, the accused revealed that his name is Shodiyor Zokirov and that he was a citizen of Uzbekistan. He later admitted to the fact that he forged the aadhar card using his photograph. He also gave up information about whom he worked with - a person named Michel, with him the accused skimmed the debit card details and other data from different ATMs which they later on used to make fake cards to withdraw money. The investigation is going on to find the co-accused, and the cards are being analysed to get any valuable information.

13. Research Challenges

Cyber forensics being a broad scope in itself induces several issues to legal and technical experts through the usage of different tools, techniques, methodologies, and various ways it functions. Some ordinary challenges arise due to the unavailability of correct guidelines for collection, possession, and presentation of electronic proof, anti-forensic methodology used by criminals, rapid modification in technology, use of unbound online tools for investigation, large data, etc. These reveal the requirement of advanced amendments and enactments in the current law and technologies with patches. [25]

With enhancements in technology, adverse improvements in cybercrimes committed happen in tandem with each other. Digital forensic specialists use forensic tools for accumulating shreds of evidence against criminals, which in turn use tools for disguising, modifying, or eliminating the traces of their crime. These are Antiforensics techniques in the field of digital forensics. Within the digital forensics space, this arises as a severe issue. Anti-forensics techniques can be sub-divided as follows:

1. Encryption - Encryption is the key concept enabling the privacy of data or information by concealing it from unauthorized personnel. Unfortunately, it is also prone to be used by criminals to camouflage their crimes.
2. Data concealment within storage space - Criminals usually hide huge chunks of data/information inconspicuously inside the storage medium by utilizing system commands and programs.
3. Covert Channel - The covert channel is a communication protocol that permits a mali- cious individual to avoid or circumvent intrusion detection technique and conceal data in transit across the network. This can also be used by a malicious individual to mask the link between the compromised system and themselves.

Some of the mainstream challenges faced in the present scenario include [26]:

- Privacy-preserving investigations:
    - In recent times, individuals tend to inculcate various elements or aspects of their lives into cyberspace, via social media or networking sites. Unfortunately, accumulating information to rebuild and locate an attack that has occurred can seriously violate users' privacy and is connected to other obstacles when cloud computing is involved.

- Rise of anti-forensics techniques:
    - Defensive measures incorporate concepts like obfuscation, encryption, and cloaking techniques while also including steganography.
    - Communication and mutual understanding between various international jurisdictions notwithstanding, investigating cybercrime and accumulating evidence are imperative in the construction of cases with all bases covered, for law enforcement. To achieve this, security specialists require the best tools to conduct investigations.
    - Digital forensics is foundational to conduct investigations that are often bound with their cyber extension. Recent upbringings in digital societies are accountable to cybercrimes and fraud causing economic deterioration or risk to individuals. As a result, the creation of the current wave of forensics tools must be done to hold up multivariate investigations, privacy preservations, and offer scalability.

- The Explosion of complexity:
    - Evidence that was restricted to a single host, is now dispersed among different virtual/ physical locations (like cloud resources, personal network – online social networks, and storage units). Consequently, more tools, competence, and time are required to recon- struct evidence appropriately. Some tasks are partially automated but resulted

in a rapid decline in the quality of the investigation, which was highly criticized by the digital investigation community.

The future of image forensics sees integration with visual perception as one of its obvious challenges. This does not emphasize only the juncture use of human and automatic inspection of visual media. From a broader outlook, understanding the perception of visual semantics might lead to the solution of one of the main limitations of present DIF techniques, which is the difference between "Innocent" retouching (like red-eye correction or artistic manipulation) and malicious tampering.

The malicious purpose was distinctly evident, taking into account Jeffrey Wong Su En's fake knighthood case (Fig.31). In several cases, manipulation can be done to beautify an image, like re-touching on models in an advertisement. Similarly, the TIME magazine cover (Fig.32) was said to be an erroneous elucidation of an artistic edit. The line between evil and na¨ıve purposes is often unclear. Regardless, some manipulations reveal an added critical effect on the semantic content of an image, and thus on the viewer too.

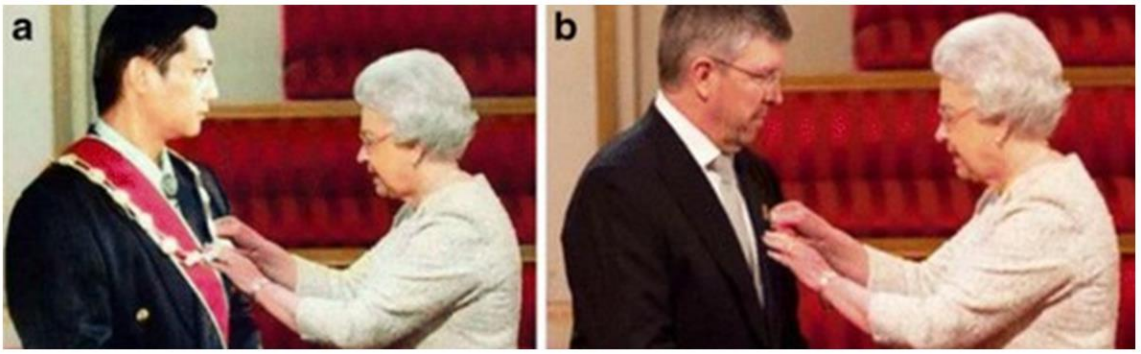


Figure 31: Jeffrey Wong Su En's fake knighthood

Figure 32: OJ Simpson

However, the researcher's collective work in visual perception, media semantics, and media security fields may produce intriguing results, that are not restricted to only the strict forensic investigation perspective. The work conducted by De Rosa and others [50] can be seen as the first step towards this direction, to a certain extent. The authors propose a theoretical framework to retrieve (semantic) dependencies among various image groups. This is significantly limited to detecting whether or not the images have been created from other sources. Over the long term, however, Image dependencies and analysis of mutation of their semantic content over these dependencies could generate useful information about their owner, roles of various websites, and their visitor's habits. Likewise, extensive forensics activity can be visualized on social networks or video databases. [1]

14. Conclusion

Forensics, as is, cannot be completely automated into a fully autonomous pipeline with the help of the currently available resources. Digital forensic tools available today are very function- specific. Procuring different tools that satisfy these functions can prove to be an expensive and tedious task. That creates the need for a single tool that performs every aspect of image detection. The tool is required to perform most of the important facets of forgery detection - Metadata Extraction, Error Level Analysis, GPS Localisation, Shadow Analysis, Hidden Pixel Extraction, and Filename Ballistics. Most images contain metadata in them, which makes the process of forgery detection more feasible. But images downloaded from social media are stripped off of most of the metadata. Such images require special methods such as Error Level Analysis, Machine Learning, and Deep Learning-based techniques. One of the largely encountered problems by researchers in the fields of Machine Learning and Deep Learning is the over-finetuning of the model to attain SoTA scores for a specific dataset. Hence the focus should be set on producing a generalised model, rather than achieving higher SoTA scores.

15. Acknowledgment

The authors would like to extend their appreciation to the University Internal Research Funds for Projects at PES University for funding this research work under project number PE-SUIRF/CSE/2020/01. The authors would like to thank PES University for their relentless encouragement and support to pursue research.

16. References

[1] Redi, J.A., Taktak, W. & Dugelay, JL. Digital image forensics: a booklet for beginners. Multimed Tools Appl 51, 133–162 (2011). URL: https://doi.org/10.1007/s11042-010-0620-1

[2] Great Learning Team. Digital Image Processing Explained. GreatLearning Blog: Free Resources What Matters to Shape Your Career!2021. URL: https://www.mygreatlearning.com/blog/digital-image-processing-explained/

[3] McAndrew, A. (2004). An introduction to digital image processing with matlab notes for scm2511 image processing. School of Computer Science and Mathematics, Victoria University of Technology, 264(1), 1-264.

[4] Pawan, Patidar & Manoj, Gupta & Sumit, Srivastava & Nagawat, Ashok. (2010). Image De-noising by Various Filters for Different Noise. International Journal of Computer Applications. 9. 10.5120/1370-1846.

[5] Sridevi M., Mala C., Sanyam S." Comparative Study of Image Forgery and Copy- Move Techniques". Advances in Computer Science, Engineering & Applications. Ad- vances in Intelligent and Soft Computing, vol 166. Springer, Berlin, Heidelberg (2012). https://doi.org/10.1007/978-3-642-30157-5_71

[6] Zheng, L., Zhang, Y., & Thing, V. L. L. A Survey on Image Tampering and Its Detection in Real-world Photos. Journal of Visual Communication and Image Representation (2018). doi:10.1016/j.jvcir.2018.12.022

[7] Singh, Ajit, and Jyoti Malik. ”A comprehensive study of passive digital image forensics techniques based on intrinsic fingerprints.” International Journal of Computer Applications 116.19 (2015).
[8] Gangwar, D. P., & Pathania, A. Authentication of digital image using exif metadata and decoding properties. IAuthentication of digital image using exif metadata and decoding properties (2018): 335-341.
[9] Harran, M., Farrelly, W., & Curran, K. A method for verifying integrity & authenticating digital media. Applied computing and informatics (2018), 14(2), 145-158
[10] Kinsella, C. (2009). U.S. Patent Application No. 12/086,927.
[11] GeeksforGeeks. Huffman Coding | Greedy Algo-3, 2021. URL:
[12] Jpeg Compression - Quantization. Robertstocker, 2012. URL:
[13] Parthiban.R. Image authentication using JPEG headers, 2014. IJERT ISSN:2278-0181
[14] Rodríguez-Santos, F., Delgado-Gutierréz, G., Palacios-Luengas, L., Vazquéz-Medina, R., Culhuacan, E. Practical implementation of a methodology for digital images authentication using forensics techniques. Advances in Computer Science: an International Journal, 2015, 4(6).
[15] Ghosh, P., Morariu, V., & Larry Davis, B. C. I. Detection of metadata tampering through discrepancy between image content and metadata using multi-task deep learning. In Pro- ceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops, 2017 (pp. 60-68).
[16] Kee, E., Farid, H. Digital image authentication from thumbnails. In Media Forensics and Security II (Vol. 7541, p. 75410E). International Society for Optics and Photonics,2010.
[17] Nowroozi, E., Dehghantanha, A., Parizi, R. M., & Choo, K. K. R. A Survey of Machine Learning Techniques in Adversarial Image Forensics. Computers & Security, 2020, 102092.
[18] Xuan, X., Peng, B., Wang, W., & Dong, J. On the generalization of GAN image forensics. In Chinese conference on biometric recognition, 2019, (pp. 134-141). Springer, Cham.
[19] Marra, F., Gragnaniello, D., Cozzolino, D., & Verdoliva, L. Detection of gan-generated fake images over social networks. IEEE Conference on Multimedia Information Processing and Retrieval (MIPR), 2018, (pp. 384-389). IEEE.
[20] Ambili, B., & George, N. A robust technique for splicing detection in tampered blurred images. International Conference on Trends in Electronics and Informatics (ICEI), 2017, (pp. 897-901). IEEE.
[21] Krawetz, N. Digital Photo Forensics: More Than Meets the Eye. Presentation at the 25th Annual Crimes Against Children Conference, 2013. URL: http://hackerfactor.com/blog/in-dex.php?/archives/565-More-Than-Meets-The-Eye.html.
[22] Antony, N., & Devassy, B. R. Implementation of Image/Video Copy-Move Forgery Detection Using Brute-Force Matching. 2nd International Conference on Trends in Electronics and Informatics (ICOEI), 2018, (pp. 1085-1090). IEEE.
[23] Prateek Paranjpe, Cyber Forensics: Case Studies from India. Case Studies. http://prateek-paranjpe.blogspot.com/p/cyber-forensics-case-studies.html
[24] Times Of India, Delhi: Uzbek national arrested for forgery, cheating, 2020. URL: https://timesofindia.indiatimes.com/city/delhi/delhi-uzbek-national-arrested-for- forgery-cheating/articleshow/79151493.cms
[25] Desire, L. Challenges faced by Digital Forensics, 2020. URL: https://legaldesire.com/challenges-faced-by-digital-forensics/
[26] Cameron, L. Future of digital forensics faces six security challenges in fighting borderless cybercrime and dark web tools, 2018.
[27] Rungta, K, What is Digital Forensics? History, Process, Types, Challenges, 2021. URL: https://www.guru99.com/digital-forensics.html
[28] EC-Council. (n.d.), What is Digital Forensics | Phases of Digital Forensics. URL: https://www.eccouncil.org/what-is-digital-forensics/
[29] Pedamkar. P, What is Digital Forensics? EDUCBA, 2021. URL: https://www.educba.com/what-is-digital-forensics/
[30] Zabala, A., & Pons, X. Image Metadata: compiled proposal and implementation. Geoinfor- mation for European-wide Integration, Millpress, Rotterdam, 2002. pp: 674-652.
[31] Piva, A. An overview on image forensics. International Scholarly Research Notices, 2013.

[32] Khalaf, R. S., & Varol, A. Digital Forensics: Focusing on Image Forensics. In 2019 7th International Symposium on Digital Forensics and Security (ISDFS), 2019 (pp. 1-5). IEEE.
[33] Sharma, V., Jha, S., & Bharti, R. K. Image forgery and it's detection technique: a review. International Research Journal of Engineering and Technology (IRJET),2016 (pp. 756-762.
[34] Thakur, T., Singh, K., & Yadav, A. Blind approach for digital image forgery detection. International Journal of Computer Applications, 2018. 975, 8887.
[35] Altheide, C., & Carvey, H. Digital forensics with open-source tools, 2011. Elsevier.
[36] Hoffman, C. How to See Exactly Where a Photo Was Taken (and Keep Your Location Private), 2017. - https://www.howtogeek.com/211427/how-to-see-exactly-where-a-photo- was-taken-and-keep-your-location-private/
[37] FotoForensics. (n.d.). Tutorial-ELA. URL: https://fotoforensics.com/tutorial-ela.php
[38] Photo Forensics: Detect Photoshop Manipulation with Error Level Analysis, 2020. URL: https://resources.infosecinstitute.com/topic/error-level-analysis-detect-image-manipulation/
[39] Yarlagadda, S. K., Güera, D., Montserrat, D. M., Zhu, F. M., Delp, E. J., Bestagini, P., & Tubaro, S. Shadow removal detection and localization for forensics analysis. IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2019, (pp. 2677-2681). IEEE.
[40] Sample, I. What are deepfakes – and how can you spot them? The Guardian, 2020. URL: https://www.theguardian.com/technology/2020/jan/13/what-are-deepfakes- and-how-can-you-spot-them
[41] Rungta, K. What is Digital Forensics? History, Process, Types, Challenges. Hidden Pixels, 2021. URL: https://whatis.techtarget.com/definition/image-metadata
[42] Contributor, T. image metadata., WhatIs.Com, 2015. https://whatis.techtarget.com/definition/image-metadata
[43] JPEG Metadata Format Specification and Usage Notes. (n.d.). JPEG. URL: https://docs.oracle.com/javase/8/docs/api/javax/imageio/metadata/doc- files/jpeg*metadata.html*
[44] List of JPEG Markers – DiskTuna // Photo Repair & Photo Recovery. (n.d.). JPEG Markers. URL: https://www.disktuna.com/list-of-jpeg-markers/
[45] Photo Metadata, IPTC, 2018. URL: https://iptc.org/standards/photo-metadata/
[46] Digital asset management software. (n.d.). Bridge. https://www.adobe.com/in/products/bridge.html
[47] Wikipedia contributors. Exif, 2021. URL: https://en.wikipedia.org/wiki/Exif
[48] Di Leom, M., DOrazio, C. J., Deegan, G., & Choo, K. K. R. Forensic collection and analysis of thumbnails in android. In 2015 IEEE Trustcom/BigDataSE/ISPA, 2015 (Vol. 1, pp. 1059-1066). IEEE.
[49] List of JPEG Markers – DiskTuna // Photo Repair & Photo Recovery. (n.d.-b). JPEG Markers. URL: https://www.disktuna.com/list-of-jpeg-markers/
[50] De Rosa A, Uccheddu F, Costanzo A, Piva A, Barni M, Exploring image dependencies: a new challenge in image forensics, 2010. Proc SPIE 7541