TELKOMNIKA Telecommunication, Computing, Electronics and Control
Vol. 18, No. 6, December 2020, pp. 3096~3106
ISSN: 1693-6930, accredited First Grade by Kemenristekdikti, Decree No: 21/E/KPT/2018
DOI: 10.12928/TELKOMNIKA.v18i6.15295

Classification and evaluation of digital forensic tools

Azra Parveen[1], Zishan Husain Khan[2], Syed Naseem Ahmad[3]
[1,2]Department of Applied Sciences and Humanities, Faculty of Engineering and Technology,
Jamia Millia Islamia (A Central University), India
[3]Department of Electronics and Communication Engineering, Faculty of Engineering and Technology,
Jamia Millia Islamia (A Central University), India

Article Info

Article history:

Received Jan 24, 2020
Revised Jun 10, 2020
Accepted Aug 4, 2020

Keywords:

Digital forensic tools
Digital image forgery
Forged images
Image forensic
Software forensic tools

ABSTRACT

Digital forensic tools (DFTs) are used to detect the authenticity of digital images. Different DFTs have been developed to detect the forgery like (i) forensic focused operating system, (ii) computer forensics, (iii) memory forensics, (iv) mobile device forensics, and (v) software forensics tools (SFTs). These tools are dedicated to detect the forged images depending on the type of the applications. Based on our review, we found that in literature of the DFTs less attention is given to the evaluation and analysis of the forensic tools. Among various DFTs, we choose SFTs because it is concerned with the detection of the forged digital images. Therefore, the purpose of this study is to classify the different DFTs and evaluate the software forensic tools (SFTs) based on the different features which are present in the SFTs. In our work, we evaluate the following five SFTs, i.e., "FotoForensics", "JPEGsnoop", "Ghiro", "Forensically", and "Izitru", based on different features so that new research directions can be identified for the development of the SFTs.

Corresponding Author:

Azra Parveen,
Department of Applied Sciences and Humanities, Faculty of Engineering and Technology,
Jamia Millia Islamia (A Central University),
New Delhi-110025, India.
Email: parveenazra999@gmail.com

1. INTRODUCTION

In real life applications we have seen that digital images (DIs) can be manipulated using sophisticated image editing software to misinterpret the content of the DIs. Therefore, DIs are no longer trusted by the court of law or society until it is investigated by forensic experts [1]. There are different applications of image processing in the field of science and engineering, for example, in expression recognition system [2], image processing analysis [3], and digital image forensics (DIF) [1]. The objective of DIF is to elicit the origin of the image; and verify the authenticity of the images. This field has received much attention by the Computing and Electronics research community who are working in active and passive DIF techniques [1]. In active DIF techniques, prior knowledge of the image is necessary to detect the authenticity of the DIs like watermarking and forensic hash. [1]. In the age of the internet, people upload their pictures on social media and it is difficult to get the prior information about each and every image. To deal this situation, researchers have started to detect the forged images without access to the sources or devices. Here we consider an example of the "Iranian defense officials, who made the news with their blatant misuse of Photoshop after releasing

a photo purporting to show their much-trumpeted stealth fighter jet soaring over snow-capped Mount Damavand. Earlier, aviation experts had claimed that the jet shown in the hangar in their press photos was not genuine, because there were clear visual signs that it was a fake model not capable of flying. A blogger soon produced clear evidence that the flight photo was also faked. The jet in the photo was viewed at the exact same angle and with the exact same light reflections as in one of the photographs from the hangar. Furthermore, the scene of the mountain with some exposure adjustments was identical to one found on a stock image site. Thus, the flight image was revealed to be a composite photo", as shown in Figure 1 [4].

Figure 1. Fighter jet soaring over snow-capped Mount Damavand [4]

People post the images of their "functions", "vacations", "social events", and "graduation ceremonies" on Internet. From these images it is difficult to spot the fake images from the original images. Hany Farid, who is "a mathematician and digital forensics expert", suggested different ways to check the originality of the DIs when it pops up on Twitter or Facebook. If an image has been re-circulated from another website then it can be discovered by "reverse image search" (RIS), using Google Images or TinEye [5]. Whenever there is a natural disaster in any place, people circulate the same silly images of sharks swimming down the street". This type of images can be checked from RIS process. Burrowing into image data can be used to detect the forged image quickly. There are different websites where you can upload your photos and it will strip out the metadata of your images. This metadata includes the "make of the camera", "time of the day the photo was snapped" and "GPS coordinates, if it was enabled". Keeping in view the user's privacy, anything uploaded on the Twitter or Facebook will have its metadata automatically stripped. In today's digital era, "Seeing Is No Longer Believing" because it is easier to tamper digital images due to the image editing software like Adobe Photoshop, Pixelmator, Inkscape, and Fireworks [1, 6]. Fake or forged images could flare-up violence. Therefore, it is important for those people who are addicted to the social media to check the authenticity of digital pictures or news before sharing it on their wall or friend lists. The research problem, objective, and contributions of our work are given in section research problem, objective and contributions, respectively.

- Research problem

Different surveys or literature reviews in the area of digital image forgery have been performed to identify the research gaps in the literature [1, 7, 8]. For example, Walia and Kumar [8] performed a systematic scrutiny by using the guidelines of Kitchenham's [9] in the area of digital image forgery detection. The same guideline was adopted by Parveen *et al.* [1] to perform the "systematic literature review in the area of pixel-based copy–move image forgery detection techniques". In literature, different types of the DFTs have also been developed to detect the authenticity of the images like "forensics-focused operating systems" (FFOS), (ii) computer forensics, (iii) "memory forensics", (iv) "mobile device forensics", and (v) "software forensics". Based on our review, we identify that there is no classification and evaluation of digital forensic tools (DFTs) in the literature of image forensic science [10, 11].

- Objective

The objective of this paper is to extend our previous work [5] and to classify and evaluate the selected SFTs so that new research directions can be identified for the development of SFTs. Here, we choose the SFTs for the evaluation because in literature most of the focus is on the passive DFTs in which researchers and

academicians develop the algorithms for the forgery detection; and implement it in the form of tools or some prototypes. As per our knowledge, there is no study which classifies and evaluates the DFTs. Therefore, in this paper, an attempt has been made for the classification of DFTs and evaluation of the SFTs.

- Contributions

The contributions of the present work are as follows: (a) classification of digital forensic tools (DFTs); and (b) evaluation of software forensic tools (SFTs) based on the following features which are present in SFTs: (i) "error level analysis" (ELA), (ii) "metadata analysis" (MA), (iii) "last save quality" (LSQ), (iv) "JPEG luminance and chrominance" (JLC), (v) digest, (vi)"file type extension" (FTE) and MIME type, (vii) "image width and height" (IWH), (viii) "bits per sample" (BPS), (ix) "color components" (CC), (x) "cryptographic hash function" (CHF), (xi) "clone detection" (CD), (xii) "principal component analysis" (PCA), (xiii) "noise analysis" (NA), (xiv) GPS-Localization (GPS-L), (xv) "Devise signature analysis" (DSA), (xvi) "Double JPEG detection" (DJD), (xvii) JPEG structure/coefficients/ghost detection (JSCGD), and (xviii) Sensor pattern analysis (SPA). This paper is structured as follows: Related work is given in section 2. Section 3 presents the classification of DFTs. The identified features for the evaluation of five selected software forensic tools (SFTs), i.e., "FotoForensics", "JPEGsnoop", "Forensically", "Ghiro", and "Izitru" are given in section 4. After that we use two SFTs for the analysis of the digital images; and it is presented in section 5. Conclusion and suggestions for future research work in the area of SFTs are given in section 6.

2. RELATED WORK

In this section we present the related work in the area of image forgery detection algorithms and SFTs. Vaishnavi and Subashini [10] proposed a method for copy move forgery detection by means of "symmetry based local features". Hegazi *et al.* [11] employed "density-based clustering" for the detection of forged images. Lee *et al.* [12] employed "histogram of oriented gradients" for the detection of forged images. Raju *et al.* [13] used "binary discriminant features" for forgery detection. Polar coordinate system was used by Fadl *et al.* [14] to check the authenticity of digital images. Alberry *et al.* [15] used fast "scale invariant feature transform" based method for the detection of forged images. In our previous work [6], we proposed a method for the detection of forged images using DCT. In addition to the image forgery detection algorithms, different software forensic tools (SFTs) have also been developed to detect the forged images, i.e., "FotoForensics", "JPEGsnoop", "Ghiro", "Forensically", and "Izitru". In literature, we have identified few studies which have focused on DFTs. For example, Parveen *et al*. [5] evaluated the different DIF tools; and check the authenticity of the images using FotoForensics and JPEGsnoop tools. Kaur *et al.* [16] presented a method based on the photo forensic tool to detect the fake or hoax images using "HxD" hex editor. This editor was used to generatethe following information about the images: (a) "JPEG file interchange format" (JFIF), (b) camera specifications including make and model, (c) quantization table values, and (d) Huffman values. Carner [17] discussed the different tools which are used to check the authenticity of the audio, video and images. Based on our review [1], we have identified that in literature there is no study which presents an insight into forensic tools; and evaluates these tools on the basis of different features which are present in SFTs. Therefore, to address this issue in this paper we classify and evaluate the DFTs.

3. CLASSIFICATIONS OF DIGITAL FORENSIC TOOLS

In this section, we classify the digital forensic tools (DFTs). In literature, we have identified five types of DFTs, i.e., (i) forensics-focused operating systems (FFOS), (ii) computer forensics, (iii) memory forensics, (iv) mobile device forensics, and (v) software forensics [5]. The classification of DFTs is given in Figure 2.

3.1. Forensics-focused operating systems

Forensic-focused operating systems (FFOS) based DFT is dedicated to security and penetration testing of an OS. It is divided into two parts, i.e., (i) Debian-based FFOS and (ii) Gentoo-based FFOS. Kali Linux is a Debian-based FFOS and it is designed for digital forensics and penetration testing. Parrot Security OS is a cloud-oriented Linux distribution which is used to perform security and penetration tests. Pentoo, which is based on Gentoo Linux, is designed for security assessment and penetration testing [18].

3.2. Computer forensics

In the list of the computer forensics tools, Autospy is a "graphical user interface (GUI) software to the command line digital investigation analysis tools in the Sleuth Kit" which is used to analyze the file systems like "new technology file system" (NTFS), "file allocation table" (FAT), and "extensible file allocation table" (ExFAT). It is employed for extracting "exchangeable image file format" (EXIF) values [19]. Belkasoft Evidence Center is a digital forensic tool which is created by Belkasoft. Among various computer forensic

tools, belkasoft evidence center tool has been applied on different types of the artefacts in any data source, i.e., "physical and logical drives", "mobile device backups", and "memory dumps". In the list of the computer forensic tools, computer online forensic evidence extractor (COFEE) was developed by Microsoft for the extraction of the evidences from the Windows computer. Digital forensics framework (DFF) is employed to "collect, preserve and reveal digital evidence without compromising systems and data". It offers GUI and the classical tree view. Forensic toolkit (FTK) was developed by AccessData. FTK scans the hard drive of the computer to collect the different types of the information. For example, it locates all the deleted E-mails and scans the disk for password dictionary after applying the text strings. ISEEK tool was developed by Adams *et al.* [20] for high speed, distributed data acquisition. Forensic explorer (FEX) is used for the preservation, analysis and presentation of electronic evidence. This tool includes the following users, i.e., "law enforcement", "government", "military and corporate investigation agencies".

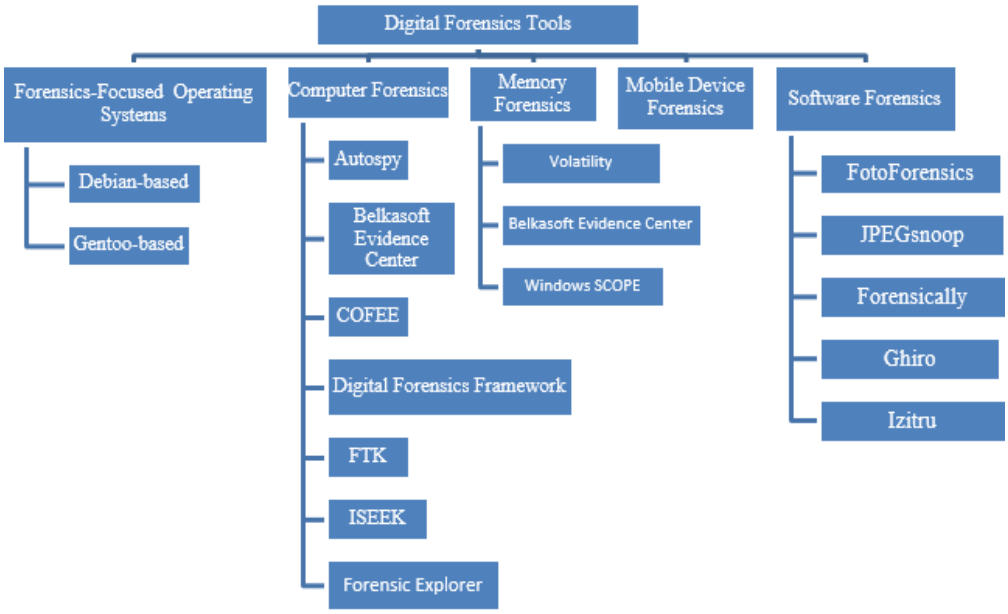

Figure 2. Classification of digital forensic tools

3.3. Memory forensics

Volatility is an important memory forensic tool for forensic analysis of volatile memory. It is written in Python and supports 32- and 64-bit machines. Using this tool, information about running process, open network sockets and network connections can be extracted. Belkasoft evidence center is also used for the memory forensics in addition to the computer forensics. In the list of the memory forensic tools, Windows SCOPE support the identification of the URLs, credit cards detailed in the captured memory.

3.4. Mobile device forensics

Belkasoft evidence center is the common tool which is used in computer forensic, memory forensic and also in the mobile device forensics. In the list of the mobile device forensics, micro systemation is a hardware and software package which is specialized in the deleted data.

3.5. Software forensics tools

In this section we discuss some of the selected software forensic tools (SFTs), i.e., FotoForensics, JPEGsnoop, Forensically, Ghiro, and Izitru, which are used to detect the forged images. An insight into these tools is given below:

3.5.1. FotoForensics

This tool is used to decode any type of the forged pictures and manipulations. In this tool, error level analysis is used to identify the different compression levels in the image. Practically, JPEG images have same error level. If the image contains different error levels then it simply shows the digital modification in the image. FotoForensics works like a microscope which highlights those details of the image that the human eye may not be able to identify. Following features are used for the analysis of the digital images like error level analysis, metadata analysis, last save quality, and color adjustment [5].

3.5.2. JPEGsnoop

To examine and decode the inner details of the images, JPEGsnoop tool is the best choice because it is free windows application. The JPEGsnoop tool was designed to expose those details from the images to decide whether the image has been forged or not. Using JPEGsnoop tool we can extract the following information of an image, i.e., quantization table matrix (chrominance and luminance), Chroma subsampling, estimates JPEG quality setting, JPEG resolution settings, Huffman tables, EXIF metadata, RGB histograms. In this paper, we have used JPEGsnoop tool for our experimental work because it is easy to understand and download it on our system [5].

3.5.3. Forensically

It is a free digital forensic tool which includes "clone detection", ELA, and "meta-data extraction". In this tool, the objective of the clone detection is to highlight the copied regions within an image. This feature is used as an indicator that the picture has been manipulated. Error level analysis compares original image to recompressed version. ELA is a forensic method which is used to determine whether the picture has been digitally modified or not. With ELA, we identify the portion of digital images with different level of compressions. ELA identifies the areas in an image which are at different compression levels. JPEG images have the same compression levels. If any portion of an image has different error level then it likely indicates that the image has been modified. ELA highlights differences in the JPEG compression rate. The noise analysis feature of this tool is used to identify manipulations in the image like airbrushing, and deformations. This tool works well on high quality images. In this tool, principal component analysis is used to identify certain manipulations and details in the images [5].

3.5.4. Ghiro

Ghiro is an open source software for the digital image forensics. It has the following features that are used to show the authenticity of digital images, i.e., metadata extraction, GPS localization, MIME information, error level analysis, thumbnail extraction, signature engine, and hash matching. In Ghiro, content of a file is described by the "multipurpose internet mail extensions" (MIME). MIME is detected using magic number inside the image. Metadata is a special feature of the Ghiro which identifies the following: name of the owner, copyright and contact information, and what camera created the file. This tool mainly extracts the EXIF metadata, "international press telecommunication council" (IPTC) metadata, and "extensible metadata platform" (XMP) metadata of an image. "Exchangeable image file format" (EXIF) metadata includes the standard EXIF tags, Canon Maker Note tags, Fujifilm Maker Note tags, Minolta Maker Note tags, Nikon Maker Note tags, Olympus Maker Note tags, Panasonic Maker Note tags, Pentax Maker Note tags, Samsung Maker Note tags, Sigma/Foveon Maker Note tags, and Sony Maker Note tags [5].

3.5.5. Izitru

Izitru, pronounced as "is it true", is an online software tool which is used to test the validity of the uploaded pictures. In this tool, uploaded images are analyzed on the basis of the following test, i.e., "analysis of the device signature", "JPEG structure", "JPEG coefficient", "Sensor patterns", and "double JPEG detection" [21].

4. FEATURES OF SOFTWARE FORENSIC TOOLS

In this section, we explain different features which are present in SFTs. Based on our review [1, 5, 6, 20-25], we have identified following features which plays an important role to detect the forged images, i.e., (i) "error level analysis" (ELA), (ii) "metadata analysis" (MA), (iii) "last save quality" (LSQ), (iv) "JPEG luminance and chrominance" (JLC), (v) digest, (vi)"file type extension" (FTE) and MIME type, (vii) "image width and height" (IWH), (viii) "bits per sample" (BPS), (ix) "color components" (CC), (x) "cryptographic hash function" (CHF), (xi) "clone detection" (CD), (xii) "principal component analysis" (PCA), (xiii) "noise analysis" (NA), (xiv) GPS-Localization (GPS-L), (xv) "Devise signature analysis" (DSA), (xvi) "Double JPEG detection" (DJD), (xvii) JPEG structure/coefficients/ghost detection (JSCGD), and (xviii) Sensor pattern analysis (SPA). Therefore, in this section, we evaluate the selected five software forensic tools, i.e., FotoForensics, JPEGsnoop, Forensically, Ghiro, and Izitru based on the above features. A brief description about these features is given below:

(i) Error level analysis (ELA) is one of the most successful techniques for the detection of the fake images. If the image is not altered, the 8X8 block of the image has the same error levels. If some image has been altered then that image has different error levels. Therefore, in the literature of digital image forensic, ELA has been used to detect whether the image has been forged or not. For example, Gunawan *et al.* [26] apply the ELA for the development of the algorithm for the detection of manipulated images. In another study, Warif *et al.* [27] evaluated the ELA in digital images.

(ii) Metadata (MA) is a "set of data that describes and gives information about other data". In image forensic tools, metadata is used to describe those data that may be useful to get the information about the image. For example, in Ghiro tool, metadata contains the following information about an image, i.e., EXIF, "Extensible Metadata Platform" (XMP), and "International Press Telecommunications Council" (IPTC). Because of the importance of the metadata, Salama *et al*. [28] performed the metadata based forensic analysis of that information which is available on web.
(iii) Last save quality (LSQ) gives the information about the percentage of the last saved quality of the image.
(iv) JPEG luminance and chrominance (JLC): brightness, hue, and saturation are the three main properties of a color source that our eyes use to distinguish among different colors. Brightness represents the amount of energy that stimulates the eye and varies on a gray scale from black to white. Hue represents the actual color of the source and each color has different frequency/wavelength and the eye determines the color from this. Saturation represents the strength of the color. A pastel color has a lower level of saturation than a color such as red. A saturated color such as red has no white in it. The term luminance is used to refer to the brightness of a source; and the hue and saturation are referred to as its chrominance.
(v) The objective of digest is to fast the searching process within the large database [26].
(vi) FTE/MIME: A multipurpose internet mail extension (MIME) was designed to "extend the format of email to support non-ASCII characters", "attachments other than text format", and "message bodies which contain multiple parts".
(vii) Image width and height (IWH) represents the size of an image.
(viii) Bits per sample (BPS) denote the number of pixels per sample.
(ix) Hue, saturation, and luminance are the color components (CC) of an image.
(x) Cryptographic hash function (CHF) is used to verify the authenticity of the data. Two files can be identical, if the checksum generated from each file has the same value; and the value of the checksum is generated through the same CHF. Commonly used CHF are MD5 and SHA-1.
(xi) Clone detection (CD) is an important criterion which is used to detect the clones in an image.
(xii) Principal component analysis (PCA) is a technique for the extraction of features from an image or from a data set. This technique combines the input variables in some particular way and it is used to drop the least important variables while considering the most important parts of all the variables.
(xiii) Noise analysis (NA) is one of the important criteria for the detection of the forged images. It is the random variations of the brightness in DIs.
(xiv) Global positioning system (GPS) localization provides the longitude and latitude of the DIs. This feature reads the position of the DIs where the photo was taken.
(xv) Device signature analysis (DSA) serves as a criterion for effective document analysis. Detection of signature from the background is a key research problem in document image retrieval [29].
(xvi) Double JPEG Detection (DJD) is an important concept for the detection of forged images. Different methods have been developed for detecting double JPEG compression when the information about the primary compression is given in terms of quantization table [30]. Yang *et al*. [30] proposed a method for the detection of double JPEG compression when the quantization matrix is same.
(xvii) JPEG structure/coefficients/ghost detection (JSCGD) method is employed for distinguishing the single and double JPEG compression, which is an indication for the image manipulation and detection [31].
(xviii) Sensor pattern analysis (SPA) is used in the image forensic as a method to identify the camera from which the picture was taken. In this method, the reference pattern noise for each camera is determined which is achieved by averaging the noise obtained from different images. Lukas *et al*. [32] proposed a method for the identification of the camera by using sensor pattern noise.

It is not possible to implement all the identified 18 features in single DFTs. Therefore, there is a need to develop a method for the selection of the identified features, so that the selected features can be implemented in the tool [33]. Therefore, the multi-criteria decision-making algorithms [34] like analytic hierarchy processes (AHP). can be used to compute the ranking values of the SFTs so that appropriate SFTs can be selected for the detection of the forged images. The above features have been used for the evaluation of the SFTs by considering different set of images. The detailed description about the evaluation is given in the next section.

5. RESULTS AND DISCUSSION

The objective of this section is to present the results of our work. With the help of the 18 features, as discussed in previous section, we evaluate the five software forensic tools (SFTs) in order to identify that which feature(s) is/are common among different SFTs; and which is not supported by the SFTs. To analyze the SFTs, six different images have been considered, i.e., image 1, image 2, image 3, image 4, image 5, and image 6, as shown in Figures 3-8, respectively. These six images were evaluated on the basis of 18 features. The output of these images is exhibited in Figures 9-14, respectively. During our analysis, we found that ELA is the key

feature of the three image forensic tools, i.e., FotoForensics, Forensically, and Ghiro. Metadata (MA) is mostly supported feature in the FotoForensics, JPEGsnoop, and Ghiro tools, which includes the following: resolution of the image, camera make and model. JLC is also the common feature which captures the quantized luminance and chrominance data in the following tools: FotoForensics, JPEGsnoop, and Forensically. LSQ helps to find out the quality of the last save image and it is supported by only FotoForensics tool. GPS-localization (GPS-L) is only supported by the Ghiro tool. Among various SFT, Izitru is the only tool which detects the double JPEG compression and ghost in the images. The DSA and SPA are only supported by izitru. The result of the evaluation of SFTs is exhibited in Table 1. The symbol "√" in Table 1 indicates that corresponding feature is present in the SFT. For example, in Table 1, under JPEGsnoop tool column "√" is present infront of MA, JLC, IWH, BPS, and CC. It means that these features are present in JPEGsnoop tool. Similarly, the symbol "X" indicates features which are not supported by SFTs.

Table 1. An evaluation of different software forensic tools

Selected features	Software Forensic Tools				
	FotoForensics	JPEGsnoop	Forensically	Ghiro	Izitru
ELA	√	X	√	√	X
MA	√	√	X	√	X
LSQ	√	X	X	X	X
JLC	√	√	√	X	X
Digest	√	X	X	X	X
FTE/MIME type	√	X	X	√	X
IWH	√	√	X	X	X
BPS	√	√	X	X	X
CC	√	√	X	X	X
CHF	√	X	X	√	X
CD	X	X	√	X	X
PCA	X	X	√	X	X
NA	X	X	√	X	X
GPS-L	X	X	X	√	X
DSA	X	X	X	X	√
DJD	X	X	X	X	√
JSCGD	X	X	X	X	√
SPA	X	X	X	X	√

Figure 3. Image-1 for testing

Figure 4. Image-2 for testing

Figure 5. Image-3 for testing

Figure 6. Image-4 for testing

Figure 7. Image-5 for testing

Figure 8. Image-6 for testing

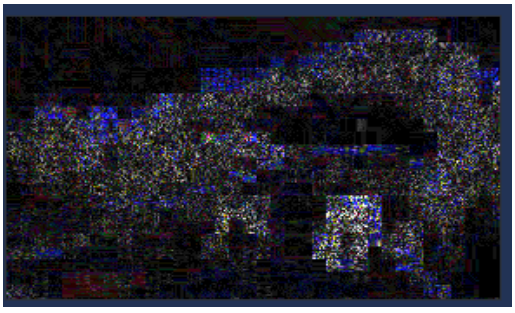

Figure 9. Output of image-1

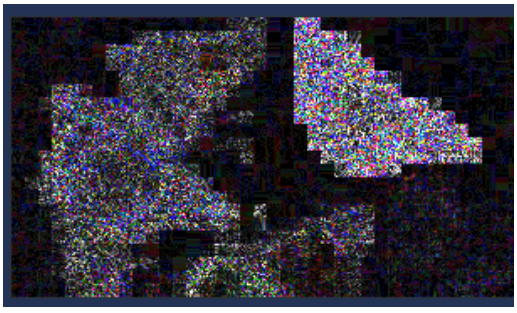

Figure 10. Output of image-2

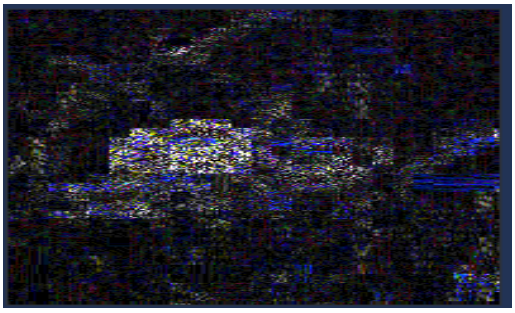

Figure 11. Output of image-3

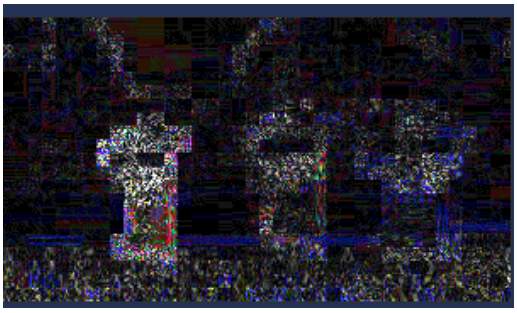

Figure 12. Output of image-4

Figure 13. Output of image-5

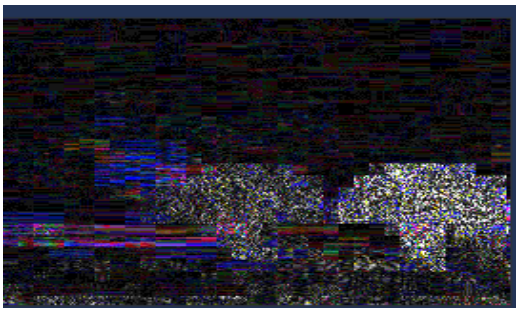

Figure 14. Output of image-6

We compared the results of our work with [5]. As a result, we found that in [5] only four DFTs were evaluated for the analysis of the digital images, i.e., FotoForensics, JPEGSnoop, Forensically, and Ghiro. In our work, we extend the work of [5] by introducing one more DFT for the analysis, i.e., izitru. In addition to this, we have also classified the DFT into five types, see Figure 2. Based on our critical analysis, we found that these tools do not discuss about the type of the feature extraction method which has been used to

extract the key features from the images. Feature extraction methods are broadly classified into two parts, i.e., "block-based method", and "key-point based method". In literature following feature extraction methods have been used in the image forgery detection algorithms, i.e., "(i) discrete cosine transform" (DCT), (ii) "discrete wavelet transform" (DWT), (iii) "principal component analysis" (PCA), (iv) "singular value decomposition" (SVD), (v) "histogram of oriented gradients", (vi) Zernike moment, (vii) "Fourier Mellin transform" (FMT), (viii) "polar complex exponential transform", (ix) Fourier transform, (x) "polar cosine transform" (PCT), (xi) PatchMatch algorithm, (xii) polar harmonic transform, (xiii) local binary patterns, (xiv) blur invariant moment, (xv) polar coordinate system, (xvi) "scale invariant feature transform" (SIFT), (xvii) "speedup robust features" (SURF), (xviii) J-Linkage algorithm, (xix) Harris corner points. The classification of the selected feature extraction methods used in image forgery detection algorithms is given is Figure 15. In addition to the feature extraction methods, the SFTs also do not discuss about the feature selection methods i.e., (i) Exhaustive search (ii) Lexicographically sorting, (iii) KD-Tree, (iv) Radix Sorting, (v) Counting Bloom Filters, (vi) Best-Bin-First, which have been used to select the features during the image forgery detection.

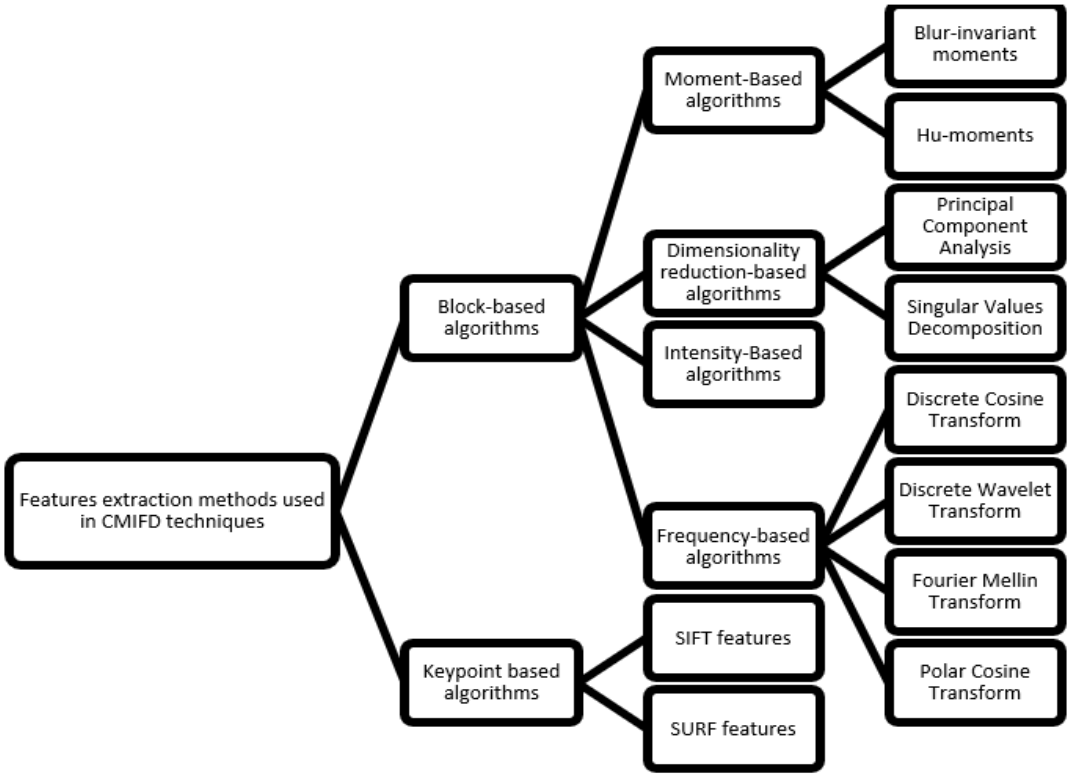

Figure 15. Feature extraction methods used in image forgery detection algorithms [6]

6. CONCLUSION

Digital image forensic algorithms have been developed to check the authenticity of the digital images. In addition to image forgery detection algorithms, different digital forensic tools (DFTs) have also been developed to detect the doctored images. In this paper, we present the classification of the DFTs; and among various tools, we evaluate the software forensic tools (SFTs) so that type of the features which are used in these tools can be identified. We evaluated the five selected SFTs, i.e., FotoForensics, JPEGsnoop, Forensically, Ghiro, and Izitru, on the basis of the 18 features, as discussed in section 4. Based on our evaluation, we identify that the selected tools do not reveal the basic concepts which have been used in the tools for the detection of the forged images. For example, these tools do not discuss about the type of the feature extraction and feature selection methods, which have been used in the development of the tools.

After evaluating the selected tools, we identify the following research issues for future work: (a) much work is needed in the area of DFTs in which the software developer should discuss the type of the algorithms which have been used in the tools for the detection of fake or doctored images, (b) there is a need of systematic literature review in the area of image forgery detection by considering the DFTs; and try to map the techniques and concepts

used in the digital image forgery detection algorithm and DFTs. Such type of mapping will be useful to propose some new methodologies for the detection of fake images, (c) combination of feature extraction and feature matching techniques plays an important role during image forgery detection. Therefore, the information about these two parameters and feature dimensions can also be useful to propose some new DFTs.

REFERENCES

[1] A. Parveen, Z. H. Khan, and S. N. Ahmad, "Pixel-based copy-move image forgery detection techniques: A systematic literature review," *5th IEEE International Conference on Computing for Sustainable Global Development*, New Delhi, India, pp. 663-668, 2018.

[2] A. Chater, A. Lasfar, "New approach to the identification of the easy expression recognition system by robust techniques (SIFT, PCA-SIFT, ASIFT and SURF)," *TELKOMNIKA Telecommunication, Computing, Electronics and Control*, vol. 18, no. 2, pp. 695-704, 2020.

[3] A. W. Altaher, S. K. Abbas, "Image processing analysis of sigmoidal Hadamard wavelet with PCA to detect hidden object," *TELKOMNIKA Telecommunication, Computing, Electronics and Control*, vol. 18, no. 3, pp. 1216-1223, 2020.

[4] Fourandsix Technologies, Inc., "Photo Tampering Throughout History," 2013. [Online]. Available: http://pth.izitru.com/2013_02_02.html

[5] A. Parveen, Z. H. Khan, and S. N. Ahmad, "Identification of forged images using image forensic tools," *Proceedings of the 2nd International Conference on Communication and Computing Systems,* Gurgaon, India 2018.

[6] A. Parveen, Z. H. Khan, and S. N. Ahmad, "Block based copy move image forgery detection using DCT," *Iran Journal of Computer Science*, vol. 2, pp.89-99, 2019.

[7] G. K. Birajdar, V.H. Mankar, "Digital image forgery detection using passive techniques: a survey," *Digital Investigation*, vol. 10, no. 3, pp. 226-245, 2013.

[8] S. Walia, K. Kumar, "Digital Image Forgery Detection: A Systematic Scrutiny," *Australian Journal of Forensic Sciences*, pp. 1-39, 2018.

[9] B. Kitchenham, *et al.,* "Systematic literature reviews in software engineering-A tertiary study," *Information and Software Technology*, vol. 52, no. 8, pp. 792-805, 2010.

[10] D. Vaishnavi, T. S. Subashini, "Application of local invariant symmetry features to detect and localize image copy move forgeries," *Journal of Information Security and Applications*, vol. 44, pp. 23-31, 2019.

[11] A. Hegazi, A. Taha, M. M. Selim, "An improved copy-move forgery detection based on density-based clustering and guaranteed outlier removal," *Journal of King Saud University - Computer and Information Sciences*, 2019.

[12] J. C. Lee, C. P. Chang, W. K. Chen, "Detection of copy–move image forgery using histogram of orientated gradients," *Information Sciences*, vol. 321, no. 10, pp. 250-262, 2015.

[13] P. M. Raju, M. S. Nair, "Copy-move forgery detection using binary discriminant features," *Journal of King Saud University - Computer and Information Sciences,* 2018.

[14] S. M. Fadl, N. A. Semary, "Robust Copy–Move forgery revealing in digital images using polar coordinate system," *Neurocomputing*,vol. 265, pp. 57-65, 2017.

[15] H. A. Alberry, A. A. Hegazy, G. I. Salama, "A fast SIFT based method for copy move forgery detection," *Future Computing and Informatics Journal,* vol. 3, no. 2, pp.159-165, 2018.

[16] B. Kaur, M. Blow, and J. Zhan, "Authenticity of digital images in social media," *Cyber Security Research and Education Institute,* The University of Texas at Dallas, USA, 2014. [Online] Available: *csi.utdallas.edu/events/NSF/papers/paper03.pdf*

[17] D. Carner, "Detect and Prevent File Tampering in Multimedia Files," 2017. [Online] Available*: http:/ /forensicpro tection.com/Detecting_and_preventing_file_tampering.pdf.*

[18] Wikipedia, "List of digital forensic tools,". [Online] Available*:* https://en. wikipedia.org/ wiki/ List_of_digital_forensics_tools

[19] B. C. Hatalova, Maria, "Tool for forensic analysis of digital traces," Master's Thesis, Faculty of Informatics, Masaryk University, Czech Republic, 2018.

[20] R. Adams, G. Mann, V. Hobbs, "ISEEK: A tool for high speed distributed forensic data acquisition," *The Proceedings of 15th Australian Digital Forensic Conference*, 2017

[21] T. Thongkamwitoon, "Digital forensic techniques for the reverse engineering of image acquisition chains," Ph. D. Thesis. Communication and Signal Processing Group, Department of Electrical and Electronic Engineering, Imperial College London, 2014.

[22] H. Farid, "Image forgery detection: A survey," *IEEE Signal Processing Magazine*, vol. 36, no. 2, pp.16-25, 2009.

[23] B. Mahdian, S. Saic, "A bibliography on blind methods for identifying image forgery," *Signal Processing. Image Communication*, vol. 25, no. 6, pp. 389-399, 2010.

[24] J. Fridrich, D. Soukal, and J. Lukas, "Detection of copy-move forgery in digital images," *Digital Image Forensic Workshop*, pp. 1-10, 2003.

[25] V. Christlein, C. Riess, J. Jordan, C. Riess, E Angelopoulou, "An evaluation of popular copy-move forgery detection approaches," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 6, pp.1841-1854, 2012.

[26] T. S. G. Gunawan, *et al*., "Development of photo forensics algorithm by detecting Photoshop manipulation using error level analysis," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 7, no. 1, pp. 131-137, 2017.

[27] N. B. A. Warif, *et al*., "An evaluation of error level analysis in image forensics," *IEEE International Conference on System Engineering and Technology*, pp. 23-28, 2015.

[28] U. Salama, V. Varadharajan, M. Hitchens, "Metadata based forensic analysis of digital information in the Web," *Annual Symposium of Information Assurance and Secure Knowledge management,* pp. 9-15, 2012.
[29] G. Zhu, Y. Zheng, D. Doermann, S. Jaeger, "Signature detection and matching for document image retrieval," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 31, pp. 11, 2009.
[30] J. Yang, J. Xie, G. Zhu, S. Kwong, and Y. Q. Shi, "An effective method for detecting double JPEG compression with the same quantization matrix," *IEEE Transactions on Information Forensic and Security*, vol. 9, no. 11, pp. 1933-1942, 2014.
[31] S. Azarian Pour, M. Babaie-Zadeh, A. R. Sadri, "An automatic JPEG ghost detection approach for digital image forensics," *24th IEEE Iranian Conference on Electrical Engineering*, 2016.
[32] J. Lukas, J. Fridrich, and M. Golijan, "Digital camera identification from sensor pattern noise," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 2, pp. 205-214, 2006.
[33] C. W. Mohammad, M. Shahid, and S.Z. Hussain, "Fuzzy attributed goal-oriented software requirements analysis with multiple stakeholders," *International Journal of Information Technology*, pp. 1-9, 2018.
[34] M. Sadiq, "A fuzzy-set based approach for the prioritization of stakeholders on the basis of the importance of software requirements," *IETE Journal of Research*, vol. 63, no. 5, pp. 616-629, 2017.

BIOGRAPHIES OF AUTHORS

Azra Parveen is pursuing Ph. D. in Electronic Science from Department of Applied Sciences and Humanities, Faculty of Engineering and Technology, Jamia Millia Islamia (A Central University), New Delhi-110025, India. She received her M.Tech. in Electronics and Communication Engineering (ECE) from Indira Gandhi Delhi Technical University for Women, Delhi, in 2016. She did B. Tech. in ECE from Meerut Institute of Engineering and Technology affiliated with UPTU, Lucknow, UP, India, in 2008; and Diploma in Electronics Engineering from Aligarh Muslim University, Aligarh, UP, India, in 2005. She has worked as Lecturer in ECE at Shobhit Institute of Engineering and Technology, Gangoh, UP, India, from August 2008 to December 2012. She has published her Ph. D. research work in the following Conferences and Journals: (i) IEEE IndiaCom-2018 (ii) ICCCS-2019, Taylor and Francis Group, London (iii) Iran Journal of Computer Science-2019, Springer. Her area of interest includes Digital Image Forensics and Information Systems.

Zishan Husain Khan is working as Professor in Department of Applied Sciences and Humanities, Faculty of Engineering and Technology, Jamia Millia Islamia (A Central University), New Delhi-110025, India. He has worked as Post- doctoral fellow at Center for Nanoscience and Technology, National Tsing Hua University, Hsinchu, Taiwan, from December 2001 to January 31, 2005. Prof. Khan established the Center of Nanotechnology at King Abdul Aziz University, Jeddah, Saudi Arabia. He has published more than 100 papers in International Journals and presented more than 36 papers in Conference and Workshop. His area of research includes Nano-chalcogenides for memory devices, Nanostructures - Carbon Nanotubes, Semiconducting Nanoparticles, and Image Processing.

Syed Naseem Ahmad was born in 1952. He did his schooling from Minto Circle High School, Aligarh till 1968. Prof. Ahmad received his B.Sc. and M. Sc. Engineering in Electrical Engineering from Z. H. College of Engineering and Technology, Aligarh Muslim University (AMU), Aligarh, UP, India, in 1975 and 1979, respectively. He has worked with Philips Arabia from 1980 to 1985; as Assistant Professor at University Polytechnic, AMU, Aligarh, till May 1986; Assistant Professor at Post Graduate Department of Electronics at University of Kashmir from 1986 to 1990. Prof Ahmad served as Assistant Professor, Department of Electrical Engineering, Faculty of Engineering and Technology (FET), Jamia Millia Islamia (JMI), A Central University, New Delhi-25, India, from October 1990 to July 1995. From 1995 to July 2017, he worked in various positions at Department of Electronics and Communication Engineering, FET, JMI, New Delhi, 25, India. Prof. Ahmad has supervised at least nine Ph. D. and published more than 75 papers in various National and International Journals. Currently, Prof. Ahmad is supervising three Ph.D. in the area of Wireless Communications, Image processing, and Binary Decision Diagrams.