International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 8 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT183815

Authentication of Digital Image using Exif Metadata and Decoding Properties

D. P. Gangwar, Anju Pathania
Central Forensic Science Laboratory, Sector 36-A, Chandigarh, DFSS, MHA, Government of India

ABSTRACT

This work presents a robust analysis of digital images to detect the modifications/ morphing/ editing signs by using the image's exif metadata, thumbnail, camera traces, image markers, Huffman codec and Markers, Compression signatures etc. properties. The details of the whole methodology and findings are described in the present work. The main advantage of the methodology is that the whole analysis has been done by using software/tools which are easily available in open sources.

Keywords : Metadata, Exif, JPEG, Digital Image, Marker, Huffman, Codec.

I. INTRODUCTION

Now days the digital images are very popular in the uses due to the high availability of digital cameras in mobile phones. For some people, a picture may be irrelevant or just for fun, but for others, it may represent evidence which could be used to clarify the real facts for legal, civil, administrative or criminal implications. Therefore, a digital image could have a really high impact in our life and it could be much more representative than the oral or written description of an events. With the technological advancement a digital image could be easily edited or morphed with the tools, which are easily available in open sources platform. As per court of law the digital image could be considered as important evidence, but it has to be proved that the image is original and has not been edited or morphed. In this work a new methodology was used to authenticate the digital image. It is based on the exif metadata and decoding properties of digital images, which always present in hidden form in JPEG(Joint Photographic Experts Group) header.

Each image has its own metadata. There are three class of metadata as Technical Metadata, Descriptive Metadata and Administrative Metadata. The Exif(exchangeable image file format) metadata decoding properties such as image thumbnail, camera traces, signatures of software used in editing of the digital image, Hoffman codec have been studied. The JPEG uses a lossy form of compression based on the discrete cosine transform (DCT). The Exif metadata of the JPEG image consist a lot of information regarding a sequence of segments, each of which begins with a 0xFF byte followed by a byte indicating what kind of marker it is. Some markers consist of just those two bytes. Common JPEG markers are SOI (Start Of Image), SOIf0 (Start Of Frame), baseline DCT , SOS (Start Of Scan), APPn (Application-specific), EOI(End Of Image). Huffman codes, camera information such as make and model, image file directories (IFDs), GPS, creation and modification of IFDs, and the total number of entries in each of these. Some manufacturers of camera customize their metadata in such a way that they do not conform to the EXIF standard. These

customizations yield errors when parsing the metadata. We consider these errors to be a feature of camera design and therefore count the total number of parser errors, as specified by the EXIF standard.

II. LITERATURE REVIEW

Several researchers have utilized different techniques to detect the forgery in digital images. [1] M.Harran, et al. in his study "A method of verifying integrity and authenticating digital media" mentioned about tools, which could be used for extraction the metadata and mentioned the potential of metadata used for authentication of digital file. **[2]** Parthiban R et al. in his work "Image Authentication using JPEG Headers" Stated the methods of image authentication in details. [**3]** Francisco Rodríguez-Santos et al in his work Practical implementation of a methodology for digital images authentication using forensics techniques had concluded that the metadata, thumbnail, camera traces and compression signature found in digital image provides a robust analysis that grant certainty and reliability of the dictum result**. [4]** D.S.Sellva Manoj, et.al in his work " Digitized Authentication For Image Forensics" highlighted a determined forgery could conceal their traces of tampering by extracting the signature of a camera, modifying the image, and then resaving the image with the appropriate EXIF format and all of the appropriate parameters: image size, image quantization table, image Huffman code, thumbnail size, thumbnail quantization table, and thumbnail Huffman code.

III. METHODS AND MATERIALS

In this work the methodology utilized is based on robust analysis of digital images by analyzing the Exif metadata and decoding properties such as the image thumbnail, the camera traces and Marker of image, FID, Hufmain codec etc. The data were extracted from the digital image using various freeware tools such as Exiftool, JPEGSnoop, Opanda IExif 2.3, HxD, JPEGSnoop.

The sample images were taken from different sources such as camera and mobile phones like Samsung(OnPro7), Samsung J5, Samsung J7, Micromax(A106), Redmi Note 5(ME17) and SONY digital camera . For editing in sample photo images the most common and free-ware software like Adobe Photoshop, PhotoScape, Microsoft editor/viewer etc were used.

The software Opanda IExif 2.3, ExifTool by Phil Harvey (available from www.sno.phy.queensu.ca/ phil/exif- ~ tool/), HDX, JPEGSnoop, HxD etc, which is easily available from open sources, were utilized in present work. Every software has own features and limitation. The JPEGsnoop is the very good software for decoding the JPEG image. The JPEG snoop reports countless details including image quality, EXIF/IPTC metadata, Huffman table, JPEG marker, Error detection, PSD parsing, IPTC parsing, Batch Processing etc. The HxD also is a good freeware tool that can be used for decoding the digital image in binary and hex form. The other software such Opanda2.3 Exif viewer, Exif Read, freeware software may also be utilized for robust analysis of various exif metadata properties. For detection of editing/tempering in jpeg image the below mentioned Parameters have been studied.

When a digital image is captured, the camera details such as make, model, resolution, Image width /length, Exposure Time, F. Number, Focal length, ISO Speed Ratings, Shutter Speed Value, Interoperability IFD Pointer, Interoperability Index etc were studied. Thus, if the image has been modified, it is possible to find inconsistencies change of above features of camera and image. There are many software programs for image processing which are used to modify digital images. But many software

delete the thumbnail Info which could be very use full for identification of editing of image.

The digital image has lot of decoding features such as markers and Huffman Codec. Every JPEG file starts from binary value '0xFFD8', ends by binary value '0xFFD9'. There are several binary 0xFFXX data in JPEG data, they are called as "Marker", 0xFFD8 means SOI(Start of image), 0xFFD9 means EOI(End of image). When an image is edited using any software a lot of change occurred in this process. The deeply and bit by bit analysis of these features of original and edited image gave a very valuable and unique information, which is very helpful in verification of the authenticity of digital image.

IV. RESULTS AND DISCUSSION

From the metadata of the jpeg image file a lot of information such as image size, make & model of camera, X ,Y resolution, date and time of original and edited, GPF Info, Exposure Time, F Number, Exposure Program, Shutter Speed Value , Aperture Value, Brightness Value, Exposure Bias Value, Max Aperture Value, ISO Speed, and Thumbnail Info such as Image Width, Image Length, Compression, Orientation, etc. were obtained from the original and edited images.

The tracing the make and model of the camera, used to take the image, is not a difficult task and it can be traced out easily many software as shown **fig.1** using Ponda Exif viewer. The original date and time of capturing the image can also be easily identified using same or other software such as Opanda IExif 2.3, ExifTool, ExifRead, Jeffrey's Image Metadata Viewer, HXD viewer, JPEG snoop as given **Fig.1 & 2.** The mostly software are not capable to show the date and time of editing. For this we have used some software such as https://www.get-metadata.com/, normal properties from window software and KUSO_EXIF_Viewer_EN to identify the date and time when the image was edited, which are shown in **fig.2**. The identification of software used to modified the image could be also easily identified as shown fig**. 3 &4.** Thumbnail info of the jpeg image gives a very crucial information of image originality. The mostly image editing software does not retain thumbnail info in editing process. Hence, the absence of thumbnail in the direct indicator of image editing **fig.5 &6.**

Markers and Huffman Codec Analysis: Every JPEG file starts from marker Marker: SOI (xFFD8 , ends by Marker: EOI (End of Image) (xFFD9). There are several binary 0xFFXX data in JPEG data, they are called as "Marker", 0xFFD8 means SOI(Start of image), 0xFFD9 means EOI(End of image). In original image just after SOI the APP1 (xFFE1) marker start and if the image edited the extra marker i.e. Marker: APP0 (xFFE0) observed in JPEG snoop fig. **7 & 8**. The Endian (denoting or relating to a system of ordering bytes in a word, or bits in a byte) make changed from Intel (little) to Motorola (big). EXIF IFD1 and Embedded JPEG Thumbnail have been removed in edited image fig. **9 &10**. Huffman table length shapely changed 418 to 31. We have also tried to identify the individual features of same model of the mobile camera using HXD fig.**10 & 11**. The digital image taken from the two different mobile having same make and model can also be distinguished by using HXD data fig.**11 & 12**.

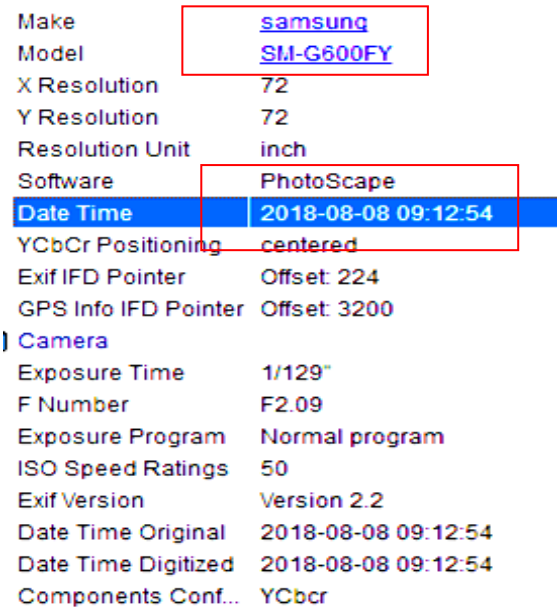

Figure 1. Showing the make, model of camera and the software used in edit image editing

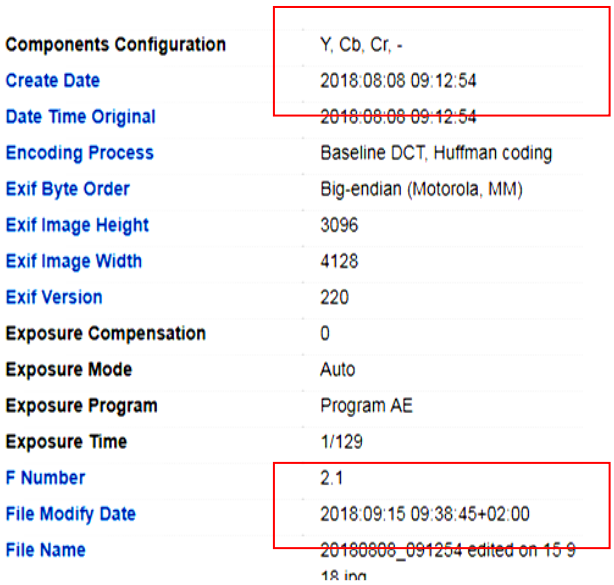

Figure 2. Showing the original & edited date & time

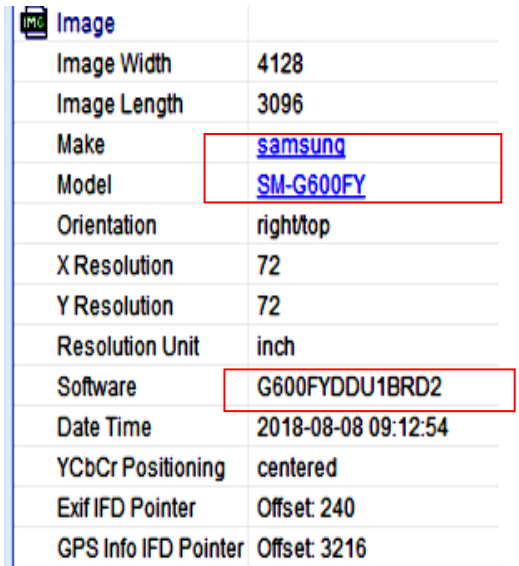

Figure 3. Showing original software

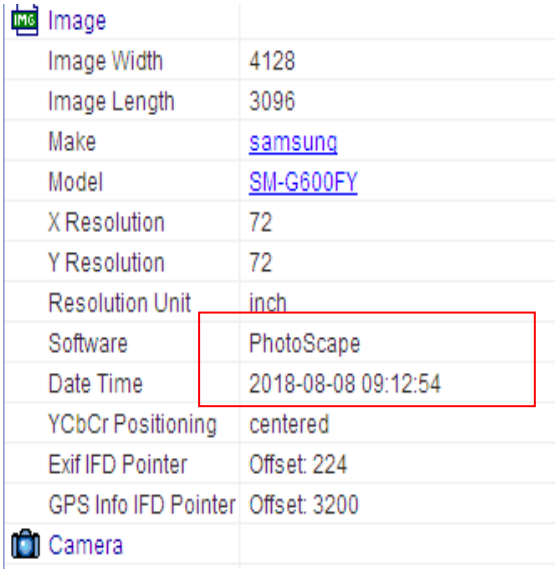

Figure 4. Showing software use for editing

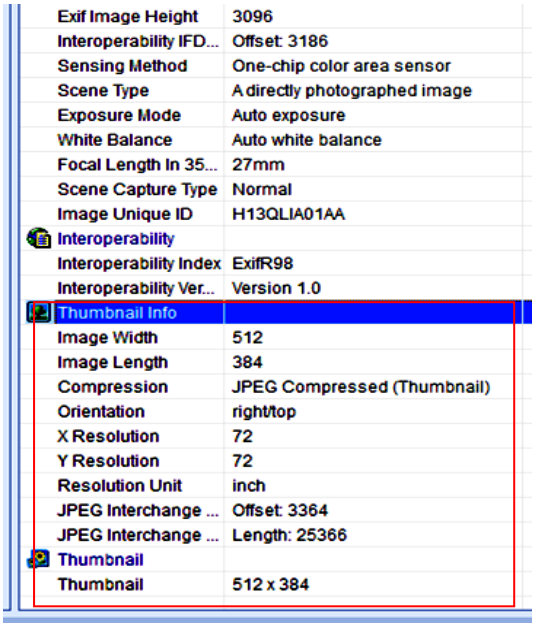

Figure 5. Thumbnail Info is present

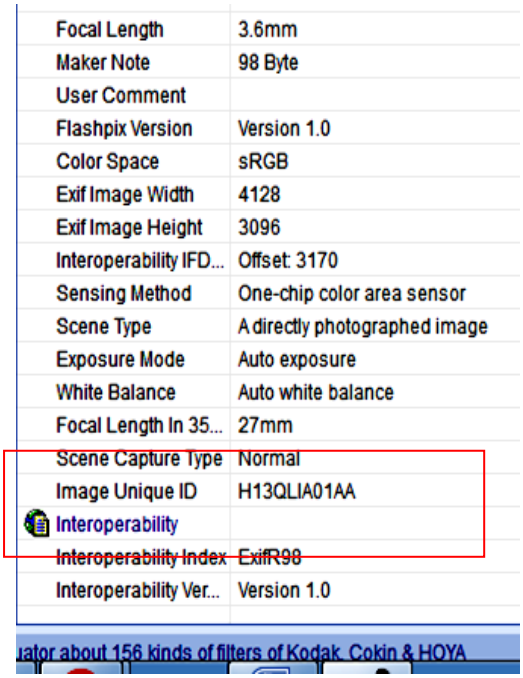

Figure 6. Thumbnail Info is absent

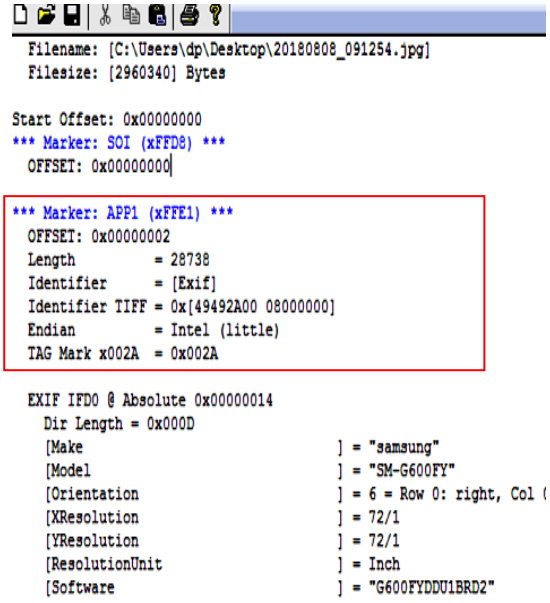

Figure 7. Original Image start (SOI) with marker APP1

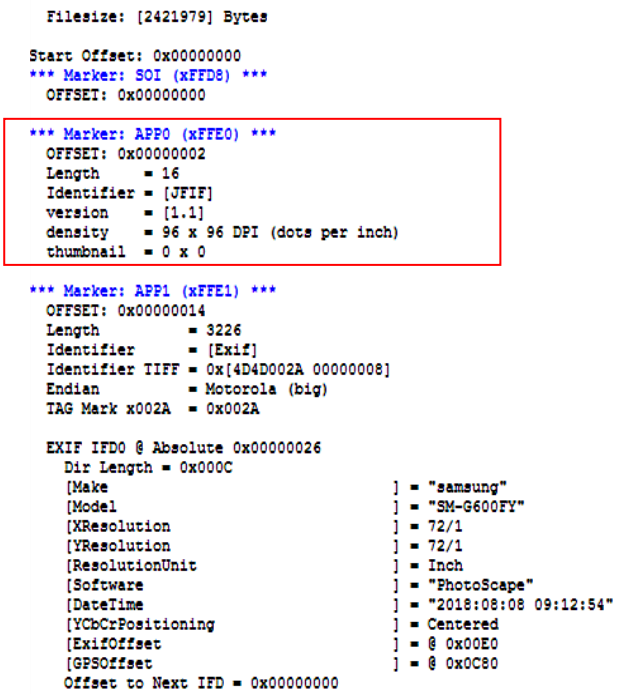

Figure 8. Edited Image SOI start with marker APP0

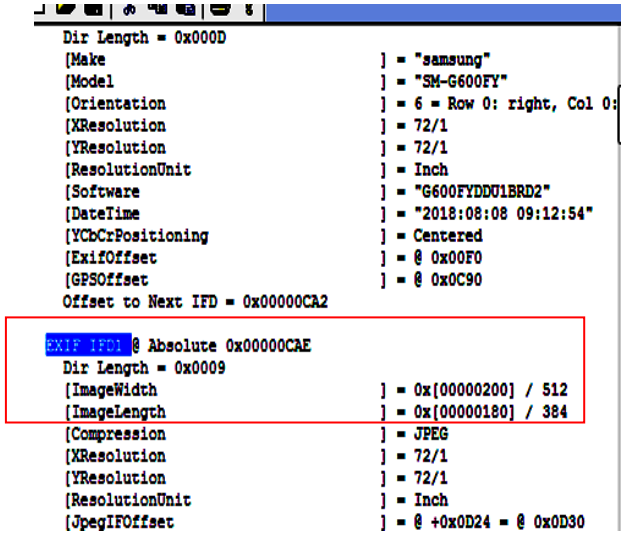

Figure 9. Marker EXIF IDF1

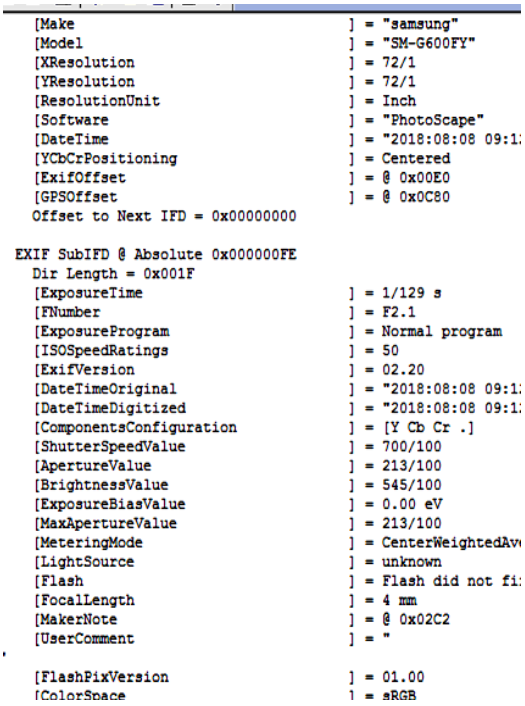

Figure10. Absent of EXIF IDF1

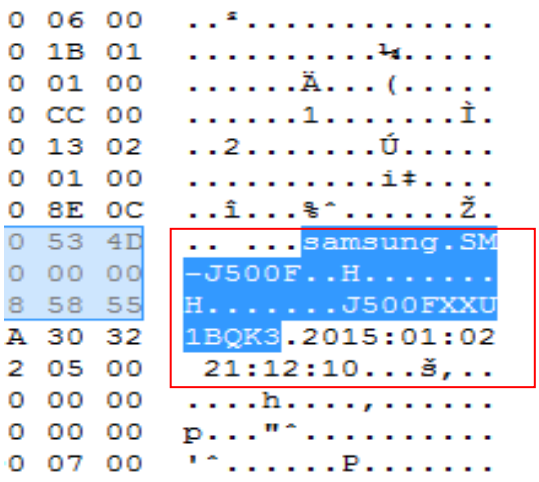

Figure 11: Showing image writing programme

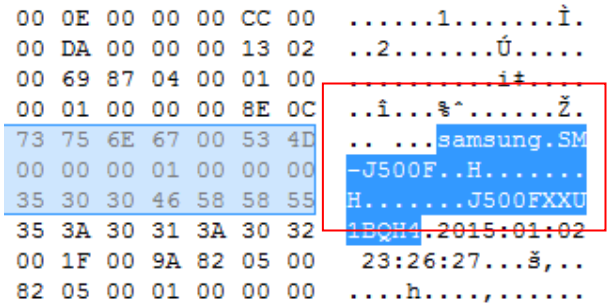

Figure.12 Showing image writing programme

V. CONCLUSION

From the above research output it was found that the authenticity of the digital image could be verified by robust analysis of different exif metadata and decoding properties using different free-ware software tools. The software or programme used for editing/morphing of the image, original date & time and the date& time when the image was edited could be identified with these tools. The absence of thumbnail Info details, presence of extra marker i.e. APP0 (xFFE0), absence of IFD1 and the shapely decrease the length of Huffman Codec recommended that the image has been edited. Hence, this methodology could be employed successfully for authentication of digital images for forensic, legal and other purpose.

VI. ACKNOWLEDGMENTS

The authors are very thankful to the Director, Central Forensic Science Laboratory Chandigarh for his valuable suggestion and guidance. I also wishes to thank to younger daughter (Naina) for not disbursing to me when the this story was written at home.

VII. REFERENCES

[1]. M. Harran, et al, "A method of verifying integrity and authenticating digital media" Applied Computing and Informatics, 1492018) PP 145-158.

[2]. Parthiban.R "Image Authentication using JPEG Headers" International Journal of Engineering Research & Technology (ISSN:2278-0181) Vol.3 Issue 4, April 2014.

[3]. Francisco Rodríguez-Santos et al, Practical implementation of a methodology for digital images authentication using forensics techniques "Advances in Computer Science: an International Journal, Vol. 4, Issue 6, No.18 , November 2015.

[4]. D.S.Sellva Manoj, et all, Digitized Authentication For Image Forensics. International Journal of Scientific & Engineering Research, Volume 4, Issue 5, May-2013.

Cite this article as :

D. P. Gangwar, Anju Pathania, "Authentication of Digital Image using Exif Metadata and Decoding Properties", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 3 Issue 8, pp. 335-341, November-December 2018. Available at
doi : https://doi.org/10.32628/CSEIT183815
Journal URL : http://ijsrcseit.com/CSEIT183815