Volume: 12 Issue: VI Month of publication: June 2024

DOI: https://doi.org/10.22214/ijraset.2024.63278

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue VI June 2024- Available at www.ijraset.com

GHIRO Unveiled: A Comprehensive Approach to Image Forensics and Suspect Detection

Kiranbhai R Dodiya[1], Dr. Kapil Kumar[2]
[1]Research scholar, Department of Biochemistry &Forensic Science, Gujarat University, Ahmedabad. Gujarat, India -380009
[2]Coordinator, Department of Biochemistry & Forensic Science, Gujarat University, Ahmedabad, Gujarat, India 38009

***Abstract:** In contemporary society, the ubiquity of digital photography has engendered a paradigm shift in how individuals perceive and interact with visual information. This proliferation, however, has concurrently birthed an inherent vulnerability: the susceptibility of digital images to manipulation. The ramifications of this susceptibility extend across diverse sectors, including but not limited to public discourse, law enforcement, political narratives, and media representations. In light of the escalating sophistication of digital editing tools, the pervasiveness of counterfeit photographs has become an increasingly pressing concern, precipitating a palpable erosion of trust in the integrity of visual media. This research addresses this difficulty by propounding a methodological framework centred around Ghiro software—a commendable exemplar of open-source innovation tailored to expedite the forensic scrutiny of digital imagery. Ghiro, with its automated algorithms, operates as a stalwart sentinel in elucidating alterations perpetrated upon original photographs. Its efficacy, epitomised by a judicious amalgamation of computational prowess and forensic acumen, positions it as a formidable bulwark against the surreptitious incursions of digital manipulation. Methodologically, this study adopts an empirically grounded approach, wherein the efficacy of Ghiro in discerning subtle alterations within digital photographs is subjected to rigorous scrutiny. Ghiro's capacity to unveil an array of manipulations—ranging from pixel-level modifications to intricate compositing— is unequivocally showcased through meticulously designed experimental protocols. Notably, the study accentuates Ghiro's utility as an automated tool, thereby mitigating the temporal and cognitive burdens traditionally associated with manual forensic analysis. These findings have direct implications for professionals in the fields of digital photography, law enforcement, and media representation, providing them with a powerful tool to combat digital image manipulation.*

The findings elucidated within this research underscore Ghiro's indispensability as an influential instrument in fortifying the integrity of digital imagery. By its open-source architecture, Ghiro augurs a paradigm shift in collaborative forensic practices, engendering an ecosystem wherein communal knowledge and technological innovation converge to combat the proliferation of counterfeit photographs. In extrapolating these findings, this research advocates for the pervasive adoption of Ghiro within forensic contexts, thereby auguring a renewed epoch of trust and accountability within the digital milieu

Keywords: Image Forensics, Digital Manipulation, Ghiro Software, Authentication, Counterfeit Detection.

I. INTRODUCTION

In today’s world, the use of digital images has grown remarkably across social media and other networking sites. Image manipulations are increasing daily due to more accessible access to image editing software. Image forensics aids in the detection of manipulated digital images. Digital image forensics, or Photo Forensics, is a newly emerging sub-field of Digital Forensics that aids in verifying the authenticity of digital image files.

A. What is a Digital Image?

A digital image is a collection of fixed elements with a unique value at a specific location. These elements represent image elements, picture elements, and pixels. The elements of a digital image are indicated mainly by pixels. Pixels are arranged in a rectangular array. The dimensions of the pixel array describe the size of an image. For instance, the number of columns in an array is the image width, and the number of rows in an array indicates the height of the image. The number of pixels in a digital image distinctively represents the image size. The digital image is represented by resolution, type of intensity, and intensity range.

1) *Resolution:* It depicts the spatial scale of image pixels. Resolution is termed “PPI” (pixels per inch), “dpi” (dots per inch), and “LPI” (lines per inch). LPI is mainly used in printing newspapers and magazines, whereas dpi indicates printer resolution, and PPI indicates a pixel array.

2) *Intensity Type:* Different types of intensity are applied for each pixel to get a different image. Every pixel has its unique intensity value. If all the pixels are used with the same intensity value, all images will be in the same colours. For instance, all the images will be black, white, or grey. The intensity of black and white images ranges from darkest grey to lightest grey, i.e., from black to white. At the same time, the intensity of colour images ranges from the darkest to lightest shade of three different colours, i.e., Red, Green, and Blue. The mixture of these colour intensities produces the colour image. Thus, black and white images are known as grayscale images and colour images are known as RGB images.
3) *Intensity Range:* The intensity range of digital images is represented in bits. An 8-bit intensity range has 256 possible values. Black-and-white photos have a single 8-bit intensity range, whereas colour images have an 8-bit intensity range for each colour.[1].

B. Creation of Digital Image

Most digital images are built using a digital camera, computer graphics, or artificial intelligence. In a digital camera, lenses focus the light source to fall on the camera's sensors. The camera sensors, which consist of photodiodes, generate the digital image signals. Every photodiode transmits a different signal to the processor based on the light intensity and colour. The signals received by the processor store the processed signals in the camera's memory as a compressed file, i.e., as JPEG or as an uncompressed file. Further, if the image is edited for any modification or enhancement like sharpening, blurring, or brightening, the image will be recompressed and saved again in JPEG format.[2].

C. Formats of Image Files

Images are stored in a particular file format on storage media. File format describes the process of storing image information in the file and presenting the stored information on an output device. Image files can store data in compressed, uncompressed, or vector formats. Algorithms used for image compression reduce the storage space by reducing the data required to reconstruct an image. This helps in the faster transmission of an image across a network. There are a varied number of image file formats. However, the most frequently used online formats are JPEG, PNG, and GIF.[2][3].

II. DIGITAL IMAGE MANIPULATION

Digital image manipulation is the process of modifying the complete appearance of an image by enhancing its existing features and adding certain secondary elements. Cropping, Image splicing, cloning, morphing, and blurring are some techniques used in image manipulation.[4].

1) *Cropping:* It is a common manipulation technique practised by everyone to improve an image by eliminating unnecessary or irrelevant details from an image. It can also be called a copy-move attack or region duplication.
2) *Image Splicing:* In this technique, the selected regions from different images are pasted together to create a new image.
3) *Cloning:* This technique hides some original image contents by copying specific regions of an image and then pasting them to new locations within the same image. Morphing is a technique for transforming one image into another. It provides a unique effect in animations and motion images.
4) *Blurring:* Generally, blurring makes an image smooth, making the edges invisible. It is carried out using an image convolution matrix.[5].

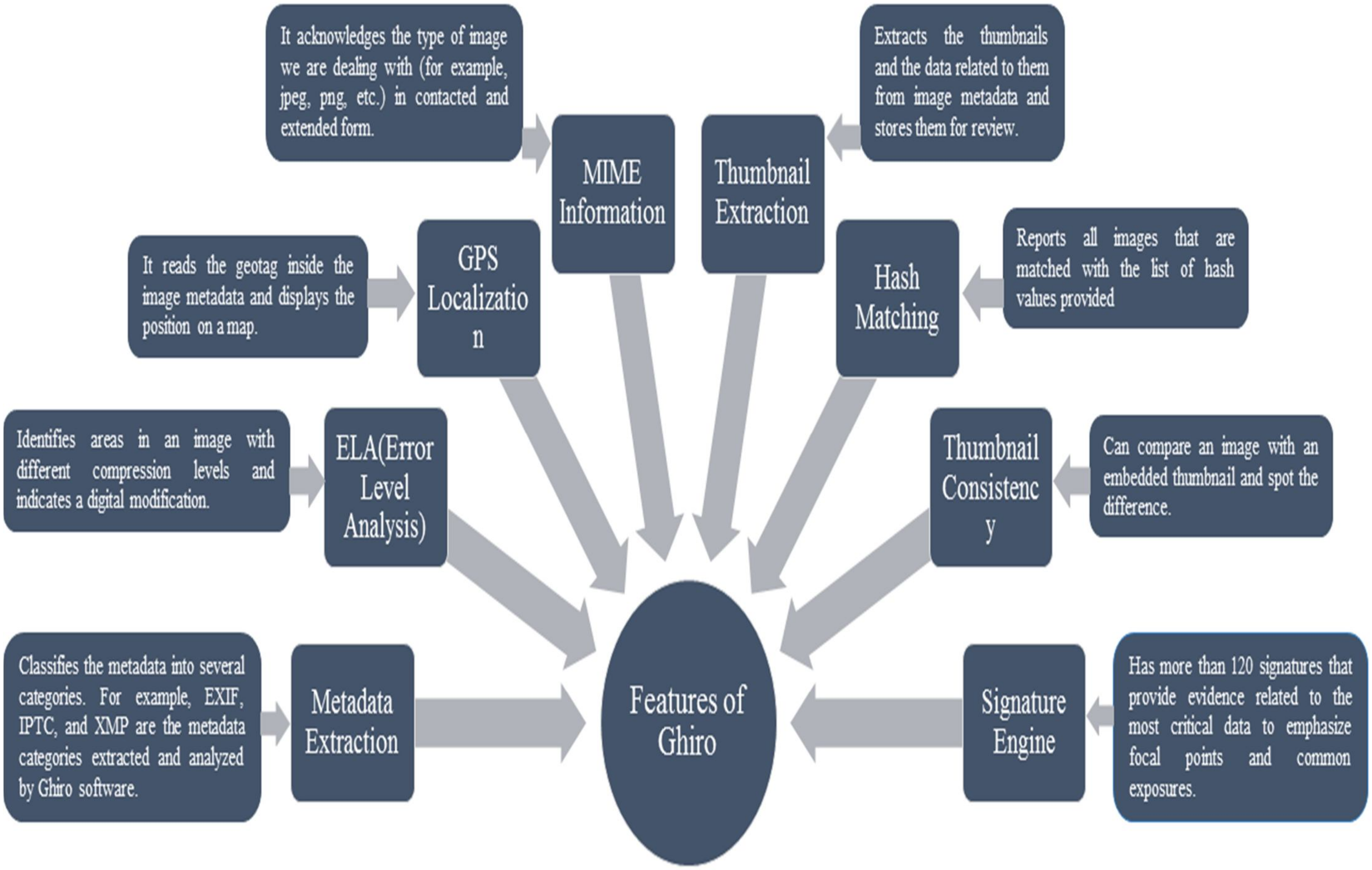
There are different open-source tools available such as GIMP, Photo Lemur, Coral paint shop, Light Zone, and Paint.NET, for easy editing of digital images.[6].

III. METHODOLOGY

The authenticity of an image can be confirmed by detecting whether an image is subjected to any manipulation. The detection techniques may be able to find certain unnoticed anomalies in images. The practical means of detecting image manipulation include certain pre-processing operations produced during an image's formation, like an embedded watermark or signature, image hash, image shielding, message authentication code, and image checksum. The utmost detection tools or methods depend on Metadata analysis, Clone Detection, and Error level analysis. Specific image forensic tools use unique algorithms to detect image manipulation based on Format-based techniques, Camera-based techniques, Pixel-based techniques, etc. Many freeware tools are available to aid in detecting image manipulation or alteration. In our experiment, we detected the manipulation of digital images using Ghiro software.

A. Ghiro Software

Ghiro is an open-source and fully automated software used for digital image forensics. Digital Images consist of tons of information. It helps analyse many images and extract information for a report. Alessandro Tanasi Jekil and Marco Buoncristiano Burlone developed Ghiro. This open-source software consists of many features that help quickly analyse manipulated images.[7]. The features of Ghiro include:

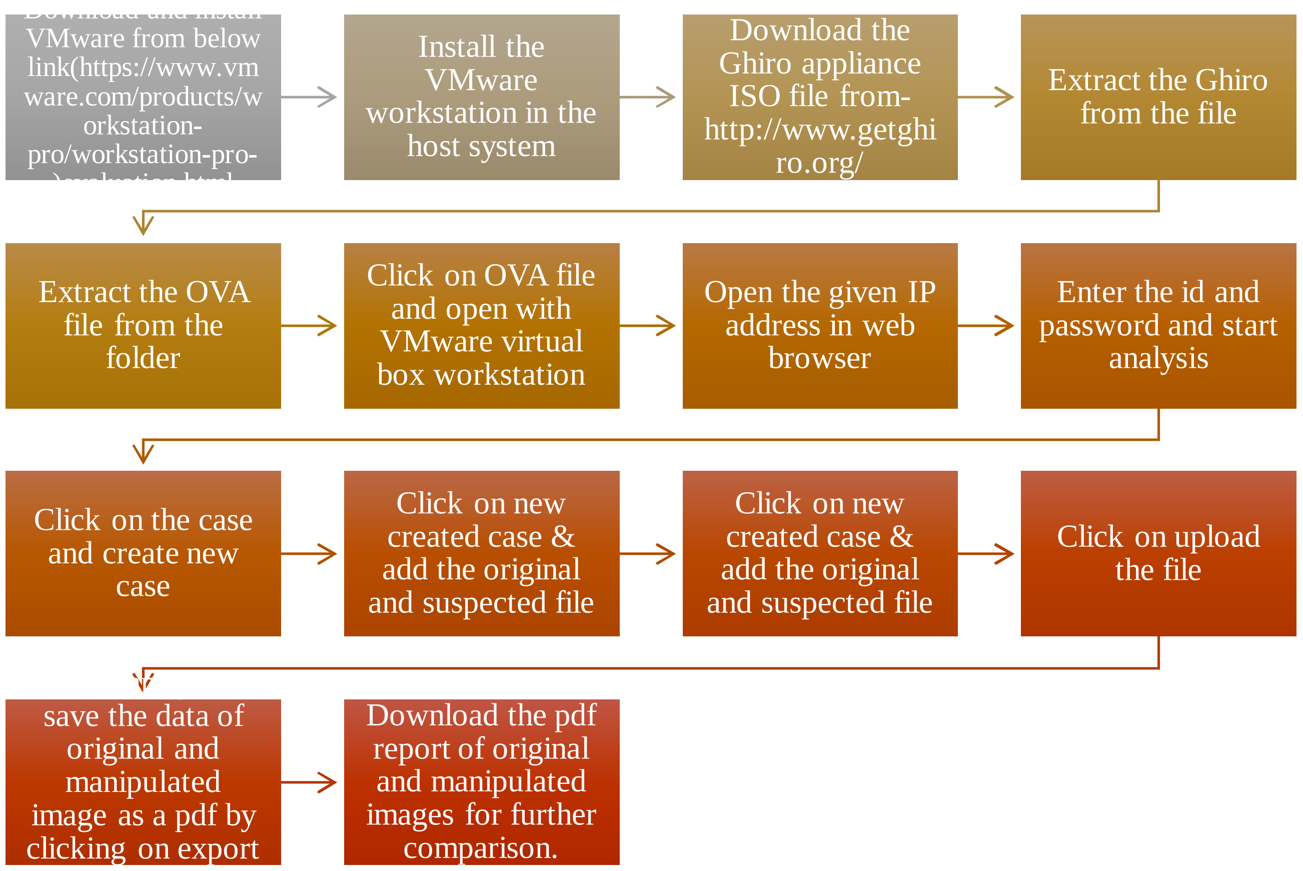

It acknowledges the type of image we are dealing with (for example, jpeg, png, etc.) in contacted and extended form.
MIME Information
Thumbnail Extraction
Extracts the thumbnails and the data related to them from image metadata and stores them for review.
It reads the geotag inside the image metadata and displays the position on a map.
GPS Localization
Hash Matching
Reports all images that are matched with the list of hash values provided
Identifies areas in an image with different compression levels and indicates a digital modification.
ELA(Error Level Analysis)
Thumbnail Consistency
Can compare an image with an embedded thumbnail and spot the difference.
Classifies the metadata into several categories. For example, EXIF, IPTC, and XMP are the metadata categories extracted and analyzed by Ghiro software.
Metadata Extraction
Features of Ghiro
Signature Engine
Has more than 120 signatures that provide evidence related to the most critical data to emphasize focal points and common exposures.

Flowchart showing the Features of Ghiro Software [7]

B. *Working with Ghiro*

The experimentation with the Ghiro software was carried out in a virtual box or VMware. The "OVA" version of the software is instrumental because it is the fastest way to initiate the Ghiro software. After downloading it, within a few minutes, it will be set up to analyse the images. When the "OVA" is opened in a virtual box, a screen displays the instructions for starting. It shows the IP address of the appliance and a browser link to set up the Ghiro. Then, we have to enter the IP address in the browser, which takes us to the login screen and fill in the credentials. After logging, we can set up the Ghiro software successfully. The dashboard in the home screen confirms the setup process that says, “Welcome to Ghiro”.

You must click the “case” option for image analysis and create a new case by adding specific information, such as case name, description, etc. Then, we open the latest case and upload the original and suspected file. The analysed data of both files can be saved as a separate PDF file for further comparison of original image data with manipulated data.[7].


Download and install VMware from below link(https://www.vmware.com/products/workstation-pro/workstation-pro-)evaluation.html
Install the VMware workstation in the host system
Download the Ghiro appliance ISO file from- http://www.getghiro.org/
Extract the Ghiro from the file
Extract the OVA file from the folder
Click on OVA file and open with VMware virtual box workstation
Open the given IP address in web browser
Enter the id and password and start analysis
Click on the case and create new case
Click on new created case & add the original and suspected file
Click on new created case & add the original and suspected file
Click on upload the file
save the data of original and manipulated image as a pdf by clicking on export
Download the pdf report of original and manipulated images for further comparison.

Flowchart showing the Ghiro software's setup process and analysis of original and manipulated images.

Ten original images were selected for this study. Out of those, we randomly chose some photos for editing. Below are the pictures: one is original, and the other is suspected and analysed by the open-source Ghiro software.

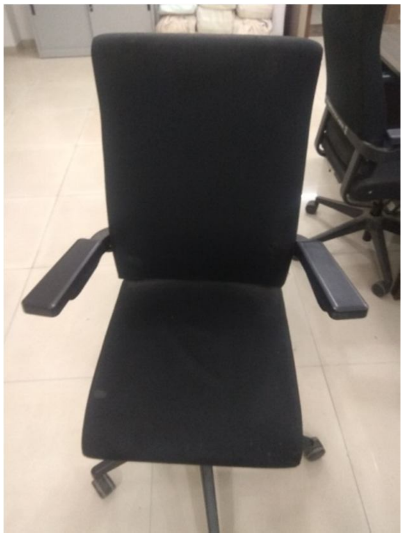


Figure 1: Original Image

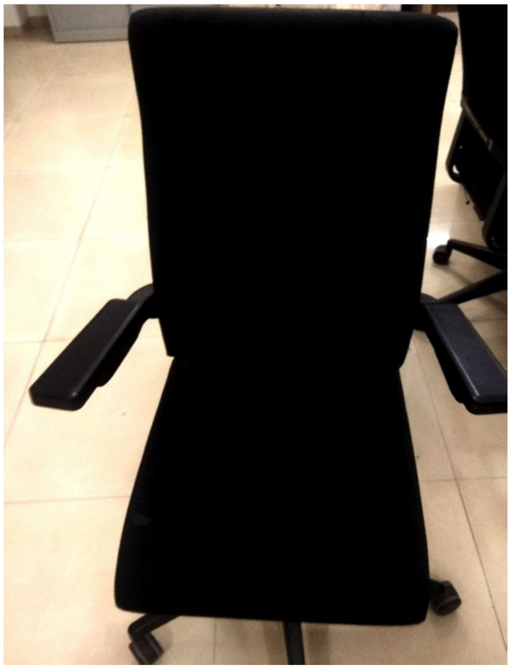


Figure 2: Manipulated Image

IV. RESULT AND DISCUSSION

The analysed data of both the original and suspected images are downloaded as a PDF file, which is then used for comparison.

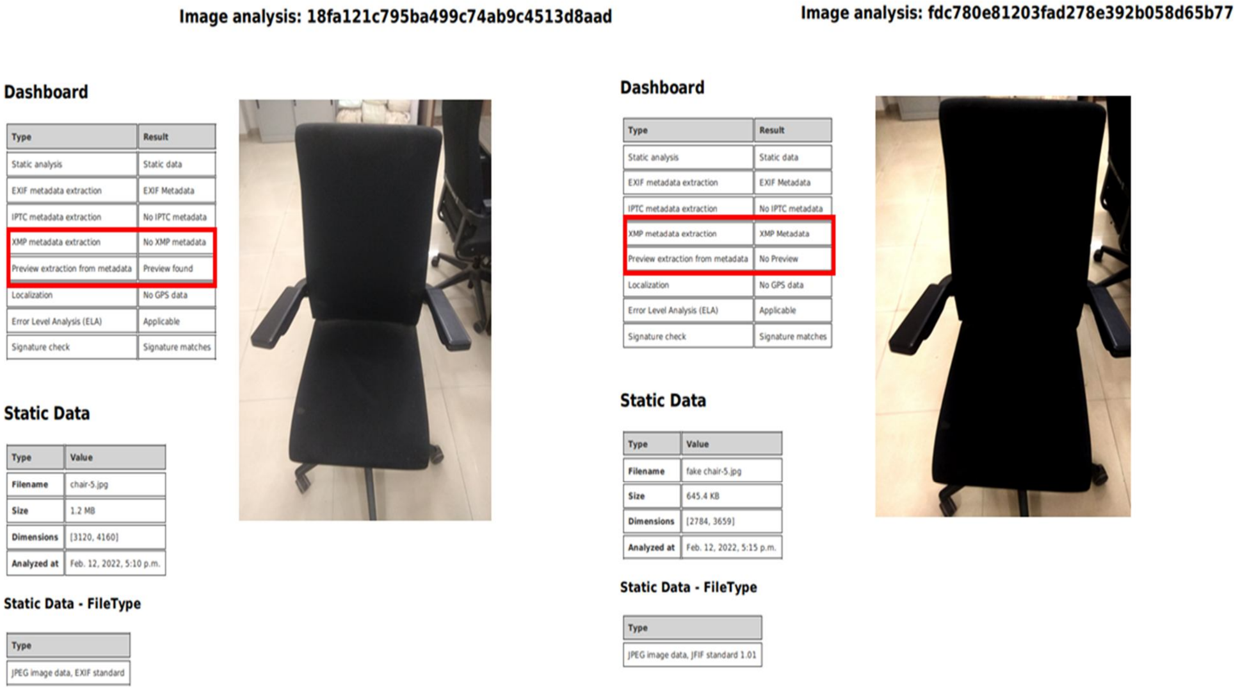


Image analysis: 18fa121c795ba499c74ab9c4513d8aad

Dashboard

Type	Result
Static analysis	Static data
EXIF metadata extraction	EXIF Metadata
IPTC metadata extraction	No IPTC metadata
XMP metadata extraction	No XMP metadata
Preview extraction from metadata	Preview found
Localization	No GPS data
Error Level Analysis (ELA)	Applicable
Signature check	Signature matches

Static Data

Type	Value
Filename	chair-5.jpg
Size	1.2 MB
Dimensions	[3120, 4160]
Analyzed at	Feb. 12, 2022, 5:10 p.m.

Static Data - FileType

Type
JPEG image data, EXIF standard

Image analysis: fdc780e81203fad278e392b058d65b77

Dashboard

Type	Result
Static analysis	Static data
EXIF metadata extraction	EXIF Metadata
IPTC metadata extraction	No IPTC metadata
XMP metadata extraction	XMP Metadata
Preview extraction from metadata	No Preview
Localization	No GPS data
Error Level Analysis (ELA)	Applicable
Signature check	Signature matches

Static Data

Type	Value
Filename	fake chair-5.jpg
Size	645.4 KB
Dimensions	[2784, 3659]
Analyzed at	Feb. 12, 2022, 5:15 p.m.

Static Data - FileType

Type
JPEG image data, JFIF standard 1.01

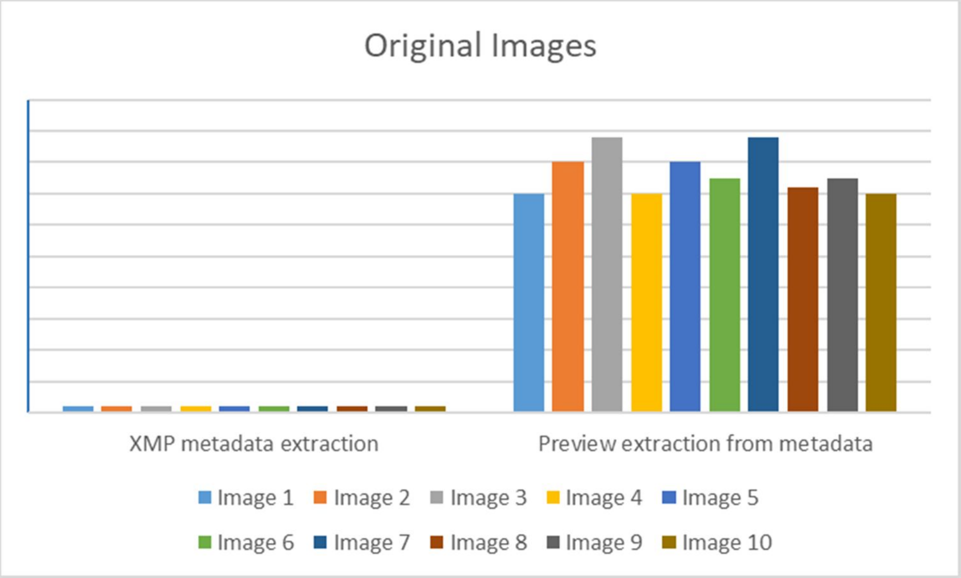
Comparison of Original and suspected image data

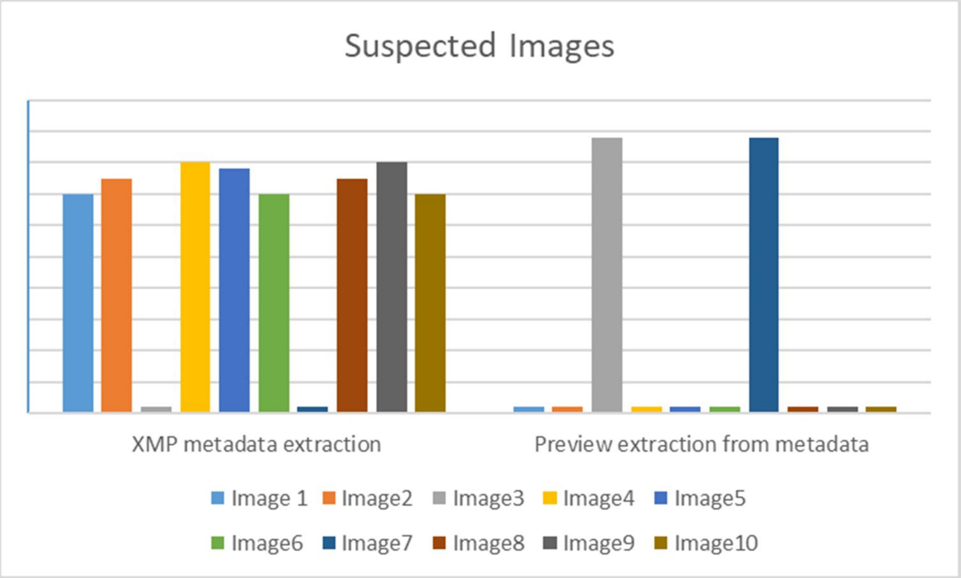
No XMP metadata was found in the original image, but preview extraction from metadata was. We found the XMP metadata in the suspected image, but preview extraction from metadata was not found. By careful examination of the result, we have found that the alleged image contains the XMP metadata, a change in file size, and no preview, confirming that the image is subjected to manipulation.

The table gives you comparative data of ten original and suspected images.

SR. NO.	FEATURES	ORIGINAL IMAGE	SUSPECTED IMAGE
1.	XMP metadata extraction	No XMP metadata	XMP metadata found
	Preview extraction from metadata	Preview found	No preview found
2.	XMP metadata extraction	No XMP metadata	XMP metadata found
	Preview extraction from metadata	Preview found	No preview found
3.	XMP metadata extraction	No XMP metadata	No XMP metadata
	Preview extraction from metadata	Preview found	Preview found
4.	XMP metadata extraction	No XMP metadata	XMP metadata found
	Preview extraction from metadata	Preview found	No preview found
5.	XMP metadata extraction	No XMP metadata	XMP metadata found
	Preview extraction from metadata	Preview found	No preview found
6.	XMP metadata extraction	No XMP metadata	XMP metadata found
	Preview extraction from metadata	Preview found	No preview found
7.	XMP metadata extraction	No XMP metadata	No XMP metadata
	Preview extraction from metadata	Preview found	Preview found
8.	XMP metadata extraction	No XMP metadata	XMP metadata found
	Preview extraction from metadata	Preview found	No preview found
9.	XMP metadata extraction	No XMP metadata	XMP metadata found
	Preview extraction from metadata	Preview found	No preview found
10.	XMP metadata extraction	No XMP metadata	XMP metadata found
	Preview extraction from metadata	Preview found	No preview found

In the above table, we have considered certain features of Ghiro software, like XMP, Preview metadata extraction, and Dimensions. Comparing the results, we have observed that the suspected image shows XMP metadata, a change in size, and the presence of dimensions. All these data confirmed that the photos numbered 1,2,5,6,8,9,10 were subjected to manipulation, and image no. 3 and 7 were found original.





V. CONCLUSION

In this internet and social media era, a question arises on the authenticity of a digital image. Digital images are widely used nowadays as evidence of history and present happenings in police investigations, law enforcement, journalist's reports, medical examinations, and many more. Numerous crimes are being reported daily due to manipulated images' convenient creation. In this paper, we proposed Ghiro software for detecting manipulated and original images. With the help of Ghiro software, one can quickly identify the original and manipulated image. By observing metadata information of both original and suspected images through analysis in Ghiro software, we can confirm the authenticity of an original image.

REFERENCES

[1] "Digital Image Processing Basics - GeeksforGeeks." Accessed: Jun. 13, 2024. [Online]. Available: https://www.geeksforgeeks.org/digital-image-processing-basics/

[2] A. Tanasi, "Photo Manipulation: Software to Unmask Tampering," Digital Investigative Journalism: Data, Visual Analytics and Innovative Methodologies in International Reporting, pp. 179–190, Jan. 2018, doi: 10.1007/978-3-319-97283-1_17.

[3] A. Piva, "An Overview on Image Forensics," Int Sch Res Notices, vol. 2013, no. 1, p. 496701, Jan. 2013, doi: 10.1155/2013/496701.

[4] "Digital Media Literacy: The Problem with Photo Manipulation." Accessed: Jun. 13, 2024. [Online]. Available: https://edu.gcfglobal.org/en/digital-media-literacy/the-problem-with-photo-manipulation/1/

[5] S. Patel and K. Shah, "Need of Photo Forensics in Era of Social Media," 2021. [Online]. Available: www.ijcrt.orgwww.ijcrt.org

[6] "10 Best GIMP Alternatives in 2024: Best Image Editor." Accessed: Jun. 13, 2024. [Online]. Available: https://www.geeksforgeeks.org/gimp-alternatives

[7] "Ghiro - automated digital image forensics tool." Accessed: Jun. 13, 2024. [Online]. Available: https://getghiro.org/