A Mini Project Report

On

"TOOL FOR DIGITAL FORENSICS OF IMAGE"

by

Samir Hasan Shaikh (.)

Kaylan Arjun Sansare (.)

Lina Pravin Birari (.)

Under the guidance of

Dr. B.S.Shirole

Department of Computer

Engineering

S.M.E.S. Sanghavi College

of Engineering, Nashik.

SAVITRIBAI PHULE PUNE UNIVERSITY

2022_2023

Department of Computer Engineering

S.M.E.S. Sanghavi College of Engineering

Date:

CERTIFICATE

This is to certify that,Samir Hasan Shaikh (.) Kalyani Arjun Sansare (.) Lina Pravin Birari (.) of class **T.E Computer**; have successfully completed their mini project work on **"TOOL FOR DIGITAL FORENSICS OF IMAGE"** at **Institute of Technology,Management & research, Nashik** in the partial fulfillment of the Graduate Degree course in **B.E** at the department of **Computer Engineering** in the academic Year 2022-2023 Semester – I as prescribed by the Savitribai Phule Pune University.

{ Dr. B.S.Shirole}
Project Guide

{ Prof. Puspendu.Biswas}
Head of Department

ACKNOWLEDGEMENT

With deep sense of gratitude we would like to thanks all the people who have lit our path with their kind guidance. We are very grateful to these intellectuals who did their best to help during our project work.

It is our proud privilege to express deep sense of gratitude to **Dr.A.D. Lokhande,** Principal Sanghavi college of engineering, Nashik for his comments and kind permission to complete this project.We remain indebted to **Prof.Puspendu.Biswas**, H.O.D. of Computer Engineering Department for his timely suggestion and valuable guidance.

The special gratitude goes to **Dr.B.S.Shirole** excellent and precious guidance in completion of this work .We thanks to all the colleagues for their appreciable help for our working project. With various industry owners or lab technicians to help, it has been our endeavor to throughout our work to cover the entire project work.

We also thankful to our parents who providing their wishful support for our project completion successfully .And lastly we thanks to our all friends and the people who are directly or indirectly related to our project work.

Samir Hasan Shaikh (.)

Kalyani Arjun Sansare (.)

Lina Pravin Birari (.)

ABSTRACT

Image trustworthiness has become a challenge these days, resulting into lack of affordable veritable tool that ensures viable admissibility as evidence in the court of law. Existing tools in this category are characterized with high cost. This study presented a cost-effective approach that could assist forensic experts in establishing the reliability of image by checking discrepancy in Exchangeable Image File Format (EXIF) metadata and detecting the presence of double compression artifact. Experimental set up using Discrete Cosine Transform and EXIF metadata parameters techniques shows that the approach presented here has an improved outcome over some existing techniques for image authenticity check required in digital forensics investigation.

TABLE OF CONTENTS

INTRODUCTION

1.1 Title

Design and develop a tool for digital forensics of images.

1.2 Problem Statement

Design and develop a tool for digital forensics of images.

1.3 Objective

To design a tool for digital forensics of images.

1.4 Introduction

In today's world, photography has become almost everyone's hobby. This is as a result of advances in technology which brought about availability of handy and pocket-sized digital cameras at avoidable prices especially, the availability camera in mobile phones.

Many people use these pictures for reminiscence; others use them for website decoration while some use them as evidence to support claim. The high potential of visual media and the ease with which they are captured, distributed and stored is such that they are used to convey information.

Digital images have become one of the major information carriers in our modern daily lives. While people enjoy the efficiency of information exchange, the security and trustworthiness of digital images have become a crucial issue due to the ease of malicious processing, for instance, embedding secret messages for covert communications, altering origin and content of images with popular image editing software. These malicious usages could give rise to serious problems if they are taken advantage of by terrorist organizations, treated as evidence in court, or published by mass media for information dissemination.

There is a saying that "a picture is worth a thousand words", in recent years, this trust in picture has been eroded due to availability of advance image-editing software with little or no prior training in its usage which has made image manipulation easy.

Nowadays, modern photo editors and advance image editing techniques make image editing extremely easy to manipulate original images in such a way that any alterations are impossible to catch by an untrained eye, and can even escape the scrutiny of experienced editors of reputable news media. Even the eye of a highly competent forensic expert can miss certain signs of a fake image, potentially allowing forged (altered) images to be accepted as court evidence. As digital technology advances, the need for authenticating digital images, validating their content and detection of forgeries is inevitable.

Before the advent of computers, photo manipulations were carried out with different techniques such as double-exposure, piecing photos, retouching with ink, paint, scratching, Polaroids, etc. Airbrushes were also used, whence the term “airbrushing” for manipulation. Darkroom manipulations are sometimes regarded as traditional art rather than job related skill. In the early days of photography, the use of technology was not as advanced and efficient as it is now. The results are similar to digital manipulation but they are harder to create (Photo Manipulation, 2014).

An attempt has been made by major camera manufacturers to address this, such attempt includes introduction of secure digital certificates, watermarking, and so on. Watermarking is the process of embedding information into a digital signal in a way that is difficult to remove.Watermarking may be visible (as depicted in Figure 1.1 a and Figure 1.1b) or invisible; all these have been applied in the area of digital photography with a view to protecting the content and for future authentication. Visible digital watermarking is one of the modern widely used techniques. Invisible watermarking techniques hide some specific copyright, authentication, or other information inside the image for author’s identification to protect author’s right and restrict the intruder’s ability of unlimited copying and unauthorized use of the information. Also, these watermarks might add some other important information, for example, recipient marks to trace the image distribution, hidden annotation, key notes, etc.

SOFTWARE AND HARDWARE REQUIREMENTS

2.1 Software Requirements

- Windows XP/7/8/10
- Visual Studio Code
- Python 3.8

2.2 Hardware Requirements

- Personal Computer with minimum of Pentium 4 processor.
- 512MB Ram.
- 80GB Hard drive or higher configuration.

DESCRIPTION

Digital Image Forensics

Digital image forensics is a branch of digital forensics. Also known as forensic image analysis, the discipline focuses on image authenticity *and* image content. This helps law enforcement leverage relevant data for prosecution in a wide range of criminal cases, not limited to cybercrime.

How is digital image forensics performed?

Digital image forensics is performed on local machines and can be used in both open and closed source investigations. It's a highly sophisticated field of investigation which requires several software applications and specialist training.

The scope of digital image forensics is so wide-reaching because digital imagery is data-rich, by comparison to film photography. Using a variety of techniques, digital image forensics investigators can mine everything from camera properties to individual pixels for information.

What are the different types of digital image evidence?

A huge variety of digital evidence can be gleaned from a single image. These evidence forms can be split into two main groups which are used to complement one another:

Image Authenticity Evidence

- Pixel data (e.g. colour information)

- Metadata (e.g. descriptive, structural, administrative, reference, statistical)

- Street furniture (e.g. bollards, benches, bins)

Digital image forensics techniques

Two common uses of digital image forensics techniques are:

A) When a suspect denies their presence in an image.

B) When a suspect claims that an incriminating image has been faked.

In these different examples, law enforcement use digital image forensics techniques flexibly to reach a conclusion.

EXAMPLE A: DIGITAL IMAGE FORENSICS TECHNIQUES

If identities are somehow obscured, deconvolution can be applied to reverse image blurring. Geolocation, metadata and exif data can also help to either prove or disprove a defendant's presence at a crime scene.

EXAMPLE B: DIGITAL IMAGE FORENSICS TECHNIQUES

In the age of deep fakes, image authentication is crucial. Reviewing colour space and colour level anomalies would help to assess the digital photo's authenticity. Landmarks could also be used to help prove or disprove the suspect's whereabouts.

Digital Image Lifecycle

The life cycle of a digital image can be represented as a composition of several steps collected into three main phases: acquisition, coding, and editing. During acquisition, the light coming from the real scene framed by the digital camera is focused by the lenses on the camera sensor (a CCD or a CMOS), where the digital image signal is generated. Before reaching the sensor, however, the light is usually filtered by the CFA (Color Filter Array), a thin film on the sensor that selectively permits a certain component of light to pass through it to the sensor. In practice, to each pixel, only one particular main color (Red, Green, or Blue) is gathered. The sensor output is successively interpolated to obtain all the three main colors for each pixel, through the so-called demo saicing process, in order to obtain the digital color image. The obtained signal undergoes additional in-camera processing that can include white balancing, color processing, image sharpening, contrast enhancement, and gamma correction.Finally, the generated image can be post processed, for example, to enhance or to modify its content. Any image editing can be applied to an image during its life: the most used ones are geometric transformation (rotation, scaling, and so on), blurring, sharpening, contrast adjustment, image splicing (the composition of an image using parts of one or more parts of images), and cloning (or copy-move, the replication of a portion of the same image). Finally, after editing, very often the image is saved in JPEG format, so that a recompression will occur.

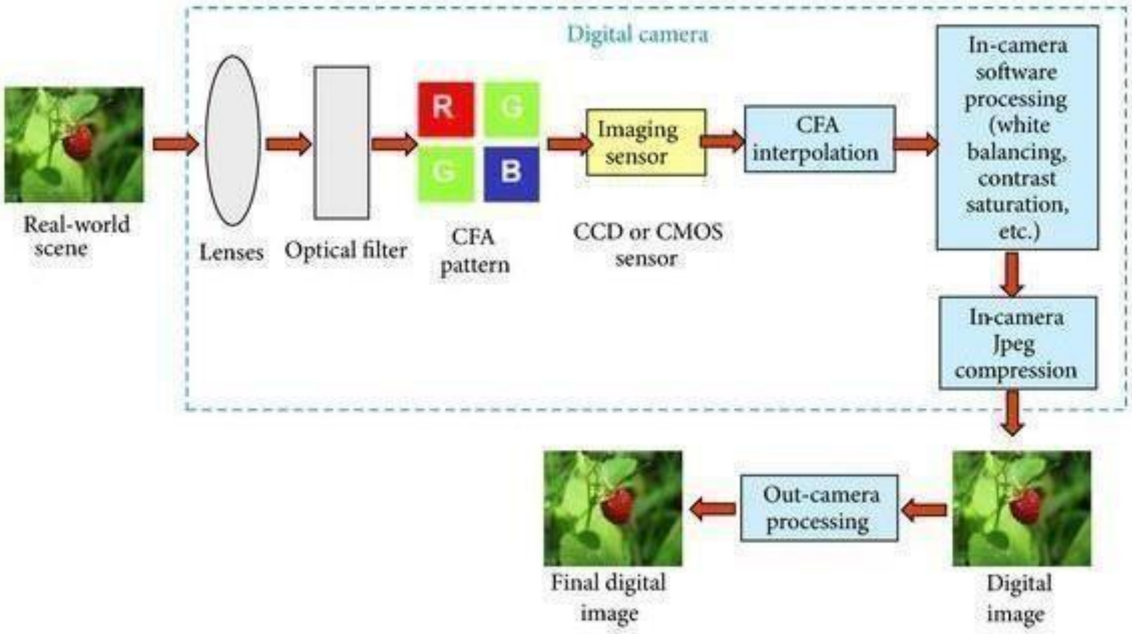


Fig 3.1. Digital Image Lifecycle

ALGORITHM AND ARCHITECTURE

4.1 Algorithm

- ➢ Input an Image to be checked.
- ➢ Decompress the image and divide it into 8 x 8 block and extract metadata from JPEG header.
- ➢ Check consistency in the metadata extracted.
- ➢ Check for inconsistency in the peak value of the image histogram.
- ➢ Classify the image into single or double compression class.

4.2 Architecture

The architectural view of the proposed model is presented in Figure 4.1. It consists of five phases i.e. Input, pre-processing, EXIF Analyzer, JPEG compression Analyzer and Classification phase.

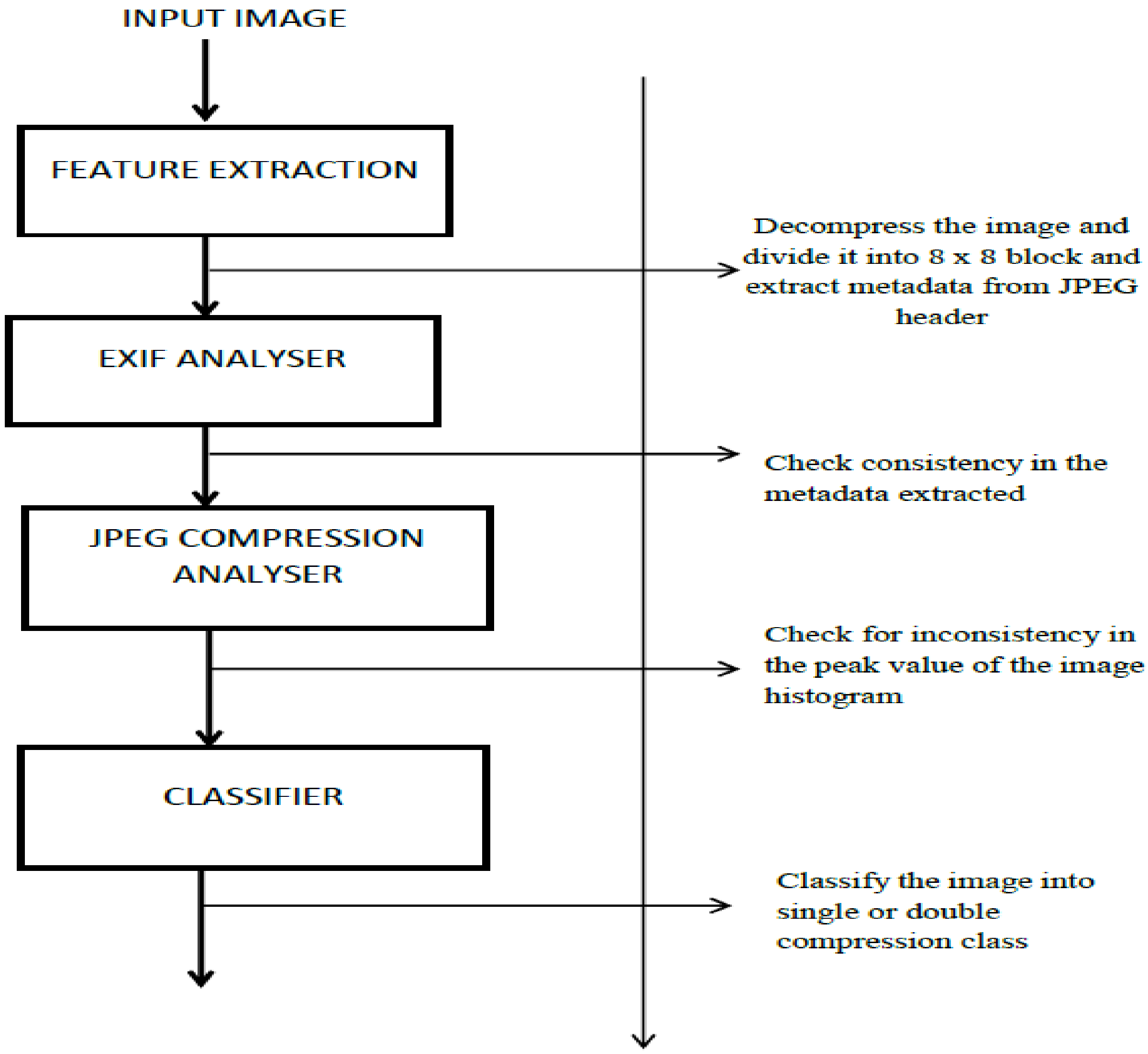


Fig. 4.1 Architecture Diagram

ADVANTAGES AND DISADVANTAGES

5.1 Advantages

- Heaps of granular data. The more data available to law enforcement, the greater chance it has of digitally identifying a suspect’s criminal activity.

- Flexible use cases. Digital image forensics techniques can be used in open and closed source investigations.

- Validated approaches and algorithms. Scientific underpinnings of discipline mean that it’s highly accurate and reliable.

5.2 Disadvantages

- Time and labour intensive. Open-source digital image forensics investigations can be built from a single and often minute clue. Painting a complete picture of a case can take many months.

CODE WITH OUTPUT

```
import os
import hashlib

from PIL import Image
from PIL import ExifTags

from PIL import Image, ImageChops

def extract_metadata(image_path):
    metadata = {}
    try:
        with Image.open(image_path) as img:
            # Extract EXIF metadata
            exif_data = img._getexif()
            if exif_data:
                for tag, value in exif_data.items():
                    tag_name = ExifTags.TAGS.get(tag, tag)
                    metadata[tag_name] = value
    except Exception as e:
        print(f"Error extracting metadata: {e}")

    return metadata

def calculate_image_hash(image_path):
    try:
        with open(image_path, 'rb') as img_file:
            image_data = img_file.read()
            image_hash = hashlib.md5(image_data).hexdigest()
            return image_hash
    except Exception as e:
        print(f"Error calculating image hash: {e}")
        return None

import os

# Change the working directory to the directory where your script is located
os.chdir(os.path.dirname(r"C:\\Users\\rutuj\\Downloads\\CSDF.jpeg"))

def main():
    image_path = input(r"C:\\Users\\rutuj\\Downloads\\CSDF.jpeg")

    if not os.path.exists(r"C:\\Users\\rutuj\\Downloads\\CSDF.jpeg"):
        print("Image file not found.")
        return

    metadata = extract_metadata(image_path)
    image_hash = calculate_image_hash(image_path)

    print("Metadata:")
    for key, value in metadata.items():
        print(f"{key}: {value}")
```

```
    if image_hash:
        print(f"Image MD5 Hash: {image_hash}")

if __name__== "_main_":
    main()
```

C:\\Users\\rutuj\\Downloads\\CSDF.jpeg CSDF.jpeg

Metadata:
Image MD5 Hash: e3e1c9efcc8861967ff4cb31f54aabea

```
from IPython.display import Image

# Replace 'image.jpg' with the path to your image file
img_path = r"C:\\Users\\rutuj\\Downloads\\CSDF.jpeg"
Image(filename=img_path)
```

pip install matplotlib

Requirement already satisfied: matplotlib in c:\users\rutuj\anaconda3\lib\site-packages (3.7.0)
Requirement already satisfied: contourpy>=1.0.1 in c:\users\rutuj\anaconda3\lib\site-packages (from matplotlib) (1.0.5)
Requirement already satisfied: cycler>=0.10 in c:\users\rutuj\anaconda3\lib\site-packages (from matplotlib) (0.11.0)
Requirement already satisfied: fonttools>=4.22.0 in c:\users\rutuj\anaconda3\lib\site-packages (from matplotlib) (4.25.0)
Requirement already satisfied: kiwisolver>=1.0.1 in c:\users\rutuj\anaconda3\lib\site-packages (from matplotlib) (1.4.4)
Requirement already satisfied: numpy>=1.20 in c:\users\rutuj\anaconda3\lib\site-packages (from matplotlib) (1.23.5)
Requirement already satisfied: packaging>=20.0 in c:\users\rutuj\anaconda3\lib\site-packages (from matplotlib) (22.0)
Requirement already satisfied: pillow>=6.2.0 in c:\users\rutuj\anaconda3\lib\site-packages (from matplotlib) (9.4.0)
Requirement already satisfied: pyparsing>=2.3.1 in c:\users\rutuj\anaconda3\lib\site-packages (from matplotlib) (3.0.9)

Requirement already satisfied: python-dateutil>=2.7 in c:\users\rutuj\anaconda3\lib\site-pack ages (from matplotlib) (2.8.2)

Requirement already satisfied: six>=1.5 in c:\users\rutuj\anaconda3\lib\site-packages (from p ython-dateutil>=2.7->matplotlib) (1.16.0)

Note: you may need to restart the kernel to use updated packages.

[notice] A new release of pip is available: 23.2.1 -> 23.3
[notice] To update, run: python.exe -m pip install --upgrade pip

```
import matplotlib.pyplot as plt
import matplotlib.image as mpimg

# Replace 'image.jpg' with the path to your image file
img_path = r"C:\\Users\\rutuj\\Downloads\\CSDF.jpeg"
img = mpimg.imread(img_path)

# Display the image
plt.imshow(img)
plt.axis('off')  # Turn off axis labels and ticks
plt.show()
```


```
pip install Pillow
```

Requirement already satisfied: Pillow in c:\users\rutuj\anaconda3\lib\site-packages (9.4.0)
Note: you may need to restart the kernel to use updated packages.

[notice] A new release of pip is available: 23.2.1 -> 23.3
[notice] To update, run: python.exe -m pip install --upgrade pip

```
from PIL import Image
```

```
from PIL import Image, ImageChops
```

def error_level_analysis(original_path, manipulated_path, tolerance=10): original_image = Image.open(original_path)

manipulated_image = Image.open(manipulated_path)

diff = ImageChops.difference(original_image, manipulated_image)

diff.show()

```
    # Rest of your code for error level analysis

# Call the function
original_image_path = "C:\\Users\\rutuj\\Downloads\\CSDF.jpeg"
manipulated_image_path = "C:\\Users\\rutuj\\Downloads\\CSDF.jpeg"

print("Authentic-->>>>>>>>>>>>>>>>>>>>>> \n")
error_level_analysis(original_image_path, manipulated_image_path)

print("\n\n\nManipulated--->>>>>>>>>>>>>>>>>> \n")
manipulated_image_path = "C:\\Users\\rutuj\\Downloads\\CSDF Copy.jpeg"
error_level_analysis(original_image_path, manipulated_image_path)
```

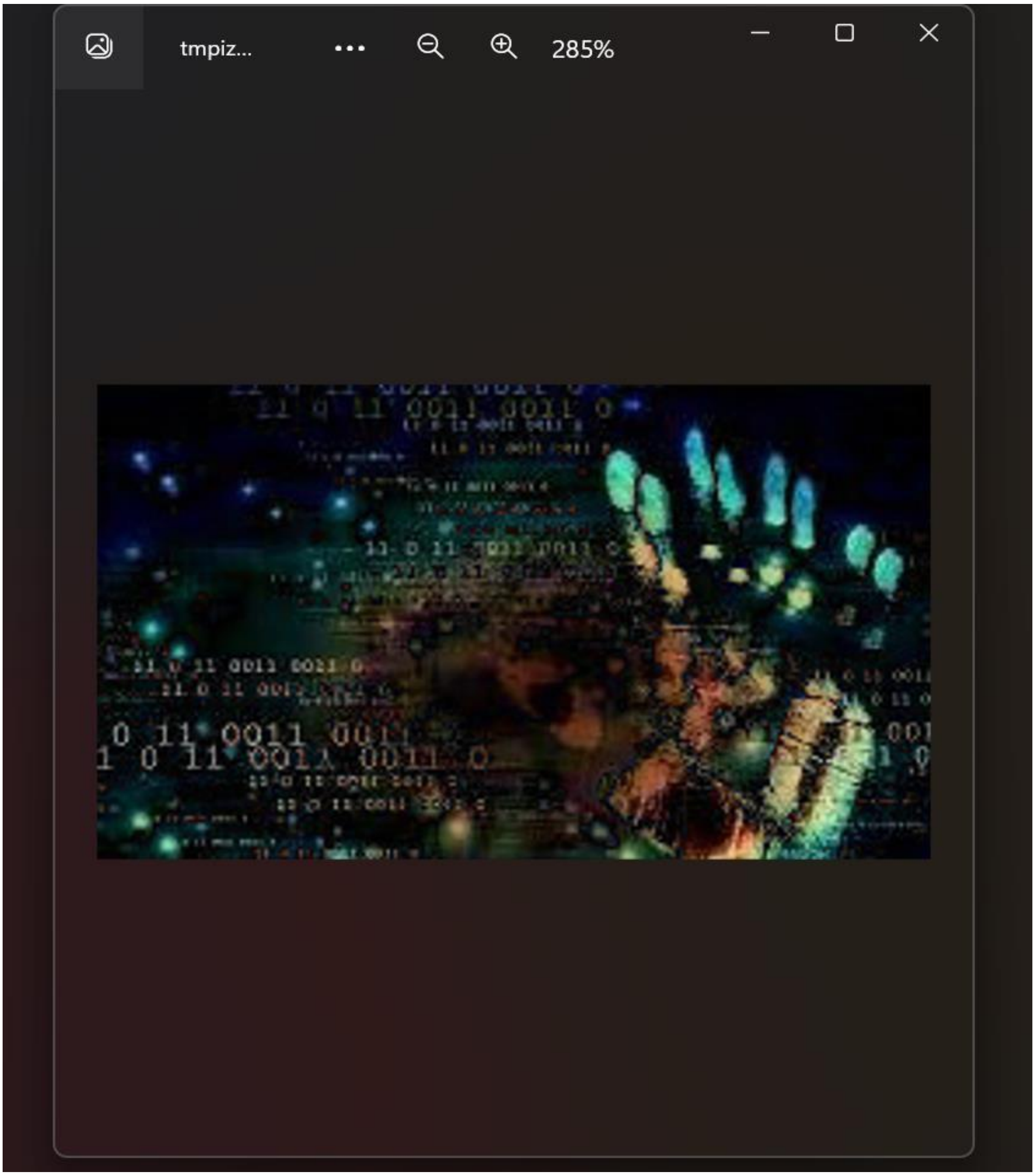
```
Authentic-->>>>>>>>>>>>>>>>>>>>>>



Manipulated--->>>>>>>>>>>>>>>>>>
```

RESULT

MANIUPULATED IMAGE



CONCLUSION

In this project, a new tool that will aid forensic experts in the discharge of their duty has been designed and implemented. Nowadays, image manipulation is not only carried out by experts but also those that have little or no knowledge about photo editing. This is due to modern, sop histicated and easy to use photo editing software.

This project is able to present a approach which can help in the detection of image/photo man ipulation which may be difficult to be detected by human eye. The hybridized tool combines

Metadata extracted from image under suspicion and analyses the statistical data of the image w ith a view to detecting manipulation evidence. Hence learnt to design and develop tools for digital forensics of image