NFSU JOURNAL OF CYBER SECURITY & DIGITAL FORENSICS

NFSU – Journal of Cyber Security and Digital Forensics
Volume –3, Issue – 2, December 2024
E – ISSN – 2583-7559

ANALYZING AND DETECTING TAMPERED IMAGES USING FORENSICS TOOLS IN DIGITAL IMAGE FORENSICS

Nibedita Hens

School of Forensic Sciences
National Forensic Sciences University Gandhinagar, India

Krishna Venkoba Gubballi

School of Forensic Sciences
National Forensic Sciences University Gandhinagar, India

Dr. Kapil Shukla

School of Forensic Sciences
National Forensic Sciences University Gandhinagar, India

Dr. Krishna Modi

School of Forensic Sciences
National Forensic Sciences University Gandhinagar, India

Abstract **- This paper explores the techniques and methods of analyzing tampered or fake images. Along With the increasing prevalence of digital image manipulation, there is a growing need for reliable methods to detect and verify the authenticity of digital images. The paper first discusses the various types of image tampering, including splicing, copy-move, and retouching. It then explores the different techniques used to analyze and detect each type of tampering. where it goes with detailed information on two tools that are used for tampering forensically - Beta and Foto-Forensics with different types of image samples like social media, WhatsApp, and Normal images from phones or cameras along with filters or the features of the tool like clone detection, Error level analysis, Noise analysis, Luminance Gradient, etc, It also examines the limitations associated with analyzing tampered or fake images, such as the availability of ground truth data, limited accuracy, limited scope, and the computational complexity of some techniques..**

Keywords - Digital image forensics, image authentication, copy- move tampering, image splicing, fake image detection.

I. INTRODUCTION

Since the first Digital photograph was taken by Steven Sasson, a kodak engineer in 1975, the world has experienced a technological transformation that has remarkably changed how images are shared, created, and perceived. A digital imaging, which uses electronic sensors to record and store images in digital format, has reformed photo, photography, making capturing, storing, and sharing visual data easier.

However, along with this technological advancement has also caused an expansion of concerns about the authenticity and reliability of digital images, as they are highly vulnerable to manipulations.

A digital image manipulation ranges from simple adjustments like brightness and contrast to complex changes or alterations such as cloning, splicing, or even using advanced deep-learning techniques to generate highly realistic fake images. where there are so many powerful software used for editing are easily accessible to user, and allows images to be manipulated in ways which have been raised critical concerns about the authenticity of digital images, emphasizing the need for dependable methods to systematically evaluate their authenticity.

In recent years advancements of machine learning and artificial intelligence has further complicated the images of digital image manipulation. Deep learning-based techniques, such as generative adversarial network made the creation of hyper-realistic fake images that are challenging to detect using traditional methods, where these advancements have made it more difficult to differentiate between authentic and manipulated images, highlights the urgent need for more sophisticated image forensic techniques.

Image forensics is a branch of digital Forensics focused on the identification and verification of image authenticity. It includes the analysis of digital images to determine their source and to detect any modifications made after capture. Its important in contexts where digital images are used as evidence, such as social media, journalism, legal proceedings, and other domain where integrity of image plays important role.

Digital image forensic addresses two primary questions:

A. Where does the image originate ?

B. Has the image been altered since its capture ?

By examining characteristics such as image metadata, lighting inconsistencies, and noise patterns, image forensics aims to detect tampering and restore trust in digital images. This could be done by two approaches:

- Active (non- blind) forensics, which relies on pre-embedded watermarks or signature.
- passive (Blind) Forensics which detects modifications without any prior information.

The increasing penetration of digital image manipulation poses outstanding challenges for information security, social trust, legal evidence integrity. This paper explores the evolving landscape of digital image forgery and detection techniques that combine traditional forensic methods with advanced machine learning algorithms. This paper also says about limitations of current methods and the ongoing development of more robust solutions. This research aims to contribute to the fight against digital misinformation and ensure the ethical use of visual media.

II. LITERATURE SERVEY

Recent studies have shown that machine learning techniques, particularly transfer learning with AlexNet andg convolutional neural networks (CNNs), can effectively detect fake images on social media platforms by accurately classifying anomalous content. One approach to enhance the reliability of this detection involves error level analysis (ELA), which examines discrepancies in compression ratios between genuine and altered sections of images. By integrating modified neural networks that identify tampered areas and reconstruct parts of the original image, alongside incorporating image metadata as a supplementary feature, these methods together provide a robust defense against misinformation and malicious content [1][2][3].

In addition, ensemble techniques such as eXtreme Gradient Boosting efficiently solve the problem of unbalanced data, proving the success of deep learning methods [4][5]. Image forgery detection has also been explored using sophisticated hybrid models that combine deep learning with conventional methods to achieve higher accuracy. A model that integrates Convolutional Neural Networks (CNNs) with Recurrent Neural Networks (RNNs) extracts spatial and temporal features efficiently, successfully detecting image and video forgery. This method is specifically strong against identity swaps, trickery editing, and other complicated visual manipulations [6]. Advanced deep learning algorithms are in the making to counteract the growing danger of highly realistic fake images, with advanced neural network architectures planned to efficiently discriminate between authentic and manipulated media. This emphasis on security and integrity is necessary as a result of the growing misuse of realistic deepfake images for harmful intentions. Innovative methods in deepfake detection, such as those utilizing Fisher face Local Binary Pattern Histogram (FF- LBPH) alongside Deep Belief Networks (DBN) and Restricted Boltzmann Machines (RBM), have demonstrated high accuracy in recognizing deepfake faces. These methods are tested on public datasets, demonstrating their efficacy in detecting synthetic images.[7][8].

Various studies combine a dual-branch Convolutional Neural Networks (CNNs) with Error Level Analysis (ELA) and noise residuals for enhanced detection of image tampering. Combining spatially rich model (SRM) features with ELA, these methods deliver higher accuracy than conventional methods, segregating genuine images from manipulated ones [9]. Hybrid methods are critical in the identification of different forms of image forgery, including natural image changes, computer-generated images, spliced images, and copy-move forged images. Hybrid methods utilize sophisticated feature extraction with Extreme Learning Machine (ELM) classifiers to efficiently detect multiple forms of tampering. Hybrid methods improve the detection accuracy of tampered images by combining conventional image processing with deep learning methods. They offer a complete solution by not only identifying the tampered areas but also distinguishing between genuine images and those that are artificially created. This adaptability highlights the efficiency of these techniques in image forensics [10].

Sophisticated deep learning algorithms have been created to identify forged image documents by examining parameters like illumination consistency and inter-channel correlations, applying methods like image recoloring and deep discriminative networks to determine the probability of manipulation, thus outperforming conventional detection techniques in accuracy. In addition, detailed reviews on image forgery detection have provided a clear comparison between traditional approaches and contemporary deep learning methods with their performance judged on standardized sets and benchmarks, offering insightful performance comparison of existing traditional and emerging algorithms. Apart from detection, certain works also focus on recovering tampered images; as an example, one novel scheme combines JPEG compression with edge detection to detect and recover manipulated sections, maintaining integrity of the image during transmission through embedding edge properties before compression and hence providing an effective solution in handling tampered JPEG images [11][12][13].

Image Forgery Detection Based on CNN and Transfer Learning [5]	-Convolutional Neural Network (CNN) -VGG-16 -ResNet50 -Metadata Analysis -Error Level Analysis (ELA)	Proposed a CNN-based approach combined with metadata and ELA analysis to detect image forgery. Achieved high accuracy in distinguishing real and fake images.
Detection of Real and Fake Image Using Deep Learning Algorithm [6]	-GAN -ELA (Error Level Analysis) -Deep Learning -Convolutional Neural Networks (CNN)	Proposed a method to detect real and fake images using ELA and CNN. Implemented an app for image upload and classification using Firebase.
Deep Learning Model for Deep Fake Face	-Fisherface Algorithm -Local Binary Pattern Histogram (LBPH) -Deep Belief Network	Developed a hybrid deep learning model for deep fake detection. Used Fisherface for dimensional reduction

Recognition and Detection [7]	(DBN) -Restricted Boltzmann Machine (RBM)	and DBN with RBM for classification. Achieved improved efficiency and accuracy in fake face detection.
A Detailed Analysis of Image and Video Forgery Detection Techniques[8]	-Deep Learning -Traditional Keypoint & Block-based Methods	Found that deep learning-based methods outperform traditional approaches in accuracy but require large datasets and computational power. Highlighted the need for generalized forgery detection techniques
Detection of Image Tampering Using Deep Learning, Error Levels, and Noise Residuals [9]	- Deep learning (CNN) - Error Level Analysis (ELA) - Spatial Rich Model (SRM) - CASIA dataset	Proposed a dual-branch CNN for tampering detection.Achieved 98.55% accuracy. Combined traditional techniques with deep learning for better detection.
A Hybrid Technique to Discriminate Natural Images, Computer Generated Graphics, Spliced, Copy-Move Tampered Images, and Authentic Images Using Features and ELM Classifier [10]	- Laplacian of Gaussian - Autocorrelation - Extreme Learning Machine (ELM) classifier - Grey-Level Co-occurrence Matrix (GLCM)	Detects CGI vs. Natural images and image forgery (splicing, copy- move). Robust against post-processing operations like blurring and compression. Achieved high detection accuracy across multiple tampering types.
Fake Image Document Detection via a Deep Discriminate Model [11]	- Deep learning model - Inter-channel correlation analysis - Illumination consistency check	Detects image recoloring and tampering. Uses a feature fusion network to refine classification. Designed to differentiate recolored images from natural ones.
Detection and Restoration of Tampered JPEG Compressed Images [12]	-JPEG compression -Edge Detection -Interpolation	Detects tampered images and reconstructs altered areas using embedded edge data.

Several techniques utilize robust information-hiding schemes to protect tampered cover images by encoding secret data into binary formats through vector quantization, which preserves image quality and enables the recovery of hidden information even after tampering, thus demonstrating resilience against various attacks. Additionally, watermarking frameworks have been developed for the authentication and self-recovery of tampered color images, employing XOR operations for authentication watermarks and half-toning strategies for recovery watermarks, leading to high-quality watermarking and effective image reconstruction compared to other methods [14][15].

A. Literature review

Name of the paper	Tools Used	Findings
Detecting Fake Images on Social Media using Machine Learning [1]	-Convolutional Neural Network (CNN) -Alexnet -Transfer Learning, - MATLAB (Deep Learning Toolbox)	The proposed Alexnet network achieved 97% accuracy in detecting fake images, outperforming Classic CNN and Alexnet with Transfer Learning. This method is effective for monitoring and tracking social media content, helping to detect fraud and protect against electronic attacks.
Tampered and Computer-Generated Face Images Identification Based on Deep Learning [2]	-Convolutional Neural Network (CNN) -eXtreme Gradient Boosting (XGBoost) -Cost-Sensitive Learning	Proposed a deep learning-based framework to detect manipulated facial images and GAN-generated images. Achieved better performance in detecting tampered images under imbalanced dataset scenarios.
Deep Fake Image Detection Based on Pairwise Learning [3]	-Generative Adversarial Networks (GANs) -DenseNet -Contrastive Loss -Pairwise Learning	Developed a novel Common Fake Feature Network (CFFN) that improves fake image detection by leveraging pairwise learning, achieving superior performance over existing deepfake detection methods
Fake Image Detection Using Machine Learning [4]	-Error Level Analysis (ELA) -Convolutional Neural -Network (CNN) -Transfer Learning (AlexNet, VGG16)	Developed an image forensics program to detect fake images. The model achieved high accuracy in identifying tampered images by analyzing compression ratios and metadata.
A Robust Information Hiding Scheme for Tampered Cover Images [13]	-Vector Quantization (VQ) -Watermarking	Recovers hidden secret information even if the cover image is tampered with, ensuring data integrity.
Comprehensive Analyses of Image Forgery Detection Methods [14]	-Digital watermarking -Digital signature -Pixel-based forgery detection -Deep learning-based methods -Camera artifact analysis	Evaluates various image forgery detection techniques, highlighting strengths and weaknesses, and discusses limitations of deep learning-based approaches.
Watermarking Framework for Authentication and Self-Recovery of Tampered Colour Images [15]	LU Decomposition, XOR operations, Half-toning technique, Arnold Sampling, LSB renumbering, GLCM feature extraction, Peak Signal-to-Noise Ratio (PSNR) evaluation	The proposed framework detects and recovers tampered images using watermarking techniques. It improves security in digital image authentication and achieves high PSNR values, ensuring effective image reconstruction.

be copied from one portion of a photo and pasted onto another portion of the same shot to give the impression that there are two people in the image.

3. **SPLICING-** This form of image manipulation entails the creating a single image by combining two or more photographs. An example of a spliced image is when two images of separate individuals are combined to give the impression that they are in the same place.

Tampered images can be created through various techniques that manipulate visual content. Forge images are formed by using editing software to copy and paste sections of an image

this could be done by tool like "stamp" tool. A tool "lasso" is another tool used for splicing that may be aligning or blending two images. "Dodge" and "Burn" used for lightening or darkening the selected parts of image. image scan also be altered through cropping, color correction, and splicing by adobe photoshop. Additionally, stolen or reused images may be used without consent or credit.

Table.1. Literature review *(Table.1. is of Literature review speaks about tools used and findings of research.)*

III. METHODOLOGY & IMPLEMENTATION

Tampered and fake images are manipulated visuals designed may mislead viewers, impacting public perception and the spread of misinformation. Where it may Various forms of alteration, such as editing expressions or adding elements, complicate the integrity of images. Analysis of these images is essential to identify false information and maintain credibility in law enforcement or media which give critical evidence in legal cases. By exposing this manipulation we can preserve trust in media, promote accuracy, and foster informed decision- making in society.

Now let's understand the various types of tampered and fake images. This overview explores manipulation techniques, their purpose, and detection methods to discern authenticity:

A. Types Of Tampered Images

1. Retouching- A picture is manipulated to alter its appearance by the process of retouching. It can be accomplished by changing an image's brightness or contrast, removing or adding objects, or reorienting an image's colour. For example, a retouched photo may involve photo editing to soften an individual's skin or eliminate spots.
2. Cloning - It is also referred to as Copy-Move Forgery. In an effort to conceal or replicate an object, this type of image alteration involves copying and pasting part of one picture on another section of the same picture. For example, in a copy-move forgery, a person's face may

B. Types Of Fake Images

There are three types of fake images

1. Synthetic Images: Entirely made-up pictures not depicting real events, created using deep learning algorithms or digital methods. Examples include illustrations and computer-generated imagery.
2. Manipulative Images: These can be either real or altered but are presented misleadingly. Examples are propaganda images, political ads, or selectively edited news photos. This category includes "photo-bombed" images, where objects or people are added to the original scene.
3. Deep Fakes: Realistic images generated by deep-learning algorithms that depict events or actions that never happened. Images of individuals appearing to do or say things they never actually did, as well as pictures of objects appearing to be in different places than they actually.

Forge images are created by using software like Adobe illustrator or blender, artificial visuals, with CGI techniques involves 3D design and rendering. Deep learning algorithms can generate realistic synthetic images. Where photoshop used for manipulating images , this may change colours, add or remove objects, and use techniques may misled viewers. Elements can added while capturing by photo-bombed. At last Deep fakes leverage generative adversarial network (GANs) to produce synthetic images or videos by learning from exiting content.

C. Detection Techniques

- Forensic analysis: Forensic analysis is the process of carefully examining a picture using specialised software tools like FTK or Autopsy. This entails binary analysis of the picture, detection of any detecting any irregularities in the picture data and any indications of tampering or fabrication.
- Clone detection: Finding regions of an image that have been copied or duplicated is known as "clone detection." Software instruments like Adobe Photoshop, ImageJ, or Tungsten can be used for this.
- Error level analysis: Error level analysis is a technique that analyzes the compression ratios of different regions of an image to identify possible editing mistakes.the compression levels of different parts of an image, as altering the compression level of an element of an image might.
- Pixel analysis: Pixel-by-pixel examination of a photograph for inconsistencies is "pixel analysis." For example, if two distinct photographs were taken and spliced together to form a single image, there could be patterns in the pixels of the two parts that are noticeably different.
- Metadata analysis: Metadata analysis refers to the examination of information about an image file, including when and when it was photographed, with which camera or device it was taken, and under which settings it was taken.

D. Popular Tools for Image Analysis

- adobe Photoshop: Adobe Photoshop is a program for altering photos that is used to check them for alterations or fabrications. It provides a number of tools that can track down changes to a picture's metadata, spot irregularities in the color, texture, or other aspects.
- Forensic Toolkit (FTK): Forensic Toolkit (FTK) is a digital forensics tool used to examine pictures for indications of tampering or forgery. Used for picture analysis, including the capacity to examine image metadata, find areas that have been cloned or spliced, and spot discrepancies in color, texture, or lighting.
- ExifTool: command-line-tool for extracting and examining image information. It gives important details about a photograph, like the date and time it was shot, the camera used to capture.
- Image Forensics Tool (IFT): Image Forensics utility (IFT) is an open-source software utility used to examine images for signs of tampering or fakery. It also helps to capture the image and any editing software used to change it.
- Error Level Analysis (ELA): Detecting image compression levels and locating regions of an image that have been edited or altered can both be done using the software tool

NFSU JOURNAL OF CYBER SECURITY & DIGITAL FORENSICS

NFSU – Journal of Cyber Security and Digital Forensics
Volume –3, Issue – 2, December 2024
E – ISSN – 2583-7559

known as error level analysis (ELA).

I. IMPLEMENTATION

Fotoforensic and forensic beta are tools used in digital image forensics for analyze and detect tampered or fake images.

A. Fornsically Beta

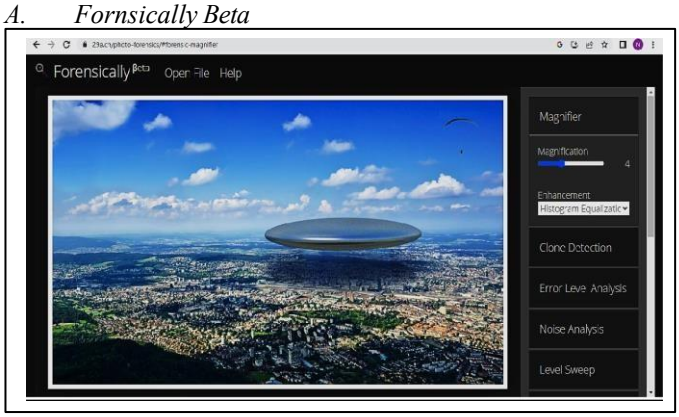
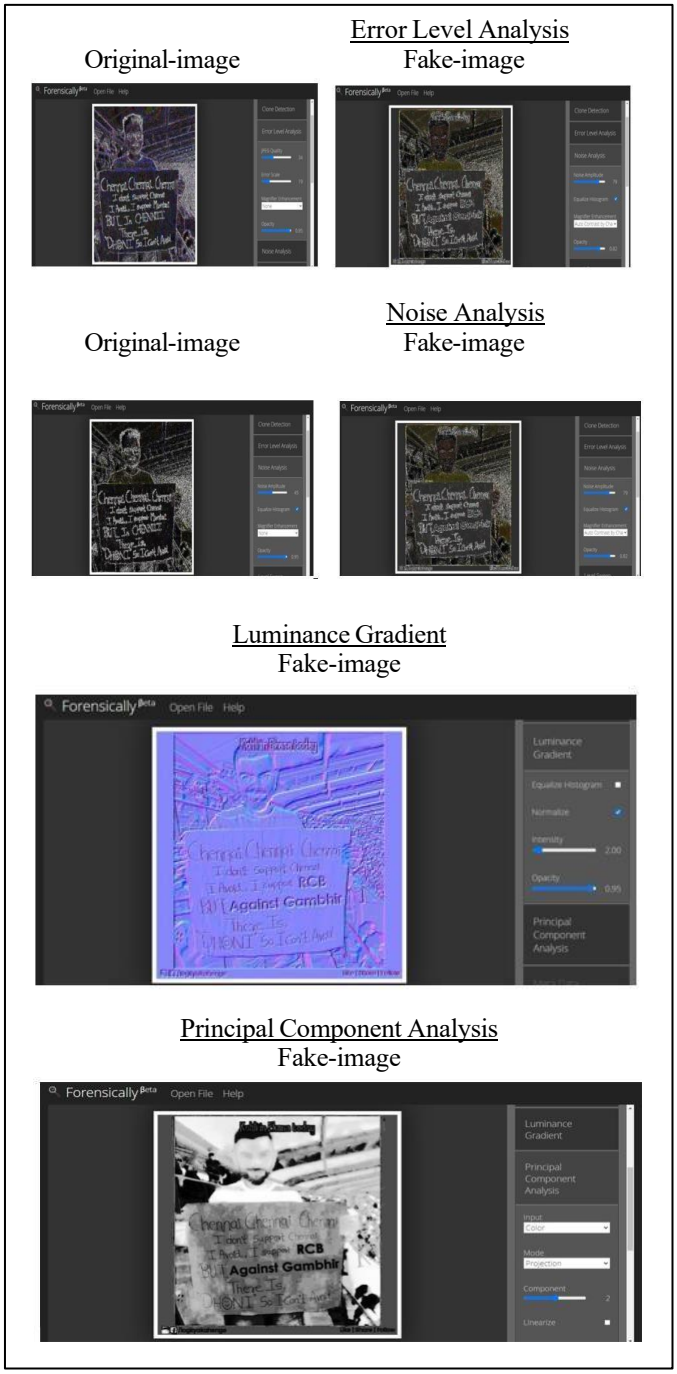


Fig.1. Forensic Beta Interface *(Fig.1.represents the user interface of forensic Beta, a digital image forensic tool used for detecting image manipulation.)*

This tool is a collection of unpaid tools for digital picture forensics. it's functionality like Metadata extraction, error level analysis, and clone identification are just a few of the features. Highlights copied areas in an image using clone detection. The Error level analysis is the process of comparing an image's original and compressed versions. As a result, changed regions may be noticeable in a variety of ways. They could, for instance, be darker or brighter compared to nearby, unaltered locations. The Noise Analysis - This tool essentially functions as a reverse de-noising technique. Instead of simply the noise, the rest of the image is also removed.

B. Fotoforensics

Fig.2. Foto-Forensics Interface *(Fig.2. is the interface of Foto-Forensics, a digital forensic tool used for detecting image tampering)*



This tool utilizes sophisticated algorithms to decode any potential photoshop and modification it makes use of Error Level Analysis (ELA) to locate portions of an image that are compressed at various degrees. With JPEG photos, the level of inaccuracy should be consistent throughout the entire image. If an extensive portion of the image has a different error level, there has likely been a digital alteration.

IV. ANALYSIS OF ORIGINAL AND TAMPERED IMAGE

1) Forensically Beta

I. Sample from social media

NFSU JOURNAL OF CYBER SECURITY & DIGITAL FORENSICS

NFSU – Journal of Cyber Security and Digital Forensics
Volume –3, Issue – 2, December 2024
E – ISSN – 2583-7559

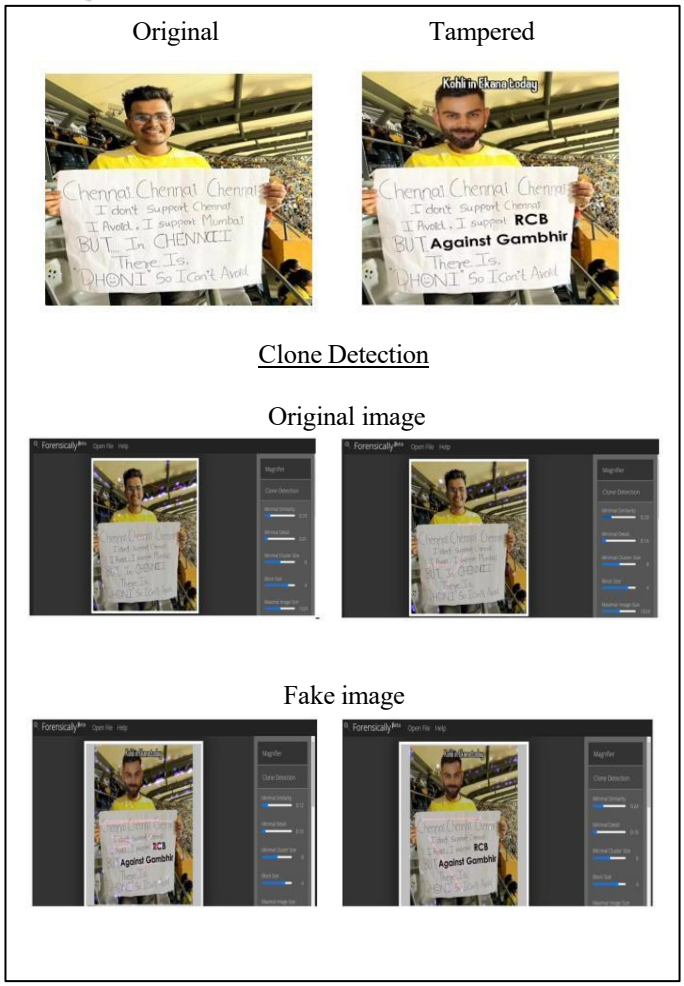
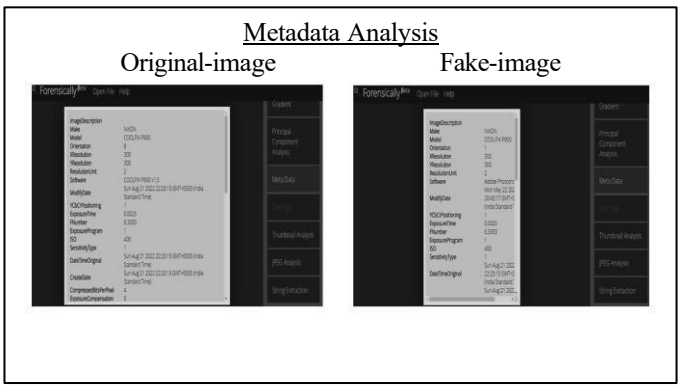


Fig.3. Analysis of Social Media Image Using Forensic Beta
(Fig.3. is the forensic analysis of a sample image sourced from social media using Forensic Beta)



II. Sample from what's-app

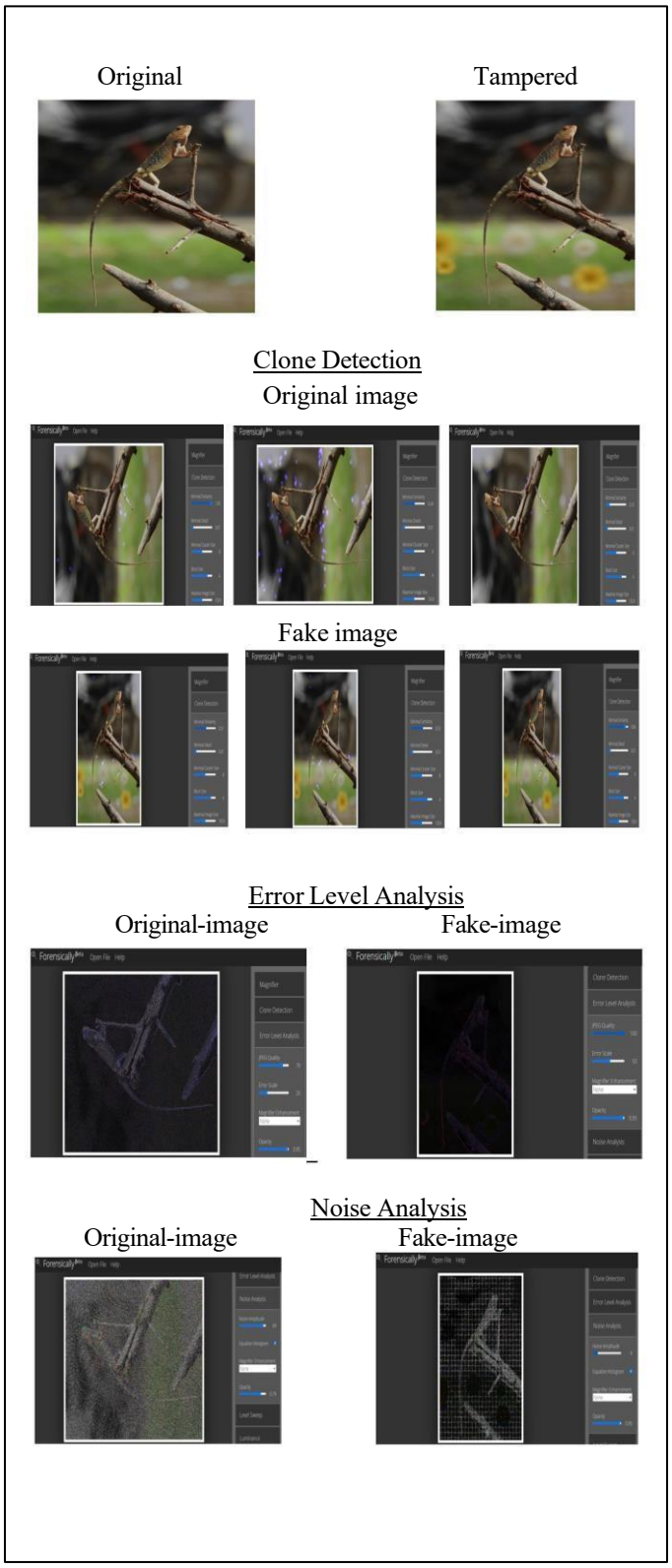


Fig.4. Analysis of WhatsApp Image Using Forensic Beta
(Fig.4. is the forensic examination of a sample image received via WhatsApp using Forensic Beta.)

III.
ample from camera/ phone

Original

Tampered

Clone Detection

Original image

Fake image

Error Level Analysis

Original-image

Fake-image

Noise Analysis

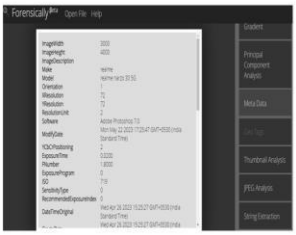
Original-image

Fake-image

Metadata Analysis

Original-image

Fake-image



NFSU JOURNAL OF CYBER SECURITY & DIGITAL FORENSICS

NFSU – Journal of Cyber Security and Digital Forensics
Volume –3, Issue – 2, December 2024
E – ISSN – 2583-7559

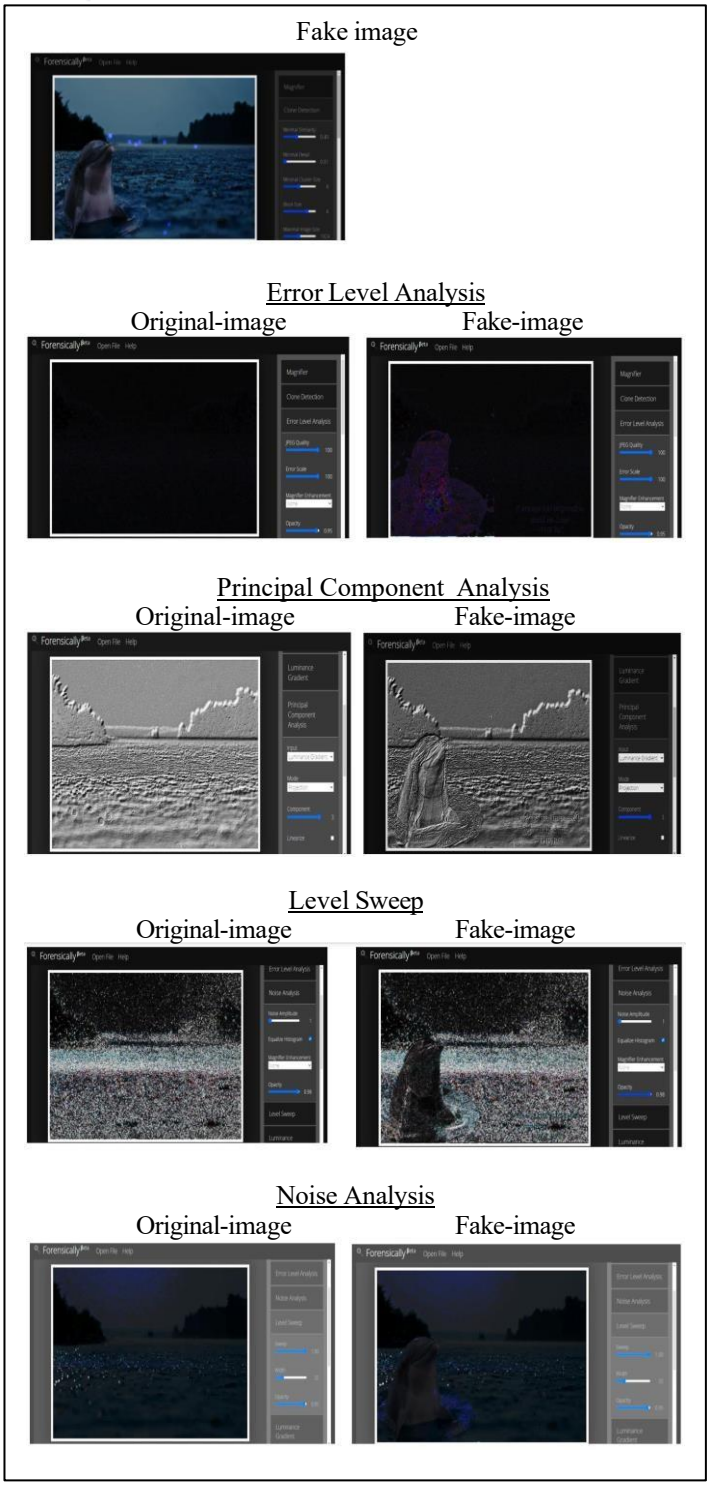


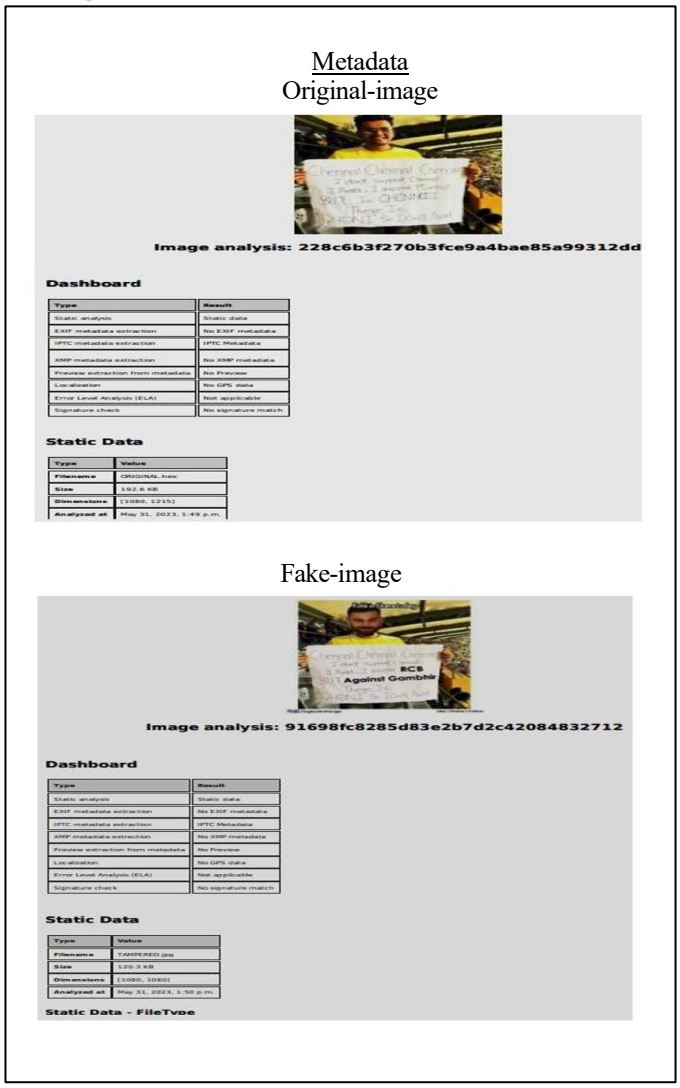
Fig.5.Analysis of Camera-Captured Image Using Forensic Beta *(Fig.5. is analysis of an image taken directly from a phone camera using Forensic Beta.)*

IV. Sample from normal Image

Fig.6.Analysis of a Sample Image *(Fig.6. i s analysis of a sample image using Forensic Beta)*

NFSU JOURNAL OF CYBER SECURITY & DIGITAL FORENSICS

NFSU – Journal of Cyber Security and Digital Forensics
Volume –3, Issue – 2, December 2024
E – ISSN – 2583-7559



2) Foto forensics

I. Sample from social media

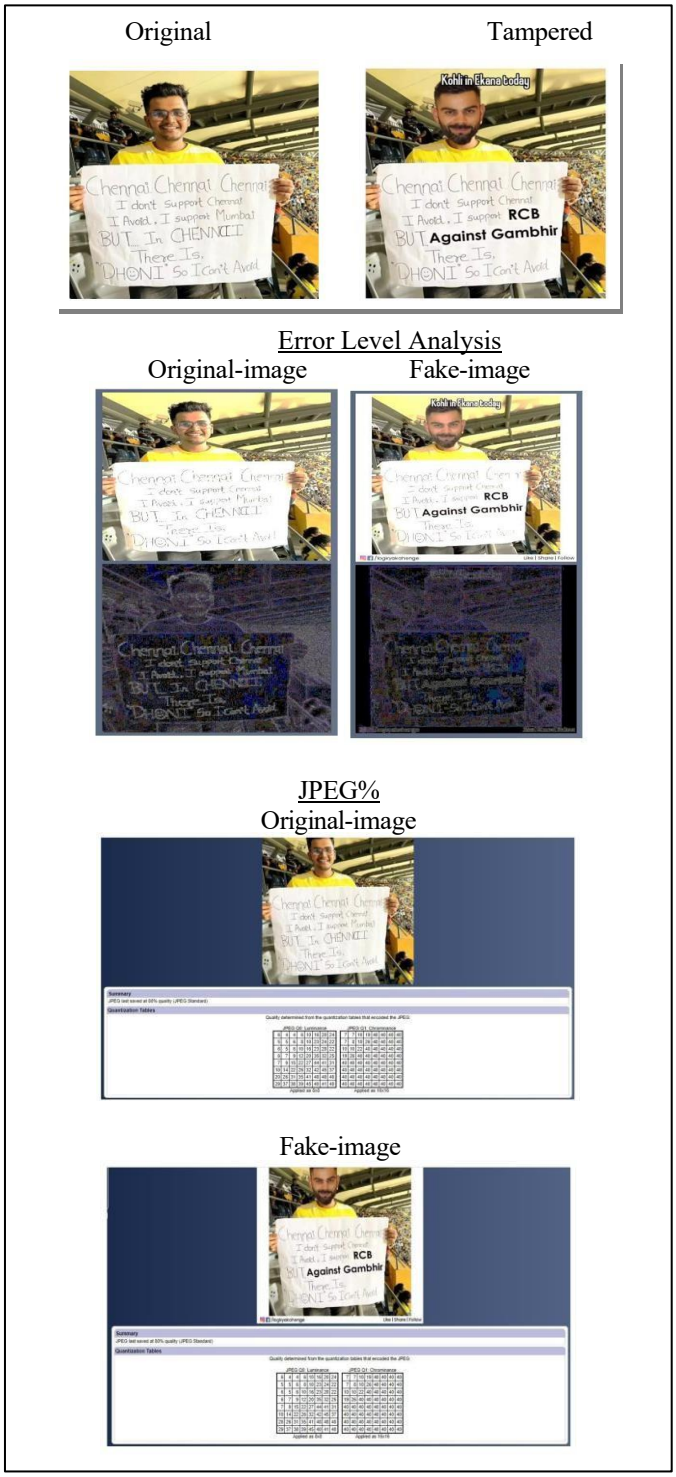
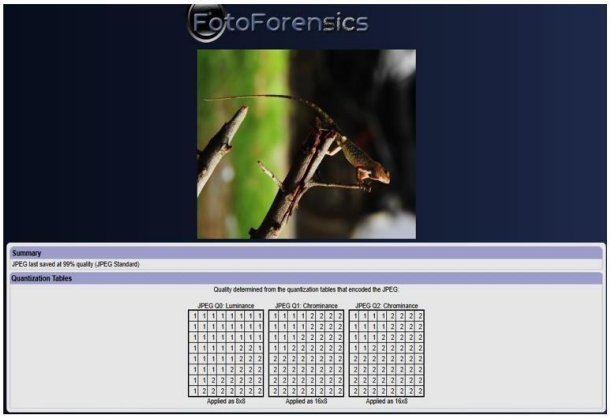


Fig.7.Analysis of Social-Media Image Using Foto-Forensics

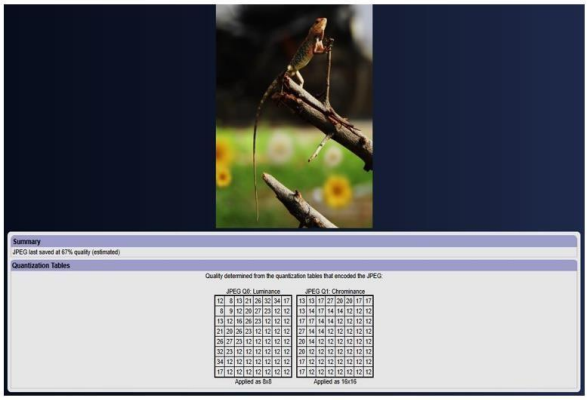
(Fig.7. is an analysis of a social media image using Foto-Forensics.)

JPEG%

Original-image

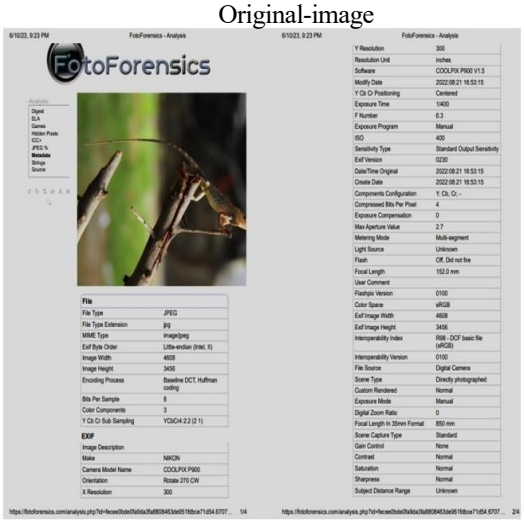


Fake-image



Metadata

Original-image



II. Sample from what's-app

Original

Tampered

Error Level Analysis

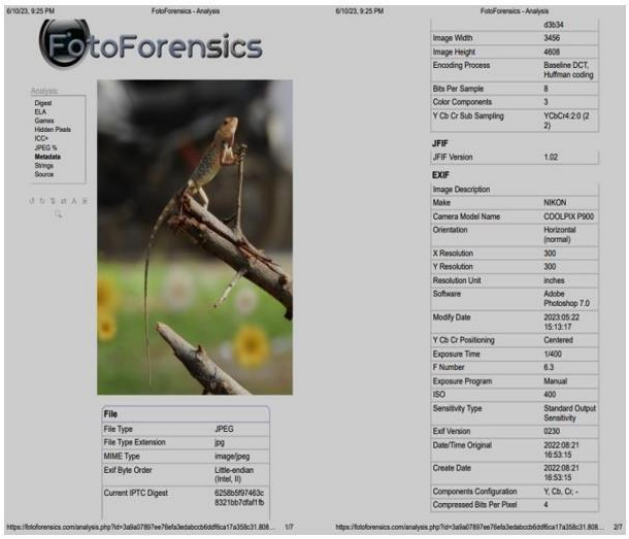
Original-image

Fake-image

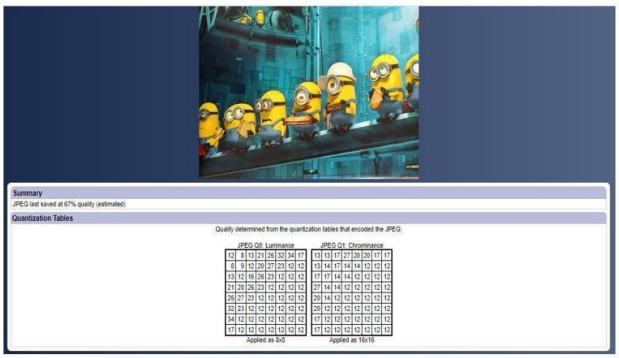
NFSU JOURNAL OF CYBER SECURITY & DIGITAL FORENSICS

NFSU – Journal of Cyber Security and Digital Forensics
Volume –3, Issue – 2, December 2024
E – ISSN – 2583-7559

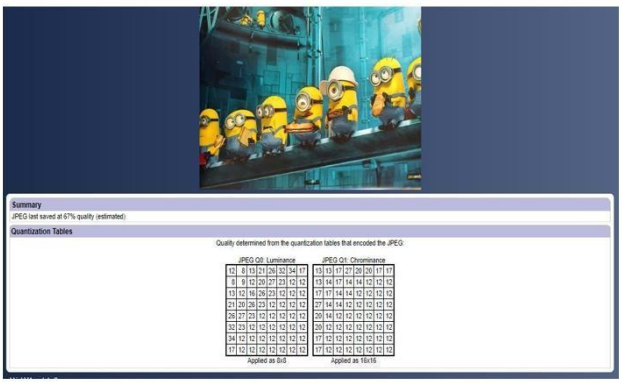
Fake-image



JPEG%
Original-image



Fake-image



Metadata
Original-image

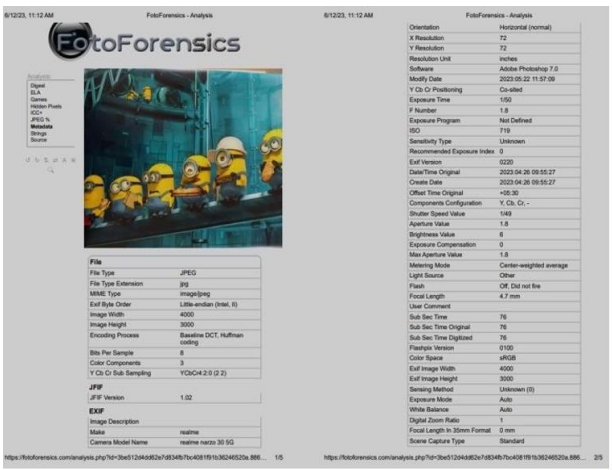


Fig.8.Analysis of WhatsApp Image Using Foto-Forensics
(Fig.8. is an analysis of a WhatsApp image using Foto-Forensics.)

NFSU JOURNAL OF CYBER SECURITY & DIGITAL FORENSICS

NFSU – Journal of Cyber Security and Digital Forensics
Volume –3, Issue – 2, December 2024
E – ISSN – 2583-7559

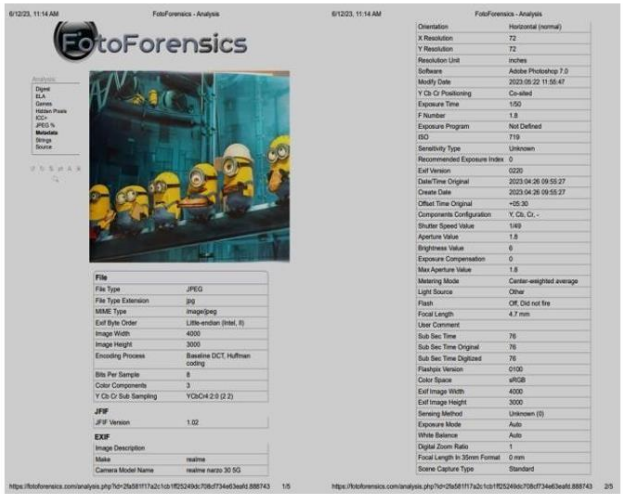
V. SAMPLE FROM CAMERA/ PHONE

Original Tampered

Error Level Analysis

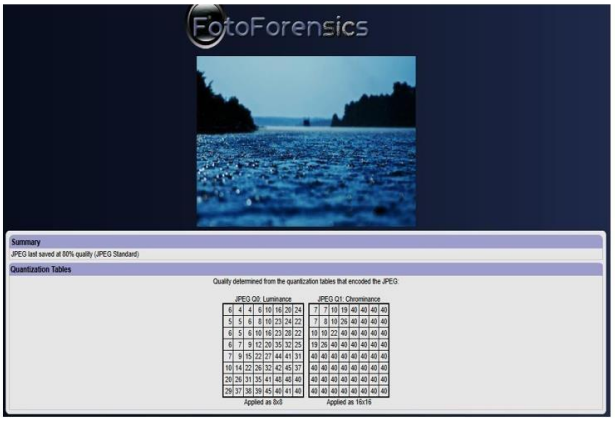
Original-image Fake-image

Fake-image



JPEG%

Original-image



Fake-image

Metadata

Original-image

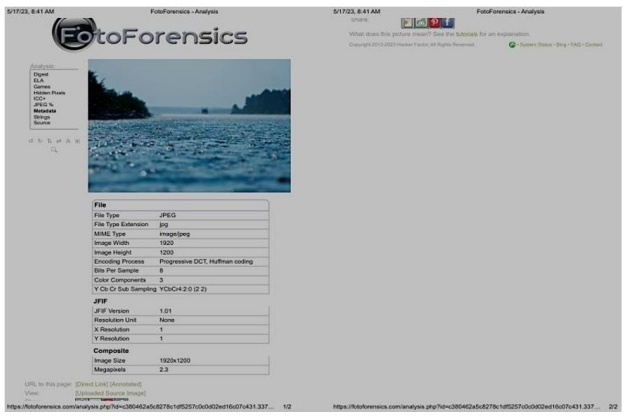


Fig.9. Analysis of Camera-Captured Image Using Foto-Forensics *(Fig.9. is analysis of a phone-captured image using Foto-Forensics.)*

NFSU JOURNAL OF CYBER SECURITY & DIGITAL FORENSICS

NFSU – Journal of Cyber Security and Digital Forensics
Volume –3, Issue – 2, December 2024
E – ISSN – 2583-7559

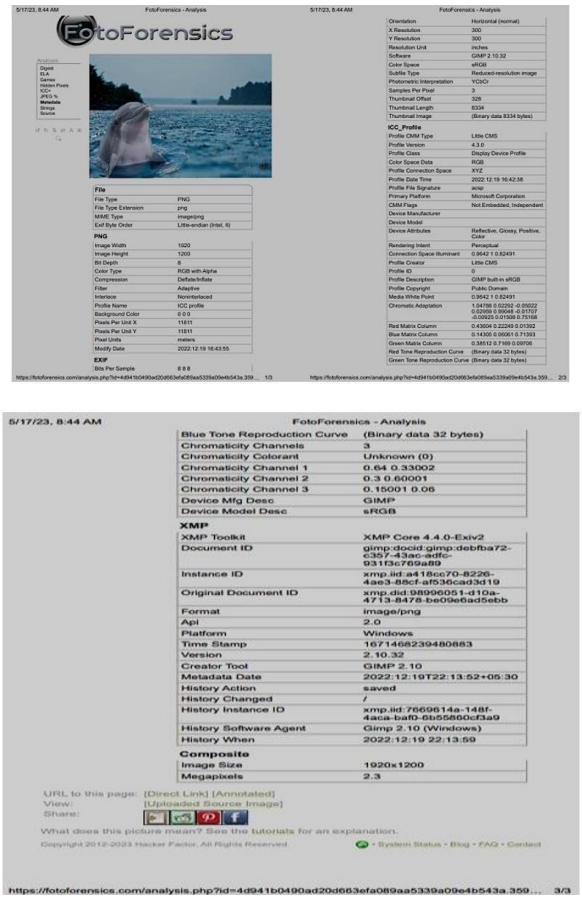
VI. SAMPLE FROM NORMAL IMAGE

Original Tampered

Error Level Analysis

Original-image Fake-image

Fake-image



A.
BSERVATION TABLE : Forensically Beta

Features	Sample from Social Media	Sample from What's app	Sample from Phone or Camera	Normal sample
Clone detection	Yes	No	No	No
Error level analysis (ELA)	Yes	No	Yes	Yes
Noise analysis	Yes	No	Yes	Yes
Luminance gradient	Yes	No	No	Yes
Principal Component Analysis	Yes	No	No	Yes
Metadata Analysis	No	Yes	Yes	No

Table.2. Observation Table: Forensically Beta *(Table.2. observation table for forensically beta which have types feature or the examination and with different samples)*

Fig.10.Analysis of a Sample Image *(Fig.10. is analysis of a sample image using Foto forensics)*

VII. OBSERVATION AND RESULTS

Forensic beta and Foto-forensics are two tools used for the analysis of image tampering by using ELA, noise analysis, and metadata inspection. Where forensic beta detects compression inconsistencies, while Foto-forensic highlights Unnatural peaks of a histogram, both tools identified edited regions, confirming manipulation, here the table will Summarize the findings,

A tool forensically Beta was used to analyzing a image's from different sources, like social media, WhatsApp, and cameras. This tool gives insights into various feature such as clone detection, error level analysis, noise analysis, luminance gradient, principal component analysis and metadata analysis. here are some findings,

- Clone detection was effective for images of samples of social media, it identifying duplicated regions.
- Error level analysis and noise analysis working to all kinds of samples but not for what's-app sample.
- Luminance gradient and PCA was very help full for a detection of inconsistencies in camera or mobile but not in what's-app samples.
- Metadata analysis was effective for a mobile, camera, and what's-app also but unavailable for social media samples.

B. OBSERVATION TABLE: FOTO- FORENSICS

Features	Sample from Social Media	Sample from What's app	Samplefrom Phone or Camera	Normal sample
Error level analysis	No	No	Yes	Yes
JPEG%	No	Yes	No	Yes
Metadata analysis	No	Yes	Yes	Yes

Table.3. Observation Table: Foto-forensics *(Table.3. observation table Foto-Forensic which have types feature or the examination and with different samples.)*

A Foto-Forensics was used to analyzing a image's from different sources, like social media, WhatsApp, and camera. This tool gives insights into various feature such as Error level analysis, JPEG quality percentage (JPEG%), and metadata analysis to detect potential tampering. Here are some findings,

- ELA was most effective for mobile or camera images, where due to heavy compression in what's app and social media samples removed critical forensic traces.
- JPEG % analysis worked exclusively for what's app and mobile or camera sample.
- Metadata analysis extracted details from mobile and what's app images but failed for social media images due to meta data stripping by platform.

VIII. LIMITATIONS OF DETECTION TECHNIQUES

The limitations of current detection methods for detecting altered or fake images emphasis the need for more study and advancement in this field. These restrictions include, among others:

Limited accuracy: There is frequently a high rate of false positives and false negatives, and the accuracy of detection methods can differ widely. This may be as a result of the algorithms' limitations, the image's quality, or the sophisticated of the methods used to tamper with or fake the data.

Limited scope: Existing monitoring techniques often only have a restricted area of applicability and may only be able to detect certain types of manipulation or forgery. For example, some will only be capable of detecting changes to image metadata, whereas others will only be able to determine picture pixel tampering.

Limited availability: Most of the detection techniques being used are out of reach to the majority because they require specialized software or hardware. This might lower their applicability in situations where quick and accurate detection of tampering or fraud is a priority.

Lacking training data: Many detection techniques rely on machine learning techniques, which require extensive training data to perform well. But it can be hard to obtain lots of good-quality training data, particularly for rare or advanced types of tampering or forgery.

Limited knowledge: There is still much we do not know about how to produce and identify changed or forged pictures. Additional research is needed to understand the constraints and possible prejudices of existing detection techniques, and the methods underlying those who tamper with or create fake images.

In general, despite notable improvements in the field of fake image and tampering detection, there are numerous issues that need further research and development. We can only hope to be able to effectively curb the propagation of manipulated and counterfeit images by continuously enhancing our understanding and detection mechanisms.

IX. CONCLUSION

Image analysis is a crucial talent in the current digital era. We need to be able to tell what is real from what is fake when attempting to figure out an image's authenticity, comprehend its context and meaning, or use it as evidence.

This paper aims to create a picture forensics program that can detect any type of photo modification using various tools. For Error level analysis (ELA), we can rely on the Forensically Beta tool and Foto-forensics tool. Foto-forensics tool is quite good with Clone Detection. For Metadata Analysis, we can rely on Foto-forensics but not on the Forensically Beta tool. Level Sweep and Principal Component Analysis don't work well in the Forensically Beta tool.

To visualize the difference between the metadata of the tampered and original image, we need to check the file size, dimension, quality and compression view of the tampered image. The suggested methods were able to recognize the changed picture while also displaying the specific position of the adjustments.

We can get better at analysing pictures and avoiding the effects of false information by employing these methods like image comparison between various tools and metadata analysis.

X. REFERENCES

[1] AlShariah, N. M., & Khader, A. (2019). Detecting Fake Images on Social Media using Machine Learning. International Journal of Advanced Computer Science and Applications, 10(12). https://doi.org/10.14569/ijacsa.2019.0101224

[2] Lavanya, P., Jagruthi, B., Srinidhi, M., Mallesh, P., & Sreyas Institute of Engineering and Technology. (2020). IMAGE FORGERY DETECTION. In Juni Khyat (Vol. 10, Issue 5, p. 12) [Journal-article]. https://www.junikhyat.com

[3] Kishore, V. & Vaibhav Kishore. (2022). FAKE IMAGE DETECTION USING MACHINE LEARNING (By University Grants Commission, Integral University, Integral University, Integral University, University Grants Commission, Integral University, Dr. Faiyaz Ahmad, Mrs. Kavita Agrawal, Dr. Faiyaz Ahmad, Mrs. Kavita Agrawal, Dr. Mohammad Suaib, Dr. Mohammad Suaib, Dr. Faiyaz Ahmad, & Dr. Faiyaz Ahmad).

[4] Dang, L. M., Min, K., Lee, S., Han, D., & Moon, H. (2020). Tampered and Computer-Generated Face Images Identification Based on Deep Learning. Applied Sciences, 10(2), 505. https://doi.org/10.3390/app10020505

[5] Hsu, C., Zhuang, Y., & Lee, C. (2020). Deep fake image detection based on pairwise learning. Applied Sciences, 10(1), 370. https://doi.org/10.3390/app10010370

[6] Tyagi, S., Yadav, D., & The Author(s), under exclusive licence to Springer- Verlag GmbH Germany, part of Springer Nature 2021. (2022). A detailed analysis of image and video forgery detection techniques. In The Visual Computer (Vols. 39–39, pp. 813–833). https://doi.org/10.1007/s00371-021-02347-4

[7] Reddy, C. V., Anusha, H., Dhanush, N., Madhushree, T. P., & Nischay, P. (2021). Detection of real and fake image using deep learning algorithm. International Research Journal of Modernization in Engineering, Technology and Science, 3(7), 367–371. 1628083553.pdf

[8] St, S., Ayoobkhan, M. U. A., Kumar, K., V., Bacanin, N., K, V., Štěpán, H., & Pavel, T. (2022). Deep learning model for deep fake face recognition and detection. PeerJ Computer Science, 8, e881. https://doi.org/10.7717/peerj- cs.881

[9] Chakraborty, S., Chatterjee, K., & Dey, P. (2024). Detection of image tampering using deep learning, error levels and noise residuals. Neural Processing Letters, 56(2). https://doi.org/10.1007/s11063-024-11448

[10] Sharma, S., & Ghanekar, U. (2018). A hybrid technique to discriminate Natural Images, Computer Generated Graphics Images, Spliced, Copy Move tampered images and Authentic images by using features and ELM classifier. Optik, 172, 470–483. https://doi.org/10.1016/j.ijleo.2018.07.021

[11] Anil, M., Shiva, K., Tulasi, Y., Jayasri, G., Teja, B. P., Sai, E. K. M., Sanketika Vidya Parishad Engineering College, & Sanketika Vidya Parishad College of Engineering. (2020). FAKE IMAGE DOCUMENT DETECTION VIA a DEEP DISCRIMINATE MODEL. International Research Journal of Engineering and Technology (IRJET), 07(04), 6391. https://www.irjet.net

[12] Sharma, P., Kumar, M., & Sharma, H. (2022). Comprehensive analyses of image forgery detection methods from traditional to deep learning approaches: an evaluation. Multimedia Tools and Applications, 82(12), 18117–18150. https://doi.org/10.1007/s11042-022-13808-w

[13] Wu, H.-C., Chang, C.-C., & Department of Computer Science and Information Engineering, National Chung Cheng University, Minghsiung, Chiayi 621, Taiwan, ROC. (2002). Detection and restoration of tampered JPEG compressed images. In The Journal of Systems and Software (Vols. 64–64, pp. 151–161). https://www.elsevier.com/locate/jss

[14] Shen, J., & Wang, C. (2014). A robust information hiding scheme for tampered cover images. The Imaging Science Journal, 62(7), 395–401. https://doi.org/10.1179/1743131x14y.0000000080

[15] Balakumar, Britto, & Umadevi. (2022). WATERMARKING FRAMEWORK FOR AUTHENTICATION AND SELF-RECOVERY OF TAMPERED COLOUR IMAGES. International Research Journal of Modernization in Engineering Technology and Science. https://doi.org/10.56726/irjmets32175