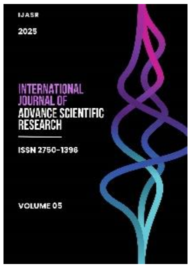
International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 05 ISSUE 03 Pages: 45-52
OCLC – 1368736135



Journal Website: http://sciencebring.com/index.php/ijasr

Research Article

DETECTION AND ANALYSIS OF MULTIMEDIA DATA ALTERATION IN CYBERSECURITY BASED ON MARKOV CHAIN MODEL

Submission Date: January 30, 2025, **Accepted Date:** February 25, 2025,
Published Date: March 21, 2025
Crossref doi: https://doi.org/10.37547/ijasr-05-03-07

Melikuziev Rustambek Shukhrat ogli
Associate Professor of the Department Tashkent University of Applied Sciences, Tashkent University of Humanities, Uzbekistan

Abstract

This article analyzes methods for detecting unauthorized changes in multimedia data based on the Markov chain model and related problems. The article examines the application of the Markov chain model in detecting manipulation of multimedia materials, in particular images and videos. The capabilities of the Markov chain model, in particular, how it works effectively in detecting unauthorized changes in images, the development of its algorithms and how manipulations can be detected using them are analyzed. The article also examines the main difficulties and problems that arise in analyzing multimedia data, the advantages and limitations of tools for fast and efficient analysis of materials of various sizes. This article is mainly aimed at highlighting the application of the Markov chain model in detecting manipulations in multimedia materials and its importance in the field of digital forensics.

Keywords

Markov chain model, multimedia data, unauthorized modification, manipulation detection, digital forensics, image manipulation, video analysis, document analysis, statistical analysis, analysis algorithms, signal analysis, network tools, network communication, cybersecurity, analysis methods, multimedia analysis tools, deepfake technologies, cyber fraud, network security, security assurance, image and video editing, manipulation detection, document preservation, multimedia analysis tools.

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 05 ISSUE 03 Pages: 45-52
OCLC – 1368736135

Introduction

Digital forensics and manipulation of multimedia data have become a serious risk and threat in recent years[1]. The increase in the number of crimes related to image manipulation during the period 2020-2024 shows that the number of crimes related to image manipulation is increasing year by year. This has further increased the need and necessity for this field (Table 1).

Image manipulation is not only a technical issue, but also raises social and legal problems. This type of crime is often associated with violations of personal rights, damage to reputation and even fraud. Altered images, false information and their illegal distribution can lead to an invasion of citizens' privacy, which can cause serious material and moral damage.

Table 1.

The manipulation of multimedia data in the field of digital forensics

Years	Number of crimes related to image manipulation	Number of crimes related to manipulation of mobile devices	Number of crimes related to online fraud
2020	1500	3000	5000
2021	1800	3500	6000
2022	2000	4000	7000
2023	2300	4500	7500
2024	2500	5000	8000

This problem requires the development of digital forensics, especially specialized software tools for detecting and investigating image manipulation. For example, tools such as EnCase Forensic, FTK (Forensic Toolkit), X1 Social Discovery, and PhotoDNA are effective in analyzing digital evidence. Programs such as PhotoDNA are most effective in detecting image manipulation, providing a high level of accuracy in quickly identifying manipulated images.

As the number of crimes increases, so does the economic and social cost [2] . In 2020, image manipulation-related crimes caused an estimated $500,000 in damage, and by 2024, this damage is expected to reach $800,000 (Figure 1). These figures highlight the need for expertise and resources in the field of image manipulation and digital forensics. Therefore, effective countermeasures against digital forensics and multimedia data manipulation, as well as the introduction of advanced technologies in the prevention and investigation of such crimes, are urgent. Forensic analysis methods need to be further developed to reduce threats to data security and privacy.

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 05 ISSUE 03 Pages: 45-52
OCLC – 1368736135

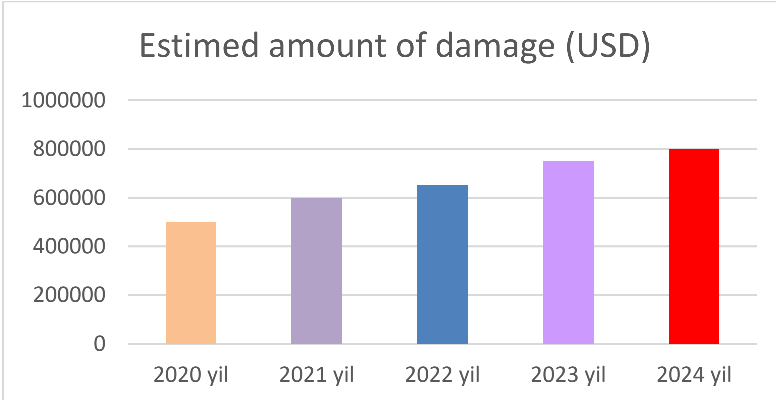
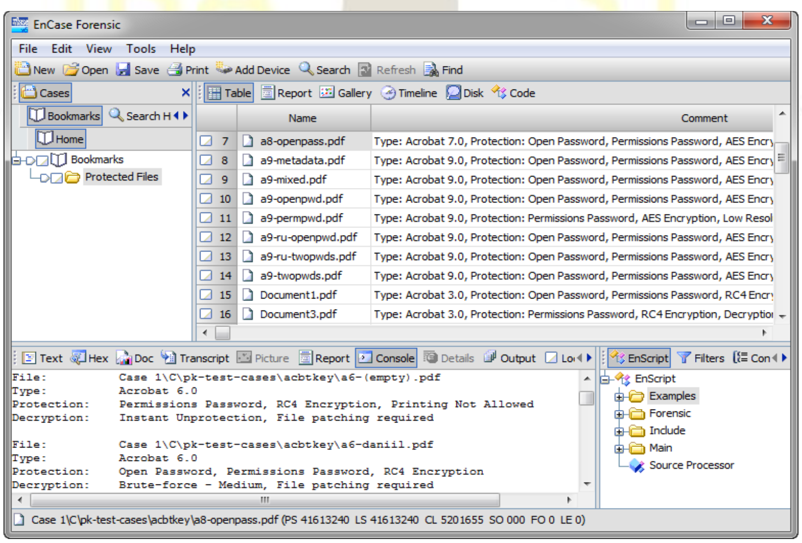


Figure 1. Diagram of the amount of damage caused by crimes committed through the manipulation of multimedia data

In the field of digital forensics, there are several software tools for detecting image manipulation, document analysis, and other forensic analyses based on Markov chain models. The following software tools are widely used in the field of forensics and digital forensics:

1. EnCase Forensic is a very popular and widely used program in digital forensics. It is mainly useful for analyzing digital evidence, recovering files stored on a computer, studying file systems, and analyzing images. EnCase also helps in detecting manipulations, such as changes in file systems, and recovering deleted or hidden files. Another useful feature of EnCase is the ability to automatically analyze documents and images, which helps forensic experts quickly review large amounts of data. This program in the field of digital forensics is an excellent tool for storing documents, analyzing them, and detecting errors (Figure 2).



International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 05 ISSUE 03 Pages: 45-52
OCLC – 1368736135

Figure 2. Multimedia documents and the images analysis in doing applicable EnCase Forensic software of the tool general appearance.

2. FTK (Forensic Toolkit) is another important tool widely used in digital forensic analysis. FTK is mainly effective for analyzing disks, recovering files, and detecting manipulated or hidden data. This program is particularly useful for generating detailed reports on the data being analyzed and for quickly scanning large numbers of files. FTK allows users to recover deleted files, especially data in various formats such as images and documents. It also acts as a powerful tool for detecting changes and manipulations made to files, which plays an important role in forensic investigations. The FTK interface is also intuitive and allows users to quickly analyze data (Figure 3).

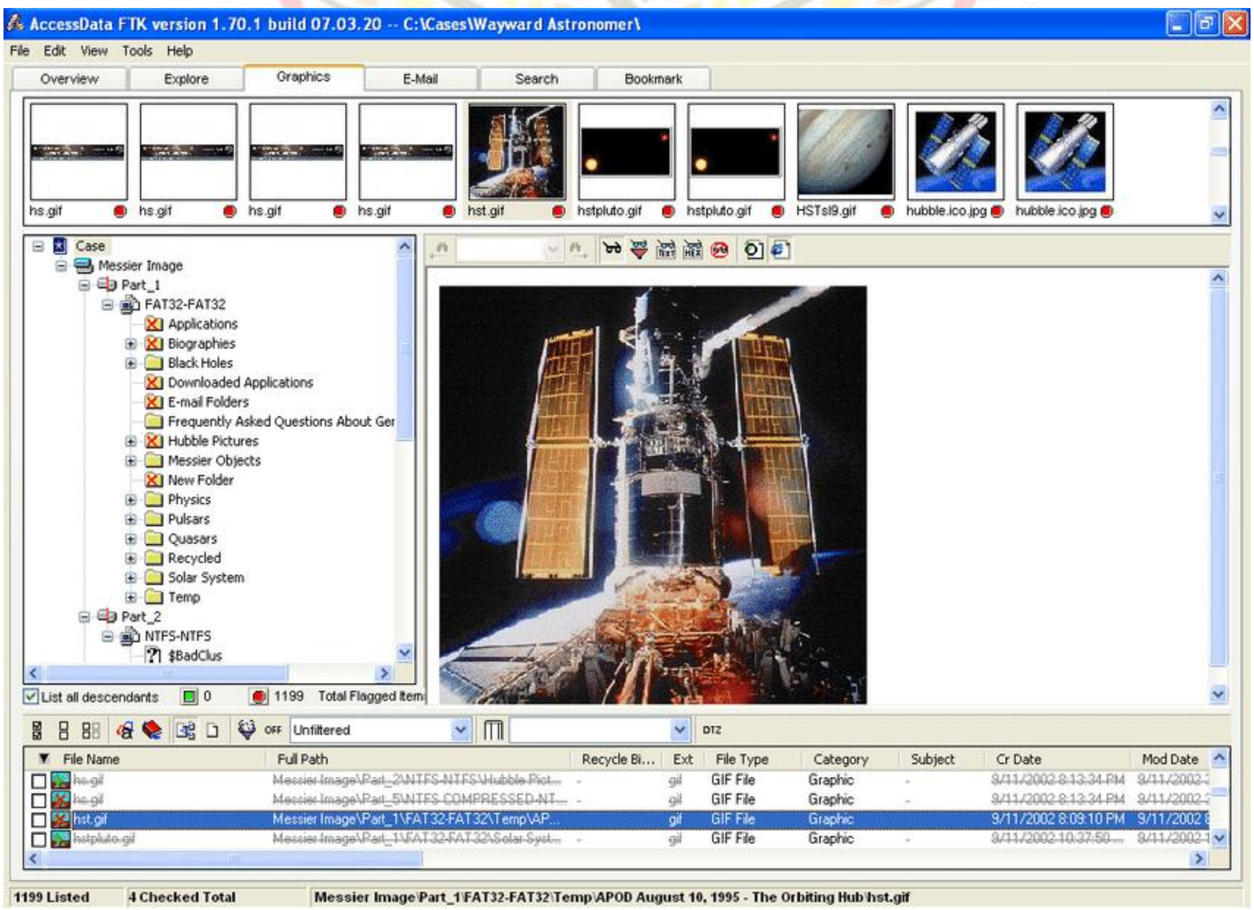


Figure 3. Manipulation made or hidden data determination for applicable FTK (Forensic Toolkit (software) of the tool general appearance .

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 05 ISSUE 03 Pages: 45-52
OCLC – 1368736135
ISSN-2750-1396

3. X1 Social Discovery is a software tool designed to collect and analyze information from social media and web pages. It is also used in forensics, including the study of images and documents. This program allows you to monitor and analyze all activity on social networks, including modified or deleted posts, messages and user profiles. The program is used, in particular, by law enforcement agencies and digital forensics specialists to identify evidence related to actions performed by users and information on social networks. X1 Social Discovery also allows you to quickly and efficiently index files, detect changes, search for messages and posts, and generate reports on the collected data. This program is known for its high efficiency and accurate results in analyzing social networks and online resources (Figure 4).

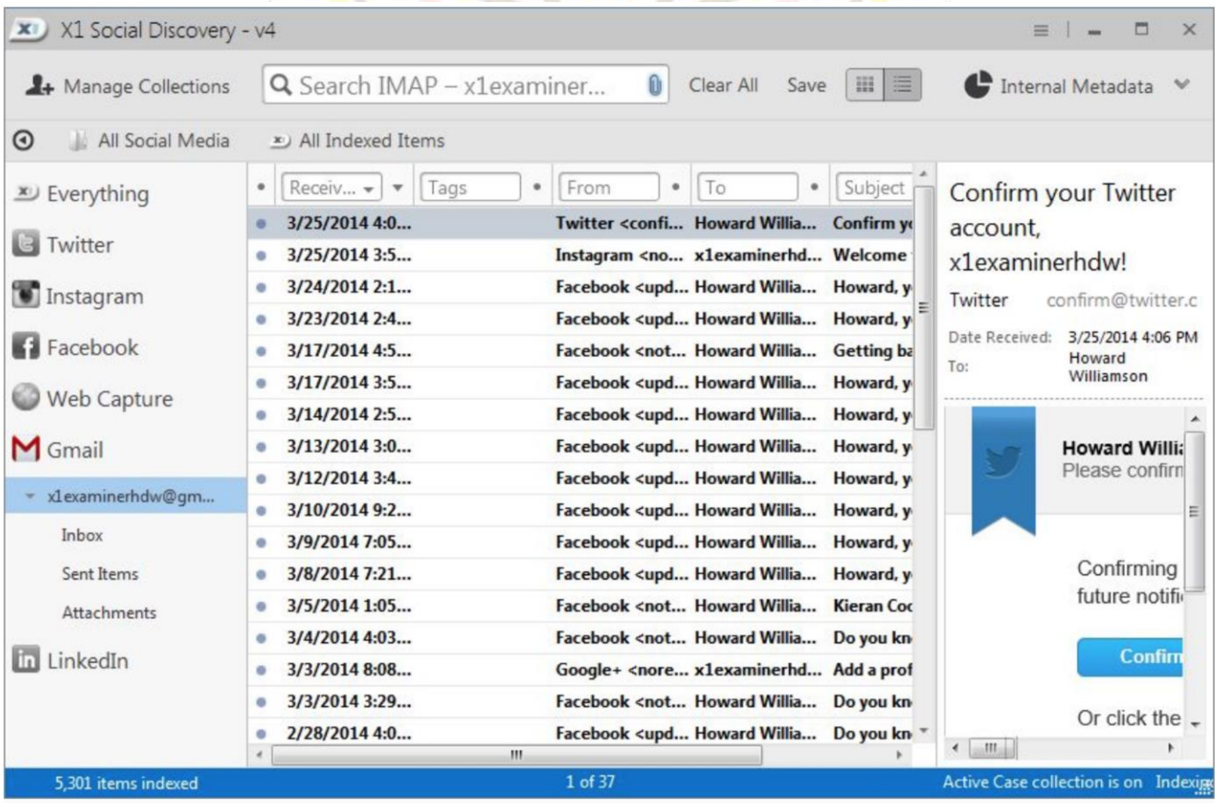


Figure 4. Social networks and online in sources data changes determination for applicable X 1 Social Discovery software of the tool general appearance

4. Cellbrite UFED (Universal Forensic Extraction Device) is a powerful forensic tool widely used in extracting and analyzing data from mobile devices and other digital devices. This program is specifically designed to recover and analyze data from mobile devices (smartphones, tablets, SIM cards, SD cards and other mobile devices). With Cellbrite UFED, you can recover and analyze images, messages, call logs, contacts, geolocation data and various other data stored on phones. It also provides the ability to recover

deleted data, break security locks on devices or access data by breaking passwords (if possible). These features are especially important for law enforcement agencies and digital forensics professionals. Cellbrite UFED provides the ability to extract complete and deep information from mobile devices, which helps to identify not only images and messages, but also other important data stored on devices (Figure 5).

Figure 5. Images , messages and other mobile data in inspection applicable Cellbrite UFED hardware - software of the tool general appearance .

5. PhotoDNA — images identification to do and manipulations determination for working issued special software tool . It initially Microsoft by working issued and currently social networks , police and other the right protection to do offices by is being used . Main purpose child's exploitation or pornography with related crimes identification , as well as images and videos manipulation to do or change circumstances [8] . PhotoDNA the images with a digital " signature " compares . This signature of the image to oneself typical characteristics (e.g. , colors , textures) and shapes) see comes out and every one to the image unique identification number gives . From that then , PhotoDNA this the number global images base with compares and similar the images quickly This determines software tool manipulation made or changed the images in determining also effective is , that is of the image initial identification number changed if the image manipulation that was done shows . This The tool is basically a file . exploitation with related the content determination and such the images distribution or to keep against in the fight is useful [9]. PhotoDNA many online platforms and the right protection to do offices by is used because she is very effective and fast in a way big in size the images scanner and commit violations to determine help Also , PhotoDNA personal data and personal security provides , because she is only images and their with digital

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 05 ISSUE 03 Pages: 45-52
OCLC – 1368736135

" signatures " works , that is original images o ' is not changed or personal to the information damage not delivered (Figure 6).

Figure 6. The working mechanism of the PhotoDNA software tool.

Software tools used in the field of forensics and digital forensics cover a wide range of needs, from detecting image manipulation to extracting information from mobile devices to analyzing documents. These tools are effectively used in crime investigation, examining digital evidence, and detecting manipulated images.

An analysis of the capabilities and effectiveness of the above tools is presented in Table 2[10,11]:

Table 2.

Analysis of multimedia data tampering detection tools based on Markov chain model

Software Tool	Scope of use	Speed	Efficiency
EnCase Forensics	More than 80%	Fast and efficient analysis of 95% of images and files	Detect 90% of manipulated files
FTK (Forensic Toolkit)	80%	Changes are detected at 60% speed	85% detection of file system manipulations
X1 Social Discovery	More than 70%	90% of altered posts on social media are detected	80% of modified social media data recovery
Cellebrite UFED	75%	Identify images and messages from mobile devices at 85% speed	95% deleted data recovery
PhotoDNA	More than 90%	Detecting 95% of manipulated images	98% image identification and manipulation detection

Digital forensics and crimes related to the alteration of multimedia data have increased significantly in recent years. Along with the increase in crimes, the effectiveness of software tools used to detect image manipulation and digital manipulations is also important, and tools such as EnCase Forensic, FTK, PhotoDNA are highly effective in detecting image and document

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 05 ISSUE 03 Pages: 45-52
OCLC – 1368736135

manipulation. These tools not only help in detecting crimes, but also effectively help in combating them.

Conclusion

Since 2020, accurate data on the number of crimes and strategies for combating them has been collected using image manipulation and digital manipulation detection tools. At the same time, the technologies and methodologies used in the field of digital forensics have developed rapidly in recent years, becoming increasingly powerful in analyzing evidence from social networks, mobile devices and other digital sources. This, in turn, provides more effective approaches to combating digital crimes and their consequences.

To prevent and combat cybercrime, it is important to develop innovations in the field of digital forensics and choose the right software tools. There is also an increasing opportunity to identify and prevent recent trends in crimes by analyzing social networks, mobile devices and other digital sources. This will be an important factor in effectively using data and technology, reducing the growth of crimes and combating crime.

References

1. https://www.fbi.govhttps://www.microsoft.com/en-us/security/blog/2020/10/05/photodna-impacting-cyber-crime-and-child-exploitation-with-advanced-technology/).
2. https://www.europol.europa.eu.
3. W. Oppenheim, RW Schafer, "Discrete-Time Signal Processing", Boston, Massachusetts, USA, 2010, ISBN: 978-0131988421, pp. 45-96.
4. W. Oppenheim, RW Schafer, "Discrete-Time Signal Processing", Boston, Massachusetts, 2010, ISBN: 978-0131988421, pp. 33-144.
5. John G. Proakis, Dimitris G. Manolakis, "Digital Signal Processing: Principles, Algorithms, and Applications", India, 2014, ISBN: 978-0133750366, pp. 200–300.
6. Sanjay Sharma, "Digital Signal Processing: Theory and Practice", New Delhi, India, 2014, ISBN: 978-1107067345, pp. 161-218.
7. Saeed V. Vaseghi, S. Xie, Advanced Digital Signal Processing and Noise Reduction, Beijing, China, 2011, ISBN: 978-0470661380, pp. 45-88.
8. Rafael C. Gonzalez, Richard E. Woods, Digital Image Processing, Boston, 2017, ISBN: 978-0133356724, pp. 155-244.
9. Rafael C. Gonzalez, Richard E. Woods, Digital Image Processing, Boston, 2017, ISBN: 978-0133356724, pp. 13-52.
10. Nihad A. Hassan, "Digital Forensics and Cyber Crime", Cham, Germany, 2016, ISBN: 978-3-319-46988-4, pp. 33-42.
11. Eoghan Casey, "Handbook of Digital Forensics and Investigation" Eoghan Casey, Amsterdam, Netherlands, 2011, ISBN: 978-0-12-374266-3, pp. 117-128.