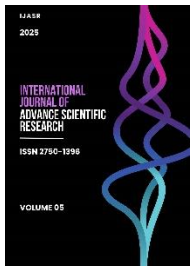
International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 05 ISSUE 03 Pages: 53-60
OCLC – 1368736135



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

Research Article

METHODS OF USING THE CAPABILITIES OF FOURIER TRANSFORM AND STATISTICAL MODELS IN DETECTING UNAUTHORIZED MODIFICATION OF MULTIMEDIA DATA

Submission Date: January 30, 2025, **Accepted Date:** February 25, 2025,
Published Date: March 21, 2025
Crossref doi: https://doi.org/10.37547/ijasr-05-03-08

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

ABSTRACT

This article reviews existing tools for detecting unauthorized modification of multimedia data and their problems. The article analyzes Fourier transform and statistical models as one of the most widely used methods for detecting manipulation in multimedia documents. The process of determining the frequency spectrum of data and its changes using Fourier transform, as well as analyzing images and videos using statistical methods, is shown. The article also provides an analysis of the main problems encountered in analyzing multimedia data, including the large volume of data and tools for improving the efficiency of analysis. Innovative approaches and methods are considered to ensure the efficiency of analysis, which will allow developing more effective and faster methods for detecting unauthorized modification of multimedia materials.

KEYWORDS

Cybersecurity, multimedia data, digital forensics, network tools, innovative solutions, unauthorized modification, signal analysis, fourier transform, frequency spectrum, manipulation detection, deepfake technologies, cyber fraud, pdf documents, network exchange, security assurance, analysis algorithms, Forensic analysis, digital documents, statistical analysis, probability distribution, color distribution, Fourier transform, digital forensics.

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 05 ISSUE 03 Pages: 53-60
OCLC – 1368736135

INTRODUCTION

Today, the development of servers and other network devices used in global or local networks equipped with various hardware and software that enhance the preservation of multimedia data in its original form is one of the main goals of cybersecurity and digital forensics. The field of cybersecurity and digital forensics seeks to ensure that multimedia data is delivered to safe recipients without any changes during the exchange process on the network, and to detect unauthorized changes . In order to ensure the security of multimedia data in global and local networks, countries are developing innovative solutions that allow detecting unauthorized changes to multimedia data .

Scientific research is being conducted in the world to create systems that allow detecting and analyzing unauthorized changes in multimedia data using technical systems, software tools and computer devices. This is leading to measures to detect unauthorized changes in multimedia data using non-traditional methods and to develop new approaches and algorithms. Countries consider it important to create secure networks to ensure the security of multimedia data and prevent unauthorized changes , and to create methods that prevent data from being changed in open networks, as well as algorithms and tools to detect unauthorized changes in multimedia data .

According to the analysis, crimes using video editing and deepfake technologies increased on social media in 2020, unauthorized image editing and cyberfraud as a result of the rise of deepfake technologies in 2021, and crimes involving manipulation of PDF documents and editing images increased in 2022 (Figure 1).

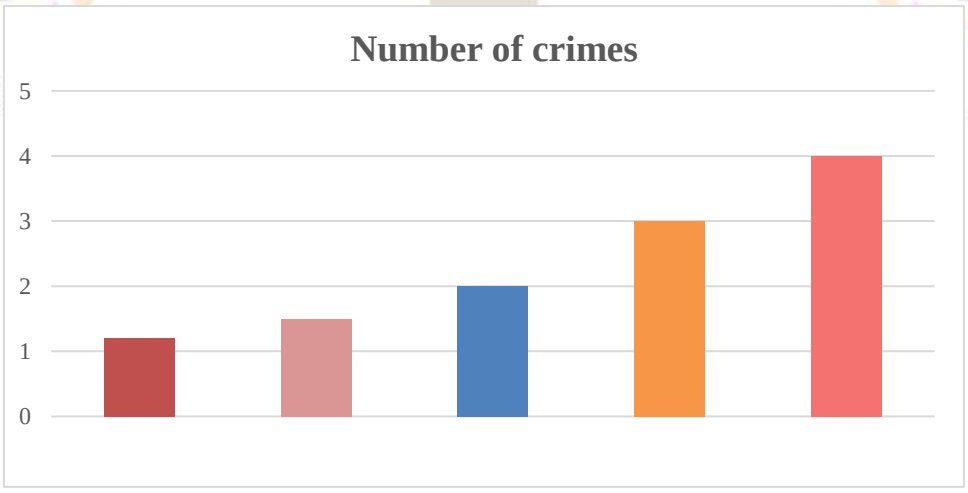


Figure 1. Diagram of the dynamics of the development of cybercrime against multimedia data.

The chart shows that by 2023, the number of cyber frauds and cyber crimes committed via the Internet has increased significantly, mainly related to frauds involving dangerous materials. In 2024, the number of

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 05 ISSUE 03 Pages: 53-60
OCLC – 1368736135

digital crimes continued to grow, including the editing of digital files, images and videos, and the number of cyber attacks.

Multimedia information is a combined and interrelated form of different types of information (text, images, video, audio, etc.). This information is developed and used to include one or more factors, for example, to increase the user's ability to receive information, to better understand the information, or to make a presentation.

Multimedia content is ubiquitous in our daily lives, frequently found on the internet, television programs, mobile applications, and interactive media. It can come in a variety of forms and formats, each with its own unique characteristics.

II. Detection of unauthorized modification of multimedia data based on Fourier transform

The Fourier transform (FT) is mainly used to analyze the frequency content of a signal or image. The Fourier transform allows a signal or image to be transformed from the time or space domain to the frequency domain. This method can be used to detect unauthorized changes, such as manipulation or filtering.

The Fourier transform uses the following formula to convert the signal *x (t) to the frequency domain:*

$$X(f) = \int_{-\infty}^{\infty} x(t) e^{-j2\pi ft} dt \quad (1)$$

Here:

$x(t)$ is the representation of a signal or image in the time (or space) domain,

$X(f)$ is the frequency domain representation of a signal or image,

f is the frequency,

t is time,

j— complex unit ($j = \sqrt{-1}$).

Tamper detection uses Fourier transform to examine the abnormal frequency content of a signal. If the original file has been manipulated, changes will be visible in its frequency spectrum[1].

If an image is manipulated, such as by cropping or adding an additional object, new frequency components may appear in its Fourier transform spectrum. By analyzing these changes, the manipulation can be detected.

If a signal has been manipulated, changes can be observed in its frequency spectrum (i.e., $X(f)$). Abnormal frequency content is mainly understood to mean the following situations:

1. **Appearance of new frequency components** : As a result of unauthorized modifications, new frequency components (new frequencies) can be added to the signal spectrum.
2. **Frequency spectrum change** : The frequency spectrum of a manipulated signal changes. For example, image cropping, splicing, or other manipulation processes leave distinct traces in the spectrum.

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 05 ISSUE 03 Pages: 53-60
OCLC – 1368736135

To check the frequency content of a manipulated signal, the spectrum of the signal is obtained by Fourier transformation and abnormal changes are checked against it. The main steps are as follows:

1. **Converting a signal to the frequency domain using Fourier transform** : Using the Fourier transform to calculate the frequency spectrum of a signal, $X(f)$ is found by expression 2.10.
2. **Spectrum analysis** : The amplitude and phase of each frequency component *f in the spectrum of a signal* are analyzed. Typically, the amplitude spectrum is expressed as $/X(f)/$ because it indicates the strength or energy of the frequency components of the signal.
3. **Frequency spectrum normalization** : By analyzing the normal state of a signal, it is possible to determine the natural distribution of its frequency spectrum. If the signal has been manipulated, abnormal changes will be visible in the normalized spectrum.
4. **Detecting Abnormal Components** : To detect new frequency components that have emerged as a result of signal manipulation, it is necessary to observe unclear or unexpected changes in the spectrum. For example, if a signal has been clipped or a spurious object has been added, new peaks or high-frequency components may appear in the spectrum.
5. **Spectrum analysis using statistical tests** : Statistical methods are also used to detect anomalies in the spectrum. For example, by examining the dispersion or correlation function of the spectrum, it is possible to determine whether a signal has been manipulated.

If the manipulation results in the appearance of new frequency components in the spectrum, this change can be expressed mathematically in the following form. Suppose we have an original unmanipulated signal $x(t)$ and its Fourier transform $X(f)$. We call the manipulated signal $\dot{x}\sim(t)$. Its spectrum after the Fourier transform is:

$$\dot{X}(f)=\int_{-\infty}^{\infty}\dot{x}(t)e^{-j2\pi ft}dt \qquad (2)$$

If $\dot{X}(f)$ and $X(f)$ manipulation , if we compare because of appearance was abnormal frequency composition as follows is defined as :

$$\Delta X(f) = \dot{X}(f) - X(f) \qquad (3)$$

A signal is considered manipulated if the spectrum of Δ X(f) contains unexpected or unknown components. Such components differ from the original frequency content of the signal[3].

The process of checking for abnormal frequency content in a signal using the Fourier transform is based on transforming the signal from the time domain to the frequency domain and analyzing its spectrum. As a result of the manipulation, new frequency components may appear in the spectrum. These changes can be determined by mathematical calculations, for example, *X(f) and* Using the comparison of $\dot{X}(f)$.

The Discrete Fourier Transform (DFT) is used in the analysis of digital signals and images. The DFT is essentially a digital version of the transformation of a signal from the time or space domain to the frequency domain. The DFT is used in the analysis of many multimedia files.

The DFT for a digital image or signal is defined based on Expression 4.

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 05 ISSUE 03 Pages: 53-60
OCLC – 1368736135

$$X_k = \sum_{n=0}^{N-1} x_n e^{-j2\pi \frac{kn}{N}}, \quad k = 0, 1, 2, ..., N-1 \qquad (4)$$

Here:

x_n — values of an image or signal in the time or space domain,

X_k — components in the frequency domain,

N is the length of the discrete signal.

New components may appear in the spectrum of an image manipulated using DFT, which is used to detect manipulation[4].

Statistical models are used to detect changes in multimedia data using probability and statistical analysis methods. In this method, the original features of an image or signal (e.g., color distribution, texture) are described by a statistical model and then how these features change as a result of manipulation is examined. Changes in these features as a result of manipulation are also detected.

III. Detecting unauthorized modification of multimedia data based on statistical models

Statistical models are used to describe the characteristics of an image or signal. These characteristics are expressed in terms of statistical parameters, such as color distribution, texture, and pixel correlation. Basic statistical methods, such as probability distribution, covariance, variance, and central moments, are analyzed.

The color distribution of an image represents the probability distribution of the color values of each pixel in the image. Colors are divided into R , G , and B (red, green, and blue) components. Image manipulation can change the color distribution, so statistical analysis is used to detect changes in the color distribution[5].

Probability distributions are used to model the colors or other features of an image. Suppose the distribution of colors in an image is represented as $p(x)$, *where x represents* a color component (e.g., R , G , or B) of the image:

$$p(x)=P(X=x) \qquad (5)$$

If an image is manipulated, its color distribution $p(x)$ may change. The color distribution of the manipulated image is represented by $p'(x)$. The difference in color distribution can be determined based on Expression 6:

$$\Delta p(x)=p'(x)-p(x) \qquad (6)$$

Here $\Delta\, p(x)$ denotes the change caused by the manipulation.

Textures represent repetitive structures in an image, such as surface structures, color distributions, and other features. Many statistical methods are used in texture analysis, such as co-occurrence matrices, Haar transforms , and Gabor filters .

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 05 ISSUE 03 Pages: 53-60
OCLC – 1368736135

The co-occurrence matrix can be used to model the texture of an image. This matrix measures the correlation between each pixel in the image and its neighbors.[6] For example, the value *p(i,j) represents the probability that* color components *i* and *j* co-occur in an image (Expression 7).

$$p(i,j) = P(X_i = i \text{ va } X_j = j) \quad (7)$$

If the image is manipulated, the values in the co-occurrence matrix will change. The changes resulting from the manipulation can be checked using the following expression :

$$\Delta p\ (i,j) = p'(i,j) - p(i,j) \quad (8)$$

Statistical moments (such as the first and second moments) and correlations can be used to analyze the unique features of an image. These methods are useful for detecting changes in the texture of an image. If the texture of an image changes as a result of manipulation, changes in these moments and correlation values will also be observed.

Probability distribution comparison methods are used to detect multimedia data alteration. This involves measuring the difference between the probability distributions of the original image and the manipulated image.

The chi-squared test is used to test the similarity of two probability distributions.[7] The difference between the color distributions of an image, *p(x)* and *p′(x),* can be calculated using Expression 9.

$$x^2 = \sum_x \frac{(p'(x) - p(x))^2}{p(x)} \quad (9)$$

If x^2value big if so , then in the picture manipulation to be This test measures the difference between the probability distributions of the original image and the manipulated image. The main methods of statistical analysis and the probability and statistical methods used to detect manipulation are listed in the table below .

Table 1.

Basic methods of statistical analysis and probability and statistical techniques used to detect manipulation

Analysis Method	Feature	Detection Method
Color dispersion	Distribution of color components	The difference between *p(x)* and *p′(x)*
Co-occurrence matrix	Tissues and their connections	The difference between *p(i,j)* and *p′(i,j)*
Haar transform/ Gabor filter	Tissue structure size	Tissue changes
Chi-Square Test	To test the similarity of distributions	x^2calculate the value

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 05 ISSUE 03 Pages: 53-60
OCLC – 1368736135

ISSN-2750-1396

Statistical models use probability distributions, texture models, and statistical tests to detect the alteration of multimedia data. Color distribution and texture analysis play an important role in determining how the manipulated image has changed compared to the original features. Probability methods such as the chi-square test are effectively used to statistically test for the presence of manipulation.

Markov chain models can be used to detect unauthorized changes in the texture analysis of images. Each state of the Markov chain is associated with the texture of the image, and the values of each pixel are determined based on previous values.

The transition probabilities for a Markov chain are given by:

$$P(x_{i+1} + |x_i) = \frac{P(x_1, x_2, \ldots, x_{i+1})}{P(x_1, x_2, \ldots, x_i)} \quad (10)$$

Here:

$P(x_{i+1} + |x_i)$— probability of moving from the *i* -th pixel to *the i+1* -th pixel,

x_1 and x_{i+1}— corresponding pixels.

In a Markov chain model, if the image is manipulated, the sequence of probabilities can change.

Conclusion

Advanced technologies in the fields of cybersecurity and digital forensics are playing an important role in combating new and complex threats in our time. With the development of the Internet and digital technologies, problems such as cyberthreats and cyberfraud are becoming more widespread. In solving these problems, the effectiveness of multimedia data analysis, signal analysis and manipulation detection methods deserve special attention. In the field of digital forensics, many advanced algorithms and methodologies are being developed for detecting changes and analyzing image manipulation. Mathematical methods such as Fourier transform, Haar transform and Gabor filters are used to detect manipulations in images and videos. Also, statistical analysis tools such as probability distributions, color distribution and co-occurrence matrix play an important role in detecting changes in image and video materials. At the same time, the detection of manipulations carried out through social networks and digital documents has a great impact on the future development of cybersecurity and forensic analysis. Crime detection and security processes are becoming more effective through the analysis of images and videos using advanced mathematical methods such as Markov chains and discrete Fourier transforms.

In general, the development of digital forensics and cybersecurity, using network tools and innovative solutions, provides significant advances in combating threats in the digital environment. Their effective application creates new opportunities for detecting cybercrime and manipulation, which helps to shape best practices in ensuring security.

References

1. W. Oppenheim, RW Schafer, "Discrete-Time Signal Processing", Boston, Massachusetts, USA, 2010, ISBN: 978-0131988421, pp. 45-96.

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 05 ISSUE 03 Pages: 53-60
OCLC – 1368736135

2. W. Oppenheim, RW Schafer, "Discrete-Time Signal Processing", Boston, Massachusetts, 2010, ISBN: 978-0131988421, pp. 33-144.
3. John G. Proakis, Dimitris G. Manolakis, "Digital Signal Processing: Principles, Algorithms, and Applications", India, 2014, ISBN: 978-0133750366, pp. 200–300.
4. Sanjay Sharma, "Digital Signal Processing: Theory and Practice", New Delhi, India, 2014, ISBN: 978-1107067345, pp. 161-218.
5. Saeed V. Vaseghi, S. Xie, Advanced Digital Signal Processing and Noise Reduction, Beijing, China, 2011, ISBN: 978-0470661380, pp. 45-88.
6. Rafael C. Gonzalez, Richard E. Woods, Digital Image Processing, Boston, 2017, ISBN: 978-0133356724, pp. 155-244.
7. Rafael C. Gonzalez, Richard E. Woods, Digital Image Processing, Boston, 2017, ISBN: 978-0133356724, pp. 13-52.