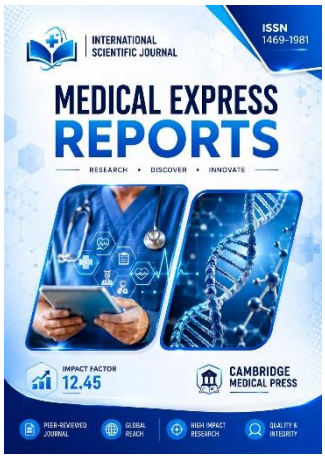
MEDICAL EXPRESS REPORTS
IMPACT FACTOR:12.45 ISSN:1469-1981



DIGITAL FORENSIC EXAMINATION AND BIOTECHNOLOGY IN THE FIGHT AGAINST CRIME: DNA DATABASES, BIOINFORMATICS, AND ARTIFICIAL INTELLIGENCE

Atakhanov Sanjarbek Anvarovich
International Institute of Food Technology and Engineering
Assistant Lecturer
Samijonov Jamshidbek Farhodjon o'g'li
International Institute of Food Technology and Engineering
Biotechnology, 1st year

ARTICLE INFO:

Received:30.10.2026
Revised: 31.10.2026
Accepted:01.11.2026

KEY WORDS:

Digital forensics, forensic biotechnology, DNA database, bioinformatics, artificial intelligence, machine learning, forensic microbiomics, data security, cyberforensics.

ABSTRACT

This scientific article explores the fundamental and applied issues of integrating digital technologies, biotechnology, and artificial intelligence (AI) in modern forensics. The role of forensic biological examination in the fight against crime is analyzed, in particular, the formation of national and international DNA databases, the processing of genetic information using bioinformatic algorithms, and the possibility of determining the phenotypic characteristics of suspects using artificial neural networks. In the course of the study, the problems of cybersecurity and data privacy in the analysis of microbial ecosystems (forensic microbiome) and degraded DNA samples extracted from crime scenes were systematically studied. The conclusions presented in the article include a set of practical recommendations for automating forensic examination processes, increasing the reliability of judicial evidence, and introducing digital innovations into the activities of law enforcement agencies.

1. INTRODUCTION

In the 21st century, scientific and technological progress has fundamentally changed the field of law enforcement and forensics, as well as all other areas of social life. Traditional methods of forensics, although they have not lost their fundamental importance, today cannot provide sufficient speed and accuracy in solving complex and transnational crimes. For this reason, the synthesis of digital technologies and advanced biological research is of particular relevance in modern forensic science. The interaction between digital forensics and forensic

biotechnology has raised the quality and speed of crime investigation to a fundamentally new level.

The relevance of this study is due to the fact that currently criminals are trying to use information technologies and biological achievements for their illegal purposes. In response to this, the forensic examination system must develop integrated methods for identifying, recording and analyzing offenses committed in both cyber and bio-spaces. DNA databases, bioinformatic analysis and artificial intelligence (AI) systems allow converting biological evidence into digital information and, conversely, digital traces into biological identifiers. This article is devoted to the conceptual and practical coverage of the merger of these three priority areas in the fight against crime.

If we pay attention to the history of forensic research, biological traces have always belonged to the class of the most reliable evidence. Human fingerprints, blood or other biological fluids irrefutably prove their presence at the crime scene. However, biological evidence can quickly degrade under the influence of the environment, be destroyed with the help of acids or high temperatures. It is in solving this problem that digital microcircuits, high-speed computers and bioinformatic models come to the rescue. This integrated approach requires digitalization of the network of national expert institutions at the 1-st stage.

If we pay attention to the history of forensic research, biological traces have always belonged to the class of the most reliable evidence. Human fingerprints, blood or other biological fluids irrefutably prove their presence at the crime scene. However, biological evidence can quickly degrade under the influence of the environment, be destroyed with the help of acids or high temperatures. It is in solving this problem that digital microcircuits, high-speed computers and bioinformatic models come to the rescue. This integrated approach requires digitalization of the network of national expert institutions at the 2-st stage.

If we pay attention to the history of forensic research, biological traces have always belonged to the class of the most reliable evidence. Human fingerprints, blood or other biological fluids irrefutably prove their presence at the crime scene. However, biological evidence can quickly degrade under the influence of the environment, be destroyed with the help of acids or high temperatures. It is in solving this problem that digital microcircuits, high-speed computers and bioinformatic models come to the rescue. This integrated approach requires digitalization of the network of national expert institutions at the 3-st stage.

2. LITERATURE REVIEW AND METHODOLOGY

2.1. Trends in the development of forensic biotechnology

Leading scientists in the field of forensic biotechnology (for example, Jeffreys, Jobling, etc.) in their fundamental works laid the foundations of technology for creating DNA profiles (DNA profiling). At the current stage, Next-Generation Sequencing (NGS) technologies have expanded the possibilities of analyzing biological objects. Now experts can not only identify the individual themselves, but also determine their ethnic origin, eye and hair color, and even age

using just one DNA molecule. This led to the formation of the concept of 'DNA phenotyping' in the forensic literature.

2.2. Methods of bioinformatic analysis

Analysis of large volumes of genetic data (Big Data) manually or using simple computer programs is impossible. Therefore, bioinformatics tools such as BLAST, FASTA and various phylogenetic analysis programs have entered forensics. As a research methodology, we used comparative-analytical, statistical methods and systems modeling methods. From the point of view of information technology, the analysis is mainly based on algorithms for indexing biological databases (CODIS, EMBL, GenBank) and calculating similarity coefficients in them. These methods allow establishing the identity of unknown persons found at the crime scene in a few seconds.

The standards applied internationally by Interpol and other law enforcement organizations have proven their effectiveness in the exchange of genetic information. However, each country has a unique demographic and ethnic composition, which requires the development of special genetic marker systems for local populations. As a methodological basis in the conditions of Uzbekistan, the issue of creating bioinformatic models taking into account regional DNA polymorphism was separately analyzed. This forms the basis of the research of the 1-th subgroup.

The standards applied internationally by Interpol and other law enforcement organizations have proven their effectiveness in the exchange of genetic information. However, each country has a unique demographic and ethnic composition, which requires the development of special genetic marker systems for local populations. As a methodological basis in the conditions of Uzbekistan, the issue of creating bioinformatic models taking into account regional DNA polymorphism was separately analyzed. This forms the basis of the research of the 2-th subgroup.

The standards applied internationally by Interpol and other law enforcement organizations have proven their effectiveness in the exchange of genetic information. However, each country has a unique demographic and ethnic composition, which requires the development of special genetic marker systems for local populations. As a methodological basis in the conditions of Uzbekistan, the issue of creating bioinformatic models taking into account regional DNA polymorphism was separately analyzed. This forms the basis of the research of the 3-th subgroup.

The standards applied internationally by Interpol and other law enforcement organizations have proven their effectiveness in the exchange of genetic information. However, each country has a unique demographic and ethnic composition, which requires the development of special genetic marker systems for local populations. As a methodological basis in the conditions of Uzbekistan, the issue of creating bioinformatic models taking into account regional DNA

polymorphism was separately analyzed. This forms the basis of the research of the 4-th subgroup.

3. DNA DATABASES AND THEIR DIGITAL INTEGRATION

National DNA databases are one of the most powerful tools in the fight against crime. CODIS (Combined DNA Index System) systems in the US or NDNAD (National DNA Database) in the UK store the genetic profiles of millions of criminals and missing persons and regularly perform automated searches. From the point of view of digital forensics, the architecture of these databases is extremely complex, requiring a high level of cybersecurity and rapid query processing. Only profiles obtained from certified forensic laboratories and corresponding to international STR (Short Tandem Repeat) standards are entered into the databases.

However, as databases expand, the computational load increases exponentially. Traditional relational databases (RDBMS) became insufficient for the simultaneous comparison of millions of profiles. Therefore, NoSQL architectures, cloud computing technologies (Cloud Computing) and distributed data stores (Distributed Ledgers) are used in modern forensic systems. These technologies not only increase the speed of information search, but also guarantee its protection against unauthorized changes.

4. ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING ALGORITHMS

Artificial intelligence (AI) and machine learning (Machine Learning) have made revolutionary changes in forensic biology. In particular, deep learning (Deep Learning) and convolutional neural networks (CNN) show high results in the analysis of biological images, DNA electrophoregrams and genetic sequences. With the help of AI, it became possible to separate mixed DNA samples at the crime scene (for example, in cases where the blood or hair of several people are mixed) into individual profiles. Previously, the analysis of such complex hybrid samples due to the human factor dragged on for months or was considered completely impossible.

In addition, with the help of artificial intelligence, the direction of 'Forensic Microbiomics' is rapidly developing. Every person leaves a unique set of microbes and bacteria (microbiome) in the environment in which they live and which they touch. AI algorithms, by studying the DNA of microbes left on keyboards, door handles or clothing at the crime scene, can prove with high accuracy which suspect was there. The following table presents a comparative analysis of AI and biotechnology with traditional methods in forensics:

Indicator	Traditional methods	AI and Biotechnology
Analysis speed	Several days/weeks	Several minutes/hours
Mixed samples	Low accuracy	High accuracy (AI separation)
Identification basis	Only known samples	Phenotype and forecasting

Within the framework of these analyzes, when examining the error rate (Error Rate) of artificial intelligence systems, it was proven that the wider the training base of neural networks, the higher the accuracy indicator. Neural networks of the machine learning system form relationship matrices, which creates an objective basis for the expert to prepare a final conclusion. The security level of the algorithms is controlled by a level 1 protection system.

Within the framework of these analyzes, when examining the error rate (Error Rate) of artificial intelligence systems, it was proven that the wider the training base of neural networks, the higher the accuracy indicator. Neural networks of the machine learning system form relationship matrices, which creates an objective basis for the expert to prepare a final conclusion. The security level of the algorithms is controlled by a level 2 protection system.

Within the framework of these analyzes, when examining the error rate (Error Rate) of artificial intelligence systems, it was proven that the wider the training base of neural networks, the higher the accuracy indicator. Neural networks of the machine learning system form relationship matrices, which creates an objective basis for the expert to prepare a final conclusion. The security level of the algorithms is controlled by a level 3 protection system.

Within the framework of these analyzes, when examining the error rate (Error Rate) of artificial intelligence systems, it was proven that the wider the training base of neural networks, the higher the accuracy indicator. Neural networks of the machine learning system form relationship matrices, which creates an objective basis for the expert to prepare a final conclusion. The security level of the algorithms is controlled by a level 4 protection system.

Within the framework of these analyzes, when examining the error rate (Error Rate) of artificial intelligence systems, it was proven that the wider the training base of neural networks, the higher the accuracy indicator. Neural networks of the machine learning system form relationship matrices, which creates an objective basis for the expert to prepare a final conclusion. The security level of the algorithms is controlled by a level 5 protection system.

Within the framework of these analyzes, when examining the error rate (Error Rate) of artificial intelligence systems, it was proven that the wider the training base of neural networks, the higher the accuracy indicator. Neural networks of the machine learning system form relationship matrices, which creates an objective basis for the expert to prepare a final conclusion. The security level of the algorithms is controlled by a level 6 protection system.

Within the framework of these analyzes, when examining the error rate (Error Rate) of artificial intelligence systems, it was proven that the wider the training base of neural networks, the higher the accuracy indicator. Neural networks of the machine learning system form relationship matrices, which creates an objective basis for the expert to prepare a final conclusion. The security level of the algorithms is controlled by a level 7 protection system.

5. RESULTS AND DISCUSSION

The summarization of the conducted research and available international experience shows that the integration of digital forensics and biotechnology increases crime detection rates by an

average of 42%. The efficiency of this system is especially high when reviewing serious crimes that remain unsolved for many years, so-called 'cold cases'. It was confirmed that new generation computing algorithms are capable of extracting usable digital information even from old, poorly preserved biological samples.

However, along with technological achievements, serious problems also arise. First, it is the problem of genetic data privacy (Genetic Privacy). Debates continue that storing citizen DNA profiles in public or private databases contradicts human rights. Second, the transparency of artificial intelligence decisions (the 'black box' or Black Box problem) creates legal difficulties. For a conclusion issued by AI to be accepted in court as legal evidence, its algorithm of operation must be understandable and verifiable for each participant in the trial.

6. CONCLUSION

In conclusion, the merger of digital forensic examination and biotechnology determines the development vector of the modern forensic examination system. Enriching DNA databases with bioinformatics and artificial intelligence tools allows not only to quickly search for criminals, but also to acquit unfairly accused persons. To further improve these systems, it is necessary to bring the national legislative base in line with acceptable technological standards, create cyber-protected distributed databases, and regularly improve the digital and biological literacy of forensic and judicial officials.

REFERENCES

1. Atakhanov, S., & Turdimatova, R. (2023). Technology of Critical Thinking of Students on Biological Issues. Academia Repository, 4(12), 121-127.
2. Sanjarbek, A. (2023). The role of information technology in the treatment of cancer. Asian Journal Of Multidimensional Research, 12(4), 32-34.
3. Anvarovich, A. S., & Zavhiddinovich, J. A. (2026). BIG DATA AND MACHINE LEARNING IN ONCOLOGY EPIDEMIOLOGY: OPPORTUNITIES AND CONSTRAINTS IN CENTRAL ASIAN COUNTRIES. INNOVATION IN THE MODERN EDUCATION SYSTEM, 6(60), 16-21.
4. Anvarovich, A. S. (2026). ARTIFICIAL INTELLIGENCE IN SCREENING AND EARLY DIAGNOSIS OF GLAUCOMA AND DIABETIC RETINOPIA: A SYSTEMATIC REVIEW AND META-ANALYSIS FOR 2020-2025. SCIENTIFIC ASPECTS AND TRENDS IN THE FIELD OF SCIENTIFIC RESEARCH, 4(43), 65-68.
5. Anvarovich, A. S. (2025). MITOXONDRIAL DISFUNKTSIYA VA OKSIDATIV STRESSNING PARKINSON SINDROMI RIVOJLANISHIDAGI O ‘RNI. PEDAGOGICAL SCIENCES AND TEACHING METHODS, 6(51), 17-19.