Pakistan Journal of Criminology
Vol. 16, No. 03, July—September 2024 (275-294)

Steganographic Technologies in the Identification of Convicted Persons

Yerbol Tokzhanov[1], Dina Kalmaganbetova[2],
Assel Kussainova[3], Svetlana Baimoldina[4] &
Saltanat Sarybekova[5]

Abstract

The purpose of this study was to comprehensively investigate and analyse the features of steganographic technology, which is used in Kazakhstan in the context of identification of convicted persons to protect information and minimise the violation of its integrity. The following methods were used during the study: analysis, comparison, structural-functional method, and formal-legal method. The study examined the legislation of Kazakhstan and assessed the ethical and legal issues associated with the use of steganography in the identification of convicts, which includes discussion of privacy, data security, and compliance with human rights laws. This study identified problematic aspects and potential areas for improvement of the public administration system of steganographic technologies in Kazakhstan. Furthermore, such a tool as steganography and its potential use for data exchange by criminals, as well as the prospects of countering this exchange by information security specialists were considered.

Keywords: Authentication; Information; Swot Analysis; Cryptography; Forensic Science; National Security.

Introduction

Steganographic technologies are still relevant in the field of convicted person identification due to their significant role in information security. They can also be useful in various fields, including law enforcement, due to their ability to reveal information concealed by criminals. There are several other important reasons for investigating steganographic technologies in the context of convicted

[1] Doctoral Student, Department of Criminal Prosecution and Operational Investigative Activities, Law Enforcement Academy under the Prosecutor General's Office of the Republic of Kazakhstan, Kosshy, Republic of Kazakhstan, Kazakhstan. yer.tokzhanov@gmail.com

[2] Senior Lecturer, Department of Criminal Law Disciplines, L.N. Gumilyov Eurasian National University, Astana, Republic of Kazakhstan, Kazakhstan. kalmag.dina@outlook.com

[3] Center for Research of Problems in the Field of Protection of Public Interests, Law Enforcement Academy under the Prosecutor General's Office of the Republic of Kazakhstan, Kosshy, Republic of Kazakhstan, Kazakhstan. asselkussainova@outlook.com

[4] Senior Lecturer, Department of Criminal Law Disciplines, L.N. Gumilyov Eurasian National University, Astana, Republic of Kazakhstan, Kazakhstan. s_baimoldina@hotmail.com

[5] Senior Lecturer, Department of Criminal Law and Procedure, Taraz Regional University named after M.Kh. Dulaty, Taraz, Republic of Kazakhstan, Kazakhstan. s.sarybekova@hotmail.com

person identification. One is digital footprint concealment: convicted offenders can use steganography to conceal digital footprints related to their criminal activities, such as photographs, videos, or documents. Another important reason is to protect national security: the study of steganographic technologies allows law enforcement agencies to identify and prevent potential threats to national security (Kumar & Kumar, 2018; Sopilko & Rapatska, 2023), because steganography can be used by terrorists or other criminal groups to organise terrorist attacks or other criminal activities.

The problematic of this study is that the effectiveness of the use of steganographic technologies in the identification of convicted persons in the Republic of Kazakhstan is insufficient. The issues related to steganographic technologies are understudied in Kazakhstan. One of the few studies is the research of A. Baitursynuly (2022). The scientist states that the roots of steganographic technology go deep into the past, and various forms of steganography have evolved over many centuries. The first references were in the ancient world. Ancient civilisations such as the Egyptians and Romans are known to have used various methods of shorthand for important documents and court proceedings.

Kazakhstan has a national institute specialising in information security. Its main objective is to conduct research that is of strategic importance for the phased replacement of imported resources. The initiator and author of this idea, who is the director of the Research Institute of Information Security and Cryptology at L.N. Gumilyov Eurasian National University and a member of the Public Council of the Ministry of Defence and Aerospace Industry of the Republic of Kazakhstan, shared the following information in one of his interviews: V. Volkov (2018) states that the problems associated with ensuring the study of the topic of steganography in the field of national security are considered to be among the most urgent both for Kazakhstan and for all countries of the world. These issues are integral to security, both at the level of the individual country and for the entire humanity. The expert recognises that this is one of the key global issues requiring immediate attention and decisive action. A.A. Kassymzhanova et al. (2021) considered the legal aspects of guaranteeing national security and assessed external threats that may affect the security of the Republic of Kazakhstan and concluded that it is necessary to further study the legislative framework of the Republic of Kazakhstan to minimise national threats.

Within the framework of this study, it is worth paying attention to the scientific work of J. Fridrich (2009), who considers steganographic technologies from the standpoint of their technical implementation in the penitentiary system. He argues that steganographic methods by their very nature can be complex and difficult to understand. Developers of steganographic tools are constantly improving their techniques to conceal information more effectively. This means that law enforcement agencies must constantly learn new methods and means of detecting steganography. A similar opinion is held by I. Warren et al. (2020), who note that steganographic technologies are constantly evolving. This leads to the fact that law enforcement agencies need a lot of material, technical, and time resources to analyse and identify hidden information to fight crime effectively. In general, significant research in steganographic technologies is being conducted in Kazakhstan. However, the state of this area is still at a rather low level in comparison with other countries, many issues on this subject require modernisation and detailed investigation using different methods.

The purpose of this study was to review steganographic methods used in Kazakhstan in the penitentiary system to identify convicted persons, considering compliance with the legislation of the country, to ensure the protection of information and minimise possible violations of its integrity.

Materials and Methods

This study used the laws of Kazakhstan (Law of the Republic of Kazakhstan "On National Security"…, 2012), which regulate various aspects such as protection of state interests, prevention of terrorism and extremism, cybersecurity (Council of Europe, 2001), and other issues related to ensuring the security of the state and its citizens. To investigate the subject of steganographic technology in the identification of convicted persons in Kazakhstan, the study used a variety of materials, including official laws and regulations governing the use of steganography in legal proceedings and in the identification of convicted persons, the texts of international conventions (Convention No. 100 concerning…, 1951; Convention No. 156 on…, 1981), which may be relevant to the use of steganography in criminal and judicial cases, an example of such a documents is the Convention on Cybercrime (Council of Europe, 2001), T.A. Kulibaev (2016), in which steganographic technology was used in investigations, and the use of steganography in the identification of convicted persons.

The analysis was used to collect data on cases where steganography was used in Kazakhstan during crime investigation and/or court proceedings (Adanbekova et al., 2022). The study also analysed what steganographic methods and technologies have been used in the context of the identification of convicted persons in Kazakhstan. Furthermore, this method helped to explore the legislative framework related to the use of steganography in criminal and judicial cases. Based on the analysis, an assessment of the effectiveness of the steganographic method in the identification of criminals in Kazakhstan was provided. The data analysis allowed for the systematisation and analysis of available data and information to better understand the role of steganographic technologies in the identification of criminals in a particular country such as Kazakhstan. The comparison method is an important part of the research on the topic, which helped to better understand the context of steganography application in Kazakhstan and evaluate its effectiveness. This method helped to identify the strengths and weaknesses of steganography in criminal and judicial proceedings, to compare the effectiveness of steganographic methods used in Kazakhstan.

The structural-functional method is a valuable tool for researching this subject, which helps to structure the complex interrelationships in the phenomenon under study. Using this method, the key elements and components associated with the use of steganography in the identification of convicted persons in Kazakhstan were identified. These elements include technical aspects of steganography, legal regulations, methodologies, and application practices. Furthermore, the structural-functional method helped to find the relationship between these elements. For instance, what technological methods of steganography are used in Kazakhstan and what regulations govern their use, what law enforcement agencies carry out the identification of convicted persons using steganography and what technical limitations they face. Overall, the structural-functional method helped to understand the complex structures and interrelationships accompanying the use of steganography in the identification of convicted persons in Kazakhstan and contributes to a better understanding of this topic and the development of practical solutions.

The study of this topic also employed a formal-legal method, which helped to assess the compliance of the practice of steganography with the legislation and norms of international law. Using this method, the study investigated the national legislation of Kazakhstan, which regulates the use of steganography in judicial and criminal proceedings, which includes the analysis of the relevant articles of the Criminal Code, Criminal Procedural Code, as well as sublegislative acts. The formal-legal method helped to identify potential problems and shortcomings in legislation and its application, namely contradictions between different laws, unclear norms, and violations of citizens’ rights. This method helped to develop recommendations to improve the legal framework, including suggestions for changes in legislation or improvements in procedures and practices.

Results

Steganography is a method of covert transmission of information that involves hiding some data (message) inside other data (medium) in such a way that an observer, unaware of it, cannot detect the presence of the concealed message. This method is different from cryptography, which relies on the encryption of data to conceal the content of a message. Instead of encryption, steganography uses various methods to embed data into other data in a way that is not suspicious. Examples of media in which hidden messages can be concealed are images, sound files, video files, text documents, and even other data formats. Various methods can be used to embed hidden data into the media, such as changing subtle bits in an image or sound, using special algorithms to embed information, and many other techniques.

Steganography can be used for a variety of purposes, both for the covert transmission of sensitive information and for authentication and data protection purposes. However, it can also be abused for illegal or malicious purposes, and therefore it is of interest to cybersecurity and forensic science (Metelskyi & Kravchuk, 2023; Shestak & Tsyplakova, 2023). According to Oxford English Dictionary, steganosystem (short for 'steganographic system') is the basis for creating a covert data communication channel (Electronic Oxford English Dictionary). There is limited information on steganographic technology usage statistics because many steganographic use cases may go undetected or stay secret. Nevertheless, steganographic techniques can be used in a variety of applications and purposes (Ardhianto et al., 2020). Here are a few areas where they can be applied:

1. Computer security: steganography can be used to hide information from malicious hackers or intruders to prevent sensitive data leakage.

2. Forensics and law enforcement: steganography can be used by criminals to hide information about illegal activities, and law enforcement can use steganography to identify and analyse concealed data.
3. Military and intelligence operations: in the field of military and intelligence operations, steganography can be used to conceal essential information, exchange data with agents.
4. Corporate security: companies can apply steganography to protect sensitive commercial data and secrets.
5. Medicine and healthcare: steganography can be used to conceal medical information in images and transmit it over open communication channels.
6. Media: the use of steganography can be related to journalism and the publication of confidential documents or reports.

Considering steganography through SWOT analysis can help to assess their current state and potential for development. SWOT analysis is a strategic analytics technique that helps to assess internal strengths and weaknesses as well as external opportunities and threats to an organisation or project. It identifies the key factors that influence success and development, which helps to develop more effective strategies. Some elements that can be included in a SWOT analysis of steganography are presented in Table 1.

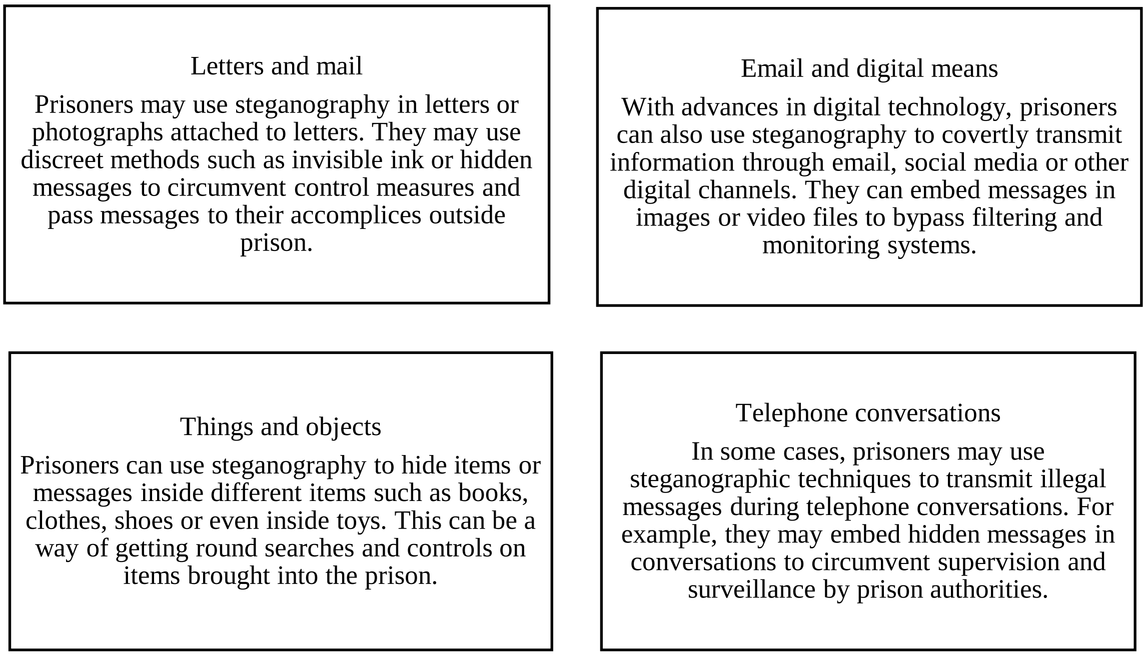
Table 1: SWOT analysis of steganographic technologies

Strengths	**Weaknesses**
Secrecy: steganographic techniques allow information to be concealed within other data, making it difficult for unauthorised observers to discern. Security: properly implemented steganographic technologies can provide an additional layer of security and privacy for transmitted data. Variety of applications: steganography can be used in a variety of fields, including cybersecurity, digital media, medical data, and even art.	Computational resources: some steganography techniques can be computationally expensive, requiring large resources to embed and extract hidden information. Detection: steganographic methods can be detected if proper analysis techniques are applied to them. This can reduce their effectiveness. Legal and ethical issues: the use of steganography can expose questions of legality and ethics, especially in the context of cybersecurity and compliance with data protection laws.
Opportunities	**Threats**
Developments in cybersecurity: steganography can be part of innovative methods to secure data and combat cyberthreats. Research and development: there is potential for further research and development in steganography, which could lead to new and more effective techniques. Media and art applications: steganography can be used to create interesting artificial works and content.	Abuse: steganography can be abused to covertly transmit malicious code or information, posing a security risk. Legislation and regulation: some have laws and regulations that restrict the use of steganography, particularly in the context of cybersecurity. Technological advances: as technology advances to analyse and detect steganography, new threats to its effectiveness may arise.

Source: compiled by the authors of this study.

A SWOT analysis can help to better understand the current state and prospects of steganographic technologies, as well as identify strategies for improvement and development. Moreover, steganographic technologies can have various applications in the prison system for security, supervision, and efficient organisation of work (Law and Justice, 2019). The use of steganographic technologies in the prison system has a history, although such technologies are most often associated with cybersecurity and the covert exchange of information in digital environments (Vilks et al., 2022). In the context of prisons, prisoners can use steganography to transmit illegal communications or plan offences or used to identify prisoners. Here are some examples of the use of steganography by inmates in the prison system, which are presented in Figure 1.

Figure 1: Use of steganography by prisoners in the penitentiary system



Letters and mail

Prisoners may use steganography in letters or photographs attached to letters. They may use discreet methods such as invisible ink or hidden messages to circumvent control measures and pass messages to their accomplices outside prison.

Email and digital means

With advances in digital technology, prisoners can also use steganography to covertly transmit information through email, social media or other digital channels. They can embed messages in images or video files to bypass filtering and monitoring systems.

Things and objects

Prisoners can use steganography to hide items or messages inside different items such as books, clothes, shoes or even inside toys. This can be a way of getting round searches and controls on items brought into the prison.

Telephone conversations

In some cases, prisoners may use steganographic techniques to transmit illegal messages during telephone conversations. For example, they may embed hidden messages in conversations to circumvent supervision and surveillance by prison authorities.

Source: Amirtharajan & Rayappan (2013).

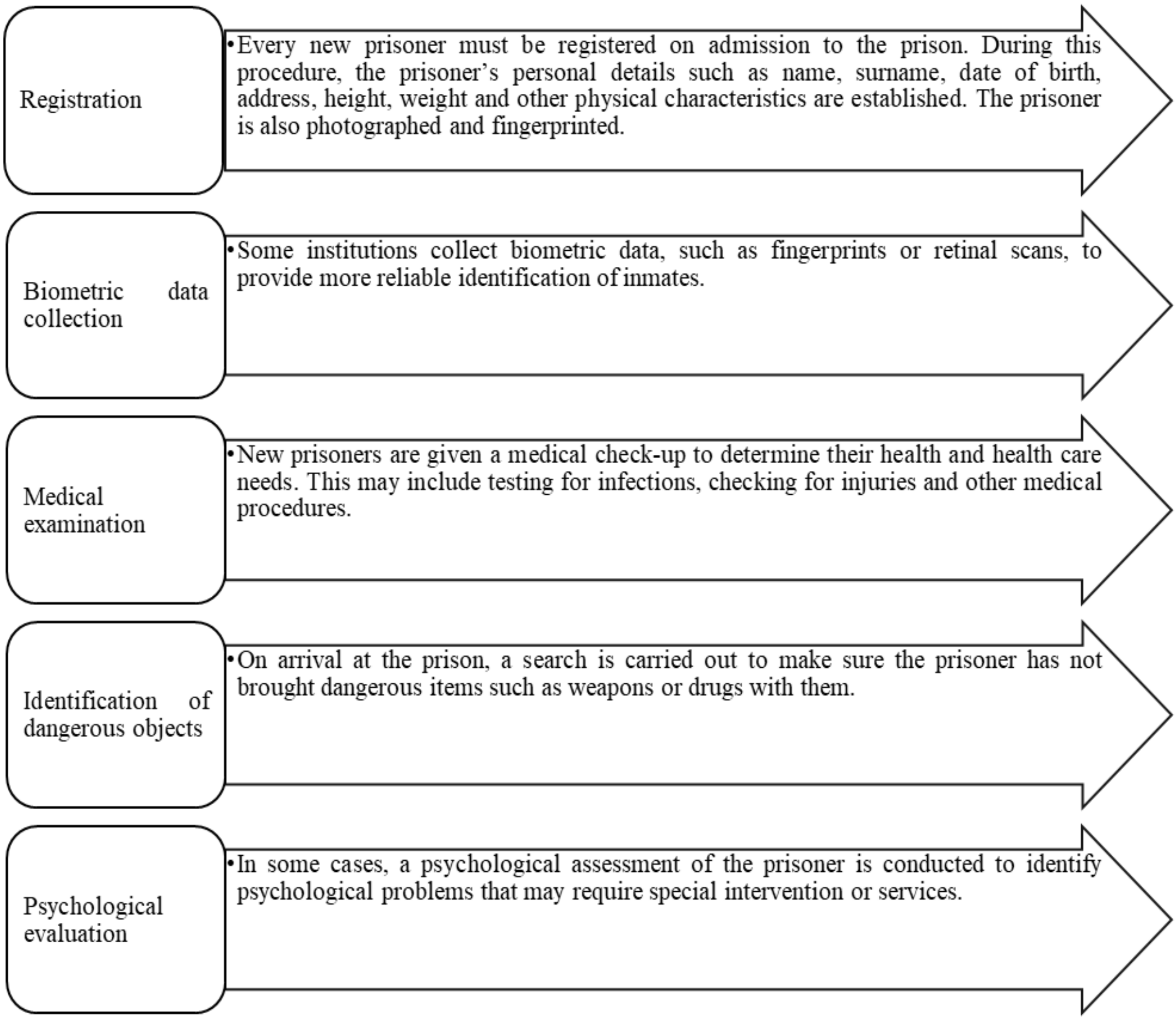
The prison administration is constantly improving methods of monitoring and detecting such attempts. Security professionals and control officers in prisons are constantly developing and implementing new methods and technologies to detect steganographic messages and items. The administration uses such steganographic techniques in its work for greater control over the preservation of the country's national security; recording meetings and conversations:

steganographers may attend committee or court meetings within institutions and record conversations between inmates, administrators, and other participants. This produces accurate records that can be used as evidence or to enforce laws and procedures; documentation of psychological sessions: steganography can be useful when conducting sessions with psychologists or psychiatrists.

Recordings of sessions can be useful for diagnosing and monitoring prisoners: disciplinary hearings: where disciplinary hearings or investigations are necessary, steganography can be used to document testimony and evidence; medical consultations: it may also be possible to use stenography in medical consultations and examinations of prisoners to ensure that medical histories are accurately maintained; training and professional development: training prisoners in shorthand can provide them with skills and opportunities for future employment upon release; telephone monitoring: in some cases, shorthand can be used to monitor prisoners' telephone conversations with outside parties to prevent illegal activities or smuggling; creating educational materials: steganograph recordings can be used to create educational materials or case studies on prisoners' behaviour and reactions (Altynbassov et al., 2017). Moreover, steganographic technologies can be used for gender identification of prisoners, but to date there is no scientific research and practical applications worldwide on the issue of gender identification of prisoners using steganographic technologies.

A general analysis of prisoner identification was conducted, which shows that prisoner identification in prisons varies between countries and prison systems. However, common identification methods include the following procedures in that defined order (Figure 2).

Figure 2: Structure of state management in the field of science technology



Registration

- Every new prisoner must be registered on admission to the prison. During this procedure, the prisoner's personal details such as name, surname, date of birth, address, height, weight and other physical characteristics are established. The prisoner is also photographed and fingerprinted.

Biometric data collection

- Some institutions collect biometric data, such as fingerprints or retinal scans, to provide more reliable identification of inmates.

Medical examination

- New prisoners are given a medical check-up to determine their health and health care needs. This may include testing for infections, checking for injuries and other medical procedures.

Identification of dangerous objects

- On arrival at the prison, a search is carried out to make sure the prisoner has not brought dangerous items such as weapons or drugs with them.

Psychological evaluation

- In some cases, a psychological assessment of the prisoner is conducted to identify psychological problems that may require special intervention or services.

innovation in the Republic of Kazakhstan

Source: Muralidharan et al., (2022).

In analysing the identification of prisoners, an interesting fact was found that prisoners can be identified by category. Prisoners can be categorised according to characteristics such as level of dangerousness, length of sentence, age, and other factors. Other factors include gender identification, specifically cases of transgender identification (Saifnazarov & Saifnazarova, 2023). There is no research on this issue, so by analysing general information, it can be concluded that transgender people may face a range of unique challenges while in prison due to their gender identity. Here are some of the challenges transgender inmates may face:

1. Location procedure: Determining which prison or colony a transgender prisoner will be held in can be difficult. In some cases, it depends on biological sex, in others on legal sex or gender identity.
2. Security: transgender prisoners are often subject to threats and violence from other prisoners and even prison staff. Keeping them safe can be a daunting task.
3. Medical care: Many transgender prisoners may require medical care for their gender identity, such as hormone therapy or surgery. Access to this medical care may be limited.
4. Policies and procedures: Prison systems should have clear policies and procedures to ensure equal rights and safety for transgender prisoners.
5. Isolation: in some cases, transgender prisoners are placed in isolation or segregation units, which can cause feelings of isolation and depression.

Social and human rights organisations, as well as lawyers, are actively working to improve conditions and protect the rights of transgender prisoners (Gurunath et al., 2021). They train prison staff on gender identity and advocate for laws and standards regarding the rights of transgender people. Moreover, the identification and placement of transgender inmates in prisons depends on the laws and policies adopted in a particular country or jurisdiction, as well as the policies and practices adopted by the prison or jail. Different countries and states may have different rules and procedures, and therefore the local context should be considered. However, some countries and states recognise the right of transgender prisoners to self-identify according to their gender identity. This means that transgender prisoners can be accommodated according to their preferences for gendered spaces and treatment. When a transgender person enters the criminal justice system, various procedures may be used to determine their gender identity and make placement decisions (Kessler, 2004). These procedures may include the following: self-identification: some jurisdictions allow transgender prisoners to self-identify their gender and gender identity. This may include using an appropriate name and location for the placement; professional assessment: in some cases, doctors or psychologists may conduct an assessment of an inmate’s gender identity to determine the safest and most appropriate placement; facility policies and standards: prison or correctional facilities may have their own policies and standards regarding the placement of transgender inmates, which may vary from place to place.

Some countries and states have legal frameworks and guidance documents that regulate the treatment of transgender prisoners and ensure that their rights are protected. These norms aim to prevent discrimination and human rights violations in the context of criminal punishment. Approaches to identifying and accommodating transgender prisoners can vary substantially by location and legislation, and therefore it is important to refer to the concrete regulations and policies in the relevant region. With regard to steganographic technology, it can be used to identify convicted persons when prisoners have changed gender and attempted to conceal their identity to avoid punishment. However, steganography is not the best method. For such purposes, other methods are commonly used such as biometric identification; police registration; inspection and survey, biometric security systems (Pelosi & Easttom, 2021). Different countries have different policies and practices regarding transgender prisoners. Information on the gender identity of prisoners in Kazakhstan and elsewhere is limited. For up-to-date statistics on this issue, it is necessary to refer to official studies, law enforcement reports or organisations involved in monitoring the penal system in Kazakhstan or other countries. Such data may be available from the Ministry of Justice, the Corrections and Human Rights Monitoring Committee and other organisations involved in the analysis of criminal data and prisoners' rights. Requests for such information can also be addressed to non-governmental organisations that may be involved in prisoners' rights issues and monitoring of prison and penal conditions. But to date, the collection and publication of such data has been restricted for reasons of prisoner privacy and security of processing. Statistical data relating to gender identity is also missing for the purposes of prisoner confidentiality and security. Notably, the use of stenography in the prison system must comply with laws and security standards and consider the rights of prisoners to confidentiality and fair trial.

At all times and throughout many eras, issues related to national security have occupied a prominent position both in the life of individual states and in the context of the global community. Especially these problems became urgent in the 20th-21st centuries, the period of global integration. In modern times, humanity faces new types of threats to individual rights, society, and sovereign states. These threats include the use of steganographic technologies in the prison sector, in the gender identification of prisoners, and in information security systems (Kurylo et al., 2023). National security represents a fundamental element of state strategy within any sovereign nation (Sharyi et al., 2019). The Constitution of the Republic of Kazakhstan (1995), adopted in 1995, established the fundamental legal principles aimed at ensuring the preservation of the integrity, independence, and sustainability of Kazakhstan as a sovereign state subject. Legal norms, including constitutional provisions, laws of general and special nature, as well as international treaties, serve as the basis for ensuring the national security of the Republic of Kazakhstan. Kazakhstan, as a sovereign state, has ratified a range of key international agreements dealing with various aspects, such as the protection of human rights and freedoms, countering international terrorism, and ensuring environmental security. It should be emphasised that in the system of sources of law, the Constitution is supreme. Article 4 of the Constitution of the Republic of Kazakhstan (1995) states that the Constitution has supreme legal force and direct effect on the entire territory of the country. International treaties that have been ratified by the Republic of Kazakhstan take precedence over national laws.

Many international treaties relate to ensuring the rights and freedoms of citizens. The three major documents that prescribe human rights throughout the world are combined into what is sometimes referred to as the International Bill of Human Rights. These instruments include the Universal Declaration of Human Rights (1948) adopted by the UN General Assembly in 1948, the International Covenant on Economic, Social and Cultural Rights (1966) adopted in 1966, and the Optional Protocol to the International Covenant on Economic, Social and Cultural Rights (2008) of 2008. It also includes the International Covenant on Civil and Political Rights (1966), adopted in 1966, and its two Optional Protocols, Optional Protocol to the International Covenant on Civil and Political Rights (1966) and Second Optional Protocol to the International Covenant on Civil and Political Rights, aiming at the abolition of the death penalty (1989). The Universal Declaration of Human Rights (1948) has had a significant impact on subsequent universal and regional human rights treaties, as well as on national constitutions and other legislation.

Action in the field of human rights has resulted in the establishment of a range of norms that are now considered binding standards of international law. Such norms include the prohibition of torture and other forms of ill-treatment, as well as the prohibition of racial and gender discrimination, and the prohibition of slavery. Following the adoption of the Universal Declaration of Human Rights (1948), UN has developed and adopted a range of international treaties dealing with concrete aspects of human rights. These include the International Convention on the Elimination of All Forms of Racial Discrimination (1965), Convention on the Elimination of all Forms of Discrimination Against Women (1979) and Optional Protocol to the Convention on the Elimination of All Forms of Discrimination against Women (1999), Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (1984) and Optional Protocol to the Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (2002), Basic Principles for the Treatment of

Prisoners (1990), Body of Principles for the Protection of All Persons under Any Form of Detention or Imprisonment (1988) and Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power (1985).

Human rights are therefore a universal and inalienable set of norms applicable to all human beings without discrimination based on race, colour, sex, language, religion, national or social origin, and other aspects. It is also important to note the existence of international agreements aimed at combating terrorism, including the International Convention for the Suppression of the Financing of Terrorism (1999), the United Nations Convention Against Transnational Organised Crime and the Protocols Thereto (2004) and the Shanghai Convention on Combating Terrorism, Separatism and Extremism (2001). It may be noted that Kazakhstan has assumed the obligation to ratify all the above international treaties, which implies not only the need to bring national legislation into compliance with these treaties, but also the obligation to consider the requirements of these agreements in the work of state bodies. The concept of security includes the state of being protected from various types of threats. Law of the Republic of Kazakhstan "On National Security" No. 19-V (2012) considers six different aspects of national security: public, military, political, economic, informational and environmental. From all the above, it can be concluded that Kazakhstan has a developed legal framework, and these laws and legal acts are actively applied in the activities of the country's penitentiary system to improve the level of national security.

Discussion

The study of steganographic technologies stays relevant in the field of identification of convicted persons, as they play an important role in ensuring information security, in ensuring the development of the penitentiary system of the country. The research and development of steganography and steganographic message analysis techniques are still an important part of the work of law enforcement and information security professionals, as criminals and terrorists are constantly improving their methods of covert communication and information concealment. This helps to ensure the safety and security of the public from potential threats. In this context, it is difficult to deny the opinion of scientist Yu. Poita (2020), who points out that national security and knowledge of the legal framework of the country are significant for ensuring stability, protecting the interests of the state and its citizens, as well as for participation in the world community and maintaining peace and security on the world stage. It should be added to this statement that national security and the study of a country's legal framework are important in the field of law and order, as the legal framework defines the rules and procedures by which society functions. This includes the rights and duties of citizens, the rule of law and the system of legal proceedings. Law and order are an essential element in ensuring national security and social stability.

Another group of scientists A.A. Kassymzhanova et al. (2021), having investigated the importance of national security in Kazakhstan, concluded that the Law of the Republic of Kazakhstan "On National Security" No. 19-V (2012) defines a list of threats to national security (Art. 6), which do not correlate with the types of national security (Art. 4), which leads to the need to amend the law (Goffman, 2007). Therefore, at present the concept of "national security" should be understood through the lens of three categories: the individual, society, and the state. This follows from the constitutional norms, where the main value is proclaimed a person, their rights and freedoms, which directly depends on the development of steganographic technologies, the application of technology in the penitentiary system. Moreover, ensuring national security in the penitentiary system requires a comprehensive approach, including proper management of institutions, training of staff, rehabilitation of prisoners and cooperation with other authorities. This helps to minimise potential threats to society and national security. Attention should be paid to aspects such as prevention of escape and riot, for this purpose penitentiary institutions should be organised and managed in such a way as to prevent escape and riot of prisoners. This is important to prevent the threat to national security that escaped prisoners may pose. Next is to ensure the safety of personnel. Staff working in the prison system should be trained and equipped to ensure the safety of both the prisoners and their own. This helps prevent violence and conflict in institutions that could have potential national security implications (Saktaganova et al., 2023). Other aspects include cooperation with law enforcement agencies. The prison system should cooperate with the various law enforcement agencies to ensure that information is shared and coordinated to prevent and investigate crime both inside and outside the institutions.

E.N. Begaliev (2019) notes that the steganography method should be more actively used to identify the source of origin of material objects in order to counter cases of economic smuggling, theft, fraud, forgery of documents, violations of intellectual property rights and other offences. One cannot disagree with this statement, but it should be added that special attention should be paid to the development of innovative technologies, such as the use of artificial intelligence, as it can help automate the process of selecting programmes, which makes steganography more effective and less visible (Kulchytskyi, 2023). Or introduce the use of quantum technology: Quantum computing and quantum cryptography can provide new opportunities for steganography, as they can offer more secure methods of transmitting high-value information between law enforcement agencies. It can be added that this method should also be introduced in the penitentiary system, for the possibility of identification of convicted persons, as it was previously stated that prisoners try to avoid punishment for the committed crime in all possible ways, one of the ways is a change of sex, change of legal sex, which further causes difficulties in gender identification. This method is rarely used in practice because changing legal gender is only allowed in some countries (USA – in the United States the procedures for changing legal gender depend on the state. Many states allow gender reassignment based on self-identification, without the need for surgery or other medical procedures; Canada; UK; Netherlands; Australia). The study found an example of legal gender reassignment, which subsequently led to freedom (Law and Justice, 2019). There was a case in the US, a former US military intelligence analyst Bradley Manning had a gender-affirming procedure, became a woman called Chelsea, after which she was pardoned and released after seven years in prison instead of a 35-year sentence. Therefore, with the help of stenographic technologies it is possible to achieve correct identification by adhering to the law, regulatory documents.

A study by a group of foreign scientists R.J. Mstafa et al. (2017), who believe that implementation efficiency, concealment ability and reliability are the three main requirements included in any successful steganographic method. Firstly, the effectiveness of implementation can be determined by answering the following questions: how secure is the steganographic method of hiding hidden information inside the carrier object; how accurate are the qualities of the steganograms after the hiding procedure; is it possible to detect a secret message on the steganogram (Hasnaoui & Mitrea, 2014; Mstafa & Elleithy, 2015). In other words, a steganography method is highly effective if it incorporates the characteristics of encryption, imperceptibility and undetectability. It may be added that these requirements need to be applied by law enforcement agencies to successfully identify convicted persons (Qazanfari & Safabakhsh, 2014).

B. Kapila and T. Thind (2021) investigated the need for innovation in the penitentiary system. They argue that innovations in steganography may include the development of better algorithms for hiding data, as well as methods for detecting hidden data. This can help in protecting information from unauthorised access and ensuring data security in today’s world where information is exchanged so quickly and extensively. Moreover, with the use of steganography, data can be hidden inside various media files such as images, audio, or video without significantly increasing their size or degrading their quality. This can be useful in a variety of areas including cybersecurity, confidential communication, research, and more. M. Pelosi and C. Easttom (2021) in their recent study propose the application of certain software in steganography, which is useful as evidence in trials or requests for extradition of initial or additional charges for convicted persons. They argue that steganography has long been used to counter forensic investigations. The use of steganography as an anti-crime forensic technique is becoming increasingly common. These scientists have developed a new software concept that will allow digital forensics specialists to clearly identify and attribute cases that may compromise the integrity, confidentiality of information (AlSabhany et al., 2020; Khakhanovskyi & Hrebenkova, 2022). This methodology is embodied in a software implementation called CounterSteg. CounterSteg software allows detailed analysis and comparison of the original image and any modified image.

Hence, it can be concluded that all the above scholars are right in their statements. Overall, the study of steganography in the legal, criminal field helps to ensure security and law enforcement in the digital age where information can be easily hidden or altered using steganography technologies, including the identification of imprisoned individuals.

Conclusions

Through a comprehensive study of this topic, the following conclusions can be reached. Steganographic technologies in prisoner identification represent an interesting and promising tool that can be used in various areas of law enforcement and security. Steganography as a method of covert transmission of information can be effectively applied to the identification of prisoners. This technology allows data to be embedded in images, sound files or videos, allowing information to be hidden from unauthorised persons. The use of steganography in prisoner identification can help combat illegal information sharing and security threats in prisons and other institutions. Prisoners can use steganography to circumvent control systems and transmit prohibited messages.

Steganography can also be useful in monitoring prisoners' online communications. Prisoners may try to hide information in text messages, photos, and other multimedia data, and the use of steganography can help detect such attempts. However, steganographic technologies can pose a challenge to law enforcement because they make it more difficult to detect hidden information. This requires the development and application of specialised tools and analysis techniques. It is important to comply with legislation and regulations when steganographic techniques are used to identify prisoners. Transparency and respect for human rights should be at the centre of any practices related to the monitoring and identification of prisoners.

The study performed a SWOT analysis of steganographic technology, which helped in identifying the strengths and weaknesses of this technology. Steganographic technology can effectively complement existing identification and control methods in institutions where it is needed. However, they must be used following established procedures and best practices to ensure safety and compliance with the law. Kazakhstan is actively developing its legislative infrastructure, but it is still not improved.

References

Adanbekova, Z., Omarova, A.B., Yermukhametova, S., Assanova, S. & Tynybekov, S. (2022). Features of an electronic transaction as evidence in court. *Revista de Direito, Estado e Telecomunicacoes*, 14(1), 98-112.

AlSabhany, A.A., Ali, A.H., Ridzuan, F., Azni, A.H. & Rosmadi Mokhtar, M. (2020). Digital audio steganography: Systematic review, classification and analysis of the modern state of technology. *Computer Science Review*, 38, 100316.

Altynbassov, B., Myrzatayev, N., Tastekeev, K., Saktaganova, I. & Osmanova, D. (2017). Organizational and legal aspects of fee-based education in the Republic of Kazakhstan. *Journal of Advanced Research in Law and Economics*, 8(7), 2072-2077.

Amirtharajan, R. & Rayappan, J.B.B. (2013). Steganography-time to time: A review. *Research Journal of Information Technology*, 5(2), 53-66.

Ardhianto, E., Warnars, H.L.H.S., Soewito, B., Gaol, F.L. & Abdurachman, E. (2020). Improvement of steganography technique: A survey. In: *Proceedings of the 1st International Multidisciplinary Conference on Education, Technology, and Engineering (IMCETE 2019)* (pp. 289-292). Amsterdam: Atlantis Press. https://www.atlantis-press.com/proceedings/imcete-19/125935468

Article 4 of the Constitution of the Republic of Kazakhstan. (1995). https://constitutionrk.kz/razdel-1/statya-4

Baitursynuly, A. (2022). *Selected works*. Astana: Ministry of Science and Higher Education of the Republic of Kazakhstan, Language Policy Committee. https://abai.institute/assets/pdf/11d25590cf6f0ea7e6c9ed6d2db05f6a.pdf

Basic Principles for the Treatment of Prisoners. (1990). https://www.ohchr.org/en/instruments-mechanisms/instruments/basic-principles-treatment-prisoners

Begaliev, E.N. (2019). On the prospects of integrating steganographic technologies into the structure of individual varieties of material objects. *The Bulletin of the Academy of Law Enforcement Agencies Scientific Journal*, 13(3). https://online.zakon.kz/Document/?doc_id=37137111&pos=8;-118#pos=8;-118

Body of Principles for the Protection of All Persons under Any Form of Detention or Imprisonment. (1988). https://www.ohchr.org/en/instruments-mechanisms/instruments/body-principles-protection-all-persons-under-any-form-detention

Constitution of the Republic of Kazakhstan. (1995). https://www.akorda.kz/ru/official_documents/constitution

Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment. (1984). https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-against-torture-and-other-cruel-inhuman-or-degrading

Convention No. 100 concerning Equal Remuneration for Men and Women Workers for Work of Equal Value. (1951). https://www.un.org/ru/documents/decl_conv/conventions/remuner.shtml

Convention No. 156 on Equal Treatment and Equal Opportunities for Men and Women Workers: Workers with Family Responsibilities. (1981). https://www.ilo.org/wcmsp5/groups/public/---ed_norm/---normes/documents/normativeinstrument/wcms_c156_ru.htm

Convention on the Elimination of all Forms of Discrimination Against Women. (1979). https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-elimination-all-forms-discrimination-against-women

Council of Europe. (2001). Convention on cybercrime. https://rm.coe.int/booklets-bc-2-protocols-guidance-notes-en-2022/1680a6992a

Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power. (1985). https://www.ohchr.org/en/instruments-mechanisms/instruments/declaration-basic-principles-justice-victims-crime-and-abuse

Electronic Oxford English Dictionary. https://www.oed.com/

Fridrich, J. (2009). *Steganography in digital media*. Cambridge: Cambridge University Press. https://assets.cambridge.org/97805211/90190/frontmatter/9780521190190_frontmatter.pdf

Goffman, F.G. (2007). *Conflict in the 21-st century: The rise of hybrid wars*. Arlington: Potomac Institute for Policy Studies. https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf

Gurunath, R., Klaib, M.F.J., Samanta, D. & Khan, M.Z. (2021). Social media and steganography: Use, risks and current status. *IEEE Access*, 9, 153656-153665. https://ieeexplore.ieee.org/abstract/document/9599677

Hasnaoui, M. & Mitrea, M. (2014). Multi-symbol QIM video watermarking. *Signal Processing: Image Communication*, 29(1), 107-127. https://doi.org/10.1016/j.image.2013.07.007

International Convention for the Suppression of the Financing of Terrorism. (1999). https://treaties.un.org/doc/db/terrorism/english-18-11.pdf

International Convention on the Elimination of All Forms of Racial Discrimination. (1965). https://www.ohchr.org/en/instruments-mechanisms/instruments/international-convention-elimination-all-forms-racial

International Covenant on Civil and Political Rights. (1966). https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

International Covenant on Economic, Social and Cultural Rights. (1966). https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-economic-social-and-cultural-rights

Kapila, B. & Thind, T. (2021). Review and analysis of data security using image steganography. In: *2021 2nd International Conference on Computation, Automation and Knowledge Management (ICCAKM)* (pp. 227-231). Dubai: IEEE.

Kassymzhanova, A.A., Tifine, P., Tursunkulova, D.A., Ibrayev, N.S. & Nusipova, L.B. (2021). Political and legal analysis of threats to the national security of the Republic of Kazakhstan in the context of globalization. *Journal of Actual Problems of Jurisprudence*, 99(3), 14-25.

Kessler, G.C. (2004). An overview of steganography for the computer forensics examiner. *Forensic Science Communications*, 6(3), 218688. https://www.ojp.gov/ncjrs/virtual-library/abstracts/overview-steganography-computer-forensics-examiner

Khakhanovskyi, V. & Hrebenkova, M. (2022). Identification, collection, and investigation of electronic imagery as sources of evidence. *Law Journal of the National Academy of Internal Affairs*, 12(4), 28-39.

Kulchytskyi, V. (2023). Role of intellectual property in the development of the state's innovation potential. *Law. Human. Environment*, 14(3), 23-45.

Kulibaev, T.A. (2016). On the actual directions of development of modern criminalistics. In: *Proceedings of the International Scientific and Practical Conference "Aubakir Readings"* (pp. 3-5). Almaty: Almaty Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan.

Kumar, V. & Kumar, D. (2018). A modified DWT-based image steganography technique. *Multimedia Tools and Applications*, 77(11), 13279-13308.

Kurylo, V., Karaman, O., Bader, S., Pochinkova, M. & Stepanenko, V. (2023). Critical thinking as an information security factor in the modern world. *Social and Legal Studios*, 6(3), 76-83.

Law and Justice. (2019). *Chelsea Manning freed from jail for now*. https://www.dw.com/en/chelsea-manning-freed-from-jail-on-contempt-charge-for-now/a-48681869

Law of the Republic of Kazakhstan "On National Security" No. 19-V. (2012). https://www.akorda.kz/ru/security_council/national_security/zakon-respubliki-kazahstan-o-nacionalnoy-bezopasnosti-respubliki-kazahstan

Metelskyi, I. & Kravchuk, M. (2023). Features of cybercrime and its prevalence in Ukraine. *Law, Policy and Security*, 1(1), 18-25.

Mstafa, R.J. & Elleithy, K.M. (2015). A novel video steganography algorithm in the wavelet domain based on the KLT tracking algorithm and BCH codes. In: *2015 Long Island Systems, Applications and Technology* (pp. 1-7). Farmingdale: IEEE.

Mstafa, R.J., Elleithy, K.M. & Abdelfattah, E. (2017). A robust and secure video steganography method in DWT-DCT domains based on multiple object tracking and ECC. *IEEE Access*, 5, 5354-5365.

Muralidharan, T., Cohen, A., Cohen, A. & Nissim, N. (2022). The infinite race between steganography and steganalysis in images. *Signal Processing*, 201, 108711.

Optional Protocol to the Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment. (2002). https://www.ohchr.org/en/instruments-mechanisms/instruments/optional-protocol-convention-against-torture-and-other-cruel

Optional Protocol to the Convention on the Elimination of All Forms of Discrimination against Women. (1999). https://www.ohchr.org/en/instruments-mechanisms/instruments/optional-protocol-convention-elimination-all-forms

Optional Protocol to the International Covenant on Civil and Political Rights. (1966). https://www.ohchr.org/en/instruments-mechanisms/instruments/optional-protocol-international-covenant-civil-and-political

Optional Protocol to the International Covenant on Economic, Social and Cultural Rights. (2008). https://www.ohchr.org/en/instruments-mechanisms/instruments/optional-protocol-international-covenant-economic-social-and

Pelosi, M. & Easttom, C. (2021). Identification of LSB image steganography using cover image comparisons. *Journal of Digital Forensics, Security and Law*, 15, 6.

Poita, Yu. (2020). “Hybrid” threats to national security: Analysis of the legal framework of Kazakhstan. *Kazakhstan-Spectrum*, 94(2), 24-34.

Qazanfari K. & Safabakhsh R. (2014). A new steganography method which preserves histogram: Generalization of LSB^{++}. *Information Sciences*, 277, 90-101.

Saifnazarov, I. & Saifnazarova, F. (2023). Experience in addressing the gender issue in post-Soviet countries. *Social and Legal Studios*, 6(3), 152-161.

Saktaganova, I., Surkova, S., Smatlayev, B., Zhussupov, A. & Abdilov, K. (2023). Effectiveness of human protection from domestic violence under the administrative legislation of the Republic of Kazakhstan. *Rivista di Studi sulla Sostenibilita*, 13(1), 279-294.

Second Optional Protocol to the International Covenant on Civil and Political Rights, Aiming at the Abolition of the Death Penalty. (1989). https://www.ohchr.org/en/instruments-mechanisms/instruments/second-optional-protocol-international-covenant-civil-and

Sharyi, V.I., Samoilenko, L.Y. & Ovcharenko, A.O. (2019). Strategic priorities of states in the black sea region. *Journal of Advanced Research in Law and Economics*, 10(6), 1786-1793.

Shestak, V.A. & Tsyplakova, A.D. (2023). Criminological Features of the Cybersecurity Threats. *Revista de Direito, Estado e Telecomunicacoes*, 15(2), 187-203.

Sopilko, I. & Rapatska, L. (2023). Social-legal foundations of information security of the state, society and individual in Ukraine. *Scientific Journal of the National Academy of Internal Affairs*, 28(1), 44-54.

The Shanghai Convention on Combating Terrorism, Separatism and Extremism. (2001). https://www.refworld.org/pdfid/49f5d9f92.pdf

United Nations Convention Against Transnational Organized Crime and the Protocols Thereto. (2004). https://www.unodc.org/documents/middleeastandnorthafrica/organised-crime/UNITED_NATIONS_CONVENTION_AGAINST_TRANSNATIONAL_ORGANIZED_CRIME_AND_THE_PROTOCOLS_THERETO.pdf

Universal Declaration of Human Rights. (1948). https://www.un.org/ru/documents/decl_conv/declarations/declhr.shtml

Vilks, A., Kipane, A., Kudeikina, I., Palkova, K. & Grasis, J. (2022). Criminological Aspects of Current Cyber Security. *Revista de Direito, Estado e Telecomunicacoes*, 14(2), 94-108.

Volkov, V. (2018). *Head of the Research Institute of Informational Security of Kazakhstan: “National cryptography is an archival issue for the state”.* http://surl.li/oemzd

Warren, I., Mann, M. & Molnar, A. (2020). Lawful illegality: Authorizing extraterritorial police surveillance. *Surveillance & Society*, 18(3), 357-369.