**Universitatea “Alexandru Ioan Cuza” din Ia**ș**i**

Facultatea de Informatică



LUCRARE DE LICENȚĂ

**propusă de**

**Butnaru Vasile-Cristi**

Sesiunea: iunie-iulie,2022

**Coordonator** ș**tiin**ț**ific**

Asist.Dr. Anca-Maria Nica

1

**UNIVERSITATEA “ALEXANDRU IOAN CUZA” DIN IA**Ș**I**

**FACULTATEA DE INFORMATICĂ**

**Image Steganography using sudoku puzzle**

**Butnaru Vasile-Cristi**

Sesiunea: iunie-iulie,2022

**Coordonator** ș**tiin**ț**ific**

Asist.Dr. Anca-Maria Nica

Cuprins

[Contribuții](#page8) [8](#page8)

[**CAPITOLUL 1**](#page9)[**DETALII TEHNICE**](#page9)[**9**](#page9)

[**1.1**](#page9)[**9**](#page9)

[**1.2**](#page10)[**10**](#page10)

[**1.3**](#page12)[**12**](#page12)

[**CAPITOLUL 2**](#page20)[**IMPLEMENTAREA APLICAȚIEI**](#page20)[**20**](#page20)

[**2.1**](#page20)[**Modul de funcționare al aplicației**](#page20)[**20**](#page20)

[**2.2**](#page25)[**Tehnologii folosite**](#page25)[**25**](#page25)

[**CAPITOLUL 3**](#page27)[**CONCLUZII ȘI DIRECȚII VIITOARE**](#page27)[**27**](#page27)

[Bibliografie](#page28) [28](#page28)

Introducere

Steganography is one of the methods used to hide the exchange of information, which can be defined as the study of invisible communication, which usually involves hiding the presence of the transmitted message. That way, if it's successful, the message won't get the attention of the interceptors and attackers. Using steganography, information can be hidden in various embedded environments called carriers. These carriers can be images, audio files, video files, and text files.

In this modern age, computers and the Internet are the main means of communication to connect different parts of the world as a global virtual world. Therefore, people can exchange information easily, and distance is no longer a barrier to communication. However, the safety and security of long distance communication remains an issue. This is especially important in the case of confidential data. The need to address this issue has led to the development of steganography schemes. Steganography is a powerful security tool that provides a high level of security, especially when combined with encryption.

Steganography is different from cryptography. The purpose of cryptography is to secure communications by modifying data in ways that others cannot understand. Steganography, on the other hand, tends to hide the existence of the message itself, making it difficult for the observer to figure out where the message is. In some cases, sending encrypted messages may attract attention, while invisible messages may not. Therefore, cryptography is not the best solution for secure communication; it's just part of the solution. These two sciences can be used together to better protect information. In this case, even if the steganography fails, the message cannot be retrieved because encryption is also used.

As mentioned above, images are considered the most popular file format in steganography. They are known to form causal environments because you access any pixel of the image. In addition, hidden information may remain invisible to the naked eye. However, image steganography will exploit the "holes" in the human visual system.

1.1 Istoria Steganografiei

Throughout history, people hide information in different ways. The word "steganography" actually comes from the Greek and means "covered text". In a short time, researchers have used it in thousands of different ways. In the 5th century BC, the Greek tyrant Histiaus was captured by King Darius at Susa. Histiaeus had to send an esoteric message to his son-in-law in Miletus, Aristagoras, and to do so, Histiaeus shaved the head of a slave and tattooed his message on his scalp. Once the slave's hair was long enough to hide the tattoo, he was sent to Miletus. In ancient Greece, another method was to remove the wax from the wax tablet, then write the message and apply the wax again. The person responsible for receiving the information simply has to remove the wax from the tablet to see the information. This is invisible ink. Another popular form of steganography.

The ancient Romans were able to write between the lines using invisible ink and substances such as juice, urine and milk. Using invisible, albeit seemingly harmless, ink, a letter can reflect very different information written between the lines. Even invisible ink has been used recently, as in World War II. In addition to invisible ink, the Germans also used Microdot technology during World War II. The information, especially the photos, is too small to be found. In 1550, the Italian mathematician Jerome Cardan proposed a secret writing scheme using a perforated paper mask. The user of these papers is forced to write his secret message in these holes after placing the mask on a blank sheet of paper.

The next step is to remove the mask to fill in the blanks on the page so that the message appears as harmless text. This technique, steganography, is now widely used to computerize digital data files, as the carrier and network are considered high-speed forwarding channels. The following sections describe the classification of image file steganography, including an overview of the most important digital imaging steganography techniques.

1.2 The Origins

Traces of steganography already existed in ancient Greece, when Herodotus gave two examples in his stories, but the first recorded use of the term was in 1499 by Johannes Tritermius (Johannes Trithemius in Steganographia, a treatise on cryptography and steganography, disguised as a The author initially decided not to print and even destroyed much of the content, arguing that it should not see the light of day, but the text continued to circulate as a provisional draft and was published posthumously in 1606. Many people throughout history have used this technique to send messages securely, for example, it was known that spy women used knitwear to send messages during both world wars, possibly by making irregular seams or deliberately leaving a hole in material.

1.3 Steganography technique

In steganography, there are two types of messages: the first are "containers" of messages, and the second are secret messages, in which the task of one is to hide the contents of the other so that it can not be seen by anyone who has ears to it. . Often, hidden messages appear to be (or belong to) something else: an image, article, list, or other cover text. For example, hidden information can be invisible ink between rows of private letters. In essence, there are two main models of steganography: injection steganography and generative steganography.

Injection staging is the most commonly used and involves the introduction (injection) of a secret message into another message that acts as a container so that it is invisible to the human eye and virtually indistinguishable from the original message. The generation phase involves taking the secret message and building a suitable container around it so that you can optimally hide it.

From a technological point of view, replacement is undoubtedly the most common, so much so that when we talk about steganography, we often refer implicitly to this model. It can be seen that this technique is based on the fact that most communication channels (telephone lines, radio transmissions, etc.) carry signals that are always accompanied by some kind of noise. This noise can be replaced by a signal - the secret message - which has been transformed so that, if you do not know a secret key, it is indistinguishable from the real noise and can therefore be used without raising suspicions of spreading the case.

1.4 Modern Steganography

In 1985, personal computers began to be used for classic steganography applications. Subsequent development has been quite slow, but today there is an abundance of steganography software. As a form of secrecy, steganographic algorithms differ from cryptographic algorithms in that the plausible form of the data generated must be considered to avoid suspicion. In digital steganography, electronic communications may include layered steganographic encoding, such as document files, image files, programs, or protocols. Multimedia files are very suitable for steganographic transfer due to their large size. For example, a sender might send a harmless image file and adjust the color by one hundredth of a pixel to match the alphabetic characters.

So today, steganography is an ideal tool for creating secret communication channels for espionage, cybercrime and complex scenarios in which the privacy of public and private subjects is violated.

**2 Steganography Techniques**

2.1 Linguistic Steganography

Linguistic technique is used to hide the message inside the cover text

In an obvious way, the presence of the message is imperceptible to a stranger. It is divided into two types:

A) Semagrams: use only symbols and signs to hide

information. Moreover, it is classified in two ways:

i) Visual Semagrams: Physically used visual semagrams used every day to convey a message. For example: positioning articles on a specific website.

ii) Text Semagrams: This type is used to hide a message by changing the look of the wearer's text or changing the font size and type, or by adding extra space between words and using various flowery letters or handwritten text.