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

# Facultatea de Informatică



## LUCRARE DE LICENȚĂ

**propusă de**

**Butnaru Vasile-Cristi**

Sesiunea: iunie-iulie,2023

**Coordonator** ș**tiin**ț**ific**

Asist.Dr. Anca-Maria Nica

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

**FACULTATEA DE INFORMATICĂ**

Steganography

## Butnaru Vasile-Cristi

Sesiunea: iunie-iulie,2023

**Coordonator** ș**tiin**ț**ific** Asist.Dr. Anca-Maria Nica

# Cuprins

# 1. Introduction

# - description of the field (many bibliographic references)

# -History

# -motivation

# - Staged evolution from a scientific point of view (improvements)

# - brief description of the chapters (problems, future directions)

# 2. Technologies used/Theoretical concepts

# - the IT part (libraries, languages, links)

# - theoretical concepts (formulas, definitions)

# 3. Description of the contribution

# -relevant pieces of code.

# - description with printscreen of the application

# 4. Conclusions

# REFERENCES

Introduction

What is steganography?

Steganography means hiding a message in different forms of data, such as: image, video, sound, etc. An important aspect that after hiding the secret message in the file given for insertion is that the modification of the file is not visible. A characteristic of steganography is that the steganographic information is never obvious to the user.

With the expansion in digital-communication technologies and the rapid growth of network bandwidth, the Internet has turned out to be a commonly used channel for transmitting many documents—for instance, audio, video, image, and text—in digital form. Many practices have been offered and developed for providing the secure transmission of data. The focus of the current research is on the design of data-hiding techniques used for transmitting secret data where digital images are selected as the cover-media. This chapter has identified the problems in the present image-steganography schemes.

The term steganography is often confused with cryptography due to some mutual similarities. Nonetheless, they differ from each other on many grounds. Cryptography changes the data shape to maintain secure communication; thus, intruders fail to understand the data. Conversely, steganography methods tend to hide the presence of the data, thus making it impossible for spies to read and steal the private embedded information. In some circumstances, transmitting encrypted data may be more vulnerable, whereas hidden message are not. Thus, cryptography is not the only or best solution to secure information from external threats (Abdul-mahdi et al., 2013)

**History**

From the point of view of history, the first to use steganography were the Egyptians, through the use of hielographs. Hyeloglyphs are characters instead of images. They were also used as a secret form of writing messages so that only those who knew them could read them correctly. This is also the great advantage in using steganography.

Those who used steganography differently are the Chinese who carried information through messengers. More precisely, a piece of silk where the message was written so that later that silk would be rolled on a piece of wax ball and transported by a person to the destination.

Steganography's origins may be traced back to prehistoric times. The Greek historian Herodotus recorded one of the oldest known examples of steganography in Histories, when a message was tattooed on a slave's shaved head and then allowed to regenerate before being transmitted. The message was hidden until the receiver shaved the slave's head and uncovered the hidden message. During Emperor Augustus' reign, the Roman poet Ovid described a type of steganography known as "nulla figura," which involves concealing secret messages within the spacing and arrangement of characters in a text. Steganography evolved during the medieval and Renaissance periods. The usage of invisible inks during the Renaissance is one prominent example. These inks were created by combining ingredients such as milk, lemon juice, or alum, which became visible when exposed to particular chemicals or heat. Giambattista della Porta, an Italian philosopher and physicist, authored "De Furtivis Literarum Notis" (On the Secret Notations of Letters) in the 16th century. Invisible inks and secret writing were among the techniques outlined in the book for hiding information. The creation of microdots in the 18th century was a significant advancement in steganography. Microdots are tiny photos or papers that carry highly compressed data. During WWII, spy organizations utilized them to bury signals within seemingly innocuous things such as postage stamps or letters. Steganography has evolved with the introduction of digital technologies. Steganography in the digital environment is embedding hidden information into digital assets such as photographs, audio files, or movies. This can be accomplished by modifying the file's least significant bits or by employing more complex techniques such as spread spectrum modulation.

In many areas, there is less need for people to write down what people say. With the ability to record audio, which could be done right away and was easy to share, stenography started to be done by machines and combined with other jobs. In the past, it was common for secretaries to know some form of shorthand. Today, however, many secretaries can get by with computers and touch type. Email has also cut down on the need for short lines by making long-distance contact easier. In the past, a boss might have asked a secretary to write down what they were saying and send it to someone else. Now, the vast majority of managers just say what they are thinking out loud.

Still, stenography is still the best choice in some areas. Legal processes, for example, need these kinds of written records. Most court systems are built around rules and past decisions, which are often written down. Lawyers, judges, and clients have to deal with complicated legal codes. While binders full of hundreds of pages of proof might seem strange to some, this kind of paperwork is useful. For a fight between two or more people to be fair, they have to agree on a set of rules. This is true in both games and arguments. Having written papers as the basis of a court system gives everyone a fair chance. And while audio files may be easier to record, they are usually harder to find than text files. In court, both big and small details can be just as important.

This need is met by court writers, who write down what is said during trials and other hearings. Most use stenotypes, which are word machines with keys that can be used to represent more than one letter. As with other shorthand methods, you need special training to use a stenotype. However, unlike most typists who are tied to a keyboard, stenographers can keep up with busy talks while using a stenotype.

Shorthand is also used in the field of medicine. Due to how hard the job is, the formal names of diseases and their cures are often long. The human body is difficult, so it shouldn't be a wonder that there are many ways it can get hurt or break down. Most of the time, doctors and nurses use shorthand to talk about illnesses and to write prescriptions. This saves time in an area where a few seconds can mean the difference between life and death, though the risks are not always so high.

Shorthand is a way to communicate. Even though newer tools have taken its place in most areas, it looks like stenography will still be used for the near future in a few. Those who are well-suited to their niches, whether they are natural or professional, tend to do well in them.

**Stegonography nowdays**

A novel image steganography technique in order to hide the ciphered voice data has been suggested in this work. The doctor's voice comments belonging to a coronavirus disease 2019 (COVID-19) patient are hidden in a medical image in order to protect the patient information. The introduced steganography technique is based on chaos theory. Firstly, the voice comments of the doctor are converted to an image and secondly, they are ciphered utilizing the suggested encryption algorithm based on a chaotic system. Then, they are embedded into the cover medical image.

A lung angiography dual-energy computed tomography (CT) scan of a COVID-19 patient is used as a cover object. Numerical and security analyses of steganography method have been performed in MATLAB environment. The similarity metrics are calculated for R, G, B components of cover image and stego image as visual quality analysis metrics to examine the performance of the introduced steganography procedure. For a 512 × 512 pixel cover image, SSIM values are obtained as 0.8337, 0.7926, and 0.9273 for R, G, B components, respectively. Moreover, security analyses which are differential attack, histogram, information entropy, correlation of neighboring pixels and the initial condition sensitivity are carried out. The information entropy is calculated as 7.9993 bits utilizing the suggested steganography scheme. The mean value of the ten UACI and NPCR values are obtained as 33.5688% and 99.8069%, respectively. The results of security analysis have revealed that the presented steganography procedure is able to resist statistical attacks and the chaotic system-based steganography scheme shows the characteristics of the sensitive dependence on the initial condition and the secret key. The proposed steganography method which is based on a chaotic system has superior performance in terms of being robust against differential attack and hiding encrypted voice comments of the doctor. Moreover, the introduced algorithm is also resistant against exhaustive, known plaintext, and chosen plaintext attacks.

**Sudoku**

Introduction:

Sudoku, a popular number puzzle, has captured the attention of millions worldwide with its captivating combination of logic and mathematical reasoning. In this essay, we delve into the intricacies of Sudoku, exploring its origins, rules, solving strategies, and the reasons behind its enduring appeal. Join us on this exciting journey as we unravel the mysteries of this captivating game.

Origins and Rules of Sudoku:

The origins of Sudoku can be traced back to 18th century Switzerland, although similar number placement puzzles were found in ancient cultures. The modern version gained popularity in the late 20th century, thanks to Japanese publisher Nikoli, who introduced it as "Sudoku" in 1984. The game consists of a 9x9 grid divided into nine 3x3 boxes. The objective is to fill each cell with a number from 1 to 9, ensuring that each row, column, and box contains all nine digits without repetition.

Logic behind Sudoku:

Solving a Sudoku puzzle requires a logical approach, devoid of guesswork. The key lies in applying deductive reasoning and elimination techniques. Players start with a partially filled grid and use the given numbers as clues to fill in the remaining cells. The first step involves identifying cells with only one possible number. Then, techniques like "elimination," "only choice," and "naked/hidden subsets" are employed to uncover additional numbers based on the constraints of rows, columns, and boxes.

Solving Strategies:

Various solving strategies exist to tackle Sudoku puzzles of different difficulties. The "cross-hatching" technique involves scanning rows and columns to identify missing numbers, while "pencil marking" involves using small notations in cells to keep track of potential candidates. More advanced techniques include "X-wing," "swordfish," and "XY-wing," which

utilize patterns and logical deductions to solve complex puzzles. The most challenging Sudoku puzzles often require a combination of these strategies and a sharp analytical mindset.

Benefits and Appeal:

Sudoku offers a multitude of benefits beyond mere entertainment. Its puzzles serve as excellent brain exercises, sharpening critical thinking skills, logical reasoning, and concentration. Playing Sudoku regularly can improve problem-solving abilities and memory retention. Additionally, the game provides a sense of accomplishment and satisfaction as players conquer progressively difficult puzzles, fostering a desire for continuous improvement.

Variations and Adaptations:

Over time, Sudoku has evolved to include various adaptations and variations. These include different grid sizes, such as 4x4 and 6x6, as well as unconventional shapes like irregular and overlapping grids. Additionally, themed Sudoku puzzles incorporate letters, symbols, or pictures, adding an extra layer of challenge and creativity to the game. Online platforms, mobile apps, and Sudoku competitions have further popularized the game, allowing enthusiasts to indulge in their passion and compete with fellow Sudoku aficionados worldwide.

Conclusion:

Sudoku, with its blend of logic, pattern recognition, and deductive reasoning, has captivated puzzle enthusiasts globally. Its origins, rules, logical strategies, and inherent benefits make it a highly engaging and mentally stimulating game. The enduring appeal of Sudoku lies in its ability to challenge and entertain players of all ages, fostering a love for logical problem-solving. So, pick up a Sudoku puzzle and embark on this fascinating journey, where numbers align, and puzzles unravel with the power of your mind.

**Types of steganography**

Various techniques or actions are used in hiding the message, which are analyzed throughout the process. Steganography has 6 categories:

- Cover generation technique

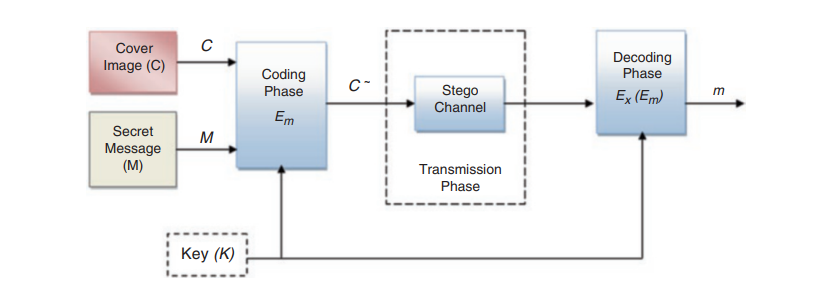
- Replacement system technique

- Domain transformation techniques

- Statistical spectrum techniques

- Distortion technique

Steganographic system model



What does the work propose

# This paper proposes hiding a text message using the sudoku game solution.

# Specifically the sudoku game with 9 rows and 9 columns. First, the desired message for insertion is converted to base 9.

# Then a solved 9X9 sudoku is generated and the values, inside it are decremented by 1 as we see below in image 1.

# The Sudoku solution is transformed into a reference matrix (image 2)

# 

# 

# 

# Image 1

# Image 2

# Cum ascundem mesajul în imagine

# 

# The secret message will be text type received as input data, after which it will be read to you. By means of a function it will be converted from text to decimal and then from decimal to base 9. The following message will be a list of numbers in base 9 of the form S= s1, s2, s3, ....

# After the image is opened, the pixels of that image will be extracted and put into a list one row at a time. The list will be of the form:

# Pixels= [ R1, G1, B1, R2, G2, ....]

# Items in the pixel list will also be converted to base 9.

# They start by taking 2 pairs of values, from the pixel list (R1,G1), (B1, R2). The value 9 is added to each value in the pair to ensure that we are in the middle of the reference matrix. The chosen pair will be the values, for the X axis and the Y axis in the reference matrix. After the center is determined, 3 chosen candidate elements vertically, horizontally and the box will be calculated. All these candidate elements will contain 9 distinct elements.

# CEH – elementul candidat orizontal

# CEV – elementul canditat vertical

# CEB – elementul canditat casuța

# 

# How data is extracted from the image

# The image is made up of RGB pixels (R for red, G for green and B for blue). We convert the image into pixels and form a list of pixel values (R1, G1, B1, R2, B2......). after which we select a pair of 2 values.

# Ex: (R1, B1), (B1, R2) and so on.

# The value pair is converted to base 9.

# Pi.x =Ci.x % 9, Pi.y = Ci.y % 9

# We take these pixels as the guide axes for the reference matrix used in hiding the message. Pi.x becomes the row and Pi.y becomes the column for the matrix M (the reference matrix).

# Value found at location M[Pi.x][Pi.y] represents our secret message. This represents only a fragment of the secret message, we must select the next pair of values to be able to extract the complete message. The method for extracting the message is called "Least significant byte" (LSB).

# We have to take into account that in the first 10 pairs, after the extraction we will find out the length of the secret message that we have to extract later.

# In this paper we have proposed the revised version of. În earlier work only the RED & GREEN components of cover image pixel were used. So embedding capacity was 3 bits per pixel and reference matrix used was of order 27 X 27. În proposed system, before embedding the secret data is compressed and encrypted so that more and variable digital media are shared with more security. Since RED, GREEN & BLUE components of cover image pixel are used, the embedding capacity per pixel is 4.5 bits.

# Thereference matrix used is of order 9 X 9. By using reference matrix, candidate elements (CEH, CEV, CEB) are chosen in such way that less distortion is produced in cover image after embedding the data. In previous system only one type of digital media was embedded in single cover image. But in proposed system multiple digital media can be embedded in single cover image. System provides two layer security one by using a random Sudoku among 6.671x1021 possible solutions and other by using strong encryption algorithm. The proposed system can be used in the fields where more priority is given to security instead of amount of data shared. So this can be used in wide range of applications like military, medical imaging, banking etc. Stego image generated holds more data and is less distorte compared to other proposed system. Stego images are in lossless format and less space for stego images can be obtained if this method is extended for stego images in loss format.

Types of steganography

Steganography uses various techniques to hide information and thus can be divided into multiple categories:

* Text steganography – this type hides the secret message inside any piece of text which can be sent to the desired recipient without anyone other than the participants even knowing that a secret is concealed within that piece of text.
* Image steganography – this type hides the secret message within any selected picture, by encoding the information that we want to send secretly in the pixels of the image. The picture containing the secret message exactly matches the initial image so that anyone intercepting it will not realize that a message is hidden within it.
* Video steganography – this type hides pieces of secret information inside videos. This category is becoming more popular in the last years because of its power. Because of the complexity of videos, the capacity for encoding secret messages throughout the video is increased.
* Audio steganography – this type hides the secret message inside an audio file, modifying it to encode the desired piece of information within it. This process is not detectible, the original sound is identic with the modified one.
* Network steganography – this type uses common network protocols (e.g., TCP/IP protocol suite) to hide the secret message. This technique can conceal information within the payload, the header or both.

# **Bibliography**

# - https://pubmed.ncbi.nlm.nih.gov/34316095/

<https://www.crime-research.org/articles/Stegano26/>

[https://www.telsy.com/steganography-from-its-origins-to-the-present/#:~:text=The%20origins,as%20a%20book%20about%20magic](https://www.telsy.com/steganography-from-its-origins-to-the-present/" \l ":~:text=The origins,as a book about magic).

<https://moosmosis.org/2020/06/15/an-overview-of-shorthand-history-and-types-of-shorthand/>

<http://ijses.com/wp-content/uploads/2021/03/117-IJSES-V4N12.pdf>

https://www.ukessays.com/essays/english-language/background-of-steganography.php