licenta

de Cristi Butnaru

Data depunerii: 21-iun.-2023 04:56AM (UTC+0200)
ID-ul depunerii: 2120058648
Numele fişierului: Steganography.pdf (908.16K)
Numărul cuvintelor: 7674
Numărul caracterelor: 41133

Universitatea “Alexandru Ioan Cuza” din Iași
Facultatea de Informatică

LUCRARE DE LICENȚĂ

propusă de

Butnaru Vasile-Cristi

Sesiunea: iunie-iulie,2023

Coordonator științific

Asist.Dr. Anca-Maria Nica

27
UNIVERSITATEA "ALEXANDRU IOAN CUZA" DIN IAȘI

FACULTATEA DE INFORMATICĂ

Steganography

Butnaru Vasile-Cristi

Sesiunea: iunie-iulie,2023

Coordonator științific 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)

1. Introduction

With the growth in exchange of digital data through network, the security of data became a matter of concern across the globe. The distribution of digital data raised a concern as the data are attacked and manipulated by unauthorized person. The Internet provides a method of communication to distribute information and thus approach of hiding secret message in different multimedia is increased [1]. Data hiding techniques are increasing day by day with more effective approach. Steganography is a data hiding technique aiming to transmit a message on a channel, where some other information is already being transmitted. The goal of steganography is to hide messages inside digital media in order to avoid drawing suspicion of the hidden data from a third party. It includes a vast array of secret communications methods that conceal the message's very existence [2].

Steganography does not alter the structure of the secret message, but hides it inside a medium so it can't be seen The technique replaces unused or redundant bits of the digital media with the secret data. The redundant bits are those bits that can be altered without drawing suspicion. The concept is to embed the hidden object into a significantly larger object so that the change is undetectable by the human eye. The security of the steganography depends on the data encoding system. Once the encoding system is known, the steganography system is defeated. Steganography programs allow the user to select a carrier that they wish to use as the vector to carry the hidden data [3]. All digital file formats can be used for steganography, but those formats that have a high degree of redundancy is more suitable. The digital media which are used for secret communication includes text, images, audio and videos which provide excellent carriers for hidden information. The most popular cover objects used for steganography are digital images. Digital images often have a large amount of redundancy data, and this is what steganography uses to hide the messages. A steganographic system involves two parties, the sender who encodes the secret message in the cover medium and the receiver who extracts the message from the cover. Steganography has mainly applicable in the field of computer security, cybersecurity, digital forensics, copyright protection, feature tagging, secret communication, watermarking, intelligence agencies, military agencies, etc.

The most important requirements for steganographic system are the security (undetectable) and capacity [1]. As steganography is emerging increasingly in the field of data protection methods, simultaneously techniques of detecting secret data inside digital file are also emerging. The security of a steganographic system is defined by its ability to overcome attacks. The attacks are based on the statistical and structural image file properties. The method to detect the presence of steganography is called steganalysis. Most steganographic techniques involve changing properties of the cover source and there are several ways of detecting these changes. While steganography deals hiding secret data, the role of steganalysis is to detect and estimate hidden data inside digital file from observed data with little or no knowledge about the steganography method and/or its parameters.

1

There exist several steganographic techniques to embed data securely in a carrier medium and tools to detect reliably the presence of any secret message in a steganogram. Steganographic technique consists of embedding and extracting mechanism. Image-based steganographic techniques can be classified into two categories: spatial domain and frequency (transform) domain.

A secret message is generally considered as an encrypted data, where bits of encrypted message are embedded in pixels of the cover image. The trivial steganography technique is based on the least significant bit (LSB) substitution in which the LSB of the pixels is modified to embed the secret message. In the spatial domain, this type of techniques can be broadly classified into two categories: LSB replacement and LSB matching. In case of LSB replacement [2, 3], the least significant bit of each pixel of the cover image is replaced by the next bit of the secret message to be embedded. In LSB matching [4], if there is a mismatch between least significant bit of a byte in the cover image and next bit of the secret message to be embedded, then embedding, in general, is done by increasing or decreasing randomly the content of the byte of the cover image by 1, except at the boundary values. In some techniques, the decision to increase or decrease the content of a byte is governed by the score of the distortion function [5]. Embedding in two least significant bits is an extension of LSB replacement. There are multiple ways to embed data by flipping the least and the second least bits of a cover image [6].

In case of transform domain, the LSB-based embedding is done by modifying the LSB of non-zero DCT coefficients of a cover image. There exist several ways to embed data in transform domain such as modification of quantization table, heuristic based, utilizing non-shared selection, and side information at sender side [7].

Steganalysis tools track the distortion caused during the data embedding to detect the presence of the secret message in an image. These tools are classified as visual, structural, and non-structural [8, 9]. Visual steganalysis attacks analyze images for some distortions which are visible to human vision system. The distortions could be visible in stego image or in LSB plane extracted from the stego image. Structural attacks analyze structural properties of an image to find any anomaly which are introduced by steganography. Structural detectors such as histogram attack [10], sample pair analysis (SPA) [11], RS method [12], and weighted stego [13] can reliably detect presence of stego data and even estimate message length. Non-structural detectors use feature extractors to model cover image and to compute distortion between the cover and the stego image to detect embedding. A classifier is trained by the feature set from large number of stego and cover images. During training, the classifier learns the differences in features, and this learning is used to classify a fresh image into stego or clean image. Non-structural detectors such as subtractive pixel adjacency matrix (SPAM) [14] and spatial-rich model (SRM) [15] claim better probability of detection of embedding in a stego image. Features based on steganalysis techniques use support vector machine (SVM) or ensemble classifiers [16] for supervised learning. SVM is not suitable for any high-dimension feature vector, while this is not the case with ensemble classifier but its performance is comparable to SVM.

Most of the current steganography techniques are based on model-preserving principles. These techniques are designed by finding a model for cover images, and embedding modifications are done in such a way that this model is preserved. Highly undetectable stego (HUGO) [5], ASO [17], universal wavelet relative distortion (UNIWARD) [18], and maximum mean discrepancy (MMD) [19] are designed on this principle. HUGO preserves features used by SPAM for steganalysis, thus preserving features space model. Similarly, UNIWARD preserves a wavelet-based model, while MMD preserves parametric-based model. Generally, these techniques embed

message by minimizing a defined embedding distortion function heuristically. But, in [20], a non-heuristic distortion function is used to preserve the Kullback Leibler distance.

In [21], an embedding technique, known as pixel value difference technique (PVD) has been proposed. In this technique, the image is divided into non-overlapping blocks of adjacent pixels which are randomly selected, and data is embedded into each of its pixels. The amount of data embedded, i.e., the number of last significant bits used, is directly proportional to the differences in the intensities of adjacent pixels. This uneven embedding in PVD leads to unusual steps in the histogram of pixel difference in the stego image. An improved technique (IPVD), proposed in [22], has exploited this vulnerability. Adaptive edge LSB technique (AE-LSB) [23] has also removed this uneven pixel difference by introducing a readjusting phase and has provided better capacity. All these techniques are edge adaptive in a way that they can embed more data where pixel difference is high but they have one fundamental limitation. These techniques consider pixel pair at random, rather than selecting on the basis of higher differences. So, they may end up by embedding data at random places in the image and by distorting the texture in LSB plane of the image. Performance of these techniques are found to be poor [24].

In hiding behind corners (HBC) [25]b technique, corner pixels are used to contain hidden data. Data is embedded by using simple LSB substitution. Such embedding leads to many structural asymmetries and could easily be detected by structural steganalysis tools like chi-square [10], sample pair analysis (SP) [26], and weighted stego (WS) [27]. Thus, the HBC technique which maintains texture in LSB plane, offers poor security.

Edge adaptive image steganography (EALMR) [24] technique is based on LSB matching revisited (LSBMR) [3] technique which alleviates some of the above said limitations. EALMR calculates the difference between two adjacent pixels. If this difference is greater than a pre-defined threshold, then both pixels are marked as edge pixels, and one bit of data is hidden in each of them using LSBMR. This technique has some limitations. Difference of intensities of adjacent pixels may not be an edge point; any such technique may embed data in smoother parts even though there are some unused prominent edges. So, any well-known edge detection algorithm can be used to find edge pixels and to hide data in the detected edges. Further, since EALMR compares a pixel with its adjacent pixel, it can find edges only in one direction. To overcome this limitation, an image can be divided into some non-overlapping but equal size

blocks, and each block is rotated in the range of set {0°, 90°, 180°, 270°} to see edge pixels in more than one direction inside a given block. But, poor edge selection results in detection by steganalysis tools like targeted attack [28] and blind attacks SPAM [14] and SRM [15].

In [5], HUGO steganographic technique is presented. Its design is derived from the image model obtained from the feature set of SPAM steganalyzer. It is based on the minimum-embedding impact principle, where embedding is done in such a way that the distortion in a stego image is minimum. It preserves a model utilized by SPAM steganalyzer to derive steganalytic features in such a way that it does not over-fit to a SPAM feature set. Dimensionality of the feature set has been tremendously enhanced so that the technique is not detectable by minor modification in SPAM steganalyzer. Instead of using Markov transition matrix to compute SPAM features, co-occurrence matrix is used to derive those features. But, it may have minor degradation in performance. Detectable parts of the model are identified by Fisher linear discriminant (FLD criteria) [29]. It rates individual features' importance for embedding changes. The parts of the model not vulnerable to embedding changes are identified using criteria optimized in FLD. In [30], it is shown that HUGO is vulnerable against steganalysis that uses other models drawn from different domains.

In [31], embedding distortion cost is computed through directional residual obtained using Daubechies wavelet filter bank [32]. The objective is to limit the embedding changes to those parts of the cover image that are difficult to model in multiple directions. Embedding is done in textures or noisy parts and avoiding smooth regions and clean edges of empirical cover images. Distortion function, called as UNIWARD [31], is used to compute delectability map. Syndrome trellis code (STC) [33] and detectability map are used to embed payload while minimizing the embedding distortion. The same distortion design technique can be used for spatial and transform domains.

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.

COMPARISON OF WATERMARKING, STEGANOGRAPHY, AND CRYPTOGRAPHY

Cryptography and watermarking are the two methods of data concealment. The secret

message is encrypted and delivered in an unintelligent format using the cryptography technology. Cryptography scrambles the data, but Steganography only conceals the data. This is the fundamental distinction between the two. The confidential data is scrambled using cryptography so that any unauthorized user would only be able to decipher nonsense. Due to the permutation and substitution used in the secret data to be transmitted, any unauthorized user cannot receive the message.

Cryptography is distinct from steganography. While cryptography encrypts the data, steganography mostly conceals it. Steganography offers significantly more security than cryptography since there is no chance that an unauthorized user will be aware that a message is being conveyed, but there will always be a suspicion with cryptography. This makes them more vulnerable to hacking or suppression.

Authentication and copyright protection are the two main purposes of watermarking. A watermark can be added to an image to make it more recognized. Additionally, it may be used to label a digital file to indicate whether it is meant to be seen by others (visible watermarking) or only by the author (invisible marking). Watermarking is primarily used to stop unauthorized copying and ownership claims of digital assets.

STEGANOGRAPHY, CRYPTOGRAPHY, AND WATERMARKING CHARACTERISTICS

Steganography, cryptography, and watermarking all communicate secret information in a way that only the recipient is able to decipher the data; this is their shared trait. These methods, which were used in antiquity, have been applied in the digital era. The hidden messages are now almost hard to extract or find. Steganography and watermarking are closely related in the digital realm and are mostly utilized in digital photographs. These can also be used in various ways. Both require cover objects since they are unable to exist on their own. Watermarking requires a carrier item that it is designed to protect, whereas steganography requires a cover media to transport the hidden information. Since they are connected by their commonalities, certain alterations may be necessary to go from one approach to another. Due to the similarities between them, it might be challenging to tell them apart, yet there is a notable difference between them. Data is encrypted using cryptography in one of two ways: safe or unbreakable (such as one-time pad) systems, or breakable (such as RSA) systems. Everyone is aware of the communication that is conducted through both platforms. But deciphering codes takes a long time and is sometimes unsuccessful.

The robustness of the code is determined by the challenges encountered while trying to reverse it in various permutations and combinations. It is utilized for security because of its sturdiness. For example, internet banking, shopping, and other activities all employ cryptography. The credit card number, expiration date, and other vital details are encrypted and transferred to prevent unauthorized access.

Steganography enables a large carrier capacity while retaining the faithfulness of the cover media and the secrecy of the embedded message. The effectiveness of the steganographic approach is that a media file shouldn't have been altered in order to be embedded without the user being aware of it. The Steganographic approach is rendered ineffective if the malevolent person is aware of any alterations. Because the hidden message is so delicate, the entire secret message is damaged if the stego picture is changed. The success of a strategy depends on its capacity to deceive an unexpected user. There may be several levels of communication. A digital picture can include a hidden message that can then be inserted in other digital media or video clips.

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.

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.

Text steganography

In the year 500 BC, in ancient Greece one of the first use of steganography was documented. Histiaeus, a Greek despot was the ruler of an area of Ionia named Miletus, under the Persian King, Darius the Great. Because he has proven himself to be wise and faithful in previous combats, Darius decided to make Histiaeus his personal advisor. However, Histiaeus had other plans. He was plotting to betray the king and take Ionia for himself with the help of his nephew, Aristagoras. In order to do this, he needed to send a message to Aristagoras, who was still living in Miletus. The message needed to be secret, since it contained the instruction to his nephew to instigate the Greek people to riot against the Persians stationed in Miletus. The method that he used to conceal the secret message was to shave one of his slaves' head and tattoo the message on it. When the hair grew back, the tattoo could not be seen, and the message could be delivered secretly. This example shows that even from ancient times, people have used resourceful methods of concealing messages and ensuring secret communication between parties.

In more recent times, intelligence agencies used steganography to gain advantages in warfare by communicating in secret. One of the methods used was Microdot, which consisted in drastically reducing the size of the text and inserting it in another text or image to prevent it from being detected. Although this method was extensively used by the Germans and the French in World War II, the Soviet agent Alexander Foote claimed in his book, "Handbook for Spies", that Microdots were used before World War II by the Soviet intelligence service.

In the current context of digitalization and the continuous development of web applications, text steganography was also heavily influenced it needed to be adapted.

We can classify test steganography into 3 categories:

-Format-based method

-Linguistic method

-Random and statistical generation method

1. Format-based method

This form of steganography is based upon the fact that the human eye cannot detect the differences of a text's features if they are designed in a specific way. For example, we can change the physical features of text symbols by moving some lines up and down in order to hide information. Then we can slightly change the position of the words or encode data by creating a pattern from white spaces between words or the spaces between paragraphs. We can also rely on the symbols of a language to encode messages by modifying physical features of words, practice called feature-based encoding. Naharuddin, Wibawa and Sumpeno propose in their publication "A high capacity and imperceptible text steganography using binary digit mapping on ASCII characters" [aici pui referinta la asta] a model that maps the binary digits of the secret message with the binary digits of the cover text using the American Standard Code for Information Interchange (ASCII) characters. In the paper "A high capacity text steganography scheme based on permutation and color coding" [aici referinta la aici] two approaches are used, permutation and numeration systems, to offer a method based on color coding.

2. Linguistic method

This method hides secret information inside text files. The author of "Topic-aware Neural Linguistic Steganography Based on Knowledge Graphs" [referinta la asta] proposed a model that is topic-aware and neural-linguistic that also follows the Encoder-Decoder architecture. It uses a topic-specific knowledge graph (KG) and the bitstream of the secret message to encode it in text. Another technique that uses Adaptive Dynamic Grouping (ADG) to recursively embed secret information was suggested in "Provably Secure Generative Linguistic Steganography" [referinta la asta]. This method dynamically groups tokens according to their probability in their semantic context, thus ensuring that the generated steganographic text has increased undetectability.

3. Random and Statistical Generation

This technique is based on statistically analyzing a language and its characteristics and using them to generate cover text. Markov Chains models can be used to calculate the transition

probability between words, as demonstrated in “STBS-Stega: Coverless text steganography based on state transition-binary sequence” [referinta la asta], thus improving the quality of the generated cover text. An improved method is described in “Automatically Generate Steganographic Text Based on Markov Model and Huffman Coding” [referinta la asta] which uses Hoffman coding in addition to Markov Chains to automatically generate steganographic text.

3. Image Steganography

3.1 Transform Domain Based Steganographic Techniques

Transform domain based steganography techniques take advantage of Discrete Cosine Transformation (DCT) used in the JPEG compression process [2]. In transform domain technique image is first transformed into the frequency domain and then the message is embedded in the discrete coefficients and finally the inverse transform is performed to restore the image. JPEG is a lossy digital image compression system which reduces image‘s file size to a great extent. Firstly, an image is converted to a YUV representation space, breaks up each color plane into 8 x 8 blocks of pixels blocks and then each of these 8 x 8 pixel blocks are transformed into an array of 64 DCT coefficients [4]. Next a quantizer rounds each of these coefficients. Then an array of streamlined coefficients is formed, which are further compressed via a Huffman encoding scheme or similar. The quantized DCT coefficients are then used to embed hidden message

3.2 Spatial Domain Based Steganographic Techniques

The spatial domain-based method operates on the spatial domain, modifying both the secret data and the cover medium. In this method, the secret message can be concealed by altering the least significant bit (LSB) of an image file. LSB steganography is a classic and straightforward technique that embeds secret messages in a specific subset of the LSB plane of the image [2].

One major advantage of this technique is that modifying the LSB plane has minimal impact on the overall image quality as perceived by humans.

he spatial-domain technique directly embeds messages in the pixel intensities of images. Therefore, the advantages of the spatial domain approach include its simplicity in terms of mathematical derivation and the ability to leverage statistical image models to establish upper bounds on the performance of message length estimation. This technique does not require any transformation or decomposition of the original images. It is a straightforward method suitable for real-time processing.

3.3 Palette based Steganographic Methods

Palette-based or indexed colors images, which allow for 8 bits per pixel, employ a technique where the 256 most frequently used colors in the image are identified. A color lookup table, also referred to as a color map or color palette, is created and stored alongside the image [6]. This approach ensures that any modifications to the image do not affect its visual perception. Notably, even identical images can have completely different color maps. Additionally, information can be embedded by selecting specific pixels and organizing the palette in a manner where neighboring colors are closely situated within a specified distance, including the use of Chroma Difference [7]. Palette-based images are commonly used as cover images to facilitate secure and efficient transmission and storage within a communication system.

Furthermore, due to the color quantization process, which introduces some alterations, the stego message can blend in as noise. If palette-based images have lower resolutions, they can be transmitted more rapidly compared to 24-bit resolution images [7]. Palette-based steganography techniques primarily focus on GIF or BMP images and tend to perform better when embedding data in grayscale images.

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.

Characteristics of Steganography

To hide a message in the cover file, we must consider hiding capacity, perceptual transparency, robustness, tamper-resistance. Like many other things in life, in steganography, trade-offs are made, or more precisely, sacrifices are made. In order for the hiding of a message to be safe, we must have redundancy for the changes made after hiding the message. This redundancy subsequently lowers the payload. The exact opposite is also true. With little or no redundancy (robustness) the payload of the secret message can be larger.

Hiding Capacity: This feature deals with the size of information that can be hidden inside the cover file. A larger hiding capacity allows use of a small cover and thus reduces the band-width required to transmit the stego–media. For example, if we have an RGB image with a size of 200 x 200 pixels, that means that we have 120,000 color values to be used as cover values for the secret message (200:width x 200:height x 3:R,G,B), then if we use only one bit per color channel for hiding the message we have a hiding capacity of 120,000 bits or 15,000 bytes, if we use 2 bits per color channel for hiding the message we have 30,000 bytes, but if we use only one color channel and one bit per pixel, the hiding capacity will be 40000 bits or 5000 bytes.

Perceptual Transparency: Perceptual transparency is an important feature of steganography. Each cover-media has certain information hiding capacity. If more information or

data is hidden inside the cover, then it results in degradation of the cover–media. As a result, the stego–media and cover–media will appear to be different. If the attacker notices this distortion, then our steganographic technique fails and there is the possibility that our original message can be extracted or damaged by the attacker. Figure 2 illustrates the Perceptual Transparency concept, it is almost impossible to detect any difference between Figure 1.a and Figure 1.b only by watching them.Tamper–resistance: Of all the features, this feature is very important. This is because, if the attacker is successful in destroying the steganographic technique then the tamper–resistance property makes it difficult for the attacker or pirates to alter or damage the original data.

Steganalysis

Steganalysis is a scientific technique used to detect if a file (be it an image file, sound, video, etc.) contains a hidden message or not. Steganalysis is also used to perfect the process of detecting and extracting hidden messages. We say that we were successful in using the steganalisys method if we found the secret message and extracted it from the cover medium. With this technique we can also check the security of a steganographic technique. To say that a steganographic technique is effective, the hiding of the message should not be visible both to the human eye and to a computer analysis.

The objectives of steganalysis are:

- the main objective is for it to detect the existence of a secret message in an image file

-it is also used to extract secret information

- can be used to determine as precisely as possible the number of changes in the digital image

-distinguishing images that have a secret hidden message in their component and images that do not have a secret message in their component

Types of attacks on steganography

A steganographic algorithm can be called strong depending on how much it resists attacks. Even though the purpose of steganography is to hide a message, there are many attacks by which steganography data can be tested.

There are many forms of attack, which may have the purpose of extracting, detecting, disabling or destroying hidden data. When deciding the type of attack, take into consideration what kind of information is available to the steganalist.

In steganography many attacks are implemented to check if the given file contains a secret message. The cryptographic attack is very similar to the stegonographic attack and similar techniques are used.

Based on the information available to the attacker, the following types of attacks are defined:

Stego-only attack: In this type of attack, only the steganographic environment is available to the attacker, following which the hidden information is extracted.

Know-carrier attack: In this type of attack, both the steganographic media and the original cover media are available to the attacker, and a comparison will be made between the two.

Chosen-stego attack: The steganographic environment and the tool used (algorithm) are available for analysis

Chosen-message attack: To create a steganographic environment, a message and a tool are chosen to do an analysis later. The goal is to find a pattern in the steganographic environment.

Destroy everythink attack: Often the attacker does not want to know the secret message, this technique involves the destruction of the entire steganographic environment that contains the secret message.

Random tweaking attacks: This technique aims to distort the message, so that the secret message becomes unreadable.

Add new Information: Attackers often use the same technique to hide the message in the file.

After entering the new message in the stego file, the original message is overwritten.

Reformat attack: One way of using a secret message hack is to change the format of the stego file.

Compression attack: The stego file is compressed so that the message can be lost both partially and completely.

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)

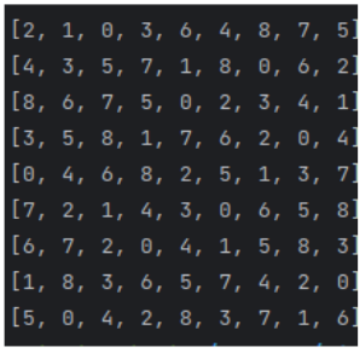


Image 1

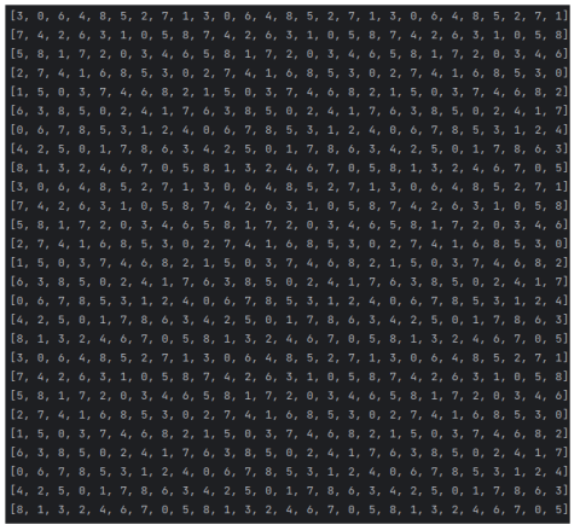


Image 2

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, ...]

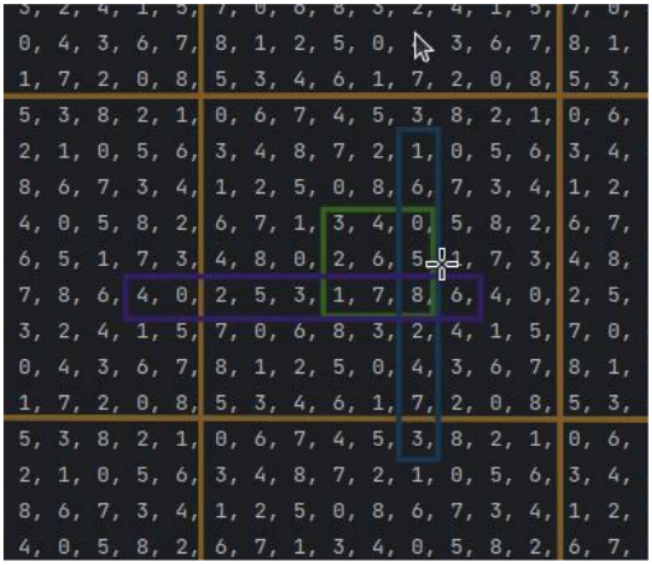
Items in the pixel list will also be converted to base 9.

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).

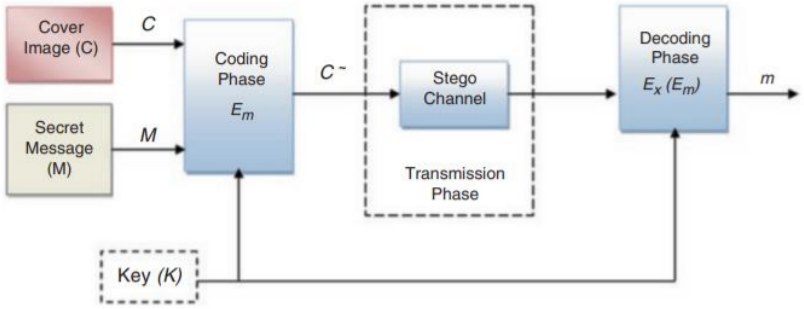
Value found at location M[Pi.x][Pi.y] represents our secret message. This represents only a fragment of the secret message, we must select the next pair of values to be able to extract the complete message. The method for extracting the message is called "Least significant byte" (LSB). We have to take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

Steganographic system model



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://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

https://sci-hub.se/https://ieeexplore.ieee.org/document/1203220

licenta

RAPORT PRIVIND ORIGINALITATEA

49%	48%	32%	31%
INDICE DE SIMILITUDINE	SURSE DE PE INTERNET	PUBLICAŢII	LUCRĂRILE STUDENŢILOR

SURSE PRINCIPALE

1	jis.eurasipjournals.springeropen.com Sursă de pe Internet	19%
2	www.ijert.org Sursă de pe Internet	12%
3	www.researchgate.net Sursă de pe Internet	5%
4	www.trustwave.com Sursă de pe Internet	3%
5	citeseerx.ist.psu.edu Sursă de pe Internet	3%
6	moosmosis.org Sursă de pe Internet	2%
7	Abid Yahya. "Steganography Techniques for Digital Images", Springer Science and Business Media LLC, 2019 Publicaţie	1%
8	www.ukessays.com Sursă de pe Internet	1%

9	Vikas S. Kait, Bina Chauhan. "BPCS steganography for data security using FPGA implementation", 2015 International Conference on Communications and Signal Processing (ICCSP), 2015 Publicaţie	1 %
10	flylib.com Sursă de pe Internet	<1 %
11	Submitted to University of Tennessee Knoxville Lucrarea studentului	<1 %
12	Submitted to Nottingham Trent University Lucrarea studentului	<1 %
13	Submitted to University of Wales Swansea Lucrarea studentului	<1 %
14	Submitted to University of Asia Pacific Lucrarea studentului	<1 %
15	Submitted to Alexandru Ioan Cuza University of Iasi Lucrarea studentului	<1 %
16	www.freshpatents.com Sursă de pe Internet	<1 %
17	www.mdpi.com Sursă de pe Internet	<1 %

18	"Proceedings of the 2nd International Conference on Data Engineering and Communication Technology", Springer Science and Business Media LLC, 2019 Publicaţie	<1 %
19	Lubacz, Jozef, Wojciech Mazurczyk, and Krzysztof Szczypiorski. "Vice over IP", IEEE Spectrum, 2010. Publicaţie	<1 %
20	Mohamed Buke, Hakan Tora, Erhan Gokcay. "Effect of secret image transformation on the steganography process", 2017 24th IEEE International Conference on Electronics, Circuits and Systems (ICECS), 2017 Publicaţie	<1 %
21	Natalia Livak, Maksim Kubrikov, Anna Kubrikova. "Digital educational track formation methodology", AIP Publishing, 2022 Publicaţie	<1 %
22	R. Gurunath, Ahmed H. Alahmadi, Debabrata Samanta, Mohammad Zubair Khan, Abdulrahman Alahmadi. "A Novel Approach for Linguistic Steganography Evaluation Based on Artificial Neural Networks", IEEE Access, 2021 Publicaţie	<1 %
23	repository.stcloudstate.edu Sursă de pe Internet	<1 %

24	Lingyun Xiang, Shuanghui Yang, Yuhang Liu, Qian Li, Chengzhang Zhu. "Novel Linguistic Steganography Based on Character-Level Text Generation", Mathematics, 2020 Publicaţie	<1 %
25	Muhammad Askari, Ahsan Mahmood, Zafar Iqbal. "A novel font color and compression text steganography technique", 2023 International Conference on Communication, Computing and Digital Systems (C-CODE), 2023 Publicaţie	<1 %
26	Mohammed Abdul Majeed, Rossilawati Sulaiman, Zarina Shukur, Mohammad Kamrul Hasan. "A Review on Text Steganography Techniques", Mathematics, 2021 Publicaţie	<1 %
27	profs.info.uaic.ro Sursă de pe Internet	<1 %

Excludeţi citările	Activat	Excludeţi similitudinile < 5 words	
Excludeţi bibliografia	Activat		