

Ministry of Higher Education & Scientific Research

University of AL-Qadisiyah

College of Computer Science & Information Technology

Department of Computer



steganography based on integer wavelet transform

prepared by :

Hussein Ali Rahman

Salah Hassan Shaker

Raed Jayad Henedy

Hiba Mohsen Waheed

College of Computer Science & Information Technology

University of AL-Qadisiyah

Under the supervision of

Dr. Rana jumaa Sarih

2018 A.C

1440 A.H

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

قَالُوا سُبْحَانَكَ لَا عِلْمَ لَنَا إِلَّا مَا عَلَّمْتَنَا إِنَّكَ أَنْتَ الْعَلِيمُ الْحَكِيمُ

صدق الله العلي العظيم

الأهداء

الى من جرع الكأس ليسقيني قطرة حب
الى من كلت انامله ليقدّم لنا لة سعادة
الى من حصد الاشواك ليمهد لي طريق العلم

الى القلب الكبير

(والدي العزيز)

الى من ارضعتني الحب والحنان

الى رمز الحب وبلسم الشفاء

الى القلب الناصع بالبياض

(والدتي العزيزة)

الى القلوب الطاهرة الرقيقة والنفوس البريئة الى رياحين حياتي

(اخواتي واخواني)

الان تفتح الاشرعة وترفع المرساة لتنتطلق السفينة في عرض بحر واسع
هو بحر الحياة وفي هذه الظلمة لا يضيء الا قنديل الذكريات ذكريات الاخوة

البعيدة الى الذين احببتهم واحبوني

(زملائي وزميلاتي)

كلمة شكر

لابد لنا ونحن في خطواتنا الاخيرة في حياتنا الجامعية من وقفة نعود أعوام قضيناها في رحاب كليتنا مع اساتذتنا الكرام الذين قدموا لنا الكثير باذلين بذلك جهودا كبيرة في بناء جيل الغد لتنبعث الامة من جديد ...

وقبل ان نمضي نقدم اسمى ايات الشكر والامتنان والتقدير والمحبة الى الذين حملوا اقدس رسالة في الحياة

الى الذين مهدوا لنا طريق العلم والمعرفة ..

الى جميع اساتذتنا الكرام

كما انني اتوجه بالشكر الجزيل الى من علمتنا التفاؤل والمضي الى الامام الى من رعتنا وحافظت علينا الى من وقفت الى جانبنا عندما ضللنا الطريق مشرفة البحث ...

الدكتورة رنا جمعة سريح

واخيرا اريد اشكر جميع زملائي وزميلاتي ومن اجتمعت معهم باجمل سنين من حياتي

Table of contents

Chapter1

1.1 Introduction	2
2.1 verview of Steganography	3
2-1-1 Steganography Definition	3
3-1-1 Categories of steganography	3
3-2-1 Image Steganalysis^[4]	5
4-2-2 Steganalysis types	5

Chapter2

1-2 Challenges of steganography	6
2-2 Applications of steganography	7
3-2 Matlab	13
Conclusion	14

Abstract

Steganography is becoming an significant region of research in latest years. It is an talent and the science of communication, authentication and many extra devotions. It contracts with the techniques of hiding the communication message and its presence from the unintentional user. In image steganography, secret communication is accomplished over embedding a message into an image as cover file and generates a stego-image having hidden information. There are numerous image steganography techniques are used each have its authorities and cons.in this project , Steganography technique is applied on the transformmmation domain(integer wavelet transform).

Chapter 1

1-1 Introduction

After the growing of the Internet one of the utmost significant parameters of information technology and has been the security of information. Cryptography was generated as a technique for securing the privacy of communication and many different ways have been developed to encrypt and decrypt data so as to keep the message invisible.

unluckily it is sometimes not sufficient to keep the contents of a message secret, it may also be needful to keep the presence of the message secret . The technique used to execute this, called steganography . Steganography is the technique and science of invisible communication . This is achieved across hiding information in another information, thus hiding the presence of the communicated information. The word steganography is coming from the Greek words “stegos” meaning “cover”and“grafia”meaning “ writing” defining it as “covered writing”[1].

In image steganography the information is secreted In particular in images . Two other technologies that are closely connected to steganography are watermarking and fingerprinting . These technologies are fundamentally concerned with the protection of ideological property.

In watermarking all of the cases of an entity are “marked” in the same way. The form of information concealed in objects when using watermarking is usually a signature to signify origin or ownership for the purpose of copyright protection.

With fingerprinting on the other hand, different, unique marks are embedded in distinct copies of the carrier object that are provided to unlike customers. This

enables the intellectual property owner to identify customers who break their licensing agreement by provisioning the property to third parties.

In watermarking and fingerprinting the truth that information is covered indoor the files may be General knowledge sometimes it may even be visible while in steganography the imperceptibility of the monitoring that there is information hidden inside a file, while a successful attack on a watermarking or fingerprinting system would not be to detect the mark, nonetheless to eliminate it. The enrollment and analysis of water-marks to protect copyrighted material is accountable for the modern rise of interest in digital steganography and data embedding[2].

۲-۱ verview of Steganography

To extend an overview of steganography, terms and concepts should first be clarified. An overview of the different types of steganography is presented at a later stage.

2-1 -1Steganography Definition

Steganography is the way of hiding a file, message, image, or video inside another file, message, image, or video. The word steganography gather the Greek words steganos meaning "covered, or protected," and graphein meaning "writing". Steganography mentions to the science of "invisible" connection. Different cryptography, where the objective is to secure connection from an eavesdropper[3].

۳-1 Categories of steganography

Nearly all numerical file formats can be used for steganography, but the formats that are more appropriate are those with a high degree of redundancy.

Redundancy can be clear as the bits of an entity that provide precision far larger than necessary for the object's use and show. The redundant bits of an object are those bits that can be altered without the alteration being discovered simply. Image and audio files specifically comply with this constraint, whereas research has also discovered other file formats that can be used for information hiding. Figure 1 shows the four main categories of file formats that can be used for steganography.

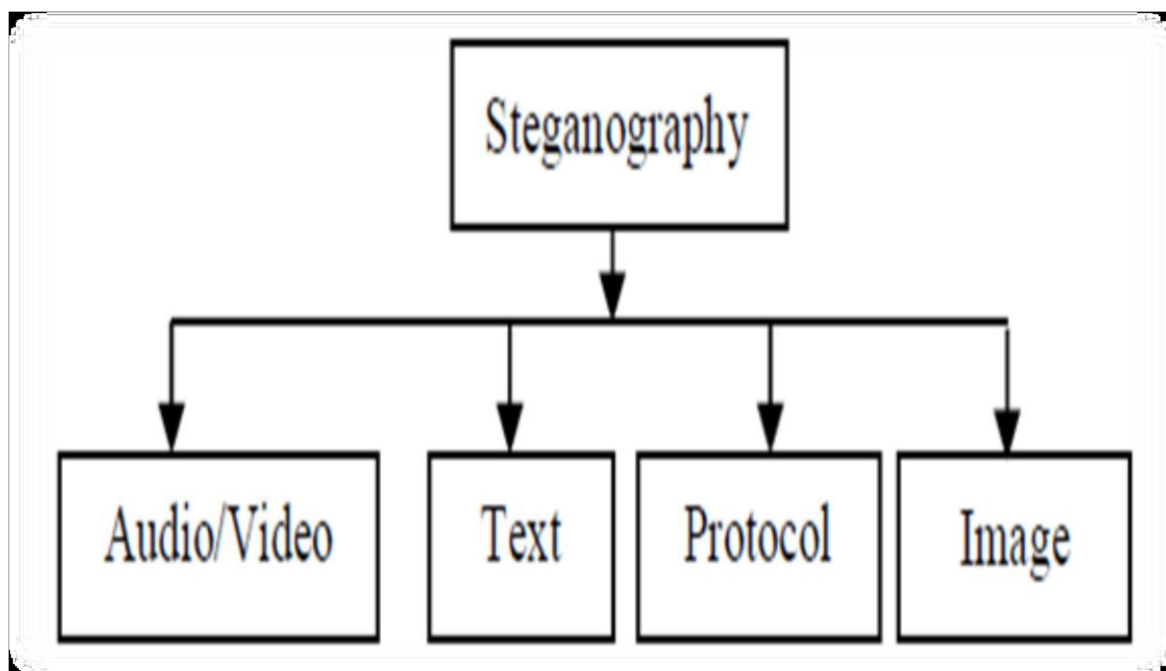


Figure 1: Categories of steganography

To hide a secret message in every n th letter of every word of a text message. It is only since the beginning of the Internet and all the different digital file formats that its importance has decreased. Text steganography using digital files is not used very often since text files have a very small amount of redundant data.

Given the proliferation of digital images, particularly on the Internet, and given the large amount of redundant bits present in the digital representation of an image, images are the most popular cover objects for steganography. To hide

information in audio files similar techniques are used as for image files. One different technique unique to audio steganography is masking, which exploits the assets of the human ear to hide information. A faint, but audible, sound becomes inaudible in the presence of another louder audible sound. This property creates a channel in which to hide information. Although nearly equal to images in steganographic, the larger size of meaningful audio files makes them less popular to use than images. The word protocol steganography mentions to the technique of embedding information within messages and network. The period protocol steganography denotes to the method of embedding information in messages and network control protocols used in network transmission. In the layers of the OSI network model there exist secret channels where steganography can be used. An instance of where information can be secret is in the header of a TCP/IP packet in some fields that are both optional or are never used[2].

3-2-1 Image Steganalysis^[4]

Steganalysis is the partition of steganography and is the science of discovering concealed information. The main goal of steganalysis is to disruption steganography and the discovery of stego image. All steganalysis algorithms rest on steganographic algorithms presenting algebraic differences between cover and stego image.

4-2-2 Steganalysis types

The talent of discovering Steganography is mentioned to as Steganalysis. It is the method of identifying steganography by checking several factor of a stego media. The chief step of this method is to recognize a disbelieved stego media. After that steganalysis method decides whether that media holds concealed message or not and then try to recover the message from it.

In cryptanalysis, it is pure that the interrupted message is encoded and it surely contains the secreted message then the message is knotted. However in the case of steganalysis this may well not be true.

He supposed means can or can not be with secret message. The steganalysis method begins with set of supposed information streams. Then the set is reduced with the help of loan statistical methods. In the case of Visual discovery steganalysis technique, a set of stego images are compared with original cover images and note the visible difference. Signature of the secret message can be resulting by matching numerous images. Cropping or padding of image also is a visual clue of hidden message because some stego tool is cropping or padding utter spaces to appropriate the stego image into static size.

Variance in file size between cover image and stego images, surge or decline of unique colors in stego images tin too be used in the Visual Discovery steganalysis method. Experts and inspectors are annoying new ways to try and find out ways of discovering secret files and translation them unusable.

The U. S. Management has slender Wetstone Technologies to effort with the U.S. Air Force to investigation algorithms that can be used to discern embedded files in digital, audio and video format. Steganalysis is the technique to detect steganography or reverse steganography. The investigation to device strong steganographic then steganalysis method is a incessant process.

Chapter 2

1-2 Challenges of steganography

Growing steganography applications, increases the trials among them obtainable steganography challenges and applications have absorbed on, first challenge of theoretical work was applied to the security of hiding methods that the skill to protected the covered data from third party, the another encounter physique of work communicates to guarantee forcefulness of the secreted data in

contradiction of mischievous outbreaks and the third challenge physique of work communicates to the volume of a system to fleece a huge quantity of information on multimedia without vicissitudes to the arrival of the cover data.

The multimedia tests for steganography data safety rise once several a hateful challengers do several data processing operations to affect the process to discover or recuperate the concealed data.

Additional challenge of the multimedia steganography is a digital image actuality used as carriers, discovering the existence of secret information postures noteworthy challenges. Though the existence of secret message is frequently invisible to the human eye, it finally changes the measurements of an image. Though the hybrid multimedia steganography postures important challenges and a pattern in other word defined as a set of measurements that categorizing points in a given multidimensiona space[5].

2-2 Applications of steganography^[6]

A Multimedia steganography has applications in the various areas such as internet communication, multimedia database systems, medical imaging, telemedicine, criminals, biometrics hiding and military communications . The communication has many reasons why two parties might wish to share secretly. The reason may be kindly, might be two lovers wants to communicate secrecy and conceal their relationship. It might be political resason, as a dissident people or organization desiring to share a secrecy messages among themselves, or might be with a forbidden organization outside their country. Criminal used as a term in the case of organized crime or terrorism. There are probably many other applications of steganography, Of course, successful steganography is not detectable, and so most successful applications may never become public.

those various areas of Multimedia steganography has applications that we referred above are:

Military And Intelligence Agencies : Military and intelligence agencies are essentially required to communicate unobtrusively, even if the messages are encrypted, the detection of a signal may lead fast to an attack on the cover-media. For this reason, military and intelligence agencies use techniques to make signals hard for the adversary to detect messages such as Spread Spectrum Modulation (SSM) or Meteor Scatter Transmission (MST) . Military organizations in the information hiding techniques also underlie many attacks on multi secure level systems. A virus or other malicious code proliferates the techniques from low security level to high security level and then the operating system using a covert channel in the signal or data may be directly hiding information in data that may be declassified .

Healthcare Industry:Healthcare industry and medical imaging systems are benefiting fromSteagnography techniques. They use DICOM (digital imaging and communications in medicine) which separates image data from the caption, such as the name of the patient, the date, and the physician. Sometimes the link between image and patient is lost or misplaced so to conceal the data, such as the name of the patient in the image could be a useful safety measure .

Another good technique of a healthcare industry is hiding messages in DNA sequences used to protect intellectual property in medicine, molecular biology . It is still questioning whether such techniques. would have any effect on the accuracy of the diagnosis of the healthcare industry .

Criminals: Unobtrusive communications of criminals through various technologies such as mobile phones and monitoring of an individual's phone calls in a democracy

where the country monitors its citizens is significantly restrained by national laws for the safety purpose. Criminal used as a term in the case of organized crime or terrorism, such as FBI in United States wiretapping of the individual cell phones by national laws and it is permitted only to them by a judge's order. The operations within the environment used as the cell phone of every one is wiretapping without knowing that he or she is under surveillance. The essential aim to find the criminal organization of surveillance is to identify all members even if the communication is encrypted where they can reliably infer the identity of co-conspirators by simply identifying the recipients of messages that were encrypted. In criminal investigations has to use the cellphone and e- mail for finding the exact location of the suspect and tracing the data that can be under surveillance in the global cell phones and e-mails. National security agency (NSA) is spying the information since 2005, where the U.S. government, with the help of major telecommunications carriers has involved in illegal dragnet surveillance of domestic communications and record of millions of ordinary Americans since at least 2001. The Electronic Frontier Foundation (EFF) is the first line of defending your right in the digital world, based in San Francisco, used to protect the fundamental rights regardless of technology lead to stop it and bring government surveillance programs within the rules and regulation of the law.

Anonymous Communications: The goal of anonymous communications specifically in anonymous remailer is to preserve communications privacy within the shared public network environment. It can also help to provide good security beyond the content of privacy and integrity. It is including anonymous remailers and Web proxies that can be used in various applications such as online elections that the legitimate users to vote privately, online free speech, political claims, consume sexual material and use digital cash, abused techniques such as defamation, blackmail and unsolicited commercial mailing . In the anonymous communications hiding techniques are not very clear so that the techniques should be designed in a

perfect manner and providing such facilities requires careful thought about the possible abuses, which might be nonobvious Anonymous remailer is to exchange encrypted messages for a criminal organization to communicate among its members that identify they have something to hide. The use of anonymous remailers is not illegal and does not have the authority to deny access to such remailers. Anonymous remailers rely on information being securely stored on the remailers, which indirectly hold the information needed to direct the mail to its intended recipient, even when law enforcement agencies have number of occasional demanded to access to this information, even if the remailers are located in other countries the anonymous remailers cannot guarantee anonymity. There are a possible advantages and disadvantages of anonymous communication steganography.

Plausible Deniability: Plausible deniability techniques used in steganography in situations where plausible deniability is required when communication of two parties are involved in an activity which is somehow illicit and they wish to avoid being caught . It can be used as legitimate motives such as fair voting, personal privacy and limitation of liability that obviously motivated for plausible deniability.

Dissidents: Steganography for dissidents used in many countries in the world where the political dissent is neither tolerated nor legal. The dissident organizations have to take precaution when they communicate with each other especially with international organizations. The environment that dissidents operate in is usually overtly hostile. Such as dissidents are aware that they are under surveillance and the adversary is extremely powerful and possibly ruthless. Dissidents have three ways to conceal the communications (encryption, anonymous remailers, and steganography).

Hiding Person Identification: The incorporate of Digital Steganography and biometrics are the Fascinating scientific area which falls under the umbrella of

security system. Biometrics represents automated methods of identifying a person Characteristics . Biometric data is not replaceable and not secret joint with the existence of various types of attacks that can be possible in a biometric system. Although, to make the issue of security and integrity of biometric data criticality.

Covert Channels In Operating Systems : In operating system when both communication partners have to access to one computer system or running on one host channels. These methods of imperceptible transmission occurred when concern person is worried about various possibilities of security leaks in high-security operating systems . The covert channels can make security when one part of the operating system at a specified level of security is able to send a service to another part of the system with a many possibilities for the security level. The cover channel for the system of Open System Interconnect (OSI) network model is usable to communicate secretly. There are various ways for sharing data as the timestamp of an IP packet, where the packets can be sent at an odd time increments represent a logical one, the system of collision detection in the Ethernet physical layer can be modified and Internet control message used.

Video Communication Systems: Video communication systems Steganography used to embed secret messages within video conferencing systems that have been recorded. The system stores messages into a lossy DCT-based video compression. The video conferencing system such as An Integrated Services Digital Network (ISDN) in a Global System for Mobile Communications (GSM) telephone conversation (up to 8 Kbps) could be concealed without degrading to the video signal and thus making the secret communication apparent. Thus, all communication depends on the video image nature used as cover.

Executable Files: Data hiding in executable Files has many redundancies to solve a specific problem in the way of independent ensuing instructions to be scheduled.

Code obfuscation techniques, primarily developed to protect re-engineering of software products, can be used to store additional information in executable files such as "branch insertion" and "loop condition insertion" transforms in to obfuscate Java code.

Monitoring And Copyrighted On The Web : Automatic monitoring of copyrighted material on the web is used as a robot search on the web for marked material and identifies possible illegal usage. An alternative technique downloads images from the Internet, computes a digest of them, and compares this digest with digests registered in its database.

Audit Of Radio Transmissions: Automatic audit of radio transmission in a computer can eavesdrop to a radio station and look for signals, in which the broadcast has to show a particular music or advertisement .

Data Augmentation: Information augmentation is an additional benefit of the public. , it can conceal the information by using the index pictures or music tracks in order to provide an efficient retrieval of information from databases .

Tamper Proofing : Tamper proofing of steganography in a digital object may be a signed "summary" of it, which used to prevent or detect unauthorized modifications.

3-2 Matlab

MATLAB (matrix laboratory) is a multi-paradigm numerical computing environment. A proprietary programming language developed by MathWorks, **MATLAB** allows matrix manipulations, plotting of functions and data, implementation of algorithms, creation of user interfaces, and interfacing with programs written in other languages, including C, C++, C#, Java, Fortran and Python.

Although **MATLAB** is intended primarily for numerical computing, an optional toolbox uses the MuPAD symbolic engine, allowing access to symbolic computing abilities. An extra package, Simulink, increases graphical multi-domain simulation and model-based design for dynamic and embedded systems.

MATLAB users come from various backgrounds of engineering, science, and economics.

Integer Wavelet Transform In Matlab this is achieved using lifting schemes. Define a lifting scheme with **liftwave** , **lwt2** and **ilwt2** for the transformations.

Ls= liftwave(WNAME) returns the lifting scheme associated with the wavelet specified by **WNAME**. **LS** is a structure, not an integer, and used by **ilwt** , etc.

ilwt performs a 2-D lifting wavelet decomposition with respect to a particular lifted wavelet that you specify.

X = ilwt2(AD_In_Place,W) calculates the reconvened matrix **X** using the approximation and detail coefficients matrix **AD_In_Place**, obtained by a lifting wavelet decomposition. **W** is a lifted wavelet name .

im2bw converts the grayscale image to a binary image.

BW = im2bw(I, level) converts the grayscale image to a binary image. The output image **BW** replaces all pixels in the input image with luminance greater than level with the value 1 (white) and replaces all other pixels with the value 0 (black).

Specify level in the range [0,1]

Conclusion

In the current world, the data transfers using internet is rapidly growing because it is so easier as well as faster to transfer the data to destination. Normally, image steganography method does not provide much attention on the basic demand of secrecy and privacy. But in our proposed work the main importance is given to the secrecy as well as the privacy of information. The embedding process is hidden under the transformation of cover image. These operations provide sufficient secrecy. On the other hand to obtain privacy, IWT is used. The embedding capacity of the cover image is increased.

List of references

- [1]T. Morkel , J.H.P. Eloff , M.S. Olivier “AN OVERVIEW OF IMAGE STEGANOGRAPHY” Information and Computer Security Architecture (ICSA) Research GroupDepartment of Computer ScienceUniversity of Pretoria, 0002, Pretoria, South Africa , page 2.**
- [2] Parmar Ajit Kumar Maganbhai1, Prof. Krishna Chouhan” A Study and literature Review on Image Steganography” *1M-Tech Research Scholar, 2Research Guide, Department of Electronics & Communication, SIRT Bhopa, page 1***
- [3] Eric Cole *Ronald D. Krutz, Consulting Editor, “Hiding in Plain Sight: Steganography and the Art of Covert Communication” Publisher: Bob Ipsen Published by Wiley Publishing, Inc., Indianapolis, Indiana Published simultaneously in Canada ,2003 , page5.***
- [4]T. Morkel , J.H.P. Eloff , M.S. Olivier “AN OVERVIEW OF IMAGE STEGANOGRAPHY” Information and Computer Security Architecture (ICSA) Research GroupDepartment of Computer ScienceUniversity of Pretoria, 0002, Pretoria, South Africa , page 4.**
- [5] Stefan Katzenbeisser Fabien A. P. Petitcolas “Information hiding techniques for steganography and digital watermarking” British Library Cataloguing in Publication Data ,2000, page 31**