Watermarking in Computer Security

Josna Sojan[1], Dhanya Job[2]

UG Scholar
Department of Computer Sciences,
Santhigiri College of Computer Sciences,
Vazhithala
josnasojan99@gmail.com

Head Of Department
Department of Computer Sciences,
Santhigiri College of Computer Sciences,
Vazhithala
dhanyajob@santhigiricollege.com

Abstract: Computer security also known as cybersecurity or IT security, is the protection of information systems from theft or damage to the hardware, the software, and to the information on them, as well as from disruption or misdirection of the services they provide. Computer security is mainly concerned with three areas –confidentiality, integrity and availability or CIA triad. Confidentiality is a set of rules that only authorized users can access the data resources and information. Integrity means only authorized users should be able to modify the data when needed. Availability means data should be available to users when needed. Security mechanisms are technical tools and techniques that are used to implement Security Services. A mechanism might operate by itself, or with others, to provide a particular. Examples of common security mechanisms are as follows Encryption, Steganography, Water Marking[1].

Keywords: confidentiality, integrity, availability, encryption, steganography, water marking.

1. Introduction

The Internet has transformed our lives in many good ways. Unfortunately, this vast network and its associated technologies also have brought in their wake, the increasing number of security threats. The most effective way to protect yourself from these threats and attacks is to be aware of practices. This paper is an introduction to computer security and its key concepts. Computer security basically is the protection of computer systems and information from harm, theft, and unauthorized use. It is the process of preventing and detecting unauthorized use of your computer system. Often people confuse computer security with other related terms like information security and cyber security. One way to ascertain the similarities and differences among these terms is by asking what is being secured. Computer security is securing information from unauthorized access, modification & deletion. Also it will secure a standalone machine by keeping it updated and patched and also will communicate over the computer networks[2]. The key objectives of computer security are Confidentiality, Integrity, Availability. Also known as the CIA TRIAD. It is a model designed to guide policies for information security within an organization. The model is also sometimes referred to as the AIC TRIAD to avoid confusion with the central intelligence agency. Confidentiality is a set of rules that limits access to information. It is roughly equivalent to privacy. Measures under taken to ensure confidentiality are designed to prevent sensitive information from reaching the wrong people, while making sure that the wrong people can infact get it. The method to enhance confidentiatily is encryption. Integrity involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle. Data must be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people. Integrity can be ensured by the method hashing.
Availability is the best ensured by rigorously maintaining all hardware, performing hardware repairs immediately when needed and maintaining a correctly functioning operating system environment that is free of software conflicts. It is also important to keep current with all necessary systems upgrades. Security mechanisms are technical tools and techniques that are used to implement Security Services. A mechanism might operate by itself, or with others, to provide a particular. Examples of common security mechanisms are as follows Cryptography, Steganography, Water Marking. Encryption is the process that scrambles readable text so it can only be read by the person who has the secret code, or decryption key. It helps provide data security for sensitive information. Steganography is a method of hiding secret data, by embedding it into an audio, video, image or text file. It is one of the methods employed to protect secret or sensitive data from malicious attacks. "Watermarking" is the process of hiding digital information in a carrier signal; the hidden information should, but does not need to, contain a relation to the carrier signal. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners[3].

2. Security Aspects

2.1. Cryptography

Cryptography is the practice and study of techniques for secure communication in the presence of third parties called

adversaries. Encryption is the process of taking plain text, like a text message or email, and scrambling it into an unreadable format called “cipher text.” This helps protect the confidentiality of digital data either stored on computer systems or transmitted through a network like the internet. The recipient have to use a “secret” encryption key a collection of algorithms that scramble and unscramble data back to a readable format[4].

2.1.1. Public Key Cryptography

Public key cryptography is an encryption technique that uses a paired public and private key algorithm for secure data communication. A message centre uses a recipient public key to encrypt a message. To decrypt the sender’s message, only the recipients private key may be used. The two types of PKC algorithms are RSA which is an acronym named after this algorithms inventors: Rives, Shamir and Adelman, and Digital Signature Algorithm(DSA). PKC encryption evolved to meet the growing secure communication demands of multiple sectors and industries, such as the military.

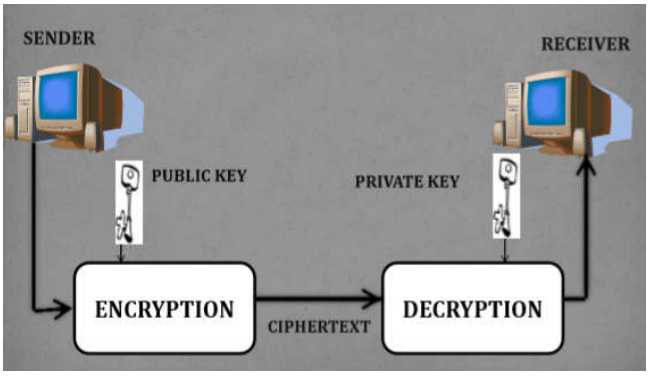

Figure 1: Public Key Cryptography

2.1.2. Private Key Encryption

Private key encryption is the form of encryption where only a single private key can encrypt and decrypt information. It is a fast process since it uses a single key. However, protecting one key creates a key management issue when everyone is using private keys. The private key may be stolen or leaked. Key management requires prevention of these risks and necessities changing the encryption key often, and approximately distributing the key[5].

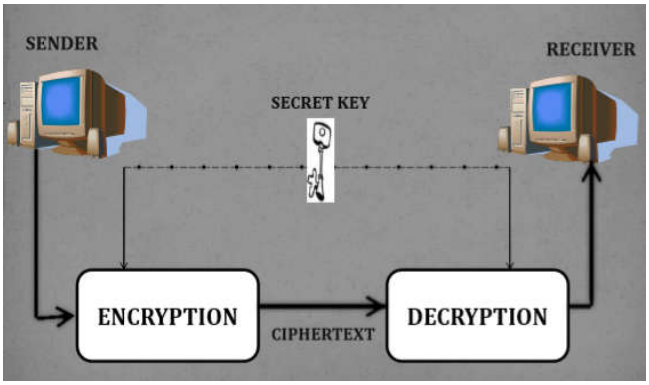

Figure 2: Private Key Cryptography

When the intended recipient accesses the message, the information is translated back to its original form. This is called decryption. To unlock the message, both the sender.

2.2. Steganography

Steganography is a method of hiding secret data, by embedding it into an audio, video, image or text file. It is one of the methods employed to protect secret or sensitive data from malicious attacks.
The word steganography combines the Greek words steganos, meaning "covered, concealed, or protected", and graphein meaning "writing". Types of steganography:

- Text steganography is a sub part of steganography that hides the message behind other cover text file. Moreover,hiding the text behind HTML coding of web pages makes the detection of steganography impractical as web pages are a fundamental building blocks of the internet.
- Image steganography refers to hiding information(text, images or audio files) in another image or video files. The current project aims to use steganography for an image with another image using spatial domain technique. This hidden information can be retrieved only through proper decoding technique.
- Steganography over video file means by hiding video in another video file, random byte hiding and LSB technique. Secure video Steganography is a challenging task of sending the embedded information to the receiver without being detected.
- Audio Steganography is a technique used to transmit hidden information by modifying an audio signal in an imperceptible manner. It is the science of hiding some secret text or audio information in a host message. The host message before steganography and stego message after steganography have the same characteristics[6].

2.3. Watermarking

"Watermarking" is the process of hiding digital information in a carrier signal; the hidden information should, but does not need to, contain a relation to the carrier signal. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners.

A digital watermark is a kind of marker covertly embedded in a noise-tolerant such as audio, video or image data. It is typically used to identify ownership of the copyright of such signal. It is prominently used for tracing and authentication. Both steganography and digital watermarking employ steganographic techniques to embed data covertly in noisy signals. While steganography aims for imperceptibility to human senses, digital watermarking tries to control the robustness as top priority[7].

Watermarking are of two types : Visible watermarking and invisible watermarking.

2.3.1. Visible Watermarking

Visible watermarking is the process of embedding data (watermark) into a multimedia object (video/image) such that the embedded watermark is perceptible to a human observer. Many times, visible watermarks occlude important portion of multimedia objects. Unlike invisible watermarking, visible watermarking consists in the overlaying of a logotype related to ownership into the original image in a perceptible manner, so visible watermarking can perform copyright protection in more direct and immediate manner than invisible watermarking. Generally, the embedded visible watermark may reduce the commercial value of the digital image, although it is translucent; therefore recently several removable visible watermarking techniques were proposed. However, there are many applications in which the permanent visible watermarking is more suitable. The digital library, e-commerce and digital press are the main applications of the permanent visible watermarking. The digital library can offer users some digitalized documents, photograph, and arts with visible watermark pattern, and the users can read or look at them freely; however they cannot use these digital materials for other purpose, such as illegal sale, due to the visible watermark. In the case of e-commerce, an owner of some products, such as arts or professional photographs, can take pictures of his/her merchandise and put them on Internet for advertisement purpose. The images of merchandise can attract attention of possible customers; if these images contain translucent visible watermark, then an illegal use of these pictures can be avoided. In the case of the digital press, the protection of exclusive material is very important. A visible translucent watermark indicates the originality of their materials and avoids its illegal use.
A visible watermarking algorithm should satisfy some requirements which are as follows:

- Embedded watermark should be perceptible in grey and colour host images.
- Embedded watermark should be perceptible in any image regions with different characteristics: texture, plain, and edge.
- Embedded watermark should not be too obtrusive, so details of host image may be perfectly recognizable.
- Watermark embedding should not obscure or brighten considerably the host image, the watermarked area should be sufficiently perceptible by the HVS, and the degradation of nonwatermarked area is almost nullified.
- Embedded watermark should be robust against several common attacks.
- Watermark embedding process should be automatic for all kinds of images.

2.3.2. Invisible Watermarking

Invisible watermark is hidden in the original content. It can be observed by an authorized person only. Watermark is inserted in such a way that changes made the pixel value are perceptually not noticed and it can be recovered only with appropriate decoding mechanism[8].

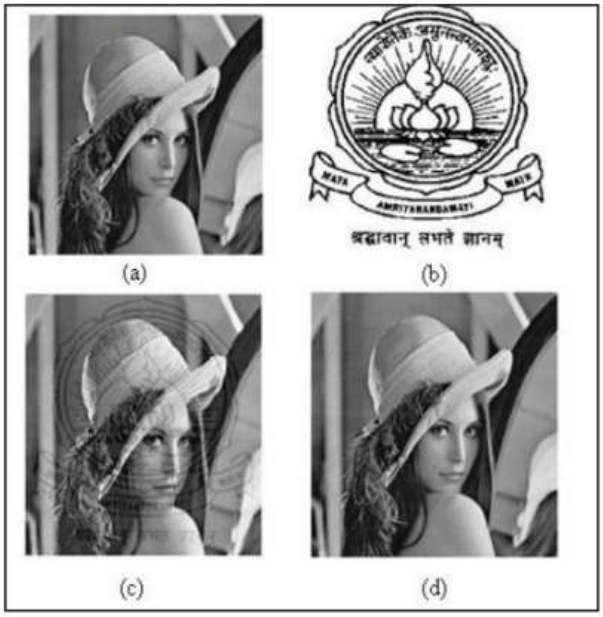

Figure 3: (a) the Original Lena Image (b) the Logo to be Watermarked (c) Visible Watermarked Image and (d) Invisible Watermarked Image

2.3.3. Applications of Watermarking

There are various applications of Digital Image Watermarking. Digital watermarking is used in several applications. The aim of every application is to providing security of the digital information. Following are the most important applications.

- Copyright Protection: The one of the most important application of watermarking is copyright protection from the unauthorized user. Ownership of digital media can be established in the case of a copyright dispute by using the embedded data as a proof.

- Broadcast Monitoring: This application is used to monitor unauthorized broadcast station. It can verify whether the content is really broadcasted or not.

- Tamper Detection Fragile watermarks are used for tamper detection. If the watermark is degraded or destroyed, it indicates presence of tampering and hence digital content cannot be trusted.

- Data Authentication and Verification:The watermark is inserted to detect if the image has customized or not, this process can be used for verification. Integrity verification can be achieved by using fragile or semi fragile watermark which has low robustness to modification in an image.

- Fingerprinting: The main purpose of fingerprinting is to protect clients. If someone got a legal copy of a product, but redistributed illegally, fingerprinting can

prevent this. This can be achieved by tracing the whole transaction by inserting single robust watermark for each receiver.

- Content Description: This watermark can contain some detailed information of the host image such as labeling and captioning. The capacity of watermark for this kind of application should be relatively large and there is no strict requirement of robustness.

- Medical Applications: In medical field the watermarking is important for the purpose to protect the hospital's information from unauthorized people such as patient's report etc. Security and verification of such data are now becoming very significant in medical field where the digital data are easily distributed over the internet.

3. Theoretical Aspects

Digital watermarking is very much common now a days because it is easily available and it secure our data from illegal use. It has two major techniques i.e. spatial domain and transform domain .In the spatial domain techniques, we insert the watermark by modifying the pixel values. Transform domain watermarking: The watermark is inserted into the coefficients of transform domain. Various types of transform domain techniques are DCT, LSB and Fourier Transfer. From robustness and hiding (imperceptibility) point of view, transform domain techniques are better than spatial domain techniques.

3.1. Least Significant Bit (LSB)

LSB (least significant bit) is the most commonly used technique in spatial domain. It selects the some random pixels of the cover image to insert the watermark.

Step 1: Conversion of RGB image to Gray scale image.
Step 2: Find double precision for image.
Step 3: Transfer most significant bits to low significant bits of watermarked image.
Step 4: Make least significant bits of host image zero.
Step 5: Add shifted version (step 3) of watermarked image to modified (step 4) host image.

3.1.1. Advantage

- It is easily performed on images.
- It provides high perceptual Transparency.
- When LSB technique is used to insert the watermark, quality of image will remains same.
- Easy to implement.

3.1.2. Drawback

LSB technique is less robust to common signal processing operations Sensitive to noise.

3.2. Discrete Cosine Transform

DCT It is commonly used for the signal processing. In this we transform the image into the frequency domain. It is used in many areas like pattern recognition, data compression, and image processing. This technique is more robust than spatial domain watermarking techniques. The main steps used in DCT are:

Step 1: Take the image and divide it into non overlapping 8*8 blocks.
Step 2: Calculate forward DCT of each of the non overlapping blocks.
Step 3: Use HVS blocks selection criteria.
Step 4: Now use highest coefficient selection criteria.
Step 5: Then embed watermark in the selected coefficient.
Step 6: Now take inverse DCT transform of each block.

3.3. Discrete Fourier Transform (DFT)

DFT offers more robustness against geometric attacks like scaling, cropping, translation, rotation, etc. It decomposes an image in sine and cosine form. In this, embedding may be done in two ways: direct embedding and the template based embedding. In the direct embedding technique we modifying DFT magnitude and phase coefficients and then the watermark is inserted. The template based embedding technique introduces the concept of templates. In DFT domain, during embedding process, we embed the template, which is used to find the transformation factor. When the image is transformed, firstly this template is searched and it is then used to resynchronize the image. After this, detector is used to extract the embedded spread spectrum watermark. Cons: Implementation is complex. And the computational cost is also higher[9].

4. Accuracy of Watermarking

4.1. Capacity

Watermark capacity or data payload refers the amount of secret information present in watermark image. It simply means that how much amount of information, we able to insert in the image. Data payload or capacity is the number of bits a watermark encodes within a unit of time.

4.2. Peak signal-to-noise ratio (PSNR)

The PSNR block computes the peak signal-to-noise ratio, in decibels, between two images. This ratio is used as a quality measurement between the original and a compressed image. The higher the PSNR, the better the quality of the compressed, or reconstructed image.

4.3. Mean-Square Error (MSE)

The mean-square error (MSE) and the peak signal-to-noise ratio (PSNR) are used to compare image compression quality. The MSE represents the cumulative squared error between the compressed and the original image, whereas PSNR represents a measure of the peak error. The lower the value of MSE, the lower the error.

5. Advantages of Computer Security

- The computer security will defend us from critical attacks.
- It helps us to browse the safe website.
- Security will defend from hacks and virus.
- Minimizes computer freezing and crashes.
- Protect data from theft.
- Protects the computer from being hacked.
- Gives privacy to users.

6. Disadvantages of computer security

- When the parent organization takes on several projects, it is common for each on to be fully staffed.
- Firewalls can be difficult to configure correctly.
- Makes the system slower than before.
- Need to keep updating the new software in order to keep security up to date.
- Could be costly for average user.

7. Conclusion

Computer security attempts to ensure the confidentiality, integrity, and availability of computing systems and their components. Three principal parts of a computing system are subject to attacks: hardware, software, and data. Watermarking is the practice of imperceptibly altering a piece of data in order to embed information about the data. According to the definition there are two important characteristics of watermarking. First, information embedding should not cause perceptible changes to the host medium. Second, the message should be related to the host medium. In this sense, the watermarking form a subset of information hiding techniques, which also include cases vulnerabilities. Some provisions for cyber security have been incorporated into rules framed under the Information Technology Act 2000.Some provisions for cyber security have been incorporated into rules framed under the Information Technology Act 2000 Update in 2013[10]. Digital watermarking is use of a kind of marker covertly embedded in a digital media such as audio, video or image which enables us to know the source or owner of the copyright. This technique is used for tracing copyright infringement in social media and knowing the genuineness of the notes in the banking system.

References

[1] contrib.andrew.cmu.edu

[2]Schatz, Daniel; Bashroush, Rabih; Wall, Julie (2017. *Journal of Digital Forensics, Security and Law*. **12** .

[3]International Journal of Scientific & Engineering Research, Volume 4, Issue 6, June-2013 1902.

[4]www.geeksforgeeks.org

[5] *securitytrails.com*

[6] Ingemar J. Cox: Digital watermarking and steganography. Morgan Kaufmann, Burlington, MA, USA, 2008

[7] *Pahati, OJ (2001-11-29. . Archived from on 2007-07-16*. Retrieved

[8] M. Swanson, B. Zhu, A. Tewfik, and L. Boney, "Robust audiowatermarking usingperceptual masking," Signal Process, Special Issue onWatermarking, 1997

[9]International Journal of Scientific & Engineering Research, Volume 4, Issue 6, June-2013 1902

[10] IJCSMC, Vol. 3, Issue. 6, June 2014

Author Profile

Josna Sojan pursuing Bachelor of Computer Application from Santhgiri College of Computer Sciences, Vazhithala in 2018-2021.

Dr. Dhanya Job received M.Sc., M.Tech.M.Phil.Ph.D. in Computer Science. Data Security is the area of specialization. Currently working as Head of the Department in Santhgiri College of Computer Sciences, Vazhithala.