IJO -INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND ENGINEERING

(ISSN: 2814-1881) Mojirade A. AWODUN *

https://ijojournals.com/ *Volume 07 || Issue 09|| September, 2024 ||*

Data Hiding Technique in Information Technology: A Review

[1]Mojirade A. AWODUN & [2]Mobolaji O. TENIBIAJE

[1,2]Department of Computing and Information Science, School of Physical Sciences, Bamidele Olumilua University of Education, Science and Technology, Ikere-Ekiti, Ekiti State, Nigeria.

Abstract

Data hiding techniques has received much attention in several application areas and with the widespread growth of digital information and improved internet technologies, the demand for improved information security has greatly increased due to identity theft, data distribution, privacy leakage and illegal copying. Data hiding can be done in text, image, audio, video and in other form of information. The traditional data hiding techniques have to be upgraded and need to be used in conjunction with other techniques for the integration, confidentiality and security of digital information. Cryptography, steganography and watermarking are various techniques proposed to protect and secure the Digital information.

Keywords: Data Hiding, Information Technology, internet technology, Cryptography, steganography

Introduction

Information Technology is the most essential aspect in today's world. Based on this fact computer application is still developing to handle securely the financial as well as the personal data more effectively. These data are extremely important from every aspect and we need to secure this from unauthorized access. Security is the process of preventing and detecting unauthorized use of data or computer or network. Prevention measures help us to stop unauthorized users from accessing any part of computer system. Information hiding is the ability to prevent certain aspects of a class or software component from being accessible to its clients, using either programming language features (like private variables) or an explicit exporting policy.

Detection helps to determine whether or not someone attempted to break into the system, if they were successful, and what they may have done. In achieving this height of security we may use various data hiding techniques. However, presently data encryption is not enough, we also need to secure the presence of data.

Cryptography is referred to as "the study of secret". Encryption is the process of converting normal text to unreadable form. Decryption is the process of converting encrypted text to normal text in the readable form (Iman & Abi-Char, 2015). Cryptography converts the original message into non readable format and sends the message over an insecure channel. The authorized person has the capability to convert the non-readable message to the readable one (Monika & Pradeep, 2012).

Steganography is sometimes confused with cryptography, but there are some distinctive differences between the two. In some cases steganography is often preferred to cryptography because in cryptography the cipher text is a scrambled output of the plaintext and the attacker can guess that encryption has been performed and hence can employ decryption techniques to acquire the hidden data. Also, cryptography techniques often require high computing power to perform encryption which may hinder small devices that lack enough computing resources to implement encryption (Nosrati, et al, 2011).

In information security there are many encryption algorithms which can be categorized into private (symmetric) and public (asymmetric) keys encryption. In Symmetric keys encryption, only

IJO -INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND ENGINEERING

(ISSN: 2814-1881) Mojirade A. AWODUN *

https://ijojournals.com/ *Volume 07 || Issue 09|| September, 2024 ||*

one key is used to encrypt and decrypt data. The key needs to be distributed before transmission between entities. If weak key is used in algorithm then everyone may decrypt the data. The effectiveness of Symmetric key encryption depends on the size of key used. For the same algorithm, encryption using longer key is harder to break than the one done using smaller key. There are many examples of strong and weak keys of cryptography algorithms like RC2, DES, 3DES, RC6, Blowfish, and AES. RC2 uses one 64-bit key .DES uses one 64-bits key. Triple DES (3DES) uses three 64-bits keys while AES uses various (128,192,256) bits keys. Blowfish uses various (32-448); default 128bits while RC6 used various (128,192,256) bits keys. Asymmetric key encryption or public key, two keys are used; private and public keys. Public key is used for encryption and private key is used for decryption. (Abdul, et al, 2009).

Literature Review

According to Cory (2014) who opined that data hiding is a software development technique specifically used in object-oriented programming (OOP) to hide data members. Data hiding ensures exclusive data access to class members and protects object integrity by preventing unintended or intended changes. Data hiding is also known as data encapsulation or information hiding. Data hiding also reduces system complexity for increased robustness by limiting interdependencies between software components.

In computer science, information hiding is the principle of segregation of the design decisions in a computer program that are most likely to change, thus protecting other parts of the program from extensive modification if the design decision is changed. The protection involves providing a stable interface which protects the remainder of the program from the implementation (the details that are most likely to change).

Data Security

Data security is the practice of keeping data protected from corruption and unauthorized access. The focus behind data security is to ensure privacy while protecting personal or corporate data. Privacy, on the other hand, is the ability of an individual or group to seclude information about themselves and thereby reveal them selectively (Ishaque, et al, 2011). Data privacy or information privacy is the relationship between collection and dissemination of data, technology, the public expectation of privacy, and the legal issues. Data privacy issues can arise from a wide range of sources such as healthcare records, criminal justice investigations and proceedings, financial institutions and transactions, biological traits, residence and geographic records and ethnicity. Data security or data privacy has become increasingly important as more and more systems are connected to the Internet. There are information privacy laws that cover the protection of data or information on private individuals from intentional or unintentional disclosure or misuse. Thus, hiding the data in a kind of form such as within an image is vital in order to make sure that security or privacy of the important data is protected (Pramendra & Vijay, 2014).

IJO -INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND ENGINEERING

(ISSN: 2814-1881) Mojirade A. AWODUN *

https://ijojournals.com/ *Volume 07 || Issue 09|| September, 2024 ||*

History of Data Hiding

The concept of information hiding was first described by David Parnas in 1972. Before then, modularity was discussed by Richard Gauthier and Stephen Pont in their 1970 book Designing Systems Programs although modular programming itself had been used at many commercial sites for many years previously – especially in I/O sub-systems and software libraries – without acquiring the 'information hiding' tag – but for similar reasons, as well as the more obvious code reuse reason (Raju et al, 2010).

The term "digital watermark" was first coined in 1992 by Andrew Tirkel and Charles Osborne. Watermarks are identification marks produced during the paper making process. The first watermarks appeared in Italy during the 13th century, but their use rapidly spread across Europe. They were used as a means to identify the papermaker or the trade guild that manufactured the paper. The marks often were created by a wire sewn onto the paper mold. Watermarks continue to be used today as manufacturer's marks and to prevent forgery (Watermarkingworld, 2009).

Data hiding techniques have been widely used to provide copyright protection, data integrity, covert communication, non-repudiation and authentication, among other applications. In the context of increased dissemination and distribution of multimedia content (text, audio, video etc) over the internet, data hiding methods, such as digital watermarking and steganography are becoming more and more relevant in providing multimedia security (Megias et al, 2021).

Techniques of Data Hiding

In data hiding, three famous techniques can be used. They are watermarking, steganography and cryptography.

1. **Steganography**

Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the message. This can be achieved by concealing the existence of information within seemingly harmless carriers or cover. Here carrier can be text, image, video, audio, etc. (Vikram & Kuyeri, 2014). Steganography is a technique where information or files are hidden within another file in an attempt to hide data by leaving it in plain sight. “Steganography produces dark data that is typically buried within light data (e.g., a non-perceptible digital watermark buried within a digital photograph).” Some experts have argued that the use of steganography techniques are not very widespread and therefore shouldn’t be given a lot of thought. Most experts will agree that steganography has the capability of disrupting the forensic process when used correctly.

There are several steganography techniques used for hiding data such as batch steganography, permutation steganography, least significant bits (LSB), bit-plane complexity segmentation (BPCS) and chaos based spread spectrum image steganography (CSSIS).

There three types of steganography protocols used:

i. ***Pure Steganography*** is defined as a steganographic system that does not require the exchange of acipher such as a stego-key. This method of Steganography is the least secure means by which to communicate secretly between the sender and receiver can rely only upon the presumption that no other parties are aware of this secret message. Using open systems such as the Internet, we know this is not the case at all.

ii. ***Secret Key Steganography*** is defined as a steganographic system that requires the exchange of a secret key (stego-key) prior to communication. Secret Key Steganography takes a cover message and embeds the secret message inside of it by using a secret key (stego-key). Only the parties who know the secret key can reverse the process and read the secret message.

iii. ***Public Key Steganography*** is defined as a steganographic public key during the encoding process and only the private key, which has a direct mathematical relationship with the public key, can decipher the secret message. Public Key Steganography provides a more robust way of implementing a steganographic system because it can utilize a much more robust and researched technology in Public Key Cryptography. It also has multiple levels of security in that unwanted parties must first suspect the use of steganography and then they would have to find a way to crack the algorithm used by the public key system before they could intercept the secret message (Sadoon, 2009).

Audio Steganography Techniques

1. ***Echo Hiding*:** Echo hiding used to embeds secret data in a audio file by pass an echo into the discrete signal. This technique has advantages of providing a high data transmission rate and robustness when we make comparison of echo hiding to other methods.
2. ***Phase Coding*:** Phase coding exploits HAS insensitivity to relative phase of deferent spectral components. In this method we can replace selected phase components from the original sound signal spectrum with hidden information due to inaudibility of information, phase components medication should be kept small. It is a very effective coding methods in terms of the SNR ratio.
3. ***Parity Coding*:** This technique is one of the robust audio steganographic techniques. Instead of breaking a signal into individual samples, it breaks a signal into separate samples sections and embeds each bit of the secret message information from a parity bit.
4. ***Spread Spectrum*:** this technique spread out the encoded information across the available frequencies. This is analogous to a system using an implementation of the LSB coding that randomly spreads the message bits over the entire sound file. This method spreads the secret data over the audio file frequency spectrum which uses a code that is independent of the original signal.

   Advantage: It maintains a high level of robustness.

   Disadvantage: Quality of file is being effected due to presence of noise in audio file.
5. ***Tone insertion:*** Tone insertion used on the inaudibility of lower power tones in the presence of significantly higher ones. This method used resist to attacks such as low-pass filtering and bit truncation in cyber addition to less embedding capacity, embedded information could be maliciously extracted when inserted.
6. ***LSB (Least Significant Bit)*:** In LSB coding, the ideal data transmission rate is 1 kbps per 1 kHz. In LSB coding, two least significant bits of a data is replaced with two message bits. If we increase the amount of information encoded it will also increase the noise in the sound file. Like a sound file that was recorded in a bustling subway station would masklow-bit encoding noise (Navneet & Sunny, 2014).

2. Cryptography

Cryptography converts the original message in to non readable format and sends the message over an insecure channel. The people who are unauthorized to read the message try to break the non readable message but it is hard to do it so. The authorized person has the capability to convert the non readable message to the readable one (Monika & Pradeep, 2012).

The art of protecting information by transforming it (*encrypting* it) into an unreadable format, called cipher text, only those who possess a secret *key* can decipher (or *decrypt*) the message

into plain text. Cryptography is the practice and study of techniques for secure communication in the presence of third parties (called adversaries).

More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce (Bellare, et al, 2005).

Encrypted messages can sometimes be broken by cryptanalysis, also called *codebreaking*, although modern cryptography techniques are virtually unbreakable. As the Internet and other forms of electronic communication become more prevalent, electronic security is becoming increasingly important. Cryptography is used to protect e-mail messages, credit card information, and corporate data. One of the most popular cryptography systems used on the Internet is *Pretty Good Privacy* because it's effective and free (Webopedia, 2014).

Types of Cryptography

Encryption algorithms can be classified into two broad categories- Symmetric key Cryptography and Asymmetric Key Cryptography.

i. Symmetric Key Cryptography

In symmetric Cryptography the key used for encryption is similar to the key used in decryption. Thus the key distribution has to be made prior to the transmission of information. The key plays a very important role in symmetric cryptography since their security directly depends on the nature of key i.e. the key length etc. There are various symmetric key algorithms such as DES, TRIPLE DES, AES, RC4, RC6, BLOWFISH.

ii. **Asymmetric Key Cryptography**

In Asymmetric Cryptography, two different keys are used for encryption and decryption- Public and Private. The public key is meant for general use so it is available to anyone on the network. Anyone who wants to encrypt the plaintext should know the Public Key of receiver. Only the authorized person can be able to decrypt the cipher text through his own private key.

Private Key is kept secret from the outside world. Symmetric Encryption Algorithm runs faster as compared to Asymmetric key algorithms. Also the memory requirement of Symmetric algorithm is lesser as compared to asymmetric (Monika & Pradeep, 2012).

Cryptography Goals

There are five main goals of cryptography. Every security system must provide a bundle of security functions that can assure the secrecy of the system. These functions are usually referred to as the goals of the security system. These goals can be listed under the following five main categories:

i. ***Authentication*****:** The process of proving one's identity. This means that before sending and receiving data using the system, the receiver and sender identity should be verified.

ii. ***Privacy/confidentiality*****:** Ensuring that no one can read the message except the intended receiver. Usually this function is how most people identify a secure system. It means that only the authenticated people are able to interpret the message content and no one else.

iii. ***Integrity*****:** Assuring the receiver that the received message has not been altered in any way from the original. The basic form of integrity is packet check sum in IPv4 packets.

iv. ***Non-repudiation*****:** A mechanism to prove that the sender really sent this message which

means that neither the sender nor the receiver can falsely deny that they have sent a certain message.

v. ***Service Reliability and Availability*:** Since secure systems usually get attacked by intruders, which may affect their availability and type of service to their users. Such systems provide a way to grant their users the quality of service they expect.

3. Watermark

A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as audio or image data. It is typically used to identify ownership of the copyright of such signal. "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 (Ingemar, 2008). The needed properties of a digital watermark depend on the use case in which it is applied. For marking media files with copyright information, a digital watermark has to be rather robust against modifications that can be applied to the carrier signal. Instead, if integrity has to be ensured, a fragile watermark would be applied. Both steganography and digital watermarking employ steganographic techniques to embed data covertly in noisy signals. But whereas steganography aims for imperceptibility to human senses, digital watermarking tries to control the robustness as top priority. Since a digital copy of data is the same as the original, digital watermarking is a passive protection tool. It just marks data, but does not degrade it nor controls access to the data. A watermark is embedded into a digital signal at each point of distribution. If a copy of the work is found later, then the watermark may be retrieved from the copy and the source of the distribution is known. This technique reportedly has been used to detect the source of illegally copied movies. Digital watermarking may be used for a wide range of applications, such as:

1. Copyright protection
2. Source tracking (different recipients get differently watermarked content)
3. Broadcast monitoring (television news often contains watermarked video from international agencies)
4. Video authentication (Khan & Mirza, 2007).

Other Forms of Data Hiding

Other forms of data hiding involve the use of tools and techniques to hide data throughout various locations in a computer system. Some of these places include memory, slack space, hidden directories, bad blocks, alternate data streams and hidden partitions.

One of the more well known tools that is often used for data hiding is called Slacker. Slacker breaks up a file and places each piece of that file into the slack space of other files, thereby hiding it from the forensic examination software. Another data hiding technique involves the use of bad sectors. To perform this technique, the user changes a particular sector from good to bad and then data is placed onto that particular cluster. The belief is that forensic examination tools will see these clusters as bad and continue on without any examination of their contents (Rogers, 2005).

Encryption

One of the more commonly used techniques to defeat computer forensics is data encryption. File level encryption encrypts only the file contents. This leaves important information such as file name, size and timestamps unencrypted. Parts of the content of the file can be reconstructed from other locations, such as temporary files, swap file and deleted, unencrypted copies. Most encryption programs have the ability to perform a number of additional functions that make digital forensic efforts increasingly difficult. Some of these functions include the use of a key file, full-volume

encryption, and plausible deniability. The widespread availability of software containing these functions has put the field of digital forensics at a great disadvantage. The majority of publicly available encryption programs allow the user to create virtual encrypted disks which can only be opened with a designated key. Through the use of modern encryption algorithms and various encryption techniques these programs make the data virtually impossible to read without the designated key (Hal, et al, 2007).

Importance of Data Hiding

The most important reason for hiding the internal implementation details of a class is:

1. To prevent programmers from relying on those details, you can safely modify the implementation without worrying that you will break existing code that uses the class.
2. Another reason for encapsulation is to protect your class against accidental or willful stupidity. A class often contains a number of interdependent fields that must be in a consistent state. If you allow a programmer (including yourself) to manipulate those fields directly, he may change one field without changing important related fields, thus leaving the class in an inconsistent state. If, instead, he has to call a method to change the field, that method can be sure to do everything necessary to keep the state consistent. Similarly, if a class defines certain methods for internal use only, hiding these methods prevents users of the class from calling them.
3. When all the data for a class is hidden, the methods define the only possible operations that can be performed on objects of that class. Once you have carefully tested and debugged your methods, you can be confident that the class will work as expected. On the other hand, if all the fields of the class can be directly manipulated, the number of possibilities you have to test becomes unmanageable.
4. Internal fields and methods that are visible outside the class just clutter up the API. Keeping visible fields to a minimum keeps your class tidy and therefore easier to use and understand.
5. If a field or method is visible to the users of your class, you have to document it. Save yourself time and effort by hiding it instead.

Forensic implications of Data Hiding

Without question, the most frightening side effect of these digital warrens is the inability of modern forensic tools to easily recover the data. With workstations now shipping with RAID 5 stacks and terabytes of disk space, manual investigation of hard drives at the byte level is simply not viable. Today's crooks and criminals seldom take extraordinary measures to conceal data. Most of the forensics work in law enforcement involves very basic data recovery techniques with a few popular forensics tools. However, it would be unwise to expect this to continue, as crooks and their misdeeds become more sophisticated. A mainstay of modern forensics tools is a file carver. File carvers attempt to reconstruct the disk contents without using the operating system's meta-level information (Hal, et al, 2006).

Combining Steganography and Cryptography in Data Hiding

A system that combined the techniques of cryptography and steganography to provide efficient method of hiding data from any unauthorized users was presented. An audio medium was used for the steganography and the Least Significant Bit algorithm was employed to encode the message inside the audio file. This proposed system does not tamper with the original size of the file even after encoding and also suitable for any type of audio file format. The encryption and decryption techniques used with this system make its security more robust. (Abikoye, et al, 2012).

Those who seek the ultimate in private communication can combine encryption and steganography. Encrypted data is more difficult to differentiate from naturally occurring phenomena than plain text is in the carrier medium. There are several tools by which we can encrypt data before hiding it in the chosen medium. In some situations, sending an encrypted message will across suspicion while an invisible message will not do so. Both methods can be combined to produce better protection of the message. In case, when the steganography fails and the message can be detected, it is still of no use as it is encrypted using cryptography techniques.

The implementation of two techniques like Steganography and Cryptography will improve the security of the information secret. This combined will fulfill the prerequisites, e.g. memory space, security and strength for important information transmission across an open channel. It will also be a powerful mechanism which enables people to communicate without interference of eavesdroppers even knowing there is a style of communication in the first place. (Abdulzahra, et al, 2014).

Summary

Information Technology is one of the most essential aspects in today's world. Based on this computer application keeps developing to securely handle both the personal and financial data more effectively. These data are very important from every aspect and this has to be secured from unauthorized access. Information security is an aspect of information that deals with detecting and preventing unauthorized use of data, computer or network. Preventive measures enable us to stop unauthorized users from having access to any part of computer system (Bandyopadhyay & Roy, 2010).

Conclusion

The study showed the importance of data hiding techniques as stated below:

i. It can be used by other researchers in the field of information security
ii. It will increase the level of confidentiality of information exchanged over the internet
iii. Access to information by malicious individuals such as hackers will no longer be possible as they will be unable to locate which form of media was used to hide the information
iv. Government monitoring will be impossible as information hidden in other forms of media will go undetected by them
v. Man in the Middle Attacks will be rendered ineffective

References

Abdul. Elminaam, D. S., Abdul Kader, H. M., & Hadhoud, M. M. (2009). Performance Evaluation of Symmetric Encryption Algorithms. *Communications of the IBIMA,* 8, ISSN: 1943-7765

Abikoye, O. C., Adewole, K. S., & Oladipupo, A. J. (2012). Efficient Data Hiding System Using Cryptography and Steganography. *International Journal of Applied Information Systems*, 4, ISSN: 2249-0868.

Bandyopadhyay, S.K., & Roy, S. (2010). Information Security through Data Encryption And Data Hiding. *International Journal Of Computer Applications,* 4(12), ISSN: 0975 – 8887.

Bellare Mihir, Rogaway Phillip. (2005). *Introduction To Modern Cryptography*, 10.

Abdulzahra, H, Ahmad, R. & Noor, N. M. (2014). "Combining cryptography and steganography for data hiding in images," *ACACOS, Applied Computational Science*, pp. 978–960, 2014

Hardikkumar, V. D. (2012). Steganography, Cryptography, Watermarking: A Comparative *Study. Journal of Global Research in Computer Science*, 3(12).

IJO -INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND ENGINEERING

(ISSN: 2814-1881) Mojirade A. AWODUN *

https://ijojournals.com/ *Volume 07 || Issue 09|| September, 2024 ||*

Data Hiding Technique in Information Technology: A Review

Hal, B., David, H., & Michael, S. (2006). Data Hiding Tactics For Windows And Unix File Systems. w*ww.Berghel.Net/Publications/Data_Hiding/Data_Hiding.Php*

Ingemar, J. C. (2008). Digital Watermarking And Steganography. *Morgan Kaufmann, Burlington, Ma, Usa.*

Ishaque, M. Qudus, K., AbdulSattar, S. (2011). Investigation Of Steganalysis Algorithms For Multiple Cover Media. *Ubiquitous Computing And Communication Journal*, 6(5).

Iman, C. & Abi-Char, P. (2015). Comparative Analysis of block Cipher- Based Encryption Algorithms: A survey. *Information Security and Computer Fraud, 3(1), 1-7.*

Khan, A., & Mirza, A. M. (2007). *Genetic Perceptual Shaping: Utilizing Cover Image And Conceivable Attack Information During Watermark Embedding. Infusion,* 8(4), 354-365.

Megias D., Mazurczyk W. & Kuribayashi M. (2021), Data Hiding and its Applications: Digital watermarking and Steganography. *Appl. Sc. 2021, 11, 10928. https://doi.org/10.3390/app112210928.*

Monika, A., & Pradeep, M. (2012). Cryptography Based On Blowfish Algorithm. *International Journal Of Engineering And Advanced Technology (IJEAT)*, 1(6). ISSN: 2249 – 8958

Navneet, K. & Sunny, B. (2014). Audio Steganography Techniques-A Survey. *Navneet Kaur Int. Journal of Engineering Research And Applications.* 4(6). Pp.94-100. ISSN : 2248-9622,

Nosrati, M., Karimi, R., Nosrati, H., & Nosrati, A. (2011). Embedding Stego-Text In Cover Images Using Linked List Concepts And Lsb Technique. *Journal Of American Science,* 7(6), 97-100.

Pramendra Kumar & Vijay Kumar S. (2014). *Information Security Based on Steganography & Cryptography Techniques: A Review. International Journal of Advanced Research in Computer Science and Software Engineering. 4(10).*

Raju, H., Shantanu, P., & Agostino, C. (2010). Watermarking Techniques for Relational Databases: Survey, Classification and Comparison. The Journal of Universal Computer Science, 16(21),

Rogers, D. M. (2005). Anti-Forensic Presentation Given To Lockheed Martin. San Diego.

Sadoon Hussein Abdullah. (2009). *Steganography Methods And Some Application (The Hidden Secret Data In Image).*

Vikram, M. A., & Keyuri, M. Z. (2014). Methods And Approach For Secure Steganography. *Vikram M Agrawal Et Al, Int. J. Computer Technology & Applications*. 5 (3), ISSN 1045-1080.

http://www.webopedia.com/TERM/C/cryptography.html 2014.

http://www.watermarkingworld.com/digital_watermarking

Cory Janssen(2014)