DATA HIDING TECHNIQUES: A Review

[1]Akanksha Chaturvedi, [2]Shikha Chaudhary,[3]Shyam Lal Jat, [4]Vijay Kr. Sharma
akankshachaturvedi138@gmail.com , shikha.chaudhary18@gmail.com, shyam5815@gmail.com,
vijaymayankmudgal2008@gmail.com
Department of Computer Science & Engineering
Rajasthan Institute of Engineering & Technology, Jaipur

Abstract : Today's time security is great concern in every field of computer. Protection of data is very basic requirements when there is a need of send the data or message over the network. Every day attacker tries to break the security. Encryption, Water marking and steganography are the basic technique to protect the data. Both the Watermarking and steganography are used to protect the data when the data is very important or more security is required. In this paper we present the data hiding techniques in detail.

1. **Introduction:**

Information Security system is a such type of system in which we are protecting information's from unauthorized access, unauthorized communication of data and use that.

The information security system is a combination of security of communication and computer security. Physical securityis also included as well as which is need because of natural disaster theft and many other[1][2][3].

A secure communication and data management in any department needs following types of security to protect the data and communication.

I. Personal Security:-To provide the security to the personal information of individual or a group of individuals in terms of communication and operations.

II. Physical Security:- This security needs to protect physical entities.

III. Information Security :- To protect information and data from the unwanted entities.

IV. Operation Security:-To protect the data which is used in operations or in a series of activities.

V. Communications Security:To protect communication between twoor more individuals,groups,organizations.

VI. Network Security :-To protect the networks and connections by unauthorized access.

2. Components Of Information Security

I. **Integrity :** Integrity refers to the truthfulness of data or resources, and this term is used to prevent the data or information from improper or unauthorized change. Integrity can be of many types like data integrity,origin integrity and many more.The data integrity is related to the content of the information while the origin integrity is related to the source of the data. The main purpose of integrity is to ensure that information remains intact and unaltered. This means watching out for alterations through malicious action, natural disaster, or even a simple innocent mistake. Integrity includes both the correctness and the trustworthiness of the data.

II. There are two additional objectives also :

Authenticity: The meaning of authenticity is being original and trust worth or verifiable. It is essential to ensure that the data, communication, transaction are genuine which is used in the e-business, banking sector and government organizations. It is important to validate the authorized users who are using it.

Accountability: Accountability has actions of an entity can be graphed individually to that entity which supports no repudiation, deterrence, fault isolation, intrusion, detection and prevention. Non-repudiation means one's intention to satisfy their constraint to a contract. It also means that both the parties cannot deny the transactions received or transferred in between them.

III. **Confidentiality:** Confidentiality is the obscuration of information or resources. It means the information is seen only by the authorized people. this is the most common aspect to keep the information secret from unauthorized access for information security. The basic need to hold the information secure from the use of computers in insightful fields such as government and many industry. In today’s scenario, there are many sensitive fields in the world of computers like government organizations, banking sectors and industries. These sectors need secrecy to protect the information which they have or communicate.

IV. **Availability:** The ability to use the desired information and the resource is termed as availability. Availability means when we need the information we can access it. The information needs to be available only to the authorized user and applications which are used by an organization. Information has no use if it is not available. In some circumstances information needs to be varied constantly, which means that it must be reachable to those certified users to access it. The condition of availability that is related to security is that anyone may intentionally arrange to refuse access to data or to a service by making it unavailable.

3. Types of Data Hiding Techniques:

1. **Steganography:** Steganography is the art and science of writing hidden messages where only the sender and receiver can find the existence of the image[4][5][6].

Techniques of steganography:

- Digital
- Printed
- Network
- Digital text etc.

2. Watermarking:

Digital Watermarking defines methods and technologies that hide information, for example a number or text, in digital media, such as images, video or audio. The hiding process has to be such that the changes of the media are imperceptible. This means that the modifications of the pixel values have to be invisible for images. Depending on the application, the watermark must be either robust or fragile. By "robust", we mean the capability of the watermark to resist manipulations of the media, such as loss compression (where compressing data and then decompressing it retrieves data that may well be different from the original, but is close enough to be useful in some way), scaling, and cropping, among others. The watermark may need to be fragilein some cases. "Fragile" means that the watermark must not resist tampering, or would resist only up to a certain, predetermined extent[1][4][7].

Watermarking Properties

Watermarking demands advantageous properties which is based on the application of watermarking system. Some of the properties are as follow

I. Effectiveness: Effectiveness is the important property for the watermark process.This means that the watermark should be detective to achieve the goal of the watermarking.

II. Host signal Quality:In the process of watermarking, host signal(image, video, audio etc.)should not effect too much that it creats changes in the signal quality.The watermark should be unnoticeable.

III. Watermark Size :Watermark is generally use to owner identification or security verification of host signal and it always use when data is transmitted. So it is important that the dimensions of watermark should be minimum because it will enhance the size of data to be transmitted.

IV. Robustness: Robustness is crucial premises for all watermarking systems. There are so many purpose by which watermark is degraded, altered during transmission, attacked by hackers in corporative media applications. So watermark should robust, So that it bear up against all the attacks and threats.

Conclusion: The paper tells the basic need or importance of the data hiding in today's daily life. So development steps of Water marking and steganography technique are similar but according to their use they different then each other. Watermarking is used to copyright operations but for data protection point of view one can use the steganography technique.

Reference

[1]. Cox I. J., Kilian J. Leighton F. T. and Shamoon T. 1997, " Secure Spread Spectrum Watermarking for Multimedia". IEEE Trans. On Image Processing, Vol. 6, No. 12, pp. 1673- 1687.

[2]. 25] Neubauer C. and Herre J. 2000a, "Audio Watermarking MPEG-2 AAC Bitstream", 108th AES Convention, Audio Engineering Society Preprint 5101- 5176.

[3]. Baras, C.; Moreau, N.; Dymarski, P.; , "Controlling the inaudibility and maximizing the robustness in an audio annotation watermarking system," Audio, Speech, and Language Processing, IEEE Transactions on , vol.14, no.5, pp.1772-1782, Sept. 2006doi: 10.1109/TASL.2006.879808

Alomari R S, Al-Jaber Ahmed; "A Fragile Watermarking Algorithm for Content Authentication "; International Journal of Computing & Information Sciences; Vol-2; Issue 1; pp 27-37; April 2004.

[4]. Sharma V.K., Srivastava D.K. (2017) Comprehensive Data Hiding Technique for Discrete Wavelet Transform-Based Image Steganography Using Advance Encryption Standard. In: Vishwakarma H., Akashe S. (eds) Computing and Network Sustainability. Lecture Notes in Networks and Systems, vol 12. Springer, Singapore.

[5].Bender, W., Gruhl, D., & Morimoto, N. (1996). Techniques for data hiding. IBM Systems Journal, 35(3), 313-336.

[6].Vijay Kumar Sharma,Dr. Devesh Kr Srivastava and Dr. Pratistha Mathur, "A Study of Steganography Based Data Hiding Techniques", International Journal of Emerging Research in Management & Technology,ISSN: 2278 - 9359 (Volume - 6, Issue -4), April 2017.

[7]. S. Katzenbeisser and F. A. P. Petitcolas, Hiding Techniques for Steganography and Digital Watermarking, S. Katzenbeisser and F. A. P. Petitcolas, Eds. Boston, MA: Artech House, 2000.