ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

Steganography, Cryptography and Watermarking: A Review

Suraj Kumar Dubey [1], Vivek Chandra [2]

PhD Scholar, Department of Computer Science, MATS University, Raipur, Chhattisgarh, India[1]

Professor, Department of Electrical and Electronics Engineering, CSIT, Durg, Chhattisgarh, India[2]

ABSTRACT: In this digital era, it is simple to produce and create multiple copies of the data which can either be text, audio, image, softwares etc. This creates a problem concerning the protection of the intellectual and production rights. The problem may be solved by information hiding techniques that hides the important data. This paper presents an overview of basics information hiding techniques. The paper concludes with the application areas of information hiding techniques.

KEYWORDS: Steganography, Cryptography, Watermarking.

I. INTRODUCTION

Information/Data hiding is an act of protecting information/data from any inadvertent change. It can also be defined as the process of hiding the details of an object. A common use of information hiding is to hide the data so that if it is changed, the change is restricted to a small subset of the total data. It helps to prevent programmers from intentionally or unintentionally changing parts of a program. Information hiding techniques are categorized as: Steganography, Cryptography and Watermarking [1]. The three main categories of information hiding techniques are shown in figure 1.

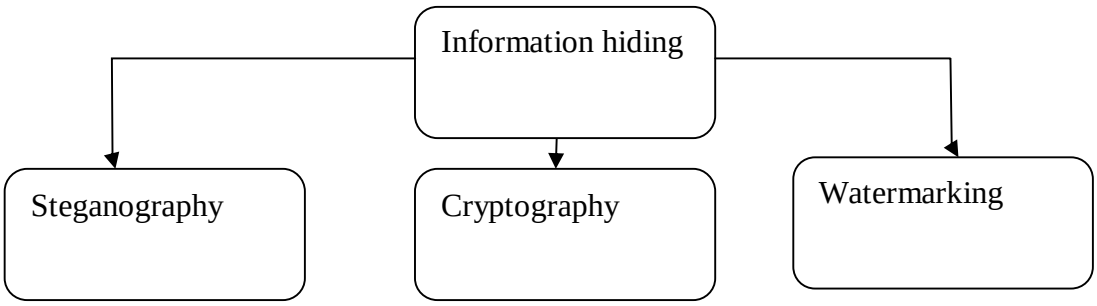

Figure 1: Information hiding techniques

II. STEGANOGRAPHY

It is a science of hiding information from unauthorized person. Steganography is a practice of concealing a file, message, image, or video within another file, message, image, or video. A basic steganography model is shown in figure 2.

The secret message and the cover message are first fed to encoder using steganography techniques and then the same encryption algorithm in reverse order is implemented to recover the original secret message and the original cover. Key plays very important role for retrieving the original message.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

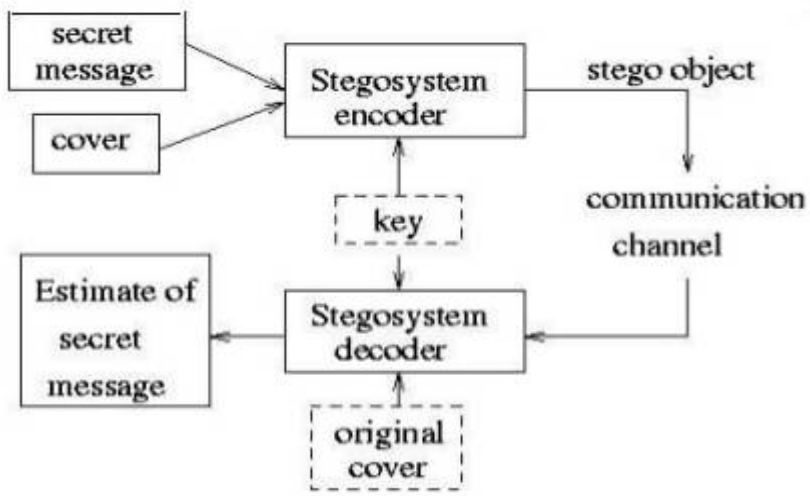

Figure 2. Process of Steganography

The advantage of steganography is that the message to be transmitted is not detectable to the casual eye. In fact, unauthorized people should not even suspect that a hidden message exists. Digital steganography is the art of hiding data within data. Goal of steganography is to hide data well enough that unintended recipients do not suspect the steganography medium of containing hidden data [2]. Media files are ideal for steganography transmission because of their large size. Steganography can be split into two types i.e. Fragile and Robust [3][4].

Fragile: It involves embedding information into a file which is destroyed if the file is modified. This method is not suitable for recording the copyright holder of the file since it can be so easily removed. It is useful in situations where it is important to prove that the file has not been tampered. This technique is considered to be easier for implementation than robust methods.

Robust: Embedded information cannot be easily destroyed. The watermark should be hidden in a part of the file where its removal would be easily perceived.

III. CRYPTOGRAPHY

Human being from ages had two inherent needs (i) to communicate and share information and (ii) to communicate selectively. These two needs gave rise to the art of coding the messages in such a way that only the intended people could have access to the information. Unauthorized people could not extract any information, even if the scrambled messages fell in their hand. Steps involved in cryptography are shown in figure 3.

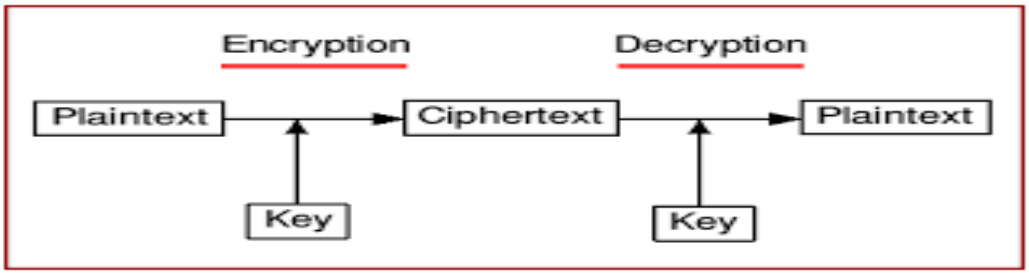

Figure 3: Cryptography model

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

The plaintext and key are used to encrypt the original message. The encrypted message is called as ciphertext. Decryption is the reverse, in other words, moving from the unintelligible ciphertext back to plaintext. The original plain text is retrieved using the same key[5].

Encryption: The process of locking up information using cryptography is encryption. Locked information is encrypted message.

Key: A secret, similar to password that is used during encryption and decryption.

Decryption: The process of unlocking encrypted information using cryptography.

A cryptosystem is an implementation of cryptographic techniques and their accompanying infrastructure to provide information security services. Cryptosystems are divided as [6]:

- **Cryptography:** It is an art of making cryptosystem capable of providing information security.
- **Cryptanalysis:** It is an art of breaking the cipher text.

Cryptography deals with the cipher text for transmission or storage. It involves the study of cryptographic mechanism with the intention to break them. Cryptanalysis is also used during the design of the new cryptographic techniques to test their security strengths.

IV. WATERMARKING

A watermark is a form of text or image that is impressed onto a text or image which provides evidence of its authenticity. Digital watermarking is an extension of watermarking concept in digital world. Watermarking embeds a signal directly into the data and the signal becomes an integral part of the data, travelling with the data to its destination. Here, it can be assumed that the valuable data is protected as long as the watermark is present (and detectable) in it. Thus, the goal of a watermark must be to always remain present in the host data. A digital watermark life cycle is shown in figure 4.

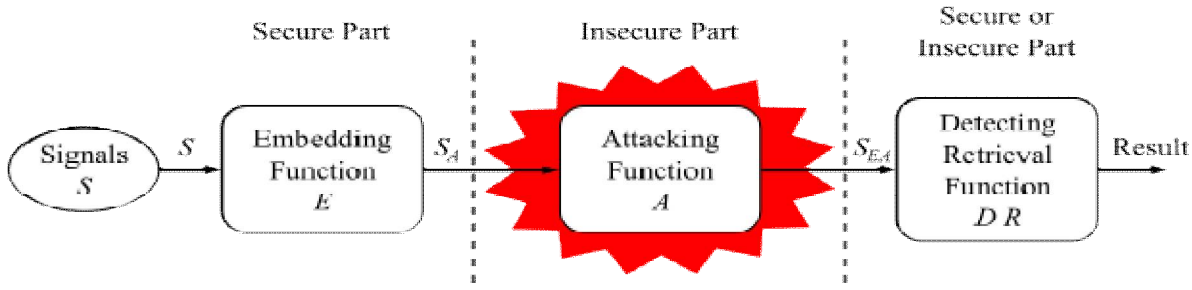

Figure . 4: Digital watermark life-cycle phases with embedding, attacking, and detection and retrieval functions(Google Source)

In this the data is embedded with the watermark and is allowed to travel through the channel (which is insecure). And finally the water is extracted to check authenticity of the data [7].

Watermarking is of two types- visible watermarking and invisible watermarking.

- **Visible Watermarking**: It refers to the information visible on the data. Visible watermarks are typically logos or text.
- **Invisible Watermarking**: It is not visible or perceivable, but it can be detected by different means. It may also be a form or type of steganography and is used for widespread use. It can be retrieved easily.

V. STEGANOGRAPHY VS WATERMARKING[8][9]

- Steganography involves hiding the intended message within a seemingly harmless message whereas cryptography involves coding the message using an encryption key and sending it as cipher text.
- In steganography, information is just hidden while in watermarking it hidden and protected.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

- Robustness: This criterion is different in both the cases. Steganography is mainly concerned with detection of the hidden message while watermarking concerns potential removal by a pirate.
- Steganographic communications are one- to- one while watermarking techniques are usually one-to-many.
- A steganography/watermarking system is considered as insecure already if the detection of steganography/watermarking is possible.

VI. CRYPTOGRAPHY VS STEGANOGRAPHY[10][11][12][13]

- Cryptography is the study of hiding information, while steganography deals with composing hidden messages so that only the sender and the receiver know that the message even exists.
- In Cryptography, the encrypted message is visible to the all whereas in steganography, only the sender and the receiver know the existence of the message.
- Cryptographic methods try to protect the content of a message while steganography hide both the message as well as the content.
- Cryptography involves the use of mathematics and number theory to hide data. Not much mathematics is involved in steganography.
- In steganography, the insertion of the secret data should not affect the quality of the message file. The secret code is visible to the opponent in case of cryptography.
  By combining Steganography and Cryptography one can achieve better security.

VII. APPLICATIONS

Steganography is applicable to, but not limited to, the following areas [14][15].

- To establish secure and secret communications where cryptographic encryption methods are not available.
- Steganography is utilized military applications, where the two parties' communications are of large importance.
- The health care, and especially medical imaging systems, may very much benefit from information hiding techniques.
- These techniques are applied for protection of data alteration.
- Steganography is also applicable to media database systems.

Cryptographic techniques are utilized in following domains [16][17]

- Authentication/Digital Signatures: Authentication is the process by which claimed identities of users are verified.
- Secure Communication is the most straight forward use of cryptography.
- Another application of cryptography, called secret sharing, allows the trust of a secret to be distributed among a group of people.
- Time stamping which uses blind signature schemes that allow the sender to get a message receipted by another party without revealing any information about the message to the other party.
- Electronic money transfer techniques are utilizing cryptographic concept for secure transfer of funds.
- Secrecy in storage is usually maintained by a one-key system and the key is provided at the beginning of sessions.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

Applications of watermarking [18][19][20]

- Temper proofing to find out if the data was tempered.
- Ownership Assertion to prove ownership
- Fingerprinting to identify the buyer of the content
- Broadcast monitoring to determine royalty payments.

VIII. CONCLUSION

Information hiding plays an important role in protecting, maintaining secrecy in this digital world. In this paper basics of the three information hiding techniques i.e. steganography, cryptography and watermarking were discussed. Differences in between the techniques were also explored. The application areas of the techniques are also provided.

REFERENCES

[1] Dhand, Geetika. "Information Hiding Techniques.", In proceeding of the national conference, INDIAcom-2008.
[2] Katzenbeisser, Stefan, and Fabien Petitcolas, “Information hiding techniques for steganography and digital watermarking”, Artech house, 2000.
[3] Petitcolas, Fabien AP, Ross J. Anderson, and Markus G. Kuhn, "Information hiding-a survey.", Proceedings of the IEEE , Vol. 87, No. 7, pp.1062-1078, 1999
[4] Cummins, Jonathan, Patrick Diskin, Samuel Lau, and Robert Parlett, "Steganography and digital watermarking", School of Computer Science, The University of Birmingham Vol. 14, No. 60, 2004.
[5] Menezes, Alfred J., Paul C. Van Oorschot, and Scott A. Vanstone., “Handbook of applied cryptography”, CRC press, 1996.
[6] Mao, Wenbo., “Modern cryptography: theory and practice”, Prentice Hall, Professional Technical Reference, 2003.
[7] Schneier, Bruce., “Applied cryptography: protocols, algorithms, and source code in C”, John Wiley & Sons, 2007.
[8] Desai, Hardikkumar V, "Steganography, Cryptography, Watermarking: A Comparitive Study.", Journal of Global Research in Computer Science, Vol. 3, No. 12, pp. 33-35, 2013.
[9] Bailey, Karen, and Kevin Curran, "An evaluation of image based steganography methods.", Multimedia Tools and Applications, Vol. 30, No. 1, pp. 55-88, 2006.
[10] Suryakant, P.V., Bhosale, R.S. and Panhalkar, A.R., “A novel security scheme for secret data using cryptography and steganography” International Journal of Computer Network and Information Security, Vol. 4, No. 2, pp.36, 2012.
[11] Manoj, I. Venkata Sai, "Cryptography and steganography.", International Journal of Computer Applications , Vol . 1, No. 12, pp. 63-68.,2010.
[12] Singh, N. Suresh, AR Sajeev Ambi, and M. Sreelal, "Cryptography & Steganography.", Biometrics and Bioinformatics, Vol. 5, No. 6, pp. 245-248, 2013.
[13] Joseph, A., and V. Sundaram., "Cryptography and Steganography–A survey.", 2011
[14] Johnson, Neil F., and Sushil Jajodia, "Exploring steganography: Seeing the unseen.", Computer, Vol. 31, No. 2 , 1998.
[15] Fridrich, Jessica., “Steganography in digital media: principles, algorithms, and applications”, Cambridge University, Press, 2009.
[16] Konheim, Alan G, "Applications of Cryptography." , Computer Security and Cryptography, pp. 480-505.
[17] Ryabko, Boris, Jaakko Astola, and Mikhail Malyutov., "Applications to Cryptography.", In Compression-Based Methods of Statistical Analysis and Prediction of Time Series, Springer International Publishing , pp. 45-70., 2016.
[18] Saini, Lalit Kumar, and Vishal Shrivastava. "A survey of digital watermarking techniques and its applications." arXiv preprint arXiv:1407.4735 , 2014.
[19] Cox, Ingemar J., Matthew L. Miller, and Jeffrey A. Bloom. "Watermarking applications and their properties." In Information Technology: Coding and Computing, 2000. Proceedings. International Conference on, pp. 6-10. IEEE, 2000.
[20] Cox, Ingemar J., Matthew L. Miller, Jeffrey Adam Bloom, and Chris Honsinger. *Digital watermarking*. Vol. 1558607145. San Francisco: Morgan Kaufmann, 2002.