International Journal of Enterprise Computing and Business Systems
ISSN (Online) : 2230-8849
Volume 5 Issue 2 July 2015
International Manuscript ID : ISSN22308849-V5I2M98-072015

SAFETY AND CONCEALING INFORMATION UTILIZING COMBINATORIAL DATA HIDING PROFICIENCIES

Bhavsar Dharmeshkumar Bhalchandra
Research Scholar
Shri Venkateshwara University
Uttar Pradesh, India

Dr. Parveen Kumar
Professor
Shri Venkateshwara University
Uttar Pradesh, India

ABSTRACT

Steganography and Watermarking are proficiencies which forbid unauthorized users to have entry to the significant data. Though both has the same aim as Cryptography but with a different approach. The Steganography and digital watermarking provide methods which users may conceal and mingle their data amongst other data which made them unmanageable to recognize by attackers. Conveying secret data and establishing hidden relationship has been a great interest. Steganography/watermarking and Encryption both pertains to the art and science of hiding a secret message in a cover media such as picture, text, signals or sound in such a way that no one, except the intended recipient knows the existence of the data. In this paper, we review certain proficiencies of steganography and digital watermarking and the difference these technologies have from Encryption proficiencies.

International Journal of Enterprise Computing and Business Systems
ISSN (Online) : 2230-8849
Volume 5 Issue 2 July 2015
International Manuscript ID : ISSN22308849-V5I2M98-072015

I. INTRODUCTION

Because of the rapid innovation of applications programming on the Internet in the past two decades, there has been increasing interest in means of concealing data in other data [1]. Much proficiency is useable to forbid unauthorized users from replicating data without proprietor license [2, 3]. Two of these proficiencies are cryptanalysis and steganography [4, 5]. Users may conceal significant data amongst an image by utilizing an invisible watermark when they communicate data. Moreover, a visible watermark may be utilized in many applications such as author, creator, and document. Cryptography is other technology for hiding data employing Keys and changing data.

Steganography is the art of communicating in a way which hides a secret message in the central data. A watermark can be perceived as an attribute of the carrier. It shall comprise data such as copyright, license, tracking and authorship. Their earliest use seems to have been to record the manufacturer's trademark on the product so that the authenticity could be clearly established without degrading the aesthetics and utility of the stock. [6].

In this paper we shall discuss the data hiding techniques available and how Steganography/watermarking becomes more significant in conjunction with cryptography.

Following figure shows dissimilar techniques of data hiding [7].

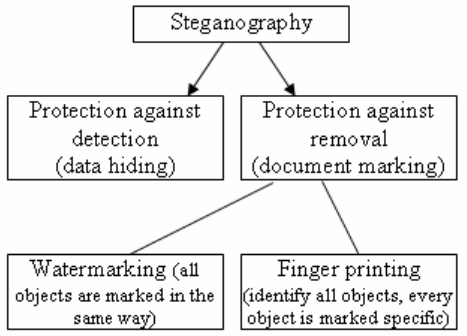

Figure-1. Data Hiding Techniques.

II. CRYPTOGRAPHY vs. STEGANOGRAPHY

Users on the internet have to send, share or receive confidential data most of the time [8]. With the increasing count of users and the increasing count of unauthorized access of confidential data, data safety played an important role. Therefore, the central matters now are to mitigate and to lessen the affect of the chances of the data being detected throughout transmission. Cryptography deals message encryption but the communication is easily aroused suspicious but on the other hand, steganography deals with secret message hiding but the communication is invisible. This is the major differences amongst cryptography and steganography.

It is often thought that by encrypting the traffic, the communications will be secured but this has not been

International Journal of Enterprise Computing and Business Systems

ISSN (Online) : 2230-8849

Volume 5 Issue 2 July 2015

International Manuscript ID : ISSN22308849-V5I2M98-072015

adequate in real live situation [9]. In cryptography technique, people turn aware of the existence of data by observing coded data, although they are unable to comprehend the data. Steganography hides the existence of the message so that intruders can't detect the communication and thus provides a higher level of safety than cryptography. Both steganographic and cryptographic systems provide secret communications but dissimilar in terms of system breaking. If the intruder can read the message in cryptographic then it is broken but steganographic is considered broken once the intruders detect the existence of the secret message [28]. Steganography system is more fragile than cryptography systems in terms of system failure. This is because if the communication is detected even without decoding the message, a steganographic system is considered a failure [10].

III. STEGANOGRAPHY AND WATERMARKING

In the given steganographic model, message is the data that the sender wishes to remain it confidential. It can be plain text, ciphertext, other image, or anything that can be embedded in a bit stream such as a copyright mark, a covert communication, or a serial count.

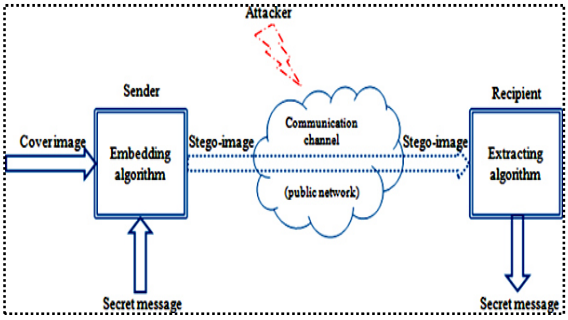

Figure-2. **Steganographic Process Model**.

Password is known as stegocentral, which ensures that only recipient who knows the corresponding decoding central will be able to extract the message from a cover-object. The cover-object with the secretly embedded message is then called the stegoobject.

Figure-3. **Steganographic Process Model**.

In the above figure image before steganography and after steganography has been shown.

Engrafting and Detection Processes

In engrafting process the secure data will be engrafted into the host data erstwhile call cover data

International Journal of Enterprise Computing and Business Systems
ISSN (Online) : 2230-8849
Volume 5 Issue 2 July 2015
International Manuscript ID : ISSN22308849-V5I2M98-072015

and send to the destination. User may utilize secret keys. First, symmetric key which both sender and receiver have the same key for encryption and decryption data. Second, asymmetric key both transmitter and receiver utilizes dissimilar kinds of keys. Watermarked data is the data which has to be sent to destination which comprises of mixing logo, cover and key data which seems to anyone which is one piece of data [11]. Figure-4 demonstrates engrafting process.

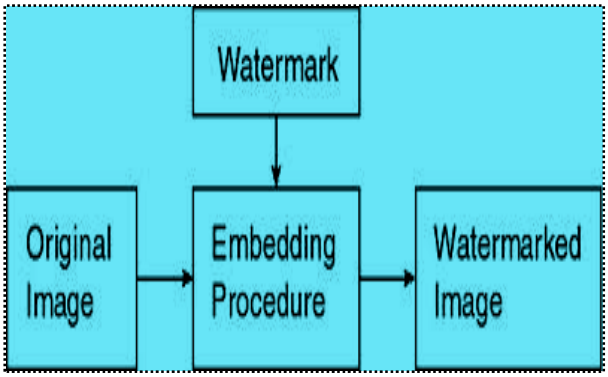

Figure-4. Watermark Engrafting Process

In detection process, when the watermarked data reaches to the destination as one piece of data which in reality it is a group of mixed data. The logo data will be extracted from the mixed data by utilizing key. Splitting of those three signals needs to utilize one of proficiencies in both spatial and frequency domains. The extraction process depends on the kind of the algorithm which utilize the quality of recovered signals is dissimilar from utilizing one algorithm to others. Also the count of decomposition levels which is utilized in engrafting process affects directly to the quality of the data which have been sent it by user which is utilizing the same count of reconstructions levels [12]. Figure-5 demonstrates detection process.

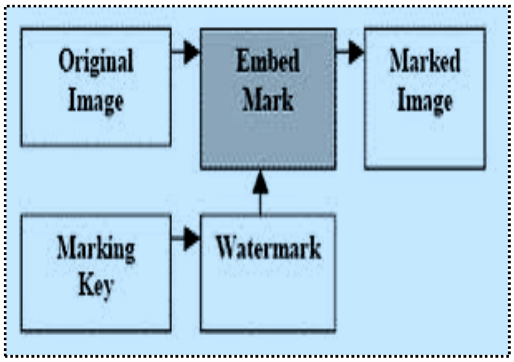

Figure-5. Watermark Detection Process

IV. CONCLUSION

In spite of many vantages of the internet, it has also unfolded a novel mean for invasion of our secrecy and intellectual property by unauthorized users. In recent technology era due to the quick development in data Technology and Communication and the Internet, the safety of the data and the data has elevate concerned. Every day, confidential data has been compromised and unauthorized access of data has crossed the limits. Great measures must be taken

to secure the data and data [13,14]. Steganography and Encryption are rescue to address these aspects. Steganography combined with encryption will be a powerful and effective tool that provides high level of safety [15, 16].

In this paper, review of steganography and watermarking has been shown. This paper further highlighted a review of research and development of Steganography and watermarking and with an intent to find their difference with usage of encryption technology. It is suggested that future research like Steganalysis, technology Watermarking Engrafting combined with Encryption, discover advanced platform and possible unbreakable algorithms.

V. REFERENCES

[1] Chang, C.-C., Chuang, J.-C., & Lin, P.-Y. (2013). A grayscale image steganography established upon discrete cosine transformation. [Technical report]. Journal of Digital Data Management, 8(2), 88+.

[2] McBride, B. T., Peterson, G. L., & Gustafson, S. C. (2009). A novel blind method for detecting novel steganography. Digital Investigation, 2(1), 50-70. doi: 10.1016/j.diin.2005.01.003

[3] Min-Jen, T., & Jung, L. (2011, 6-9 Nov. 2013). The quality evaluation of image recovery assault for visible watermarking algorithms. Paper presented at the Visual Communications and Image Processing (VCIP), 2011 IEEE.

[4] Husainy, M. A. F. A. (2009). Image steganography by representing pixels to letters. [Report]. Journal of Computer Science, 5(1), 33+.

[5] Ibrahim, B., Jabri, R., & Zoubi, H. A. (2012). Data concealing: a generic approach. [Technical report]. Journal of Computer Science, 5(12), 933+.

[6] "Steganography: The art of hide data in a plain sight", IEEE, February/March, 2009.

[7] Fabien A.P. Petitcolas, Ross J. Anderson, and Markus G. Kuhan, "data hiding – A Survey", Proceedings of the IEEE, July, 1999, Vol. 87, No.7.

[8] Arvind Kumar and Km. Pooja "Steganography- A Data Hiding Technique", International Journal of Computer Applications (0975 – 8887) Volume 9– No.7, November 2012.

[9] Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn "data Hiding A Survey "Proceedings of the IEEE, special matters on security of multimedia content, 87(7):1062{1078, July 1999.

[10] Banasthali Vidyapith, Rajasthan "picture Steganography Techniques: A Review Article", Bulletin of Engineering, Faculty of Engineering, Hunedoara, Romania, July-September,2013.

[11] Adel Almohammad "Steganography-established Secret and dependable Communications: Improving Steganographic Capacity and Imperceptibility" A thesis submitted for the level of Doctor of Philosophy, Department of data Systems and Computing, Brunel University, August,2013.

[12] El-Emam, N. N. (2007). Concealing a large amount of data with high security utilizing steganography algorithm. [Article]. Journal of Computer Science,

ISSN (Online) : 2230-8849
Volume 5 Issue 2 July 2015
International Manuscript ID : ISSN22308849-V5I2M98-072015

3(4), 223+.

[13] Farshchi, S. M. R., & Toosizadeh, S. (2014). High secure communication utilizing chaotic double compression steganography proficiency. [Report]. International Journal of Research and Reviews in Computer Science, 527+.

[14] T. Morkel , J.H.P. Eloff and M.S. Olivier "An Overview of picture Steganography".Dec 2013

[15] Amanpreet Kaur, Renu Dhir, and Geeta Sikka "A advanced picture Steganography established On First Component Alteration Technique" (IJCSIS) International Journal of Computer Science and data safety,Vol. 6, No. 3, 2009.

[16] Nagham Hamid, Abid Yahya, R. Badlishah Ahmad and Osamah M. Al-Qershi "ImageSteganography Techniques: An Overview" International Journal of Computer Science and safety (IJCSS), Volume (6): matters (3): 2013.