

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320-088X

IJCSMC, Vol. 3, Issue. 6, June 2014, pg.275 – 278

REVIEW ARTICLE



A REVIEW ON DATA COMPRESSION USING STEGANOGRAPHY

Tamanna Garg, Sonia Vatta

School of Computer Science & Engineering

Bahra University, Shimla Hills, India

garg.tamanna1@gmail.com, soniavatta@yahoo.com

Abstract – This paper presents a review of steganography and various steganography techniques used for data compression. The purpose is to have a deep study of various steganographic techniques used for data compression. The main objective is to find out a technique, which can hide a large amount of data. To fulfil the purpose, various researches and projects done earlier are taken into consideration.

Keywords - steganography, cryptography, LSB, embedding, extraction, secret key, compression

I. INTRODUCTION

Steganography is related with hiding of data in any kind of media in such a way that only the sender and the intended recipient could know about the existence of the message. The word steganography is originated from two Greek words Steganos and Graphei. Steganos meaning “covered or protected” and graphei meaning “writing”. So the meaning of Steganography is “Concealed writing”. The first use of the term was in 1499 by Johannes Trithemius. Steganography includes the concealment of information within media files. Media files are ideal for steganographic transmission because of their large size. For example, a sender might start with a random image file and adjust colour of every 120th pixel to correspond to a letter in the alphabet, a change that someone not specifically looking for it is unlikely to notice it.

In this work, a review of steganography and various steganography techniques related to the enhancement in data compression rate and security of the hidden data has been narrated. This review will help the future researchers to find the questions to carry out further research in the field. This literature review has been done in order to find out the limitations in earlier works.

II. REVIEW OF LITERATURE

In any research field, the review of literature provides great help to find the limitations to bring further improvements in the field. So in relation to that many research developments have been taken into consideration.

Great scholar **James C. Judge** in his work on ' **Steganography: Past, Present, Future**' stated that steganography is the term applied to any number of processes that will hide a message within an object, where the hidden message will not be apparent to an observer [1]. **Muhalim bin Mohamed Amin et al** in their project on ' **Information Hiding Using Steganography**' has put forward that the system used to enhance the compression rate using LSB technique by randomly dispersing the bits of the message in the image. This technique makes it harder for unauthorized people to extract the original message[2].The pioneer researcher **T. Morkel et al** in their work on ' **An Overview of Image Steganography**' asserted that different applications have different requirements of the steganography technique used. For example, some applications may require absolute invisibility of the secret information, while others require a larger secret message to be hidden [3].

Shawn D. Dickman in his project on ' **An Overview of Steganography**', stated that Steganography is a useful tool that allows covert transmission of information over an overt communications channel [4]. **Namita Tiwari et al** in their research on ' **Evaluation of Various LSB based methods of Image Steganography on GIF File Format** 'proposed that many different carrier file formats can be used, but digital images are the most popular because of their frequency on the Internet[5]. **English, R.** in his work on ' **Comparison of high capacity steganography techniques**', stated the implementation of the Bit Plane Complexity Segmentation (BPCS) algorithm and provide a comparison in terms of effectiveness and hiding capacity with the least significant bits algorithm (LSB) using 4 bits. The BPCS algorithm provided a much more effective method for obtaining a 50% capacity since visual attacks did not suffice for detection [6].

Prominent research scholar **Yongzhen Zheng et al** in their work on ' **Identification of Steganography Software based on Core Instructions Template Matching** ' proposed an approach, which was based on the principles of LSB Replacement Steganography algorithm and which was used to identify steganography software by Core Instructions Template Matching [7]. **Saddaf Rubab and Dr. M. Younus** in their research on ' **Improved Image Steganography Technique for Colored Images using Huffman Encoding with Symlet Wavelets**' stated a new devised algorithm to hide text in any colored image of any size using Huffman encryption and 2D Wavelet Transform. The results proved that there is very negligible image quality degradation. It gives more capacity for larger image sizes. It enhances security and also preserves the image quality. By inserting Huffman codes into the three components of colored image it becomes complicated [8]. **Amit Asthana and Sherish Johri** in their project on ' **An Adaptive Steganography Technique for Gray and Colored Images**' proposed a novel and more robust image steganography technique that embeds message into a cover media, hides its existence and can verify the reliability of the information being transmitted to the receiver. Also it could embed more data than related previous steganography schemes by hiding secret data in cover-image [9].

Dilip Vishwakarma et al in their work on ' **Novel Steganography Technique for Information Hiding**' stated that Increase in tolerance level would allow using all range blocks so that more data can be stored. However low tolerance is desirable in order to give an image that is visually close to the original. The encoding technique can find out the possibility to hide maximum amount of data in an image without degrading its quality [10].**Neha Batra and Pooja Kaushik** in their project on " **Implementation of Modified 16×16 Quantization Table Steganography on Colour Images**" proposed that a novel steganographic method based on the JPEG quantization table modification. Instead of dividing cover image into 8×8 blocks, the cover image is divided into nonoverlapping blocks of 16×16 pixels to embed secret information. It has been found that capacity which is the amount of information embedding in colour images increases as the number of modified quantized DCT coefficients increases. So more data can be embedded using of 16×16 Quantization Tables as compared to 8×8 tables [11].

Shamim Ahmed Laskar and Kattamanchi Hemachandran in their project on ' **High Capacity data hiding using LSB Steganography and Encryption**' proposed a high capacity data embedding approach by the combination of Steganography and cryptography. The combination of these two methods will enhance the security of the data embedded. The main objective in this work was to provide resistance against visual and statistical attacks as well as high capacity [12].**Hemalatha Sharma et al** in their research on ' **A Secure and High Capacity Image Steganography Technique**' provides a novel image steganography technique to hide multiple secret images and keys in color cover image using Integer Wavelet Transform (IWT). However the disadvantage of the approach is that it is susceptible to noise if spatial domain techniques are used to hide the key [13].

R.Poornima and R.J.Iswarya in their work on ' **An Overview of Digital Image Steganography** 'stated that Hiding Capacity plays a vital role for efficient covert communication. In this work, high capacity image steganography schemes are discussed for different file formats. Covert communication is taking place by encrypting the password for information to be protected. The intended receiver will decrypt the information using that password [14].Research scholars **Dipesh Agrawal & Samidha Diwedi** in their project on ' **Analysis of random bit image steganography techniques**'propounded that many steganography techniques can be used like least significant bit (LSB), layout management schemes replacing only 1 & apos;s or only zero & apos;s from lower nibble from the byte for hiding secret message in an image [15].

Elham Ghasemi et al in their work on '**High Capacity Image Steganography Based on Genetic Algorithm and Wavelet Transform**' stated the application of wavelet transform and genetic algorithm (GA) in a novel steganography scheme. A GA based mapping function to embed data in discrete wavelet transform coefficients in $4 * 4$ blocks on the cover image has been employed. The optimal pixel adjustment process (OPAP) is applied after embedding the message. This work introduced a novel steganography technique to increase the capacity and the imperceptibility of the image after embedding [16]. **Rahul Jain and Naresh Kumar** in their research on '**Efficient data hiding scheme using lossless data compression and image steganography**' stated a data hiding scheme using image steganography and compression has been proposed. The improved embedding capacity of the image is possible due to preprocessing the secret message in which a lossless data compression technique is applied. This preprocessing reduces the size of the secret data by a significant amount and thus permits more data into the same image [17]. **Prashant Dahake** in his project on '**An Efficient Encryption Using Data Compression towards Steganography**' stated that compactness is achieved using data compression technique, that is by using arithmetic coding. In proposed system additional security is provided to data by using Encryption technique, which makes use of any cryptographic algorithm and it, is applied on the compressed data [18].

The study of earlier developments has concluded that the existing techniques were capable of hiding small amount of data and were less secure. So the purpose is to find a technique which will hide large amount of data and will also provide more security.

III. CONCLUSION

This paper covers review of steganography and its various techniques of steganography used for data compression rate. It has concluded from the literature review that there were certain limitations in the existing techniques related to data compression rate and data security. So further research in the field is recommended to rectify those limitations.

REFERENCES

- [1] James. C.Judge, "Steganography: Past, Present, Future", GSEC Version 1.2f, SANS Institute 2001.
- [2] M.M. Amin, .M. Salleh, S. Ibrahim, M.R Katmin (2003), "Information Hiding Using Steganography", 4th National Conference on Telecommunication Technology Proceeding 2003 (NCTT2003), Concorde Hotel, Shah Alam, Selangor, 14-15 January 2003, pp. 21-25.
- [3] T Morkel, JHP Eloff and MS Olivier, "An Overview of Image Steganography," in Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa, June/July 2005 (Published electronically).
- [4] Shawn D.Dickman "An Overview of Steganography", James Madison University Infosec Techreport, July 2007, JMU-INFOSEC-TR-2007-002.
- [5] Namita Tiwari, Dr.Madhu Shandilya, "Evaluation of Various LSB based methods of Image Steganography on GIF File Format", International Journal of Computer Applications (0975-8887), Volume 6-No.2, September 2010.
- [6] English, R., "Comparison of high capacity steganography techniques", Soft Computing and Pattern Recognition (SoCPaR), 2010 International Conference of, 7-10 Dec. 2010.
- [7] Yongzhen Zheng, Fenlin Liu ; Xiangyang Luo ; Chunfang Yang , "Identification of Steganography Software based on Core Instructions Template Matching," in Multimedia Information Networking and Security (MINES), 2012 Fourth International Conference on, Shanghai , 4-6 Nov. 2011.
- [8] Saddaf Rubab, Dr. M. Younus, " Improved Image Steganography Technique for Colored Images using Huffman Encoding with Symlet Wavelets" IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 1, March 2012.
- [9] Amit Asthana, Sherish Johri, " An Adaptive Steganography Technique for Gray and Colored Images" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 5, May 2012.
- [10] Dilip Vishwakarma, Satyam Maheshwari, Deepak Chopra, " Novel Steganography Technique for Information Hiding" International Journal of Computing, Communications and Networking, Volume 1, Issue 2, September 2012.
- [11] Neha Batra, Pooja Kaushik, " Implementation of Modified 16×16 Quantization Table Steganography on Colour Images " International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 10, October 2012.
- [12] Shamim Ahmed Laskar and Kattamanchi Hemachandran, " High Capacity data hiding using LSB Steganography and Encryption" International Journal of Database Management Systems (IJDMS) Vol.4, No.6, December 2012.

- [13] Hemalatha S, U Dinesh Acharya, Renuka A and Priya R. Kamath,"A SECURE AND HIGH CAPACITY IMAGE STEGANOGRAPHY TECHNIQUE"Signal & Image Processing: An International Journal (SIPIJ) Vol.4, No.1, February 2013.
- [14] R.Poornima, R.J.Iswarya," An Overview Of Digital Imagesteganography" International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.1,February 2013.
- [15] Dipesh Agrawal & Samidha Diwedi, "Analysis of random bit image steganography techniques" IJCA Proceedings on International Conference on Recent Trends in Engineering & technology 2013 ICRTET, New York, USA, 1-4, May 2013.
- [16] Elham Ghasemi, Jamshid Shanbehzadeh, and Nima Fassihi,"High Capacity Image Steganography Based on Genetic Algorithm and Wavelet Transform"
- [17] Rahul Jain," High Capacity data hiding using LSB Steganography and Encryption" International Journal of Engineering Science and Technology (IJEST)
- [18] Prashant Dahake , "An efficient encryption using data compression towards steganography"