A NOVEL INFORMATION HIDING TECHNIQUE FOR SECURITY BY USING IMAGE STEGANOGRAPHY

[1]M. SITARAM PRASAD [2] S. NAGANJANEYULU [3]CH. GOPI KRISHNA [4] C. NAGARAJU

[1]Professor of School of computing, K.L. University, Vaddeswaram, Guntur-522 502,A.P.,India

[2]Associate Professor of IT, LBR College of Engineering, Mylavaram-521 230, A.P.,India

[3] Student IV/IV B.Tech of IT, LBR College of Engineering, Mylavaram-521 230, A.P.,India

[4] Professor & Head of IT, LBR College of Engineering, Mylavaram -521 230, A.P.,India

E-mail: **email2msr@yahoo.com, svna2198@gmail.com, cnrcse@yahoo.com**

ABSTRACT

In this paper a novel method is proposed to provide more security for the key information with the combination of image compression and data encryption method. This method requires less memory space and fast transmission rate because of image compression technique is applied. Steganography plays an important role in information security. Since the rise of the Internet one of the most important factors of information technology and communication has been the security of information. It is the art of hiding the fact that communication is takes place, by hiding information in other information. Many different file formats can be used, but digital images are the most popular because of their frequency on the Internet. For hiding secret information in images, there exist a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points. Many applications have different requirements of the steganography technique used. Some applications may use absolute invisibility of the secret information, but others require a larger secret message to be hidden. This method has been implemented and tested on varies images and data. It provides better security for encrypted data and no distortion in the image quality.

Keywords: *Steganography, Compression, Digital water marking, Public Key, Encryption, Decryption and Fingerprinting*

1.INTRODUCTION

Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement is called steganography. It is the art and science of

invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. Today steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels. Steganography differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret [1]. Steganography and cryptography are both ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised. Once the presence of hidden information is revealed or even suspected, the purpose of steganography is partly defeated [2]. The strength of steganography can thus be amplified by combining it with cryptography. Two other technologies that are closely related to steganography are watermarking and fingerprinting [3]. These technologies are mainly concerned with the protection of intellectual property, thus the algorithms have different requirements for steganography. These requirements of a good steganographic algorithm will be discussed here. In the watermarking methods all of the instances of an object are "marked" in the same way. The kind of information hidden in objects when using watermarking is usually a signature to signify origin or ownership for the purpose of copyright protection [4]. With fingerprinting on the other hand, different, unique marks are embedded in distinct copies of the carrier object that are supplied to different customers. This enables the intellectual property owner to identify customers who break their licensing agreement by supplying the property to third parties [5]. In watermarking and fingerprinting the fact that information is hidden inside the files may be public knowledge – sometimes it may even be visible – while in steganography the imperceptibility of the information is crucial [6]. A successful attack on a steganographic system consists of an adversary observing that there is information hidden inside a file, while a successful attack on a watermarking or fingerprinting system would not be to detect the mark, but to remove it [5]. Research in steganography has mainly been driven by a lack of strength in cryptographic systems. Many governments have created laws to either limit the strength of a cryptographic system or to prohibit it altogether [2], forcing people to study other methods of secure information transfer. Businesses have also started to realise the potential of steganography in communicating trade secrets or new product information. Avoiding communication through well-known channels greatly reduces the risk of information being leaked in transit [6]. Hiding information in a photograph of the company picnic is less suspicious than communicating an encrypted file.

2. IMAGE STAGENOGRAPHY

To a computer, an image is a collection of numbers that constitute different light intensities in different areas of the image [3]. The numeric value representation forms a grid and the individual points are referred to as pixels. Image is the most popular cover objects used for steganography. In the domain of digital images

many different image file formats exist, most of them for specific applications. For these different image file formats, different steganographic algorithms exist. Image steganography techniques can be divided into two groups: those in the Image Domain and those in the Transform Domain [2]. Image also known as spatial – domain techniques embed messages in the intensity of the pixels directly, while for transform – also known as frequency – domain, images are first transformed and then the message is embedded in the image [9]. Image domain techniques encompass bit-wise methods that apply bit insertion and noise manipulation and are sometimes characterized as "simple systems" [7]. The image formats that are most suitable for image domain steganography are lossless and the techniques are typically dependent on the image format. Steganography in the transform domain involves the manipulation of algorithms and image transforms [10]. These methods are used to hide messages in more significant areas of the image, making it more robust [4]. Many transform domain methods are independent of the image format and the embedded message may survive conversion between lossy and lossless compression [11].

3. IMAGE COMPRESSION

When working with larger images of greater bit depth, the images tend to become too large to transmit over a standard Internet connection. In order to display an image in a reasonable amount of time, techniques must be incorporated to reduce the image's file size. These techniques make use of mathematical formulas to analyse and condense image data, resulting in smaller file sizes. This process is called compression [7]. Compression plays an important role in choosing which steganographic algorithm to use. Lossy compression techniques result in smaller image file sizes, but it increases the possibility that the embedded message may be partly lost due to the fact that excess image data will be removed [1]. Lossless compression though, keeps the original digital image intact without the chance of lost, although is does not compress the image to such a small file size [8]. Different steganographic algorithms have been developed for both of these compression types. In this paper Quantization compression technique is applied.

4. QUANTIZING COMPRESSION

This technique involves reducing the number of gray levels in the Image. Thus reducing the number of bits required to hold an image. Let P be the number of pixels in an original image to be compressed to N gray levels. Create a histogram of the gray levels in the original image. Identify N ranges in this histogram that approximately P/N pixels lie in each range. Identify the median gray level in each range. Clearly, a loss of information has gone on but this has been minimized by ensuring that the groupings are as equal as possible. After this operation key and information is placed in this Resultant Image.

5. PROPOSED ALGORITHM

Step1: Read the information from the file.

Step2: Encrypt the message through the public or private key

Step3: Read the image file

Step4: Compress the image by the Quantizing technique

Step5: Compute the threshold (T), based on average gray value

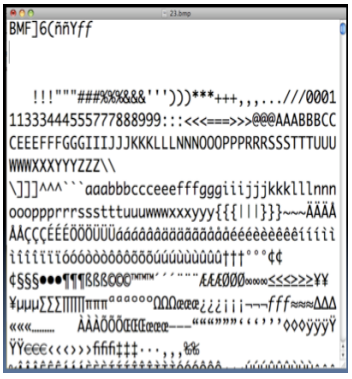
Step6: Place the key information in the Image where value>T

Step7: Send through internet to the destination

Step8: Decompress image and extract key information.

6. EXPERIMENTAL RESULT

Before key information



Key information

After embedding

7. CONCLUSIONS

This method provides better security for information than traditional methods. This method requires less memory space and fast transmission rate because image compression technique is applied. This method should not show any distortion in quality of the Image. This algorithm is easy to implement and does not require much CPU horsepower. Quantizing compression is efficient with files that contain lots of repetitive data. This can be text file if they contain lot of space for indenting but line-art images that contain large white or black areas are far more suitable. Computer generated color images also give good compression.

8. LIST OF REFERENCES

[1] Moerland, T., "Steganography and Steganalysis", *Leiden Institute of Advanced Computing Scienc*e,www.liacs.nl/home/tmoerl/privtech.pdf

[2] Silman, J., "Steganography and Steganalysis: An Overview", *SANS Institut*e, 2001

[3] Jamil, T., "Steganography: The art of hiding information is plain sight", *IEEE Potentials*, 18:01, 1999

[4] Wang, H & Wang, S, "Cyber warfare: Steganography vs. Steganalysis", *Communications of the ACM*,47:10, October 2004

[5] Anderson, R.J. & Petitcolas, F.A.P., "On the limits of steganography", *IEEE Journal of selected Areas in Communications*, May 1998

[6] Marvel, L.M., Boncelet Jr., C.G. & Retter, C., "Spread Spectrum Steganography", *IEEE Transactions on image processing, 8:08*, 1999

[7] Dunbar, B., "Steganographic techniques and their use in an Open-Systems environment", *SANS Institute*, January 2002

[8] Artz, D., "Digital Steganography: Hiding Data within Data", *IEEE Internet Computing Journal*, June 2001

[9] Simmons, G., "The prisoners problem and the subliminal channel", *CRYPTO*, 1983

[10] Chandramouli, R., Kharrazi, M. & Memon, N., "Image steganography and steganalysis: Concepts and Practice", *Proceedings of the 2 nd International Workshop on Digital Watermarking*, October 2003

[11] Currie, D.L. & Irvine, C.E., "Surmounting the effects of lossy compression on Steganography", *19 th National Information Systems Security Conference*, 1996.

Prof. M. Sitaram Prasad received his B.E degree in Computer Science from University of Mysore in 1989, M.Tech degree in Information Technology from Institute of advanced Studies in Education University in 2005, M.E degree in Computer Science from Vinayaka Missions University in 2007. Currently, he is working as a professor in K. L. University in School of Computing. He has got 10 years of teaching experience. He is a member of CSI.

Mr. S. Naganjaneyulu received his MCA degree from Acharya Nagarjuna University, Guntur, in 1999. M.Tech degree in Computer Science from Dr. M.G.R. University, Chennai in 2007 and pursuing his Ph.D in Digital Image Processing from Nagarjuna University, Guntur. Currently, he is working as a Associate Professor of IT in Lakireddy Bali Reddy College of Engineering, Mylavaram, India. He has got 9 years of teaching experience.

Mr. Ch. Gopi Krishna pursuing his B.Tech Degree from Lakireddy balireddy college of engineering. He is the topper in the college

Prof. C. NagaRaju received his B.Tech degree in Computer Science from J.N.T.U, Ananthapur, M.Tech degree in Computer Science from J.N.T.U, Hyderabad and pursuing his Ph.D in digital Image processing from J.N.T. University,Hyderabad. Currently, he is working as a Professor & Head of IT in Lakireddy Bali Reddy College of Engineering, Mylavaram. He has got 14 years of teaching experience. He has published twenty research papers in various national and international journals and about twenty-eight research papers in various national and international conferences. He has attended twenty seminars and workshops. He is a member of various professional societies like IEEE, ISTE and CSI.