A Strong Encryption Method of Sound Steganography by Encoding an Image to Audio

V. J. Rehna, *Member, IACSIT* and M. K. Jeya Kumar

***Abstract*—The recently created technology of steganography entices a wide audience from the casual observer, to the scientific professional. Steganography is defined as the art and science of writing hidden messages in such a way that the hidden message is unnoticed by someone that is not aware of its content. This paper attempts to reveal new and current angles of steganography. When the hidden message is an image which is encoded into an audio file, the process is termed as Sound Steganography. In this work, we have designed a practically secure sound steganographic method, an algorithm which could encode a picture into sound and then read it again in order to obtain image through sound. The algorithm used is simple and optimal, named the color palette substitution. Sound steganography is implemented in two stages, namely image cryptography, where the image is encoded to sound, being the first and reading the sound in a frequency spectrum, being the second. Also the image converted audio is embedded over another music file to form a stronger encryption. MATLAB 7.0.1 with image processing and signal processing toolboxes is used as the development tool for implementing the algorithm.**

***Index Terms*—Cryptography, encryption, steganography, sound steganography.**

I. Introduction

Steganography is the art of hiding the fact that data communication is taking place, by hiding information (image/sound/text) in other information (sound/image). It is in general defined as the art and science of writing hidden messages in such a way that the hidden message is unnoticed by someone that is not aware of its content. The word steganography is of Greek origin and means ―concealed writing‖ from the Greek words *steganos* meaning ―covered or protected‖, and *graphein* meaning ―to write. The first recorded use of the term was in 1499 by Johannes Trithemius in his Steganographia, a treatise on cryptography and steganography disguised as a book on magic. Generally, messages will appear to be something else: images, articles, shopping lists, or some other cover text and, classically, the hidden message may be in invisible ink between the visible lines of a private letter.

In the contemporary world we see there is unsecured usage of internet, that is, any person can misuse the information that is being exchanged. To avoid this, the techniques such as Steganography, Watermarking and Cryptography were designed which are forms of encryption of information [1]. Where the information is either converted from one form to other or just represented in different form and then sent over a network. Easy access of highly confidential information of a healthy organization and misuse of normal steganographic process are some of the other major shortfalls in the present scenario. However, our work doesn't fit perfectly in this definition because our objective is to reach the practical result of encoding of image into sound and then read it again in order to obtain image through sound to overcome the shortfalls of the present steganographic operations. This technique is known to be sound steganography. The main aim of sound steganography is to successfully encode image into sound for later visualization of the image by reading sound in a frequency spectrogram. This paper attempts to reveal new and current angles of steganography.

Manuscript received February 12, 2012; revised April 25.2012. This work was carried out as a part of the research work at the Image Processing Lab, Atria Institute of Technology, Anand Nagar, Bangalore, Karnataka, India.

V. J. Rehna is with HKBK College of Engineering, Arabic College Post, and Bangalore, India (e-mail: rehna_vj@ yahoo.co.in).

M. K. Jeyakumar, is with the Department of Computer Applications, Noorul Islam University, Kumaracoil, Kanyakumari District, Tamil Nadu, India (e-mail: jeyakumarmk@yahoo.com).

II. Encryption Techniques

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. Apart from steganography, the other common encryption techniques are cryptography and watermarking [2]. Steganography is the practice of hiding private or sensitive information within something that appears to be nothing out of the usual. Steganography is often confused with cryptology because the two are similar in the way that they both are used to protect important information. The difference between the two is that Steganography involves hiding information so it appears that no information is hidden at all. If a person or persons views the object that the information is hidden inside of he or she will have no idea that there is any hidden information, therefore the person will not attempt to decrypt the information. Steganography in the modern day sense of the word usually refers to information or a file that has been concealed inside a digital picture, video or audio file. What Steganography essentially does is exploit human perception, human senses are not trained to look for files that have information hidden inside them, although there are programs available that can do what is called steganalysis [3].

The advantage of steganography, over cryptography alone, is that messages do not attract attention to themselves [4], [5]. Plainly visible encrypted messages, no matter how unbreakable will arouse suspicion, and may in themselves be incriminating in countries where encryption is illegal. Therefore, whereas cryptography protects the contents of a

message, steganography can be said to protect both messages and communicating parties [6].

In watermarking [7], an eavesdropper may be able to detect the hidden message in a cover message but he cannot remove or replace it whereas in steganography, the eavesdropper cannot even detect the presence of the hidden information. Therefore, we can say that cryptography and watermarking is about protecting the content of messages, steganography is about concealing its very existence [8]. Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size. As a simple example, a sender might start with an innocuous image file and adjust the color of every 100th pixel to correspond to a letter in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it.

When hiding information inside audio files, the technique usually used is low bit encoding which is almost similar to LSB algorithm that is generally used in Images. The problem with low bit encoding is that it is usually noticeable to the human ear, so it is a rather risky method for someone to use if they are trying to mask information inside of an audio file. Spread Spectrum is another method used to conceal information inside of an audio file [9]. This method works by adding random noises to the signal the information is conceal inside a carrier and spread across the frequency spectrum. Echo data hiding is yet another method of hiding information inside an audio file. This method uses the echoes in sound files in order to try and hide information. By simply adding extra sound to an echo inside an audio file, information can be concealed. The thing that makes this method of concealing information inside of audio files better than other methods is that it can actually improve the sound of the audio inside an audio file [10].

III. Methodology

An important characteristic underlying the design of image processing systems is the significant level of testing and experimentation that normally is required before arriving at an acceptable solution. This characteristic implies that the ability to formulate approaches and quickly prototype candidate solutions generally plays a major role in reducing the cost and time required to arrive at a viable system implementation. As development tool, we used MATLAB 7.0.1 along with its signal processing and image processing toolbox [11]. This powerful tool is a high performance computing language for technical computing, which integrates computation, visualization, and programming in an easy-to-use environment where problems and solutions are expressed in familiar mathematical notation. MATLAB is an interactive system whose basic data element is a matrix. This allows formulating solutions to many technical computing problems, especially those involving matrix representations, in a fraction of the time it would take to write a program in a scalar non-interactive language such as C. We applied the use of MATLAB in every step of the project, from reading the picture to the reading of the audio file with a frequency spectrum from a spectrogram code [12].

The main aim of the work is to design a practically secure sound steganography methodology. The implementation of Sound Steganography is done in two stages:

- The first stage is image cryptography which is encoding of the image into sound.
- The second stage is to read the sound in a frequency spectrum.

These processes work together to accomplish the objective by creating a sound steganography code with good characteristics and achieving interesting results [13].

The encoding makes a mapping translation, for each pixel, vertical positioning into frequency, horizontal position into time-after-click, and brightness into oscillation amplitude. The frequency reading is made by a digital process computed from the signal using the short-time Fourier transform, where the time is divided in parts, and Fourier transformed to calculate magnitude of the frequency spectrum for each part. Each part corresponds then to a vertical line in the image; it is a measurement of magnitude versus frequency for a specific moment in time. The block diagram implementation of sound steganography is shown in Fig. 1.

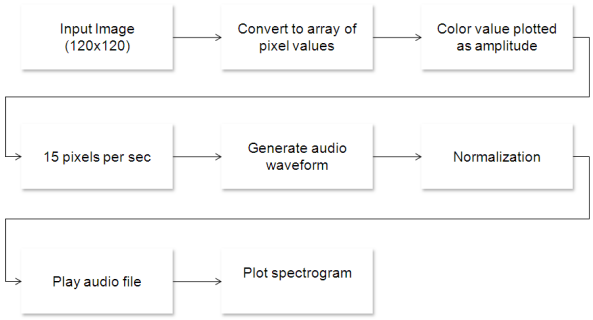

Fig. 1. Block diagram to convert image to sound

An input image of size 120x120 pixels, Fig. 2, having four colors is chosen for converting to an audio file. The pixel values of this image are tabulated as an array which is in turn plotted as the amplitude in the frequency spectrum. An audio wave is generated with 15 color values incorporated in one second of time. The wave is normalized and the audio file can be played. The spectrogram is also plotted by windowing. For the generalized-cosine windows (Blackman, Hamming, and Hann), the sampling parameter determines whether the window samples are computed in a periodic or symmetric manner. Here the spectrogram is plotted using the Hann window which gave the sharpest result.

In the second stage, we have tried embedding the audio wave generated from the image, over a music file to form a stronger encryption [14].

A. Color Palette Substitution

In computer graphics, a palette is either a given, finite set of colours for the management of digital images (that is, a *colour palette*), or a small on-screen graphical element for choosing from a limited set of choices, not necessarily colours (such as a *tools palette*). This is but the total number of colours that a given system is able to generate or manage. The RGB colour model [15] is today the most usual method to produce and encode colours; but colours in palettes may or

may not be reproduced through red-green-blue primaries, depending on a given display hardware. To express that a given palette usage is based in the RGB colour model; the term *RGB palette* is commonly employed. The RGB colour model is usually assumed by default for palettes, if not otherwise noted.

Color depth denotes how many bits are employed to store color information in the image pixels: the more the colors managed, the more the bits employed. The pixel's bit patterns can be interpreted as whole integer numbers (which is the case for indexed color images' indices) or by assigning some bits for color related management, as relative intensities for every primary red-green-blue in RGB true color images. Indexed color palette sizes often have up to 2 raised to some power entries, which easily match pixel's depth bit patterns: $2^2 = 4$, $2^4 = 16$ or $2^8 = 256$ is the most common choices. High color uses RGB full palettes either 15-bits and 16-bits depth, while true color uses RGB full palettes of 24-bits depth or greater. In this work, we make use of this algorithm to implement sound steganography [16].

IV. Results and Discussion

The code produced to make the encoding and reading is able to provide good final results, though some settings adjustments are important to perform the tests. For the application and tests we have chosen a picture with four colors, Fig. 2. The results are optimized if the pictures in study have the 120 x 120 pixels of size. The spectrogram output for Sound Steganography which very well indicates the color pattern with respect to the audio output is shown in Fig. 3.

Fig. 2. Input image which is being converted to sound

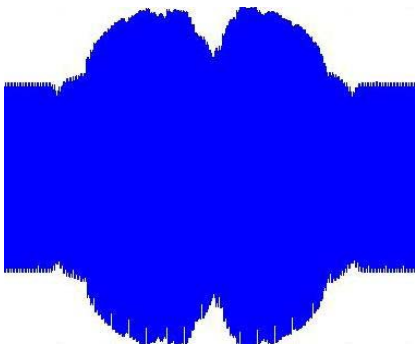

Fig. 3. Spectrogram output.

On the black part of the test image, the code maintained the color but was not able to get the white part of the picture as it was predictable. However, the definitions of the boundaries of the picture shapes are more blurry than on the other test images. This makes the picture not so well defined in shape and color. Once again, we applied different window plot settings and the best result was achieved with the Hann plot window. We tried different settings where we found interesting changes on the results. From the wide variety of tests done, we present one of the settings which gave the best result. Concerning the sound that is produced by the picture encoding it is, as expected, nothing more than noise. However, it is possible to hear the differences between frequencies of the color that are present on the pictures. That noise variation fits perfectly with the picture's shapes.

V. Conclusion and Future Work

Using this technique, we can avoid misuse and hacking of files through internet. We were able to get good and interesting results with our experiments. This process of sound steganography is better when compared to the present steganographic process [17], as we are employing the technique of converting an image to sound. Also the image converted audio is embedded over another audio file for stronger encryption. With the successful implementation of the project, encoding image into sound for later visualization of the image by reading sound in a frequency spectrogram is possible which can be used to avoid illegal access of highly confidential information and to avoid misuse of present steganographic methods [18].

In the future, this work can be enhanced by implementing the decryption process for the sound steganography where the image converted audio is converted back to the original image. It is also possible to construct a code with sophisticated algorithms better suited for embedding audio over a music file and compare the results. All these can help in forming a stronger encryption for the security of important data.

Acknowledgment

The authors thank the reviewers for their valuable comments and suggestions that helped us to make the paper in its present form.

References

[1] W. Peter, "Disappearing cryptography: information hiding: steganography and watermarking," *Amsterdam: MK/Morgan Kaufmann Publishers*, 2002.

[2] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for Data Hiding," 1996.

[3] P. Fabian and A. P. Katzenbeisser, Stefan, "Information Hiding Techniques for Steganography and Digital Watermarking," *Artech House Publishers*, 2000.

[4] N. Johnson, and S. Jajodia, "Steganalysis of Images Created Using Current Steganography Software," Virginia, Fairfax. George Mason University. *Center for Secure Information Systems*.

[5] S. Singh: The code book. The science of secrecy from ancient Egypt to quantum cryptography. *Swiat Ksiazki*, pp. 19-21, 2003.

[6] E. Winfree, and D. K. Gifford, "DNA Based Computers V, Massachusetts Institute of Technology," *DIMACS Series in Discrete Mathematics and Theoretical Computer Science,* American Mathematical Society, vol. 54, 2000.

[7] J. Ingemar Cox, F. Joe Kilian, T. Leighton, and T. Shamoon, "Secure Spread Spectrum," *IEEE Transactions on Image Processing*, vol. 6, no. 12, 2005.

[8] C. Yeh and C. Kuo, "Digital watermarking through quasi m-arrays", *Proc. IEEE Workshop on Signal Processing Systems*, Taipei, Taiwan, p 456–461, "Magnetization reversal in films with biaxial anisotropy," in *Proc. 1987 INTERMAG Conf*, pp. 2.2-1-2.2-6, 1999.
[9] C. R. Gonzalez and R. E. Woods, "Digital Image Processing," *Pearson Edition*, 2005
[10] C. Rafael Gonzales, E. Richard Woods, and L. Steven Eddins, "Digital Image Processing Using Matlab," *Gatemarks Publications*, 2nd edition.
[11] Y. K. Lee and L. H. Chen. "High Capacity Image Steganographic Model." *Vision, Image and Signal Processing*, IEEE Proceedings, pp. 288-294, 2000.
[12] K. David. "The History of Steganography," *Information Hiding: First International Workshop*. Lecture Notes in Computer Science, pp. 1-5, 1996.
[13] J. R. Anderson and A. P. FabienPetitcolas, "On The Limits of Steganography," *Special Issue on Copyright and Privacy Protection. IEEE Journal of Selected Areas in Communications*, pp. 474-481, 1998.
[14] L. Y. Kwen and L. H. Chen, "An Adaptive Image Steganographic Model Based on Minimum-Error LSB Replacement," *Ninth National Conference on Information Security*, pp. 8-15, 1999.
[15] N. F. Johnson and S. Jajodia, "Exploring Steganography: Seeing the Unseen," *Computer*, vol. 31, no. 2, pp. 26–34, 1998.
[16] A. Westfeld and A. Pfitzmann, "Attacks on Steganographic Systems," in *Proc. Information Hiding—3rd Int'l Workshop*, Springer Verlag, pp. 61–76, 1999.
[17] S. Lyu and H. Farid, "Detecting Hidden Messages Using Higher-Order Statistics and Support Vector Machines," in *Proc. 5th Int'l Workshop on Information Hiding*, Springer-Verlag, 2002.
[18] T. Zhang and X. Ping, "A Fast and Effective Steganalytic Technique against JSteg-like Algorithms," in *Proc. 8th ACM Symp. Applied Computing*, ACM Press, 2003.
[19] J. Fridrich, M. Goljan, and D. Hogea, "Steganalysis of JPEG Images: Breaking the F5 Algorithm," in *Proc. 5th Int'l Workshop Information Hiding*, Springer-Verlag, 2002.
[20] S. Axelsson, "The Base-Rate Fallacy and its Implications for the Difficulty of Intrusion Detection," in *Proc. 6th ACM Conf. Computer and Comm. Security*, ACM Press, pp. 1–7, 1999.

Rehna. V. J was born in Trivandrum, Kerala State, India in 1980. She studied Electronics & Communication Engineering at the PET Engineering college, Vallioor, Tirunelveli District, Tamilnadu State, India fom 1999 to 2003. She received Bachelor‟ s degree from Manonmanium Sundarnar University, Tirunelveli in 2003. She did post-graduation in Microwave and TV Engineering at the College of Engineering, Trivandrum and received the Master's degree from Kerala University, Kerala, India in 2005. Presently, she is a research scholar at the Department of Electronics and Communication Enginering, Noorul Islam Center for Higher Education, Noorul Islam University, Kumarakoil, Tamilnadu, India; working in the area of image processing under the supervision of Dr. M. K. Jeya Kumar. She is currently working as Assistant Professor at the Department of Electronics & Communication Engineering, HKBK College of Engineering, Bangalore, India. She has served as faculty in various reputed Engineering colleges in South India over the past nine years. She has presented and published a number of papers in national/international journals/conferences. She is a member of the International Association of Computer Science & Information Technology (IACSIT) since 2009. Her research interests include numerical computation, soft computing, enhancement, coding and their applications in image processing.

M. K. Jeya Kumar was born in Nagercoil, Tamilnadu, India on 18th September 1968. He received his Masters in Computer Applications degree from Bharathidasan University, Trichirappalli, Tamilnadu, India in 1993. He fetched his M.Tech degree in Computer Science and Engineering from Manonmaniam Sundarnar University, Tirunelveli, Tamilnadu, India in 2005. He completed his Ph.D degree in Computer Science and Engineering from Dr.M.G.R University, Chennai, Tamilnadu, India in 2010. He is working as a Professor in the Department of Computer Applications, Noorul Islam University, Kumaracoil, Tamilnadu, India since 1994. He has more than seventeen years of teaching experience in reputed Engineering colleges in India in the field of Computer Science and Applications. He has presented and published a number of papers in various national and international journals. His research interests include Mobile Ad Hoc Networks and network security, image processing and soft computing techniques.