Volume 6, Issue 1, January 2016 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Novel Method of Enhancing Secrete Messages Using Steganography

R. Karthik[*]
Department of Bsc IT,
Bharathiar University, India

Dr. B. L. Shivakumar
Department of Computer Applications,
Sri Ramakrishna Engineering College, India

Abstract: In Telecommunication networks stenography is the process of hiding a message inside another message. The hidden message can only be recognized by Human Visual System (HVS) and is identified only to sender and recipient. The main objective is to convey the message over the public channel. Concurrently two methods are utilized upper level and the lower level. In the earlier days, stegnography has been implemented using some physical medium that is tangible objects. But nowadays it is applied electronically by using various intangible objects. Lower level method steganography bandwidth can be consumed to make the steganogram unreadable, even after the upper level detection. The another benefit of the lower level is that the signal channel is used to exchange the information in the effective way, thus the upper level method function communication is much harder to detect. Data can be hidden utilizing any kind of media like images in bmp, jpeg, gif format or some music file in mp3,rar format or video clip, text file etc. This paper is a challenge to study the process used in steganography, and it is used to identify where this process can be applied, so that the human contest can be exploit at large.

Keywords: Steganography, Security, Secrete message, Hidden message Encryption, Decryption, upper level and lower level

I. INTRODUCTION

The word steganography is obtained from two Greek words; "stegano" meaning protected and "graphia" meaning writing. It can be explained as the process of writing messages in a way in which the presence of secret message is known only to sender and receiver [1]. Steganography plays an essential role in information security. It assigns with embedding information in a given media without making any noticeable changes to it. In simple words, a technology hides a message inside an object. In other words, Steganography is the method of hiding a secret message inside a larger one in such a way that someone cannot know the presence or information of the hidden message. In steganography, only the sender and the receiver know the existence of the message. Although the message is there, but nobody else notices it. However, once noticed, it can be read and manipulated. On the other hand, cryptography is secret writing, anyone can see the message, but none can read it. This is because its type have been re-shuffled, or substituted by different letters, according to the method that only the sender and receiver can identify it. Steganography techniques, on the other hand, it lean to hide the reality of the message itself, which makes it hard for an observer to figure out where the message is [2]. The purpose of Steganography is to maintain secret communication between two parties. Moreover, the change of the carrier caused by inserting steganograms cannot be "visible" to the third party observer. In telecommunication networks, all the information hiding techniques that can be used to replace secret data (steganograms) is called network steganography. Hidden communication network steganography utilizes network protocols and/or relationships between them as a steganogram carrier. It is important to emphasize that for a third party observer who is not alert of the steganographic procedure, the interchange of steganograms remains hidden. This is possible because inserting hidden data into a selected carrier remains unremarkable for users not involved in steganographic communication [2]. Thus, not only the steganograms are hiding inside the carriers (network protocols) but because of the features of the carriers, the fact of the secret data interchange is also hidden.

A combination of steganography and cryptography can provide improved communication security. Let us consider the example of a ring. To hide the ring in a house to save it from theft, one can place it in a safe and then lock it using a key. This is cryptography. However, if the ring is placed behind a common object i.e. book or anything, the thief cannot probably think that the ring is hidden at such obvious place. This is steganography. Placing the ring in locker and then hiding the locker behind the wall is steganography in combination with cryptography.

II. STEGANOGRAPHY FEATURES

- Steganographic bandwidth, which illustrates how much secret data we are able to send using a particular method per time unit.
- Undetectability is defined as an inability to identify a steganogram inside certain carriers. The most preferred method to identify a steganogram is to study statistical properties of the captured data and compare them to the representative properties of that carrier.

- The final is the steganographic cost, which illustrates the degree of degradation of the carrier produced by the steganogram insertion process.

The steganographic cost depends on the kind of carrier, and if it becomes excessive, it leads to easy detection of the steganographic process. For example, if the process uses voice packets as a carrier for steganographic causes in IP telephony, then the cost is indicated in conversation degradation [3]. If the carrier is certain fields of the protocol header, then the cost is indicated as a potential loss in that protocol functionality.

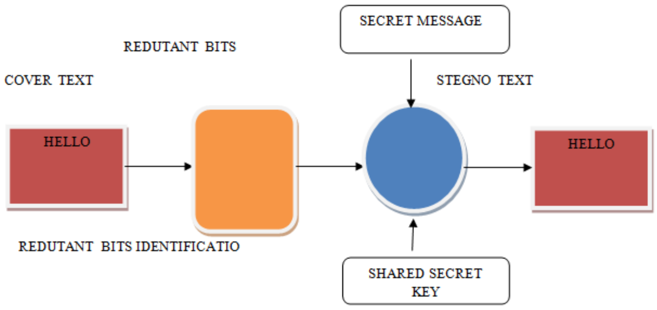

Figure 1: Generic steganography process.

III. STEGANOGRAPHY VS. DIGITAL WATERMARKING

The process of embedding information into digital document in a manner such that the embedded information may be used to verify the identity or authenticity of the owner is known as Digital Watermarking, similar to that of paper bearing watermarks. Relation between Steganography and Digital Watermarking can be described, as the main goal of steganography is to hide a message in cover medium to obtain a new data file, practically indistinguishable from the cover medium in such a way that an eavesdropper does not doubt the presence of message there. Watermarking is to hide a message in cover medium to obtain a new data file, practically indistinguishable from the cover medium in such a way that an eavesdropper can see the message but is not able to remove or replace its contents. Steganography hides messages in one-to-one communications and Watermarking hides messages in one-to many communications. Security is not a concern in steganography i.e. providing protection against removing or modification of the hidden message is not a major issue [4]. Only data embedding is the main issue. On the other hand, watermarking methods are robust, in nature, to attempts to remove or modify the hidden message.

IV. LITERATURE REVIEW

Steganography is hiding the actuality of a message by hiding information into different carriers. The major intent is to prevent the detection of hidden information.. Herodotus, a Greek historian, documented first applications of Steganography. Steganography can be discovered back to ancient Greek centuries when the message is tattooed on the messengers shaved heads. The hair then grownup to secrete the message. Their head will be shaved when they reach the recipient of the message. Another steganography technique that was used through those days is tablet wax. In order to secrete the message, the tablet was erased by wax and text was fixed on and then again covered it by wax and emerged blank upon inspections. During the century, the methods of using hidden inks were exceptionally popular. During the World War II where people used ink for writing hidden messages, this was true. The mixture will turn darker and the written message becomes noticeable upon heating. Later, the Germans introduced the microdot technique where microdots are reviewed as photographs as small as a printed phase, but with a simple format of a typewritten page. They were included in a letter or an wrapper, and because of their small sizes, they could be indiscernible. Microdots were also hidden in body parts including nostrils, ears, or under fingernails. The military and several governmental agencies are looking into steganography for their personal secret transmissions of information. They are also in eager of discerning secret information communicated by criminals, terrorists, and other violent forces. Following investigations into Al-Qaeda attack, steganography was guessed to be made use of in their attack of the World Trade Centre [4].

V. MULTILEVEL STEGANOGRAPHY

Multilevel Steganography is a new idea of information hiding in telecommunication networks that uses the characteristics of an presented steganographic method (the upper-level method) to generate a new one (the lower-level method). In typical single-method network steganography, clear communication traffic is used as a carrier for secret data. By influencing the carrier, a certain steganographic bandwidth, which is defined as the amount of the steganogram transmitted using a particular method in one second is, achieved [5].

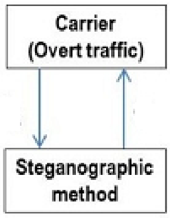

Figure 2: Typical Network Steganography

MLS case presented in Fig 2, upper-level method affects the carrier by introducing a certain cost and under this circumstance. The lower-level method depends on the upper level for its steganographic bandwidth. For this reason, the lower-level method can control the upper-level by starting a cost CSL but also the clear communication by introducing a cost C'SL. The cost C'SL based on the choice of the lower-level method and, in particular, lower-level method can have no control on the carrier i.e. it introduces no cost (C'SL ≈0).

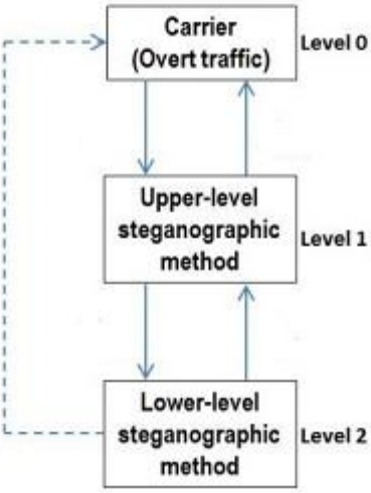
Carrier (Overt traffic)
Level 0
Upper-level steganographic method
Level 1
Lower-level steganographic method
Level 2

Figure 3: The Two-Method MLS

VI. PHYSICAL FORMS OF HIDING

Before the evolution of the computer system, messages were hidden on the tangible or physical objects. Several data hiding methods, used by different countries, have been reported in the literature besides nonliving objects, human factors also contributed in steganography. In 5th century BC, Histaiacus shaved the head of a messenger, and then wrote the secret message on his baldhead and hold back for hair to grow up to send the messenger to the other party [5]. To retrieve message, his hairs were shaved again. Obviously, this method was very time consuming. Hand positions can also be used to form some sequence of the message e.g. during Vietnam war, the captured crew members of the U.S. armed forces used hand positions during photos to be guessed by the media. Several steganographic techniques had been used during World War II. Nazis developed microdots, the microfilm chips created at high magnification and usually of the size of periods, which could carry huge information [5]. In an additional method, a security protocol was developed by ancient China in which the sender and the receiver had same paper mask having a number of holes at random locations. The sender could write down the secret message into the holes by placing his mask over a paper, remove the mask and compose a cover message. The receiver could get the secret message by placing his mask over the letter received.

A. Encoder

The encoder is the main component of the steganographic system. The "secret message" can be defined as the data that is required to remain confidential. The "cover" is the medium in which the message is embedded and which serves to secrete the existence of the message. The "stego-image" (when an image is used as cover) conveys the secret message inserted within it using an algorithm ("Secret Key"). The encoder embeds the secret message beneath cover medium [6]. Encoder is programmed because of some data hiding algorithms. The data is hidden at the redundant places of the cover file example an image, as the changes made in such regions are not easily detectable.

The secret key tells the locations of the regions of the cover image that have been replaced with the secret message. This key is used at extraction stage. The size of the hidden message must be less than or equal to the size of redundant data available for encoding otherwise the encoder would not be able to hide all the data.

B. Decoder

The function of decoder is opposite to that of the encoder. It takes a stego file, makes use of a secret shared key and based on certain algorithms extracts secret data. In case of image steganography, the exact replica of original hidden image cannot be reproduced [7].

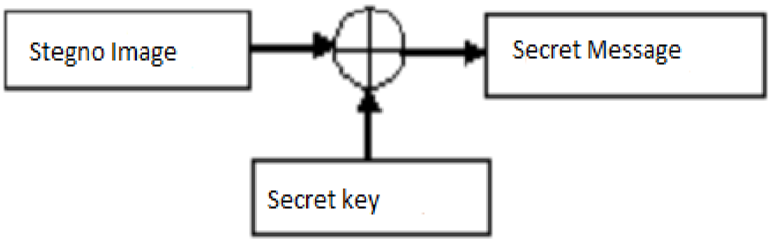

Figure 4: Block diagram of Digital Steganography

VII. STEGANOGRAPHY IN PRESENT

In the modern era, computer system has become backbone of all the great work. The use of computer system has left a good impact on steganography as well. The reason is that many cover media such as images, audio, video, text etc can be used and manipulated digitally to perform steganography. Moreover, a natural cover medium for steganography - the human DNA strand itself – has been unearthed by science.

VIII. TECHNIQUES OF STEGANOGRAPHY

Image Steganography Least significant bit method. These methods hide the most significant bits of secret message in the least significant bits of the carrier (cover) image. This method is also known as LSB method. Example: consider three pixels of 24 bit image with bit values as

01010110 11001010 10101000
00011010 11010101 01010011
10101110 01011110 11011000

These are the pixel values of the cover image. Now suppose we want to hide secret message 01010100 in these bits. Starting from the most significant bit of the secret message, we embed each of these bits in the LSB of the cover medium. This results in the pattern:

01010110 11001011 10101000
00011011 11010100 01010011
10101110 01011110 11011000

Here, the highlighted bits are the changed ones. Though this technique is very simple, it suffers from certain limitations. Embedding secret data requires large cover images and if the secret message is compressed using a lossy algorithm, then at the extraction stage, the extracted message may not be the correct one [8].

A. Filtering and Masking

Here the data is embedded by changing the intensity of pixels of the image. The luminance properties of the image are varied so that human eye is not able to notice any change. This method is more robust than LSB in many ways like compression, cropping and various image processing as it only uses the visual aspects of the cover image. Moreover, as data is hidden in the visible parts of the cover image instead of noisy regions, it is better than LSB in lossy compression algorithms [9].

B. Transformations

Message is hidden behind the cover image by modulating coefficients in transfer domain such as DCT, DFT or wavelet transform.

IX. DATA EMBEDDING TECHNIQUES

F3 key makes use of coefficients having value 1. It decrements the coefficient's absolute values if their LSB does not equal, part from coefficients having value 0, because the perfect value cannot be decremented in this case. That is why zero coefficients are not used steganographically. After embedding, the LSB of non-zero coefficients match the secret message, but bits have not been overwritten, as Chi-square test can easily detect all such changes. Main flaw in F3 technique is that numerous embedded bits become sufferer to shrinkage, which occurs when F3 decrements the absolute values of 1 and −1 resulting in a 0. Distinguishing a zero coefficient, which is logically unused, from a 0 produced by shrinkage becomes impossible for the receiver. Thus all the zero coefficients are skipped. Therefore, the sender embeds the affected bit repeatedly as he notices when he produces a zero. Shrinkage arises only when we embed a zero bit [10]. The repetition of zero bits shifts the originally equalized ratio of steganographic values in favor of the steganographically produced 0's.

F3 algorithm produces a good number of even coefficients as steganographic zeroes. Hence, this process produces more even coefficients than odd.

Embedding procedure:

1. The RGB values of the cover image are obtained.
2. The quantization table is prepared using a quality ratio q, the image is compressed and We obtain quantized DCT coefficients.
3. The embedding capacity, say C, of the cover image is computed using the formula C=hDCT-hDCT/64-h(0)-h(1)+0.49h(1) Where hDCT is the number of all DCT Coefficients' (0) is the number of AC coefficients with value zero. h (1) is the number of AC coefficients with value one [11].
4. For the security purposes, user is required to enter a password based on which random bits of the cover image are chosen to embed secret data. Moreover, based on the Password, a seed is generated that serves as the initial point to generate the pseudo- random bit stream. This bit stream is further XOR-ed with the message bit to make it random.
5. The k bits of the message are embedded into 2 k-1 coefficients randomly. If the hash of the coefficients does not match with the secret bits, then one of the coefficients is decremented by one. After decrement, if the coefficient becomes zero, shrinkage occurs, due to which the same secret bits will be embedded in the next 2 k-1 coefficients.

To embed two bits say p, q in three modifiable bit places m1, m2, m3 changing one place at most, these four cases arise:
p = m1 XOR m3, q = m2 XOR m3 change nothing
p = m1 XOR m3, q = m2 XOR m3 change m1
p = m1 XOR m3, q = m2 XOR m3 change m2
p = m1 XOR m3, q = m2 XOR m3 change m3
Select the coefficients that turn out to be zero after quantization step.

1. Dequantize these coefficients and let these be f (i, j), where (i, j) represents the jth element of ith row of the quantization matrix.
2. QET is used to find the number of bits that can be embedded into the selected coefficient. For this, following formula is used :$N(i,j)= Log2(QET(i,j) +1)$
3. Let m be the secret data to embed and E (i, j) be the quantized DCT matrix after embedding. The secret data is embedded using the formula:

$E (i, j) = f (i, j) + m$ if $QET (i, j) > 0$
Or
$E (i, j) = f (i, j) – m$ if $QET (i, j) < 0$
Where $0<=m<=|QET (i, j)|$
The embedded DCT block is coded using some compression method i.e. run-length encoding of Huffman algorithm[12].The most important step is to change the entries in the quantization table corresponding to the selected DCT coefficients by 1. It is done to avoid significant distortion in the image that will be reconstructed in extraction process.

X. EXTRATCTION PROCEDURE

The quantization matrix is searched to check the coefficients having value equal to 1 because these are the places where secret message is embedded

1. After original jpeg image is compressed, using quantization factors say q1, q2 DCT block is dequantized and the QET is made. Now, we have E (i, j) and f (i, j).
2. Putting these in equation (1) gives the value of m. Such values are collected to form the whole message string. Steganogram Sender & Steganogram Receiver.

XI. BIT PLANE STEGANOGRAPHY

BPCS is commonly known as Bit-Plane Complexity Segmentation Steganography, a few precise parts of a cover image, such as complex or noisy regions, can be used to hide data because our eyes are not sensitive to detect the slight alterations of such parts of an image [13].

1. Segment each bit-plane of the cover image into 8*8 block and distinguish between informative noisy regions on the basis of some threshold value
2. Divide the secret message into set of blocks each containing eight bytes of secret data.
3. Now, the secret file can be simple or complex. If it is simple, noticeable changes can be felt on the cover image. To avoid this, secret file should be converted into the stream of complex blocks and for this purpose, an operation known as conjugation is applied to the simple blocks [14]. Next, prepare a conjugation map that specifies which blocks of the secret file are conjugated and this map is embedded along the secret file as blocks.
4. Then replace the noisy regions of the cover file with the secret data. Record the conjugated blocks in a conjugation map.
5. Just as the secret data, conjugation map is also embedded in the cover image because it will be useful in the extraction process

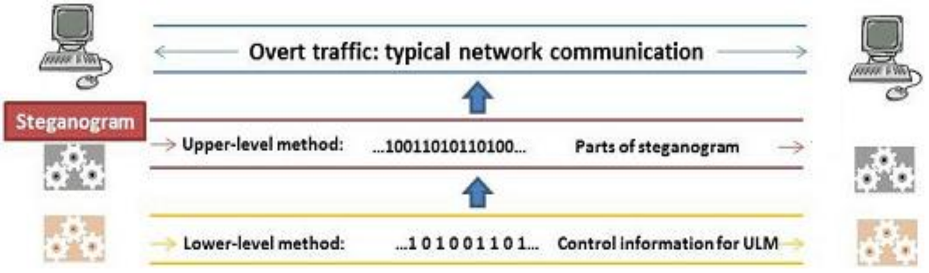

Figure 5: MLS application: lower-level method as a signalling channel to control upper-level method

XII. COVER MEDIUM

Lines shifting is the lines of the text which are vertically shifted to some extent i.e. each line is shifted 1/300 inch up or down and information is hidden in this space by creating a unique shape of the text. This method is useful for printed texts words are shifted horizontally and data is hidden in that space. This method can be identified with difficulty as sometimes, to fill a line; distance between words can be varied in natural way. The distance can be determined using special distance assessment instruments and data can be destroyed by introducing changes. If the text is retyped or some OCR is used, the hidden data gets destroyed [15]. The secret data can be sent by replacing some of its words with their synonyms certain characters such as h, p, d etc. are used to hide data by shortening or elongating their end parts. This method suffers with the problem of OCR programs and retyping the text. This method adds extra white spaces to the text and hides information in these spaces. The hidden data can be destroyed as some text editors automatically delete extra white spaces.

XIII. CONCLUSION

In this paper, a new concept and various aspects of steganography have been covered for performing hidden communication for network multi level steganography was presented information hiding solutions has several potential benefits it may provide increased steganographic bandwidth or increase undetectability. It can also be utilized for ensuring the reliability of steganogram transmission reliability or making steganogram extraction and analysis harder to perform. The methods used for steganography have advanced significantly over the past centuries, especially with the support of advancements in computing power. Steganography is not used very frequently and possibilities are numerous. New techniques to embed messages are being developed rapidly, existing are being modified while ways to detect embedded messages are also advancing. Network steganography environment binding of the overt communication process with steganographic method allows spotting some useful MLS applications that can really improve hidden communications in telecommunication networks that were not considered before. Experimental results were obtained that proved that some of the described above MLS applications can be easily applied. It turned out that the lower-level method's steganographic bandwidth is suitable to provide reliability of the upper-level steganogram (by carrying integrity hash) or to carry a cryptographic key that secret data was encrypted with, thus making it harder to extract and analyze an upper-level steganogram. It can be also utilized to increase the upper-level method undetectability by utilizing the lower level method's steganographic bandwidth to exchange control information between the covert parties that will influence the upper-level one functioning.

XIV. FUTURE WORK

will be focused on developing more efficient MLS schemes because the benefits for such constructions of hidden data exchange are considerable and they solve some open challenges related to network steganography.

REFERNECES

[1] Niels Provos and Peter Honeyman, "Hide and Seek: An Introduction to Steganography", *IEEE Computer Society,* vol. 1, *No.3,* pp. 32-44, 2003.

[2] D.Kahn and The Code breakers, "The Story of Secret Writing", New York, U.S.A.: Scribner, 1996 ISBN0-684-83130-9.

[3] Mary's Ciphers, [Online]. Available:http://www.nationalarchives.gov.uk/spies/ciphers/mary/ma1.html.

[4] "What the Returning POWs Said about Missing Men: The Pink, Blue, and White Pages," [Online]. Available: www.miafacts.org/pages.html.

[5] N. F. Johnson and S. Jajodia, "Exploring Steganography: Seeing the Unseen," Computer Journal, pp. 26- 34, Feb 1998.

[6] M.Owens, "A discussion of covert channels and steganography", SANS Institute, 2010.

[7] A.Westfeld, "F5—A Steganographic Algorithm, High Capacity Despite Better Steganalysis", Lecture Notes in Computer Science, vol. 2137/2001, pp. 289- 302, 2009.

[8] E. Kawaguchi and R. O. Eason, "Principle and applications of BPCS- Steganography," Proc. SPIE: Multimedia Systems and Applications, vol. 3528, pp. 464–472, 1998.

[9] ITU-T Recommendation: G.711 (2006), Pulse code modulation (PCM) of voice frequencies. International Telecommunications Union, Geneva, Switzerland.

[10] Luo, X., Chan, E.W.W, Chang, and R.K.C (2011) Cloak: "A Ten-fold Way for Reliable Covert Communications", In Proc. of 12th European Symposium on Research in Computer Security (ESORICS), Sep 2011.

[11] Petitcolas F, Anderson R, and Kuhn M Information hiding "A survey IEEE", Special Issue on Protection of Multimedia Content, Jul 2009.

[12] Burnett, S., Feamster, N., Vempala, and S., Chipping Away at Censorship Firewalls with User- Generated Content. USENIX Security Symposium 2010: pp. 463-468.

[13] Dhiren R. Patel, "Information Security: Theory and Practice", PHI, ISBN 978- 81-203-3351-2 2008.

[14] Marvin Zelkowitx, ed., "Quantum Cryptography. In Advances in Computers", vol. 56, Academic Press, pp. 189–244, 2002.

[15] Min Wu, Member, IEEE and Bede Liu, Fellow, IEEE, "Data Hiding in Binary Image or Authentication and Annotation", IEEE Trans. Image Processing, vol. 6, Issue 4, Aug. 2009.