Network Based Public Key Method for Steganography

[1] Samir Kumar Bandyopadhyay, [2] Tai -Hoon Kim, [3] Sarthak Parui

[1] Dept. of Computer Science & Engineering, University of Calcutta
92 A.P.C. Road, Kolkata – 700009, India
[2] School of Multimedia, Computer Science and Engineering Division, Hannam University South Korea
[3] Institute of Engineering & Management, Sector V, Salt Lake,
Kolkata-700091, India
skb1@vsnl.com, taihoonn@empal.com, sarthakparui@gmail.com

Abstract

Steganography (a rough Greek translation of the term Steganography is secret writing) has been used in various forms for 2500 years. It has found use in variously in military, diplomatic, personal and intellectual property applications. Briefly stated, 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. The original steganographic applications used "null ciphers", or clear text. A null cipher conveys that the message has not been encrypted in any way, whether it is using basic character shifting, substitution or advanced modern day encryption algorithm. So, the message is often in plain view but for a reason can either not be detected as being present or cannot be seen once detected. As is common with cryptography, steganography has its roots in military and government applications and has advanced in ingenuity and complexity. In this paper, Network Based Public Key Method for Steganography is proposed under RSA cryptographic assumptions.

***Key words**: Data, image, Hiding, Security and Encryption*

1. Introduction

Steganography is the art and science of hiding secret messages in communications over a public channel in a way that conceals the fact that there is a hidden message.

Embedding stego systems are stego systems that do the concealment by embedding a hidden text message into a given cover text to generate a normal-looking stego text. Many practical embedding stego systems have been proposed to embed hidden text in various media such as images, video, audio, and text documents in multiple languages.

Steganography is the science of hiding secret information by means of some carrier file[1]. The secret information in general is embedded into some media file like image or audio and thus it is transmitted so as to prevent an opponent from guessing that some secret information is being transmitted. So, the main objective of Steganography is not to let the opponent guess that any kind of information apart from the media file itself is transmitted. In spatial domain of Steganography by using Image as the carrier file, we, in general, invert the Least Significant Bit of a particular byte of the carrier image to embed a particular bit of Secret message [2, 3, 4]. This method is known as LSB (Least Significant Bit) masking method of Steganography.

Motivated by growing concern about the protection of intellectual property on the Internet and by the threat of a ban for encryption technology, the interest in techniques for information hiding has been increasing over the recent years [6]. The modern formulation of steganography is often given in terms of the *prisoner's problem* [7]. By embedding a secret message into a cover image, a stego-image is obtained. It is important that the stego-image does not contain any easily detectable by a warden. The un-detectability is directly influenced by the size of the secret message and the format and content of the cover image. Obviously, the less information is embedded into the cover image, the smaller the probability of introducing detectable artifacts by the embedding process. Compressed image formats have been popular domain of research for steganographic applications [6, 5]. However, limited success has been achieved for palette-based image formats (GIF/PNG). EZ Stego, one of the most popular data hiding schemes for palette-based images proposed by Machado [8], is similar to the commonly used LSB method for 24 bit colour images (or 8 bit grayscale images). After the palette colours are sorted by luminance, it embeds the message into the LSB of indices pointing to the palette colours. Message recovery is simply achieved by selecting the same pixels and collecting the LSBs of all indices to the ordered palette. Since it is based on the premise that close colours in the luminance-ordered palette palette are close in the colour space. However, occasionally colours with similar luminance values may be relatively far from each other, generating very noticeable artifact. Fridrich [2, 3] presented a steganographic method for hiding message bits into the parity bit of close colours. Although it will never replace a pixel colour by a completely different colour, which could occasionally happen in EZ Stego because ordering of the palette by luminance may introduce discontinuities in neighboring colours. However, the output stego-images generated by Fridrich's method include false contouring and noise, especially when data is embedded in hand-drawn or cartoon pictures.

In this paper, a public key method of Steganography is proposed under RSA cryptographic assumptions. In the proposed algorithm, RSA is used not to encrypt the secret message but to find the exact Byte location of the carrier file, in LSB of which a particular bit of the secret message is to be embedded. For a particular bit of the message file, we employ RSA encryption algorithm to generate a cipher. The LSB of the Red or Green or Blue value of a particular pixel represented by the cipher is then inverted only if the particular bit of the secret message is one. Likewise, we can embed the entire secret message into the carrier file and thereby we can send the embedded file called stego image and the carrier file to intended recipient. Upon receiving, recipient can apply XOR operation on the carrier image and the stego image to find the inverted LSBs. Then applying RSA Decryption algorithm on the location of a particular inverted LSB, we get the original position of the bit in the message file and thus can reconstruct the message file. Thus, this algorithm scatters the information at the time of hiding based on a particular public key-private key combination.

2. Previous Works

The majority of today's steganographic system uses images as cover media because people often transmit digital pictures over email and other Internet communication. Several methods exist to employ the concept of Steganography as well as plenty algorithms have been proposed in this regard. To propose our approach, we have concentrated on some techniques and methods, which are described below.

In the field of image security, Miroslav Dobsicek [9] has developed an interesting application of steganography where the content is encrypted with one key and can be decrypted with several other keys, the relative entropy between encrypt and one specific decrypt key Corresponds to the amount of information.

Yusuk Lim, Changsheng Xu and David Dagan Feng, 2001, described the web based authentication system consists of two parts: one is a watermark embedding system and the other is authentication system. In case of watermark embedding system, it is installed in the server as application software that any authorized user, who has access to server, can generate watermarked image. The distribution can use any kind of network transmission such as FTP, email etc. Once image is distributed to externally, client can access to authentication web page to get verification of image [10].

Min Wu and Bede Liu, June 2003, proposed [11] a new method to embed data in binary images, including scanned text, figures, and signatures. The method manipulates “flappable” pixels to enforce specific block based relationship in order to embed a significant amount of data without causing noticeable artifacts. They have applied Shuffling before embedding to equalize the uneven embedding capacity from region to region. The hidden data can then be extracted without using the original image and can also be accurately extracted after high quality printing and scanning with the help of a few registration marks.

Rehab H. Alwan, Fadhil J. Kadhim, and Ahmad T. Al- Taani, 2005, have explained a method with three main steps. First, the edge of the image is detected using Sobel mask filters. Second, the least significant bit LSB of each pixel is used. Finally, a gray level connectivity is applied using a fuzzy approach and the ASCII code is used for information hiding. The prior bit of the LSB represents the edged image after gray level connectivity, and the remaining six bits represent the original image with very little difference in contrast. The given method embeds three images in one image and includes, as a special case of data embedding, information hiding, identifying and authenticating text embedded within the digital images [12].

In 2007, Nameer N. EL-Emam proposed an algorithmic approach to obtain data security using LSB insertion steganographic method. In this approach, high security layers have been proposed through three layers to make it difficult to break through the encryption of the input data and confuse steganalysis too [13].

Prof S. K. Bandyopadhyay, Debnath Bhattacharyya, Swarnendu Mukherjee, Debashis Ganguly, Poulami Das in 2008 has proposed a heuristic approach to hide huge amount of data using LSB steganography technique. In their method, they have first encoded the data and afterwards the encoded data is hidden behind a cover image by modifying the least significant bits of each pixel of the cover image. The resultant stego-image was distortion less. Also, they have given much emphasis on space complexity of the data hiding technique [14].

There is also a good method proposed by G. Sahoo and R. K. Tiwari in 2008. Their proposed method works on more than one image using the concept of file hybridization. This particular method implements the cryptographic technique to embed two information files using steganography and due to this reason they have used a stego key for the embedding process [15]. Unfortunately, modifying the cover image changes its statistical properties, so eavesdroppers can detect the distortions in the resulting stego-image’s statistical properties. In fact, the embedding of high-entropy data (often due to encryption) changes the histogram of colour frequencies in a predictable way. So, in order to obtain more security in our prescribed method, we have embedded an entire image behind another image of twice the size of target image for a remarkable change in the final image.

3. Proposed Method

In general, secret information is like signatures, secret text, secret images, formulae etc in any convenient format. The cover file or the carrier file can be any kind of multimedia file. Here, we refer INFO_FILE as the secret message file and the cover object as COVER_IMG.

Here, as a cover object 24-bit Bitmap Image is used. The size of COVER_IMG should be at least 8 times of that of the INFO_FILE.

As for RSA assumption, we determine 3 sufficiently large numbers e, d & n to have {e, n} as the public key and {d, n} as the private key. For any file, it is trivial to get the bit re presentation. For INFO_FILE, we obtain the bit representation at first. For the image file, i.e. for COVER_IMG, we obtain the pixel representation as an array of {R, G, B} values. For every bit of INFO_FILE, say, if location of the bit is P, then we obtain C=P^e mod n; then we determine a=C/3 and b=C%3. If Pth bit of INFO_FILE is 1, then at Cth pixel of the COVER_IMG, we invert LSB of b; Now, if b=0, we invert LSB of B value, if b=1, then we invert LSB of G value, otherwise LSB of R value is inverted. From this new value, new pixel is formed. Likewise for every bit of INFO_FILE, we generate new pixel, if necessary, and thereby, we form the STEGO_IMG (the final image where the secret information is embedded). Both the COVER_IMG and the STEGO_IMG is sent to the intended recipient.

At the receiver end, we make logical XOR between the {R, G, B} values of STEGO_IMG & COVER_IMG. As a result of which we get the bits which were inverted. Say, we get G value of ath pixel is inverted. Then we get C=a*3 + 1, and original location of that bit in the INFO_FILE as P, where P=C^d mod n. Likewise, after processing the entire STEGO_IMG, we fill rest of the bits of generated INFO_FILE with zero to obtain the original INFO_FILE.

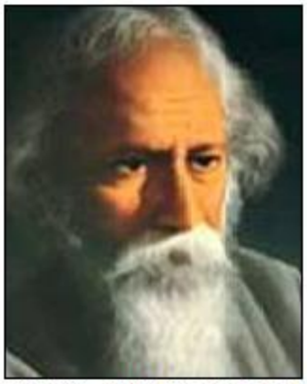
4. Result

INFO_FILE and COVER_IMG are shown in figure 1 and figure 2.

INFO_FILE [8493 bytes]

FIGURE - 1

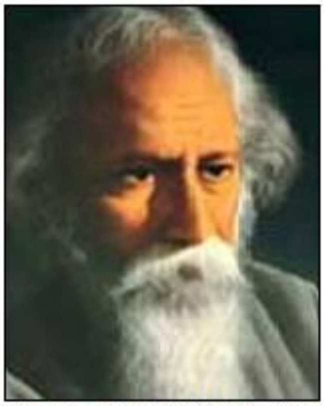
The module calculation in section III.B calculates the size of the INFO_FILE as 8493 bytes and size constraint as 67944 bytes (=8493*8). Maintaining the size constraint, we chose the cover object as COVER_IMG as in Figure 2.



COVER_IMG [91782 bytes]

FIGURE - 2

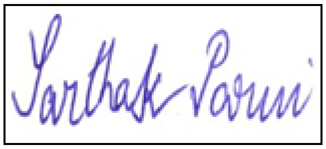
The STEGO_IMG is shown in Figure 3.



STEGO_IMG [91782 bytes]

FIGURE - 3

At the receiver side, both STEGO_IMG and COVER_IMG are passed as argument over the network. At the receiving the extracted INFO_FILE at the receiver side as shown in Figure 4.



Extracted INFO_FILE [8493 bytes]

FIGURE – 4

5. Conclusions

This paper proposes an approach to implement public key algorithm in Steganography. Here, in this paper, Public key algorithm is used based on RSA assumptions with traditional LSB modification scheme for Steganography to randomize the position of the secret bit in cover image. So, it disperses the bits of INFO_FILE throughout the COVER_IMG unsystematically. Thus it makes almost impossible for an attacker to guess the secret information.   In this paper, the basic algorithm is implemented using bitmap image as COVER_IMG and text file or any image file as INFO_FILE, but this algorithm can perfectly work with any kind of image as COVER_IMG.

References

[1] Dobsicek, M., Extended steganographic system. In: 8th Intl. Student Conf. on Electrical Engineering, FEE CTU 2004, Poster 04.

[2] Yusuk Lim, Changsheng Xu and David Dagan Feng, “Web based Image Authentication Using Invisible Fragile Watermark”, 2001, Pan-Sydney Area Workshop on Visual Information Processing (VIP2001), Sydney, Australia, Page(s): 31 - 34

[3] Min Wu, Member, IEEE, and Bede Liu, Fellow, IEEE, “Data Hiding in Binary Image for Authentication and Annotation”, IEEE Trans. Image Processing, volume 6, Issue 4, Aug. 2004 Page(s): 528 - 538

[4] Rehab H. Alwan, Fadhil J. Kadhim, and Ahmad T. Al-Taani, “Data Embedding Based on Better Use of Bits in Image Pixels”, International Journal of Signal Processing Vol 2, No. 2, 2005, Page(s): 104 – 107

[5] N.F. Johnson and S. Jajodia. Exploring steganography: seeing the unseen. In IEEE Comput., pages 26–34, February 1998.

[6] D. Kahn. The history of steganography. In R. Anderson, editor, 1st Information Hiding Workshop, Lecture Notes in Computer Science, volume 1174, pages 1–5. Springer-Verlag, 1996.

[7] Gustavus J. Simmons. The prisoners’ problem and the subliminal channel. In Advances in Cryptology: Proceedings of Crypto 83 (David Chaum, ed.), pages 51– 67. Plenum Press, 1984.

[8] R. Machado. Ez stego. http://www.stego.com.

[9] Dobsicek, M., Extended steganographic system. In: 8th Intl. Student Conf. on Electrical Engineering, FEE CTU 2004, Poster 04.

[10] Yusuk Lim, Changsheng Xu and David Dagan Feng, “Web based Image Authentication Using Invisible Fragile Watermark”, 2001, Pan-Sydney Area Workshop on Visual Information Processing (VIP2001), Sydney, Australia, Page(s): 31 – 34

[11]. Min Wu, Member, IEEE, and Bede Liu, Fellow, IEEE, “Data Hiding in Binary Image for Authentication and Annotation”, IEEE Trans. Image Processing, volume 6, Issue 4, Aug. 2004 Page(s): 528 – 538

[12]. Rehab H. Alwan, Fadhil J. Kadhim, and Ahmad T. Al-Taani, “Data Embedding Based on Better Use of Bits in Image Pixels”, International Journal of Signal Processing Vol 2, No. 2, 2005, Page(s): 104 – 10

[13]. Nameer N. EL-Emam "Hiding a large amount of data with high security using steganography algorithm", Journal of Computer Science. April 2007, Page(s): 223 – 232

[14] S.K.Bandyopadhyay, Debnath Bhattacharyya, Swarnendu Mukherjee, Debashis Ganguly, PoulumiDas, "A Secure Scheme for Image Transformation", August 2008, IEEE SNPD, Page(s): 490 – 493

[15] G. Sahoo, R. K. Tiwari, "Designing an Embedded Algorithm for Data Hiding using Steganographic