ISSN No. 0976-5697

Volume 5, No. 6, July-August 2014

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Study of Various Techniques of Steganography and Steganalysis

Dr Govind N Sarage
Asst Professor, Dept of Computer Sc
National Defence Academy, Khadakwasla Pune

Abstract: Steganography and steganalysis are important tools that allows transmission of information over and over communications channel. The purpose of steganographic communication is to hide the mere existence of a secret message. Steganography refers to the technology of hiding data into digital media without drawing any suspicion, while steganalysis is the art of detecting the presence of steganography. This paper provides a brief study on steganography and steganalysis for digital images, mainly covering the fundamental concepts, the various techniques. Some commonly used techniques for improving steganographic security and enhancing steganalytic capability are summarized and possible research trends are discussed.

Keywords: Steganography, Steganalysis, Data hiding, Security, Cryptography.

I. INTRODUCTION

Information hiding is the science of concealing the *existence* of data even when it is being sought[1]. Steganography is a sub-discipline of the broader science of information hiding and employs numerous technologies to achieve its goals: digital signal processing, cryptography, information theory, data compression, math, and human audio/visual perception, just to name a few. Steganography has two primary goals[2, 4]: 1) Security – is the hidden data perceptible by either a person or a computer, and 2) Capacity – how much data can be hidden in a given cover file. These two goals are often in competition. The more data you hide, the more likely it is to be found, i.e. it has less security and vice versa. A third goal, robustness, is what separates steganography from watermarking[3, 4] (a 2nd sub-discipline of information hiding). Robustness is the resilience of your hidden data to image/audio manipulation such as contrast, brightness, cropping, stretching, analog-to-digital-to-analog conversion, etc.[5] There is a large commercial interest in watermarking for digital rights management. Since there is also a trade-off between robustness and capacity, steganographic programs often do not attempt to be robust, and the techniques presented here are no exception.

There are three levels of failure for steganography: 1) detection, 2) extraction, and 3) destruction [6]. When hidden data is detected, generally, game over. However, if the data cannot be extracted, your objective may still be met. Extraction can be made more difficult by encrypting and/or scrambling the message data. Preventing destruction refers to maintaining the integrity of the hidden data without significant damage to the cover file. Certainly, one could always delete or overwrite the file in question, but preventing an opponent from destroying your data while keeping the value in the digital work is a challenge. For steganography, once the algorithm is known, you can use the same algorithm to insert randomized data into the same bits that carry the message[7, 9]. Message destroyed, image no worse off. Finally, for the purpose of discussion, we can rate the perceptibility in 3 easy levels: 1) Indistinguishable, 2) can see/hear distortion when looking/listening closely for it, 3) blatantly obvious to a casual observer. programs often do not attempt to be robust, and the techniques presented here are no exception

II. STEGANOGRAPHIC SYSTEM

Figure 1 shows the baseline scenario for digital steganography[9]. It depicts two parties, sender and recipient, both steganographers, who communicate covertly over the public channel. The sender executes function Embed : $M \times X^* \times K \rightarrow X^*$ that requires as inputs the secret message $\boldsymbol{m} \in M$, a plausible cover $\boldsymbol{x}(0) \in X^*$, and the secret key $\boldsymbol{k} \in K$.M is the set of all possible messages, X^* is the set of covers transmittable over the public channel and K is the key space. Embed outputs a stego object $\boldsymbol{x}(m) \in X^*$ which is indistinguishable from (but most likely not identical to) the cover. The stego object is transmitted to the recipient who runs Extract : $X^* \times K \rightarrow M$, using the secret key $\boldsymbol{k}$, to retrieve the secret message $\boldsymbol{m}$. Note that the recipient does not need to know the original cover to extract the message. The relevant difference between covert and encrypted communication is that for covert communication it is hard or impossible to infer the *mere existence* of the secret message from the observation of the stego object without knowledge of the secret key. The combination of embedding and extraction function for a particular type of cover, more formally the quintuple (X^*,M,K, Embed, Extract), is called *steganographic system[8]*, in short, *stego system*.

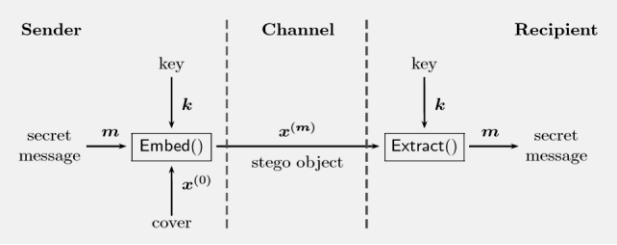

Fig. 1: Block diagram of baseline steganographic system

Steganography refers to the technique of hiding information in digital media in order to conceal the existence of the information[9]. The media with and without hidden information are called stego media and cover media, respectively. Steganography can meet both legal and illegal interests.

Steganalysis[4, 12], from an opponent's perspective, is an art of deterring covert communications while avoiding affecting the innocent ones. Its basic requirement is to determine accurately whether a secret message is hidden in the testing medium. Further requirements may include judging the type of the steganography, estimating the rough length of the message, or even extracting the hidden message. Steganography and steganalysis are in a hide-and-seek game [5, 10]. They try to defeat each other and also develop with each other.

III. STEGANOGRAPHY TECHNIQUES

In this section, we present some of the most common techniques used to embed messages in digital images. We choose digital images as cover objects because they are more related to Computer Vision and Image Processing[11, 22]. However, these techniques can be extended to other types of digital media as cover objects, such as text, video, and audio files. In general, steganographic algorithms rely on the replacement of some noise component of a digital object with a pseudo-random secret message [12]. In digital images, the most common noise component is the least significant bits (LSBs). To the human eye, changes in the value of the LSB are imperceptible, thus making it an ideal place for hiding information without any perceptual change in the cover object. The original LSB information may have statistical properties, so changing some of them could result in the loss of those properties. Thus, we have to embed the message mimicking the characteristics of the cover bits' [13, 18]. One possibility is to use a *selection method* in which we generate a large number of cover messages in the same way, and we choose the one having the secret embedded in it. However, this method is computationally expensive and only allows small embeddings. Another possibility is to use a *constructive method*.

Although LSB embedding methods hide data in such a way that human do not perceive it, these embeddings often can be easily destroyed. As LSB embedding takes place on noise, it is likely to be modified, and destroyed, by further compression, filtering, or a less than perfect format or size conversion. Hence, it is often necessary to employ sophisticated techniques to improve embedding reliability. Another possibility is to use techniques that take place on the most significant parts of the digital object used. These techniques must be very clever in order to not modify the cover object making the alterations imperceptible.

A. LSB Insertion/Modification

Among all message embedding techniques, LSB insertion/modification is a difficult one to detect [1, 14], and it is imperceptible to humans [14]. However, it is easy to destroy. A typical color image has three channels: red, green and blue (R,G,B); each one offers one possible bit per pixel to the hiding process. It is possible to hide information in the LSB fields of any digital image. Suppose that we want to embed the bits **1110** in the selected area then without the loss of generality, we have chosen a gray-scale image, so we have one bit available in each image pixel for the hiding process. If we want to hide four bits, we need to select four pixels. To perform the embedding, we tweak the selected LSBs according to the bits we want to hide.

B. FFTs and DCTs

A very effective way of hiding data in digital images is to use a Direct Cosine Transform (DCT), or a Fast Fourier Transform (FFT), to hide the information in the frequency domain. The DCT algorithm is one of the main components of the JPEG compression technique [12, 15]. In general, DCT and FFT work as follows:

1. Split the image into 8 × 8 blocks.
2. Transform each block via a DCT/FFT. This outputs a multi-dimensional array of 64 coefficients.
3. Use a quantizer to round each of these coefficients. This is essentially the compression stage and it is where data is lost. Small unimportant coefficients are rounded to 0 while larger ones lose some of their precision.
4. At this stage you should have an array of streamlined coefficients, which are further compressed via a Huffman encoding scheme or something similar.
5. To decompress, use the inverse DCT/FFT.

The hiding process using a DCT/FFT is useful because anyone that looks at pixel values of the image would be unaware that anything is different.

C. Coefficient Selection. This technique consists of the selection of the k largest DCT or FFT coefficients $\{\gamma 1 \ldots \gamma k\}$ and modify them according to a function f that also takes into account a measure α of the required strength of the embedding process. Larger values of α are more resistant to error, but they also introduce more distortions.

The selection of the coefficients can be based on visual significance (e.g., given by zigzag ordering [12]). The factors α and k are user-dependent.

The function $f(\gamma_i)$ can be

$f(\gamma_i) = \gamma_i + \alpha b_i$,

where b_i is a bit we want to embed in the coefficient γ_i.

D. Wavelets. DCT/FFT transformations are not so effective at higher-compression levels. In such scenarios, we can use wavelet transformations instead of DCT/FFTs to improve robustness and reliability. Wavelet-based techniques[16] work by taking many wavelets to encode a whole image. They allow images to be compressed by storing the high and low frequency details separately in the image. We can use the low frequencies to compress the data, and use a quantization step to compress even more. Information hiding techniques using wavelets are similar to the ones with DCT/FFT [16, 20].

IV. STEGANALYSIS

The security of a steganographic system is defined by its strength to defeat detection. The effort to detect the presence of steganography is called *steganalysis[9, 16]*.

The steganalyst is assumed to control the transmission channel and watch out for suspicious material. A steganalysis method is considered as successful, and the respective steganographic system as 'broken', if the steganalyst's decision problem can be solved with higher probability than random guessing. Note that we have not yet made any assumptions on the computational complexity of the algorithms behind the functions of the steganographers, Embed and Extract, and the steganalyst's function Detect : $X^* \rightarrow \{$cover, stego$\}$. It is not

uncommon that the steganalyst's problem can theoretically be solved with high probability; however, finding the solution requires vast resources. Without going into formal details, the implicit assumption for the above statements is that for an operable steganographic system, embedding and extraction are computationally easy whereas reliable detection requires considerably more resources.

With the indications that steganography techniques have been used to spread child pornography pictures on the internet [18], there is a need to design and evaluate powerful detection techniques able to avoid or minimize such actions. In this section, we present an overview of current approaches, attacks, and statistical techniques available in Steganalysis. Steganalysis refers to the body of techniques devised to detect hidden contents in digital media. It is an allusion to Cryptanalysis which refers to the body of techniques devised to break codes and cyphers [17, 19].In general, it is enough to detect whether a message is hidden in a digital content.
For instance, law enforcement agencies can track access logs of hidden contents to create a network graph of suspects. Later, using other techniques, such as physical inspection of apprehended material, they can uncover the actual contents and apprehend the guilty parties [18]. There are three types of Steganalysis attacks: (1) aural; (2) structural; and (3) statistical.

1. Aural attacks. They consist of striping away the significant parts of a digital content in order to facilitate a human's visual inspection for anomalies [19]. A common test is to show the LSBs of an image.

2. **Structural attacks**. Sometimes, the format of the digital file changes as hidden information is embedded. Often, these changes lead to an easily detectable pattern in the structure of the file format. For instance, it is not advisable to hide messages in images stored in GIF format. In such a format an image's visual structure exists to some degree in all of an image's bit layers due to the color indexing that represents 224 colors using only 256 values [20].

3. **Statistical attacks**. Digital pictures of natural scenes have distinct statistical behavior. With proper statistical analysis, we can determine whether or not an image has been altered, making forgeries mathematically detectable. In this case, the general purpose of Steganalysis is to collect sufficient statistical evidence about the presence of hidden messages in images, and use them to classify [17, 19] whether or not a given image contains a hidden content. In the following section, we present some available statistical-based techniques for hidden message detection.

A. χ2 Analysis

Westfeld and Pfitzmann [17, 19] have present χ2 analysis to detect hidden messages. They showed that an L-bit color channel can represent 2L possible values. If we split these values into 2L−1 pairs which only differ in the LSBs, we are considering all possible patterns of neighboring bits for the LSBs. Each of these pairs is called a *pair of value* (PoV) in the sequence.
When we use all the available LSB fields to hide a message in an image, the distribution of odd and even values of a PoV will be the same as the 0/1 distribution of the message bits. The idea of the χ2 analysis is to compare the theoretically expected frequency distribution of the PoVs with the real observed ones [18]. However, we do not have the original image and thus the expected frequency. In the original image, the theoretically expected frequency is the arithmetical mean of the two frequencies in a PoV. As we know, the embedding function only affects the LSBs, so it does not affect the PoV's distribution after an embedding. Given that, the arithmetical mean remains the same in each PoV, and we can derive the expected frequency through the arithmetic mean between the two frequencies in each PoV.
Westfeld and Pfitzmann [20] have showed that we can apply the χ2 (chi squared-test) over these PoVs to detect hidden messages. The χ2 test general formula is

$$\chi^2 = \sum_{i=1}^{\nu+1} \frac{(f_i^{obs} - f_i^{exp})^2}{f_i^{exp}},$$

where ν is the number of analyzed PoVs, f_i^{obs} and f_i^{exp} are the observed frequencies and the expected frequencies respectively. The probability of hiding, ph, in a region is given by the compliment of the cumulative distribute=Y6T4EWQn

$$ph = 1 - \int_0^{\chi^2} \frac{t^{(\nu-2)/2} e^{-t/2}}{2^{\nu/2}\Gamma(\nu/2)} dt,$$

where Γ(·) is the Euler-Gamma function. We can calculate this probability in different regions of the image. This approach can only detect sequential messages hidden in the first available pixels' LSBs, as it only considers the descriptors' value. It does not take into account that, for different images, the threshold value for detection may be quite distinct [9, 20]. Simply measuring the descriptors constitutes a low-order statistic measurement. This approach can be defeated by techniques that maintain basic statistical profiles in the hiding process [9, 20].
Improved techniques such as Progressive Randomization (PR) addresses the loworder statistics problem by looking at the descriptors' behavior along selected regions (feature regions).

B. RS Analysis

RS analysis consists of the analysis of the LSB loss-less embedding capacity in color and gray-scale images. The loss-less capacity reflects the fact that the LSB plane – even though it looks random – is related to the other bit planes. Modifications in the LSB plane can lead to statistically detectable artifacts in the other bit planes of the image.
To measure this behavior, Let I be the image to be analyzed with width W and height H pixels. Each pixel has values in P. For an 8 bits per pixel image, we have P = {0 . . . 255}. We divide I into G disjoint groups of n adjacent pixels. For instance, we can choose n = 4 adjacent pixels. We define a discriminant function f responsible to give a real number f(x1, . . . , xn) ∈ R for each group of pixels G = (x1, . . . , xn). Our objective using f is to capture the smoothness of G. Let the discrimination function be

$f(x1, \ldots, xn) = \sum_{i-1}^{n-1} |xi + 1 - xi|$

Furthermore, let F_1 be a flipping invertible function
$F_1 : 0 \leftrightarrow 1, 2 \leftrightarrow 3, \ldots, 254 \leftrightarrow 255$, and
F_{-1} be a shifting function $F_{-1} : -1 \leftrightarrow 0, 1 \leftrightarrow 2, \ldots, 255 \leftrightarrow 256$ over P. For completeness, let F_0 be the identity function such as $F_0(x) = x \; \forall \; x \in P$.
Define a mask M that represents which function to apply to each element of a group G. The mask M is an n-tuple with values in {−1, 0, 1}. The value -1 stands for the application of the function F_{-1}; 1 stands for the function F_1; and 0 stands for the identity function F_0. Similarly, we define –M as M's compliment. We apply the discriminant function f with the functions F{−1,0,1} defined through a mask Mover all G groups to classify them into three categories:

- **Regular**. $G \in RM \Leftrightarrow f(FM(G)) > f(G)$
- **Singular**. $G \in SM \Leftrightarrow f(FM(G)) < f(G)$
- **Unusable**. $G \in UM \Leftrightarrow f(FM(G)) = f(G)$

Similarly, we classify the groups R−M, S−M, and U−M for the mask −M. As a matter of fact, it holds that

$$\frac{RM + SM}{T} \leq 1 \text{ and } \frac{R-M + S-M}{T} \leq 1,$$

where T is the total number of G groups. The method's statistical hypothesis is that, for typical images
RM ≈ R−M and SM ≈ S−M.
What is interesting is that, in an image with a hidden content, the greater the message size, the greater the R−M and S−M difference, and the lower the difference between RM and SM. This behavior points out to high-probability chance of embedding in the analyzed image [21, 22].

V. CONCLUSION

In this paper, we review the fundamental concepts and notions as some typical techniques in steganography and steganalysis for digital images. Several steganographic techniques have been presented in this paper, designed mainly to raise your curiosity and intrigue. They can successfully hide/extract arbitrary data and remain visually undetectable. Modern steganalytic techniques have greatly progressed. However, there are still some unsolved challenges. From the ultimate competition between steganography and steganalysis, a byproduct, namely a natural image model, may be obtained, which is beneficial to both sides. For example, steganographic side can utilize the model to preserve image statistics, while steganalytic side can employ the model to examine if any statistic is deviated. It may also be useful in other related fields, such as digital forensics .

VI. REFERENCES

[1] R. Anderson and F. Petitcolas. On the limits of steganography. *IEEE Journal of Selected Areas in Communications*, 16:474–481, may 1998.

[2] Sara V. Hart, John Ashcroft, and Deborah J. Daniels. Forensic examination of digital evidence: a guide for law enforcement. Technical Report NCJ 199408, U.S. Department of Justice – Office of Justice Programs, Apr 2004.

[3] Sheridan Morris. The future of netcrime now (1) – threats and challenges. Technical Report 62/04, Home Office Crime and Policing Group, 2004.

[4] Niels Provos and Peter Honeyman. Hide and seek: an introduction to steganography. IEEE Security & Privacy Magazine, 1:32–44,May 2003.

[5] Andreas Pfitzmann. Information hiding terminology. In *Proceedings of the First Intl.Workshop on Information Hiding*, Cambridge, UK, May 1996. Springer–Verlag.

[6] Bruce Norman. Secret warfare, the battle of Codes and Ciphers. Acropolis Books Inc.,first edition, 1980. ISBN 0-87491-600-3.

[7] Marcus G. Kuhn. The history of steganography. In *Proceedings of the First Intl. Workshop on Information Hiding*, Cambridge, UK, May 1996. Springer–Verlag.

[8] Richard Popa. An analysis of steganography techniques. Master's thesis, The "Polytechnic" University of Timisoara, Timisoara, Romênia, 1998.

[9] Jean Kumagai. Mission impossible? In *IEEE Spectrum*, volume 40, pages 26–31, April 2003. RITA • Volume XV • Número 1 • 2008 107 Steganography and Steganalysis in Digital Multimedia: Hype or Hallelujah?

[10] Raúl Rodríguez-Colín, Feregrino-Uribe Claudia, and Gershom de J. Trinidad-Blas. Data hiding scheme for medical images. In 17th *IEEE Intl. Conference on Electronics,Communications and Computers*, pages 33–38, February 2007.

[11] Y. Li, C. T. Li, and C. H. Wei. Protection of mammograms using blind staganography and watermarking. In 3rd Intl. Symposium on Information Assurance and Security, August 2007.

[12] Peter Wayner. *Disappearing cryptography*. Morgan Kaufmann Publishers, San Francisco, CA, USA, second edition, 2002. ISBN 1-55860-769-2.

[13] The Electronic Frontier Foundation (EFF). The customer is always wrong: A user's guide to DRM in online music. At `http://www.eff.org/IP/DRM/guide/`,2007.

[14] F. C. Mintzer, L. E. Boyle, and A. N. Cases. Toward on-line, worldwide access to vatican library materials. *IBM Journal of Research and Development*, 40:139–162,Mar 1996.

[15] Rebecca T. Mercuri. The many colors of multimedia security. *Communications of the ACM*, 47:25–29, 2004.

[16] Rafael C. Gonzalez and Richard E. Woods. *Digital Image Processing*. Prentice-Hall,Boston, MA, USA, second edition, 2002.

[17] Bruce Schneier. *Applied Cryptography*. JohnWiley & Sons, New York, 1995. ISBN 0- 47111-709-9.

[18] Neil F. Johnson and Sushil Jajodia. Exploring steganography: Seeing the unseen. *IEEE Computer*, 31:26–34, Feb 1998.

[19] Andreas Westfeld and Andreas Pfitzmann. Attacks on steganographic systems. In *Proceedings* of the Third Intl.Workshop on Information Hiding, pages 61–76, London, UK, 1999. Springer Verlag.

[20] Christopher M. Bishop. *Pattern Recognition and Machine Learning*. Springer Verlab, 2006. ISBN 0-38731-073-8.

[21] Niels Provos and Peter Honeyman. Detecting steganographic content on the internet. Technical Report CITI 01-11, University ofMichigan, Ann Arbor,MI, USA, Nov 2001.

[22] Jessica Fridrich, Miroslav Goljan, and Rui Du. Detecting LSB steganography in color and grayscale images. *IEEE Multimedia*, 8:22–28, Jan 2001.