Asian Journal of Information Technology 6 (10): 1023-1029, 2007
ISSN: 1682-3915


# An Image Steganographic Framework with Improved Tamper Proofing

P. Mohan Kumar and D. Roopa
Department of CSE, Jeppiaar Engineering College, Sathyabama University
Old Mamallapuram Road, Chennai, Tamilnadu, 600-119, India

**Abstract:** This study presents a typical image steganography method that utilizes a block-matching procedure to search for the highest similarity block for each block of the important image. The bases and indexes obtained together with some not-well-matched blocks are recorded in the least significant bits of the cover image using a hop scheme. The method exhibits a high data payload, which reduces the storage and transmission-time requirements and also provides a method that prevents an observer from selectively blocking the transmission of the important image. Also, in this method the degree of tamper proofing is very high, so that it is not possible for any intruder to modify the content of the embedded data in the cover image.

**Key words:** Steganography, ciphertext, SNR, digital watermarking, information hiding and cover signal, jamming margin

## INTRODUCTION

Since the rise of the Internet, one of the most important factors of information technology and communication has been the security of information. 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 this, is called steganography.

Steganography is the art and science of invisible communication. This is accomplished through hiding one information in other information, thus hiding the existence of the communicated information. The word steganography is derived from the Greek words *stegos* meaning cover and *grafia* meaning writing (www.liacs.nl/home/tmoerl/privtech.pdf, 2007) defining it as covered writing. In image steganography the information is hidden exclusively in images.

The idea and practice of hiding information has a long history. In Histories the Greek historian Herodotus writes of a nobleman, Histaeus, who needed to communicate with his son-in-law in Greece. He shaved the head of one of his most trusted slaves and tattooed the message onto the slave's scalp. When the slave's hair grew back the slave was dispatched with the hidden message. In the Second World War the Microdot technique was developed by the Germans. Information, especially photographs, was reduced in size until it was the size of a typed period. Extremely difficult to detect, a normal cover message was sent over an insecure channel with one of the periods on the study containing hidden information (Jamil, 1999). 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 (Wang and Wang, 2004 ). 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 (Wang and Wang, 2004). 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 (Anderson and Petitcolas, 1998). These technologies are mainly concerned with the protection of intellectual property, thus the algorithms have different requirements than steganography.These requirements of a good steganographic algorithm will be discussed below. In watermarking all of the instances of an object are marked

**Corresponding Author:** P. Mohan Kumar, Department of CSE, Jeppiaar Engineering College, Old Mamallapuram Road, Chennai, Tamilnadu, 600-119, India

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 (Marvel *et al*., 1999). 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 (Anderson and Petitcolas, 1998).

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 (Wang and Wang, 2004). 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 (Anderson and Petitcolas,1998).

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, forcing people to study other methods of secure information transfer. Businesses have also started to realize 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 ( Artz, 2001). Hiding information in a photograph of the company picnic is less suspicious than communicating an encrypted file.

A steganographic system/tool must provide a method to:

- Embed data invisibly,
- Allow the data to be readily extracted,
- Promote a high information rate or capacity
- Incorporate a certain amount of robustness to removal.

In this study, we presented a method for embedding an original image into a cover image. And also the capacity of the cover image is considerably improved in addition to the advantage of high tamper proofing.

## MATERIALS AND METHODS

**Existing methods of steganography:** Steganography is not a new science. Familiar steganography techniques include invisible inks, the use of carrier pigeons, and the microdot were used from the times of ancient Greece (Johnson and Jojodia, 1998). As more of today's communication occurs electronically, there have been advancements utilizing digital multimedia signals as vehicles for steganographic communication. These signals, which are typically audio, video, or still imagery, are cover signals. Schemes where the original cover signal is needed to reveal the hidden information are known as cover escrow. They can be useful in traitor-tracing schemes such as those described in (Pfitzmann, 1996). In this scenario, copies of the cover signal are disseminated with the assignee's identification embedded within, resulting in a modified cover signal. If illegal copies of the signal are acquired, the source of the copy is established by subtracting the original cover data from the modified signal, thereby exposing the offender's identity.

However, in many applications it is not practical to require the possession of the unaltered cover signal to extract the hidden information. More pragmatic methods, known as blind schemes, allow direct extraction of the embedded data from the modified signal without knowledge of the original cover. Blind strategies are predominant among steganography of the present day. Digital steganography, or information-hiding schemes, can be characterized utilizing the theories of communication (Smith and Comisky, 1996). The parameters of information hiding, such as the number of data bits that can be hidden, the invisibility of the message, and its resistance to removal, can be related to the characteristics of communication systems: capacity, Signal-to-Noise Ratio (SNR), and jamming margin. The notion of capacity in data hiding indicates the maximum number of bits hidden and successfully recovered by the stegosystem. The SNR serves as a measure of invisibility, or detectability. In this context, the message we are trying to conceal, the embedded signal, represents the information bearing signal, and the cover image is viewed as noise. Contrary to typical communication scenarios where a high SNR is desired, a very low SNR corresponds to lower perceptibility, and therefore, greater success is achieved when concealing the embedded signal. The measure of jamming resistance can be used to describe a level of resistance to removal or destruction of the embedded signal, intentional or accidental.

One method of data hiding entails the manipulation of the Least Significant Bit (LSB) plane, from direct replacement of the cover LSB's with message bits to some type of logical or arithmetic combination between the two. Several examples of LSB schemes can be found in Schyndel *et al.* (1994), Wolfgang and Delp (1996). LSB manipulation programs have also been written for a variety of image formats and can be found in Milbrandt

(1997). LSB methods typically achieve both high payload and low perceptibility. However, because the fact that the data are hidden in the least significant bit may be known, LSB methods are vulnerable to extraction by unauthorized parties. There are, of course, many approaches that are cover escrow schemes, where it is necessary to possess the original cover signal in order to retrieve the hidden information. Examples of such schemes can be found in Cox *et al.* (1996) and Podilchuk and Zeng (1997).

A majority of the work in the area has been performed on invisible digital watermarking. This thrust can be attributed to the desire for copyright protection, spurred by the widespread use of imagery on the Internet and the ease in which a perfect reproduction of a digital image is obtained. The objective of digital watermarking is to embed a signature within a digital image to signify origin or ownership for the purpose of copyright protection. Once added, a watermark must be resistant to removal and reliably detected even after typical image transformations such as rotation, translation, cropping, and quantization.

Another method called patchwork (Bender *et al.*, 1996) alters the statistics of the cover image. First, pairs of image regions are selected using a pseudorandom number generator. Once a pair is selected,the pixel intensities within one region are increased by a constant value while the pixels of the second region are correspondingly decreased by the same value. The modification is typically small and not perceptible, but is not restricted to the LSB. A texture mapping method that copies areas of random textures from one area of the image to another is also described. Simple autocorrelation of the signal is used to expose the hidden information.

Smith and Comiskey presented several spread spectrum data-hiding methods in Smith and Comisky (1996).These techniques utilize the message data to modulate a carrier signal, which is then combined with the cover image in sections of non-overlapping blocks. The message is extracted via cross correlation between the stegoimage and the regenerated carrier; hence, cover image escrow is not necessary. A threshold operation is then performed on the resulting cross correlation to determine the binary value of the embedded data bits. Some of the hidden data may be lost if the phase of the modulated carrier is recovered in error.

A data-hiding scheme using the statistical properties of dithered imagery is proposed by Tanaka *et al.* (1990).With this method, the dot patterns of the ordered dither pixels are controlled by the information bits to be concealed. This system accommodates 2 kB of hidden information for a bilevel 256*256 image, yielding a payload of data or information hiding ratio of one information bit to four cover image bits. An information-hiding ratio of 1: 6 is obtained for trilevel images of the same size. The method has high payload but is restricted to dithered images and is not resistant to errors in the stegoimage.

Davern and Scott (1996) presented an approach to image steganography utilizing fractal image compression operations. An information bit is embedded into the stegoimage by transforming one similar block into an approximation for another. The data are decoded using a visual key that specifies.

The position of the range and domain regions containing the message. Unfortunately, the amount of data that can be hidden using the method is small and susceptible to bit errors. Additionally, the search for similar blocks in the encoder, and the decoder comparison process, are both computationally expensive operations. Recent research performed by Swanson *et al.* (1996). utilizes an approach of perceptual masking to exploit characteristics of the Human Visual System (HVS) for data hiding. Perceptual masking refers to any situation where information in certain regions of an image is occluded by perceptually more prominent information in another part of the scene Cox *et al.* (1995). This masking is performed in either the spatial or frequency domain using techniques similar to Cox *et al.* (1996), Smith and Comisky (1996) without cover image escrow.

In this study, we have proposed to develop an image steganography method from the viewpoint of first considering the payload parameter. The proposed method applies a block-matching procedure to search for the highest similarity block from a series of numbered candidate blocks generated from the cover image and embeds the indexing information in imperceptible areas of the cover image. Because of the resulting smaller size of the stego-image, this method makes the important image more secure and tamper proof.

**Proposed Scheme:** A new steganographic scheme is proposed to embed a relatively large important image into a relatively small cover image. In the proposed method, the entire important image is first divided into multiple image blocks, and each block is represented using two base-difference forms: An (odd_base + odd_difference) form and a (even_base + even_difference) form. For each block, we need to search for the odd difference block with the highest similarity from a set of numbered odd candidate blocks and for the even difference block with the highest similarity from a set of numbered even candidate blocks. The best-matching block is defined as the highest similarity odd difference block if the distance between the odd_difference, and its corresponding highest similarity odd difference block is smaller than the

distance between the even_difference and its corresponding highest similarity even difference block, and as the highest similarity even difference block otherwise. Finally, the odd_base (or even_base) and its best-matching index of each important block are recorded in the LSB planes of the cover image using a hop embedding scheme. The proposed method is explained below.

Consider the message to be transferred I of size $h_I$*$w_I$ and a cover image C of size $h_C$*$w_C$. Consider both images I and C are n-bit images. Our aim is to embed the image I in the LSB planes of C. We are going to divide the image I into multiple non overlapping blocks of size m*n. Here , the $r^{th}$ block $B_r = \{b_{11}, b_{12}, \ldots b_{mn}\}$ with block mean $\mu_r$, the odd/even base $OB_r/EB_r$ of $B_r$ is defined to be the corresponding odd/even integer closest to $\mu_r$, respectively. $B_r$ can be represented using a base-difference form

$$B_r = \begin{cases} OBr + ODIFFr \\ EBr + EDIFFr \end{cases} Or$$

Where,

$ODIFFr = (odiffij) = (bij-OBr), \quad 1 \le i \le m, \ 1 \le j \le n,$

$EDIFFr = (ediffij) = (bij-EBr), \quad 1 \le i \le m, \ 1 \le j \le n,$

In the base-difference form, we search for the index $oind_r$ of the highest similarity block of $ODIFF_r$ by comparing it with 2t-1 odd candidate blocks ($OCand_1$, $Ocand_2 \ldots OCand_{2t-1}$). Similarly, the index of the highest similarity block of is evaluated by comparing it with even candidate blocks ($ECand_1$, $ECand_2 \ldots ECand_{2t-1}$).

The distance measure between two blocks is

$$Dist(P,S) = \frac{1}{m \times n} \sum_{1 \le i \le m, 1 \le j \le n} (pij - sij)^2$$

Where pij and sij are pixels in blocks P and S.

The block-matching method described above determines the most-similar block for each original image block, but the error between a original image block and its best-matching block may still be sufficiently large to cause serious degradation to the original image. To reduce the degradation, some not well matched blocks are embedded directly in the cover image. Since the total storage of the LSB planes of C is q× hc ×wc bits and the block bases and indexes occupy $(k+t)*(h_I*w_I)/(m*n)$ bits, the remaining space in the LSB planes that can be used to hold those not-well-matched blocks is

$$q*h_C*w_C-(k+t)*(h_I*w_I)/(m*n)$$

Each block occupies m*n*k bits, and hence, the number of not-well-matched blocks that can be embedded is

$$\delta = \frac{q \times hC \times wC - (k+t) \times \frac{(hI \times wI)}{(m \times n)}}{m \times n \times k}$$

After determining the number of not-well-matched blocks that should be embedded in the cover image, the ä original image blocks with the largest errors between them and their respective best-matching blocks are embedded directly in C with their best-matching indexes set to $2^t-1$.

The following steps are applied to extract the important image from the stego-image.

1. Extract parameters hI, wI, k, q, t, z, m, n, φ and the Huffman table and apply the inverse hop scheme to extract the Huffman codes from the LSBs of the stegoimage.
2. Decode the Huffman codes to obtain the block bases and indexes and not-well-matched blocks.
3. Applying the candidate-block- generating procedure presented in the embedding process to generate $2^t-1$ odd candidate blocks and $2^t-1$ even candidate blocks from the stego-image instead of the cover image. Repeat taking the next sequential index, say, $ind_i$, that is not yet processed and execute the following substeps until the entire important image is extracted:

a. If $ind_i \neq 2^t-1$ and the corresponding base baseindi is odd, add the $ind_i$th odd candidate block to $base_{indi}$ and assign it to a new block of the important image.
b. If $ind_i \neq 2^t-1$ and the corresponding base $base_{indi}$ is even add the $ind_i$th odd candidate block to base $_{indi}$ and assign it to a new block of the important image.
c. If $ind_i = 2^t-1$ take the next not-well-matched block and use it as the reconstructed block for the current position of the important image.

Note that in steps 3a and b, reconstructed pixels greater than 255 and less than 0 are set to 255 and 0, respectively.

## RESULTS AND DISCUSSION

We have conducted two experiments to test whether the objective of the method described in this study is achieved. In the first experiment, we hide

Table 1: PSNR (A) between the stego-image and cover image and (B) between the extracted important image and original important image, in the first experiment (Unit: decibels)

| A/B | Embedded | | | | | |
|---|---|---|---|---|---|---|
| Cover | House | Jet | Lena | Milk | Scene | Tiff |
| House | | 44.31/35.41 | 44.25/37.06 | 44.26/40.59 | 44.15/31.35 | 44.28/37.93 |
| Jet | 44.42/44.42 | | 44.21/39.97 | 44.22/43.25 | 44.19/34.80 | 44.27/40.32 |
| Lena | 44.42/44.55 | 44.24/39.57 | | 44.20/43.21 | 44.18/34.52 | 44.28/40.77 |
| Milk | 44.51/43.16 | 44.30/38.97 | 44.23/39.37 | | 44.42/44.42 | 44.25/37.06 |
| Scene | 44.25/37.06 | 44.24/39.57 | 44.19/34.80 | 44.19/34.80 | | 44.28/40.77 |
| Tiff | 44.46/44.36 | 44.29/38.65 | 44.23/40.12 | 44.22/43.20 | 44.22/33.97 | |
| Mean | 44.47/44.18 | 44.28/38.39 | 44.23/39.28 | 44.22/42.50 | 44.18/33.75 | 44.28/39.88 |

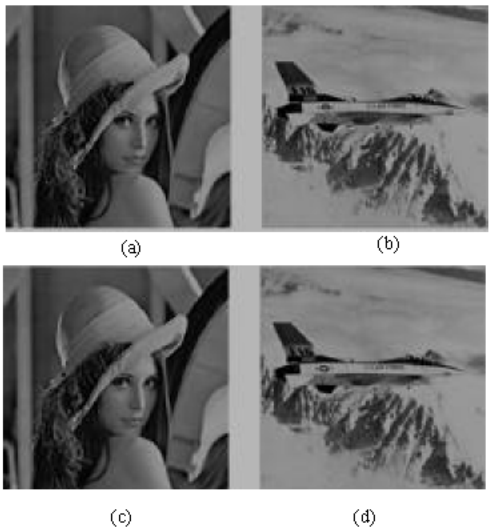


Fig. 1: Example of hiding an original image in a cover image of the same size. a Cover image. b Original image. c Stego-image. d Extracted original image

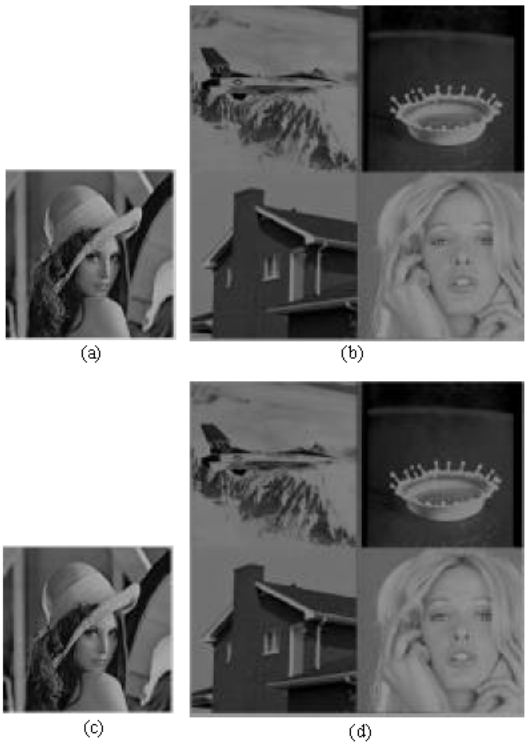


Fig. 3: Example of hiding an important image that is four times larger than the cover image. a Cover image. b Original image. c Stego-image. d Extracted original image

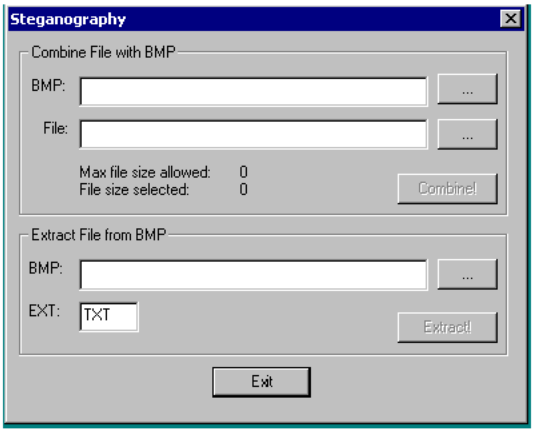


Fig 2. Applying image steganography

an original image in a cover image of the same size using the following parameters: q = 2, t = 16, z = 3, φ = 32 and a block size of 4×4. Figure 1 shows an example of this test using the cover image Lena Fig 1a and the original image Jet Fig 1b, both of which are of size 512×512 pixels. The stego-image and the extracted important image are shown in Fig. 1c and d, respectively. The Peak Signal-to-Noise Ratio (PSNR) between Fig. 1a and c is 44.22 dB, and between Fig 1b and d, it is 39.36 dB. From Fig. 1c, we can see that the quality of the stego-image is high and unintended

observers will not be aware of the existence of the hidden important image. Indeed, it is impossible to distinguish between Fig. 1c and a or between Fig 1d and b using the naked eye, which indicates that the value and normal usage of the important image are preserved. Table 1 summarizes the PSNR values of this experiment. The high values of the PSNR indicate that both the stego-image and the extracted important image are of acceptable quality.

In the second experiment, we attempted to hide an original image that was four times larger than the cover image using the following parameters: $q = 3$, $t = 16$, $z = 3$, $\varphi = 32$ and a block size of 4×8. Figure 2 and 3 shows the results of this experiment where, Fig 3a is the cover image Lena of size 512×512 pixels and Fig 3b is the important image of size 1024×1024 pixels generated by tiling four images together into a single image. The stego-image and the extracted image are shown in Fig 3c and d, respectively. The PSNR between Fig. 3a and c is 37.93 dB and between Fig 3b and d, it is 32.41 dB. In this high-payload embedding test, we can see that both the stego-image and the extracted image are still of high quality and would be considered acceptable in many applications.

## CONCLUSION

This study presents an image steganography method which is capable of storing a large amount of data and also provides tamper-proofing. Careful design of hop embedding scheme can result in both the stego-image and extracted important image being of high quality. The high hiding capacity enables users to send relatively large secret images in an environment where the size of the cover image is relatively small. For example, photographers who work in enemy areas could use this method to hide spy photographs in incurious landscape photographs and transfer these stego-photographs in a more secure and efficient way.

## REFERENCES

Anderson, R.J. and F.A.P. Petitcolas, 1998. On the limits of steganography. IEEE Journal of selected Areas in Communications.

Artz, D., 2001. Digital Steganography: Hiding Data within Data IEEE Internet Computing Journal.

Bender, W., D. Gruhl, N. Morimoto and A. Lu, 1996. Techniques for data hiding. IBM Sys. J., Vol. 35.

Cox, I. J., J. Kilian, T. Leighton and T. Shamoon, 1995. Secure spread spectrum watermarking for multimedia. NEC Res. Inst., Tech. Rep., pp: 128.

Cox, I.J., J. Kilian, T. Leighton, and T. Shamoon, Secure, 1996. Spread spectrum watermarking for images. audio and video. In Proc. IEEE Int. Conf. Image Processing, Lausanne, Switzerland, pp: 243-246.

Davern, P. and M. Scott, 1996. Fractal Based Image Steganography, in Information Hiding. First International Workshop, Lecture Notes in Computer Science, R. Anderson, Ed. Berlin, Germany: Springer-Verlag, pp: 279-294.

Jamil, T., 1999. Steganography: The art of hiding information is plain sight. IEEE Potentials, 18: 01.

Johnson, F. and S. Jajodia, 1998. Exploring steganography: Seeing theunseen, IEEE Comput. Mag., pp: 26-34.

Marvel, L.M., J.R . Boncelet, C.G. and C. Rette, 1999. Spread Spectrum Image Steganography. IEEE Trans. Image Processing, 8: 08.

Milbrandt, E., 1997. http://members/iquest.net/˜mrmil/stego/html.

Podilchuk C. I. and W. Zeng, 1997. Digital image watermarking using visual models, in Human Vision and Electronic Imaging II, B. E. Rogowitz and T. N. Pappas. Eds. SPIE., pp: 100-111.

Pfitzmann, B., 1996. Trials of Traced Traitors, in Information Hiding. First International Workshop, Lecture Notes in Computer Science, R. Anderson. Ed. Berlin, Germany: Springer-Verlag, pp: 49-64.

Smith J. R. and B. O. Comisky, 1996. Modulation and information hiding in images. In Information Hiding. First International Workshop, Lecture Notes in Computer Science, R. Anderson. Ed.. Berlin, Germany: Springer-Verlag, pp: 207-226.

Smith, J.R. and B.O. Comisky, 1996. Modulation and Information hiding in images, in Information Hiding. First International Workshop, Lecture Notes in Computer Science, R. Anderson. Ed. Berlin, Germany: Springer-Verlag, pp: 207-226.

Swanson, M. D., B. Zhu and A. H. Tewfik, 1996. Transparent robust image watermarking. In Proc. Int. Conf. Image Processing, Lausanne, Switzerland, pp: 211-214.

Swanson, M. D., B. Zhu and A.H. Tewfik, 1996. Robust data hiding for images. In Proc. IEEE Digital Signal Processing Workshop, Loen, Norway, pp: 37-40.

Tanaka, K., Y. Nakamura and K. Matsui, 1990. Embedding secret information into a dithered multi-level image. In Proc. IEEE Military Communications Conf.Monterey, CA, pp: 216-220.

van Schyndel, R., A. Tirkel and C. Osborne, 1994. A digital watermark. In Proc. IEEE Int. Conf. Image Processing, pp: 86-90.

Wang, H. and S. Wang, 2004. Cyber warfare: Steganography vs. Steganalysis. Communications of the ACM., 47: 10.

Wolfgang, R.B. and E.J. Delp, 1996.A watermark for digital images. In Proc. IEEE. Int. Conf. Image Processing, Lausanne, Switzerland, pp: 219-222.