ISSN XXXX XXXX © 2017 IJESC

Research Article Volume 7 Issue No.6

An Introduction to Steganography Techniques in the Field of Digital Image Processing

Brij Mohan Kumar[1], Prof. Y. S. Thakur[2]
PG Scholar[1], HOD[2]
Department of Electronics & Communication Engineering
Ujjain Engineering College, Ujjain, India

Abstract:
Steganography is the process of art and science in such a way that no one apart from sender and intended recipient even realizes that the communication is going on. It is also used to authenticate the digital images. Steganography is categorized into spatial domain and frequency domain techniques. This paper presents a cryptography based technique to authenticate the images and can be used to prevent image forgery. While steganography has been around for centuries, the Digital Revolution has sparked a renewed interest in the field. This paper, however, focuses specifically on the techniques employed in hiding information in digital image files.

Keywords: Authentication, security, secret message, steganography, encryption.

I. INTRODUCTION

Steganography is derived from the Greek word which means covered writing and essentially means "to hide in the plain sight". As defined by Cachin [2] steganography is the art and science of communicating in such a way that the presence of a message cannot be detected. Simple steganographic techniques have been in use for hundreds of years, but with the increasing use of files in digital media new techniques for information hiding have become required. This paper examines some early examples of Steganographic process and the general principles behind its usage. Then we will look at why it has become such an important issue in recent years. There will then be a discussion of some specific techniques for hiding information in a variety of formats and the attacks that may be used to bypass steganography. Figure 1 shows how information hiding can be broken down into different areas. Steganography can be used to hide a message intended for later retrieval by a specific individual or group. In this case the aim is to prevent the message being detected by any third party. Other major area of steganography is copyright marking, where the message to be inserted is used to assert copyright over a document.

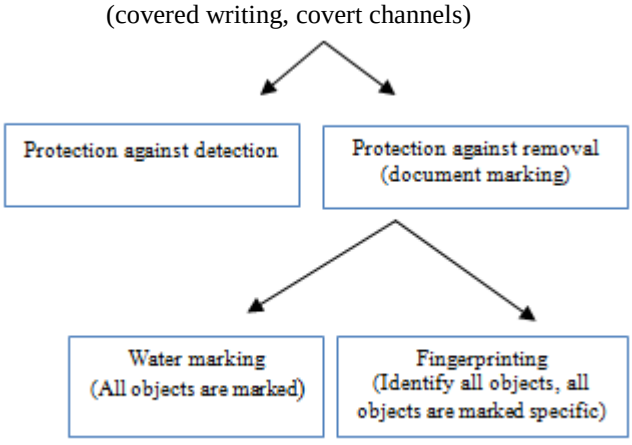


Figure.1. Types of steganography

Steganography and encryption are both used to ensure data confidentiality. However the main difference between them is that with encryption anybody can see that both parties are communicating in secret but not in stegnography. Steganography hides the existence of a secret message and in the best case nobody can see that both parties are communicating in secret. This makes steganography suitable. Adding encrypted copyright information to a file could be easy to remove but embedding it within the contents of the file itself can prevent it being easily identified and removed. Table 1 shows a comparison of different techniques for communicating in secret. Encryption, in which secure communication requiring a key to read the information. An attacker cannot remove the encryption but it is relatively easy to modify the file, making it unreadable for the intended recipient.

Table. 1. Comparison of secret communication techniques.

	Confidentiality	Integrity	Unremovability
Encryption	Yes	No	Yes
Digital Signatures	No	Yes	No
Steganography	Yes / No	Yes/ No	Yes

II. REQUIREMENTS OF HIDING INFORMATION DIGITALLY

There are a large number of different protocols and embedding techniques that made possible us to hide data in a given object. However, all of the protocols and techniques must satisfy all of requirements so that steganography can be successfully applied. Following are list of requirements that steganography techniques must satisfy:

- The integrity of the hidden information after it has been embedded inside the stego object (image, audio, video etc.) must be correct. The secret message must not change in any way, such as additional information being added, loss of information or changes to the secret information after it has

been hidden. If secret information is changed during steganography, it would defeat the whole point of the process.

- The stegonographic object must remain unchanged or almost unchanged to the naked eye. If the stego object changes significantly and can be noticed, it is possible that third party may see that information that is hidden and therefore could attempt to extract or to destroy it.
- In stegnography, changes in the stego object must have no effect on the secret message. Imagine if you had an illegal copy of an image that you would like to manipulate in various ways. These manipulations can be simple process such as resizing, trimming or rotating the image. The secret message inside the image must survive these manipulations, otherwise the attackers can very easily remove the secret message and the point of steganography will be broken.
- Finally, we always assume that the attacker knows that there is hidden information inside the stego object, So we have to always on alert.

III. EMBEDDING AND DETECTING A MARK

Figure 2 shows a simple representation of the generic embedding and then after decoding process in steganography. In this example, a secret image is being embedded inside a cover image to produce the stego image. The first step is to pass both the secret message and the cover message into the encoder. Inside the encoder, several protocols will be implemented to embed the secret information into the cover message. The type of protocol will always depend on what information you are trying to embed and what you are embedding it in. For example, you will use an image protocol to embed information inside images, audio protocol inside audio.

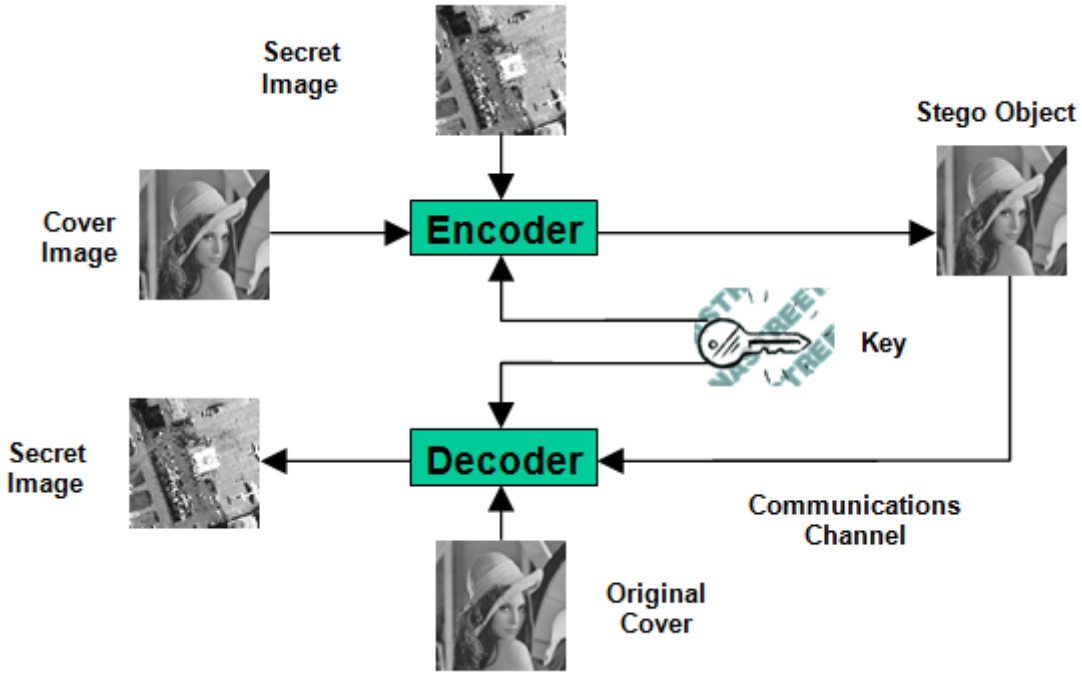


Figure. 2. Generic process of encoding and decoding.

A key is often needed in the embedding process. This can be in the form of a public or private key so you can encode the secret message with your private key and the recipient can decode it using your public key. In embedding the information in this way, you can reduce the chance of a third party attacker getting hold of the stego object and decoding it to find out the secret information successfully. In general the embedding process inserts a mark, M, in an object, I. A key, K, usually produced by a random number generator is used in the embedding process and the resulting marked object, Ĩ, is generated by the mapping: $I \times K \times M \rightarrow \tilde{I}$.

After passing through the encoder, a stego object will be produced. A stego object is the original cover object with the secret information embedded inside. This object should look almost identical to the cover object as otherwise a third party attacker can see embedded information. After producing the stego object, it will then be sent off via some communications channel, such as email, whatsapp etc, to the intended recipient for decoding. The recipient must decode the stego object in order for them to view the secret information. The decoding process is simply the reverse of the encoding process. It is the process of extraction of secret data from a stego object.

In the decoding process, the stego object is fed in to the system. The public or private key that can decode the original key that is used inside the encoding process is also needed so that the secret information can be decoded. Depending on the encoding technique, sometimes the original cover object is also required in the decoding process. Otherwise, there may not be way of extracting the secret information from the stego object. After the decoding process is over, the secret information embedded into the stego object can then be extracted and viewed also. The generic decoding process again requires a key, K, this time along with a potentially marked object, Ĩ'. Also required either the mark, M, which is being checked for or the original object, I, and the result will be either the retrieved mark from the object or indication of the likelihood of M being present in Ĩ'. Various types of robust marking systems use different inputs and outputs process.

- ***Private Marking Systems***

Private marking systems is divided into different types but all require the original image. Type 1 systems use I to help and locate the mark in Ĩ' and output the mark. Type II systems also require M and simply give a yes or no answer to the question

"does Ĩ' contain the mark M?" This can be seen as a mapping: $\tilde{I}' \times I \times K \times M \rightarrow \{0, 1\}$.
Semi-private marking systems work like Type II except they don't require the original image and simply answer the same question through the mapping:
$\tilde{I}' \times K \times M \rightarrow \{0, 1\}$.
Private marking systems shows little information and also required the secret key in order to detect the mark. Many current systems fall into this category and they are often used to prove ownership of material in court.

- ***Public Marking Systems (Blind Marking)***

Public marking systems do not require either I or M but extract n bits from Ĩ' which represents the mark: $\tilde{I}' \times K \rightarrow M$. Public marking systems have a wider range of applications and the algorithms can often be used in the private systems successfully.

- ***Asymmetric Marking Systems (Public Key Marking)***

Asymmetric marking systems allow any user to read the mark but prevent them from removing it.

IV. STEGANOGRAPHY USING IMAGES

Various steps and process of stegnography are explained below using digital images

- ***Simple Watermarking***

A very simple and widely used technique for watermarking images is to add a pattern (digital images) on top of an existing image. Usually this pattern is an image itself - a logo or something similar, which distorts the underlying image.

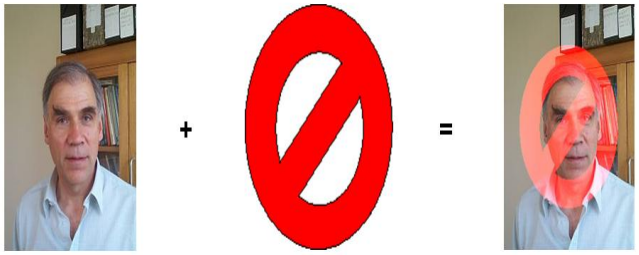


Figure. 3. Visible watermarking.

In the above given example, the red middle image is pattern while the portrait picture of Dr. Axford is the image being watermarked. If the standard image is editing it is possible to merge both images and get a watermarked image. As long as we know the watermark, it is possible to reverse any adverse effects so that the original doesn't need to be kept. This method is only applicable to watermarking, as the pattern is visible and even without the original watermark, it is possible to remove the pattern from the watermarked image with some effort and skill.

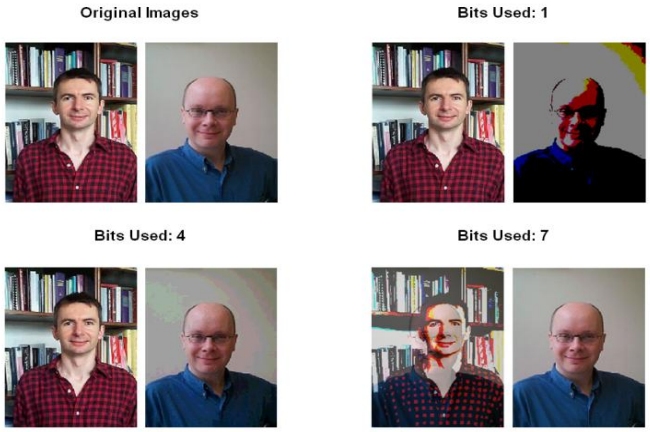
- ***LSB – Least Significant Bit Hiding (Image Hiding)***

This method is probably the easiest way of hiding information in an image and yet it is surprisingly effective. LSB is basic stegnography technique. It works by using the least significant bits of each pixel in one image to hide the most significant bits of another. For example in a JPEG image, the steps would need to be taken as….

a) First take both the host image and the image you need to hide.
b) Next chose the number of bits you wish to hide the secret image in like 8 bit or 16 bit. The more bits used in the host image, the more it deteriorates. As the number of used bits increases obviously has a beneficial reaction on the secret image increasing its clarity.
c) Now we have to create a new image by combining the pixels taken from both images. If you decide for example, to use 4 bits to hide the secret image, there will be four bits left for the host image. (PGM - one byte per pixel, JPEG - one byte each for red, green, blue and one byte for alpha channel in some image types)

Host Pixel: 10110001
Secret Pixel: 00111111
New Image Pixel: **10110011**

d) On the receiver side to get the original image back we just need to know how many bits were used to store the secret image. Then we scan through the host image, pick out the least significant bits according to the number used and then use them to create a new image with one change - the bits extracted now become the most significant bits.
Host Pixel: 10110011, Bits used: 4



New Image: **00110000**

Figure. 4. Least significant bit hiding.

- ***Direct Cosine Transformation***

Most important way of hiding data is by the way of a direct cosine transformation (DCT). The DCT algorithm is one of the main components of the JPEG compression technique as per L. Leurs [13]. This work follows as [14]:

a) First we take the image which is split up into 8 x 8 squares.
b) In next step each of these squares is transformed via a DCT, which outputs a multi dimensional array of 63 coefficients.
c) A quantizer quantizes each of these coefficients, which is the compression stage as this is where some part of data is lost.
d) Small and unimportant coefficients are rounded to 0 while larger ones lose some of their precision.
e) At this stage we should have an array of streamlined coefficients, which are further compressed via a Huffman encoding scheme or similar other scheme.
f) Decompression is done via an inverse DCT process.

Steganography via DCT is most useful as someone who just looks at the pixel values of the image would be unaware that anything is imperfectly. Also the hidden data can be distributed more evenly over the whole image in such a way as to make it more robust process. There is a technique which hides data in the quantizer stage [14]. If we wish to encode the bit value 0 in a specific 8 x 8 square of pixels, this can be done by making sure all the coefficients are even, for example by tweaking them. Bit value 1 can be stored by tweaking the coefficients so that they are odd. In this way a large image can store some data that is quite difficult to detect in comparison

to the LSB method. This is a very simple and useful method and when it works well in keeping down distortions, it is vulnerable to noise.

Original Image Watermarked Image JPEG compressed

Figure .5. Direct Cosine Transformation.

V. CONCLUSION

As steganography is becoming more widely used in digital image processing there are some issues that need to be resolved. A large variety of different techniques with their own advantages and disadvantages are present. Many of them used techniques are not robust enough to prevent detection and removal of embedded data. The used techniques should become more common and a more standard definition of robustness is required to help overcome this. A. P. Petitcolas propose a definition of robust similar to that being used by the music industry [1]. For a system to be considered robust it should have the following properties:

- The used media quality should not noticeably degrade upon addition of a mark.
- Marks should be undetectable without secret knowledge, i.e. the key.
- If multiple marks are present they should not be interference with each other.
- The marks will be such that it survive attacks that don't degrade the perceived quality of the work.

As attacks are made that work against existing techniques, the new techniques will be developed that overcome these deficiencies. The continuous use of digital media there will be drive development of new techniques and standards for stegnography are likely to be developed. Meanwhile techniques which is using by law enforcement authorities to detect embedded material it will improve as they continue to prevent the misuse of steganography.

VI. REFERENCES

[1]. F. A. P. Petitcolas, R. J. Anderson and M. G. Kuhn, "Information Hiding - A Survey", Proceedings of the IEEE, vol. 87, no. 7, pp. 1062-1078, July 1999

[2]. C. Cachin, "An Information-Theoretic Model for Steganography", Proceedings of 2nd Workshop on Information Hiding, MIT Laboratory for Computer Science, May 1998

[3]. R. Popa, An Analysis of Steganographic Techniques, The "Politehnica" University of Timisoara, Faculty of Automatics and Computers, Department of Computer Science and Software Engineering, http:// ad.informatik. uni-freiburg. de/ mitarbeiter/ will/dlib_bookmarks/digital-watermarking/ popa/ popa.pdf, 1998

[4].Herodotus, The Hisories, chap. 5 - The fifth book entitled Terpsichore, 7 - The seventh book entitled Polymnia, J. M. Dent & Sons, Ltd, 1992

[5].Second Lieutenant J. Caldwell, Steganography, United States Air Force, http://www.stsc.hill.af.mil/ crosstalk/2 003/ 06 /caldwell.pdf, June 2003

[6].BBC News, Piracy blamed for CD sales slump, BBC, http://news.bbc.co.uk/1/hi/entertainment/new_media/1841768. stm, February 2002

[7].M. Kwan, The Snow Home Page, http://www. darkside.com. au/snow/index.html, March 2001

[8].Compris Intelligence, TextHide, Compris Intelligence , http://www.compris.com/TextHide/en/

[9].P. Wayner, SpamMimic, http://www.spammimic.com, 2003

[10]. R. Hipschman, The Secret Language, Exploratorium, http://www.exploratorium.edu/ronh/secret/secret.html, 1995

[11]. S. Inoue, K. Makino, I. Murase, O. Takizawa, T. Matsumoto and H. Nakagawa, A Proposal on Information Hiding Methods using XML, http://takizawa.gr. jp/lab/nlp_xml.pdf

[12]. M. D. Swanson, B. Zhu and A. H. Tewfik, "Robust Data Hiding for Images", IEEE Digital Signal Processing Workshop, pp. 37-40,

[13].L.Leurs,JPEGCompression,http://www.prepressure.com/t echno/compressionjpeg.htm,2001

[14]. A. K. Chao and C. Chao, Robust Digital Watermarking & Data Hiding, Image Systems Engineering Program, Stanford University, http://ise.stanford.edu/ class/ee368a_ proj00/ project7/index.html,May2000