Steganography: An Introduction and various techniques in Digital Image Processing

Vikas Sharma, Manish Yadav, Ashish Kulshrestha

Abstract: Steganography is the process of image data hiding in a way that nobody other than sender and known recipient know that communication is on progress. It is also worked in authenticate the digital images. The steganography is classified in spatial domain and frequency domain methods. This research paper presents cryptography based methods to authenticate the images and can be used to protect image fraud. In steganography it has been worked around for decades, the digital revolution has enlightened and renewed area interest in this domain. This paper, focused specifically in the techniques used in protecting information in digital images.

Keywords: Authentication, Least signed bit, encryption, secret message, steganography, security.

I. INTRODUCTION

Steganography word came from the Greek word which means covered hand writing and primarily means "to hide the plain sight". As stated by Mr. Cachin [2] steganography is the science of communicating in a such different manner that the presence of message cannot be detected and found. Basic stego techniques have been in existence for centuries, but the increasing and very vast use of images and files in digital media few new techniques for information protection have become most required. This research paper examines few early methods of Steganographic process general principles behind its usage. Then we will examine, why it has became an important issue in recent time frame. There will be a brief discussion of some specific domain techniques for covering information in many other formats and the attackers which might be used to by pass steganography techniques. Here, figure 1 shows that how information data hiding could break down in different areas. The Steganography may be used to hide a data message intended for post retrieval by an individual or a group of users. In this case the basic primary aim is to protect the message being tracked by third party. So, another major field of steganography is copyright marking, where an input message used to insert copyright over a document.

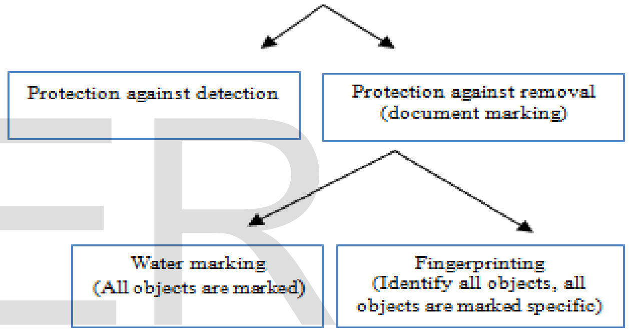

Protection against detection
Protection against removal (document marking)
Water marking (All objects are marked)
Fingerprinting (Identify all objects, all objects are marked specific)

Figure.1. Classification of steganography

Encryption and steganography are the both used to ensure the data security. However the main difference is that encryption user can see both parties are transmitting and receiving in secret manner but not in stegnography. The steganography method covers the presence of a secret message, in best case users can't see both parties are communicating in a defending way. This builds steganography is best suitable between both. And adding the encrypted copyright message and information of an digital image file can be easy to extract but embedding within contents of the digital file so itself could protect being easily identified and also removed. Table 1 puts a detailed comparison of many techniques for setting a communication in secret. The Encryption methods in which secure communication needs a right key to read the encrypted information. A cyber information attacker couldn't fetch encryption but it is comparatively easy to c modify the digital file, making it unreadable and unidentified for particular recipient.

- *Vikas Sharma, Manish Yadav, Ashish Kulshrestha are currently assistant professor in Electronics and Communication Engineering department at JECRC, Jaipur, India. E-mail: Vikassharma.ece@jecrc.ac.in*

Table. 1. Comparison of different communication techniques

	Confidentiality	Integrity	Un-removability
Encryption	Y	N	Y
Digital Signatures	N	Y	N
Steganography	Y/N	Y/N	Y

II. NEEDS FOR HIDING INFORMATION IN A DIGITAL IMAGE

There are huge number of protocols and embedding techniques which made simple ways to us cover the data in a given digital object. So, all of the process and protocols should fulfill all of the requirements so that steganography may be successfully applied. Followings are the compulsory needed that steganography techniques must fulfill:

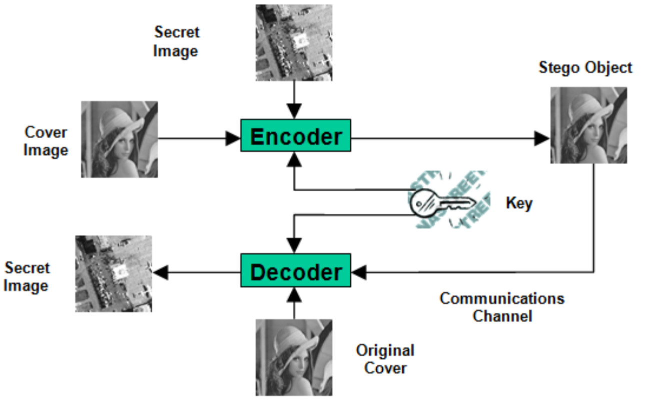
1. The integration parameter of covered information after it has been combined inside the stego object (Audio, visual, image etc.) must be right. The secret data message must not deviate in any kind of way, like as additional data information is being combined loss of data and data or changes to the covered information after has been covered. However, If coded information is altered during steganography process, this would be failure the complete point of the process

2. The stegonographic object must remain unchanged or near about unchanged our naked eyes. If the stego object changes in large and can be traced, it might be possible that someone might see the covered information which is hide therefore it could be attempted to extract or change it.

3. In stegnography method technique, changes in stego object mustn't any affect on the coded secret message. Just imagine if you have a pirated copy of an digital image that you wanted to alter in various ways. 4. So Finally, we always assume the attacker also knows there a hidden information in the stego object, So we always on alert.

III. EMBEDDING AND DETECTING A MARK

Figure 2 shows simple presentation of the basic coding and after decoding process in steganography. In given example, an image with secret message is now being embedded in a cover image to make the stego image. The very first step is, to pass both the secret information and the cover message in to encoder for coding process. In side encoder, many much protocols shall be applied and executed to combined the secret information on the cover stego message.



A key is needed in the embedding and encoding process. In the general embedding image process inserts a mark, M in the object, I a key K, generated by a random generator of number is used in the embedding process and resulting marked object $\tilde{I}$ produced by the mapping: $I * K * M = \tilde{I}$.
After getting through encoder, an image, stego object would produced. A stego image object is the original covered digital object image with the secret information coded and embedded in side it. After making the stego object, it will be sent off by a communication channel, like email, or social handle whatsapp etc, to the desired recipient for decoding.

The recipient now must er-decode the image stego object in order to view them secret information. The decoding process is a simply the basic reverse of encoding process. It is the process of extraction secret data from stego object. In the extraction, the stego object passed in to the system.

IV. STEGANOGRAPHY IN IMAGES

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

(a) ***Simple Watermarking***

A very basic and widely used process of watermarking the images to add a described pattern (digital images) over the top of an pre-existing image. Generally, this pattern is an image it self - a basic logo or something similar, which degrade and distorts the primary image.

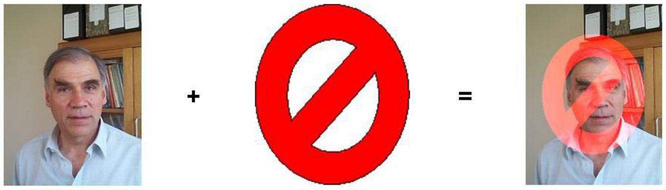


Figure. 3. Example of Visible watermarking.

In the above given example, the red logo in middle image is the pattern and the real picture of person is the image which is going to be watermarked. Generally, If the primary image going to be edited is possible to mix both images and get a new watermarked digital image. As far as we know watermarking, it would be possible to reverse any previously applied effects so the original image does not required to be store. This method is only and only better for watermarking, as the given pattern is clearly visible and without the real watermark, it could be also possible to extract the pattern from watermarked images using different process and skills.

(b) LSB – Least Significant Bit Hiding method

This technique is possibly the easiest kind of protecting information method in a digital image and it is wonderfully most effective. Whereas , LSB is a fundamental stegnography technique. It basically normally works by the least significant bits of each and every pixel available in the digital image to hide the most significant bits (MSB) of another. So just for an example in a JPEG compressed image, the steps are required to be follow as….

a) First arrange both host images and the image needed to hide.

b) After that second step is to choose the number of bits we wish to hide in the digital secret image as, 8 bit or 16 bit. The more bits we use in the host image, more it will be protected. As the number of bits raises, it mostly has a beneficial reaction over the secret image by raising its picture clarity.

c) Now in third step we have to make a new digital image by joining the image pixels received from both the digital images. If we fixed for an example, to hide 4 bits used in the secret digital image, there will be four bits remains left in the host digital image.

(PGM - one byte per pixel method, JPEG – so one single byte used each for red, green and blue (RGB). One byte for alpha channel used in some different image formats)

The host image Pixel: 10111001 (Secret image Pixel): 00110111 converted new Image Pixel: **10111011**

d) In the recipient side receiver to collect the original image back again we require to know how many was the bit length used to hold the secret digital image. Then image is rescan by the host image and brings out the LSB according to number of pixels is used and then again use them to re-create a digital image with one single change - the bits are extracted and now became the MSB.

Host Pixel: 10111011, Bits are used: 4
New Image: **00110000**

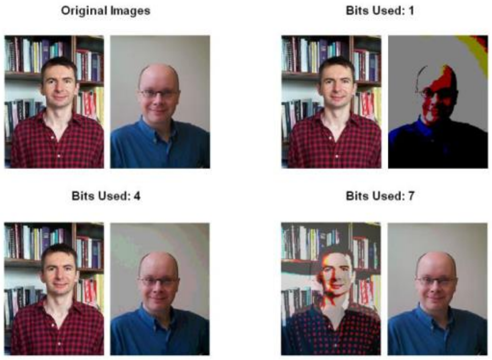


Figure. 4. Least significant bit hiding.

(c) Direct Cosine Transformation Technique

i) Firstly we have the image which is split up around into 8 x 8 squares.
ii) In the next step each squares are transformed via a DCT transformer, which give outputs in a multi dimensional array size of 63 coefficients.
iii) A basic system quantizer, analyses and quantizes each of the received coefficients, which are the normal compression stage as some part of data is degraded, lost or distorted.
iv) Few Small and less important coefficients are manipulated and rounded off to minimum value of 0 while larger values coefficients lose their precision values.
v) At thestage could have value array of stream lined co-efficients, so those are nest compressed via tech. Huffman encoding method or many such schemes.

Original Image New Watermarked Image JPEG compressed

V. CONCLUSION

As steganography technique is widely used in the digital image processing there are many some other critical issues that require and need to be resolved. A large number and variety of different hiding and securing techniques with advantages and the disadvantages are available and suitable. Many of them methods and techniques are not suitable useful and robust enough uo to prevent the detection and removal of embedded secured data. These used methods and techniques should become like useful and more suitable standard definition of degree of robustness is needed to prevent and help overcome this. According to the conclusion and research Mr. A. P. Petitcolas proposed a definition of useful method and similar to that is going to used by the music domain industry [1]. For a good secure system to be utilized considered robust so, it should have the important following qualities:

1. The details of used media quality must not considerable noticeably decrease upon addition of a mark.

2. The marks must be un-discoverable and without secret knowledge, i.e. the secure key.

3. And If there are, multiple marks are available, So, they must not be interfere and interpret with each other.

VI. REFERENCES

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

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

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

[4].Second Lieutenant Caldwell, Steganography, U.S. Air Force, http://www.stsc.hill.af.mil/ crosstalk/2 /caldwell.pdf, June 2003

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

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

[7]. M. D. Swanson, B.A. Zhu and A. H. Tewfik, “Robust Data Hiding for digital Images”, THE IEEE Digital Signal Processing technology Workshop, pp. 37-40,

[8].L..Leurs, JPEG Compression, http://www.prepressure.com/techno/compressionjpeg.htm,2001

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