International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622
Recent Trends in Mobile & Cloud Computing
(NCRMC- 08th & 09th October 2015)

RESEARCH ARTICLE OPEN ACCESS

Digital Steganography

Snehal Kulkarni
Sanmati Engineering College, Washim

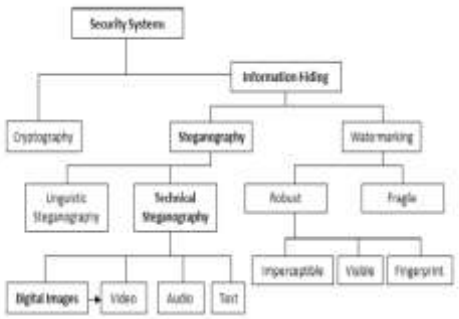
ABSTRACT
Steganography is the science that includes conveying mystery information in a suitable mixed media transporter, e.g., picture, sound, and video documents. It goes under the presumption that if the component is obvious, the purpose of assault is apparent, accordingly the objective here is dependably to hide the very presence of the implanted information. Steganography has different valuable applications. Notwithstanding, like some other science it can be utilized for sick aims. It has been pushed to the bleeding edge of current security methods by the amazing development in computational force, the increment in security mindfulness by, e.g., people, bunches, organizations, government and through scholarly interest. Steganography's definitive destinations, which are imperceptibility, power (imperviousness to different picture preparing systems and pressure) and limit of the shrouded information are the principle figures that separate it from related systems, for example, watermarking and cryptography. This paper gives a best in class audit and investigation of the distinctive existing routines for steganography alongside some regular gauges and rules drawn from the writing. This paper finishes up with a few suggestions and backers for the article arranged implanting instrument. Steganalysis, which is the art of assaulting steganography, is not the center of this overview but rather in any case will be briefly discussed.
Keywords: Stego file, private marking system, steganography, steganalysis, Watermarking

I. INTRODUCTION

The standard and idea of "What You See Is What You Get (WYSIWYG)" which we experience in some cases while printing pictures or different materials, is no more exact and would not trick a steganographer as it doesn't generally remain constant. Pictures can be more than what we see with our Human Visual System (HVS); henceforth, they can pass on more than simply 1000 words.

For a considerable length of time individuals endeavored to create imaginative techniques for mystery correspondence. The rest of this presentation highlights quickly some recorded actualities and assaults on techniques (otherwise called steganalysis). A careful history of steganography can be found in the writing.

Three methods are interlinked, steganography, watermarking and cryptography. The initial two are entirely hard to tease separated particularly for those originating from distinctive controls. Fig. 1 may annihilate such disarray. The work Displayed here spins around steganography in computerized pictures and does not talk about different sorts of steganography, (for example, phonetic or sound).



The word steganography is initially gotten from Greek words which signify "covered Writing" or “Secured Writing”

II. THE DIGITAL ERA OF STEGANOGRAPHY

With the help in PC power, the web and with the improvement of digital signal processing (DSP), data hypothesis and coding hypothesis, steganography has gone "digital". In the domain of this computerized world steganography has made a climate of corporate cautiousness that has generated different intriguing applications, in this manner its proceeding with advancement is ensured.

One of the most punctual routines to examine computerized steganography that proposed a strategy which takes after installing into the 4 LSBs (least significant bits). They inspected picture minimizing also, pollution which is referred to now as picture based steganography.The accompanying is a rundown of principle prerequisites that steganography procedures must fulfill:

a) The trustworthiness of the hidden data after it has been

Implanted inside the stego object must be right.

b) The stego object must stay unaltered or just about unaltered to the exposed eye.
c) In watermarking, changes in the stego object must have no impact on the watermark.
d) Finally, we generally accept that the attacker realizes that there is hidden data inside the stego object.

III. STEGANOGRAPHY ENCRYPTION

The reason for steganography is not to keep others from knowing the concealed data— it is to keep others from imagining that the data indeed, even exists. On the off chance that a steganography technique causes somebody to suspect the bearer medium, then the strategy has fizzled. Steganography's prosperity consequently depends intensely on the guilelessness of individuals; for illustration, when did you last check your email headers for hidden messages?

Encryption and steganography accomplish separate objectives. Encryption encodes information such that a unintended beneficiary can't focus its proposed which means. Steganography, conversely, does not modify information to make it unusable to a unintended beneficiary. Rather, the steganographer endeavors to keep a unintended beneficiary from suspecting that the information is there.

The individuals who look for a definitive in private correspondence can consolidate encryption and steganography.

Scrambled information is more hard to separate from normally happening wonders than plain content is in the bearer medium. A few existing steganography apparatuses can encode information before stowing away it in the chosen medium.

IV. STEGANOGRAPHY METHODS

This section attempts to give an overview of the most important steganographic techniques in digital images. The most popular image formats on the internet are Graphics Interchange Format (GIF), Joint Photographic Experts Group (JPEG), and to a lesser extent - the Portable Network Graphics (PNG).

Most of the techniques developed were set up to exploit the structures of these formats with some exceptions in the literature that use the Bitmap format (BMP) for its simple data structure.

We define the process of embedding as follows (a graphical representation is shown in Fig. 2):

Let C denote the cover carrier, i.e., image A, and Cc the Stego-image.

Let K represent an optional key (a seed used to encrypt the message or to generate a pseudorandom noise which can be set to { } for simplicity) and let M be the message we want to communicate, i.e., image B. Em is an acronym for embedding and Ex for Extraction.

Therefore:

$$Em: C \oplus K \oplus M \to C' \quad (1)$$

$$\therefore Ex(Em(c,k,m)) = m, \forall c \in C, k \in K, m \in M \quad (2)$$

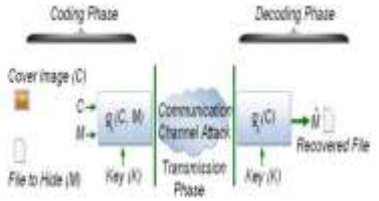


Fig. 2 Communication-theoretical view of a generic embedding process: C denotes cover image, M denotes the data to hide.

V. STEGANALYSIS

This article does not dive into the points of interest of the methods of steganalysis although this work presents, herein, a brief description and some standards that a steganographer should usually examine.

Steganalysis is the science of attacking steganography in a battle that never ends. It mimics the already established science of Cryptanalysis.

Note that steganographers can create a steganalysis system merely to test the strength of their algorithm. Steganalysis is achieved through applying different image processing techniques, e.g., image filtering, rotating, cropping, and translating.

More deliberately, it can be achieved by coding a program that examines the stego image structure and measures its statistical properties, e.g., first order statistics (histograms) or second order statistics (correlations between pixels, distance, direction).

JPEG double compression and the distribution of DCT (Discrete Cosine Transform) coefficients can give hints on the use of DCT-based image steganography. Passive steganalysis attempts to destroy any trace of secret communication, without bother to detect the secrete data, by using the above mentioned image processing techniques: changing the image format, flipping all LSBs or by undertaking a severe lossy compression, e.g., JPEG.

Active steganalysis however, is any specialized algorithm that detects the existence of stego-images. Spatial steganography generates unusual patterns such as sorting of colour palettes, relationships between indexed colours and exaggerated "noise", as can seen in Fig.3, all of which leave traces to be picked up by steganalysis tools.

This method is very fragile. "LSB encoding is extremely sensitive to any kind of filtering or manipulation of the stego-image. Scaling, rotation, cropping, addition of noise, or lossy compression to the stego-image is very likely to destroy the message.

Furthermore an attacker can easily remove the message by removing (zeroing) the entire LSB plane with very little change in the perceptual quality of the modified stego-image". Almost any filtering process will alter the values of many of the LSBs]. By inspecting the inner structure of the LSBs, Fridrich and her colleagues claimed to be able to extract hidden messages as short as 0.03bpp (bit per pixel). LSB methods can result in the "pair effect" in the image histograms. As can be seen in Fig.4, this "pair effect" phenomenon is empirically observed in steganography based on the modulus operator.

Note that it is not always the case that modulus steganography produces such noticeable phenomenon. This operator acts as a means to generate random locations (i.e. not sequential) to embed data.

It can be a complicated process or a simple one like testing, in a raster scan fashion (if a pixel value is even then embed, otherwise do nothing).

Fig.3. Steganalysis using visual inspection: (left-to-right) original image, LSBs of the image before embedding and after embedding, respectively

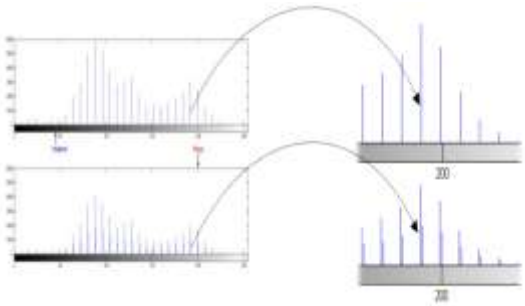


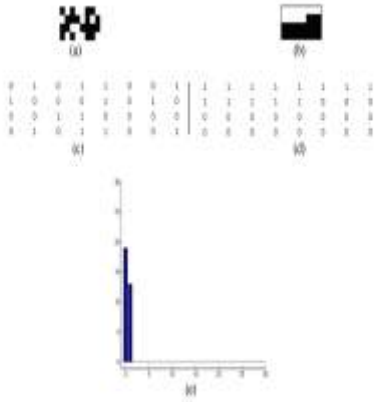
Fig. 4. Steganography based on Modulus operators. Histograms demonstrating the "pair effect": (top) original and (bottom) stego-image.

The previous histogram is given by the following discrete function:

$$H(k_i) = \sum_{i=0}^{255} g(k_i)$$

where, ki is the i th intensity level in the interval {0, 255} and g(ki) is the number of pixels in the image whose intensity level is ki . It is the nature of standard intensity image histograms to track and graph frequencies of pixel values in a given image and not their structure and how they are arranged, see Fig. 5.

Chi-square (2 F) and Pair-analysis algorithms can easily attack methods based on the spatial domain. Chisquare is a non-parametric (a rough estimate of confidence) statistical algorithm used in order to detect whether the intensity levels scatter in a uniform distribution throughout the image surface or not . If one intensity level has been detected as such, then the pixels associated with this intensity level are considered as corrupted pixels or in this case have a higher probability of having embedded data. The classical Chi-square algorithm can be fooled by randomly embedded messages, thus Bohne and Westfeld [108] developed a steganalysis method to detect randomly scattered hidden data in the LSB spatial domain that applies the Preserving Statistical Properties (PSP) algorithm.



If {o ,o ,...,o } Ri 1 2 n denote the observed data, this can be seen as the number of times the symbols 1, 0 occur in the image LSBs [45, pp. 311]. Let i e be the number of times the event is expected to occur. Then the test statistic is of the form:

$$\chi^2 = \sum \frac{(o_i - e_i)^2}{e_i}$$

To avoid detection during steganalysis attacks, data hiding methods for halftone images. The assumption set here is that the inverse halftoning process would smooth the noise occurring from data embedding. However, inspired by the steganalysis techniques for gray level images, a system able to counter-attack such methods by exploiting the wavelet statistic features extracted from the reconstructed gray level image through the inverse half toning of a given halftone image fed into the support vector machine's classifier. a statistical method that uses higher-order statistics called RS steganalysis; it is designed to provide an estimated percentage of flipped pixels caused by embedding as can be seen from Table 1 generated from Fig. 6 below.

Fig. 6. An image used to test for the RS steganalysis' performance.

Table 1. Estimated number of pixels with flipped LSBs for the test image in Fig. 6, with the actual numbers that should be detected in an ideal case (indicated in parenthesis).

Image	Red (%)	Green (%)	Blue (%)
Cover image	2.5 (0.0)	2.4 (0.0)	2.6 (0.0)
Steganos	10.6 (9.8)	13.3 (9.9)	12.4 (9.8)
S-Tools	13.4 (10.2)	11.4 (10.2)	10.3 (10.2)
Hide4PGP	12.9 (10.0)	13.8 (10.1)	13.0 (10.0)

it reveals that the performance of current state-of-the-art steganalysis algorithms for detection of r 1 steganography is highly sensitive to the used training and testing databases. Their experiments also show that the examined algorithms are not applicable in their current state since the embedding rate for testing is very likely to be unknown, while it was assumed otherwise in those algorithms. Therefore, we conclude that no single steganalysis algorithm is constantly superior.

VI. CONCLUSION

This paper presented a background discussion on the major algorithms of steganography deployed in digital imaging. The emerging techniques such as DCT are not too prone to attacks, especially when the hidden message is small. This is because they alter coefficients in the transform domain, thus image distortion is kept to a minimum. Generally these methods tend to have a lower payload compared to spatial domain algorithms. There are different ways to reduce the bits needed to encode a hidden message.

In short, there has always been a trade-off between robustness and payload. Scholars differ about the importance of robustness in steganography system design.

Steganography urges that the cover image must be carefully selected. A familiar image should not be used, it is better for steganographers to create their own images. This paper offered a few rules and suggestions on the configuration of a steganographic framework.

REFERENCES:

[1]. Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt School of Computing and Intelligent Systems, Faculty of Computing and Engineering University of Ulster at Magee, Londonderry, BT48 7JL, Northern Ireland, United Kingdom Emails: cheddad-a@email.ulster.ac.uk

[2] Yuk Ying Chung, fang Fei Xu , "Development of video watermarking for MPEG2 video" City university of Hong Kong ,IEEE 2006.

[3] C. Lu, J. Chen and K. Fan, "Real-time Frame-Dependent Video Watermarking in VLC Domain", Signal Processing : Image Communication 20, 2005, pp. 624–642.

[4]. Jonathan Cummins, Patrick Diskin, Samuel Lau and Robert Parlett, "Steganography and digital watermarking" School of Computer Science, The University of Birmingham. 2003. www.cs.unibo.it/people/phdstudents/scacciag/home_files/teach/datahide.pdf.

[5] Ravi shah , Abhinav Agraval & subramaniam Ganesham, "Frequency domain real time digital image watermarking " Oakland university.

[6] C. Lu, J. Chen, H. M. Liao, and K. Fan, "Real-Time MPEG2 Video Watermarking in the VLC Domain", Proc.of 16th International Conference on Pattern Recognition, Vol. 2, 11-15 August 2002, pp. 552-555.

[7] J. Haitsma and T. Kalker, "A Watermarking Scheme for Digital Cinema", Proceedings of the IEEE International Conference on Image Processing, Vol. 2, 2001, pp. 487–489.

[8] Christoph Busch ,Wolfgang Funk & Stephen Wolthusen ,"Digital Watermarking from concepts to Real - Time Video applications", IEEE Computer graphics and applications 1999.

[9] Chen Ming, Zhang Ru, Niu Xinxin,Yang Yixian, "Analysis of current steganography tools: Classification & features" ,Information security center, Beijing University. China.