




Review

# Digital image steganography: Survey and analysis of current methods

Abbas Cheddad  , [Joan Condell](#), [Kevin Curran](#), [Paul Mc Kevitt](#)[Show more](#)  Share  Cite<https://doi.org/10.1016/j.sigpro.2009.08.010> [Get rights and content](#) 

## Abstract

Steganography is the science that involves communicating secret data in an appropriate multimedia carrier, e.g., image, audio, and video files. It comes under the assumption that if the feature is visible, the point of attack is evident, thus the goal here is always to conceal the very existence of the embedded data. Steganography has various useful applications. However, like any other science it can be used for ill intentions. It has been propelled to the forefront of current security techniques by the remarkable growth in computational power, the increase in security awareness by, e.g., individuals, groups, agencies, government and through intellectual pursuit. Steganography's ultimate objectives, which are undetectability, robustness (resistance to various image processing methods and compression) and capacity of the hidden data, are the main factors that separate it from related techniques such as watermarking and cryptography. This paper provides a state-of-the-art review and analysis of the different existing methods of steganography along with some common standards and guidelines drawn from the literature. This paper concludes with some recommendations and advocates for the object-oriented embedding mechanism. Steganalysis, which is the science of attacking steganography, is not the focus of this survey but nonetheless will be briefly discussed.

## Introduction

The standard and concept of “What You See Is What You Get (WYSIWYG)” which we encounter sometimes while printing images or other materials, is no longer precise and would not fool a

steganographer as it does not always hold true. Images can be more than what we see with our Human Visual System (HVS); hence, they can convey more than merely 1000 words.

For decades people strove to develop innovative methods for secret communication. The remainder of this introduction highlights briefly some historical facts and attacks on methods (also known as steganalysis). A thorough history of steganography can be found in the literature [1], [2], [3].

Three techniques are interlinked, steganography, watermarking and cryptography. The first two are quite difficult to tease apart especially for those coming from different disciplines. Fig. 1 and Table 1 may eradicate such confusion. The work presented here revolves around steganography in digital images and does not discuss other types of steganography (such as linguistic or audio).

Intuitively, this work makes use of some terms commonly used by steganography and watermarking communities. The term “cover image” will be used throughout this paper to describe the image designated to carry the embedded bits. We will be referring to an image with embedded data, called herein payload, as “stego-image”. Further “steganalysis” or “attacks” refer to different image processing and statistical analysis approaches that aim to break or attack steganography algorithms (Fig. 2).

The word steganography is originally derived from Greek words which mean “Covered Writing”. It has been used in various forms for thousands of years. In the 5th century BC Histaiacus shaved a slave's head, tattooed a message on his skull and the slave was dispatched with the message after his hair grew back [1], [2], [3], [4]. In Saudi Arabia at the King Abdulaziz City of science and technology, a project was initiated to translate into English some ancient Arabic manuscripts on secret writing which are believed to have been written 1200 years ago. Some of these manuscripts were found in Turkey and Germany [5]. Five hundred years ago, the Italian mathematician Jérôme Cardan reinvented a Chinese ancient method of secret writing. The scenario goes as follows: a paper mask with holes is shared among two parties, this mask is placed over a blank paper and the sender writes his secret message through the holes then takes the mask off and fills the blanks so that the message appears as an innocuous text as shown in Fig. 3. This method is credited to Cardan and is called Cardan Grille [4].

It was also reported that the Nazis invented several steganographic methods during World War II such as Microdots, and have reused invisible ink and null ciphers. As an example of the latter a message was sent by a Nazi spy that read: “Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by-products, ejecting suets and vegetable oils.” Using the 2nd letter from each word the secret message reveals: “Pershing sails from NY June 1” [2], [6], [7].

In 1945, Morse code was concealed in a drawing (see Fig. 4). The hidden information is encoded onto the stretch of grass alongside the river. The long grass denoted a line and the short grass denoted a point. The decoded message read: “Compliments of CPSA MA to our chief Col Harold R. Shaw on his visit to San Antonio May 11th 1945” [8].

With the boost in computer power, the internet and with the development of digital signal processing (DSP), information theory and coding theory, steganography has gone “digital”. In the realm of this digital world steganography has created an atmosphere of corporate vigilance that has spawned various interesting applications, thus its continuing evolution is guaranteed. Contemporary information hiding is due to [9]. One of the earliest methods to discuss digital steganography is credited to Kurak and McHugh [10], who proposed a method which resembles embedding into the 4 LSBs (least significant bits). They examined image downgrading and contamination which is known now as image-based steganography.

Cyber-crime is believed to benefit from this digital revolution. Hence an immediate concern was shown on the possible use of steganography by terrorists following a report in USA TODAY.<sup>1</sup> Cyber-planning or the “digital menace” as Lieutenant Colonel Timothy L. Thomas defined it, is difficult to control [11]. Provos and Honeyman [3], at the University of Michigan, scrutinized three million images from popular websites looking for any trace of steganography. They have not found a single hidden message. Despite the fact that they attributed several reasons to this failure it should be noted that steganography does not exist merely in still images. Embedding hidden messages in video and audio files is also possible. Examples exist in [12] for hiding data in music files, and even in a simpler form such as in Hyper Text Mark up Language (HTML), executable files (.EXE) and Extensible Markup Language (XML) [13]. This shows that USA TODAY's claim is not supported by a strong evidence, especially knowing that the writer of the above report resigned about two years later after editors determined that he had deceived them during the course of their investigation.<sup>2</sup>

This paper's focus is on the review of steganography in digital images. For a detailed survey on steganographic tools in other media from a forensic investigator's perspective the reader is referred to [14].

Section 2 briefly discusses the applications of steganography. Methods available in the literature are described in Section 3. The main discussions and comparisons focus on spatial domain methods, frequency domain methods and also adaptive methods in digital images. It will be shown that most of the steganographic algorithms discussed have been detected by steganalysis algorithms and thus a more robust approach needs to be developed and investigated. Section 4 will give a brief analysis and set it in context. Section 5 will discuss in brief the counterfeiting of steganography, a science known as steganalysis. A conclusion is provided in Section 6.

---

## Access through your organization

Check access to the full text by signing in through your organization.

Access through **your organization**

---

## Section snippets

### Steganography applications

Steganography is employed in various useful applications, e.g., copyright control of materials, enhancing robustness of image search engines and smart IDs (identity cards) where individuals' details are embedded in their photographs. Other applications are video–audio synchronization, companies' safe circulation of secret data, TV broadcasting, TCP/IP packets (for instance a unique ID can be embedded into an image to analyze the network traffic of particular users) [1], and also checksum ...

## 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 ...

## Analysis and recommendations

As a performance measurement for image distortion, the well known peak-signal-to-noise ratio (PSNR) which is classified under the difference distortion metrics can be applied on the stego-images. It is defined as:  $PSNR = 10 \log_{10} \left( \frac{C_{\max}^2}{MSE} \right)$  where  $MSE$  denotes mean square error which is given as:  $MSE = \frac{1}{MN} \sum_{x=1}^M \sum_{y=1}^N (S_{xy} - C_{xy})^2$  where  $x$  and  $y$  are the image coordinates,  $M$  and  $N$  are the dimensions of the image,  $S_{xy}$  is the generated stego-image and  $C_{xy}$  is the cover image. Also  $C_{\max}^2$  holds the maximum value in ...

## Steganalysis

This article does not delve into the details 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 ...

## Conclusions and summary

This paper presented a background discussion on the major algorithms of steganography deployed in digital imaging. The emerging techniques such as DCT, DWT and adaptive steganography 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