**IMAGE STENOGRAPHY WITH THREE WAYS ENCRYPTION**

**YOHANNA ISAAC**

**(ST/CS/ND/20/057)**

**A SEMINAR REPRESENTED TO THE DEPARTMENT OF COMPUTER SCIENCE, SCHOOL OF SCIENCE AND TECHNOLOGY, FEDERAL POLYTECHNIC MUBI, ADAMAWA STATE, NIGERIA**

**NOVEMBER, 2022**

**IMAGE STENOGRAPHY WITH THREE WAYS ENCRYPTION**

**YOHANNA ISAAC**

**(ST/CS/ND/20/057)**

**A SEMINAR REPRESENTED TO THE DEPARTMENT OF COMPUTER SCIENCE, SCHOOL OF SCIENCE AND TECHNOLOGY, FEDERAL POLYTECHNIC MUBI, ADAMAWA STATE, NIGERIA**

**IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF NATIONAL DIPLOMA (ND) IN COMPUTER SCIENCE**

**NOVEMBER, 2022**

**Abstract**

*Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the Internet. For hiding secret information in images, there exists a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points. Different applications have different requirements of the steganography technique used. For example, some applications may require absolute invisibility of the secret information, while others require a larger secret message to be hidden. This paper intends to give an overview of image steganography, its uses and techniques. It also attempts to identify the requirements of a good steganographic algorithm and briefly reflects on which steganographic techniques are more suitable for which applications.*

**Keywords:** Stenography, Encryption, Data Security, Technique, Image stenography.

# 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 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” defining it as “covered writing”. In image steganography the information is hidden exclusively in images (Ahsan & Kundur, 2012).

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 (Bender *et al.,* 2016). 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 paper containing hidden information (Chandramouli *et al.,* 2003). 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 (Artiz, 2021). 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. The strength of steganography can thus be amplified by combining it with cryptography (Artiz, 2021).

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 (Currie & Irvine, 2006). 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. 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 (Artiz, 2021). 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 (Artiz, 2021).

# Literature Review

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 realise 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. Hiding information in a photograph of the company picnic is less suspicious than communicating an encrypted file (Chandramouli et al., 2003).

To provide an overview of steganography, terms and concepts should first be explained. An overview of the different kinds of steganography is given at a later stage. Although steganography is an ancient subject, the modern formulation of it is often given in terms of the *prisoner’s problem* proposed by Simmons, where two inmates wish to communicate in secret to hatch an escape plan. All of their communication passes through a warden who will throw them in solitary confinement should she suspect any covert communication (Dunbar, 2022).

The warden, who is free to examine all communication exchanged between the inmates, can either be passive or active. A *passive* warden simply examines the communication to try and determine if it potentially contains secret information. If she suspects a communication to contain hidden information, a passive warden takes note of the detected covert communication, reports this to some outside party and lets the message through without blocking it. An *active* warden, on the other hand, will try to alter the communication with the suspected hidden information deliberately, in order to remove the information (Bender et al., 2016).

## Different kinds of steganography

Almost all digital file formats can be used for steganography, but the formats that are more suitable are those with a high degree of redundancy. Redundancy can be defined as the bits of an object that provide accuracy far greater than necessary for the object’s use and display. The redundant bits of an object are those bits that can be altered without the alteration being detected easily. Image and audio files especially comply with this requirement, while research has also uncovered other file formats that can be used for information hiding. Figure 1 shows the four main categories of file formats that can be used for steganography (Bender et al., 2016).

Text Images Audio/ Protocol

video

Figure 1: Categories of steganography

Hiding information in text is historically the most important method of steganography. An obvious method was to hide a secret message in every *nth* letter of every word of a text message. It is only since the beginning of the Internet and all the different digital file formats that is has decreased in importance. Text steganography using digital files is not used very often since text files have a very small amount of redundant data (Ahsan & Kundur, 2012).

To hide information in audio files similar techniques are used as for image files. One different technique unique to audio steganography is masking, which exploits the properties of the human ear to hide information unnoticeably. A faint, but audible, sound becomes inaudible in the presence of another louder audible sound. This property creates a channel in which to hide information. Although nearly equal to images in steganographic potential, the larger size of meaningful audio files makes them less popular to use than images (Jamil, 2019).

The term protocol steganography refers to the technique of embedding information within messages and network control protocols used in network transmission. In the layers of the OSI network model there exist covert channels where steganography can be used. An example of where information can be hidden is in the header of a TCP/IP packet in some fields that are either optional or are never used (Handel & Sandford, 2012).

## Image steganography

As stated earlier, images are the most popular cover objects used for steganography. In the domain of digital images many different image file formats exist, most of them for specific applications. For these different image file formats, different steganographic algorithms exist (Jamil, 2019).

### Image definition

To a computer, an image is a collection of numbers that constitute different light intensities in different areas of the image. This numeric representation forms a grid and the individual points are referred to as pixels. Most images on the Internet consists of a rectangular map of the image’s pixels (represented as bits) where each pixel is located and its colour. These pixels are displayed horizontally row by row (Jamil, 2019).

### Image Compression

When working with larger images of greater bit depth, the images tend to become too large to transmit over a standard Internet connection. In order to display an image in a reasonable amount of time, techniques must be incorporated to reduce the image’s file size. These techniques make use of mathematical formulas to analyse and condense image data, resulting in smaller file sizes. This process is called compression. In images there are two types of compression: lossy and lossless. Both methods save storage space, but the procedures that they implement differ. Lossy compression creates smaller files by discarding excess image data from the original image. It removes details that are too small for the human eye to differentiate, resulting in close approximations of the original image, although not an exact duplicate. An example of an image format that uses this compression technique is JPEG (Joint Photographic Experts Group) (Johnson & Jajodia, 2018).

Compression plays a very important role in choosing which steganographic algorithm to use. Lossy compression techniques result in smaller image file sizes, but it increases the possibility that the embedded message may be partly lost due to the fact that excess image data will be removed. Lossless compression though, keeps the original digital image intact without the chance of lost, although it does not compress the image to such a small file size. Different steganographic algorithms have been developed for both of these compression types and will be explained in the following sections (Owens, 2019).

## Transform Domain

To understand the steganography algorithms that can be used when embedding data in the transform domain, one must first explain the type of file format connected with this domain. The JPEG file format is the most popular image file format on the Internet, because of the small size of the images.

# JPEG compression

To compress an image into JPEG format, the RGB colour representation is first converted to a YUV representation. In this representation the Y component corresponds to the luminance (or brightness) and the U and V components stand for chrominance (or colour). According to research the human eye is more sensitive to changes in the brightness (luminance) of a pixel than to changes in its colour. This fact is exploited by the JPEG compression by downsampling the colour data to reduce the size of the file. The colour components (U and V) are halved in horizontal and vertical directions, thus decreasing the file size by a factor of 2 (Ahsan & Kundur, 2012).

# JPEG steganography

Originally it was thought that steganography would not be possible to use with JPEG images, since they use lossy compression which results in parts of the image data being altered. One of the major characteristics of steganography is the fact that information is hidden in the redundant bits of an object and since redundant bits are left out when using JPEG, it was feared that the hidden message would be destroyed. Even if one could somehow keep the message intact it would be difficult to embed the message without the changes being noticeable because of the harsh compression applied. However, properties of the compression algorithm have been exploited in order to develop a steganographic algorithm for JPEGs.

The DCT and the quantization phase form part of the lossy stage, while the Huffman encoding used to further compress the data is lossless. Steganography can take place between these two stages. Using the same principles of LSB insertion the message can be embedded into the least significant bits of the coefficients before applying the Huffman encoding. By embedding the information at this stage, in the transform domain, it is extremely difficult to detect, since it is not in the visual domain (Ahsan & Kundur, 2012).

# Patchwork

Patchwork is a statistical technique that uses redundant pattern encoding to embed a message in an image. The algorithm adds redundancy to the hidden information and then scatters it throughout the image. A pseudorandom generator is used to select two areas of the image (or patches), patch A and patch B. All the pixels in patch A is lightened while the pixels in patch B is darkened. In other words the intensities of the pixels in the one patch are increased by a constant value, while the pixels of the other patch are decreased with the same constant value. The contrast changes in this patch subset encodes one bit and the changes are typically small and imperceptible, while not changing the average luminosity (Lee & Chen, 2020).

# Spread Spectrum

In spread spectrum techniques, hidden data is spread throughout the cover-image making it harder to detect. A system proposed by Marvel et al. combines spread spectrum communication, error control coding and image processing to hide information in images. Spread spectrum communication can be defined as the process of spreading the bandwidth of a narrowband signal across a wide band of frequencies. This can be accomplished by adjusting the narrowband waveform with a wideband waveform, such as white noise. After spreading, the energy of the narrowband signal in any one frequency band is low and therefore difficult to detect. In spread spectrum image steganography, the message is embedded in noise and then combined with the cover image to produce the stego image. Since the power of the embedded signal is much lower than the power of the cover image, the embedded image is not perceptible to the human eye or by computer analysis without access to the original image (Currie & Irvine, 2006).

## Evaluation of different techniques

All the above-mentioned algorithms for image steganography have different strong and weak points and it is important to ensure that one uses the most suitable algorithm for an application. All steganographic algorithms have to comply with a few basic requirements. The most important requirement is that a steganographic algorithm has to be imperceptible. The authors propose a set of criteria to further define the imperceptibility of an algorithm. These requirements are as follows:

**Invisibility** – The invisibility of a steganographic algorithm is the first and foremost requirement, since the strength of steganography lies in its ability to be unnoticed by the human eye. The moment that one can see that an image has been tampered with, the algorithm is compromised

**Payload capacity** – Unlike watermarking, which needs to embed only a small amount of copyright information, steganography aims at hidden communication and therefore requires sufficient embedding capacity.

**Robustness against statistical attacks** – Statistical steganalysis is the practice of detecting hidden information through applying statistical tests on image data. Many steganographic algorithms leave a ‘signature’ when embedding information that can be easily detected through statistical analysis. To be able to pass by a warden without being detected, a steganographic algorithm must not leave such a mark in the image as be statistically significant.

**Robustness against image manipulation** – In the communication of a stego image by trusted systems, the image may undergo changes by an active warden in an attempt to remove hidden information. Image manipulation, such as cropping or rotating, can be performed on the image before it reaches its destination. Depending on the manner in which the message is embedded, these manipulations may destroy the hidden message. It is preferable for steganographic algorithms to be robust against either malicious or unintentional changes to the image.

**Independent of file format** – With many different image file formats used on the Internet, it might seem suspicious that only one type of file format is continuously communicated between two parties. The most powerful steganographic algorithms thus possess the ability to embed information in any type of file. This also solves the problem of not always being able to find a suitable image at the right moment, in the right format to use as a cover image.

**Unsuspicious files** – This requirement includes all characteristics of a steganographic algorithm that may result in images that are not used normally and may cause suspicion. Abnormal file size, for example, is one property of an image that can result in further investigation of the image by a warden.

### Advantages

1. The advantage of steganography is that messages do not send consideration to themselves. Clearly detectable encrypted message no matter how tough will stimulate suspicion, and may in themselves be compromising in countries where encryption is illegitimate.
2. In steganography, cryptography secures the contents of a message, steganography can be said to secure both messages and connecting parties.
3. This approach featured security, capacity, and robustness, the three needed element of steganography that creates it beneficial in hidden exchange of data through text files and creating secret communication.
4. With the need of Steganography Corporation government and law enforcement agencies can connect privately.
5. Steganography has a double component of protection such as first, the file itself is secret and second, the data in it is encoded.

### Disadvantages

1. There are large number of information, huge file size, therefore someone can suspect about it.
2. If this approach is gone in the wrong hands such as hackers, terrorist, criminals then this can be very much critical.
3. Steganography is not without its disadvantages. However, these can be rectified and once it is performed and it can strengthen the element of steganography.
4. Most data hiding approach take advantage of human perceptual deficiency, but they have deficiency of their own. However, these can be independently rectified.
5. The major disadvantage of steganography is that, unlike cryptography, it needed a lot of overhead to hide associatively few bits of information.

### Conclusion

Although only some of the main image steganographic techniques were discussed in this paper, one can see that there exists a large selection of approaches to hiding information in images. All the major image file formats have different methods of hiding messages, with different strong and weak points respectively. Where one technique lacks in payload capacity, the other lacks in robustness. For example, the patchwork approach has a very high level of robustness against most type of attacks, but can hide only a very small amount of information. Least significant bit (LSB) in both BMP and GIF makes up for this, but both approaches result in suspicious files that increase the probability of detection when in the presence of a warden.

**Recommendations**

1. It is recommended that for an agent to decide on which steganographic algorithm to use, he would have to decide on the type of application he want to use the algorithm for and if he is willing to compromise on some features to ensure the security of others.
2. It is recommended that more review be made on the security technique and imbibe since it offers more advantages and benefits over other techniques.
3. It is also recommended that Steganography can make use of unlimited legal means to use any web site without attracting the attention of anybody, including the owners of the target web sites themselves and therefore be used as a major data security technique.

### References

Ahsan, K. & Kundur, D. (2012). Practical Data hiding in TCP/IP”, *Proceedings of the Workshop on Multimedia Security at ACM Multimedia*, 14(1), 13-23.

Artiz, D. (2021). Digital Steganography: Hiding Data within Data, *IEEE Internet Computing Journal*, 6(2), 41-78.

Bender, W., Gruhl, D., Morimoto, N. & Lu, A. (2016). Techniques for data hiding, *IBM Systems Journal*, 35, 23-45.

Chandramouli, R., Kharrazi, M. & Memon, N. (2003). Image steganography and steganalysis: Concepts and Practice, *Proceedings of the 2nd International Workshop on Digital Watermarking*, 12(1), 34-66.

Currie, D. & Irvine, C. (2006). “Surmounting the effects of lossy compression on Steganography”, *19th National Information Systems Security Conference*, 5(1), 16-23.

Dunbar, B. (2022). Steganographic techniques and their use in an Open-Systems environment, *SANS Institute*, 11(2), 33-78.

Handel, T. & Sandford, M. (2012). Hiding data in the OSI network model”, *Proceedings of the 1st International Workshop on Information Hiding*, 23(1), 23-56.

Jamil, T. (2019). Steganography: The art of hiding information is plain sight”, *IEEE Potentials*, 18(1), 13-35.

Johnson, N. & Jajodia, S. (2018). Exploring Steganography: Seeing the Unseen”, *Computer Journal*, 8(1), 12-19.

Lee, Y. & Chen, L. (2020). High capacity image steganographic model”, *Visual Image Signal Processing*, 147:03.

Owens, M. (2019). “A discussion of covert channels and steganography”, *SANS Institute*, 2002