# ANALYSIS OF IMAGE STEGANALYSIS TECHNIQUES TO DEFEND AGAINST STATISTICAL ATTACKS – A SURVEY

**Usha B.A[1], N K Srinath[2], N K Cauvery[3]**

[1, 2, 3]*Asst Professor, Prof and HOD, Professor, Dept of CSE, R V College of Engineering, Bangalore, India*
***ushaba@rvce.edu.in, srinathnk@rvce.edu.in, cauverynk@rvce.edu.in***

**Abstract**

*Steganography is the art concealing information to transmit it in such a way that nobody but the intended receiver knows the existence of the message. Steganalysis techniques work on eliminating suspicion about the existence of a message. If suspicion is raised, then the message cannot be passed covertly. One of the ways to detect the hidden message is to view the statistical properties of the image or medium in which the message is hidden. This is called a statistical attack. In this paper, we explain the nature of such attacks and present our conclusions based on reviews of existing methods of defense against statistical attacks.*

***Keywords***– *Steganalysis, Steganography, statistical attacks, JPEG images, OutGuess*

----------***----------

## 1. INTRODUCTION

Steganography comes from Greek words meaning "covered writing". Over the ages, it has developed into an art of hiding the very existence of a message when it is being relayed. Any code that can be represented digitally can act as a carrier for a message. This could be text, an image, a video or any other such "innocent looking" media. A *message* is the information hidden in anything that can be embedded into a bit stream like plain text, cipher text or even another image. A *stego-carrier* is the name given to the cover carrier and the embedded message together. A *stegokey* is any additional hidden information, such as a password, required to be able to send a message. A possible formula of the process may be represented as: [1]

Cover medium + embedded message + stegokey = stego-medium

### 1.1 Methods Used

Due to their omnipresence in the World Wide Web, images provide excellent carriers for hidden information. Many different techniques have been introduced till date [2]. Each of these can be used to test detection properties and robustness in the effort to destroy or disable the embedded message. These techniques can be broadly categorized into two groups: those in the Image Domain and those in the **Transform Domain.**

i) Image Domain tools make use of bit-wise methods that apply least significant bit (LSB) insertion and noise manipulation. These "simple system" approaches in steganography [3] set the least significant bits of image pixels equal to those of the message text.

The tools used in this group include StegoDos, S-Tools, Hide and Seek, Hide4PGP and Steganos among others. There is no loss in the image formats used in such steganography and it allows data to be directly manipulated and recovered. This approach also comprises including additional components such as masks or image objects to watermark an image.

ii) The transform domain tools involve manipulation of algorithms and image transforms such as discrete cosine transformation (DCT) and wavelet transformation. These methods hide messages in more significant areas of the covering image medium and hence may end up manipulating image properties such as brightness. Watermarking tools belong to this category. Software that implements this approach includes PictureMarc, JK-PGS, SysCop, and SureSign. This approach is more robust than bit-wise techniques but there exists a tradeoff between this robustness and the amount of information that can feasibly be added to the image. [1]

JPEG images use the Discrete Cosine Transform (DCT) to achieve image compression. The compressed data is stored as integers; however, if we need to quantize the data to encode a message, all the calculations required involve floating point data. Information is hidden in the JPEG image by modulating the rounding choices either up or down in the DCT coefficients. Detection of such an embedded message would seem to be quite difficult. In this rounding off, errors may occur and this leads to the losses in this method. The tool Jpeg-Jsteg is a steganography tool that makes use of this property. In steganography when we divide the image into 8x8 sub-images, the boundaries of these sub-images may become visible, leading to a disjoint image. This is called blocking artifact and DCT is used to minimize it. [4]

We can also use tools whose approach combines image and transform domain tools. These may include approaches like patchwork and masking which make the hidden information seem redundant. [3] Hence the steganography is successful and independent of effects like cropping and rotation. Patchwork uses a pseudo-random technique to select multiple patches of an image for marking with a watermark so that even if one is lost, the entire message is not lost. Masks use image domain tactics since they are just an extra component or image object. They also use transform domain tools for adjusting image properties or transforming them.

### 1.2 Steganalytic Detection

For a person applying Steganalysis to determine the presence of a message, the method he will use is called a steganalytic attack. There are five main types of attacks possible, namely stego-only, known cover, known message, chosen stego, and chosen message. A stego-only attack is one where only the stego-medium is available for analysis. If the "original" cover-media and stego-media are both available, then a known cover attack is available. A known message attack is used when the hidden message is revealed at some later date, and an attacker may attempt to analyze the stego-media for future attacks. The chosen stego attack is one where the steganography algorithm and stego-media are known. A chosen message attack is one where the steganalyst generates stego-media from some steganography tool or algorithm and a known message so that he can find out which tools and algorithms are used based on the patterns he can detect.

## 2. STATISTICAL ATTACKS

### 2.1. Characteristics Of A Statistical Attack

While embedding the message in a medium, there are certain statistical properties of the medium that need to be maintained. If not maintained, they can reveal the existence of a hidden message. For example if the medium is an image, examples of such properties would include PoVs. A PoV or pair of values is a tuple (2i, 2i +1) that indicates that the bit denoted by 2i is transformed onto the bit 2i+1 after encoding the message within the image. These PoVs are automatically generated when the image is encoded and can be stored. Then, for the kth pixel, the frequency histogram of the image, denoted by Yk will change and then the presence of the message will become apparent. Hence we need to maintain that Y2i+Y2i+1 remains a constant. If not, this type of attack is called a statistical attack.

The main types of statistical analysis include histographic, chi-square, generalized chi-square and pairs analysis.

Histographic analysis on JPEG sequential and pseudo-random embedding type stegosystems, such as JSteg and Outguess 0.1 can effectively estimate the length of the message embedded and it is based on the loss of histogram symmetry after embedding. $\chi 2$ makes use of the generalized Euler Gamma function and has a rigorous mathematical proof.

The generalised $\chi 2$ attack does not calculate an estimation of the message length and can be sometimes wrong if the message has a significant difference in the number of zeros compared to ones.

Pairs analysis was designed specifically for GIF images but works well for greyscale BMP images as well and can estimate the length of the message embedded. [5]

## 3. CURRENT APPROACHES IN STEGANALYSIS

At present, there are two approaches to the problem of steganalysis, one where there exists a specific steganographic technique for a specific steganographic algorithm or one where the technique is independent of it. The success of these algorithms depends on its capacity to detect the presence of an image. Decoding of a message can be cumbersome if strong cryptographic tools have been used. If the individual is able to detect the presence of a message, then the steganographic system is said to be insecure [7] and we need to find ways to ensure secure transmission of secret messages.

Here, the authors discuss the possibilities of deterministic and non-deterministic approaches in steganography. The deterministic method proves to be ineffective if both the stego and the cover are known to a third person that wants to break into the system. In [7], we see that it is impossible to have secure data in such cases. Thus, indeterminism is introduced in the embedding operation. This results in randomness each time the process is computed thus introducing uncertainty. Thus, if the attacker is aware of the stego and the cover (S and C respectively), then when S is known, C is uncertain, such that $H(C/S) > 0$ where H denotes the entropy. To ensure this, the authors in [7] introduce another variable CS from which the actual cover is selected. They assume that the steganographic function, CS and the stego are publicly known whereas the key and cover are unknown to the attackers. They prove that the cover must contain an uncertainty for the attacker to allow secure steganography between sender and recipient. Thus, to ensure security, the embedding process must be split into two: non - deterministic and deterministic parts, which are indistinguishable to the attacker.

For instance, an image taken using a camera can easily portray the area where the image was captured and the features of the camera. But, the position of the camera or the direction of the camera while capturing the image cannot be predicted accurately. Thus, the attacker is unaware of the image details and cannot distinguish between an original image and a steganographic one. Thus, we can say that preprocessing i.e. positioning of the camera initiates randomness into the cover data.

Another method to ensure secure data sending illustrates the idea of a trusted domain. In [7], we see that ISDN allows secure

communication with steganography with the aid of bit transparent transportation of digital data. Here, the attacker fails to encode the secret message without the key even if he knows the source and the embedding function. The characteristic of the output (stego or cover) cannot be determined from outside in this method.

Information hiding begins by modifying the redundant bits, which can change the statistical properties of the cover. For instance, equal likelihood of 1's and 0's occurs. But, redundant data tends to converge towards one of them. Embedding data thus weakens the correlation. [9] Thus, for secure steganography, the key and the actual cover must remain unknown to the attacker. We also need to apply additional transforms to the redundant data, which correct measurable deviations in the embedding process. This is possible by concealing the key with a symmetric cryptosystem. The embedding of the message in the image must also allow for randomness to enhance security. One must also be aware of the preprocessing techniques for effective steganographic implementation of messages.

## 4. COMMONLY USED STEGANOGRAPHY ALGORITHMS

Based on the images they operate on, the algorithms can be classified into three types – raw images, palette based and JPEG images.

### 4.1 Raw Images

We understand that the simple LSB (Least Significant Bit) embedding method operates on raw images, where the message is embedded in a subset of the LSB plane of the image usually after encryption [6]. As discussed earlier, this introduces partitioning of the image into PoVs. Since the values are mapped, it provides statistical flattening of the distribution of values.

However, the major drawback of this technique is the length constraint as it embedding can be detected only when the length is comparable to the number of pixels in the image. Analysis from [6] shows that only with prior knowledge of where the message is placed, messages of shorter length can be detected which is too strong an assumption to make.

4.2 Palette Based Images

In case of palette based images [6], we see that by observing the palette tables in GIF images and the anomalies caused by stego tools that perform LSB embedding in GIF images, we can distinguish between stego and cover images.

The author emphasizes that in order to reduce the distortion caused by embedding as proposed by EzStego in [10], the colour pallet is sorted such that the colour differences between consecutive colors is minimized. The message bits are then embedded in the LSB of the indices. Since similar pixels, which can modify due to the embedding process, get mapped to the neighboring colors in the palette, visual artifacts are minimal and hard to observe.

### 4.3 JPEG Images

JPEG format is one of the most widely used formats these days and is subjected to constant research in terms of steganalysis and steganography. One of the most frequently used algorithms is the OutGuess Embedding Program proposed by Fridrich.

It embeds the data in LSB of the DCT coefficients randomly, leaving some coefficients unchanged. In order to preserve the original histogram of DCT coefficients, the remaining coefficients are adjusted. Thus, the method that involves estimation of the original histogram proves to be ineffective. We discuss the OutGuess program again briefly. [6]

## 5. STATISTICAL EMBEDDING

In [9], the author discusses embedding techniques that distribute the hidden message uniformly across the image. Provos [9] explains that this process can be split into two stages – Identification of redundant bits and selection of bits where the data is to be placed.

Provos [9] emphasizes that the image format plays an important role in identifying the redundant bits. He also discusses the importance of pseudo random number generator (PRNG) that introduces randomness. For bit selection, a cipher is used. We understand this process from [9]. We realize that since the PRNG has a secret key, it is impossible to detect the message without the key.

## 6. STATISTICAL DETECTION

By determining that an image's statistical properties that deviate from a norm, we can figure out whether an image has been modified steganographically. Certain tests do this by measuring the entropy of the redundant data, which is higher if the image has a hidden message. [8]

We realize that DCT coefficients play a significant role in the embedding process as observed by the authors in [8]. The different steganographic systems in use include -JSteg, JSteg-Shell and JPHide and OutGuess. These are popular systems for JPEG images. These systems utilize a form of least- significant bit embedding and are detectable by statistical analysis except for the OutGuess. The authors have discussed various aspects on these systems in [8].

[8] In the JSteg system, the DCT coefficients are modified continuously from the beginning of the image. It does not support encryption and has no random bit selection. Here, the first five bits of the header contain the size of the length field in bits and the remaining ones express the size of the embedded

data. [8] In case of JPHide, detecting content is more difficult a task as the DCT coefficients isn't selected continuously from the beginning unlike the first system JSteg. It uses a fixed table that defines classes of DCT coefficients to determine the order in which the coefficients are to be modified. In this technique, the next class is chosen only after the coefficients in the current class are used. This ensures information hiding in the class even after the entire message has been embedded. This ensures enhanced security as the all the DCT coefficients involved are modified even if the message is only 8 bits long (approx. 5000 co-eff.). Using this technique, we can modify the second least significant bits of the DCT coefficients apart from the usual least significant bits.

On the other hand, we find the OutGuess technique to be more efficient than the previous two discussed in [8]. This chooses the DCT coefficients with a pseudo-random number generator. A user-supplied pass phrase initializes a stream cipher (which encrypts the content) and a pseudo-random number generator, both based on RC4. The authors observe that the newer version OutGuess 0.2 preserves statistical properties unlike the version 0.13b which is vulnerable. When the OutGuess 0.2 technique is used, the $\chi$2-test discussed earlier fails. In [9], Provos demonstrates how the OutGuess program preserves the statistical properties of the image. Thus, we can preserve data in the image and ensure effective communication without the attacker knowing the content.

## 7. NEED FOR EFFECTIVE DETECTION AND ITS APPLICATIONS

Steganography is a growing field with serious applications in the world today. There is no way to control the huge number or type of images being sent over the Internet and hence we have no way to individually inspect each of them to ascertain the presence of a hidden message. This could lead to dire consequences like terrorist activities, financial scams or even large-scale brainwashing. For example, in 2001, US officials stated that they have suspicions that terrorists communicate using steganography via the Internet.

"Hidden in the X-rated pictures on several pornographic Web sites and the posted comments on sports chat rooms may lie the encrypted blueprints of the next terrorist attack against the United States or its allies. It sounds far fetched, but U.S. officials and experts say it's the latest method of communication being used by Osama bin Laden and his associates to outfox law enforcement. Bin Laden, indicted in the bombing in 1998 of two U.S. embassies in East Africa, and others are hiding maps and photographs of terrorist targets and posting instructions for terrorist activities on sports chat rooms, pornographic bulletin boards and other Web sites, U.S. and foreign officials say." Such situations require identical counter attacks and hence the governments of various countries, as well as anti terrorism organizations, intelligence and espionage bureaus need to be able to pass steganographically-encoded information without its being threatened by statistical attacks. Even to send nuclear, defence weapons, military tactics, espionage and foreign strategy related messages; defence against statistical attack is definitely the need of the hour.

## CONCLUSIONS

In this paper we have recorded and summarized the current scenario in the highly stimulating field of Steganalysis. Defense against statistical attacks in Steganalysis holds great potential for future research considering its vast scope and extremely important applications. The methods used in status quo are sufficiently advanced and can provide suitable defence against current attacks. However, with growing awareness about steganography and the abundance of transmission media for images and hidden information, it can only be predicted that methods of attack will only become more sophisticated. In such a scenario we need to constantly observe new forms of attack and keep coming up with new techniques of defense against them.

## REFERENCES

[1] Johnson, N.F., Jajodia, S., Steganalysis of Images Created using Current Steganography Software, Workshop on Information Hiding Proceedings, Portland, Oregon, USA, 15 - 17 April 1998.

[2] Johnson, N.F., Jajodia, S: Exploring Steganography: Seeing the Unseen, IEEE Computer, February (1998) 26-34

[3] Anderson, R., Petitcolas, F.: On the Limits of Steganography, IEEE Journal on Selected Areas in Communications, Vol. 16, No. 4, May

[4] Gonzalez, R.C., Woods, R.E.: Digital Image Processing. Addison-Wesley. Reading, MA, (1992)

[5]http://www.computing.surrey.ac.uk/personal/st/H.Schaathun /projects/Past/leivaditis.pdf

[6] Mehdi Kharrazi, Husrev T. Sencar, and Nasir Memon, Image Steganography: Concepts and Practice, WSPC Lecture Notes, April 2004

[7] J.Zöllner, H.Federrath, H.Klimant, A.Pfitzmann, R.Piotraschke, A.Westfeld, G.Wicke, G.Wolf, Modeling the security of steganographic systems, Proceedings, 2nd workshop on Information Hiding, April 1998, Portland

[8] Niels Provos, Peter Honeyman, Detecting Steganographic Content on the Internet, Center for Information Technology Integration, University of Michigan

[9] Niels Provos, Defending Against Statistical Steganalysis, CITI Technical Report 01-4, Center for Information Technology Integration, University of Michigan

[10]R. Machado, "Ezstego," http://www.stego.com, 2001.