Evaluation of Different Steganalysis Methods

JesúsVélez Torres
Computer Science
Juan Ramírez, Ph.D.
Department of Electrical & Computer Engineering and Computer Science
Polytechnic University of Puerto Rico

Abstract—*After the September 11, 2001 terrorist attack on the World Trade Center the United States declared war on terrorism. The Patriot Act (H.R. 3162) was passed, which authorizes law enforcement agencies to monitor and intercept the electronic communications of suspected terrorists. This meant that telephone communication and encrypted telephony would no longer be safe for terrorists to communicate with each other. This provoked them to search for alternate means to communicate sensitive information. The New York Times, USA Today, and the United States Institute of Peace have reported that terrorists may be using steganography and cryptography on the web as a means for convert communications [1, 2, 3]. These reports have been the basis of several studies into convert communication by terrorists. It is becoming increasingly important to detect the images that contain steganography such that we can reduce foul-play. This counter technique is known as steganalysis.There are two problems in steganalysis: detecting the existence of a hidden message and decoding the message. This research is only concerned with the first problem, which is the detection of hidden messages using statistical steganalysis.*

Key Terms—*Carrier, Medium, Steganalysis, Steganography.*

INTRODUCTION

Steganography is known as the art of covert writing. Its purpose is hiding messages from a third party. This is different from cryptography in the sense that it's intended to be hidden or unknown; while cryptography makes it unreadable it does not hide its existence. The steganography process occurs when placing a hidden message in some medium like: pictures, videos, etc, this is called the carrier. The secret message is embedded in the medium for inconspicuous transportation; an encryption key may even be used to make it harder to decode the message. In summary:

SteganographyMedium = HiddenMessage + Carrier + SteganogrpahyKey

As computers increase their presence in our daily lives the amount of data stored in them increases as well. Some of this data can be sensitive and it is not surprising seeing steganography jump to the digital world. Steganography applications allow people to store any binary file in other binary file. This fact creates endless possibilities and multiple carrier formats like: sound files, movie files, picture files and other type of media files.

Steganography can be used for security reasonslike securing sensitive data, but it also hasa lot of nefarious applications; like hiding records or evidence of illegal activity, industrial espionage, fraud and communication of criminal organizations like terrorists or gangs. This is way the Department of Defense of the United States of America is really interested in developing techniques and technologies that contribute in detecting Steganography.

There are different methods of doing digital image steganography, the one that is most employed is the least significant bit substitution. This term comes from the numeric significance of bits in a byte. The most significant bit is the one with the highest arithmetic value while the lowest one is the reverse of this.

An example perfect example I found over the internet related to the least significant bit substitution is the following: first imagine hiding the character G across eight bytes of a carrier file:

10010101 00001101 11001001 10010110

00001111 11001011 10011111 00010000

A 'G' is represented in the American Standard Code for Information Interchange (ASCII) as the binary string 01000111. These eight bits can be "written" to the least significant bit of each of the eight carrier bytes as follows:

10010100 00001101 11001000 10010110

00001110 11001011 10011111 00010001

In the sample above, only half of the least significant bits were actually changed. This makes some sense when one set of zeros and ones are being substituted with another set of zeros and ones.

Least significant bit substitution can be used in RGB color encodings or palette pointers in GIF, coefficients in JPEG images and other picture files. By overwriting these bits the numeric values the byte changes, in a very subtle way which makes it unperceivable. The human senses would not be able to tell the difference between the original medium and the altered one.

Least significant bit substitution is a simple technique in steganography. But the use of it is not necessarily simple it can get really complex. The most simple or naive applicationwould overwrite all the least significant bits with hidden data. Almost all of the steganography applications use an algorithm to randomize the bits on the carrier file. This factor alone makes steganography really hard to detect, because it would look like random noise in the picture.

Another way to camouflage data in a paletted image is to modify the order of the colors in the palette or use the least significant bit encoding on the colors instead of on the image data. This techniques are really weak, however many applications for graphics order the palette colors by luminance, frequency , or other parameter and a randomly ordered palette stands out under statistical analysis.

PROBLEM

Steganography is the science of communicating in a way where communication is hidden from others. The event of September 11 caused a lot of discussion regarding as to the use of hidden communication, known as steganography, was being used by Al-Qaida and other terrorist groups. According to nameless “U.S. officials and experts” and “U.S. and foreign officials,” terrorists groups are “hiding maps and photographs of terrorists targets and posting instructions for terrorists activities on sport chat rooms, pornographic bulletin boards and other Web sites”[1]. Te FBI director Freeh tried to convince the United States government that terrorists were using steganography and encryption as a medium to communicate their plans of attack and support their organizations. He also urged law makers to enact stricter Internet usage laws, emphasizing that ignoring the problem would cause harm to the U.S.A.. The world is hastening their efforts to discover viable methods for steganography detection and prevention. In the hope of denying criminal networks the use of the internet as a communications medium. Hoping these actions will help in rendering criminals and terrorists incapable of mounting another attack that would cost more lives.

GOAL

The goal is to statistically analyze the least significant bit(s) of each color dimension of each pixel to look for some kind of a pattern. In the absence of a hidden message this should look like random noise. Addition of a hidden message will affect the entropy of the data. This difference should be detectable by comparing the entropy of unaltered picture files with the entropy of files with embedded steganography. Also I will be using several different statistical attacks and compare them to the entropy results.

RELEVANCE

Steganography made the headlines when the New York Times[2] and USA Today [1] published articles on terrorists using steganography for covert communications. The New York Times published articles regarding the French defense ministry, which then reported that terrorists could be using steganography to communicate their plans to blow up the U.S. Embassy in Paris [2]. *"The terrorists were under instruction that all their communications were to be made through pictures posted on the Internet, the defense official said."* Using steganography for malicious purposes has become a threat not only to individuals and businesses, but also to democratic governments.

Steganography and cryptography are technologies that can be used for secret and secure communications. Hypertext markup language (HTML) and the World Wide Web are technologies that can be used for open communications. When combined, steganography, cryptography, HTML and the Web can be very effective tools for covert communications among terrorist groups, drug traffickers and other nefarious groups. They can use the Internet as their global network to communicate and "hide information in plain sight" of law enforcement agencies.

The "Search for International Terrorist Entities" (SITE) Institute shows evidence that terrorists make effective use of the Web in their propaganda, recruitment, and fund raising efforts[8]. It is common knowledge that terrorist websites frequently publish and disseminate information in anonymity, and using various groupings. They could also be using the Web for covert communication. This would make it more difficult for law enforcement agencies to discover and intercept convert communications.

APPROACH

The work plan would beto hide messages like: pictures, text messages and other types of files. Given the proliferation of digital images, and the high degree of redundancy present in a digital representation of an image (despite compression), there has been and increased interests in using digital images as cover-objects for the purpose of steganography. There should be noted that there has been much work on embedding techniques which make use of the transform domain or more specifically JPEG images due to their wide popularity.

Different open source programs, which use different methods of steganography, will be used to hide messages and files into pictures. The data from the pictures, with hidden messages, will be imported to a statistics program like R language, StegSecret, Vsl Studio, etc. There will be a two part analysis, first the less significant bit portion of the pictures will be analyzed and compared with the original picture, and second the pictures will be analyzed and compared in terms of statistical attacks.

RESOURCES

For this project I will need mid range computer, that can process the data from the different open source programs, which are readily available,and will be using for the project. Some of these programs are:

- **Hide Seek:**these are two programs.Hide produces a file called outfile.gif, so the original gif is left untouched. Seek produces a file called whatever you tell it to, via the name you choose for <outfile.ext>. It works by using the Least Significant Bit of each pixel to encode. Also it uses dispersion to spread the data (and thus the picture quality degradation) out a bit throughout the image in a pseudo-random fashion
- **JP Hide Seek:** these are also two programs JPHIDE.EXE is a DOS program to hide a data file in a jpeg file. JPSEEK.EXE is a DOS

program to recover a file hidden with JPHIDE.EXE.

- **StegDetect:**is an automated tool for detecting steganographic content in images developed by Niels Provos. It is capable of detecting several different steganographic methods to embed hidden information in JEPG images. Currently, the detectable schemes are:jsteg,jphide, invisible secrets, outguess, F5(header analysis), appendx and camouflage.
- **Stegbreak:** is a tool used to launch dictionary attacks againstJsteg-Sheel, JPhide and Outguess.
- **Hide Reveal:**Composed of a Java steganographic library and GUI to use steganography. Primarily intended for research communities on security and steganography to implement new dissimulation and steganalysis algorithms.
- **StegSecret:**is a steganalysis open source project (GNU/GPL) that makes possible the detection of hidden information in different digital media. StegSecret is a java-based multiplatform steganalysis tool that allows the detection of hidden information by using the most known steganographic methods. It detects EOF, LSB, DCTs and other techniques.

Also I will use statistical programs and tools to compare and analyze my results some of these programs are:

- **Steganography Studio:**Steganography Studio software is a tool to learn, use and analyze key steganographic algorithms.It implements several algorithms highly configurable with a variety of filters. Also implements image analysis algorithms for the detection of hidden information. This software is developed in Java, allowing use in any operating system.
- **R Language:**R is a free software environment for statistical computing and graphics. It compiles and runs on a wide variety of UNIX platforms, Windows and MacOS.
- **VSL studio:**VSL is free image steganography and steganalysis software in form of graphical block diagramming tool. It allows complex using, testing and adjusting different steganographic techniques and provides simple GUI along with modular, plug-in architecture

It is important to have access to specialized books, which can be acquired online or at the university library. Lastly professor guidance will be needed, in regards to questions about some of the programs, tools, and the subject in general. I already talked to Dr. Duffany which recommended some of the tools and is an expert on R Language. Also Dr. Alfredo Cruz is guiding me through the process of developing the needed literature for the project.

STATISTICAL STEGANALYSIS

The ideal of a perfectly secure steganography is that, that the presence of hidden message should be perceptually and statistically invisible. Since embedding a secret message in a cover media needs modification of cover, steganography inevitably leaves some traces in statistical properties of the medium [4]. This encourages an eavesdropper to discover distortions in statistical properties of the cover signal, through statistical steganalysis, to detect whether it contains hidden data [5].

Recently, there have been powerful statistical techniques reported in literature. Westfeld and Pfitzmann presented a method for analysis of LSB embedding based on a definition of Pairs of Values. This principled methods provides reliable results for known placement of the message embedding and sates, if the message is scattered randomly within the cover its length is comparable to that of the cover's LSB array.

A more accurate technique was reported by Jessica Fridich and R Du which they published in October 2001. It is known as RS attack or "Reliable Detection of LSB Steganography in Grayscale and color images". The algorithm they use is very precise for the detection of pseudo-aleatory LSB steganography. Its precision varies with the image but, its referential value is 0.005 bits by pixel or .5% of the space the information occupies. In other words if the hidden information exceeds the 0.005 bits per pixel, the algorithm will detect it and give an estimate of the size.

ATTACK TESTING

It is necessary to test the attacks such that we can be confident that they are working as expected. It can be a little subjective when testing steganalytical functions and therefore a little a little harder to test. However, through the research carried out we can run sufficient tests to see that they are behaving as expected. This part discusses the testing methodology that was carried out for each of the functions that comprise the system.

Chi-Squared Attack

Andreas Pfitzmann and Andreas Westfeld[6]created a method based on statistical attack called Chi-Squared which analysisthe Pair of Valuesthat are exchanged during sequential embedding. They claim that the LSB in images are not completely random. Rather the frequencies of each of the two pixel values in each PoV tend to be far from the mean. In other words, it is rare that for the frequency of pixel value $2_k$and 2_{k+1} become equal of or near equal Pair of Values in images and bases the probability of embedding on how close to equal the level pixel are and their corresponding odd pixel values are in the test image [7]. This attack works on any sequential embedding. This type of embedding technique makes PoVs in the values we embed in. This will affect the histogram Y of the image's pixel value k, while the sum of $Y_{2i} + Y_{2i+1}$ will remain unchanged. Thus the expected distribution of the sum of adjacent values is 2 and the X^2 value for the difference between distributions with v-1 degrees of freedom is 3, from 2 and 3 we get the X2 statistic for our PoVs as in 4.

The probability of embedding is determined by calculation the p-value 5 for a sample form the values examined, which starts at the beginning of the image and gets increased for each measurement. This attack though, does not work for pseudo-random type of embedding.

Chi-Squared Attack Results

I embedded an image with data and ran some tests using several statistical tools we will first look at the results using the attack known as Chi-Squared Attack.Using the tool known as StegSecret and a specialized tool for Chi-Squared attacks I was able to determine that an image had hidden data when the technique used to embed the data was sequential. The downside to using this type of attack is that is really hard to determine if an image has data embedded if the technique used was aleatory or not sequential. This occurs because the nature of this particular algorithm is to find information that is organized on an unorganized universe.

On the Figures 1 and 2 we have the results of the original image after I applied the steganalysis algorithm. The tool used to run the statistical attack on this picture was the StegSecret tool which detected that everything was normal. This could mean two different things either the image had no data embedded in it or the steganographic method used to hide the data was not sequential. In which case the algorithm saw the picture as it should, which is a lot of pixels without any Pair of Values formed. This is where this type of attack fails; there are methods that can randomly choose the LSB on which the data is going to be hidden. On the other hand having the original image is not necessary to find that it has hidden or embedded data.

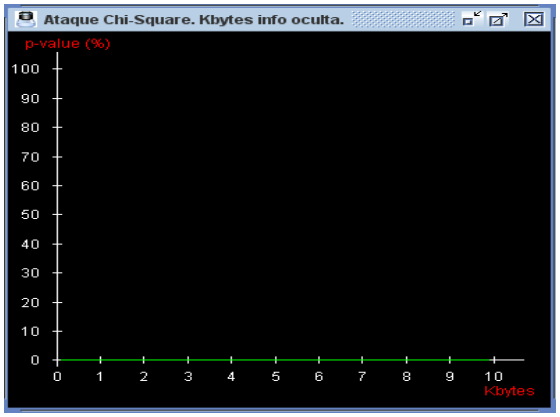


Figure 1
Results of an Image Without any Hidden Information Using StegSecrettoImplement the Chi-Squared Attack

On Figure 2 below a Sequential method was used to embed data onto de digital image. This goes against the nature of digital image LSB which is not completely random. This means that in this picture the 2k and 2k + 1 pixels where found to be equal or nearly equal Pair of values.We can see that the percentage of the PoV's is high. This means there is hidden data embedded on this image.

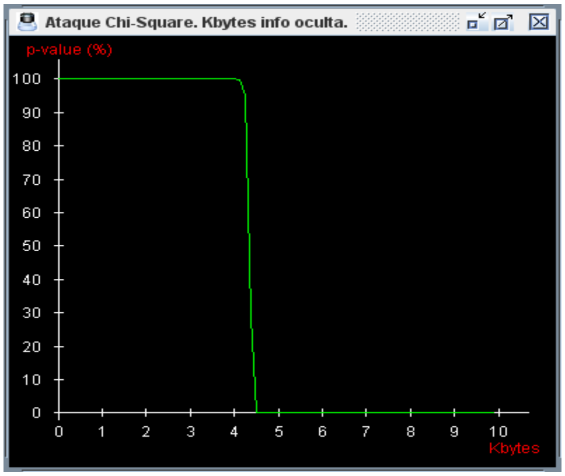


Figure 2
Results of the Same Image with Hidden Information Embedded Using a Sequential Technique

I performed a statistical attack on Figure 3 (a) using a Chi-Squared tool. On this tool instead of only considering the LSB, it also takes into account more bits. Then it checks for the Pair of Values distribution is close to 50/50. So it actually considers 8 bits of each byte, having 256 possible values, and 128 Pairs of Values.

The first step on the process is to calculate the 128 PoV's that we extract from the image by measuring frequency of the Pair of Values. After this is done a table is created by the program. This table is then compared to a second table created by calculating the theorical frequency which is 50% each of the PoV that were already calculated.

The program will output a graph with two curves. The first one in red is the result of the Chi-Squared test. If it is close to one, then the probability for a random embedded message is high. The second output is a simple idea, to add a second layer of verification: it's the average value of the LSBs on the current block of 128 bytes. So, if there is a random message embedded, this green curve will stay at around 0.5. On the graph network, every blue line represents 1 kilobyte of embedded data.

We can see that the red line is practically on top of the 0 which means there are no messages hidden on the image. Also the green line is at 1 which concurs with the first layer of the detection and there is no blue line which means that there is 0 kilobyte of embedded data.

We can see that the red line is practically on top of the 0 which means there are no messages hidden on the image. Also the green line is at 1 which concurs with the first layer of the detection and there is no blue line which means that there is 0 kilobyte of embedded data.

In Figure 3 (b) we have approximately 4 kilobytes of hidden information. The results came out positive the tool detected that there was information embedded, this is represented by the red line which is on top of 1. Also the test detected that there were in fact 4kb of information in the digital image. Lastly the green line is at 0.5 which means there is a random message hidden within the image. On the other hand I embedded the same information of Figure 3 (c) using a non-sequential method. As expected the results were negative there was no data found using the Chi-Squared attack. This proves that although this method is excellent for detecting information inserted using a sequential LSB technique, it has some flaws. As represented by the red line which is in 0, there is no data embedded. There is no blue vertical line covered and this means that there are o kilobytes of hidden information.

RS Attacks

The principle of the RS method is to estimate the four curves of the RS diagram and calculate their intersection using extrapolation. The general shape of the four curves in the diagram varies with the cover-image from almost perfectly linear to curve.Fredich collected experimental evidence that $R_{-M}$and S_{-M}curvesare wellmodeled with straight lines, while the “inner” curves $R_{-M}$and S_{-M}

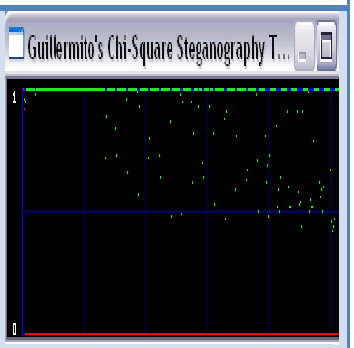
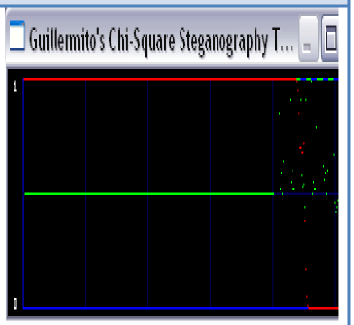
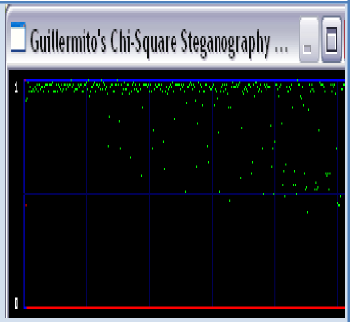
	Hidden	**Graph**
(a)	Nothing	
(b)	4kb of Sequential data	
(c)	4kb of Non-Sequential data	

Figure 3
Comparison between Images of Chi-Squared Attack with Different Kilobytes

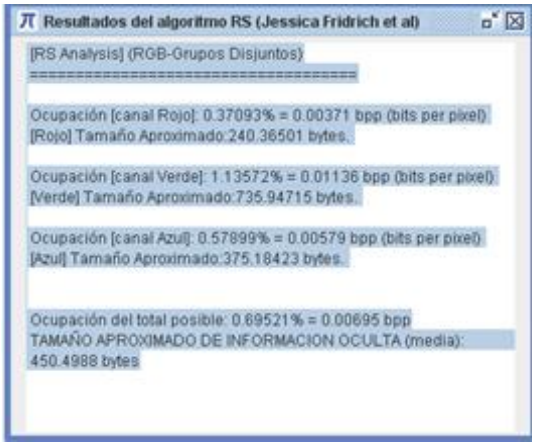
can be reasonably well approximated with second degree polynomials. The parameter of the curves can be determined from the points marked inFigure 6. RS works by partitioning images into groups consisting of n adjacent pixels, and computes the "smoothness" of each group using a discrimination function [8].

Each group is classified as "regular" or "singular" depending on whether the pixel noise within the group is increased or decreased after flipping the LSBs of a fixed set of pixels within each group. The classification is repeated for a dual type of flipping. Some theoretical analysis and some experimentation show that the proportion of regular and singular groups form curves quadratic in the amount of message embedded by the LSB method. Under these assumptions the proportions of regular and singular groups with respect to the standard and dual flipping, sufficient information can be gained to estimate the proportion of an image which data is hidden. The estimates in this method can be extremely accurate, but fails when the assumption does not hold.

Accuracy

Like any other steganalysis attack there are several different factors that can influence the accuracy of their results. First it is important to mention that even original images may indicate a small non-zero message length due to random variations. This could be both positive and negative; it puts a limit on the theoretical accuracy of the RS method. Also very noisy imageshave a difference between the number of regular and singular pixels in the image are small. This causes the lines in the RS diagram to intersect at a small angle which causes the accuracy to decrease. Lastly the message placement has a direct impact on the accuracy. This method is more accurate for messages that are randomly scattered in the stego-image than for messages concentratedin localized areas.

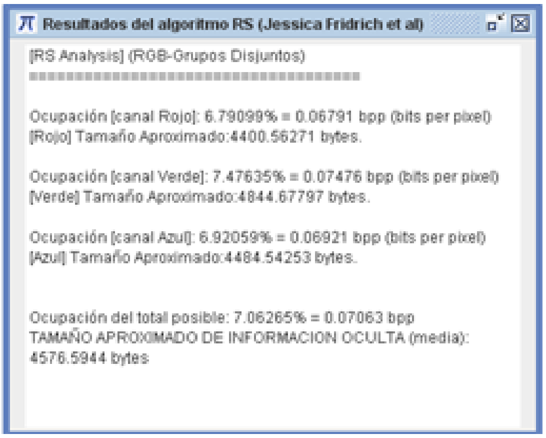
On Figure 4, I used a RS attack on an image that did not contained any hidden information. The percentage was 0.69521 % which means it has given us a false positive which is natural for any kind of test, no test is foolproof. This occurred because the sample reflected the limit for detection on this image. An image free of hidden information is suppose to show a really low percentage which indicates



```
Resultados del algoritmo RS (Jessica Fridrich et al)
[RS Analysis] (RGB-Grupos Disjuntos)
======================================

Ocupación [canal Rojo]: 0.37093% = 0.00371 bpp (bits per pixel)
[Rojo] Tamaño Aproximado:240.36501 bytes.

Ocupación [canal Verde]: 1.13572% = 0.01136 bpp (bits per pixel)
[Verde] Tamaño Aproximado:735.94715 bytes.

Ocupación [canal Azul]: 0.57899% = 0.00579 bpp (bits per pixel)
[Azul] Tamaño Aproximado:375.18423 bytes.


Ocupación del total posible: 0.69521% = 0.00695 bpp
TAMAÑO APROXIMADO DE INFORMACION OCULTA (media):
450.4988 bytes
```

Figure 4
RS Attack Applied to an Image that does not Contain Hidden Data

On Figures 5 and 6 the images had information hidden using sequential and non-sequential techniques. The tests ran on the images can back positive with a high percentage of hidden information on each. This proves that RS method can be used to attack different steganography techniques and can even calculate.

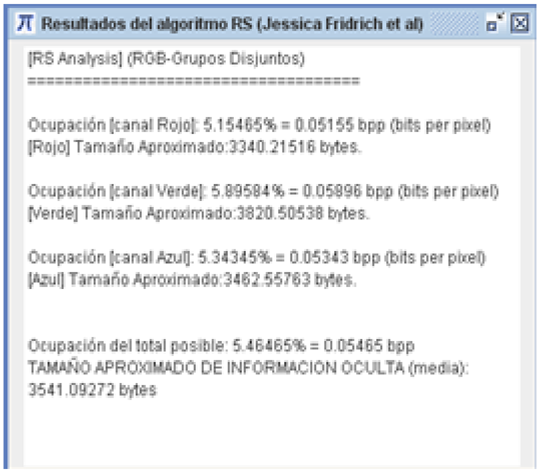


```
Resultados del algoritmo RS (Jessica Fridrich et al)
[RS Analysis] (RGB-Grupos Disjuntos)
======================================

Ocupación [canal Rojo]: 6.79099% = 0.06791 bpp (bits per pixel)
[Rojo] Tamaño Aproximado:4400.56271 bytes.

Ocupación [canal Verde]: 7.47635% = 0.07476 bpp (bits per pixel)
[Verde] Tamaño Aproximado:4844.67797 bytes.

Ocupación [canal Azul]: 6.92059% = 0.06921 bpp (bits per pixel)
[Azul] Tamaño Aproximado:4484.54253 bytes.


Ocupación del total posible: 7.06265% = 0.07063 bpp
TAMAÑO APROXIMADO DE INFORMACION OCULTA (media):
4576.5944 bytes
```

Figure 5
Contains Hidden Data Using a Non-Sequential Technique

Entropy

The entropy is a measure of uncertainty which is associated with variables that are random. This is also referred to as Shannon entropy, which qualifies the expected value of the information contained in a message, usually bits. This is a measure of the average information contentone is missing when compression, under certain constraints, on images. This treats messages to be encoded as a sequence o of independent and identically distributed random variables.



```
Resultados del algoritmo RS (Jessica Fridrich et al)
[RS Analysis] (RGB-Grupos Disjuntos)
======================================

Ocupación [canal Rojo]: 5.15465% = 0.05155 bpp (bits per pixel)
[Rojo] Tamaño Aproximado:3340.21516 bytes.

Ocupación [canal Verde]: 5.89584% = 0.05896 bpp (bits per pixel)
[Verde] Tamaño Aproximado:3820.50538 bytes.

Ocupación [canal Azul]: 5.34345% = 0.05343 bpp (bits per pixel)
[Azul] Tamaño Aproximado:3462.55763 bytes.


Ocupación del total posible: 5.46465% = 0.05465 bpp
TAMAÑO APROXIMADO DE INFORMACION OCULTA (media):
3541.09272 bytes
```

Figure 6
Contains Hidden Data Using a Sequential Embedding Technique

Digital images are co passed of different brightness pixels which occupy different regions of an image. The different pixels show different shapes, and different shapes include different information in the image. Image entropy reflects the information amount of the two-dimensional digital image pixel gray values, and they can be used to describe the pixel gray value information distribution. The difference among the image entropy corresponds to the visual differences among the images. Steganography will change the image pixel distribution probability and color information. The more information is hidden on the file, the greater the change in the entropy on that particular file.

Entropy Attack

Experimental results showed that entropy is a suitable method for discriminating stego-images from suspicions images. It can differentiate stego-images from cover images with a certain rate of success. The problem is that the original image is required for comparison, having the original file is highly improbable when dealing with professional criminals or terrorists. When using the MaxEntropy method in R image which is an extension or package in R Language.

The image was converted into 8 bit grayscale which is required by the method and then the MaxEntropy plugin was used. There are very notable changes and characteristics on the images. Figure 7 is the same test used on a different image. I show the differences in a small part of the image using red circles to mark the spots.

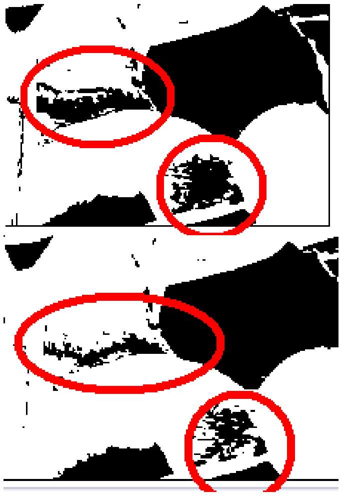


Figure 7
Comparison Between Two Images.
The Left Image has Hidden Information Using a Sequential Technique and the Images on the Right is the Original Image

CONCLUSION

In general, steganographic algorithms have determined thresholds of detection, in other words if the information is embedded having these algorithms in mind they will not work correctly. In the same way their results can vary depending from image to image. This works this way because even if the image has no hidden information, in some cases, it will return a false positive in the form of a few hundred bytes. On the other hand if we embed verylittle information the algorithms might not detect them and it would not notice a difference between the original image and the altered one. This is not applicable to RS attack.

The Chi-Squared algorithm is excellent for detecting embedded information using LSB sequential techniques. It is even better when you could use different filters to determine where information might be hidden and then apply the Chi-Squared attack to the suspected area. On the contrary the results might vary and it effectively might be lower to what it could be when we have pre-selected areas to work on.

The entropy methods plugins in R language required us to have the original image to compare the change in noise of the images. This puts this method behind the other two because the original image is not always going to be available and even if we acquire the image there is no way to tell if it has been altered which would also change the noise in it.

There is no perfect or magical way to determine if images have hidden information. This is like a cat and mouse game where you can only react to the circumstances. Every day a new method for embedding information is created. This is a continually evolving field as new steganography methods emerge new attacks will have to be developed to counter them. The best way to determine whether an image has hidden data is to use different attacks and techniques on them and working the images out. Also part of the key to a successful analysis is to have an experienced analyst that is consistent with the results uses the right tools and the right interpretation to the results.

REFERENCES

[1] Kelley, J., & TODAY, U. (n.d.). Terror groups hide behind Web encryption. *News, Travel, Weather, Entertainment, Sports, Technology, U.S. & World - USATODAY.com*. Retrieved on April 18, 2012, from

http://www.usatoday.com/life/cyber/tech/2001-02-05-binladen.htm

[2] SITE. (n.d), “The Search for International Terrorist Entities”, http://www.siteinstitute.org/

[3] Future Design of Steganographic Schemes", Lecture Notes in Computer Science, vol.3200, pp. 67-81, 2004.

[4] Saeed R. Khosravirad, TaranehEghlidos, ShahrokhGhaemmaghami, "Higher-order statistical steganalysis of random LSB steganography," aiccsa,

pp.629-632, 2009 IEEE/ACS International Conference on Computer Systems and Applications, 2009.

[5] Westfeld, Andreas and Andreas Pfitzmann. “Attacks on Steganographic Systems: Breaking the Steganographic Utilities EzStego, Jsteg, Steganos, and S-Tools–and Some Lessons Learned.” 3rd International Workshop on Information Hiding (2000).

[6] J. Fridrich. "Feature-Based Steganalysis for JPEG Images and Its Implications for Future Design of Steganographic Schemes” , Lecture Notes in Computer Science, Vol. 3200, pp. 67-81, 2004.

[7] Jessica Fridrich, MiroslavGoljan, Rui Du, "Detecting LSB Steganography in Color and Gray-Scale Images," *IEEE Multimedia*, vol. 8, no. 4, pp. 22-28, Oct.-Dec. 2001, doi:10.1109/93.959097.

[8] Abbas Cheddad, Joan Condell, Kevin Curran, Paul McKevitt, “Biometric Inspired Digital Image Steganography”, ecbs, pp. 159-168, 15th Annual IEEE International Conference and Workshop on the Engineering of Computer Based Systems (ecbs 2008), 2008.