



Steganography: Information Technology in the Service of Jihad

Rebecca Givner-Forbes

A Report For:

The International Centre for Political Violence and
Terrorism Research

A Centre of the S. Rajaratnam School of International
Studies, Nanyang Technological University, Singapore

Title	“Secret Information: Hide Secrets Inside of Pictures,” <i>The Technical Mujahid</i> , Issue 2, Safar, 1428 h. (March 2007) pp. 1-18
Author	Authorship Unknown. Published by the Al-Fajr Center for Media
Date	March 13, 2007
Source	Accessed from the “Ansar al-Jihad” mailing group.
Description of Source	This mailing group sends Jihadist publications and propaganda to anyone who signs up on their website: http://www.ansar-jihad.net/ . “Ansar al-Jihad,” is Arabic for “Supporters of the Jihad.”
Reference Available	<input type="checkbox"/> Summary Only <input type="checkbox"/> Excerpt Only <input type="checkbox"/> Partial Translation <input checked="" type="checkbox"/> Full Translation

Summary This article provides an introduction to steganography – or the concealment of data inside image or audio files - and issues associated with using steganography programs. The inclusion of this article in the pro-Jihadist “Technical Mujahid” magazine means that this information is provided overtly for the benefit of Jihadists.

Significance

- Prior to the appearance of this document, steganography was not believed to be widely used among Jihadists and their supporters. Some usage of these technologies by Jihadists had been observed in the mid 1990’s, but in recent years no data suggested that this community was taking advantage of steganography. While the appearance of this article does not mean that this has suddenly changed, it may indicate emerging interest in this technique and could foreshadow an upcoming increase in its use.
- The unknown author provides ample evidence of his own thorough understanding of the mathematics underpinning steganography as well as the issues associated with its use. He wisely avoids endorsing any particular steganography software – as steganalysis software could be quickly developed to counter any program known to be in use by Jihadists. Instead, he provides instruction on testing steganography programs for their effectiveness before using them, allowing the individual user to ensure the soundness of a particular program before using it. In this way, the author provides his Jihadist target audience with information that can help them use steganography effectively without giving away information that could help governments thwart this use.
- The article is not so detailed so that an amateur could use it as a complete how-to guide for steganography. However, it does bring up the most important points and considerations for someone exploring the potential use of these technologies.

Full Translation:

Secret Communications: Hide Secrets Inside of Pictures



[Tr note: The truncated Arabic text in the upper right-hand corner of this image reads: “a secret message from a secret soldier of al-Qaeda, Rakan Bin...to the General Command in Afghanistan and also to the...in Londonistan...about the operation...to strike nuclear stations...in the following cities that...planning...”]

The thing that scares the American Federal Bureau of Investigations more than anything else is the Mujahideen’s use of secret communication technology known as steganography.

Steganography is hiding information. It is a modern technology to transfer secret information over the Internet, through cell phones, or by way of other media. The science of concealing messages utilizes open, public algorithms to encrypt information and secure private messages. However, there is a point of weakness in this system of concealment, and that is the knowledge that encrypted information is being moved. This in and of itself represents a kind of danger for the person sending the encrypted messages. Because [intelligence] agencies can discern the [origin] of the message, it leads them to follow the person who sent this information.

This is where steganography comes in. It compensates for the weakness of [using only] encryption, because it hides the fact that any secret information is being sent at all. This is because the information is hidden inside of something else, like a picture, or a clip of music, or other [multimedia]...

This lesson is intended to familiarize [the reader] with steganography, as well as the technologies to uncover its use, or what is known as “steganography detection.” It is also intended to provide a warning against certain steganography programs because the truth of them is that they are false programs which no one should use. You may think you have hidden information, when actually this information is very easy to uncover.

In the year 1990, many different technologies began circulating, and a general concern arose regarding the use of steganography with digital technology. Among the first of these technologies was watermarking, which was used to protect the rights of the publisher for many different mediums, including pictures, and to preserve the [copy]rights of the owner. The real objective was to transfer encrypted information disguised in digital carriers [tr. note: “carrier” refers to the file in which secret data is hidden] in order to hide the fact that any information was being sent at all.

The interest in steganography came from researchers looking at digital symbols and pictures as a good technology to secure information. These technologies evoked fears in many countries that they would be used to transfer information dangerous to public security or national interest. After the manifestation of these fears, a new field of research opened which looked at how to detect the presence of disguised information. This field of research was called steganalysis.

This field gained strength because of the weakness of the steganography field. But while it grew better at identifying some methods of conveying hidden information, it failed completely elsewhere [because of] the development of other algorithms [for use in steganography]. [This failure] is compounded by the fact that hundreds of millions of pictures are distributed over the Internet, and it is impossible to analyze such a large volume.



[Picture Caption:] Illustration 2: A colored image of Zarqawi with the picture of the primary colors (RGB) which compose it. The original photo was in grayscale, and made up of 256 colors for every one. After blending [the original grayscale image] with several tints you have a colored picture.

1. Modern technologies and a long history

The concealing of information has a long historical connection with espionage and trying to transfer secrets without having them exposed. Secret [invisible] ink was one of the first [methods for doing this]. It initially relied upon the use of onions, before being further developed in the 1950's and 1960's by a chemical engineer who invented a new way to write with [invisible ink] between the lines. The spy would pen an ordinary letter to a friend, but between the lines he would use secret ink to communicate secret information. The ordinary letter would be plainly apparent, but the reader would not be able to see the real message. This secret text could be revealed upon applying a chemical substance to the paper.

Many people may remember the story of Egyptian intelligence [agent] Rifaat al-Jumain, who Egyptian intelligence recruited and provided with a Jewish name for deployment within the Zionist entity in Occupied Palestine. In the beginning, they trained him to send secret messages by writing letters to his friend in Paris. The [address of his friend] was nothing more than an apartment belonging to Egyptian intelligence in France. After communications technologies advanced, Rifaat was trained to send and receive hidden, wireless messages using morse code. This language was invented by the scientist Morse. This wireless numeric [code] first appeared in 1890. It relied upon encoding letters using only "mark" and "space." Later, this became known as "binary encoding" in digital communications.

2. Information Hiding

If encryption was concerned with protecting the secrecy of information and preventing someone from looking at the contents of a message, then the science of information hiding went one step further, by concealing the transfer of information itself. Encryption allows for the transfer of information, but it is not concerned with whether or not others are aware that an encrypted communication has taken place. The function of information hiding is to move secret information without arousing even the slightest suspicion that a transmission of information has occurred. This is done using digital mediums as cover.

A picture is the most commonly used carrier to transfer information. Bitmap and .Jpeg pictures have been used. Information can be hidden within colored pictures using a number of methods, including LSB modification or interfering with the frequency domain.

In this technology, the LSB is the color of [the smallest] element of the picture (a pixel). This is the smallest component of the picture, and changing it does not impact the appearance of the image because it is just one part in 256 parts of primary colors. The primary colors in a digital picture are red, green, and blue. This means that it is possible to utilize three bits in every pixel consisting of 24 bits.

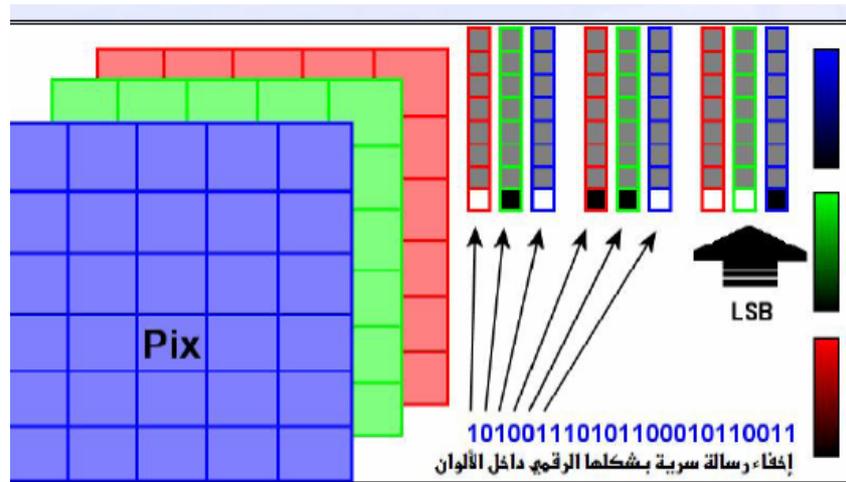
Changing the smallest component in the color involves inserting a kind of “switch” in the picture involving what is known as the signal to noise ratio, or SNR...the change to the picture is not noticeable...

In terms of summarizing [the secret message for transmission], it is necessary to consider the following:

- A) the amount of data involved
- B) the height of the picture
- C) the width of the picture

Keep in mind that [this refers to] the size of the file before compressing it, because if you use data compression, this means that the [original] size is actually a lot larger than what we are counting on here. This means, for instance, that without compression you can hide a message consisting of 300 characters in a picture consisting of 800 pixels by lifting only 1 pixel...Of course, when we compress the message, we can hide a larger amount, even twice as much.

Encryption programs that combine messages and information in this way...include: EzStego, S-Tools, and Hide and Seek. However, it is necessary to distinguish between hiding information in a picture which has not been subjected to compression and a picture which has. Compression can change the pictures and impact image quality.



[Picture Caption]: Illustration 3: Three levels comprise a colored picture, and make apparent the least significant bit (LSB) in every primary color. Every primary color consists of 8 bits. Three bits are entered in each pixel.

The expression “pix” [tr. note: means “pixel”] describes an element of the picture and the expression LSB means “least significant bit.” This picture demonstrates that each colored picture consists of three layers. Each layer describes a primary color (red, green, or blue). Each color consists of 8 bits. With that, you can symbolize 256 layers of primary color. This means that each element (pixel) of the image consists of 24 bits, and can represent 16,777,216 [possible] colors.

3. Digital Fingerprint

A digital fingerprint describes encoding ranging in its length between 128 bits and 512 bits. It verifies that a file is the original copy and has not been manipulated. This fingerprint is used in maintaining passwords inside files. This fingerprint is built upon one-way encryption algorithms. This means that it is not possible to alter the password in the fingerprint, known as a hash algorithm or message digest.



5. Steganalysis

The science of steganalysis assumes a contrary role to steganography. The purpose of steganalysis is to uncover whether specific media (an image, sound file, etc.) is concealing secret information. [The type of] analysis depends upon the type of media. For instance, if a particular image is suspicious, then technologies which handle digital images are used to analyze the (LSB) layers.

If a color image consists of 24 bits, and 3 bits (one bit from each color) arouse suspicion that there may be hidden information, 3 layers can be removed and any changes will be noticeable using statistical analysis against the different areas of the image.

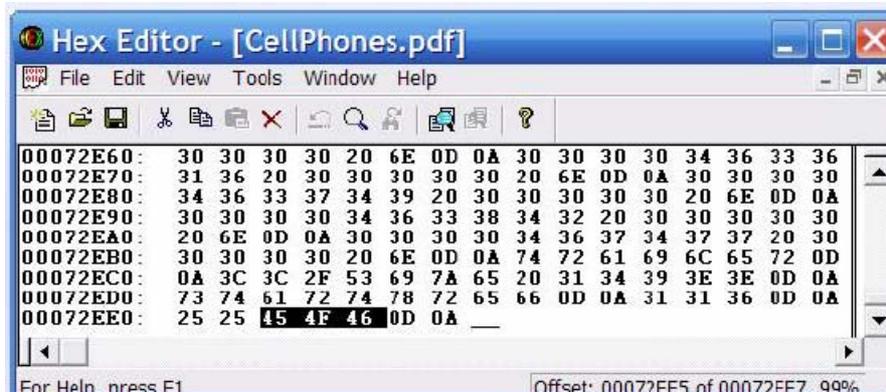
This technology will fail completely if the information is encoded before hiding it, and if it is distributed well within the image.

The kind of image in which it is easiest to detect [hidden] information is a compressed .Jpeg image. This is because the colors are combined using the Discrete Cosine Transform (DCT) method. Any changes to these colors during steganography will leave blanks in the DCT coefficients, and it will thus be easy to detect the presence of hidden information, even if it might not be possible to extract it. In order to reduce the chances that the message will be discovered, some programs exploit just a small number of color layers [rather than all 3], meaning they utilize, for instance, only the red layer.

There are Internet programs which say that they are steganography programs, but which really do not involve any steganography at all. Instead, they are based on manipulation of the beginning and end of a file. In this lesson we will expose one of the most modern of these kinds of programs: Steganography 1.8. We will reveal how it is very easy to uncover what has been hidden [using this program] by simple means...just by opening the file in a hexadecimal editor program and going to the end of the file and looking at the EOF, which is 454F46 in hexadecimal digital language. The original file here is cellphones.pdf



[Picture Caption:] Illustration 5: Steganography program – looks fine but does not work.

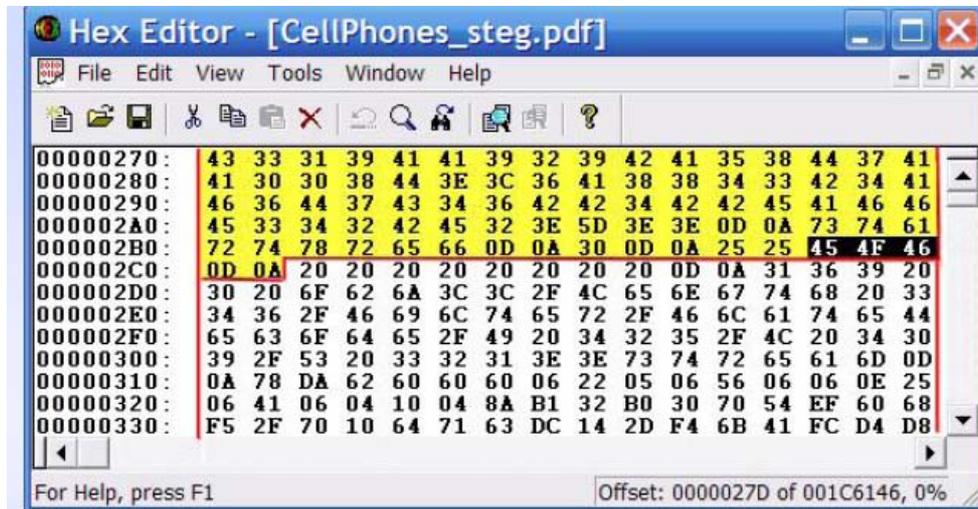


[Picture Caption:] Illustration 4 [sic]: Messages in the carrier file reveal the EOF at the end of the file.

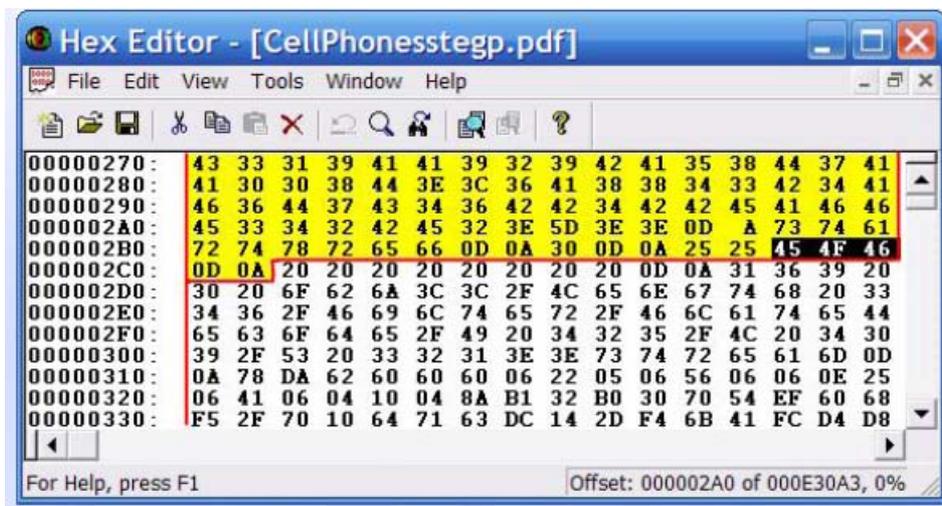
After using Steganography 1.8., we notice that the program did not actually combine the second file into the first file, but instead just stuck it on the end (Concatenation).

The next picture shows this concatenation. The first file, the carrier file, can be seen here in yellow. Beneath it is the file that this program claimed to conceal. In illustration 7, the same file was hidden using a password. A comparison of illustrations 6 and 7 reveals that there is no relationship between the password and the message – the messages in both

pictures are apparent regardless of [the use of] the password [in the second image]. This means, to put it simply, that the program does not encrypt the messages with this password.



[Picture Caption:] Illustration 6: Hiding the file without using the password



[Picture Caption:] Illustration 7: Hiding the file using password protection

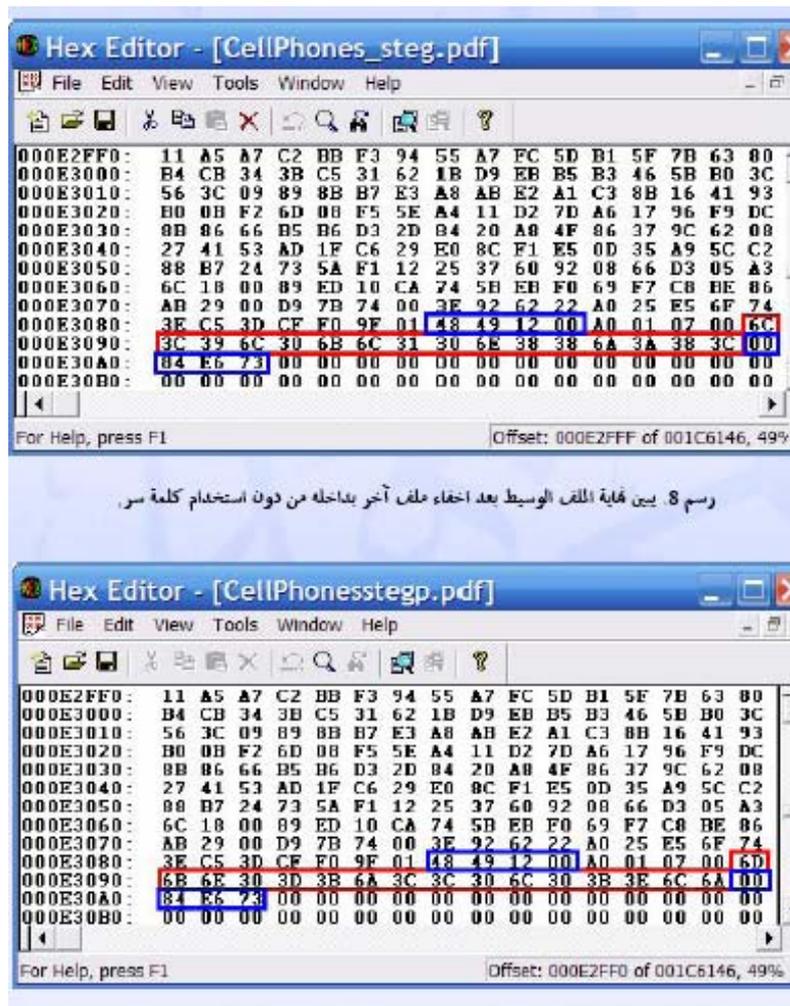
4.1 Uncovering the Secret

We undertook a number of experiments in concealing different files inside other various kinds of files. After opening the “carrier” file (the file in which the other is hidden), with the hexadecimal editor, and going to the end of the file, we noticed that there was a series of 64 bits repeating in all of the files in the portions (0084E673 and 48491200). This is represented in blue in the following picture. These 64 bits are a kind of data which may

indicate the presence of other files hidden inside. This means that the hidden file could be detected.

4.2 Password Encryption and Information

We conducted an experiment in concealing a file inside another file. The first time we did not use any password and the second time we did. The goal here was to reveal whether or not the program could encrypt the information inside (the password protected file) or not.



[Above: Illustration 8 (top) and Illustration 9 (bottom)]

Notice in illustrations 8 and 9 that before the first series in blue there is no difference between the two pictures. However, the first picture represents the hidden file without encoding (without a password) and the second file represents a hidden file with a password. Of course, there is no difference. This means that there is no type of encoding

in concealing. What the program is doing is storing a fingerprint of a password only, which relies on a message digest algorithm consisting of 128 bits (8 x 16 bits). After comparing the file in which a password was used and the file lacking a password, we discovered that the place where the fingerprint of the password was located was in the 128 bites immediately before the cipher: 0084E673.

What this program does is this: when you use the password, it provides a digital fingerprint for the password and is stored inside the file...this means that the program does not actually use protection in hiding the file...

4.3 Uncover hidden information in 3 steps

The following 3 steps reveal how to extract a file which has been concealed inside of another file [in a program which uses concatenation]:

1. Look for the fingerprint 48491200 with 0084E673 at the end of the file. If you find it, this means that the file is concealing another file. This first step is a response to the claim of the [Steganography 1.8] program that it hides information.
2. Substitute the password fingerprint consisting of the 128 bits immediately before the code 0084E673 with this special fingerprint: 6C 3C 39 6C 30 6B 6C 31 30 6E 38 38 6A 3A 38 3C. This erases the password. This step is a response to the claim of the program that it protects messages using a password.
3. Open the carrier file with the program itself and extract the hidden file. This last step reveals that what you thought was hidden and protected is actually easily extractable.

And so here is our response to the manufacturer of this program, who wrote the following sentence about the program: "Make your secrets invisible in just 3 easy steps!" [tr. note: preceding sentence in English].



The sentence above means "make your secrets hidden in 3 easy steps!" We say here that your hidden secrets can also be revealed in 3 easy steps, no matter what kind of encryption is used.

5. The Real Way to Hide Information

In steganography technologies - the carrier file – the picture or the sound file – can accommodate a specific amount of data without any alteration to the size of the file or the nature of the image or sound. Using message encryption before hiding it will amount in total encryption/concealment of the information. This works to thwart steganalysis technologies which rely upon fingerprint analysis or analysis of the image at different

color levels. Additionally, compression technologies for messages allow for increasing the size of the messages or letters that you want to hide. The following example shows the size of the data that can be hidden inside a sample image. The program used here is not known, and the technology used here has not yet been distributed.



Example 1

The picture here has a size of 380 x 512 pixels. Hidden inside of its colors are 200 pages from the Holy Koran. These pages...include more than 240 thousand characters. The encryption algorithm consists of 1024 bits and [the hidden file] is compressed at 330 percent. This concealment does not increase the size of the original picture by one bit. You cannot tell the original picture apart from the picture hiding the messages.

A picture 800 x 700 [pixels] can hide the text of the entire Koran, including the formatting and the page numbers and the numbering of the verses. This picture can also conceal a variety of kinds of files, not only text. For instance, you can hide accounting programs or voice files or images or a number of other kinds of files which you can compress before hiding inside the picture. This can all be accomplished without increasing the size of the original image [file].



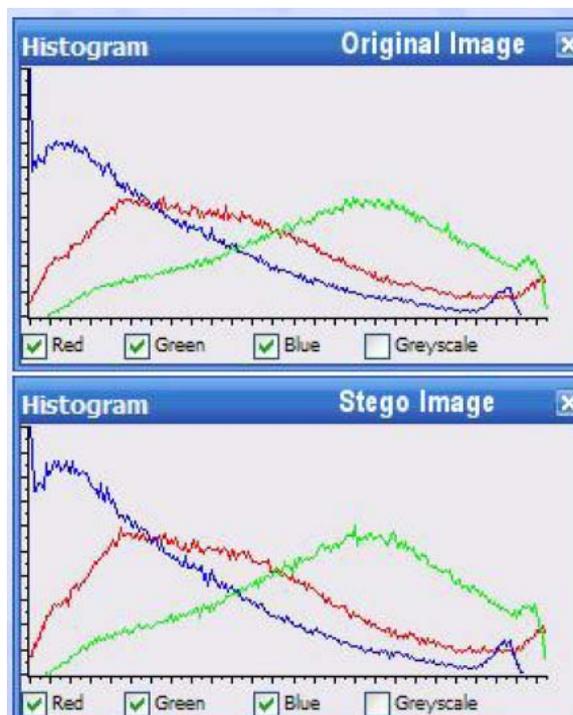
Example 2

The small picture above is 50 x 100 pixels and hides 20 statements from the Islamic Army in Iraq consisting of more than 15 thousand characters (including spaces). In terms of compression, it is at 1000 percent. This is the highest amount of compression possible. It is possible because of what is called “data redundancy.” This means that most of the statements from the Mujahideen have the same information in the beginning and end of the statement, even if the contents of the statement are different. This facilitates greater compression for these statements. It allows for a large amount of messages to be sent using this communication apparatus, including multimedia messages (MMS).

Example 3

[No illustration provided]

The image is 500 pixels wide. By lifting 3 pixels only, you will not arouse any suspicion that there is [a hidden file] present...



[Picture Caption] Illustration 10: Histogram. [A comparison] between the original picture and the same picture containing 240 thousand characters. This change does not impact...the appearance of the picture because the distribution of colors appears natural.

6. How to Choose Carrier Photos

Choosing an image in which to hide information or messages takes some prior analysis of the kind of picture. For a high level of concealment, perform steganalysis on the image prior to using it. We provide here three examples demonstrating how to choose appropriate pictures.

It is necessary here to make a distinction between graphics and photos. The former consists of a limited number of colors and layers of color which are not subject to random distribution. This makes concealing [files] inside of them impossible, because of the ease with which they may be uncovered. However, just because the presence of hidden information is discovered does not mean that it is possible to [access or view] the [encrypted] information. This depends upon the encryption algorithm, the compression, and the concealment. For this reason, do not use western programs because they may be fake, and because they may leave some kind of signature indicating that the image is a carrier altered by some specific program.

6.1 Steganalysis Using Visual and Statistical Analysis

6.1.1. Visual analysis – Example 1

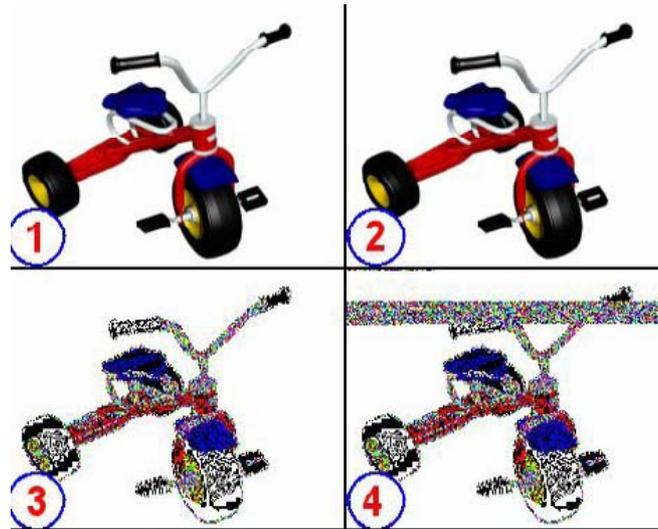
Illustration 11 [referring to picture below]:

Part 1: The original image

Part 2: The image after the concealing of data [within it]

Part 3: A layered analysis of the original image

Part 4: A layered analysis of the image in which information has been concealed. It is possible to see a band of random colors revealing the presence of a hidden message. After arriving at this result, the role of steganalysis ends. The result is that this picture is not appropriate to use as a carrier for concealed [files].



[Picture Caption:] Illustration 11: A (graphics) picture contains a limited number of colors. The hidden message within it can be discovered easily because of the homogeneous [arrangement of colors]. However, [the ability to uncover the fact that there is a hidden message does not equal] the ability to know its contents.

6.1.2. Visual Analysis – Example 2

Illustration 12:

Part 1: The original picture

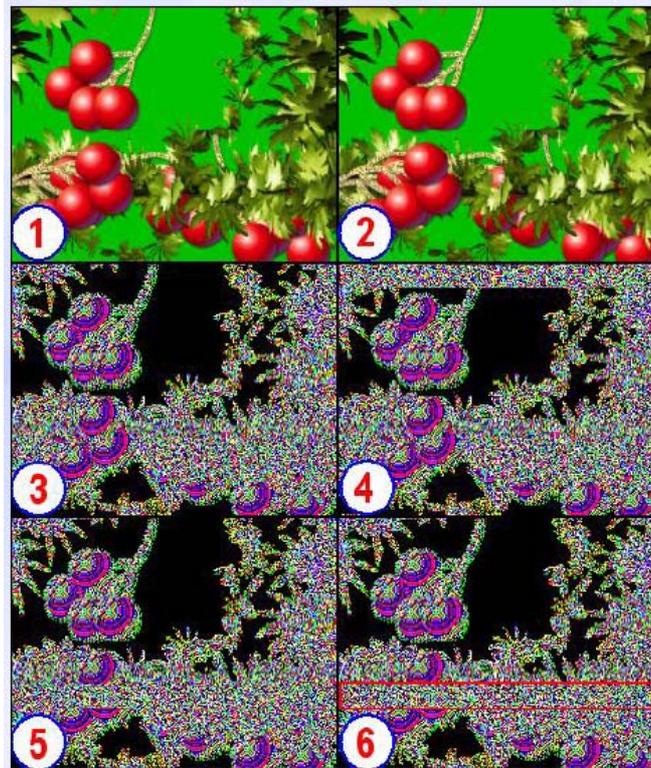
Part 2: The picture containing a secret message

Part 3: A layered analysis of the original picture

Part 4: A layered analysis of the picture carrying the message, a band of random colors can be seen at the top of the picture indicating the presence of a hidden message.

Part 5: After moving the location of the message lower down in the image to an area that also contains random colors. Visual analysis is thwarted by doing this.

Part 6: The same picture as in (5), except we have inserted a band of red color in order to indicate the location of the hidden message.



[Picture Caption:] Illustration 12: Types of graphics can be used to hide messages, but it is necessary to choose their hiding place carefully. Putting the message in the green area which looks black after layered analysis leaves it vulnerable to exposure.

6.1.3: Visual analysis – Example 3

Illustration 13:

Part 1: The original image

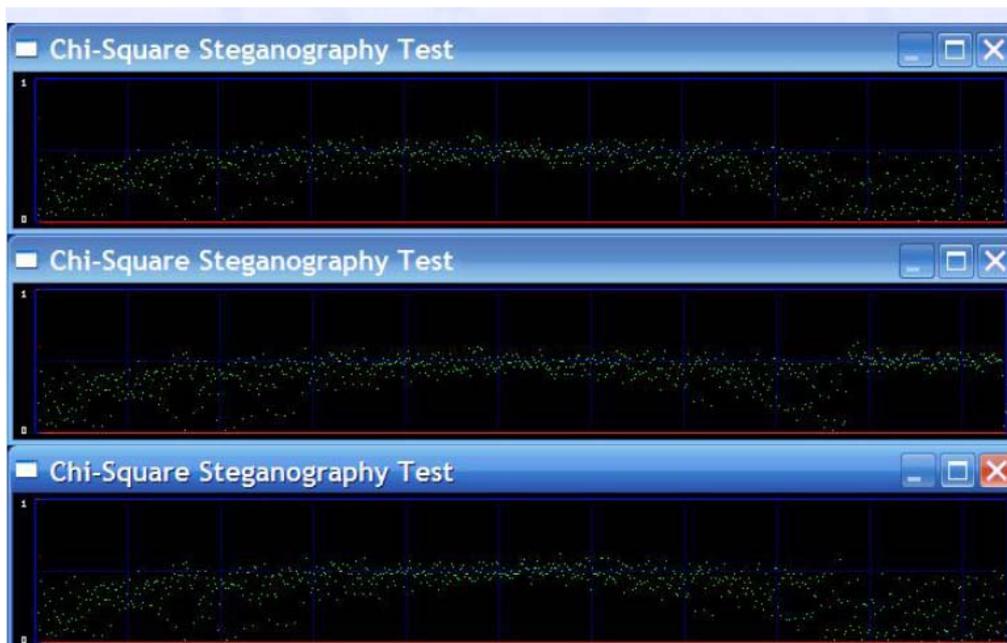
Part 2: The image after hiding a message consisting of 16 thousand characters compressed x 10. This message takes up only 9 percent of this picture, which is 190 x 250 pixels.

Part 3: A layered analysis of the original picture.

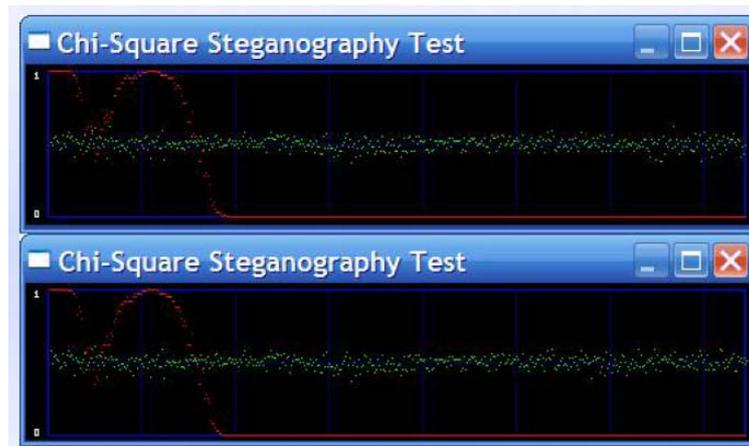
Part 4: A layered analysis of the picture in which the secret message is hidden. Of course, there is no difference between [the pictures in Part 3 and Part 4] using a layered visual analysis. Even if you were to use other analysis technologies [you would not be able to discern the message]. Technology does not exist which can determine the presence of something to 100 percent certainty in these kinds of images. Even if a specialized program were to give an indication that there was something there, it would only suggest the possibility, and [the technology] would be subject to errors [tr. note: errors = false positives]. The kinds of programs that attempt to reveal hidden messages that rely upon looking at possibilities can also yield [false positives] in ordinary pictures. This reduces their usefulness.



[Picture Caption:] Illustration 13: a layered analysis reveals that the picture has a wide variety of colors, and so messages can be hidden inside of it in such a way that a visual layered analysis cannot reveal them. These kinds of pictures are good to use for steganography.



[Picture Caption:] Illustration 14: an example demonstrating the failure of statistical analysis in recognizing 1.6 KBs of encrypted information. Above: Analysis of the picture without any [hidden] data. Below: Analysis of the picture containing hidden data. The analysis here [incorrectly] reads that both pictures contain [hidden] data, which means this analysis will lose its credibility ([this analysis corresponds to] illustration 13).



[Picture Caption:] Illustration 15: Statistical analysis fails completely to reveal the presence of concealed information. The red line at the yellow level shows that the third picture on which statistical analysis has been performed does not contain any hidden data, when in truth both pictures contain 1.6 KBs of encrypted information ([this analysis corresponds to] illustration 12).

7. Conclusion

The battle between steganography and steganalysis is ongoing in the war to move secret information. One side of this battle is represented by secret communications in which information and messages are moved without leaving any trace that a communication occurred. The other side is the attempt to stop this kind of communication. A number of programs are devoted to the former and the majority of them have counter programs that can reveal the possibility of the presence of secret messages.

In many cases, as with regards to the programs that we looked at, programs may falsely claim to conceal information. We have shown how this information can be extracted even if it has...been password protected. This has been our warning not to use programs without performing prior analysis on them.

Advanced steganography programs combine a number of developed technologies to achieve their goal. Such programs compress messages before encrypting them with algorithms consisting of 2048 bits prior to concealing them [in the carrier file]. Some programs hide short messages inside short audio messages, and some utilize a limited number of primary color layers in an attempt to reduce the chances of any change being revealed during a steganalysis process which statistically analyzes colors. Other programs hide messages or statements by utilizing modern technologies from the world of communications engineering. This is what is called “spread spectrum.” It is used to thwart most methods of steganalysis. We have also shown how to choose an appropriate photographic or natural image to counter both visual and statistical analysis. This makes

steganography a worthwhile method for transferring secret information without attracting scrutiny.