Concealing Secret Messages Using Computer Graphics

by Tom Spitzoli

"I always feel like, somebody's watching me." – Rockwell (a singer from the mid '80s), 1984

America today is a voyeuristic society of snoops,
and nothing you ever say or do is completely safe from the prying eyes of others.

America today is a voyeuristic society of snoops, and nothing you ever say or do is completely safe from the prying eyes of others. Motivations for this unsettling behavior can vary tremendously, ranging from simple curiosity and jealousy to flat-out "Friend of the Man" machinations.

To this, the authoritarian types often state, "If you're not doing anything wrong, then you have nothing to worry about." But this convenient rationale is entirely unacceptable, as the pigs often make up the rules as they go along. What's "ok" today may spell bad news for you tomorrow.

Further, many business owners and corporate executives have a legitimate need for secrecy. Product development is an expensive and time-consuming process, and it's only natural that companies would want to shield their knowledge and assets from rivals and would-be copycats.

Authoritarian types often state "If you're not doing anything wrong,
then you have nothing to worry about." But this convenient rationale
is entirely unacceptable, as the pigs often make up the rules as they go along.

Consider also the plight of someone who may have a benign, yet socially unacceptable sexual preference. Many competent individuals have lost their jobs when, through no fault of their own, they

were exposed as being homosexuals or other deviants from the norm. Even if these people successfully litigate to continue employment in their old positions, their reputations are likely tarnished beyond repair, ensuring dead-end assignments and no possibility for advancement.

The Rise of the Internet

Adding to the mix is the fact that a significant number of people now communicate via electronic channels. In particular, the Internet has enabled the average person to send and receive information quickly and inexpensively, combining the power of the telephone with the comprehensiveness of the written word.

Naturally, email traffic is rife with eavesdropping.

The FBI, in particular, has gained notoriety with the use of their “Carnivore” system, designed to spy on selected Internet targets. Assistant Director John Collingwood has stated that “Carnivore does not snoop through every Internet communication,” adding that a court order is required to begin surveillance. But the reality is quite likely different. The FBI is, after all, the organization that routinely violates its own charter by operating overseas. No worries, though: They can do this without fear of repercussion because they're a large governmental agency.

Another biggie is the National Security Agency, or NSA, whose predecessor monitored substantial, if not every, international telegraph communiqué in the 1930s and '40s. They did this with the full cooperation of the three primary civilian telegraph companies of the time, including Western Union, even though this activity was *completely illegal*. Knowing how much easier it is to have modern computers scan emails today than it was to have humans read telegraph messages back then, it's not hard to imagine what the NSA might be doing now, legal or not. After all, the Internet is essentially just a branch off of the existing long distance telcos, and who'll deny that AT&T and their friends are buddy buddy with the Man? History does repeat itself. Is it any surprise that the majority of Internet trunk carriers are headquartered in, or have a major presence in suburban D.C.?

Finally, even if you've been fortunate enough to avoid the overshadowing specter of *official* surveillance, what's to say that *private individuals* aren't taking a gander at your correspondence? Packet sniffers allow anyone “upwind” of you to monitor your Internet traffic, and the current popularity of cable modems destroys privacy as well. Basically, the Internet is one huge party line, and you depend on the honor of others to ensure the integrity of your information. Criminey!

Fighting Back

So now that we've established that complete strangers are indeed reading your email, what can be done about it? Certainly, communication via telephone and postal mail is just as susceptible to compromise. Are there no other avenues? Should you give up hope entirely?

Many people have chosen to *encrypt* their transmissions. Encryption scrambles your messages, and then, ideally, only the holder of your unique “key” can decode your transmission upon arrival at the remote end.

Packet sniffers allow anyone “upwind” of you to monitor your Internet traffic, and the current popularity of cable modems destroys privacy as well. Basically, the Internet is one huge party line, and you depend on the honor of others to ensure the integrity of your

information.

One popular encryption package is PGP, or Pretty Good Privacy. In 1991, the creator of PGP, Phil Zimmermann, became the target of a US Government lawsuit, alleging that he, Zimmermann, illegally exported what amounted to military secrets. This, in an ironic sort of way, was a pretty good indication (pun intended) that PGP was worth its salt. However, the suit was dropped a few years later, and, furthermore, PGP was granted an export license in December of 1999. While good news for Zimmermann, this turn of events surely meant that his trusty PGP had been cracked.

But, maybe encryption isn't the answer, anyway. After all, the best-kept secrets are often those in which it's not apparent that a secret's being held in the first place. When you send an encrypted email, you're essentially saying to the eavesdroppers, “Look at me! I'm sending a secret email, likely full of illegal information or other juicy tidbits. Please pay close attention, and try to decipher it if you can.”

What you really need is something inconspicuous.

A Diamond in the Rough

Thus, this revelation brings us to the ultimate topic of this article, which is hiding secret messages within computer graphics. I'll start with some easy examples of how one might do this, and then I'll provide a few exercises that are a bit more daunting. Hopefully, even if you aren't a programmer or computer fanatic, you should be able to follow along and learn how to apply these techniques to your own situation. The best part of this scheme is that it's *completely legal*. That's right: there's no law against inserting secret messages into computer graphics. So, in summary, you're in the right, and Big Brother can go fuck himself.

When you send an encrypted email, you're essentially saying to the eavesdropper, 'Look at me! I'm sending a secret email, likely full of illegal information or other juicy tidbits. Please pay close attention, and try to decipher it if you can.' What you really need is something inconspicuous.

Now then, here's what you do:

.GIF Comments

We'll start with the .GIF, the predominant image format of the Web. If you're unfamiliar with computer graphics, then you'll need to know that a wide variety of graphical encoding methods exist. That is, you can't simply “save a picture to a file,” the picture must be broken down into its components, and only then can it be made into a permanent disk file. Of course, many programs do this for you behind the scenes, but that's what needs to happen.

Different graphic file formats have their respective strengths and weaknesses. The .GIF is popular because it offers high compression – making for small file sizes and, accordingly, fast downloads – but it can only handle a maximum of 256 colors.

We're not worried about the color limitations. Instead, we care about the .GIF because it allows you to insert comments. Yes, that's right, you can stick any old text message within a .GIF file. This feature was undoubtedly intended for people who wanted to record information about the picture at hand, and not for those who seek to conceal secret messages. Nevertheless, it works for that purpose as well.

If you're not a programmer or graphic artist, then it's likely that you have no way of creating a .GIF file, much less inserting a comment. Rest assured, though, it's very easy. And you don't need to spend a fortune on software. A company called Alchemy Mindworks makes a handy little package called "GIF Construction Set," which makes the process as painless as possible. All you have to do is click on a button to insert a comment, which can even be cut-and-pasted into place.

You can order GIF Construction Set from this URL: www.mindworkshop.com/alchemy/gifcon.html

The price is only $20.00, plus $5.00 shipping. Or, you can forego the shipping if you choose their download option, in which case your registration code will be mailed to you. Finally, Alchemy Mindworks will let you download any of their numerous applications as *shareware*, which basically means, "try before you buy." Unlike other shareware utilities, however, the preview version of GIF Construction Set is fully functional and never expires. Superb!

Now, some people may note that a simple, unencrypted comment within a .GIF file is hardly high security. Any binary editor would easily be able to find the words, as would someone with access to a similar .GIF creation program. But, the secret is that very few people will ever suspect that your .GIF contains a message. After all, a graphic is a picture, not a text file. For added privacy, you could take the additional precaution of encrypting the comment within the .GIF for a double layer of security.

The .GIF comment trick may not fool the NSA, but it'll surely work wonders against the local pigs down at the county, or any of the other agencies that are wont to seize computers at the slightest provocation.

Note also that picture files are *automatically* scrambled to a degree when they're appended to emails as attachments (using base64 encoding, which turns binary files into ASCII text as per the MIME standard). So, your plain-text comments will be jumbled right along with that.

Ultimately, the .GIF comment ruse is a very easy, yet highly effective method of concealing messages.

Directly Editing Windows Bitmaps (.BMP files)

Moving along, the next strategy is even more beautiful than the .GIF comments. Using a binary editor, you can actually alter a bitmap (.BMP) file to contain a text message.

Let's take a moment to discuss why the .BMP file format is ideal for editing. Compressed file formats, such as the .GIF, don't contain straightforward image information. Instead of saying "black dot, black dot, black dot", a .GIF file says, "draw three black dots." The reasoning is simple: In cases when an entire line may be the same color, this saves a lot of space. After all, the .GIF format is designed for quick downloads.

The Windows bitmap (.BMP), on the other hand, contains no compression whatsoever. Every pixel within the image is defined by what is known as an "RGB triplet." As is the norm with computer graphics, every color has three components, red, green, and blue. Black is the absence of all color, and white is all three colors at maximum intensity. (In case you're wondering why all three colors together don't produce mush, the reason is that you're dealing with *light*, not paint. Light has different properties than paint. As you probably remember from kindergarten or independent experimentation, the three primary colors of *paint* are red, blue, and yellow, and together they form a muddy brown. So you really need five basic colors with paint, including black and white.)

Anyway, after you get just a short way into the .BMP file, the "header" information (i.e., basic file layout instruction) ceases, and the rest of the file is comprised entirely of RGB triplets. If you edit one, you simply get another color value, *not* total chaos as you would if you tried this with a .GIF. So, what may look like just a sloppy disarray of colors might actually be an order to buy a stock at a certain price, or to assassinate the Queen.

Now, just to make sure you're with me, I am *not* saying that you should edit your .BMPs with a picture editor such as Windows Paint (commonly found in the Accessories menu). This will only change the colors, and won't allow you to insert a message.

Instead, you'll need a *binary* editor, which will allow you to alter the actual bitwise contents of the file. One such editor is called HEXpert, and it's also available as shareware. You can find it at: www.download.com, and other shareware repositories. In case your conscience is gnawing away at you, the registration price is $20.00, plus $3.00 for shipping. But, as with the GIF Construction Set, the "demo" version is the same as the real thing (albeit with annoying "reminders" advising you to pay).

By using seemingly innocuous computer graphic files to transport messages, you curtail the suspicion that would almost certainly be raised if you used out-and-out encryption.

Note that there may be two programs with the name "hexpert;" one deals with disk access through low-level BIOS calls, and this is *not* what you want.

So, once you have HEXpert (the right one), all you need to do is open your .BMP, select the Edit menu, and then "Toggle Edit Mode". Slide down so that you're safely past the header information (the editing of which really *will* hose your file) and simply type away! It's no more arcane than that.

Once you're finished, just save the file as you would with any other Windows file. Tra-la! You've now successfully encoded a secret message. Obviously, you'll need to make sure that your contact at the other end has access to HEXpert as well.

For fun, you can then look at your .BMP using Windows Paint, Photoshop, or any other image manipulation program. You'll see that your "words" look just like oddly colored pixels. Therefore, to be really suave, select a bitmap that *already* has a jumble of colors before you alter it. Then your edit will fit right in.

Codes Versus Ciphers

My final example today won't use any text at all. Instead, for a virtually unbreakable code, just use colors to represent words.

For a virtually unbreakable code, just use colors to represent words.

In case you didn't know, the difference between codes and ciphers is that a code uses substitution (e.g., "Eagle" = President), whereas a cipher employs some sort of scrambling ("xbPhe53%eW" = marijuana). With enough computing horsepower, you can always unlock a cipher, but unless you have some sort of key, you're doomed against a code.

Therefore, we'll now use a form of encoding in which colors equal pre-selected words. Red could mean "The New York Mets," while blue could stand for "The Chicago Cubs." By pre-arranging what

pixels in a graphic are to be used for inserting codes, you could type messages back and forth all day without raising an iota of suspicion (unless, of course, you're already under surveillance).

Don't worry about running out of colors. Good drawing programs (or even simple ones like Windows Paint) allow you to fine-tune your colors, giving you 256 possible shades *each* of red, green, and blue. That's over 16 *million* colors! (256 x 256 x 256). Do you know 16 million words? Further, even if you're stuck with a low-res monitor, the graphic file will still contain accurate information.

Conclusion

Hopefully, this article has given you some ideas on how to bring some privacy back into your life. By using seemingly innocuous computer graphic files to transport messages, you curtail the suspicion that would almost certainly be raised if you used out-and-out encryption (ala PGP).

One final thought to keep in mind: You might not want to use pornographic images to carry your messages. Not only might these get you in trouble in their own right, but you can expect that any policeman or eavesdropper will hold this sort of thing up to intense scrutiny(!), and will possibly even redistribute the image(s). Instead, use something boring, like pictures of your grandchildren (or substitutes, if you don't have any). This is guaranteed to be “filed” right away, and will likely have a wide range of colors, so that a surreptitious edit won't be evidenced in the least.

Happy editing!