



Compression solutions get better

By Jonathan Hirshon, Consultant, Santa Clara, Calif.

[EE Times](#)

Nov 14, 2000 (10:13 AM)

URL: <http://www.planetanalog.com/showArticle?articleID=12801372>

Security and speed are two major demands of today's Web users. But both are problematic in an increasingly media-rich network environment of streaming video and audio, let alone still images.

An average consumer will experience frustration trying to upload or download images of 15 to 20 Mbytes on a 56-kbit/second modem, yet this is the size of the typical uncompressed TIFF image taken by a digital camera. Without excellent compression of this image, sending that file to a photo finisher for printing (or to your family) from home is an exercise in frustration and severely limits the deployment and usage of digital cameras. In addition, the inherent lack of security of the Web poses a significant concern for many consumers, a fact that challenges the economic viability of e-commerce. Although virtual private networks have made it possible to establish secure extranets, it still does not address the speed and upload/download time issues. These market factors demonstrate the need for a swifter, surer, high-security transmission solution for large graphics and text files.

Content compression can be as simple as removing all extra space characters, inserting a single repeat character to indicate a string of repeated characters or substituting smaller bit strings for frequently occurring characters. This kind of compression can reduce a text file up to 50 percent of its original size. In the more complex image compression, there are two approaches that may be taken: "lossy," where some redundant data is thrown out (ideally not visible to the naked eye), or "lossless." Hard compression of image files is what results in the artifacts, blurring and lack of color fidelity typically seen in Web images as a way to minimize download times. New technology makes this form of hard compression unnecessary, in virtually all cases.

The current standards for image compression on the Web are Graphic Interchange Format (GIF), developed by CompuServe, and Joint Photographic Expert Group (JPEG), an International Standards Organization (ISO) standard based on discrete cosine transform technology that was primarily deployed in the 1980s. The industry is currently evaluating alternatives to GIF for several reasons, including royalty matters surrounding a key patent used in GIF held by Unisys and the format's lack of support for 24-bit color. GIF remains the most popular bit mapped graphics file format on the Web for 8-bit color (256 colors) low-resolution images.

JPEG effectively supports full-color 24-bit images, making it the common standard for compressing photo-quality images on the Web today. The JPEG committee is a group of experts nominated by national standards bodies and major companies working to produce standards for continuous-tone image coding. The "joint" refers to the group's status as a committee working on both ISO and ITU-T standards. (ITU stands for International Telecommunications Union.) The official title of the committee is ISO/IEC JTC1 SC29

Working Group 1; it is responsible for both the JPEG and JBIG (Joint Bi-level Image experts Group) standards. The DCT algorithm used in JPEG divides an image into a matrix and further subdivides each frame in the matrix into smaller grids. From there, color, shading and background imagery are compared across the matrices for similarities. Once determined, the redundant information is noted in a form of "digital shorthand" or thrown out, depending on the form of compression used.

Wavelets ahead

The new JPEG 2000 algorithm-scheduled for deployment in 2001-is based on wavelets, a newer and more robust compression algorithm than DCT. Data on JPEG 2000 (and the original JPEG algorithm) may be found at www.jpeg.org/JPEG2000.htm.

Although wavelets offer an effective image-compression solution for the future, first-generation wavelet compression algorithms tend to demonstrate the "fuzzy windowpane" effect in hard lossy compression of images. This is a form of compression artifact similar to the "stair stepping" found in DCT-based compression algorithms such as JPEG. Newer implementations of wavelet-based compression avoid this.

Another image-compression solution currently under development is Portable Network Graphics (PNG). It was designed to replace the older and simpler GIF format and, to some extent, the much more complex TIFF format. The following description is adapted from the excellent resource on PNG, found at www.freesoftware.com/pub/png/.

For the Web, PNG has three main advantages over GIF: alpha channels (variable transparency), gamma correction (cross-platform control of image brightness) and two-dimensional interlacing, a method of progressive display. PNG also compresses better than GIF in almost every case, but the difference is generally only around 5 percent to 25 percent, not a large enough factor to encourage folks to switch on that basis alone. One GIF feature that PNG does not try to reproduce is multiple-image support, especially animations; PNG is intended to be a single-image format only.

For both professional and consumer image editing, PNG provides a useful format for the storage of intermediate stages of editing. Since PNG's compression is fully lossless-and since it supports up to 48-bit true color or 16-bit gray scale, saving, restoring and resaving an image will not degrade its quality, unlike standard JPEG, even at its highest quality settings.

And unlike TIFF, the PNG specification leaves no room for implementers to pick and choose what features they'll support; the result is that a PNG image saved in one application is readable in any other application that supports PNG. Keep in mind, for transmission of finished true color images-especially photographic ones-JPEG is almost always a better choice.

Although JPEG's lossy compression can introduce visible artifacts, these can be minimized and the savings in file size-even at high quality levels-is much better than is generally possible with a lossless format such as PNG.

However, a new compression algorithm, XCS, developed and extended by FileFlow Inc., compares favorably with JPEG, JPEG 2000 and PNG. XSC, through its use of wavelet-based subband coding, yields dramatically smaller (two to 10 times) file sizes than the equivalent JPEG file with the same visual quality. XSC was developed over a 10-year period at the Norwegian University of Science and Technology in Trondheim, as well as the University of Washington. The various elements of the image-compression

algorithms are jointly optimized to maximize the rate distortion performance while minimizing the memory usage and complexity.

While JPEG 2000 uses a similar technique, XSC uses a unique media-type optimized resource exchange-an intelligent algorithm for determining whether files are in lossy or lossless compression. This has a significant and positive impact on the final quality of the compressed file. As implemented by FileFlow, XCS is very compact and also highly portable. This makes it an attractive component for the rapidly expanding digital consumer market, with upside potential for implementation in everything from handheld computers to next-generation convergence devices. To truly compare the speed or download times of different file formats, the modem speed and quality have to remain the same.

Encryption is a key element that has been underutilized in compression algorithms for the Web. One of the attractive aspects of XSC is that in FileFlow's implementation, it uses strong cryptography to ensure the secrecy and integrity of transferred information. Encryption is supported as a layer between the message layer and the TCP layer provided by the platform. The encryption algorithm used is RC4, with an encryption key size of up to 2,048 bits (military-grade). In XSC, the algorithm is a stream cipher producing a stream of encryption bytes.

A message is encrypted by computing the bit-wise exclusive of the message bytes and the encryption bytes. An encrypted message is decrypted by performing a similar bit-wise exclusive on the recipient side. Two instances of the algorithm are needed in the file transfer, one for encryption and another for decryption. The encryption algorithm is initialized before the first byte of the transfer protocol is transferred.

Two keys are required in encryption and decryption. They are encoded as a string of hexadecimal digits when transferred from the server to the client. Keys can have as many as 256 bytes, but no fewer than 64 bytes, at least for a high degree of security. FileFlow uses 256 bytes in all transferred files. The server connects keys A and B, which must have equal lengths, by appending them. The result is a byte string encoded with two hexadecimal digits that represent each byte in the string. The string "01" is added as a prefix to the resulting string.

This prefix serves as an algorithm identifier in case the encryption algorithm is altered in a later protocol version. The resulting ASCII string is sent to the client in the key parameter. The server must guarantee that Key A and Key B are independent and unpredictable.

In summary, one of the keys to unlock the vast possibilities ahead for broadband and narrowband is advanced image compression technology. Today's design engineer has a wide range of options to consider and all offer significant and different benefits to the end user. A careful and informed decision can reap significant rewards in products designed for today's-and tomorrow's-market.

[Copyright © 2003 CMP Media, LLC](#) | [Privacy Statement](#)