






S-Tools for Windows



Introduction

-  [An overview of S-Tools](#)
-  [Shareware registration information](#)

How to...

-  [Use the WAV module](#)
-  [Use the BMP module](#)
-  [Use the FDD module](#)

S-Tools for Windows

 Collapse

Introduction

[An introduction to S-Tools](#)



[What is steganography?](#)

[Version information](#)

[Advice for effective use](#)

[Credits](#)

[Shareware registration information](#)



[What is shareware?](#)



How to...

[Use the WAV module](#)

[How do I register S-Tools?](#)



[How it's done](#)

[Advice for effective use](#)

[Command reference](#)

[Use the BMP module](#)



[How it's done](#)



[Advice for effective use](#)

[Command reference](#)

[Use the FDD module](#)



[How it's done](#)

[Advice for effective use](#)

[Command reference](#)

S-Tools for Windows

▼ Expand

Introduction

[An introduction to S-Tools](#)



[What is steganography?](#)

[Version information](#)

[Advice for effective use](#)

[Credits](#)

[Shareware registration information](#)

How to...

[Use the WAV module](#)

[Use the BMP module](#)

[Use the FDD module](#)

S-Tools for Windows

▼ Expand

Introduction

- [An overview of S-Tools](#)
- [Shareware registration information](#)



[What is shareware?](#)

[How do I register S-Tools?](#)

How to...

- [Use the WAV module](#)
- [Use the BMP module](#)
- [Use the FDD module](#)

What Is Steganography ?

Since the advent of computers there has been a vast dissemination of information, some of which needs to be kept private, some of which does not. S-Tools (Steganography Tools) brings you the capability of concealing files within various forms of data. The key to most applications of steganography is digital data, such as a scanned image, or a sampled sound. Most computer data has to be 100% accurate in order to function correctly, but digitally sampled data need not be. By making subtle alterations to sampled data it is possible to conceal information whilst retaining nearly all the content of the original sample.

Users of S-Tools can opt to encrypt their information using the strongest state-of-the-art encryption algorithms currently known within the academic world, so that even an enemy equipped with a copy of S-Tools cannot be completely sure data is hidden unless he has your secret passphrase.

You could use S-Tools to conceal private or confidential information that you don't want to fall into the wrong hands. You could use it to send information to another individual via a broadcast network such as Usenet. By agreeing on a passphrase you can keep the information out of unauthorised hands. Alternatively you could use S-Tools to verify your copyright over an image by storing an encrypted copyright statement in the graphic and extracting it in the event of a dispute.

In short, S-Tools allows you to place private information in an inconspicuous 'envelope' that will not arouse suspicion.

Version Information

S-Tools has been through a number of revisions since its first appearance in mid-1994. This is a brief summary of the changes that have occurred since version 1.

Version 2

BMP & GIF support added.

Much better data hiding. Bits now chosen with a strong random number generator.

Improved user interface.

Version 3

FDD module added.

Help file rewritten in the style of "modern" windows help files.

Secure overwriting of temporary files (3 pass with random data)

Advice For Effective Use

There are a few general tips that, if followed, will maximise the level of security that S-Tools can provide. Firstly, you must assume that any potential enemy has his own copy of S-Tools and is aware that you might be attempting to conceal data. You need to be able to convincingly deny that you are hiding data.

If you always use the encryption options provided by S-Tools, combined with a good passphrase, then it is almost impossible to prove that data is concealed in whatever "wrapper" you have chosen. It is not the same to use a package such as PGP to encrypt your file before hiding it unencrypted by S-Tools. Doing this will leave the length information of the encrypted file visible, meaning that an attacker can extract the file even though he is unlikely to be able to break the encryption algorithms used by PGP. In other words, always use the S-Tools encryption option, even if the files that you are hiding are already encrypted.

Further information, specific to each S-Tools module, is provided in the following help pages:

[Effectively using the WAV module](#)

[Effectively using the BMP module](#)

[Effectively using the FDD module](#)

What Is Shareware ?

Shareware is a form of marketing that does away with the high costs incurred by software houses that need to invest in flashy packaging and expensive advertising. It allows you to try out the software that you want before you commit yourself to buying it. The asking price for shareware, often referred to as the "registration fee" is usually considerably lower than that of commercial software.

How Do I Register S-Tools?

S-Tools is shareware, sort of. Most shareware programs ask that you send off your registration fee after a number of days have elapsed, and reinforce this through messages in the program that bother you every so often, usually when you start up or exit from it. Because of the nature of S-Tools you may not want to tell me that you are using it, in fact you may not want *anyone* to know that you are using it. That's fine by me, I am quite happy if people want to use S-Tools and never contact me at all.

However, if you don't mind writing to me, and you think that S-Tools is worth the asking price of 15 UK pounds then I will send you a printed paper manual, a version of S-Tools that includes the full 'C' source code and you can sleep easy knowing that you have done The Right Thing :-)

The address to send cash (sterling), cheques drawn on a UK bank or travellers cheques is:

Andy Brown
28 Ashburn Drive
Wetherby
West Yorkshire
LS22 5RD
United Kingdom

For e-mail contact information, see [contacting the author](#).

Credits

The algorithm used in the derivation of cryptographic keys and variables is hereby identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm"

IDEA is registered as the international patent WO 91/18459 "Device for Converting a Digital Block and the Use thereof". For commercial use of IDEA, one should contact

ASCOM TECH AG
Freiburgstrasse 370
CH-3018 Bern, Switzerland

The MPJ2 Encryption Algorithm may be used for any legal purpose without payment of royalties to the inventor or his employer. Some nations may restrict the use, publication, or export of strong encryption technology. Comments, questions, and reports of possible weaknesses should be sent to the author at:

Mike Johnson
PO BOX 1151
LONGMONT CO 80502-1151
USA

BBS: 303-938-9654
Internet: mpj@csn.org
CompuServe: 71331,2332

NSEA was proposed to sci.crypt by Peter Gutmann (pgut1@cs.aukuni.ac.nz) as a cipher free from restriction, for all to use. Peter himself admits that it may have "security holes big enough to drive a bus through", but it's here all the same if you want to use it.

A big thanks to all my friends whose attitudes to freedom of expression always seem to push me into action. Notables include Gavin, who thinks everything I do is futile and Larry, who has *the* most cool attitude ever.

Who said cypherpunks don't write code anymore?

S-Tools for Windows

▼ Expand

Introduction

- [An overview of S-Tools](#)
- [Shareware registration information](#)

How to...

- [Use the WAV module](#)



[How it's done](#)

[Advice for effective use](#)

[Command reference](#)

- [Use the BMP module](#)

- [Use the FDD module](#)

Hiding data in WAV files

Sound samples are, by their very nature, inaccurate estimates of the correct value of the sound wave at a particular moment in time. The sound samples in Windows WAV files are stored as either 8 or 16 bit values that eventually get passed to the DA convertor in your sound board. For 8 bit samples this means that the values can range between 0 and 255. 16 bit samples range between 0 and 65535.

All S-Tools does is to distribute the bit-pattern that corresponds to the file that you want to hide across the least significant bits of the sound sample.

For example, suppose that a sound sample had the following eight bytes of information in it somewhere:

132 134 137 141 121 101 74 38

In binary, this is:

10000100 10000110 10001001 10001101 01111001 01100101 01001010 00100110
(LSB of each byte shown in red)

Suppose that we want to hide the binary byte 11010101 (213) inside this sequence. We simply replace the LSB (Least Significant bit) of each sample byte with the corresponding bit from the byte we are trying to hide. So the above sequence will change to:

133 135 136 141 120 101 74 39

In binary, this is:

10000101 10000111 10001000 10001101 01111000 01100101 01001010 00100111

As you can clearly see, the values of the sound samples have changed by, at most, one value either way. This will be inaudible to the human ear, yet we have concealed 8 bits of information within the sample. This is the theory behind how S-Tools does its job. In practice, S-Tools prepends some extra information on to the front of the raw file data. 32 bits of time-dependent random garbage is prepended first. This apparently meaningless step means that two identical hidden files that are encrypted in CBC, or PCBC mode will never encipher to the same ciphertext. Secondly, the 32 bit length of the hidden file is included. This is required for S-Tools to be able to extract the hidden file. Encryption will conceal this value.

In order to further conceal the presence of a file, S-Tools picks its bits from the sample based on the output of a random number generator. This is designed to make life difficult for an attacker who might apply a statistical randomness test to the lower bits of the sample to determine whether encrypted data is hidden there (well-encrypted data shows up as pure white noise). The random number generator used by S-Tools is based on the output of the MD5 message digest algorithm, and is not easily (if at all) defeatable.

FDD module command reference

The File menu



Analyse disk

Fill free space

Hide file

Reveal file

The options menu



Encryption / never



Encryption / prompt

Encryption / always

Encryption / options

Effectively using the WAV module

Choosing a WAV module to hide your data in depends largely on two factors. Firstly ensure that the sample is capable of holding quite a lot more data than you are actually wanting to hide. This ensures that S-Tools has a lot of space in which to distribute its hidden data. The more LSBs that are left untouched by S-Tools the better.

Secondly, try and make sure that the sample you choose comes from a 'real world' source where slight interference and background noise are expected. The samples to avoid are those that come direct from a synthesiser as these are often perfect wave forms where background noise is unusual.

If you follow these two guidelines then you will significantly decrease the chances of your data being discovered by an enemy.

WAV module command reference

The File menu



Open WAV file

Save WAV file as

Hide file

Reveal file

The Options menu



Play



Play original

Encryption / never

Encryption / prompt

Encryption / always

Encryption / options

S-Tools for Windows

▼ Expand

Introduction

- [An overview of S-Tools](#)
- [Shareware registration information](#)

How to...

- [Use the WAV module](#)
- [Use the BMP module](#)
- [Use the FDD module](#)



[How it's done](#)

[Advice for effective use](#)

[Command reference](#)

Effectively using the FDD module

There are a few tips that you might like to take note of when using the FDD module. Generally speaking there isn't much advice you can give, unlike the WAV and BMP modules where the choice of sample or picture can be crucial.

If you want to create a scenario in which you can plausibly deny having any concealed data on your disks then it would make sense to fill the unused space on all your newly formatted disks with random rubbish. That way any concealed data that you do have will appear to be "lost in the noise".

Oh yes, and do remember not to write ordinary files to the disk after you have concealed information on it, there is a good chance that DOS will overwrite your hidden information if you do! Of course, there may come a time when you do want to do this...

Hiding data on floppy disks

S-Tools allows you to hide files in the unused space on floppy disks. But what exactly do we mean by "unused space". Let's take a little look at the way that DOS organises the files on a disk.

Every floppy disk, when formatted, is divided into what are called sectors. Each sector on a disk can hold (usually) 512 bytes of information. So, on a 1.44Mb disk there are $1440 \times 1024 / 512 = 2880$ sectors. When you write a file on to disk, DOS computes how many sectors it will need to hold the file and writes this information into a special area at the start of the disk known as the file allocation table (FAT).

S-Tools FDD module works by looking at the FAT to decide which disk sectors have not been used by DOS, and allowing you to hide information in them. S-Tools does not hide information in consecutive sectors on disk, as this would be too easy. Instead it uses a cryptographically strong random number generator to choose which of the free sectors it should use. To further add to the security it also allows you to fill all other unused sectors on the disk with random rubbish to confuse an attacker even more.

Analyse disk

This option displays a usage map of the selected floppy disk and tells you how much information you can hide on it.

After selecting the option you will be asked which disk drive contains the disk that you wish to analyse. S-Tools is capable of working with any capacity of disk that DOS can use (up to a maximum of 1.44Mb), although these days I'd be surprised if anyone is using anything other than the ubiquitous 1.44Mb disks.

When you have selected the disk drive there will be a short pause whilst S-Tools reads and analyses the disk's vital statistics. When this is done the main display will be updated to show the layout of the sectors on the disk. Sectors marked in red are the ones that S-Tools cannot use because DOS has already used them to store files in. The status bar at the bottom of the screen will tell you how much information you can hide on the disk.

Fill free space

This option allows you to fill the unused sectors on a disk with random garbage. This has the effect of masking the presence of any file that you might be subsequently wanting to hide on the disk, although do note that you are automatically asked whether you want to fill the free space after hiding a file.

WARNING! If you fill the free space on a disk, using this option, *after* hiding a file on it then you will lose that file. After hiding a file, S-Tools forgets all about its presence until you subsequently use the reveal operation.

Having said that, the process of filling the free space is easy. Just put the disk in a drive and select this option. You will be asked which drive contains the disk. Finally, you will be asked to enter a line of random garbage text that S-Tools uses to seed the cryptographically strong random number generator that is used to generate the garbage that fills the unused sectors on the disk. Just type as many random keystrokes as you like.

During the operation, S-Tools keeps you informed of the progress in the status bar at the bottom of the screen. If at any time you decide to give up then just press the Escape key.

Hide file

This is the option that you use when you want to hide a file on disk. To hide a file, select the disk that you want to hide it on, and choose the Hide option. If you're not sure whether the disk has enough free space to hold the hidden file then you can use the Analyse disk option to find out.

You are first asked to choose the file that you want to hide, and then the disk drive that contains the disk to hold the hidden file. If you have asked to be prompted for encryption options then you will be asked whether the file should be encrypted before hiding. I strongly recommend the use of encryption even if the file is already encrypted using some other package because the passphrase that you enter is also used to seed the random number generator that is used to choose the sectors that will hold the hidden file.

During the hide operation you will be kept informed of progress through the status bar and the main display. If at any time you feel you want to cancel the operation then just press the Escape key.

Reveal file

This is the option that you should use to reveal a file that has been hidden on a disk. Simply insert the disk into the disk drive and select this option.

You will be asked which drive holds the disk with the hidden information on it, after which S-Tools will go away and examine the disk layout. This will only take a few seconds.

If you have asked to be prompted for encryption options then you will be asked whether the file was encrypted before it was hidden on the disk. If it was, then you must supply the correct passphrase in order to reveal it.

If all goes well then S-Tools will look at the disk and decide whether a file is hidden on it. If there is a hidden file, you are told about its size and are offered the chance to either view it or save it to disk. The internal viewer is not capable of viewing files that are greater than 64K in size, and it would be silly to try to view a file that is not plain text. When you have chosen whether to view or save it, S-Tools will proceed by extracting the hidden file from the disk. You are kept informed about the process through the status bar at the bottom of the screen and may choose to cancel the operation by pressing the Escape key.

Never encrypt data

Selecting this option switches off the encryption options. Files that you hide will not be encrypted. Files that you reveal are assumed to be un-encrypted.

This is not the recommended option at all.

Prompt for encryption options

Selecting this option causes S-Tools to ask you whether you are using encryption whenever you hide or reveal a file.

This is the recommended option if you like being bothered by message boxes.

Always use encryption

Selecting this option causes S-Tools to always encrypt files when you hide them inside graphics. Files that you reveal are also considered to be encrypted.

This is the recommended option.

Encryption options

Firstly I should point out that this option is for users with an advanced knowledge of cryptography only. The default cryptography options selected by S-Tools provide an excellent level of security and should not need to be changed.

You can use this option to choose the cipher type and mode of operation that S-Tools will use when it encrypts and decrypts files that you hide.

The available ciphers are IDEA, DES, 3DES, MPJ2 and NSEA The key lengths provided for MPJ2 are 128, 256, 384 and 512 bits.

The modes of operation supported by S-Tools are ECB, CBC, PCBC, CFB and OFB. S-Tools prepends 32 bits of pseudo-random time-dependent garbage to the front of every file that it hides so that two identical files encrypted in CBC mode will never encrypt to the same ciphertext. OFB and CFB have the interesting property of enciphering the first block identically. This means that you could encipher something in CFB mode and then attempt to decipher in OFB mode. S-Tools would report that there is a hidden file but will then decrypt absolute garbage.

I'm not going to say any more here about these options since the default is just right for those without a knowledge of cryptography, and those with a good enough knowledge won't need any further explanation :)

All of these cryptographic options are saved in the S-TOOLS.INI file in your Windows directory in order to remain the same the next time you run S-Tools.

Open WAV file

This command is used to load a WAV file from disk. This is the option you need to use whether you are about to hide a file in the sound wave or you are about to reveal a hidden file from the wave. You should be familiar with the Windows standard file selection box that appears when you select this option.

Any currently loaded sound wave will be lost if you go through with this option and disregard the warnings that S-Tools will give you.

S-Tools understands a limited subset of the Windows WAV file format. That means that you may come across perfectly good WAV files that S-Tools does not recognise. S-Tools has been written to understand the most commonly used subset of the WAV file format. If do find a WAV file that S-Tools cannot understand then you can send it to me and I will do my best to update S-Tools to understand it.

S-Tools currently understands 8 and 16 bit samples, in mono or stereo. It does not understand extra information in the file, other than the sample data. It will complain if it comes across extraneous information such as cueing marks.

When the new sound wave has been loaded you will be shown a graphical representation of it in the main window, together with some information in the status bar at the bottom. This information will tell you the intended playback frequency of the sample, the number of bits per sample, whether it is a mono or stereo sample and also the maximum size file that you can hide within this sound wave. Do bear this number in mind when you come to choose a file that you want to hide!

Save WAV file as

This option is used to save a WAV file after you have hidden a file inside it. As such, this option will be disabled until you have successfully hidden a file in a wave that has been previously loaded using the Open WAV file option.

If you really are trying to conceal information then it would make good sense to delete the original WAV file after saving the new one. You don't want a potential enemy finding two apparently identical WAV files with slightly different data do you?

Hide file

This option is used to load in and hide a file within the current sound wave that you loaded using the Open WAV file option. The Windows standard file selector will make another appearance for you to use to select the name of the file that you want to hide. The size of this file must be no greater than the maximum size indicated in the status bar. If you are unsure of the size of the file that you wish to hide then you can use the Windows File Manager program to find out.

If you are having trouble fitting the file that you want to hide inside a sound wave then you might like to try compressing it using one of the popular archiving programs such as PKZIP, ARJ or LHarc.

If you have decided to encrypt the files that you hide then you will be required to enter a passphrase that will be used to encrypt the file. This passphrase must be greater than 6 characters long and must be entered identically twice in order to confirm it. The encryption systems offered by S-Tools are cryptographically strong. That means that if you forget your passphrase then neither you, or any organisation or government agency can retrieve the data for you. (I hope!)

If the file was successfully hidden then the wave displayed in the main window will change to a mixture of red and black lines. The red areas indicate where S-Tools modified the wave data to hold the hidden file. The black areas indicate where S-Tools, purely by chance, did not have to modify the original wave in order to store the hidden file.

Reveal file

This option is used to reveal a hidden file from within the current wave form that you loaded using the Open WAV file option. Do note that S-Tools cannot mark the wave form in red and black after you retrieve a WAV file from disk since it has no idea that a hidden file exists within the wave (only you know that), and even if it did it would have no way of knowing how the wave differs from the original.

If you have decided to encrypt files that you are hiding then you will be required to enter the passphrase that you used to encrypt the file when you hid it. Be sure that the encryption options are set to the same as when you encrypted the file.

When you select this option S-Tools try's to figure out whether it is plausible that a file could have been hidden within the sound wave. It could get this wrong. It is possible that S-Tools can tell you that there is a hidden file when there is not. However, S-Tools will never deny that a hidden file exists when one does. This is of course no problem since you know which of your WAV files have hidden files within them, don't you?

After confirming the likelihood of a hidden file, you will be presented with a small dialogue box that you can use to choose whether to extract the hidden file to the screen, where you can view it, or to a disk file. The former option is only suitable when the hidden file consists of text. Non-text files will show up as junk in the viewing window.

Do note that the hidden file remains within the wave form after being extracted. S-Tools has no idea what the original wave form looked like and so it cannot be re-constructed. This doesn't matter though, since you can't hear any difference between the long-forgotten original and the modified wave, can you?

Play

This option plays the sound wave after you have hidden a file inside it. You can use this option to see if you can detect any difference between the original sound wave and the one with a file concealed within it.

You need to have installed a sound driver using the Drivers option of the Windows Control Panel to be able to play a sound wave.

Play original

After hiding a file within a sound wave you will doubtless want to compare the modified wave to the original. This option will play the original sound wave.

You need to have installed a sound driver using the Drivers option of the Windows Control Panel to be able to play a sound wave.

S-Tools for Windows

▼ Expand

Introduction

- [An overview of S-Tools](#)
- [Shareware registration information](#)

How to...

- [Use the WAV module](#)
- [Use the BMP module](#)



[How it's done](#)

[Advice for effective use](#)

[Command reference](#)

- [Use the FDD module](#)

Effectively using the BMP module

When you have created a graphic with a hidden file inside it there are a few things that you should know about it. Since it is acting as a wrapper for other information, you must never convert it to another format that would result in the loss of information. In other words, **never** convert your image to a JPEG. JPEG files achieve their remarkable compression ratios by removing certain information from the image it is compressing. This will result in the loss of your file.

It is also potentially unsafe to convert to another format by loading into a paint package and then saving out again. The paint package may perform some quantization and/or optimization of the image as you load it which will result in the loss of information.

If you are unsure as to the reliability of a converter, simply use it to convert to your chosen format, then convert back again and see if you can successfully extract your file.

You can of, course, use utilities such as uuencode to convert the image to ASCII for transfer by e-mail or Usenet since all information is preserved.

BMP module command reference

The File menu



Open BMP file

Open GIF file

Save as BMP

Save as GIF

Hide file

Reveal file

The Edit menu



Copy

Paste

The Options menu



View altered

View original

Encryption / never



Encryption / prompt

Encryption / always

Encryption / options

Hiding data in pictures

All computer based pictures are composed of an array of dots, called pixels, that make up a very fine grid. Each one of these pixels has its own colour, represented internally as separate quantities of red, green and blue. Within Windows, each of these colour levels may range between 0 (none of the colour) and 255 (a full amount of the colour). A pixel with an RGB value of 0 0 0 is black, and one with a value of 255 255 255 is white.

S-Tools works by 'spreading' the bit-pattern of the file that you want to hide across the least-significant bits (LSB's) of the colour levels in the image.

For a 24 bit image this is simple because 24 bit images are stored internally as RGB triples, and all we need to do is spread our bits and save out the new file. The drawback to this is that 24 bit images are uncommon at the moment, and would therefore attract the attention of those whose attention you are trying to avoid attracting! They are also very large as they contain 3 bytes for every pixel (for a 640x480 image this is $640 \times 480 \times 3 = 921600$ bytes).

It is considerably more difficult to hide anything within a 256 colour image. This is because the image may already have over 200 colours which our meddling will carry to way over the absolute maximum of 256.

Looking at a little theory it is easy to see that an image with 32 or less colours will never exceed 256 colours, no matter how much we meddle with it. To see this, visualise the 3 LSB's of an RGB triple as a 3-bit number. As we pass through it in our hiding process we can change it to any one of 8 possible values, the binary digits from 000 to 111, one of which is the original pattern. If one colour can 'expand' to up to 8 colours, how many distinct colours can we have before we are in danger of exceeding the limit of 256? Simple, $256/8=32$ colours. There is no guarantee that 32 colours is our upper limit for every file that you want to hide though. If you're lucky the file will not change a colour to all of its 8 possible combinations and then we are able to keep one more of the original colours. In practice, however, you will often find pictures being reduced to the minimum of 32 colours.

S-Tools tries to reduce the number of image colours in a manner that preserves as much of the image detail as possible. It usually makes a very good job too, I can often not tell the difference between a 256 colour scanned image and one reduced to 32. The caveat is speed. Highly accurate colour quantization takes time -- Anybody wanna give me a DEC Alpha? No? Didn't think so.

S-Tools prepends some extra information on to the front of the raw file data before hiding. 32 bits of time-dependent random garbage is prepended first. This apparently meaningless step means that two identical hidden files that are encrypted in CBC or PCBC mode will never encipher to the same ciphertext. Secondly, the 32 bit length of the hidden file is included. This is required for S-Tools to be able to extract the hidden file. Encryption will conceal this value.

In order to further conceal the presence of a file, S-Tools picks its bits from the image based on the output of a random number generator. This is designed to defeat an attacker who might apply a statistical randomness test to the lower bits of the image to determine whether encrypted data is hidden there (well-encrypted data shows up as pure white noise). The random number generator used by S-Tools is based on the output of the MD5 message digest algorithm, and is not easily (if at all) defeatable.

Open BMP file

This option allows you to load a new Windows bitmap (BMP) file into S-Tools. This file may be either a 'clean' one that you wish to conceal some information inside, or it may already contain some concealed information that you wish to reveal.

If you already have a graphics file in S-Tools that you have hidden information inside, and it has not yet been saved, then you will be offered the chance to save it before proceeding. You should use the Windows standard file selector to choose the name of the BMP file that you wish to load.

S-Tools does not support RLE compressed BMP files. If you have one of these and attempt to load it then you will get an error message, at which point you should run it through a BMP to GIF converter and try again using the Open GIF file option.

Open GIF file

This option allows you to load a new CompuServe GIF file into S-Tools. This file may be either a 'clean' one that you wish to conceal some information inside, or it may already contain some concealed information that you wish to reveal.

If you already have a graphics file in S-Tools that you have hidden information inside, and it has not yet been saved, then you will be offered the chance to save it before proceeding. You should use the Windows standard file selector to choose the name of the GIF file that you wish to load.

The code used to read GIF files is based on the giftppm program, a part of the pbmplus package, and can be quite slow on large files - please be patient.

Save as BMP

This option is used to save a modified graphic file to disk as a Windows BMP file. You will not be able to select this option unless you have previously loaded a graphics file and hidden a file inside it. You should use the Windows standard file selector to choose the name of the file that you want to save it as.

BMP files are always saved in either 24 bit or 256 colour format. If it was loaded as 24 bit, then it will be saved as 24 bit. If it was loaded as 16 or 256 colour and then converted to 24 bit, it will be saved as 24 bit. Otherwise it will be saved with 256 colours.

Save as GIF

This option is used to save a modified graphic file to disk as a CompuServe GIF file. You will not be able to select this option unless you have previously loaded a graphics file and hidden a file inside it, and you selected the colour reduction option when hiding the file. You should use the Windows standard file selector to choose the name of the file that you want to save it as.

The GIF files saved by S-Tools are always 256 colour GIF's, as such you will not be able to select this option if you converted the image to 24 bit when hiding the file.

Hide file

This is the option that you use to conceal a file within the graphic that you loaded with one of the 'Open' options. If you have already hidden a file within the current graphic, and not yet saved it, then you will be given the option to save before continuing.

The Windows standard file selector will appear, with which you should choose the name of the file that you want to hide. If you have chosen to encrypt files that you hide, then you will be prompted for a passphrase that will be used to derive the cryptographic key used to protect your information.

This passphrase must be greater than 6 characters long and must be entered identically twice in order to confirm it. The encryption systems offered by S-Tools are cryptographically strong. That means that if you forget your passphrase then neither you, or any organisation or government agency can retrieve the data for you. (I hope!)

Now the important bit. You need to choose how S-Tools will attempt to hide your file.

Firstly, you can opt to convert the image to 24 bits (if it wasn't already) and hide the file inside it. The advantage of this approach is that the altered image will look absolutely the same as the original to the human eye. There is of course a disadvantage, and that is the size of the 24 bit image. For example, a 640x480 24 bit BMP file is over 900K in size. If size doesn't matter to you (ahem) then fine, use this option.

Most people will want to opt for the second option, which is to reduce the number of colours in the image to a sufficient level such that the file can be hidden without increasing the colour count beyond 256. If you select this option then S-Tools will search for the optimum number of colours that it can keep in the image before hiding the file. The advantage of this method is that you can keep the altered image as a GIF, or 256 colour BMP. The disadvantages are that the number of colours (and hence image definition) is reduced and the reduction process can take quite a while. Whether it is reduced beyond acceptability is your decision. Remember though, if you delete the original graphic then who's to know what it looked like?

During the quantization process a dialogue box keeps you up to date with the progress so far in what can be quite a lengthy operation - anyone want to put the kettle on?

See also:

[Advanced options](#)

Advanced options

Since it is vital that the altered image looks as perfect as possible, I chose to implement the best colour quantization algorithm that I could find, even if it turned out to be slow in operation (you can guess what's coming can't you?).

That algorithm turned out to be the one used in the ppmquant program, a part of the pbmplus graphics toolkit. It is based on a median-cut colourmap generator from Paul Heckbert's paper "Colour Image Quantization for Frame Buffer Display", SIGGRAPH '82 Proceedings, page 297. It is not this algorithm that's slow, it's the mapping of the old image colours to the new ones and that is despite my use of colour hash-tables everywhere possible (before I put the hash tables in it was really excruciating). You aren't likely to understand two of these options if you haven't seen the algorithm, and my explanations are largely lifted from comments in the source code. Still, this is how you can tune the colourmap generator to your preference:

The 'median cut box colour' governs how a colour is chosen for each 'box' that the algorithm generates. You can choose the centre of the box (ignoring the box structure), the average box colour (recommended by Heckbert), or the average pixels in the box.

The 'dimension choice' allows you to specify how the largest dimension is chosen. Either the range in RGB space can be chosen, or you can compare luminosities.

The 'Dithering' option has nothing to do with the colourmap generator. It is used to dither the image as it is converted to the new colourmap. Selecting this option (recommended) results in a final image with much better definition than without dithering. The drawback is that dithering introduces many more colours into the image than it originally had, and this slows down the mapping of the old colours to the new ones. In my opinion this is a price worth paying for the extra quality.

The two "Next # of colours" options may be used to control the way that S-Tools chooses a number of colours to reduce to. If you select "Try to solve $y=mx+c$ " then S-Tools will treat the last two colour counts that it tried as forming points on a line, and then try to extrapolate that line to find out how many colours it has to reduce to such that the limit of 256 colours is not exceeded. This method seems to work quite well in practice. If you switch this option off then S-Tools will simply pick the number of colours that falls mid-way between the pass/fail limits that it has found so far. If you think you can do better than S-Tools then you can select the "Manual assistance" option and be prompted to enter the number of colours yourself (S-Tools will give you a hint as to the value it would have chosen).

All of these advanced options are saved in the S-TOOLS.INI file in your Windows directory in order to remain the same the next time you run S-Tools.

Reveal file

This option allows you to reveal a file from a graphic that you have loaded into S-Tools.

If you have decided to encrypt files that you are hiding then you will be required to enter the passphrase that you used to encrypt the file when you hid it. Be sure that the encryption options are set to the same as when you encrypted the file.

When you select this option S-Tools try's to figure out whether it is plausible that a file could have been hidden within the graphic. It could get this wrong. It is possible that S-Tools can tell you that there is a hidden file when there is not. However, S-Tools will never deny that a hidden file exists when one does. This is of course no problem since you know which of your graphics files have hidden files within them, don't you?

Do also note that if you are using encryption on your hidden files then S-Tools has no way of knowing whether you entered a correct passphrase and will simply tell you that no file is hidden if you get it wrong.

After confirming the likelihood of a hidden file, you will be presented with a small dialogue box that you can use to choose whether to extract the hidden file to the screen, where you can view it, or to a disk file. The former option is only suitable when the hidden file consists of text and is less than 64K in size. Non-text files will show up as junk in the viewing window.

Do note that the hidden file remains within the graphic after being extracted. S-Tools has no idea what the original graphic looked like and so it cannot be re-constructed.

Copy

This option will copy the altered graphic into the Windows clipboard, from where you can view it or paste it into other applications. You can only copy an altered graphic into the clipboard, not an original one that you have just loaded from disk.

For those that know the difference, the graphic is copied as a DIB (Device Independent Bitmap), not a DDB (Device Dependent Bitmap) so as to preserve all the image information which must be a requirement so as not to lose the hidden file. Microsoft quite correctly state that since the clipboard's DIB capability is quite new, a lot of applications don't yet support it. Then, as if to encourage the status quo, their own freebie Paintbrush program doesn't support it. If it wasn't Microsoft I guess I'd be surprised.

Paste

This option will paste the contents of the Windows clipboard into S-Tools. It acts exactly like any of the 'File, open' options except that the graphic comes from the clipboard, not the disk.

S-Tools knows about both the DIB (Device Independent Bitmap) and DDB (Device Dependent Bitmap) formats and will handle both of them.

View altered

This option will cause S-Tools to display the altered graphic in its window, i.e. the one with a file hidden inside it.

Note: Either my graphics card driver is knackered (quite likely) or there is a bug in the Microsoft DIBAPI library (very likely) that causes palettes to be displayed rather erratically. I note from experiment that a Microsoft-supplied example application exhibits the same strange behaviour, but others such as Corel PhotoPaint do not, so don't panic if things look a little screwy on screen. Try saving and viewing with a DOS based viewer such as Graphics Workshop or Colorview.

BMP View original

This option will cause S-Tools to display the original graphic in its window, i.e. the one without anything hidden inside it.

Note: Either my graphics card driver is knackered (quite likely) or there is a bug in the Microsoft DIBAPI library (very likely) that causes palettes to be displayed rather erratically. I note from experiment that a Microsoft-supplied example application exhibits the same strange behaviour, but others such as Corel PhotoPaint do not, so don't panic if things look a little screwy on screen. Try saving and viewing with a DOS based viewer such as Graphics Workshop or Colorview.

Contacting the author

If you want to contact me, then I can be reached at the snail-mail address given in the [registering S-Tools](#) section of this help file.

I am also contactable via e-mail at a.brown@nexor.co.uk. I encourage and prefer PGP encrypted mail, and you can get my public keys by fingering asb@vulcan.nexor.co.uk. If you're wondering why the host name must be specified as well as the domain, it's because the gateway host at NEXOR resolves finger queries through the X.500 directory rather than the individual user's .plan file. So now you know.

I generally answer e-mail queries on the same day that I receive them, but since I am at work I can only answer personal mail during my lunch hour and after the working day is over.

This cypherpunk lives in Nottingham, England. Maybe I'll see you there.

