

Encrypt-It - Whitepaper.

Introduction

This paper describes the purpose, function, specification and pricing for the software solution **Encrypt-It**.

Encrypt-It is a program that will allow you to encrypt files and store them inside a standard 24 bit Bitmap picture. With the increasing levels of security breaches and computer crime,

Encrypt-It is a program that will prevent hackers, thieves and other less desirable people from finding and accessing sensitive information on PC's, Laptops and servers.

Purpose

Encrypting files prevents both unauthorized and unwanted access to confidential information stored on your computer. **Encrypt-It** takes encryption to the next level, by hiding the encrypted file in a standard bitmap file, using a process that does not alter the appearance of the bitmap in any perceptible manner.

There is no visible indication in the bitmap file that there is any information stored within it. The encrypted data is merged with the picture information in the bitmap in such a way that the colour content of the bitmap will be altered by an amount that is almost invisible to the naked eye and which leaves the bitmap looking as natural as the original. The fact that you even have encrypted files and placed

them inside a bitmap picture will not be known to anyone but yourself and you can safely store any information with the knowledge that only you can access it.

How does Encrypt-It work?

Encrypt-It works in two distinct stages - encrypting the data, and storing that encrypted data in a bitmap. The encryption stage uses the symmetrical encryption algorithm, a proprietary algorithm that is highly secure. The algorithm uses a password of the user's choice to both encrypt and decrypt the data and the password is not stored anywhere. The designers of **Encrypt-It** made a decision that, as the asymmetrical algorithm creates signature information used to identify the public key used to perform the encryption, the presence of this information in the final bitmap would compromise security by identifying the bitmap as containing an encrypted file. Therefore, asymmetrical encryption is not supported by **Encrypt-It**.

Encrypting with Encrypt-It

The file is first combined with a header that contains the following information:

An eight byte signature

The length of the file

The original file name

The file and this header are then encrypted. This means that there is no indication of the presence of the header until decryption occurs. Once the encryption has completed, the resulting data is combined with a 24-character bitmap file in the following manner: Each byte in the encrypted file is stored in an individual pixel in the bitmap in the following manner:

Three bits are stored in the red channel, three bits in the green channel, and two bits in the blue channel. This results in a maximum change in any one of the constituent colours of the bitmap of plus or minus seven. As there are 256 possible combinations of each colour for any pixel, the actual change to the colour as seen in the bitmap is so slight as to be imperceptible.

Decrypting with Encrypt-It

When it comes to decryption, the user enters the password used to encrypt the file. The data is then extracted from the bitmap, and an attempt is made to decrypt the header using the entered password. If this decrypts correctly (Indicated by the 8 byte header being correct), the rest of the file is then decrypted, and the original file name extracted, using the password, and is then available to view or save to disk. There are several important things to note

The password is not stored anywhere in the bitmap - if you lose or forget it, the data cannot be retrieved. When the encrypted data is stored in the bitmap, the only change to the bitmap is a slight alteration of the color of its pixels. As there is no definitive way to say what colour the pixels should be, there is no way for

anyone to ascertain with any degree of certainty that the bitmap actually contains an encrypted file.

There is a limit to the size of a file that can be stored in any given bitmap, the calculation is as follows.

The bitmap must have the following number of pixels in it: The size of the file being encrypted plus 268 bytes for the header. The number of pixels in a given bitmap can be calculated by multiplying its width by its height (these sizes are shown in the dialog box used to select a bitmap).

Only 24 bit bitmaps can be used to store the data, due to the method of combining the encrypted data with the colours of the bitmap. If you select a 16 color or 256-color bitmap, you will be warned, and given the choice of converting it to a 24-bit bitmap during processing. Doing this will result in a bitmap that is larger than the original, but the size increase is caused solely by the conversion to a 24 bit bitmap, storing encrypted data in the bitmap does not alter its size in any way.

JPEG files cannot be used to store data, as they are compressed using what is known as a "lossy algorithm". This means that when the file is saved, information contained in the picture is lost in order to save disk space. The loss of quality of the picture is normally not noticeable to the naked eye, but losing information within the picture would lead to losing information in the encrypted data, which would be disastrous. Only a single file can be stored in a bitmap. Storing another file into the same bitmap will result in the original file information being destroyed. As there is no indication in a bitmap that it contains an encrypted file, you will not be warned that this is happening, so you need to make sure you don't re-use a bitmap that contains important information. If you want to store multiple files in a single bitmap, a good suggestion is to use WinZip (or similar) to contain an archive file of all the files you wish to encrypt, and then encrypt and store this archive in the bitmap.

[Recommended System Specifications](#)

Operating System: Windows 95, 98, NT, 2000 and ME

Systems requirements: Intel Pentium 100 or above

4Mb free space

CD-Rom Drive

32 MB RAM

Frequently Asked Questions

Q: Can any bitmap file be used to store encrypted data?

A: Any 24 bit (16 million colour) bitmap can be used to store encrypted data. The use of 16 colour and 256 colour bitmaps is not supported due to the way stores its data. You can select a 16 or 256 colour bitmap, but it will be converted to a 24 bit bitmap as part of the processing.

Q: What kind of bitmap images work best?

A: Any 24-bit bitmap can be used, however, its best to avoid bitmaps with large areas of solid colour, as slight differences in colours may be visible inside large areas of a solid colour. In general, the best type of bitmap to use is a photograph, as there are many colour variations in even seemingly simple photographs (for example, of the sky).

Q: How secure is **Encrypt-It**?

A: **Encrypt-It** uses an encryption algorithm that has proved to be highly secure. In addition, as the final data is stored in a bitmap, the chances of finding the files that are encrypted and hidden is extremely rare, potential crackers aren't even aware that encrypted data exists on your machine. However, as with all encryption products, the encryption is only as secure as the password you use to encrypt the data with. **So, never write down your passwords!**

Q: What length password should I use?

A: In general, the longer the length of the password, the better (but only if it can be remembered!). It is recommended that you use a password that is at least 6 characters long, and don't use such things as names, places, or words from a dictionary. A good method to use is to take two words from a standard dictionary, and join them with another letter. So, you could choose read and barrel, and a letter such as Z. This would give a final password of readZbarrel (don't use this one yourself!). This type of password is highly resistant to "dictionary" attacks (where the potential cracker uses a dictionary of words to try and break a password).

Q: Are passwords case sensitive?

A: Yes. test, TEST, Test and even TEsT are all considered different passwords.

Q: What is the maximum file size I can encrypt?

A: That depends on the size of the bitmap you want to store the data in. To calculate the maximum size, multiply the width of the bitmap by the height of the bitmap, and subtract 268. This gives the maximum file size that can be stored in this bitmap. As by way of illustration, a bitmap size of 1280 * 960 (a common size for digital cameras) will allow you to store a file approximately 1.2MB in size. For smaller files, a bitmap of 320*240 will allow you to store approximately 80K.

Q: Can I use JPEG files to store data?

A: No. As JPEG files compress their data using what is known as a "lossy" algorithm, they are not compatible with Encrypt-It. You can, however, convert them using a third party utility (such as Microsoft Imaging, or Windows Paint in Windows 98 / 2000) to a 24-bit bitmap and use that.

Q: What happens if I forget my password?

A: If you forget a password, there is nothing you or anyone else (including ourselves) can do to get the data back. **So, don't forget your passwords?**

Q: Can I edit a bitmap that contains encrypted data?

A: There is nothing to prevent you from editing a bitmap that stores encrypted data. The File is exactly the same as any other bitmap - only some of the colours have been changed). However, if you change any of the pixels that are being used to store the data, you will corrupt the data, and won't be able to get it back properly. In general it's best not to edit a bitmap once it has encrypted data stored in it.

Q: How can I tell which of my bitmaps have encrypted data stored in them?

A: You can't. This is why the product is called "**Encrypt-It**" - there is no indication that a bitmap is anything out of the ordinary.

Q: What happens if I store an encrypted file in a bitmap that already contains an encrypted file?

A: The original data will be destroyed without warning. The reason it is impossible to give a warning is that it is impossible to tell that a bitmap contains an encrypted file.

Q: How many files can I store in a bitmap?

A: You can only store a single file in bitmap. However, you can store any file type in the bitmap, so you could use, for example, WinZip to create a zip file containing many documents and encrypt the zip file into the bitmap.

Q: Is it legal?

A: This is a difficult question to answer, the sale of Encrypt-It is not illegal. However, depending on where you live, certain types of material (such as pornographic photographs) are illegal to own and store on your computer, whether encrypted or not. **Encrypt-It** may not alter this position. If your country of residence has laws requiring you to divulge encryption keys if required by a court of law. You may be obliged to inform the court that you have bitmaps that contain encrypted information as it may not be possible for them to discover you have such data without your co-operation. If you are concerned, you should consult a legal advisor.

Please note that using **Encrypt-It to encrypt documents may be illegal in your country of residence and would therefore be in breach of the license agreement.**

Pricing Single User: £49.95

Corporate Pricing:

Upto 10 PC's or Laptops £45.00 each

Upto 25 PC's or Laptops £40.00 each

Upto 50 PC's or Laptops £35.00 each

Upto 100 PC's or Laptops £30.00 each

Over 100 PC's or Laptops. Price on Application

***Computer Communications Limited, 9 Mount Temple,
Romsey, Hampshire, SO51 5UW***

www.ccl.co.uk. tel: 0844 873 2668.