Outguess Rebirth
User Manual

October 17, 2013

Contents

List of Figures

Chapter 1

Introduction

1.1 General remarks

Outguess Rebirth software offers to the user the possibility of hiding data in image files through steganography, in order to transmit data discreetly to a correspondent (for example, exchange of steganographed images by email).
Image Steganography consists in embedding data into an image type file without affecting the original quality.
In order to guarantee a minimum of security, stenography engine works with a symmetric secret key, equivalent to a password. This key will have to be exchanged and known only by the correspondents willing to communicate and shall not be supplied to a third party.
Steganography engine of Outguess Rebirth software is based on the Outguess[1] algorithm, developed by Niels Provos. Outguess Rebirth is compatible only with JPEG images format.

1.2 Required configuration

Outguess Rebirth works on PCs with Microsoft Windows operating system, from the Windows XP version.
For Windows 2000 users (Service Pack 4), the downloading of Microsoft GdiPlus library is required for operating Outguess Rebirth. This library can be downloaded for free from the following link:

http://go.microsoft.com/fwlink/?LinkID=20993

[1] http://www.outguess.org

Chapter 2

Installation

2.1 Downloading

Outguess Rebirth is a free software available in the form of a ZIP archive at the following addressï¿½:

http://www.outguess-rebirth.com

The software does not include an installation program. To install this software, decompress the contents of the archive in a file of your choice.
Once the archive decompressed, copy the license file (license.dat) that you received by email after your registration on the official site.

Chapter 3

Operation

3.1 First launch

When launched for the first time, language used by default is English. To change languages and set software options, please refer to paragraph 4.1. Once the software launched, the main interface appears as shown belowï¿½:

The main interface is made up of several partsï¿½:

- *Event log*ï¿½(1): this window tells the user whether or not the requested operations have been completed successfully. For each operation, a new entry is generated in the log, with an icon telling whether or not the action has been successfully completed. The table below gives the meaning of each icon.

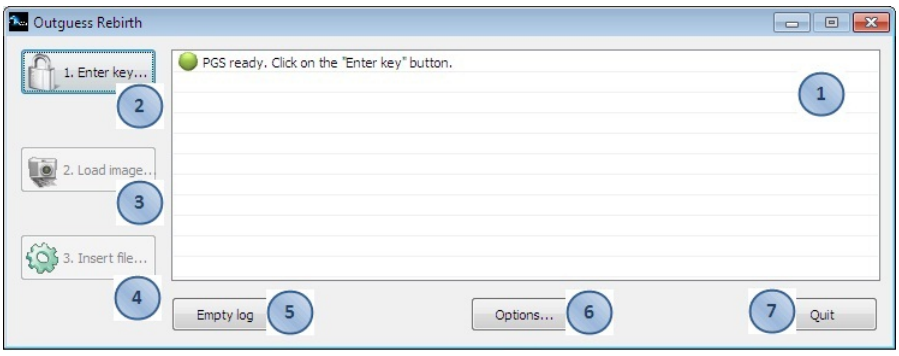

Figure 3.1: Outguess Rebirth main interface

Icon	Description
	Operation has been successfully completed
	Operation has been partly completed
	Operation has failed

Meaning of the icons for requested operations

- *"Enter key" button*ï¿½(2): the use of this button is detailed in paragraph 3.2.1.
- *"Loading image" button*ï¿½(3): the use of this button is detailed in paragraph 3.2.2.
- *"Embed/Extract file"* buttonï¿½(4): the use of this button is detailed in paragraph 3.2.3.
- *"Empty log" button*ï¿½(5): the use of this button allows to erase completely the contents of the window of the event log.
- *"Options" button* (6): the use of this button is detailed in paragraph 4.1.
- *"Quit" button*ï¿½(7): the use of this button exits the application.

3.2 Basic Functions

The process of embedding or extracting data into or from an image takes place as followsï¿½:

1. Enter the Key
2. Load an image
3. Embed or extract the data contained in an image

Once the embedding process completed, the image shall not be modified by any software (photo retouch, redimensioning, compression parameters, etc.) **Any change on a stenographed image causes the irreversible loss of the previously embedded data.**
The following paragraphs give a detailed description of the above mentioned stages.

3.2.1 Entering the key

The key is entered by clicking on the button "Enter key" in the main interface. Entering a key is required to carry out the following stages. In order to avoid any entry error, Outguess Rebirth asks the user to enter and confirm the key

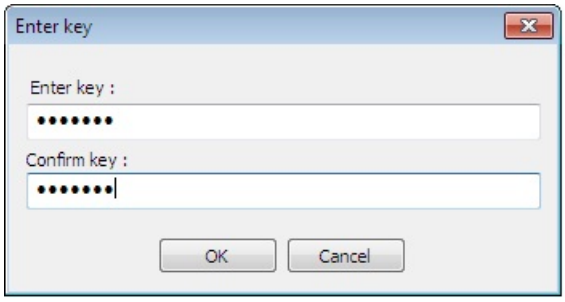

Figure 3.2: “Enter key” dialog box

used.
Capital and lower case letters are differentiated.
The key is limited to 32 characters. A key cannot be emptyï¿½; it must contain at least 4 characters.
Once the key entered and confirmed, the button OK becomes active and the user can validate his key in order to move to next stage.

3.2.2 Loading an image

To load an image, click on the button “Loading an image” in the main interface. The user then selects the image used as a carrier for the embedding or extraction operation, see paragraph 3.2.2.

Once the image loaded, the software gives you the capacity of the selected image. This capacity is the maximum data quantity (bytes) that can be embedded into the image.

Software is not able to detect whether the image has been steganographed with a key different from the one used in stage 1.

3.2.3 Data embedding or extraction

Case when the loaded image is “virgin” (not steganographed):

The software invites the user to embed data into the latter. To this end, click on the button “Embed file” in the main interface.
Select the file to be embedded, by making sure its size is smaller than the image capacity (See paragraph 3.2.3).
The event log tells you whether the embedding process has been operated successfully.

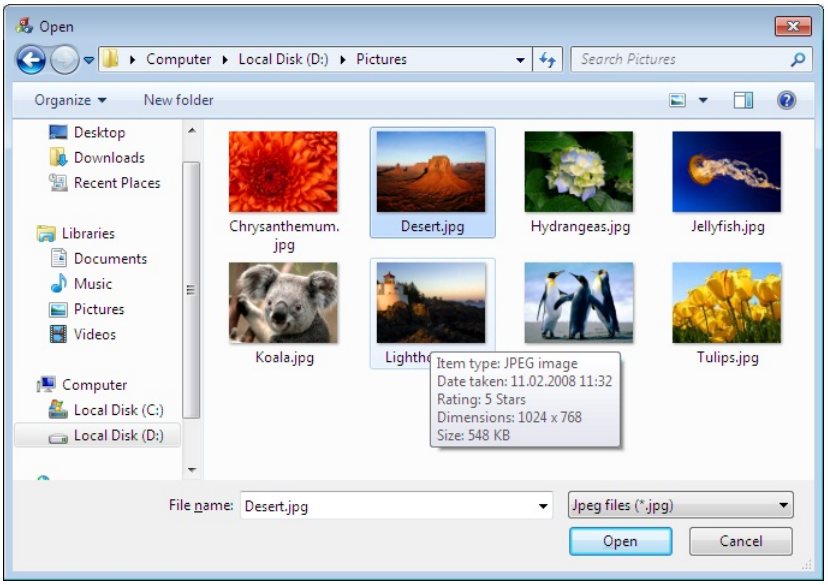

Figure 3.3: Loading an image file (picture.jpg)

- **Once the embedding process completed, the original image is overwritten by the new steganographed image.**
- **The embedded file is erasen for good if the option "Erase embedded file after steganography" is activated (See paragraph 4.1).**

Case when the loaded image is steganographed:

The software invites the user to extract the data contained in the image. To this end, click on the button "Extract file" in the main interface.
Select a place where you want to save the file contained in the image. The name and the extension of the inserted file are put into memory and automatically entered into the file-saving dialogue box.
The event log tells the user whether the extraction operation has been successfully completed. It is possible to extract several times the same data contained in an image by using the same key.

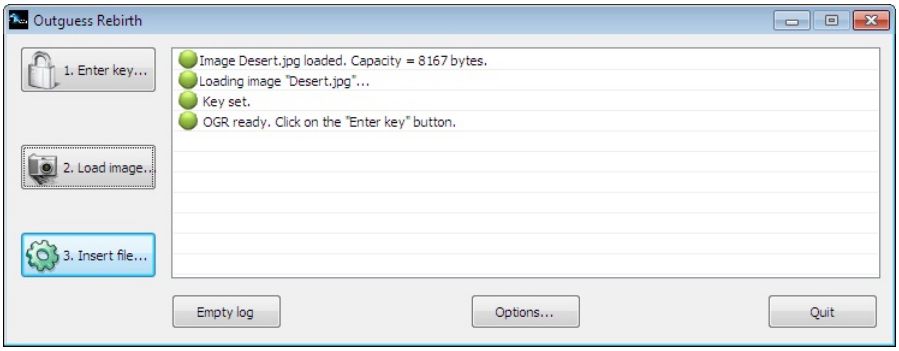

Figure 3.4: Displaying the capacity of a virgin image

If data have already been embedded into the image by using the same key, the user is informed of it by the event log. The button “Embed file” then becomes “Extract file”.

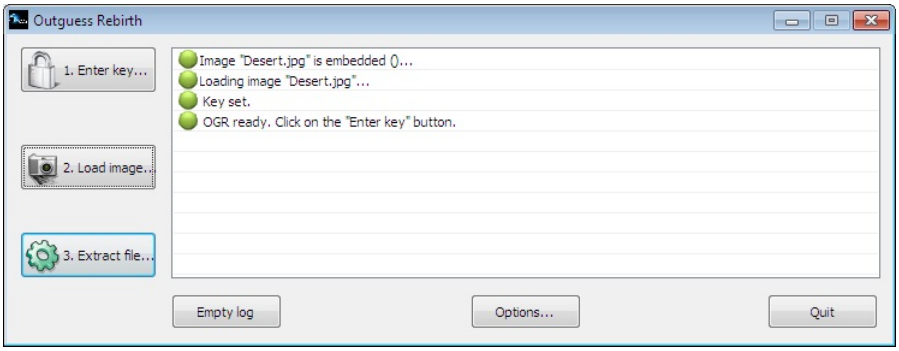

Figure 3.5: Case of a steganographed image

Chapter 4

Advanced functions

4.1 Options

The options of Outguess Rebirth are accessible through the button "Options" in the main interface:
Outguess Rebirth offers the following optionsï¿½:

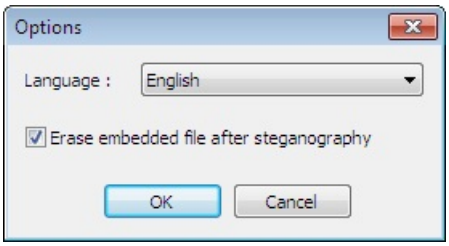

Figure 4.1: Options dialog box

- *Language*: allows to change languages. The language will change only once the operation validated by clicking on the button ï¿½ï¿½OKï¿½ï¿½. The language used by default is English.
- *Option "Erase embedded file after steganography"*: allows to erase the file embedded after a successfully completed operation of steganography. This option is activated by default.

Once the choices of the user validated, the software saves the configuration in a file: (OGR.cfg). This file is stored in the folder containing the executable of the software (OGR.exe). The next time the software is launched, the previously selected options will be put into memory.

4.2 Software update

TO-DO By clicking on “Yes”, software launches the Internet navigator by default, re-directing the user to the downloading page of the official site.

Chapter 5

Problems encountered

P1) I cannot extract the embedded data...
Please, check the following pointsï¿½:

1. 1. Has the key correctly been entered (capital or lower case letters) ?
2. 2. Has the image been altered by some software (See paragraph 3.2) ?

Any change in a steganographed image causes the irreversible loss of the previously embedded data.

Chapter 6

Frequently asked questions

Q1) Why is it possible to embed a file with a bigger size than the capacity of the image?
During the steganography process, the embedded file is previously compressed. Therefore, it is possible to embed a quantity of data higher than the capacity of the image indicated by the software.

Q2) Is it possible to embed several files in the same imageï¿½?
Currently, Outguess Rebirth can embed only one file per image. Embedding a second file in an image by using a different key will cause the irreversible loss of the first embedded file.

Q3) I have forgotten my key. Is there an emergency process to retrieve the data?
It is impossible to retrieve the steganographed data if the key used during the embedding process has not been correctly entered.