Parasite Image-based Steganography and Encryption System User Manual

.

Parasite Team

September 2, 2022

Content

1 Overview

1.1 Software Introduction

Parasite Steganography and Encryption System is an image-based message/data steganography and encryption software which integrates the advanced technologies of computer vision, image processing and data encryption. Parasite takes ordinary image as message carrier, and can automatically conceal message of any format into an image and meanwhile encrypt it with a randomly-generated unique dictionary in form of binary data stream. Through the independently-designed unique algorithm, a piece of message is embedded into an image and encrypted quietly without any changing in visual effect. With *Parasite steganography and encryption software* and by just sending an ordinary daily selfie, you can secretly, safely and securely transmit any message to any corner of the world through network.

1.2 Software Installation

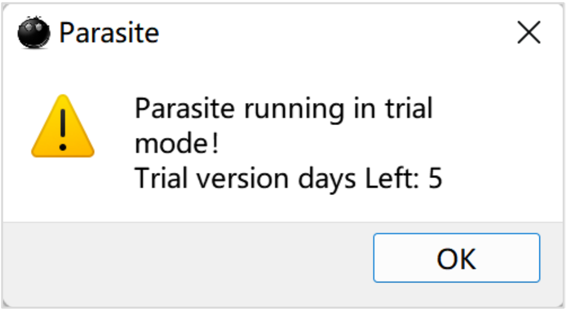
1.2.1 Installation Steps

Click and run *Parasite.exe* Setup with administrator permission, and then follow the steps shown below to complete the program installation.

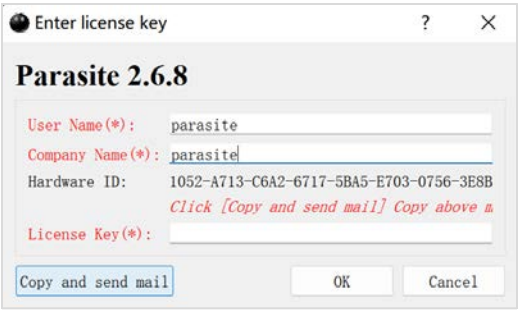
Click "Next" to install ⟶ *Select installation path* ⟶ *Create desktop shortcut* ⟶ *Prepare to install* ⟶ *Finish software installation*

After successful installation, you can double-click software icon and start running the program. The software will prompt you: "Parasite is running in trial mode", and click "OK" to start the trial.

1.2.2 Software Registration



Parasite running in trial mode!
Trial version days Left: 5



Parasite 2.6.8

User Name(*): parasite
Company Name(*): parasite
Hardware ID: 1052-A713-C6A2-6717-5BA5-E703-0756-3E8B
Click [Copy and send mail] Copy above m
License Key(*):

After installation, the software will be running in trial mode with 15 days free trial period. When the trial period expires, the program will prompt registration and authorization, then enter your username and company name (pay attention: please input lowercase English letter), and then send registration info to software developer to obtain license key. Referring to the following example:

Username: parasite (example)

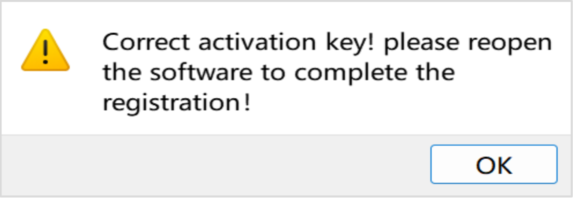
Company: parasite (example)

Hardware ID: 1111-2222-3333-4444-5555-6666-7777-8888 (example)

Copy and send above info to developer, the technician then will return you a license key as follows:

D2WA7E05-51W3E6EE-84CE89B3-3WWA6163-6AA31BEB-5B59KJ7B-5V81(example)

After license key activation, you can use *Parasite* software normally with no limit.



Correct activation key! please reopen the software to complete the registration!

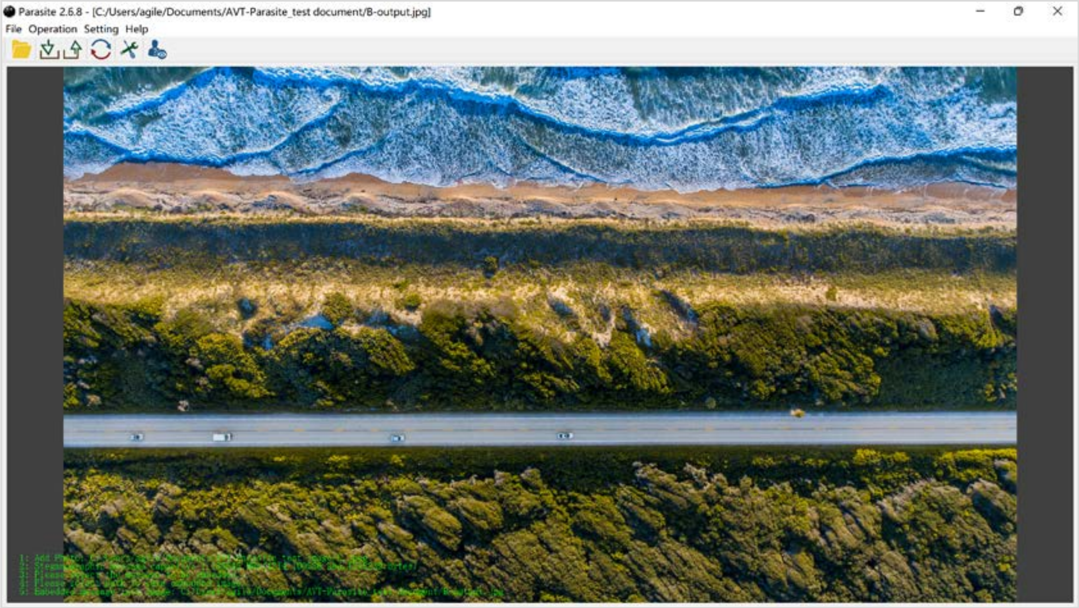
1.3 Operating Environment

Parasite software supports running on 64-bit Windows operating systems. This software does not require high hardware configuration, but we still recommend that you use a PC with i5 CPU plus 8GB memory and above hardware configuration to obtain smooth and stable software operation.

2 Software Interface and Menu

2.1 Main User Interface

This software has features of simple interface, friendly interaction and easy operation. The main interface includes title bar, menu bar, toolbar, image display panel and log panel, etc., as shown in the following figure:


Parasite 2.6.8 - [C:/Users/agile/Documents/AVT-Parasite_test document/B-output.jpg]
File Operation Setting Help

Main User Interface

1) The title bar includes a software icon, software name, software version number, maximize and minimize button, and close button;

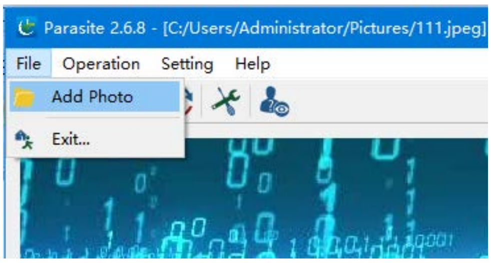
2) The menu bar includes four main menus: file, operation, setting and help;

3) The toolbar comprises various task processing buttons;

4) The log panel is used for outputting and displaying various operation information in process of using the software;

5) The image display panel is used to display the loaded image.

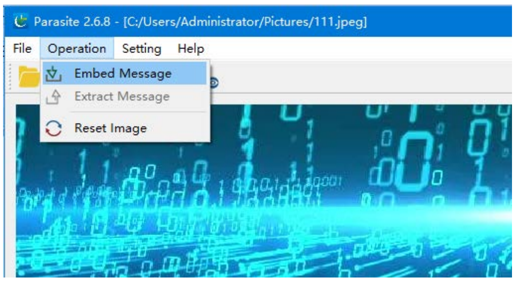
2.2 File Menu


Parasite 2.6.8 - [C:/Users/Administrator/Pictures/111.jpeg]
File Operation Setting Help
Add Photo
Exit...

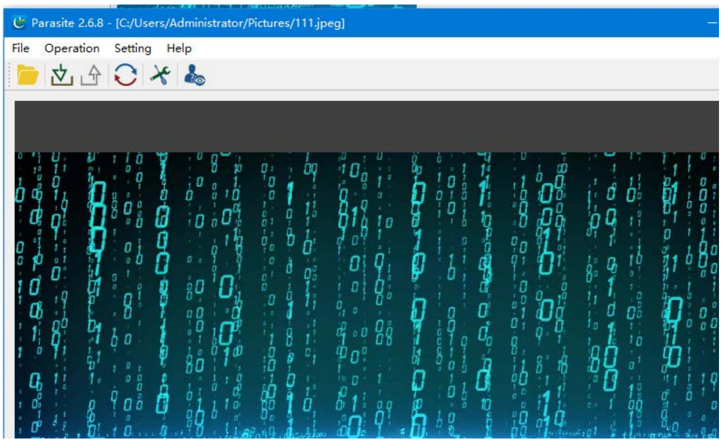
1) Add image: Add an image as message carrier (pay attention: the image you add can be original one before stenography or encrypted one after stenography). Parasite currently supports most of common image formats, such as *.jpg、*.bmp、*.png、*.tif etc. It should be noted that the capacity of embeddable message is different for images with different formats and sizes. After adding an image, the software will automatically calculate the capacity of embeddable message and display it on log panel;

2) Exit: Exit the software system.

2.3 Operation Menu



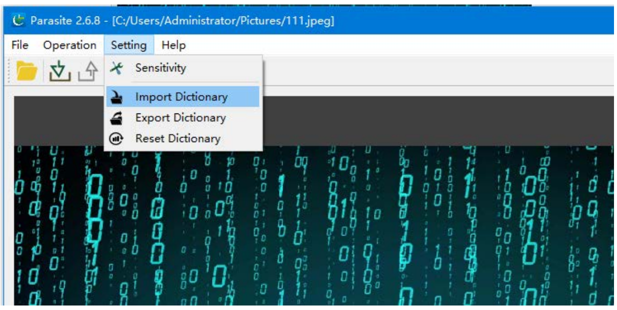
1) Embed message: This software supports embedding files in any format (*.*), it should be noted that whether a file can be embedded into a specific image depends on the size of both the file and image. The size of message/file to be embedded by this software should be less than 12% of the image size. For example, this aerial seaside landscape photo below is of 7.27 M in size and. JPG format, then the software automatically calculates out that the capacity of steganographic message is no more than 1.207413 MBs.



2) Extract message: to extract hidden message from steganographic image. If an image containing enciphered message is loaded, the software will automatically pop up a dialog box to prompt whether message extraction is needed;

3) Reset image: The software supports viewing the whole picture or partial of it by zooming in and out. Click "Reset Image" to return to default viewpoint of the image, and the shortcut key corresponding to this function is "Space" key.

2.4 Setting Menu



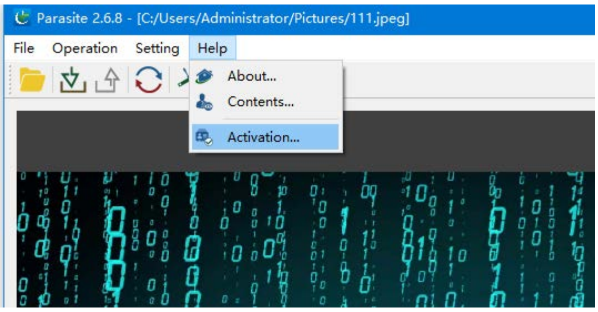
1) Sensitivity setting: to set the scrambling and encryption level of the hidden message, and the higher the setting level, the more scrambling times to be conducted;

2) Import Dictionary: to import an external dictionary file, which is used to extract hidden message encrypted by using the dictionary. It should be noted that only when the dictionary and software version are exactly the same can the hidden message be extracted, and importing different dictionary will lead to "*the hidden message encrypted by using a previous dictionary cannot be extracted*";

3) Export Dictionary: to export the dictionary after message encryption, which can be sent to image receiver in case he/she does not possess the same dictionary for message extraction.

4) Reset Dictionary: to abolish the dictionary currently used by software and generate a new one. It should be noted that once the dictionary is reset, the message embedded in stego image with the previous dictionary before resetting will NOT be extracted.

2.5 Help Menu

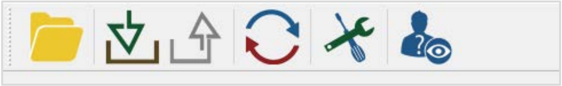


1) About: Display software copyright notice and contact information of the developer (email address, website address);

2) Help: Pop up the operation manual of software for users to view;

3) Activation: Pop up registration and authorization interface of software, and it can be used freely without any restriction after successful registration.

2.6 Toolbar



The toolbar icons from left to right are:

1) Add image: Open an original image for message embedding or a steganographic image for message extraction;

2) Embed message: You can embed file/message of any format (*.*) in an image;

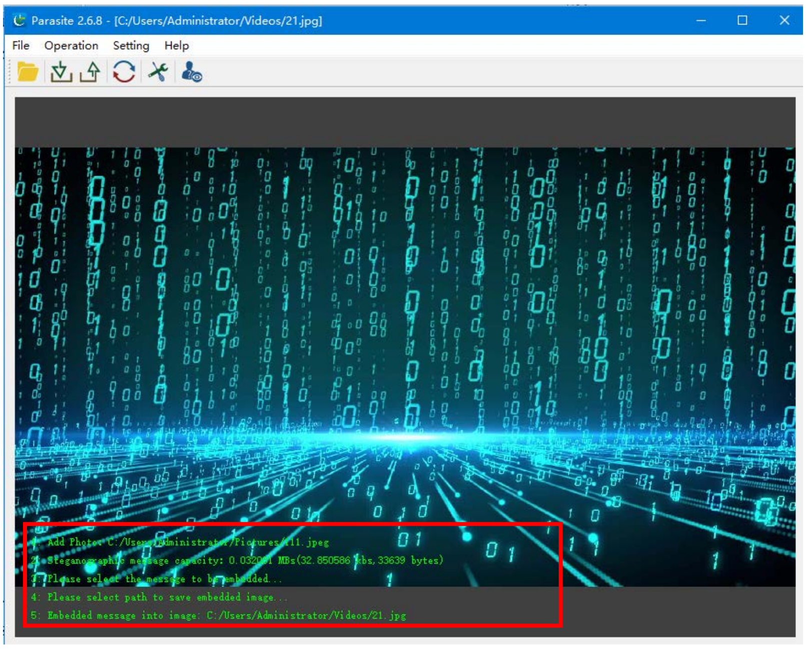
3) Extract message: Extracting hidden message from steganographic image;

4) Reset image: The software supports viewing the whole picture or partial of it by zooming in and out. Click "Reset Image" to return to default viewpoint of the image, and the shortcut key corresponding to this function is "Space".

5) Sensitivity setting: Set the scrambling and encryption level of hidden message;

6) Display contents: Display software operation manual.

2.7 Log Panel



```
1: Add Photo: C:/Users/Administrator/Pictures/111.jpeg
2: Steganographic message capacity: 0.032081 MBs(32.850586 kbs,33639 bytes)
3: Please select the message to be embedded...
4: Please select path to save embedded image...
5: Embedded message into image: C:/Users/Administrator/Videos/21.jpg
```

As shown in the above picture, each operation of software such as adding image, embedding message, extraction of message, size of embeddable message/steganographic capacity, and whether the added image contains hidden message, etc., will be output to log panel and displayed on screen, so that the software prompts user to take appropriate operations.

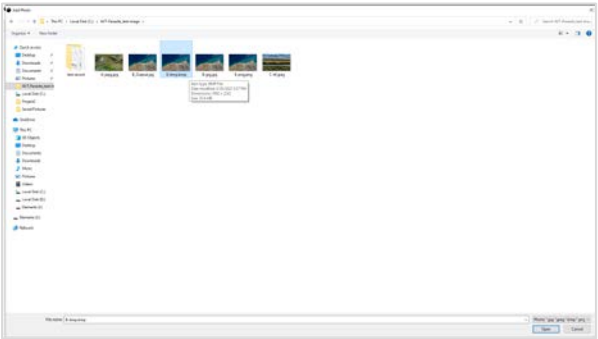
3 Operation Steps for Typical Task

Assuming that Party A use the software to embed document A into image B and then send it to Party B, and Party B extracts hidden document A from image B using the same software, we take this as an example to illustrate the operation process of typical tasks of the software:

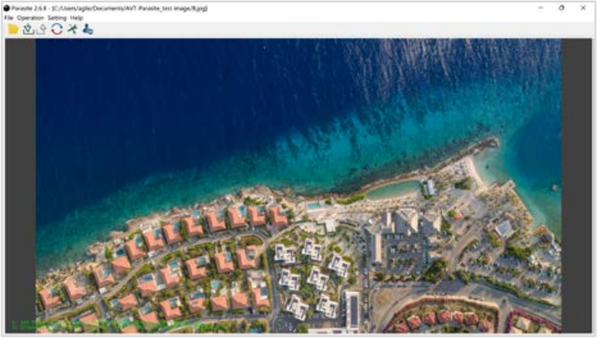
3.1 Embed Message into Image and Encrypt

3.1.1 Add Image B

After starting the software, click *Add Image* button. After adding Image B, the software automatically calculates and prompts that the size of embeddable message/file is about 1.2074 megabytes on log panel. The size and format of the original image determine the size of embeddable message also known as steganographic capacity, which is about 12% of the original image size.



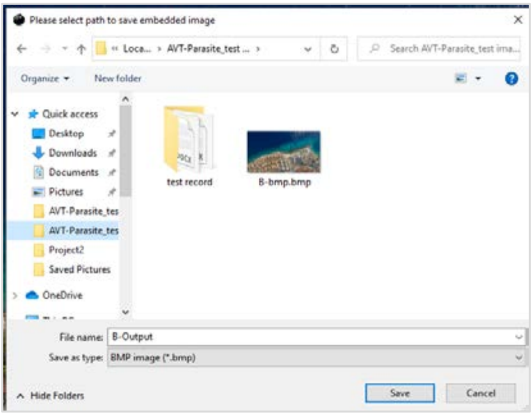
Add Image Carrier B



Calculation of steganographic capacity and display

3.1.2 Embed Message A into Image B

Click the *Embed Message* button, and the software will automatically pop up a window to let you select the path where the embedded message is located. The embedded message can be a file in any format. After the message is embedded in the carrier image, enter a new image name "*B-Output*" and select the path where the file is stored. Now the steganography process of embedding message A into image B is completed, meaning message A has been hidden and encrypted simultaneously.



Please select path to save embedded image

File name: B-Output

Save as type: BMP image (*.bmp)

3.1.3 Export Dictionary

If Party B does not have the same dictionary which Party A uses to encrypt, then Party A needs to export the dictionary and send it to Party B in an appropriate way, otherwise this step can be neglected.

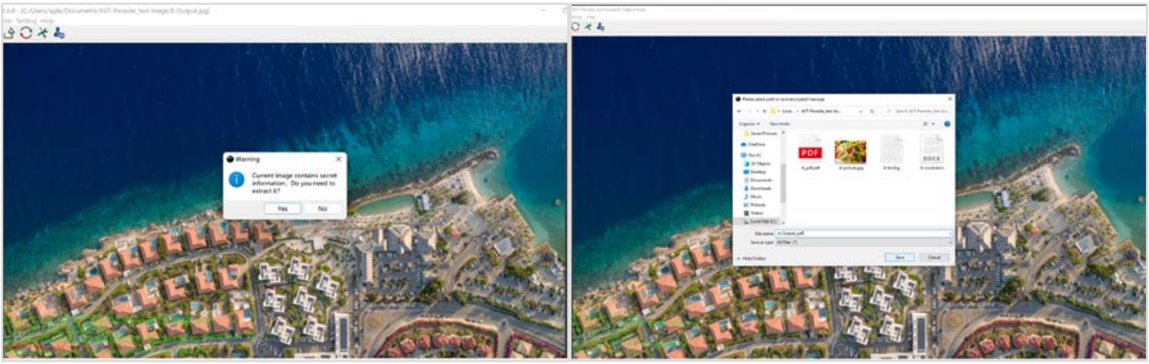
3.2 Extract Hidden Message from Image

3.2.1 Import Dictionary

After receiving image "*B-Output*"/the stego image, Party B firstly needs to import the dictionary which Party A used if he/she does not have the same dictionary, otherwise this step can be neglected.

3.2.2 Add Stego Image and Extract Message A

Party B adds the stegoimage/B-Outputto the software, and the software interface will automatically prompt "*The current image contains hidden message, do you need to extract it?*" Then click "*Yes*", select the storage path and rename the message (*“A-Output”*for example), and the hidden message will be extracted to the designated location with new file name.

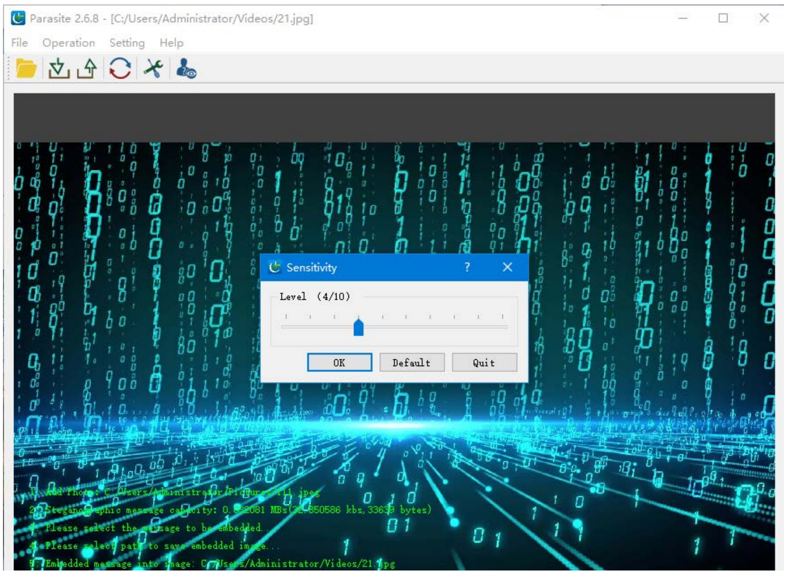

Warning

Current image contains secret information, Do you need to extract it?

3.3 Setting Dictionary

3.3.1 Sensitivity Level Setting

The software can set sensitivity/encryption level to the message embedded in image, from level 1 to level 10 corresponding to different encryption and scrambling times (the default value is 4). Although this software adopts the randomly-generated binary data stream for high-strength encryption， which is theoretically uncrackable. But it can't guarantee absolutely100% that there is no risk of being cracked at ANY time, which is especially stated here.


Parasite 2.6.8 - [C:/Users/Administrator/Videos/21.jpg]

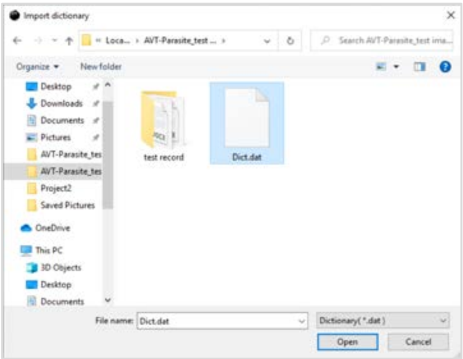
Sensitivity

Level (4/10)

```
1. Add Photo: C:/Users/Administrator/Pictures/111.jpeg
2. Steganographic message capacity: 0.032081 MBs(32.850586 kbs,33639 bytes)
3. Please select the message to be embedded.
4. Please select path to save embedded image...
5. Embedded message into image: C:/Users/Administrator/Videos/21.jpg
```

3.3.2 Import Dictionary

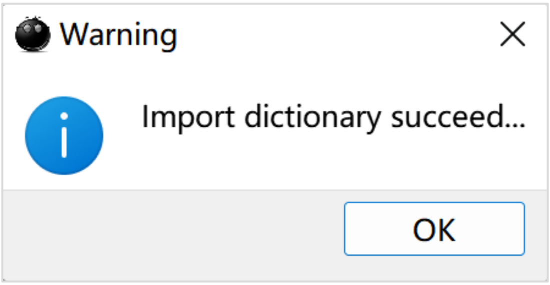
When Party B needs to extract the hidden message A from the steganographic image B sent by Party A, he needs to import the dictionary file (both parties can reach agreement in advance and share the same dictionary with each other, or one party can send the same dictionary to the other party in advance). It should be noted that only when the software version and dictionary file are exactly the same can message embedding and encryption, and message extraction be realized bidirectionally.



Import dictionary

File name: Dict.dat

Dictionary(*.dat)

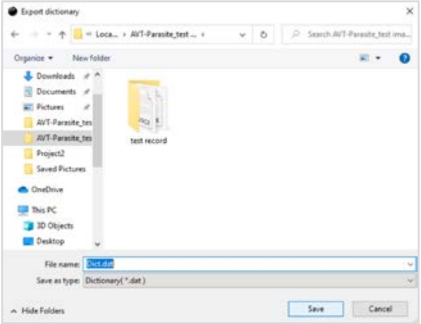


Warning

Import dictionary succeed...

3.3.3 Export Dictionary

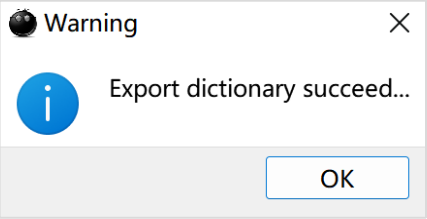
When Party A sends the image embedded with encrypted message to Party B for extraction, it needs to send the dictionary file to Party B first, and of course, both parties can also share the dictionary file in advance. It is strongly recommended to share dictionaries through other secure channels before message transmission. Do not transmit dictionary files and message carriers together or by same means under any circumstances, so as to prevent the leakage of dictionary files and message carriers at the same time.



Export dictionary

File name: Dict.dat

Save as type: Dictionary(*.dat)

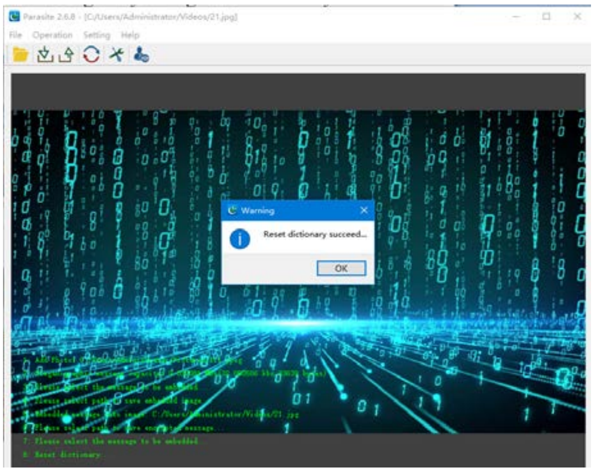


Warning

Export dictionary succeed...

3.3.4 Reset Dictionary

After a dictionary is used for a period of time, it needs to be reset to ensure the uniqueness of the dictionary and reduce the risk of cracking hidden message in image. When many dictionaries need to be generated, they can be reset and then exported many times. And each dictionary can be destroyed after transmitting a file, which will greatly strengthen the security of message carrier in network transmission.



Parasite 2.6.8 - [C:/Users/Administrator/Videos/21.jpg]

Warning

Reset dictionary succeed...

```
1: Add Photo: [illegible]
2: [illegible]
3: Please select the message to be embedded
4: Please select path to save embedded image
5: Embedded message into image: C:/Users/Administrator/Videos/21.jpg
6: Please select path to save encrypted message...
7: Please select the message to be embedded...
8: Reset dictionary...
```

4 Frequently Asked Questions (FAQ)

4.1 Why the image can be added successfully but cannot be embedded with message/file?

Images with different formats and sizes can be embedded with messages/files of different sizes. If embedded file is larger than the steganographic capacity of added image, it then cannot be embedded. After loading an image, the software will automatically calculate the capacity of embeddable message, and embedded message should usually be less than the steganographic capacity.

4.2 When Party A sent image B embedded with message A to Party B, why can't Party B extract hidden message normally?

Only when both parties use the same version software and the same dictionary, can the message in the same carrier image B be extracted bilaterally. Under the condition that the software version of both parties is the same, Party A can export a dictionary and send to Party B, and Party B can import the same dictionary to extract the hidden message in image B.

4.3 Software runs normally after successful authorization, but it is prompted that license key is needed again when reopening software?

A large number of testings have proved that this problem does exist. This problem generally occurs when the software is installed on System disk C disk. The authorization file needs to be written to the installation directory when the software license key is being activated, and this operation is rejected by Windows OS due to non-administrator permission.

Solution: Install the software on non-system disk (such as D disk), and input the user name and company name in lowercase English letter when registering software.

4.4 What if the software is hijacked or prohibited by antivirus software such as Kaspersky or McAfee during installation or use?

Parasite adopts the most advanced information security technology to encrypt and encapsulate the core algorithm of software and encapsulate the intermediate results of processing as well, this protection mode may be mistaken for abnormal operation by antivirus software.

Solution: Temporarily exit the antivirus software during installation, and then set the Parasite to security white list of the antivirus software.

4.5 If the setgo image with encrypted message is posted on social media, can you still extract the hidden message normally after downloading?

If you post stego image with hidden message to social media, then you probably will not succeed to extract the message again after downloading it. That is because most social media platform will conduct data reconstruction while posting to internet, which will corrupt the original image data format and lead to extraction failure.

5 Technical Support

For technical problems during software installation and use, you can make technical consultation through email to software vendors. We will reply to you ASAP.

Contact Parasite:

E-mail: **uavmapper@outlook.com**

WeChat: