EXPERIMENT NO 3

XIAO STEGANOGRAPHY

Aim: To hide the secret data from unauthorized users in order to prevent confidentiality, integrity and availability of data.

XIAO STEGANOGRAPHY

Xiao Steganography is a tool which is used to hide the secret data from unauthorized users in order to prevent confidentiality, integrity and availability of data. .Xiao Steganography is free software that can be used to hide secret files in BMP images or in WAV files. Usage of this tool is easy, as it can be downloaded and used. Any BMP image or WAV file can be added to its interface. Then the file, which we want to hide, is added. Xiao also supports encryption. We can select from various algorithms like RC4, Triple DES, DES, Triple DES 112, RC2 and hashing SHA, MD4, MD2, MD5.

To read the hidden message from this file, we will have to use this software again. This software will read the file and will decode the hidden file from it. But we extract the hidden file from any other software other than Xiao, as it has been hidden or encrypted using Xiao only.

Following are the various steps that show encoding and decoding as achieved by Xiao:

A. Encoding/Encrypting using Xiao

1) Open Xiao tool to implement Steganography, as shown in Fig. 1. This is the first snapshot when the tool is opened after being downloaded.

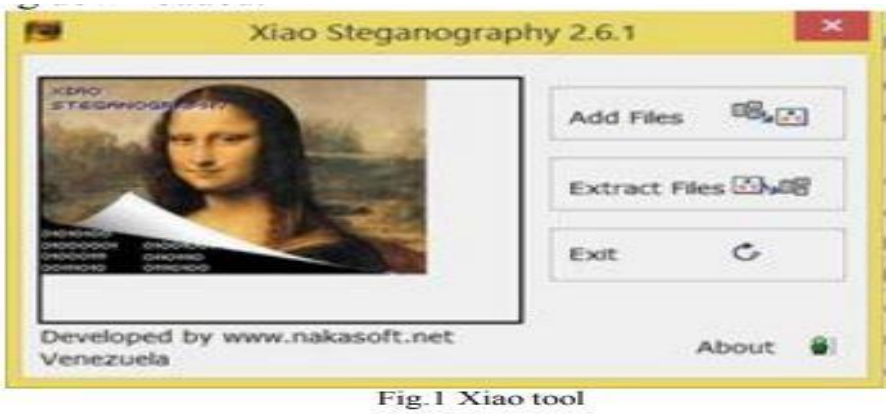

Fig.1 Xiao tool

2) As shown in Fig. 2, cover image or the target file, as popularized by Xiao is selected. For this the Load Target File option should be clicked.

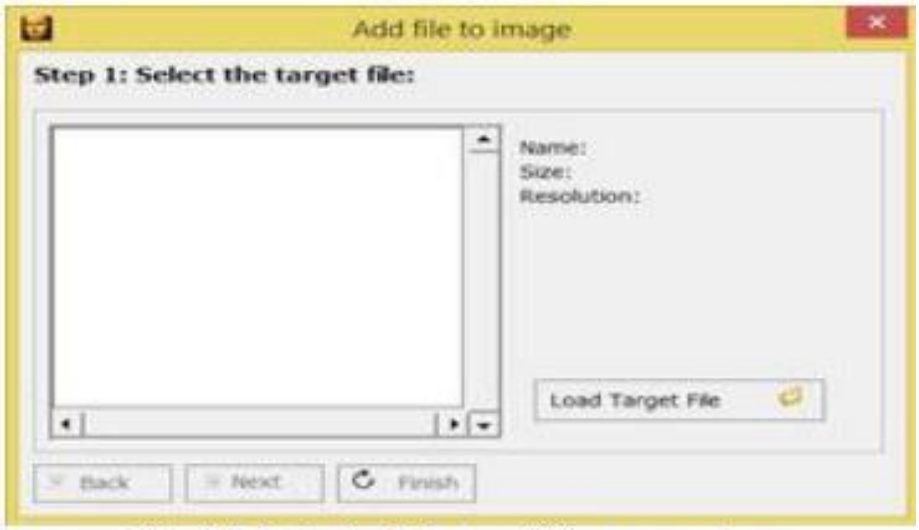

Fig. 2 Select to load the target file or cover image

3) Fig. 3 depicts out target image. The secret message will be embedded in this target file. Select this target file to conceal our secret data.

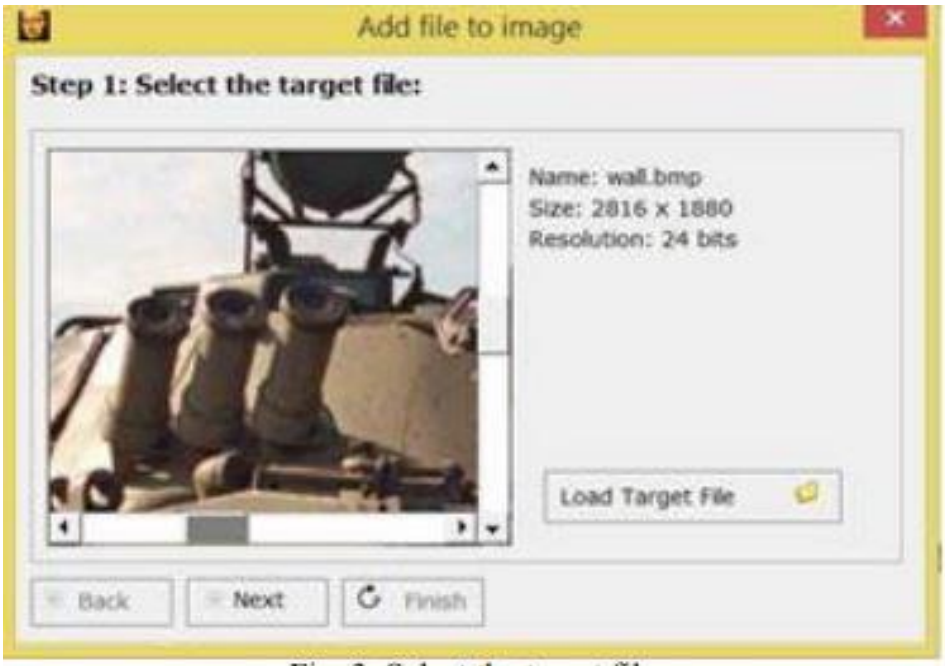

Fig. 3 Select the target file

4) By selecting on Add File button in Fig. 4, we will be able to select our Secret file or confidential data, which will be embedded in our target file. The remaining size is mentioned in KB. This suggests the size available to add the secret data in the form of files.

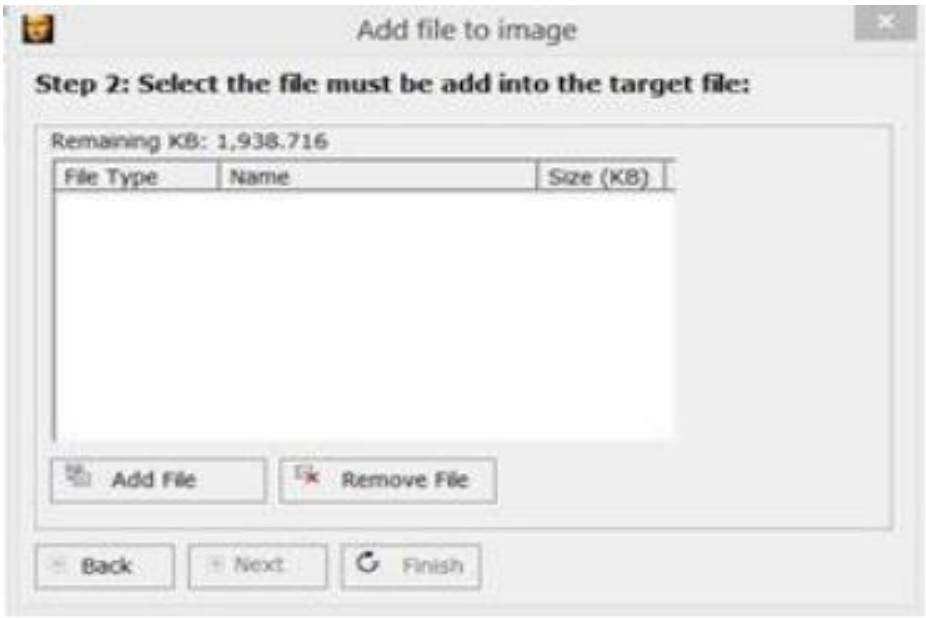

Fig. 4 Select the file to be added into the target file

5) Fig. 5 shows that we are hiding an image called Koala. Further files can be embedded using the Add File option.

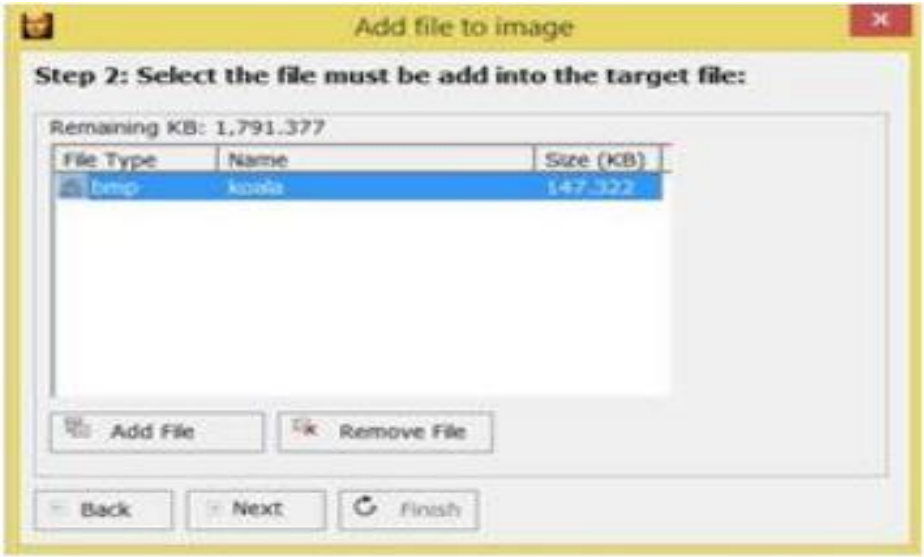

Fig. 5 Secret File added

6) In Fig. 6, we need to select the encryption option and a password to provide double security of our confidential message/image. There are four hashing algorithms and five encryption algorithms available as depicted below:

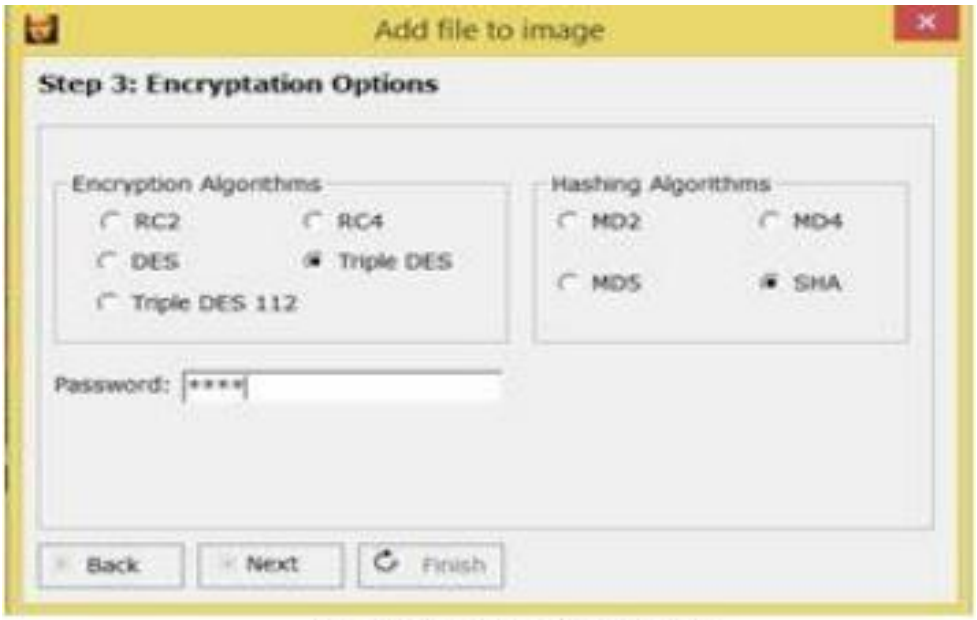

Fig. 6 Select the algorithms

7) After applying the appropriate encryption algorithm and a strong password on our secret message, we can embed it in our target files as shown in Fig. 7. This snapshot depicts a progress bar exhibiting the merging of both the files i.e. Target File or Cover Image and our Secret image.

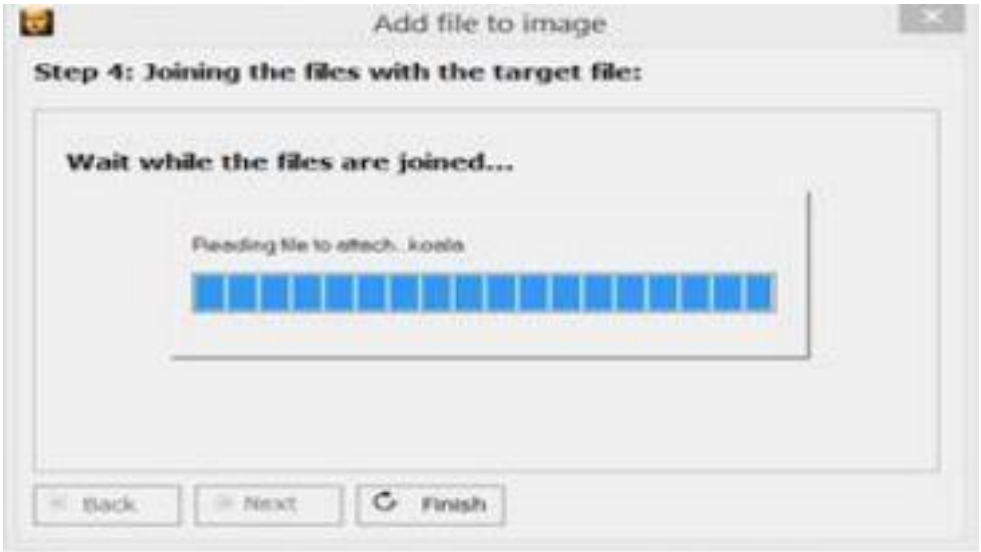

Fig. 7 Joining the files with the target file

8) All the above seven steps accord with embedding process and Fig. 8 shows that steganography was successfully accomplished.

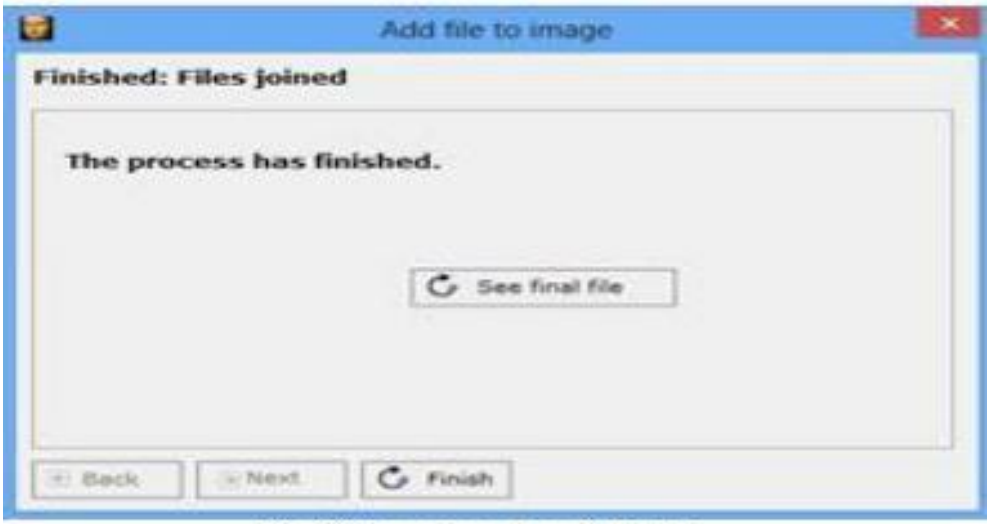

Fig. 8 The process has finished

B. Encoding/Decrypting using Xiao 1) Now at the decoding end, if an authenticated user wants to extract the secret message from the target file or the cover image, then receiver needs to click on the Extract file option as shown in Fig. 9

Fig. 9 Xiao tool – Extracting Files

2) In Fig. 10, we need to select Source file. This is the same target file or cover image which was used for encoding the confidential data.

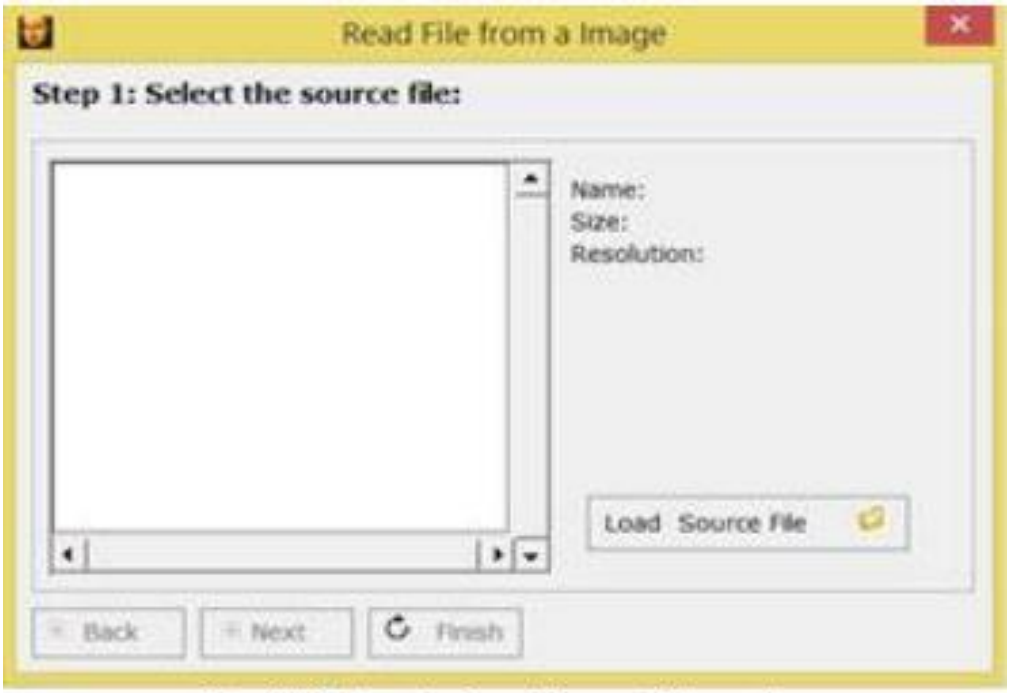

Fig. 10 Select the Load Source File option

3) Fig. 11 shows the Cover Image or the target file. By clicking on Extracting Load file, we can extract our secret koala file.

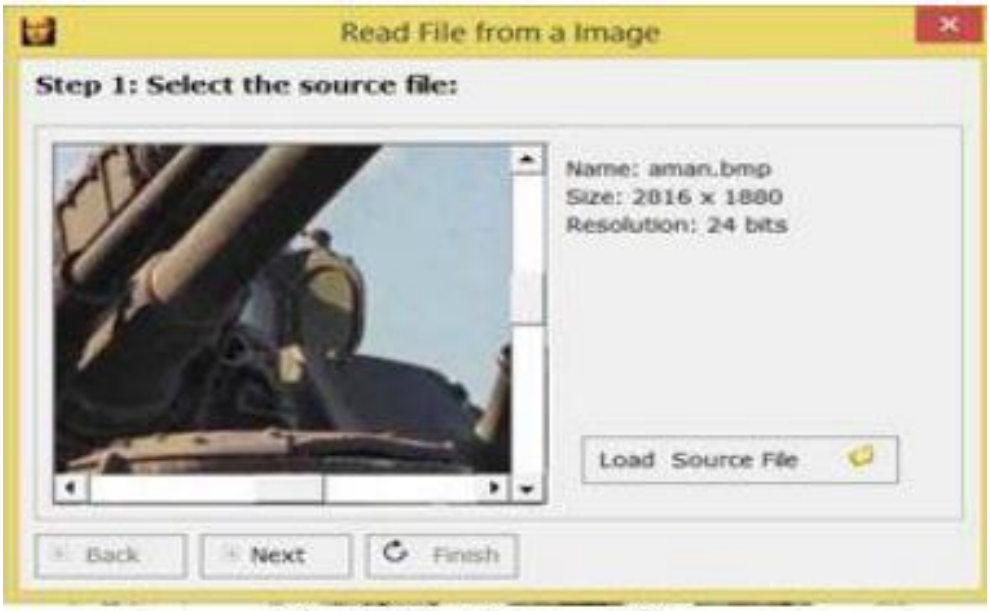

Fig. 11 Select the source file

4) Fig. 12 depicts our embedded target file ready for decryption

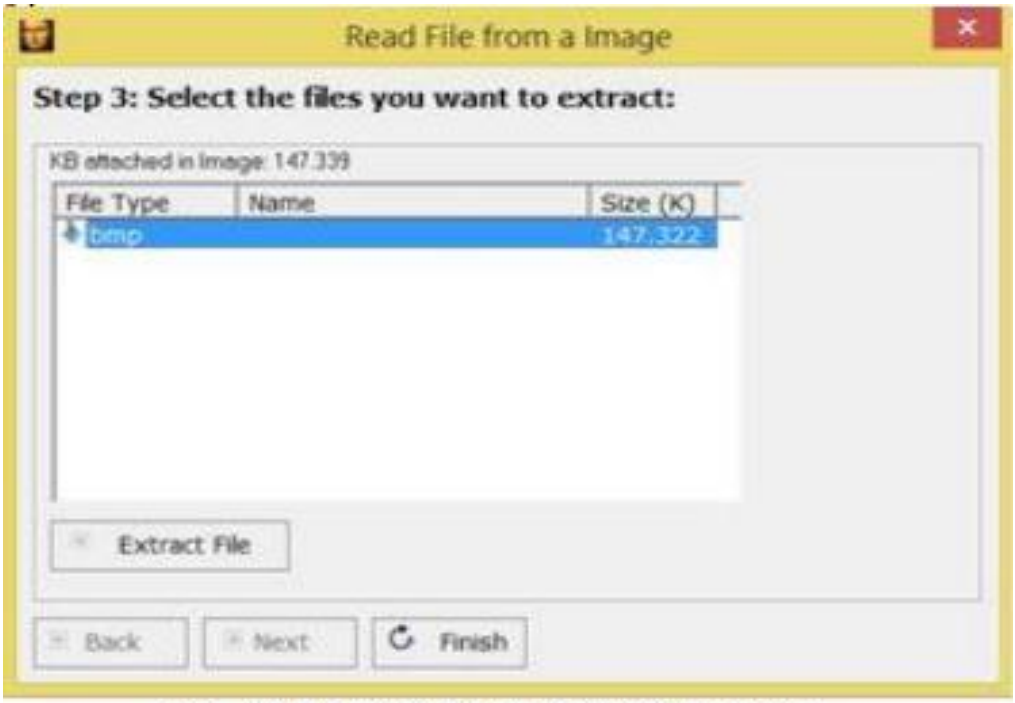

Fig. 12 Targert File to be decoded/decrypted

5) Here we can easily see our secret image koala which we embedded. This secret image is the actual message intended for the recipient which could be saved at any path using the Save As option as depicted in Fig. 13

Fig. 13 Save as file

6) Fig. 14 shows the secret file had been extracted by the receiver successfully.

Fig. 14 File extract was successful

Observation: This tool hide and retrieve data successfully.