# Performance Analysis of Open-Source Image Steganography Tools

**Urmila Pilania***

Manav Rachna University, Faridabad and 121004, India, urmila@mru.edu.in

**Rohit Tanwar**

School of Computer Science, University of Petroleum and Energy Studies, DehradunInstitution and 248007, India, r.tanwar@ddn.upes.ac.in

**Prinima Gupta**

Manav Rachna University, Faridabad and 121004, India, prinima@mru.edu.in

**Abstract**

In the present epoch, where technology is rising fast with new developments, the main challenge for the sender is to ensure that information is sent in a correct and covert mode that only the receiver is capable to recognize. Steganography is the art of concealing and transmitting secret information through carrier multimedia without being exposed. In this paper, four open-source image steganography tools are analyzed and compared on basis of image features like the type of cover image, the dimension of stego image, type of secret information, type of output image, the technique for concealing secret information, encryption support, hashing, data compression, etc. The comparative analysis of these tools based on specified parameters represents their strengths, limitations, applicability, and scope for future work as well. OpenStego image steganography tool performs amazing among the researchers and the professionals. This paper also put efforts to explore the working of the OpenStego tool on some unexplored parameters to authenticate and validate its performance.

**Keywords:** Security System; Steganography tools; Watermarking; OpenStego.

**Article history:** Received: February 20, 2021; Accepted: April 18, 2021

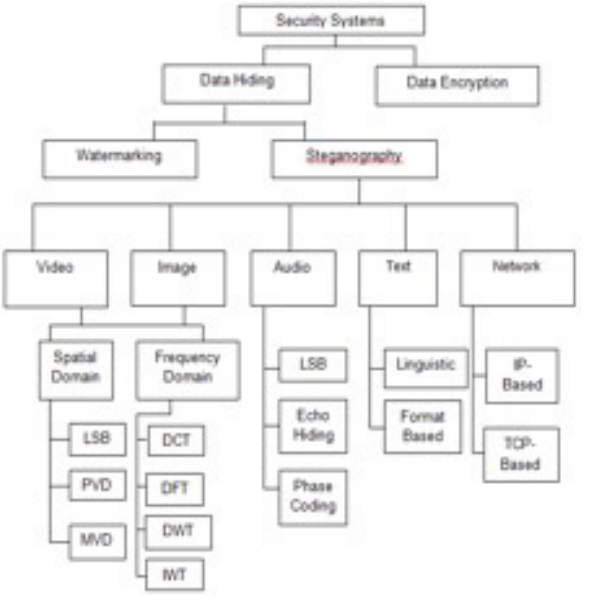
## 1. Introduction

Depending on the kind of carrier file used, steganography is categorized as text, image, audio, and video [1]. Text steganography is the simplest technique with less information concealing capacity and low imperceptibility. It will provide a double level of security when a secret key is used. It causes a problem in rewriting, modifying line-height, addition, or removal of words. Image steganography is much more powerful than text steganography in terms of security and information concealing capacity. In image steganography concealed information does not stand out by making a slight change to the color values of an image. For providing better security to concealed information in image steganography usually, more padding needs to be done around secret information. Audio steganography examines inaudible frequencies for concealing secret information [2] [3]. Video steganography has the option of concealing secret information inside inau-

dible frequencies and images as well. Further video and image steganography are divided mainly into two parts based on their domain: Spatial and Transform domain. In the spatial domain, some of the bits in a pixel are substituted by the secret information. Some commonly used spatial domain techniques are PVD (Pixel Value Differencing), RPE (Random Pixel Embedding), EBE (Edges Based Information Embedding), MPD (Multi-Pixel Differencing), LSB (Least Significant Bit), etc [4]. Whereas transform domain working is based on altering Fourier transform. Transform domain-based techniques are not easy to understand. These techniques first find the complex region for concealing secret information and then hide secret information in these regions. Some of these techniques are DCT (Discrete Cosine Transform), DWT (Discrete Wavelet Transform), IWT (Integer Wavelet Transform), and DFT (Discrete Frequency Transform) [5].

In image steganography, the location of secret information may vary. Secret information can be spread uniformly over a full image or can be concealed into complex parts where it is challenging to detect a minor change. Complex areas carry high frequency in which concealing of secret information causes minor changes in colour intensity values. Concealing secret information in the spatial domain has a great payload capacity, though this method is breakable, disposed to statistical image processing attacks. The transform domain method of image steganography is based on concealing coefficient in the frequency domain. It is much stronger against image processing attacks and compression [6]. During communication information can be secured by different methods shown in Figure 1.

Fig.1. Security system




In section II of this paper, a literature review of steganography techniques, tools, and steganalysis techniques are discussed. In section III metrics for measuring the performance of the steganography tools are explained. In section, IV steganography tools are analyzed and compared on basis of image features like the type of carrier image, dimension of stego image, type of secret information, type of output image, the technique for concealing secret information, encryption support, hashing, data compression, etc. In section V some of the observations on stego images are done in terms of PSNR and SSIM. Histogram, Entropy, and Frequency Spectrum are also plotted to compare the original secret image and stego image. At last, in sec-

tion VI conclusion for this paper is given along with some valuable suggestions for further work.

## 2. Literature Review

Steganography is the art of concealing secret information in carrier files in such a way that hackers cannot detect concealed secret information. In case concealed secret information is detected, a tool needs to be invented to confirm that secret information remains secret. A lot of research has already been done on image steganography tools related to the theoretical, mathematical, and technical development of steganography techniques. Many steganography tools exist in the market to conceal secret information inside digital carrier file. For the steganography process to take place successfully both of sender and receiver need to install the same tool at their end. These tools are categorized as to whether it is used to conceal secret information or it is used to detect the concealed secret information. Literature survey of some of these tools is listed below:

*2.1 Steganography tools*

*2.2 Steganalysis tools*

*2.1Steganography tools:* Steganography tools conceal secret information in such a way that no one can detect it. Based on the type of cover file these tools are divided into Text, Image, Audio, and Video steganography tools.

In paper [7] have used the text steganography tools (SNOW DOS 26 and wbStego4.3open) to conceal secret information. The author has chosen a carrier file and generated a stego output file with the help of these two tools by providing the different sizes of secret information. They also compared these two tools in terms of concealing capacity. They found wbStego4.3 steganography tool is better for concealing secret information. Image steganography tools can conceal a large amount of secret information as compared to text steganography tools. In paper [8] proposed Stego tools and compared different tools available freely. An image has been taken as a cover file for measuring the performance of various tools available online. Moving forward in [9], have focused on various steganography tool processes. Based on their exploration of steganography processes they divide tools into five categories: Spatial domain, transform domain, Type of document, Video compression encoding, and File structure. To provide better security in [10], focused on the traces leftover when steganography tools were installed, run, and then uninstalled. Through these leftovers, they detected concealed secret information.

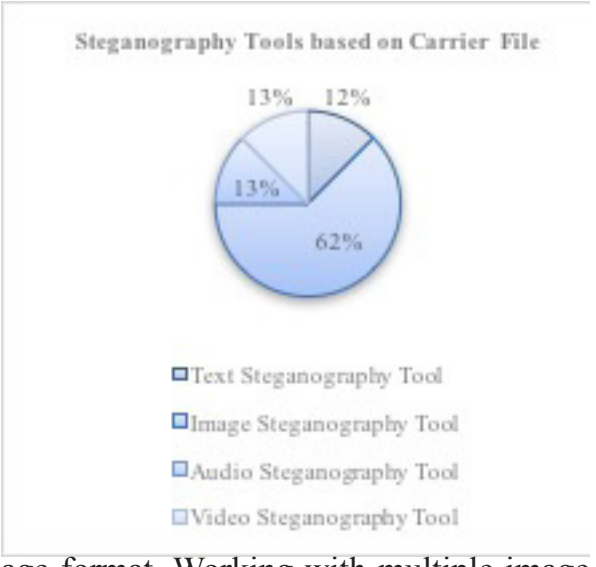
Again, comparison of different image steganography tools based on various parameters was carried out in paper [11]. They also introduced a robust and high payload steganography algorithm. Performance of steganography tool depends on the amount of secret information concealed, security, robustness, and imperceptibility. With the size of carrier file and its type performance of steganography tool varies. In paper [1], have carried out a comparison of the performance of various steganography tools. The author focused on carrier files during

communication over the network. Graphical inspection and statistical assessment methods were used to evaluate the performance of the tools. Based on different steganography algorithms in paper [12], have compared various image steganography tools. Authors have used the same input image to conceal secret information through different steganography tools and got different output stego images produced by particular tools. These stego images are then compared in terms of their PSNR value to find the best tool. Edges in cover file carry no significant information. So, author in [13], have presented image steganography where edges in the cover image are used to conceal secret information. The author analyzed that to conceal more secret information weaker edges can be used. Experimental outcomes prove that the above technique can efficiently sense MP3Stego with low concealing capacity. In [14] authors have presented a summary of broadly used open-source and freeware steganography tools. They gave information about types of a carrier file, secret information, technique used to conceal secret information, encryption provision, data compression, hashing, etc. In paper [15], a steganography tool was created by for concealing secret information. This tool works in VB (Visual Basic) environment, the author has created, implemented, and detected concealed secret information. Spatial domain techniques have a large concealing capacity but are less robust against image processing attacks. In [16], authors have concealed secret information through the StegCure steganography tool using the LSB technique. The enhanced LSB technique was used for good robustness against various attacks. StegCure tool compromises user-accessible functionality along with cooperative GUI (Graphical User interface) and cohesive navigation abilities. Again, LSB substitution technique was utilized in [17] for concealing secret information on the OpenPuff tool. For analyzing the performance of the OpenPuff tool several image formats were tried. Stego images produced by the OpenPuff tool were compared on various structures for the finest output regarding format. Different file formats are tried and tested by researchers to avoid geometric attacks.

The transform domain-based DCT technique was used by the author for concealing secret information. In [18], have introduced an overview of steganography techniques for concealing secret information in several image formats and also presented a novel system of data transmission within Microsoft word documents through JPEG (Joint Photograph Expert Group) images earlier handled by tool StegApp 1.1.0. This tool works on the conversion of the JPEG image by a domain transformation algorithm through restrictions gained by DCT.

After literature review, it is concluded that image steganography is the main focus among scholars, also shown in figure 2. Image steganography tools are secure; robust against image processing attacks, and has high concealing capacity. Some of these tools can handle any type of im-

Fig.2. Categorization of Steganography Tools




age format. Working with multiple image formats provides flexibility to image steganography tools.

*2.2 Steganalysis tools:* Steganalysis tools can determine the existence of concealed secret information as well can detect steganography tool through which you concealed secret information in carrier file [1]. In [19], have concealed secret information through the use of existing steganography tools. The author also provided a comparison between various image steganography techniques. After concealing secret information using steganography tools, steganalysis to detect the concealed information was also done. Continuing contribution to the research on steganalysis tools [20], has stated that steganography is used to conceal secret information during communication while Steganalysis tools detect the concealed secret information. A study of various open-source steganography tools was presented by the authors. A carrier file is the one that can carry secret information with itself. In [21], has delivered an acute review of steganalysis techniques existing to examine features of various stego media and analogous carrier media. They also gave a perfect representation of current development in steganography so as we could improve and invent appropriate steganalysis algorithms. Moving to the transform domain, [22] have developed the F5 algorithm which is a steganography tool offering high concealing capacity, resists against graphical and geometric attacks. F5 tool processes matrix encoding for increasing capacity of information concealing. They found that their tool is strong against some graphical and statistical attacks.

LSB is the simplest technique for concealing secret information in [23] the carrier file. have discussed experimentally various well-known steganalysis techniques for the LSB flipping method. To assess the effect of concealing through various steganalysis techniques, 20%, 50%, 70%, and 100% concealing rates were implemented. DCT techniques work in the transform domain providing better security and robustness to secret information. Authors in [24], have analyzed F5, PQ (Post Quantum Encryption Tool), and Outguess tools. They compared the robustness of these tools against different image processing attacks. SVM (Support Vector Machine) and NNP (Neural network processes) recognition tools are used for the extraction of sensitive features from the DCT domain. Their performance results show Outguess tool can bear image processing attacks as compared with F5 and PQ tools. introduced real-time image

steganalysis. They combined DNN (Deep Neural Network) and CNN (Convolutional Neural Network) techniques to detect concealed secret information. For multi-user scenarios, they analyzed a useful real-time image steganalysis function based on the outlier detection technique. Video steganography tools can conceal secret information in form of images and audio as well. In [25], authors have created an IMStego tool that requires java-based platform and conceals information in images using the LSB technique. IMStego tool provides good security and it is user-friendly with interactive GUI (Graphic User Interface). IMStego tool works well with BMP (Bitmap Images) and PNG (Portable Network Graphics) image format. Audio steganography tools are utilized in [26]. The author proposed an MP3 (Moving Picture Expert Group) audio steganalysis tool. They figure out that concealing secret information causes disturbance in an inherent correlation of quantized MDCT (Modified DCT) coefficients.

## 3. Metrics for Measuring Performance

The performance parameters measure the excellence of the output stego image. The utmost property of steganography tools is that third parties should not get suspicious about the presence of secret information. Another property of these tools is robustness which shows how the steganography tool fit resists extraction of concealed information. PSNR (Peak Signal to Noise Ratio) and SSIM (Structure Similarity Index Measure), Histogram, Entropy, and Frequency Spectrum are the techniques for measuring excellence of output stego image. MSE (Mean Square Error), PSNR, SSIM, Entropy and Histogram can be calculated by equation 1, 2, 3, 4, and 5 respectively as follows in [27]:

*3.1 MSE:* In the case of MSE, signals are matched pixel by pixel starting from left to right and top to bottom over several rows and columns. MSE is the average of the square of the difference between the original and test image. MSE is simple to calculate and it is parameter independent [28].

$$\mathrm{MSE} = \frac{1}{n}\sum_{i=0}^{i=n}[I(i) - J(i)]^2 \qquad \text{... eq. 1}$$

I(i)=Carrier File,and

J(i)=Stego File

*3.2 PSNR:* It is an engineering term for the ratio between the maximum possible power of a signal and the noise is the error introduced by compression the power of corrupting noise that affects the fidelity of its representation. PSNR is usually expressed in terms of the logarithmic decibel scale [29].

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{\mathrm{MAX}_I^2}{\mathrm{MSE}}\right) \qquad \text{... eq. 2}$$

MAX_I=Maximum Possible Power of a signal,and

MSE=the power of corrupting noise

*3.3 SSIM:* It is a grouping of components: luminance comparison, contrast comparison, and structure comparison [20]. It is a newer quality metrics compared to PSNR and MSE. Several research reports state that SSIM performs relatively better than

its opponents [30].

$$SSIM(x,y) = \left[l(x,y)^{\alpha} \cdot c(x,y)^{\beta} \cdot s(x,y)^{\gamma}\right] \quad \text{... eq. 3}$$

l(x,y)=Luminance of samples x and y,

c(x,y)=Contrast of samples,and

s(x,y)=Structure of samples

α,β,γ denote the relative importance of each component

*3.4 Entropy:* The entropy of an image is average information produced from its pixel's values in [29]. It would be well-defined as a statistical measure of the unpredictability that may be used to describe the quality of that image.

$$E = -\sum_{0}^{N-1} p_k \log_2(p_k) \quad \text{... eq. 4}$$

Where N is the number of levels and $p_k$ is probability connected with level *k*. The maximum value of entropy is achieved when probability distribution is uniform. In other words, if $N = 2^n$, then $p_k$ is constant and given by

$p_k = 1/N = 2^{-n}$

*3.5 Histogram:* A histogram is a graphical illustration of the distribution of statistical facts. It displays statistical facts using bars of different heights. Larger bars show that more statistical facts lie in that range [31].

$$Histogram = \frac{\sum_{i=1}^{n}(His(c) - His(s))^2}{\sum_{i=1}^{n} His(c)^2} \quad \text{... eq. 5}$$

Where His(c) and His(s) are histograms of original cover and corresponding stego respectively.

*3.6 Frequency Spectrum:* The spectrum is generated by the Fourier transform and is also called as frequency domain. It can spread both phase and amplitude of an image [32].

## 4. Image Steganography Tools

There exist many image steganography tools that enable the user to conceal information in the carrier image. All these tools should fulfill some requirements [8]:

a) Steganography tool must maintain the integrity of secret information even after it is extracted by a third-party user.

b) Output stego image should look similar to the carrier image.

c) Changes like editing, cropping, pivoting in output stego image should not affect concealed information.

d) Always accept that hackers may identify the existence of concealed secret information.

e) Steganography tool must be able to conceal secret information in any type of image format.

f) After concealing secret information file size should remain the same otherwise hackers may detect secret information.

The steganography tool will not be successful if a hacker suspects a carrier file [33]. While using these tools, one must guarantee whether the concealing algorithm used by these tools are prevailing all kinds of exposure by a hacker. A tool is said to be more reliable and successful if it prevents exposure of secret information concealed. Some of the image steganography tools are given below:

4.1 Xiao Steganography: This is an open-source window-based tool having a size of 2.14 MB. It was released on 4th July 2006. It is an image steganography tool used for concealing secret information in BMP images or WAV (Waveform Audio) archives [35].

How to use the Xiao Steganography tool:

• This tool is user friendly, load any BMP, GIF (Graphical Interchange Format), JPEG, JPG, PNG image, or WAV file to its interface.

• Add an image or wav file, which acts as secret information.

• It also supports encryption providing a double level of security.

• For encryption, the purpose selects any of the algorithms from RC4, Triple DES (Data encryption standard), DES, Triple DES 112, RC2 (Rivest Cipher), and for hashing SHA (Secure Hash Algorithm), MD4 (Message Digest), MD2, MD5.

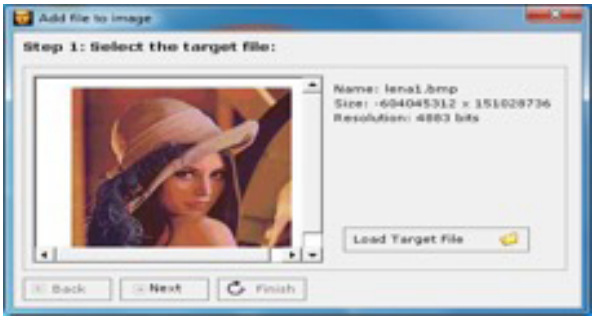
• After selecting any one of the encryption algorithms from the list save the target file.

• Then decode concealed secret information, after decoding it is visible to the user.

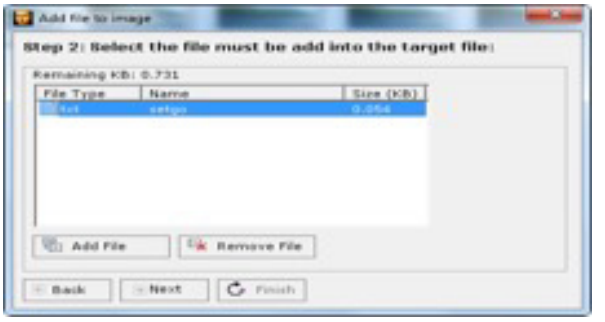
• This tool is available on Url: https://download.cnet.com/Xiao-Steganography/3000-2092_4-10535494.html.

The working of this tool is shown below in figure 3:

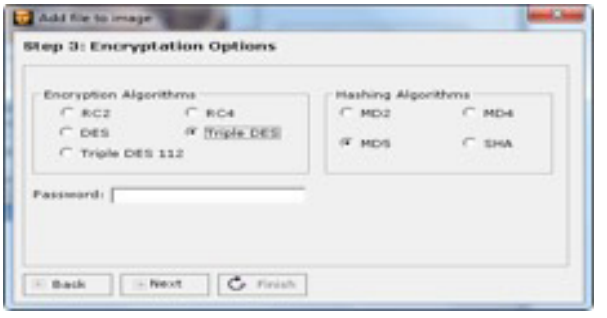
3(a) Target File



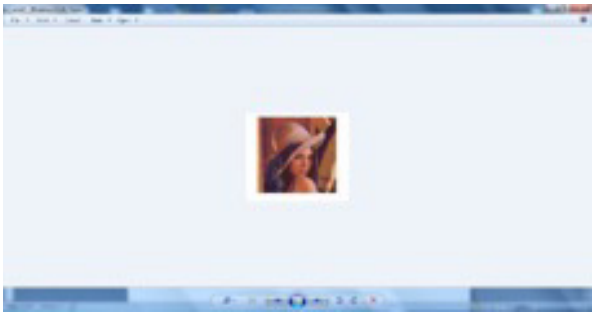

3(b) Secret File




3(c) Triple DES Encryption




3(d) Extracted File



*4.2 OpenStego:* This tool was released on 12th April 2007. Its size is 1.36 MB and compatible with Windows 2007. OpenStego tool is another good option for image steganography [36].

How to use the OpenStego tool:

• This is an open-source image steganography tool and developed on the Java platform.

• Images having format BMP, GIF, JPEG, JPG, PNG and WBMP (Wireless BMP) could be concealed with this tool.

• It always gives output in the form of JPG and PNG files only.

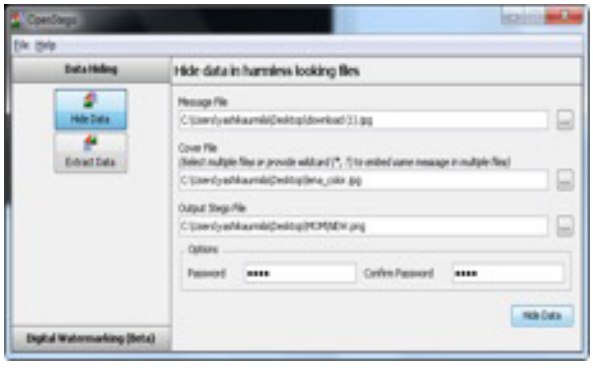
• For extraction of secret information this

tool requires a password resulting in a more secure process of concealing and decoding information.

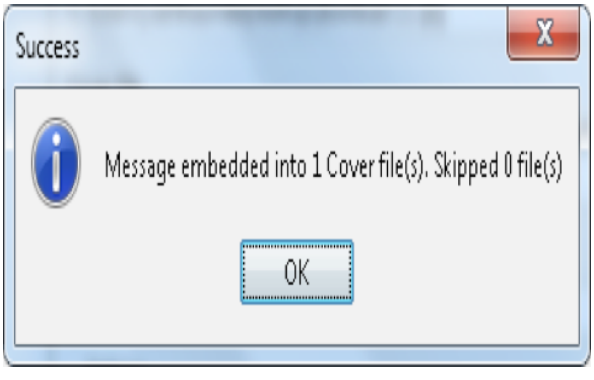
• It is available on the link: http://sourceforge.net/projects/openstego/files/.

The working of the OpenStego tool is shown below in figure 4:

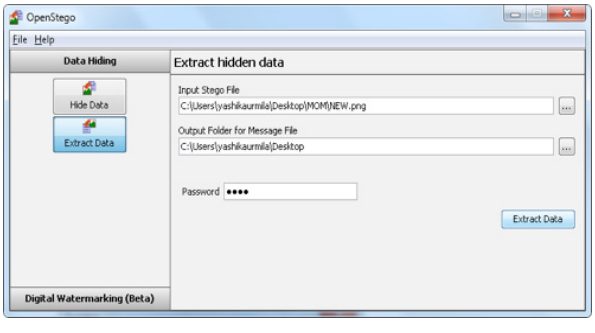
4(a) Source File




4(b) Secret File and Embedding




4(c) Extraction of File




4(d) File extracted successfully

Fig.4. Working of OpenStego Tool


*4.3 Hide'N'Send:* This tool was released on 29th May 2012 and is 530.09 KB in size. Specification for this tool is Windows 2007/XP/VISTA with .NET framework 2.0. This is a small and extremely simple image steganography tool for concealing any type of secret information behind JPEG images [37].

How to use this tool:

• Run the utility, select secret files, type of encryption algorithm, type of embedding algorithm, and type of hashing algorithms.

• For encryption purposes, any of the algorithms may be used: AES (Advanced Encryption Standard), RC4, RC2. The encryption key can be developed from the user password through the support of one of the subsequent hash functions: RIPEMD (RIPE message digest), SHA512, and MD5.

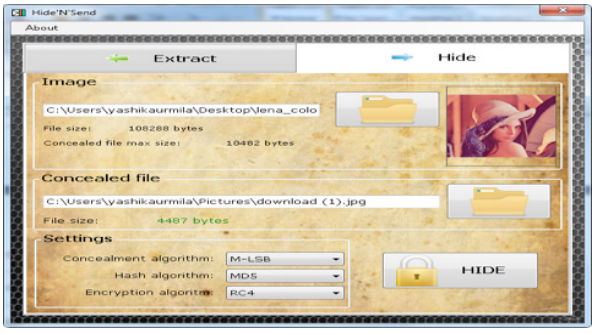
• Hide'N'Send tool uses recent steganography algorithms - F5 and LSB; select one among them by matrix coding. These algorithms conceal information directly inside the carrier image, instead of concealing in file structure as other popular tools do.

• After selecting encryption and embedding techniques click on the hide data button.

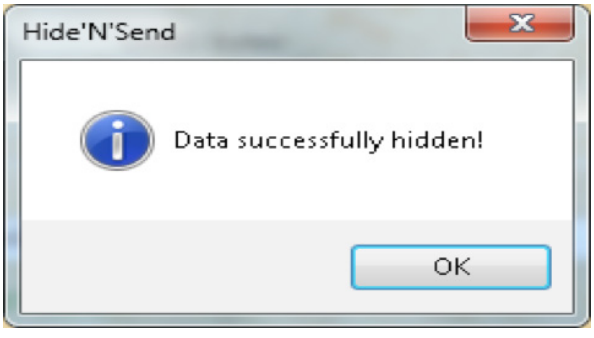
•This tool has just two tabs one for concealing secret information and the other for extraction of concealed information.

This tool is available on URL: https://www.softpedia.com/get/Security/Encrypting/Hide-N-Send.shtml. Working of Hide'N'Sendtoolisshownbelowin figure5:

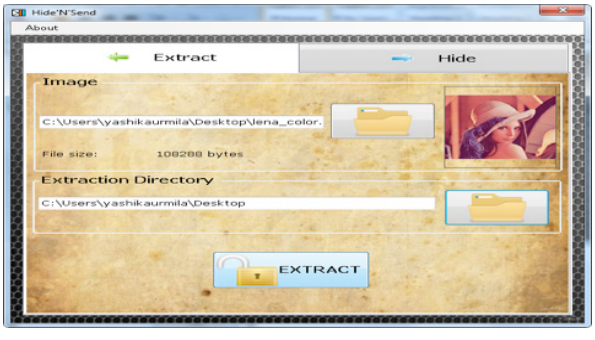
5(a) Embedding of Source File




5(b) Successfully Hidden

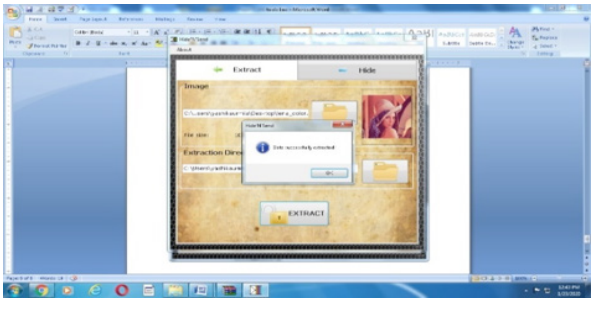



5(c) Extraction Process




5(d) Extracted Successfully

Fig.5. Working of Hide'N'Send Tool



4.4 OurSecret: This tool was released on 7th Dec 2016 and is 3.26 MB in size. Specification for this tool is Windows XP/2007. OurSecret is also an image steganography tool that is used to conceal secret information in the carrier image. Its interface has two parts, the first part conceals secret information and then another part extracts the concealed secret information [38].

How to use this tool:

• A carrier file is selected for concealing secret information by the user.

• Now secret information needs to be concealed inside the carry file. This tool is capable to conceal any type of digital multimedia information.

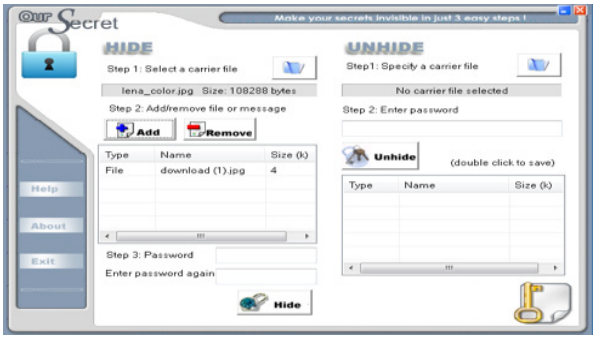
• This tool applies encryption on secret information and then conceals secret information in the carrier image.

• Secret information is extracted from the stegoimagebyclickingontheextractbutton.

This tool is available on URL: https://oursecret.soft112.com/.

The working of the OurSecret tool is shown below in figure 6:

6(a) Source File



6(b) Password Protection


6(c) Extraction of Secret Message


6(d) Extracted Secret Message

Fig.6. Working of OurSecret Tool


Table 1. Steganography Tools Comparison

| Tool Name | Concealed Data Type | Stego Image Properties | | Additional Information |
|---|---|---|---|---|
| | | Image Size (Increase by) | Output Image File | |
| Xiao Steganography | Any File Type | Remains Same | Any Type | Encryption Algorithm |
| **OpenStego** | **Any File Type** | **2 Time** | **PNG** | **Encryption, Compression, Password Protection** |
| HidenSend | Any File Type | Remains Same | JPG | Encryption Algorithm |
| OurSecret | Any File Type | 1 Time | JPG | Password Protection |

Open-source software permits operators to easily run, transform program as per their requirement, and also allow distributing replicas of the original version or their improved version. In Table 1 some open-source image steganography tools which are frequently used for concealing secret information are analyzed and compared. Information is listed year wisely according to the evolution of tools. It describes the comparison of tools based on image features like the type of cover image, the dimension of stego image, type of secret information, type of output image, the technique for concealing secret information, encryption support, hashing, data compression, etc. It has been found that OpenStego is one of the best tools among these four tools for concealing and extracting secret information. It can work efficiently with any image format without degradation in stego image quality. Carrier and secret image both are taken as JPG image, Stego image has PNG as well JPG format. This tool has the following properties:

• This tool uses 24-bit images because they offer good flexibility when used in steganography where they allow concealing more information than 8-bit images without disturbing the quality of carrier and stego images.

• This tool also provides password protection for concealing and extracting secret

information.

• Original and stego images are look similar in all aspects like color, size, contrast, intensity, and brightness, etc. So, no visual distortion may lead to the detection of secret information.

• Extracted secret information maintains its integrity when the key entered is correct.

• Concealing and extraction time for the secret image taken by this tool is small.

• It works on Windows platforms with a java environment.

• It works well with different image formats such as BMP, GIF, JPEG, JPG, PNG, and WBMP. Some of these formats are lossless like PNG, TIFF, and GIF so when image compression is required then information loss does not occur.

• Furthermore, some of the software tools used had restrictions for the format of the carrier images. These restrictions meant that the initial image had to be converted to a different format thus altering the quality of the stego image.

• This tool provides an interactive GUI.

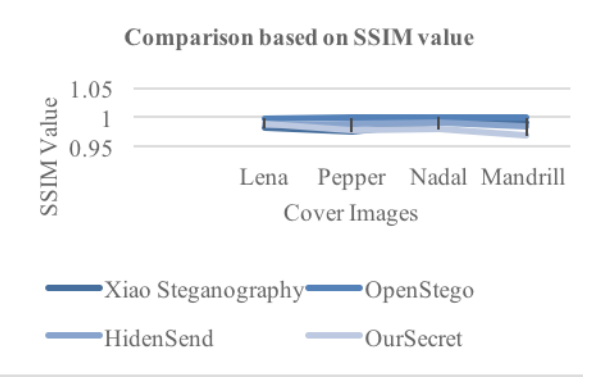
## 5. Results and Observations

Image steganography tools namely Xiao steganography, OpenStego, Hide'N'Send, and OurSecret are studied and compared their performance. By taking four different carrier images ("Lena", "Pepper", "Nadal" and "Mandrill") concealed secret information in the form of text. Imatest 4.5.13 is used to calculate SSIM and PSNR value of different stego images. Entropy, Histogram, and Frequency Spectrum are calculated in MATLAB. Different output stego images produced by the tools are compared by their SSIM, PSNR, Entropy, Histogram, and Frequency Spectrum. With the advancement in features of particular tool time and space complexity increases. Carrying more advanced features means need more memory to store. Time to complete the process of information concealing and retrieval also increases. Among the mentioned tools OpenStego has additional features so it is more complex compared to other tools.

Table 2 shows the SSIM values of steganography tools: Xiao, OpenStego, HidenSend, Oursecret. From the table one can observe that there are small variations in SSIM values of the tools discussed.

| Cover Image | Xiao Steganography | OpenStego | HidenSend | Our-Secret |
|---|---|---|---|---|
| Lena | .9812 | .9981 | .9867 | .9886 |
| Pepper | .9745 | .9988 | .9887 | .9776 |
| Nadal | .9911 | .9997 | .9913 | .9790 |
| Mandrill | .9899 | .9984 | .9851 | .9681 |

Fig.7. SSIM values




Mainly there are two approaches through which image quality can be evaluated: The objective method and the subjective method. The subjective method is the human finding method that is not based on the reference images. Whereas in the objective method mathematical comparisons

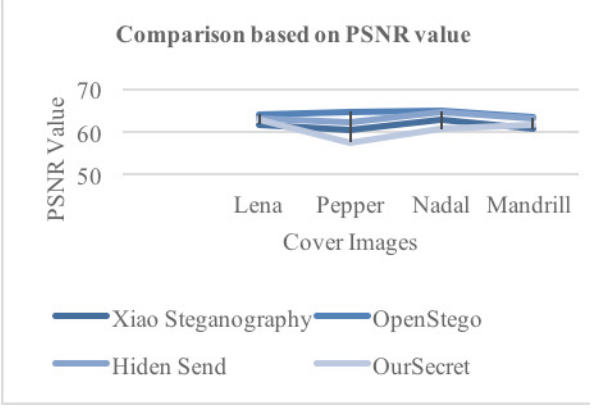
need to be done among reference image and distorted image. SSIM is a good metric to find the quality of original and stego images compared to PSNR matric. SSIM finds the similarity between the original carrier image and the stego image. Table 2 along with Figure 7, shows OpenStego tool represents the highest values of SSIM for all the inputted images. This tool gives SSIM very close to 1. SSIM value 1 means the original carrier image and stego image are almost similar in all aspects. Change in brightness and contrast of the image is not an effective element to SSIM.

Table 3. Comparison of PSNR values

| Cover Image | Xiao Steganography | OpenStego | HidenSend | OurSecret |
|---|---|---|---|---|
| Lena | 61.73 | 64.04 | 63.23 | 62.77 |
| Pepper | 60.56 | 64.71 | 62.27 | 57.56 |
| Nadal | 62.71 | 64.89 | 64.61 | 60.71 |
| Mandrill | 60.68 | 63.27 | 63.23 | 61.68 |

Table 3 along with Figure 8, shows the PSNR value of all the four steganography tools for same images.

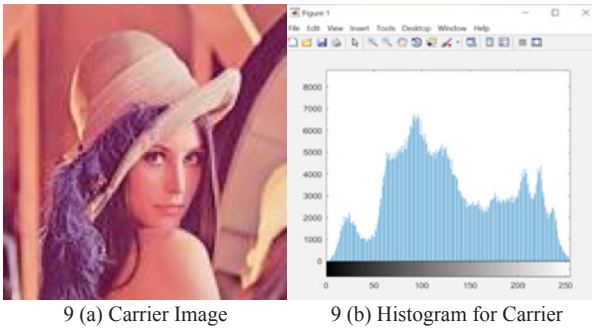
Fig.8. PSNR values




The highest value of PSNR means the OpenStego tool is better among all the four tools. A PSNR value greater than 35 shows the good quality of the output stego file [34]. PSNR compares the original secret image to the extracted secret image. PSNR is generally communicated in terms of the logarithmic decibel scale. Change in brightness and contrast of the image is a very effective element to PSNR.

Figure 9 and 10 shows the comparison of original carrier image with stego image based on histogram values. The difference can be recognized by a change in the frequency of histogram values.

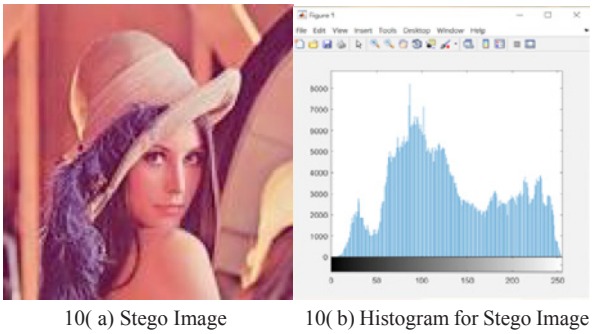
Fig.9. Histogram for Carrier Image



9 (a) Carrier Image

9 (b) Histogram for Carrier Image

Fig.10. Histogram for Stego Image



10( a) Stego Image

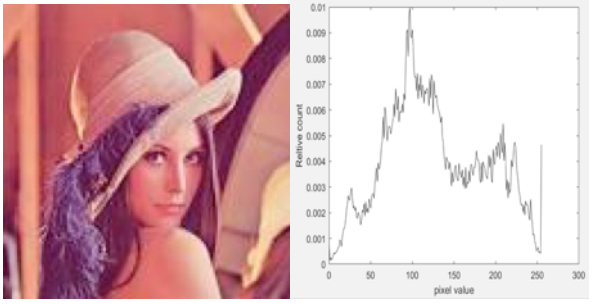
10( b) Histogram for Stego Image

By comparing the histogram of carrier and stego image in Figure 9 and 10 respectively what we can see is there is a negligible change that can be neglected by naked human eyes. The histogram is used to see the distribution of information for checking whether a process change occurred from one time period to another. If there is slight or no change in information distribution of

carrier and stego image then we can say our steganography tool is robust.

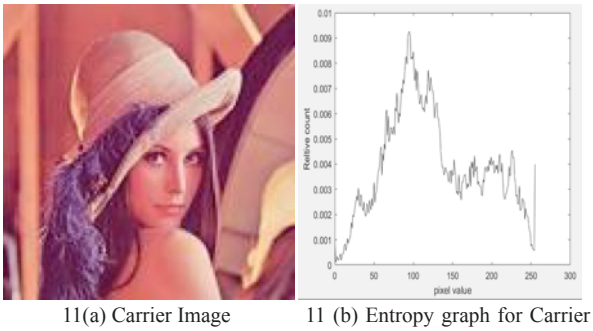
Entropy could be defined as the disorder or status of the concentration level of specific pixels in an image. Entropy efficiently analyzes an image/frame in a video. It quantitatively analyzes and evaluates individual image details. In steganography, entropy can identify the texture, contrast, color, brightness, etc. of an image. As disorder in an image increases entropy increases and can be easily identified by the hacker.

Fig.11. Entropy before Concealing Secret Information




11(a) Carrier Image 11 (b) Entropy graph for Carrier Image

Fig.11. Entropy before Concealing Secret Information




11(a) Carrier Image 11 (b) Entropy graph for Carrier Image

The entropy of carrier image and stego image is calculated in MATLAB and there is a small variation that is even not noticeable. Carrier image and stego image are shown in Figures 11 and 12 respectively along with their entropy graph. From the experimental result entropy of the carrier image was found to be 7.77774 and for the stego image frame are 7.78416.

Spectrum signifies how pixels are changing in terms of color, intensity, contrast, etc. in both amplitude and phase.

Fig.13. Frequency Spectrum before Concealing of Secret Information


13(a) Carrier image 13(b)Frequency Spectrum graph for carrier image

Fig.14. Frequency Spectrum after Concealing of Secret Information


14(a)Stego Image 14(b) Frequency Spectrum graph for Stego Image

The frequency spectrum of carrier image and stego image is calculated in MATLAB and there is a small variation that is even not noticeable. Carrier image and stego image are shown in Figures 13 and 14 respectively along with their spectrum graph.

## 6. Conclusion

This paper presents a comparative analysis of open-source steganography tools based on image features like the type of carrier image, dimension of stego image, type of secret information, type of output image,

the technique for concealing secret information, encryption support, hashing, data compression, etc. to the provides-depth assessment of tools. The realization of this study is to recognize the consistent and best tool accessible in the market for image steganography. Some of the basic tools existing in the market were chosen based on their frequent use; these tools were tried using the same input. Experimental results expose that all four tools were comparatively performing at the same level; however, some software achieves better than others. Out of all the above four image steganography tools used for comparison, ―OpenStego image steganography tool was considered to be the most efficient one because of good SSIM and PSNR values. Histogram, entropy, and spectrum graph are also drawn in MATLAB to compare the quality of the stego image from the original image. In the case of OpenStego steganography tool file has advantages over all the other tools in that it supports all the image formats and does not change the image features as well as does not reflect the visible changes. For improved information security, we inspire more researchers to pay effort on steganalysis as future scope.

**References:**

[1] M. Hofmann, "A comparative analysis of steganographic tools," Technology, no. October, 2007.

[2] V. Bhasin, P. Bedi, A. Goel, and S. Gupta, "StegTrack," pp. 318–323, 2015, doi: 10.1145/2791405.2791451.

[3] F. Djebbar, B. Ayad, K. A. Meraim, and H. Hamam, "Comparative study of digital audio steganography techniques," Eurasip J. Audio, Speech, Music Process., vol. 2012, no. 1, pp. 1–16, 2012, doi: 10.1186/1687-4722-2012-25.

[4] R. Mudusu, A. Nagesh, and M. Sadanandam, "Enhancing Data Security Using Audio-Video Steganography," Int. J. Eng. Technol., vol. 7, no. 2.20, p. 276, 2018, doi: 10.14419/ijet.v7i2.20.14777.

[5] R. Jarusek, E. Volna, and M. Kotyrba, "Robust steganographic method based on unconventional approach of neural networks," Appl. Soft Comput. J., vol. 67, pp. 505–518, 2018, doi: 10.1016/j.asoc.2018.03.023.

[6] H. T. Sencar, "Performance study of common image steganography and steganalysis techniques," J. Electron. Imaging, vol. 15, no. 4, p. 041104, 2006, doi: 10.1117/1.2400672.

[7] I. Banerjee, S. Bhattacharyya, and G. Sanyal, "Study and Analysis of Text Steganography Tools," Int. J. Comput. Netw. Inf. Secur., vol. 5, no. 12, pp. 45–52, 2013, doi: 10.5815/ijcnis.2013.12.06.

[8] R. Roy, S. Changder, A. Sarkar, and N. C. Debnath, "Evaluating image steganography techniques: Future research challenges," 2013 Int. Conf. Comput. Manag. Telecommun. ComManTel 2013, pp. 309–314, 2013, doi: 10.1109/ComManTel.2013.6482411.

[9] M. Chen, R. Zhang, X. Niu, and Y. Yang, "Analysis of current steganography tools: Classifications & features," Proc.

- 2006 Int. Conf. Intell. Inf. Hiding Multimed. Signal Process. IIH-MSP 2006, no. October, pp. 384–388, 2006, doi: 10.1109/IIH-MSP.2006.265023.

[10] R. Zax and F. Adelstein, "FAUST: Forensic artifacts of uninstalled steganography tools," Digit. Investig., vol. 6, no. 1–2, pp. 25–38, 2009, doi: 10.1016/j.diin.2009.02.002.

[11] T. Sloan and J. Hernandez-Castro, "Forensic analysis of video steganography tools," PeerJ Comput. Sci., vol. 2015, no. 5, pp. 1–16, 2015, doi: 10.7717/peerj-cs.7.

[12] H. Arif and H. Hajjdiab, "A comparision between steganography software tools," Proc. - 16th IEEE/ACIS Int. Conf. Comput. Inf. Sci. ICIS 2017, pp. 423–428, 2017, doi: 10.1109/ICIS.2017.7960030.

[13] L. L. Dominic, "Compress-Encrypt Video Steganography," vol. 1, no. 11, pp. 317–321, 2015.

[14] R. Das and I. Karadogan, "An Investigation on Information Hiding Tools for Steganography," Int. J. Inf. Secur. Sci., vol. 3, no. 3, pp. 200–208, 2014.

[15] J. Peddie and J. Peddie, "Software Tools and Technologies," Augment. Real., pp. 165–182, 2017, doi: 10.1007/978-3-319-54502-8_7.

[16] L. Y. Por, W. K. Lai, Z. Alireza, T. F. Ang, M. T. Su, and B. Delina, "StegCure: A comprehensive steganographic tool using enhanced LSB scheme," WSEAS Trans. Comput., vol. 7, no. 8, pp. 1309–1318, 2008.

[17] L. K. Gupta, A. Singh, V. K. Yadav, and A. Srivastava, "Performance Analysis of Open Puff Steganography Tool Using Various Image Formats," SSRN Electron. J., no. March, 2020, doi: 10.2139/ssrn.3550941.

[18] D. Uljarević, M. Veinović, G. Kunjadić, and D. Tepšić, "A new way of covert communication by steganography via JPEG images within a Microsoft Word document," Multimed. Syst., vol. 23, no. 3, pp. 333–341, 2017, doi: 10.1007/s00530-015-0492-3.

[19] S. Atawneh, A. Almomani, and P. Sumari, "Steganography in digital images: Common approaches and tools," IETE Tech. Rev. (Institution Electron. Telecommun. Eng. India), vol. 30, no. 4, pp. 344–358, 2013, doi: 10.4103/0256-4602.116724.

[20] D. Kundu and A. Upreti, "Study of Various Steganography Tools," 2018 Int. Conf. Autom. Comput. Eng. ICACE 2018, pp. 117–120, 2018, doi: 10.1109/ICACE.2018.8687092.

[21] A. Kolakalur, I. Kagalidis, and B. Vuksanovic, "Wavelet Based Color Video Steganography," Int. J. Eng. Technol., vol. 8, no. 3, pp. 165–169, 2016, doi: 10.7763/ijet.2016.v6.878.

[22] A. Westfeld, "F5 — A Steganographic Algorithm High Capacity Despite Better Steganalysis," pp. 289–302, 2001.

[23] A. Rashid and M. K. Rahim, "Scrutiny of Steganalysis for Flipping Steganography Method," J. Adv. Math. Comput. Sci., vol. 31, no. 5, pp. 1–18, 2019, doi:

10.9734/jamcs/2019/v31i530124.

[24] F. Ruan, X. Zhang, D. Zhu, Z. Xu, S. Wan, and L. Qi, "Deep learning for real-time image steganalysis: a survey," J. Real-Time Image Process., vol. 17, no. 1, pp. 149–160, 2020, doi: 10.1007/s11554-019-00915-5.

[25] S. A. El_Rahman, "A Comprehensive Image Steganography Tool using LSB Scheme," Int. J. Image, Graph. Signal Process., vol. 7, no. 6, pp. 10–18, 2015, doi: 10.5815/ijigsp.2015.06.02.

[26] C. Jin, R. Wang, and D. Yan, "Steganalysis of MP3Stego with low embedding-rate using Markov feature," Multimed. Tools Appl., vol. 76, no. 5, pp. 6143–6158, 2017, doi: 10.1007/s11042-016-3264-y.

[27] U. Sara, M. Akter, and M. S. Uddin, "Image Quality Assessment through FSIM, SSIM, MSE and PSNR—A Comparative Study," J. Comput. Commun., vol. 07, no. 03, pp. 8–18, 2019, doi: 10.4236/jcc.2019.73002.

[28] P. Nithyanandam, T. Ravichandran, E. Priyadharshini, and N. M. Santron, "An image steganography for colour images using lossless compression technique," Int. J. Comput. Sci. Eng., vol. 7, no. 3, pp. 194–205, 2012, doi: 10.1504/IJCSE.2012.048235.

[29] K. Kaur and B. Kaur, "DWT-LSB Approach for Video Steganography using Artificial Neural Network," pp. 20–25, 2018, doi: 10.17148/IARJSET.2018.574.

[30] A. Zaric, M. Loncaric, D. Tralic, M. Brzica, E. Dumic, and S. Grgic, "Image quality assessment - Comparison of objective measures with results of subjective test," Proc. Elmar - Int. Symp. Electron. Mar., no. October 2014, pp. 113–118, 2010.

[31] S. K. Yadav and R. K. Bhogal, "A video steganography in spatial, discrete wavelet transform and integer wavelet domain," Proc. - 2nd Int. Conf. Intell. Circuits Syst. ICICS 2018, pp. 265–270, 2018, doi: 10.1109/ICICS.2018.00060.

[32] N. D. Jambhekar, C. A. Dhawale, and R. Hegadi, "Performance analysis of digital image steganographic algorithm," ACM Int. Conf. Proceeding Ser., vol. 11-16-Nove, no. December 2017, 2014, doi: 10.1145/2677855.2677937.

[33] M. S. Subhedar and V. H. Mankar, "Current status and key issues in image steganography: A survey," Comput. Sci. Rev., vol. 13–14, no. C, pp. 95–113, 2014, doi: 10.1016/j.cosrev.2014.09.001.

[34] D. Beh, M. Yin, M. Mahari, and S. Omar, "SilentSecrecy : A Hybrid Steganographic Scheme to Conceal Information .," no. May, pp. 256–259, 2016.

[35] Web URL: https://download.cnet.com/Xiao-Steganography/3000-2092_4-10535494.html, Publisher: DB Software Laboratory, Last edit: 29-06-2006, Last access: 07-08-2020.

[36] Web URL:http://sourceforge.net/projects/openstego/files/ , Developer: Syvaidya, Last update: 17-04-2014, Last access: 08-08-2020.

[37] WebURL: https://www.softpedia.com/get/Security/Encrypting/Hide-N-Send.shtml, Developer: MRP Labs, Last update: 03-04-2014, Last access: 08-08-2020.

[38] Web URL: https://oursecret.soft112.com/, Publisher: Securekit.net, Last update: 17-04-2013, Last access: 09-08-2020.