International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048
Volume 7, Issue 12, pp 182-188, December-2023
https://doi.org/10.47001/IRJIET/2023.712026

Utilizing the Most Recent App for Confidential Communication in the Local Area Network

[1]Raqiya Saud Ahmed Al Harthi, [2]Braah Mubarak Al-Dhafri, [3]Dr. Ramesh Palanisamy

[1,2]Student, Department of Information Technology, University of Technology and Applied Sciences – Ibra, Sultanate of Oman
[3]Lecturer, Department of Information Technology, University of Technology and Applied Sciences – Ibra, Sultanate of Oman
Authors Name: [1]36J185@utas.edu.om, [2]36s1884@utas.edu.om, [3]ramesh.palanisamy@utas.edu.om

***Abstract* - The technique known as steganography involves hiding information within the information of others in order to mask the fact that communication is taking place. Nonetheless, digital photos are the most widely used carrier format because of their widespread availability online. A photo contains a lot of sensitive steganography data. While some are more complex and powerful than others, they all have their strengths and weaknesses. Depending on the application, the steganography technology used must adhere to certain specifications. For example, some applications might require that the secret data be hidden completely, while others might require that a more significant secret message be hidden. The objective of this project is to present an overview of the techniques and applications of image steganography. Additionally, it attempts to clarify what constitutes a good steganography.**

Keywords: Steganography, Taxonomy, Image Hiding, Current Techniques, Adaptive Steganography, Encryption and Decryption.

1. Introduction

Since the creation of the Internet, information security has emerged as one of the most important aspects of communication and information technology. Several methods for encrypting and decrypting data have been developed in order to safeguard the confidentiality of communications, which is the goal of cryptography. Unfortunately, there are times when protecting a message's contents alone isn't enough—it might also be necessary to protect the message's existence. The implementation technique used for this is known as steganography. Steganography is the science and art of undetectable communication. This is accomplished by blending the sent information into other data, thereby hiding its existence. Greek terms "stegos," which means "cover," and "grafia," which means "writing," are the source of the term "covered writing" (steganography) [1]. Only images utilizing image steganography have information hidden.

Message secrecy is a key component of steganography, while message confidentiality is a key component of cryptography [2]. Although none of the technologies is infallible and can be compromised, steganography and cryptography are two techniques that help protect data from unauthorized access. Once the existence of hidden information is found, or even suspected, the purpose of steganography is partially compromised [2]. Because of this, combining cryptography and steganography can make it more efficient.

Security flaws in cryptography have been the main driving force behind steganography research. It has become necessary for researchers to investigate alternative secure information transport techniques because many countries have passed laws that weaken or outright prohibit cryptographic systems [3]. Businesses now know that steganography is useful for transmitting information about upcoming goods or proprietary information. By not communicating via recognized channels, the chance of information being leaked while in transit is greatly decreased [4]. Compared to sending an encrypted file, hiding information in a photo from the office picnic is less suspicious.

This study aims to provide a state-of-the-art review of the various algorithms used for image steganography in order to demonstrate the security potential of steganography for both personal and professional use. After the summary, a brief discussion of how various image steganography techniques serve various objectives follows. Our standards for image steganography serve as the foundation for this analysis [5].

2. Literature Review

Images are thought to be the most frequently used file types in steganography, as was previously mentioned. They are well known for being non-causal media because any random pixel in the image can be accessed. Furthermore, the hidden data might not be visible to the unaided eye at all. Nevertheless, the image steganography method will take advantage of "gaps" in the HVS (human vision system).

It is possible to reconstruct the original data from the compressed data because this method will never cause the loss of original image information. [9] is an image in the BMP and GIF formats.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 12, pp 182-188, December-2023

https://doi.org/10.47001/IRJIET/2023.712026

The definition of "covered writing" for the term steganography is given by Moerland (T) [12]. The word comes from the Greek words "stages," which means "cover," and "graphic," which means "writing."

The idea of hiding information is not new; it has been practiced for a very long time. Greek historian Herodotus writes in his Histories about a nobleman called Histaeus who had to correspond with his son-in-law in Greece. He had the message permanently inked on the scalp of one of his most dependable slaves, who had had his head shaved. Once the slave's hair had grown back, the hidden letter was sent with them [Silman, J., 2001].

Steganography preserves a message's existence's confidentiality, while cryptography concentrates on protecting a message's contents [Wang, H., 2004]. Despite the fact that neither cryptography nor steganography is perfect and can be broken, they are both reliable ways to protect data from unwanted access. If hidden information is found, or even suspected to exist, it partially defeats the purpose of steganography [Wang, H., 2004]. Therefore, combining steganography with cryptography can make it stronger [12].

Patterson, R.J. (1998) points out that two more technologies that are closely related to steganography are fingerprinting and watermarking. The requirements for the algorithms are different from steganography because the main goal of these technologies is intellectual property protection.

These technologies are primarily concerned with protecting intellectual property, so their algorithmic needs differ from steganography's. These are the requirements of a good steganographic algorithm, and we will discuss them below. An object that has been watermarked is "marked" consistently all over. When watermarking an object, the type of information that is usually hidden is a signature that serves as a means of identifying ownership or origin for copyright purposes [Marvel, L.M., 1999].

The entirety of the original data should be kept; lossless compression is usually recommended. By doing this, it is possible to reconstruct the original data from the compressed data, ensuring that the original image data is never lost. BMP and GIF images share this characteristic [N.F. Johnson and S. Jajodia, 1998, Feb].

3. Proposed Solution

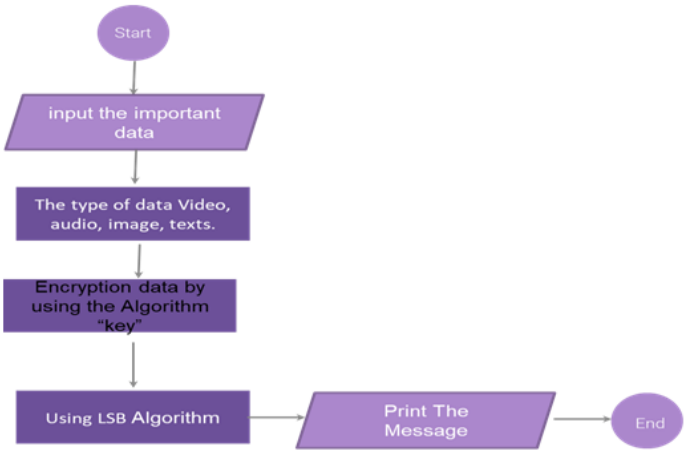
Steganography is a technique that hides sensitive or private information inside of what looks to be a regular picture. Steganography is the process of hiding text so that it seems to be a different file or a regular image. When someone looks at something that conceals information, they won't be aware that it's there. Since our senses aren't designed to look for files containing information, steganography takes advantage of human perception. With the help of this system, users can send text messages that are encased in picture files. Users input the text they want to send privately, upload the image [11], and then lock the text with a key or password. Even if hackers manage to access the text, they cannot read it because the key encrypts it.

Steganography Algorithm

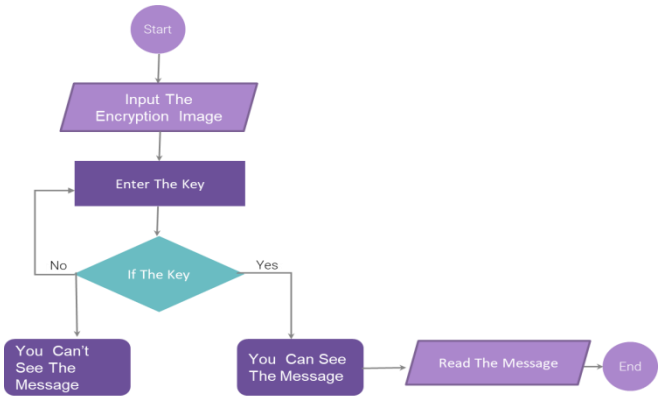
Least Significant Bit Substitution Technique (LSB)

- RSA Algorithm
- F5 Algorithms
- AES Algorithm

Flowchart

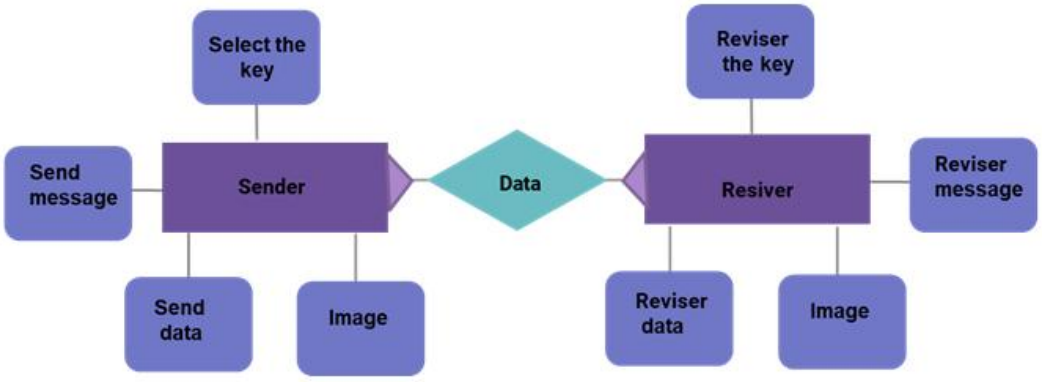


To encryption of the data.



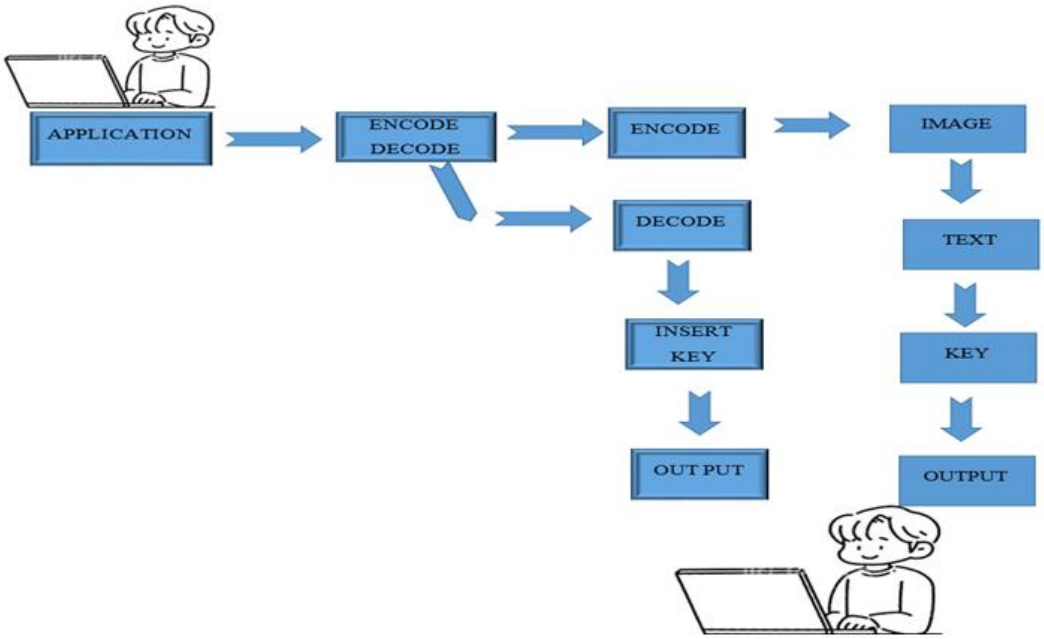
To decryption of the data.

International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 7, Issue 12, pp 182-188, December-2023
https://doi.org/10.47001/IRJIET/2023.712026



Entity-Relationship Diagram

Analysing and designing systems, including structured systems



Structured systems

4. Sample Program

```
import tkinter as tk
from tkinter import ttk
from tkinter import filedialog
class App(tk.Tk):
def __init__(self):
    super().__init__()
self.geometry("800x400")
self.title('Steganography Application')
```


International Research Journal of Innovations in Engineering and Technology (IRJIET)
ISSN (online): 2581-3048
Volume 7, Issue 12, pp 182-188, December-2023
https://doi.org/10.47001/IRJIET/2023.712026

```
self.resizable(0, 0)
        # configure the grid
self.columnconfigure(0, weight=1)
self.columnconfigure(1, weight=3)
self.create_widgets()
defcreate_widgets(self):
        label1 = ttk.Label(self, text="Steganography Application", font=('arial', 20))
        b1 = ttk.Button(self, text="ENCODE", command=self.encode)
        b2 = ttk.Button(self, text="DECODE", command=self.decode)
        b3 = ttk.Button(self, text="EXIT", command=self.destroy)
        label1.grid(column=1, row=0, sticky=tk.W, padx=5, pady=5)
        b1.grid(column=0, row=1, sticky=tk.E, padx=5, pady=5)
        b2.grid(column=1, row=1, sticky=tk.W, padx=5, pady=5)
        b3.grid(column=2, row=1, sticky=tk.W, padx=5, pady=5)
def encode(self):
defget_key():
            key = entry_key.get()
label_result.config(text=f"Key entered: {key}")
key_window.destroy()
defget_image():
image_path = filedialog.askopenfilename(initialdir="/", title="Select Image", filetypes=(
            ("Image files", "*.png;*.jpg;*.jpeg;*.gif"), ("all files", "*.*")))
label_result.config(text=f"Image selected: {image_path}")


        # Create the main window
main_window = tk.Tk()
main_window.title("Two Rounds Input")


        # Round 1: Insert Key
key_window = tk.Toplevel(main_window)
```


International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 12, pp 182-188, December-2023

https://doi.org/10.47001/IRJIET/2023.712026

```
key_window.title("Insert Key")
label_key = tk.Label(key_window, text="Enter Key:")
label_key.pack(pady=10)
entry_key = tk.Entry(key_window, show='*')  # Use show='*' to hide the entered characters (e.g., for a password)
entry_key.pack(pady=10)
button_key = tk.Button(key_window, text="Submit Key", command=get_key)
button_key.pack(pady=10)
    # Round 2: Insert Image
label_result = tk.Label(main_window, text="")
label_result.pack(pady=10)
button_image = tk.Button(main_window, text="select image", command=get_image)
button_image.pack(pady=10)
button_image = tk.Button(main_window, text="enter text", command=get_image)
button_image.pack(pady=10)
button_image = tk.Button(main_window, text="writ key", command=get_image)
button_image.pack(pady=10)
button_image = tk.Button(main_window, text="encoding", command=get_image)
button_image.pack(pady=10)
def decode(self):
defon_button_click():
user_input = entry.get()
print("User entered:", user_input)
defget_key():
        key = entry_key.get()
label_result.config(text=f"Key entered: {key}")
key_window.destroy()
defget_image():
image_path = filedialog.askopenfilename(initialdir="/", title="Select Image", filetypes=(
        ("Image files", "*.png;*.jpg;*.jpeg;*.gif"), ("all files", "*.*")))
label_result.config(text=f"Image selected: {image_path}")
```


International Research Journal of Innovations in Engineering and Technology (IRJIET)

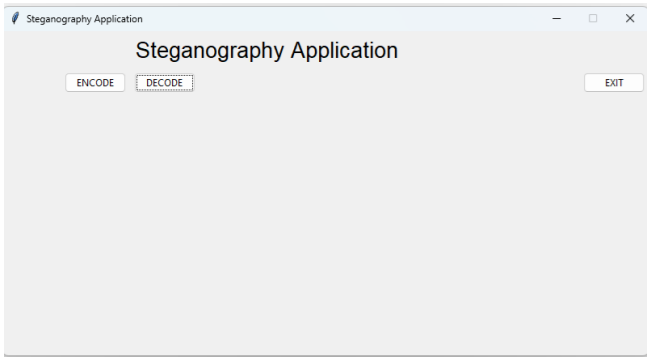
ISSN (online): 2581-3048

Volume 7, Issue 12, pp 182-188, December-2023

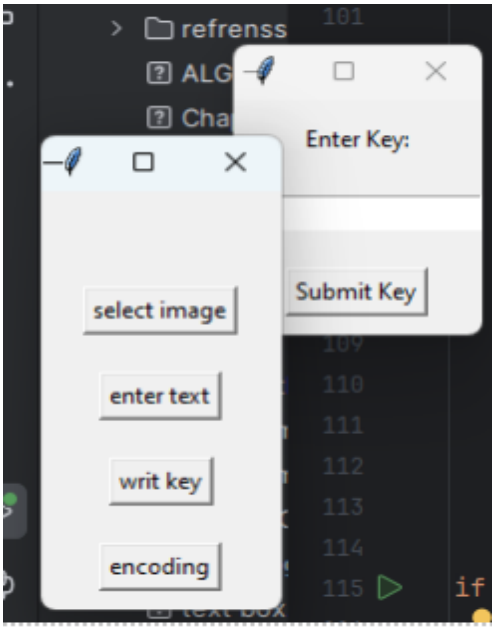
https://doi.org/10.47001/IRJIET/2023.712026

5. Result and Discussion

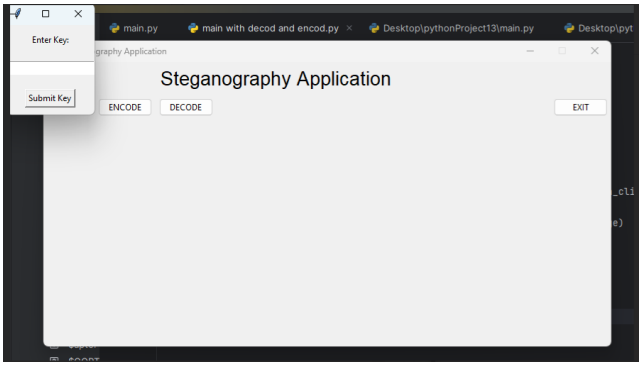
There exist a multitude of techniques for hiding information in photos, even though the scope of this research was limited to a small subset of the main image steganography methods. There are distinct methods for hiding messages in each of the major image file formats, each with pros and cons of their own. Whereas the other approach has a larger payload capacity, the first lacks robustness. One such technique is the patchwork approach, which can only hide a very small amount of data but is highly resistant to most attacks. In both BMP and GIF, this is offset by the least significant bit (LSB), but both methods result in files that are suspicious and are more likely to be discovered when a warden is around. An agent must decide which steganography algorithm to use based on the type of application he plans to use it for and whether he is willing to forgo some features in order to protect the security of others.



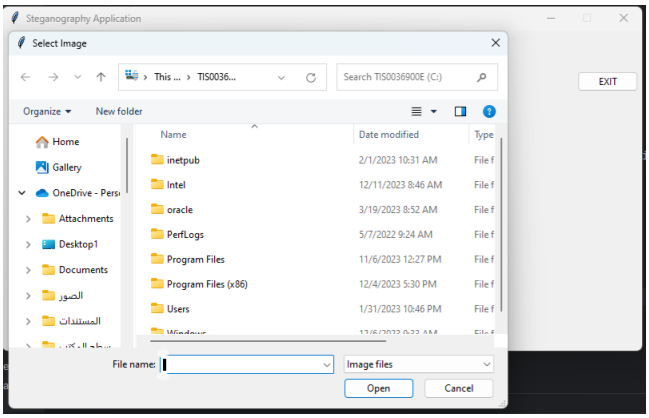
System Process 1 (encode or decode section)



System Process 2 (image selection)



System Process 3 (key enter)



System Process (path selection)

Sensitive or private information can be concealed inside an otherwise ordinary image using a technique called steganography. Text can be obscured to appear as a regular image or a separate file by using steganography. Reconstructing the original data from the compressed data is possible because this method will never lead to the loss of original image information. It's a BMP and GIF image here. AES, LSB, RSA, F5, and other steganography algorithms are among the many available. An algorithm called Least Significant Bits (LSB) is the most widely used steganography technique. The message gets embedded into the image file, which has three bytes of data for each pixel, using the LSB technique.

6. Conclusion

In order to conceal their existence, secrets are transferred using steganography under covers that appear innocent. Digital steganography and its offshoots are finding greater and greater uses. Steganography is appealing to some people as a covert means of enforcing rules and passing notes. Within this project, the definition of steganography, the range of algorithms that can be used, and the best algorithm to use were all studied.

ISSN (online): 2581-3048
Volume 7, Issue 12, pp 182-188, December-2023
https://doi.org/10.47001/IRJIET/2023.712026

REFERENCES

[1] Moerland, T., "Steganography and Steganalysis", Leiden Institute of Advanced Computing Science, www.liacs.nl/home/ tmoerl/privtech.pdf

[2] Wang, H & Wang, S, "Cyber warfare: Steganography vs. Steganalysis", Communications of the ACM, 47:10, October 2004.

[3] Dunbar, B., "Steganographic techniques and their use in an Open-Systems environment", SANS Institute, January 2002.

[4] Artz, D., "Digital Steganography: Hiding Data within Data", IEEE Internet Computing Journal, June 2001.

[5] N.F. Johnson and S. Jajodia. (1998, Feb.). "Exploring steganography: seeing the unseen." IEEE Computer Journal. [On line]. 31(2), pp. 26-34. Available: http://www.jjtc.com/pub/r2026.pdf [Jun. 2011].

[6] Aldawood, H. and Skinner, G. (2019) "Reviewing cyber security social engineering training and awareness programs—pitfalls and ongoing issues," Future Internet, 11(3), p. 73. Available at: https://doi.org/10.3390/fi11030073.

[7] Silman, J., "Steganography and Steganalysis: An Overview", SANS Institute, 2001.

[8] Anderson, R.J. & Petitcolas, F.A.P., "On the limits of steganography", IEEE Journal of selected Areas in Communications, May 1998.

[9] Marvel, L.M., Boncelet Jr., C.G. &Retter, C., "Spread Spectrum Steganography", IEEE Transactions on image processing, 8:08, 1999.

[10] N.F. Johnson and S. Jajodia. (1998, Feb.). "Exploring steganography: seeing the unseen." IEEE Computer Journal. [On line]. 31(2), pp. 26-34. Available: http://www.jjtc.com/pub/r2026.pdf [Jun. 2011].

[11] Secure binary image steganography using F5 algorithm based on data ... (n.d.). Retrieved April 30, 2023, from https://www.researchgate.net/publication/309068311_Secure_binary_image_steganography_using_F5_algorithm_based_on_data_hiding_and_diffusion_techniques

[12] H. Yang and A. C. Kot, "Pattern-based data hiding for binary image authentication by connectivity-preserving," IEEE Transactions on Multimedia,vol. 9, no. 3, pp. 475–486, 2007.

[13] R.Poornima, R.J.Iswarya, "An Overview of Digital Image Steganography", International Journal of Computer Science & Engineering Survey (Vol.4, No 1), February 2013.

[14] Cachin, C.: An Information-Theoretic Model for Steganography. In: Aucsmith D. (eds.):Information Hiding: 2nd International Workshop. Lecture Notes in Computer Science, Vol.1525. Springer-Verlag, Berlin Heidelberg New York (1998) 306–318.

[15] Chandramouli, R. and Memon, N.: Analysis of LSB Based Image SteganographyTechniques. Proceedings of ICIP 2001 (CD version). Thessaloniki, Greece (2001).

[16] Fridrich, J., Goljan, M., and Du, R.: Detecting LSB Steganography in Color and GrayscaleImages. Magazine of IEEE Multimedia: Special Issue on Security, Vol. Oct-Dec (2001) 22–28.

[17] Katzenbeisser, S. and Petitcolas, F.A.P.: On Defining Security in SteganographicSystems.Proceedings of SPIE: Electronic Imaging 2002, Security and Watermarking of MultimediaContents, Vol. 4675. San Jose, California (2002).

[18] Anderson, R.J. and Petitcolas, F.A.P.: On the Limits of Steganography. IEEE Journal of Selected Areas in Communications: Special Issue on Copyright and Privacy Protection), Vol. 16(4) (1998) 474"481.

[19] T. Filler, J. Judas, and J. J. Fridrich, "Minimizing additive distortion in steganography using syndrome-trellis codes," IEEE Transactions on Information Forensics and Security, vol. 6, no. 3, pp. 920–935, Sept. 2011.

Citation of this Article:

Raqiya Saud Ahmed Al Harthi, Braah Mubarak Al-Dhafri, Dr. Ramesh Palanisamy, "Utilizing the Most Recent App for Confidential Communication in the Local Area Network" Published in *International Research Journal of Innovations in Engineering and Technology - IRJIET*, Volume 7, Issue 12, pp 182-188, December 2023. Article DOI https://doi.org/10.47001/IRJIET/2023.712026

****

