Journal of Advances and Scholarly Researches in Allied Education
Vol. 19, Issue No. 5, October-2022, ISSN 2230-7540

Recent advances for hiding content in image Steganography

Amjad Khan[1]*, Ali Akhtar[2], Zafrul Hasan[3], Mohammad Serajuddin[4]

[1] Researcher, Prince Sultan Bin Abdulaziz College for Emergency Medical Services King Saud University, Riyadh

[2] Researcher, College of Pharmacy, King Saud University, Riyadh

[3] Researcher, College of Nursing, King Saud University, Riyadh

[4] Researcher,College of Dentistry, King Saud University, Riyadh

Abstract - This paper's primary objective is to investigate and describe the several deep learning approaches currently used for picture steganography. Traditional approaches, The most common deep learning approaches for photo steganography are convolutional neural network (CNN) based methods and generative adversarial network (GAN) based methods. The authors of this work set out to aid their fellow researchers by gathering pertinent data on the most recent developments, difficulties, and potential future directions in this area. The pictures to be concealed are embedded by first transforming the cover image to luminance and chrominance components. An excellent example of the class of permutation-based algorithms that may better survive channel degradations is the chaotic Baker map, which is used to encrypt the secret pictures. In this study, an OFDM system with channel equalization was used for wireless communication.

Keywords - Steganography, OFDM, equalization, Authenticity, Communication

--------------------------------- x --------------------------------

INTRODUCTION

Steganography is the practice of concealing data. Steganography may also refer to "secret writing," another name for the practice. When it comes to encryption, attackers are more likely to focus on the most readily apparent encrypted information, regardless of how secure it is. Steganography is preferable to cryptography because it reduces the likelihood that the presence of secret information will be detected. Stego media refers to media that contains hidden messages, whereas cover media refers to media that is used to conceal communications but does not itself conceal any information. To avoid leaking sensitive data, attackers use steganalysis methods. To avoid raising suspicion from an eavesdropper, a steganographic system conceals information under seemingly innocuous cover medium. It is possible to insert text into other media types, such as images and audio files. Cryptography, on the other hand, is the study of mathematical approaches for ensuring things like privacy, reliability, authenticity, and correct data creation.

Cryptography and steganography function well together in the realm of Network Security. The existence of the communication is concealed, as opposed to only its contents, which is what cryptography does. It's also quite different from watermarking. Although watermarking protects against tampering with or deletion of data, it has no effect on the data's continued existence. However, Steganography's primary struggle is for survival.

LITERATURE REVIEW

Mohammed Abdul Majeed et.al (2021) An ongoing need to protect records and the information they contain has arisen, whether those records are paper or digital. This is due to the fact that document forgery and counterfeiting are widespread worldwide, endangering not just national security but also the financial well-being of people, communities, and whole industries. Since this is a problem, people are thinking about ways to safeguard their creations and prevent infringement. Steganography, cryptography, and encoding are just a few of the methods used to safeguard sensitive data. One such approach is steganography, when information is secretly sent by embedding it into another message (cover media). Cover material including films, photos, and sounds are often used in steganography studies. Because it's so hard to spot duplicate bits in a text file, steganography using text is often overlooked. Altering a document's properties allows you to insert data into it. These features might be intentionally misspelled words or phrases, resized typefaces, or hidden characters. However, due to the tiny modification in the document, an attacker or other third party would be able to tell. To fix this, the document has to be altered in a way that is undetectable to the naked eye yet accessible to a computer for decoding. A survey of the relevant literature is presented here. We begin with a primer on what text steganography is and how it works in general. Each category's associated methods are dissected, and a special emphasis is placed on the way in which a novel method of concealing sensitive information is presented. In addition, we survey the literature on text steganography, including works published between 2016 and 2021, focusing on the development of techniques and algorithms. This work seeks to aid other researchers by gathering the existing approaches, problems, and future directions in this subject.

B. Chitradevi et.al (2020) If you want to send sensitive information without raising suspicion, you may use a method called steganography, which entails concealing it inside a seemingly innocuous file or message and then retrieving it once it reaches its intended recipient. Steganography may be used in tandem with encryption to further conceal and safeguard sensitive information. The Greek terms steganos and the Greek root graph (writing) combine to get the word steganography (write). To communicate secretly, steganography was developed. The picture is altered in such a manner that only the sender and the recipient will be able to see the message. Secret information is difficult to discover because it is unseen.

Swati Bhargava et.al (2019) In this day and age, when new technological advancements are constantly being developed, safety must be given first attention. Steganography and other cryptographic methods are only two of the many methods used to conceal information in files. Image encryption using LSB bits, DWT, and the RSA method is presented in this article. The research also introduces novel approaches that combine encryption and steganography to obfuscate data and conceal knowledge using picture processing (IP). The hidden image may be concealed inside another image using LSB bits and DWT techniques. When the RSA algorithm is used, utilising the recipient's public key, the secret message is encrypted; the recipient's private key is then used to decode the message. DWT's cover picture may be used to conceal a hidden image. Decode the text by removing the concealed image off the cover using DWT. Using chosen cryptography and steganography set of rules, the proposed method is implemented on the MATLAB platform. Determining the PSNR and MSE is the next step. Find the cover and stego picture's entropy. This way of transmitting digital data is safe for use in online conversations.

Ahmed Uz Zaman et.al (2018) The goal of the "Steganography" initiative is to encrypt a data file. Since individuals are worried about their data being compromised while being sent over the internet. There are several options available to prevent sensitive information from falling into the wrong hands. In addition to encryption, steganography may be used to keep sensitive information safe. While cryptography is used to encrypt a message so that it is difficult to decipher, steganography is used to conceal data or a hidden message. For this reason, the suggested method combines steganography with encryption to send information securely. A picture may carry the message. The article implements a substitution encryption technique using BMP steganography, which is known for its great performance. The IDEA (International Data Encryption Algorithm) algorithm is utilized for encryption in this implementation. Here's how the IDEA algorithm works: the sender feeds it a TEXT document and a secret key, and the algorithm returns an encrypted BMP image. It's also possible to build in a "Voice Recognition System" framework, which would allow the message to be deciphered by vocal input. The potential further development of this article lies in the following.

Manish Chaudhary et.al (2017) In today's global scenario, the Internet permeates almost every sphere of our existence. Because of this, the Internet has become the primary means through which people exchange and discuss information. Information security during transmission is of the highest importance because of the Internet's fast expansion and the resulting problem of illegal access to sensitive data. Popular methods of secure transmission include encrypting data and steganography. When compared to encryption, steganography's ability to insert secret data into some cover material makes it much more trustworthy. Steganography, in contrast to cryptography, is not used to conceal messages from prying eyes; rather, it conceals information by making it seem as if it were part of a completely ordinary communication that has no practical use to an outsider. Even though there are many other forms of data that may be hidden using Steganography—including text, images, audio, video, and protocols—recent advances have focused on picture steganography because of its high data concealing capacity and challenging identification. Hiding sensitive information in digital photographs is possible using a wide variety of methods, including LSB, ISB, MLSB, etc. In this article, we'll take a look back at the history of steganography, as well as the many data-hiding and security approaches that make use of digital pictures, to assess their use and drawbacks.

STEGANOGRAPHY MEDIUMS

Steganography employs a wide variety of approaches, some more appropriate than others for protecting certain types of data or media.

- **Image Steganography**: When an image is used as a cover object in a steganographic scheme, the technique is called "image steganography.

- **Video Steganography**: In video steganography, any kind of data may be concealed using a digital video format. Hiding information in video stills by adjusting their values (from 7.667 to 8, for instance) is possible thanks to the discrete cosine transform (DCT), which is imperceptible to the naked eye. Video steganography uses common video file formats such as MP4, AVI, and others.

- **Audio Steganography**: Voice over Internet Protocol has increased the need for audio steganography (VOIP). Since sound is used to conceal data, this method is known as "Audio Steganography." Audio steganography makes use of digital audio codecs like WAVE, MPEG, and others.

- **Network Steganography**: In this method, a network protocol (such UDP, ICMP, etc.) is employed as a cover object and a carrier.

- **Text Steganography:**Capitalization, white space, the number of tabs, and other similar formatting features are employed in this method to conceal information.

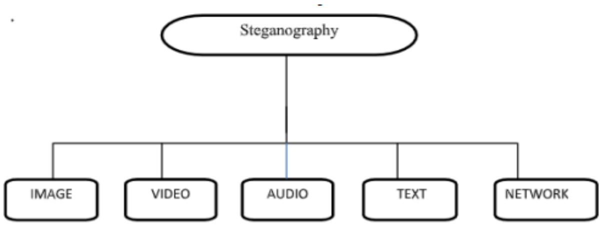


Figure 1: Different Mediums to achieve steganography

GAN-BASED STEGANOGRAPHY METHODS

Goodfellow et al in 2014 proposed General Adversarial Networks as a new form of deep Convolutional Neural Networks. To solve problems associated with image generation, GANs use game theory to fine-tune an adversarial generative model. The generating network and discriminator network in a GAN architecture compete with one another to create a high-quality image. The generator model takes the input picture and outputs an image that closely resembles the original. The produced pictures are sorted into "fake" and "real" categories by the discriminator networks. The generator model is trained to closely resemble the input data with as little noise as feasible, and both networks are then compared. In order to detect the phony pictures, a discriminator model is trained. Since then, other extensions to GAN have been developed, each one making the method more suited to generating synthetic images.

The area of picture creation is one where GANs have shown their worth. Steganography is an example of an image creation problem in which one is given two images and expected to produce a third picture (the stego image). There are now five distinct approaches to picture steganography that all make use of a GAN architecture: models based on Alice, Bob, and Eve; the coverless model; the three-network GAN model; cycle-GAN-based architectures. We've broken down each section and explained how it's put into action.

The generator and the discriminator are the two fundamental parts of a GAN model. Some of the approaches to picture steganography incorporate a novel network called the steganalyzer. The three parts serve primarily in the ways that are,

- G, a generator model that creates stego graphics by combining the cover with a random message.
- D, a discriminator model used to determine whether or not the picture produced by the generator is genuine.
- S, a steganalyzer that can determine whether a given picture contains any kind of hidden information.

The three models (G, D, and S) are pitted against one another to see which can provide the most convincing results closest to the input cover photo. The quality and realism of the steganographic picture are determined by a combination of the D and S error values and a parameter alpha between [0, 1]. Not like the GAN, this revision of G amplifies not just D's mistake but all errors, but the error of the linear combination of the classifiers D and S.

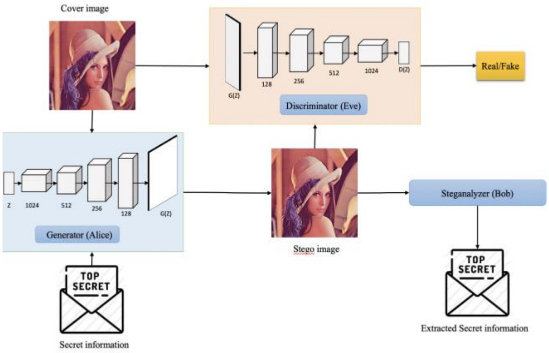


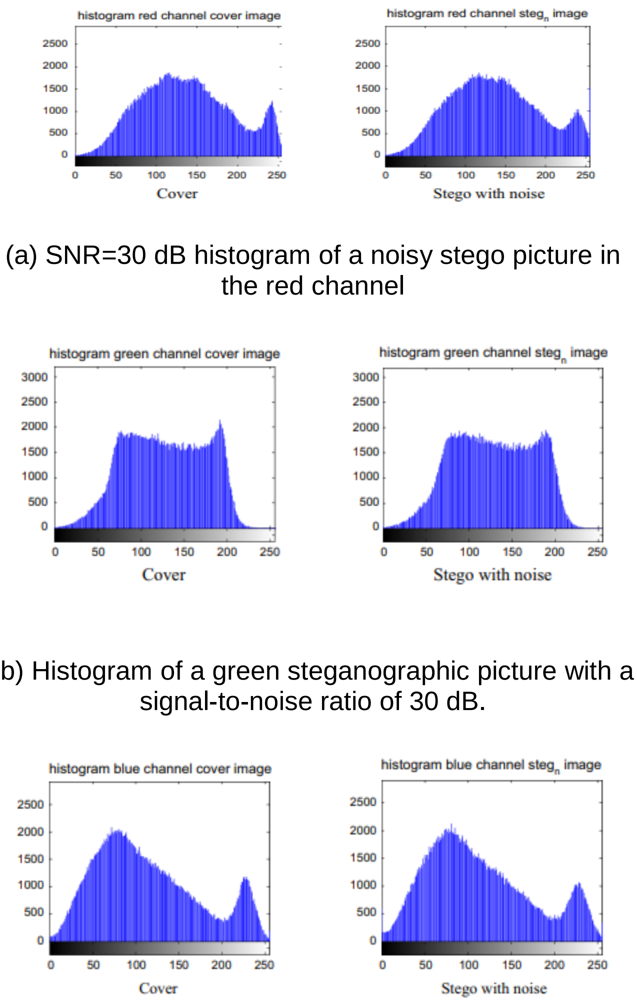
Figure 2: General working overflow of SGAN and.

Both and employ DCGANs, whereas and use a WGAN with a basic architecture consisting of four fractionally convolutional layers and a functional layer activated by hyperbolic tangents. The steganalyzer listens in on the generator and provides the probability while the discriminator recognizes and recovers the hidden message from the stego images generated by the generator. The SGAN operating concept is shown in Figure 2.

GAUSSIAN AND RAYLEIGH FADING CHANNELS FOR OFDM-BASED STEGANOGRAPHIC IMAGE TRANSMISSION

Images Hidden in Steganography are Transmitted through OFDM

- The input to the OFDM system shown in the figure is a steganography picture retrieved using an embedding approach.



(a) SNR=30 dB histogram of a noisy stego picture in the red channel

(b) Histogram of a green steganographic picture with a signal-to-noise ratio of 30 dB.

(c) Histogram of a low-SNR (30 dB) blue channel stego picture compared to the cover image.

Figure 3: Stego image at SNR=30 dB compared to the cover image.

Fig. 3 demonstrates that the Stego picture maintains a high quality despite the presence of noise. Reconstructed pictures at SNR=30 dB are shown in Figure 4.

• Quadrature amplitude modulation (QAM) of order 2 was employed in the OFDM modulation block. Using a constellation size that is proportional to the quantity of noise in the communication channel yields high efficiency when QAM is used.

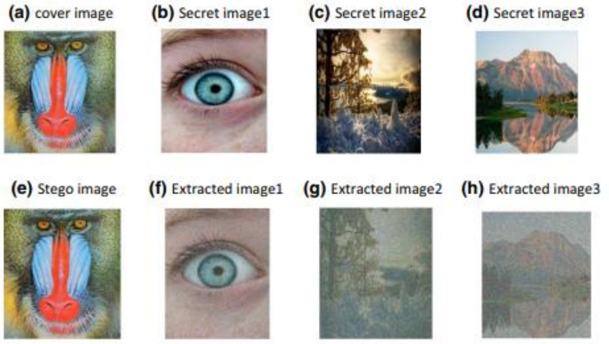


Figure 4: Reconstructed images at α1=0.08 with noise at SNR=30 dB

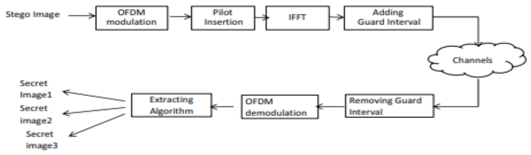


Figure 5: OFDM transmit model for steganography image

- In order to determine whether an OFDM symbol transmission has begun, in this case, the received signal does indeed include the pilot symbol. It may also be used for estimations in channels. Analysis and implementation of channel estimation in an OFDM system, Sam in employed pilot symbols; thanks to their unique symmetry, the receiver doesn't need to be aware of the pilot symbol.
- The Inverse Fast Fourier Transform computations performed by the IFFT block allow for efficient signal processing.
- Using OFDM with a Guard Interval (GI) is one way to combat the Rayleigh channel effect since it is resilient against propagation delays and cuts down on interference for subsequent users.

CONCLUSION

In recent years, GAN architecture's capacity to handle image reconstruction problems has attracted a lot of interest. In the case of picture steganography, A steganographic picture that is almost identical to the cover image is reconstructed using the cover image and the secret data. This study assesses the problems that have been encountered, the gaps that have been identified, and the potential future directions that have been opened up. By using an OFDM system, this study analyses how additive white Gaussian noise and multipath fading channels affect both the steganographic image and the returned data. The OFDM system has been modified to mitigate distortion caused by interference from wireless channels.

REFERENCE

1. Manish Chaudhary et.al "Survey on Image Steganography and its Techniques" DOI: 10.21817/ijet/2017/v9i3/170903S049 Vol 9 No 3S July 2017
2. Ahmed Bakhtiyar Uz Zaman "Security during Transmission of Data Using Web Steganography" May, 2018
3. B. Chitradevi et.al "A Survey On Image Steganography Types and Hiding Techniques" International Journal of Trendy Research in Engineering and Technology Volume 4 Issue 6Oct' 2020 ISSN NO 2582-0958
4. Swati Bhargava et.al "Hide Image And Text Using Lsb, Dwt And Rsa Based On Image Steganography"DOI:10.21917/ijivp.2019.0275
5. Mohammed Abdul Majeed et.al "settings "A Review on Text Steganography Techniques"https://doi.org/10.3390/math9212829
6. J. S. Lee, Y. M. Kuo, P. C. Chung, and E. L. Chen, "Naked image detection based on adaptive and extensible skin color model," Pattern Recognition, vol. 40, pp. 2261-2270, Aug 2007.
7. D. Ganguly, M. H. Mofrad, and A. Kovashka, "Detecting Sexually Provocative Images," presented at the 2017 IEEE Winter Conference on Applications of Computer Vision (WACV), 2017.
8. Senarathne and K. De Zoysa, "ILSB: Indexing with Least Significant Bit Algorithm for Effective Data Hiding," International Journal of Computer Applications vol. 161, 2014
9. K. Rao and H. Wu, "Structural similarity based image quality assessment," in Digital Video image quality and perceptual coding, ed: CRC Press, 2005, pp. 261-278.
10. O. F. Rashid, Z. A. Othman, and S. Zainudin, "A novel DNA sequence approach for network intrusion detection system based on cryptography encoding method," International Journal on Advanced Science, Engineering and Information Technology, vol. 7, pp. 183-189, 2017
11. M. A. Alsarayreh, M. A. Alia, and K. A. Maria, "A Novel Image Steganographic System Based on Exact Matching Algorithm and Key-Dependent Data Technique," Journal of Theoretical and Applied Information Technology, vol. 95, p. 1212, 2017.
12. Baby and H. Krishnan, "Combined Strength of Steganography and Cryptography-A Literature Survey," International Journal of Advanced Research in Computer Science, vol. 8, 2017.
13. N. Patel and S. Meena, "LSB based image steganography using dynamic key cryptography," presented at the International Conference on Emerging Trends in Communication Technologies (ETCT), 2016.
14. B. Furht, E. Akar, and W. A. Andrews, Digital Image Processing: Practical Approach: Springer, 2018.
15. S. Sun, "A new information hiding method based on improved BPCS steganography," Advances in Multimedia, vol. 2015, 2015.

Corresponding Author

Amjad Khan*

Researcher, Prince Sultan Bin Abdulaziz College for Emergency Medical Services, King Saud University, Riyadh