Society for Multidisciplinary & Advanced Research Techniques (SMART)
Trinity University, Lagos, Nigeria
SMART Scientific Projects & Research Consortium (SMART SPaRC)
Harmarth Global Educational Services
ICT University Foundations USA
IEEE Computer Society Nigeria Chapter

33rd ECOWAS iSTEAMS ETech Multidisciplinary Conference (ECOWAS-ETech)

# Safe Information Hiding Using Steganography

**Patricia Eduafo Enninful**
Ghana Institute of Management & Public Administration
GreenHills Accra, Ghana
**E-mail:** patricia.enninful@st.gimpa.edu.gh

## ABSTRACT

Besides cryptography, steganography can be employed to secure information. With advances in technology, most information is kept and shared electronically through the internet. As the use of the internet increases, the rate at which data is used and exchanged each day also increases. This data can easily be seen, manipulated and accessed by hackers. In order for this data to be protected from these malicious persons a process known as steganography can be employed. Steganography is one of the data hiding techniques that hides information in any medium. It involves hiding secret information behind a cover file such that the existence of that information is not easily noticed or recognized. Basically steganography is used to hide information in digital media. In contrast to cryptography, the message or encrypted message is embedded in a digital host before passing it through the network, thus the existence of the message is unknown. Besides hiding data for confidentiality, this approach of information hiding can be extended to copyright protection for digital media such as audio, video, and image.

**Keywords:** Safety, Information, Hiding, Cybersecurity, Biometrics, Cryptography, Steganography

**Proceedings Citation Format**
Patricia Eduafo Enninful (2022): Safe Information Hiding Using Steganography. Proceedings of the 33rd ECOWAS iSTEAMS Emerging Technologies, Scientific, Business, Social Innovations & Cyber Space Ecosystem Multidisciplinary Conference. University of Ghana/Academic City University College, Ghana. 29th Sept – 1st Oct, 2022.
Pp 161-166 www.isteams.net/ghanabespoke2022. dx.doi.org/10.22624/AIMS-/ECOWASETECH2022P33

## 1. INTRODUCTION

The growing possibilities of modem communications need the special means of security especially on computer networks. Network security is becoming more important as the number of data being exchanged on the Internet increases. Data confidentiality and integrity are required to protect against unauthorized access. This has resulted in an explosive growth of the field of information hiding.

In addition, the rapid growth of publishing and broadcasting technology also requires an alternative solution in hiding information. The copyright of digital media such as audio and video in digital form may lead to large-scale unauthorized copying. This is because the digital formats make it possible to provide high image quality even under multi-copying. The problem of unauthorized copying is of great concern especially to the music, film, book and software publishing industries. To overcome this problem, some invisible information can be embedded in the digital media in such a way that it could not be easily extracted without a specialized technique such as Steganography (Hrytskiv, 1998).

## 2. RELATED LITERATURE

Varade et al, 2016 implements Audio-Steganography in which the data is hidden into another medium such as an audio file. Here the message is hidden in MP3 like sound files. The process of hiding the data behind the audio file is more complicated as compared to other steganography types or mediums. This paper deals with different types of audio stenographic methods with the advantages and disadvantages. First One is LSB coding, which is most commonly used and simplest technique but more efficient in providing security. Second is Phase coding which has disadvantage of low data transmission rate. Third one is spread spectrum in which the noise is introduced in the process of hiding data behind audio files.

Rosziati 2011, introduces a new system called Steganography Imaging System (SIS).The two levels of security is provided in the proposed system. In this system cryptography is not used for first level of security instead Username and password is used to provide the login security. Here the secret key is used only to retrieve secret message from the image not for the encrypting purpose. In the proposed system, first the secret message is transferred to text file. Then the text file is compressed to zip file. At the next level the zip file is converted into binary codes to embed the message into image. The purpose of using zip file is that zip file is more secure than the normal text file.

Khosala et al 2014 is a combination of Video Steganography and Digital Watermarking which provides strong backbone for its security. This paper presents a new algorithm which is used for better security and transferring of data efficiently from source and destination. This paper uses the concept of Digital watermarking along with steganography. In digital watermarking the digital signal or pattern is inserted into digital content. This process can be used on any of the steganography types either audio, image or text. In this process first the secret data is converted into binary form. Then the LSB technique is applied to replace the least bit of cover image pixel with the binary bit. After applying LSB we get the stego image. Now the combined DWT and DCT technique is applied on stego image to get watermarked image. The watermarked image is then securely transferred to the destination.

Steffy, 2014 deals with hiding the image as secret information behind the frames of video. Along with the LSB approach, the Masking-Filtering techniques are used to hide the secret image in frame. In this paper first the video is converted into frames and stored in the separate file. Only one frame is used to hide the input image. The Masking and Filtering techniques are generally used to conduct the analysis of the image. The Significant areas are selected to embed the secret image to provide more security. These two techniques are usually applied to only 24 bit and gray scale images. To embed the message into the video clips a key is used called the stego key.

In Sahu et al, the first step is to encrypt the data. For encryption process of data, the most popular technique called the AES algorithm is used. Along with the AES algorithm pixel swapping technique is also used to embed message in video. In the pixel swapping technique randomly one frame is selected, after selecting the frame separate the Red, Green, Blue channel of that frame. Next for data hiding the particular channel is selected, in this case the paper makes use of blue channel. For every selected frame, the pixel positions of blue channel are swapped with the use of key. Encrypt the message using AES algorithm. Embed this encrypted message into the pixels to enhance the double level security.

The concept of PSNR value calculation is used in this paper to compare the original and stego image. PSNR is Peak Signal-to-Noise Ratio. Both the PSNR values are compared, if we get the more value in the stego image, then we can say the proposed system is secured. In Al-Hazaime 2012, the most common steganographic technique is Least Significant Bit (LSB).The above paper deals with the advanced LSB technique to hide data into images. In the common technique the least bits of the image is changed with the message bit but in this advanced technique it is suggested that the message bits are randomly inserted in the image.

This advanced LSB technique is introduced in order to provide better security to system. In this advanced LSB technique the message bits are inserted into image, not only in the least bit of but also in the other bits in the random manner. In this process the message bit and the pixel bit randomly chosen is compared. If the message bit and pixel bit are identical then 1 is inserted into least significant bit otherwise 0 is inserted if the message bit is not identical with image bit. This paper compares the stego image and original image with the two techniques Mean-Squared Error (MSE) and Peak Signal-to-Noise Ratio. In the case of MSE measurement the value must be as less as possible. If it is 0 means that there is no change in original image and encrypted image.

## 3. FINDINGS

The word steganography comes from the Greek Steganos, which means covered or secret and -graphy means writing or drawing. Therefore, steganography means, literally, covered writing. Steganography is the art and science of hiding information such that its presence cannot be detected (Cachin, 1998). A secret information is encoded ina manner such that the very existence of the information is concealed. Paired with existing communication methods, steganography can be used to carry out hidden exchanges. The main goal of steganography is to communicate securely in a completely undetectable manner (Memon, 2001) and to avoid drawing suspicion to the transmission of a hidden data. It is not to keep others from knowing the hidden information, but it is to keep others from thinking that the information even exists. If a steganography method causes someone to suspect there is a secret information in a carrier medium, then the method has failed (Artz, 2001). Until recently, information hiding techniques received very much less attention from the research community and from industry than cryptography. This situation is however changing rapidly and the first academic conference on this topic was organized in 1996.

Since then, there has been a rapid growth of interest in steganography. This is due to two main reasons:

i. The publishing and broadcasting industries have become interested in techniques for hiding encrypted copyright marks and serial numbers in digital films, audio recordings, hooks and multimedia products.
ii. Moves by various governments to restrict the availability of encryption services have motivated people to study methods by which private messages can be embedded in seemingly innocuous cover messages.

## 4. RESEARCH GAPS

The basic model of steganography consists of Carrier, Message and Password. Carrier is also known as a cover-object, which embeds the message and serves to hide its presence. Message is the data that the sender wishes to remain confidential. It can he plain text, ciphertext, image, or anything that can be embedded in a hit stream such as a copyright mark, a covert communication, or a serial number. Password is known as a stega-key, which ensures that only the recipient who knows the corresponding decoding key will be able to extract the message from a cover-object. The cover-object with the secretly embedded message is then called the stego-object.

Recovering message from a stego-object requires the cover-object itself and a corresponding decoding key if a stego-key was used during the encoding process. The original image may or may not be required in most applications to extract the message. There are several suitable carriers that can he used as the cover-object as listed below:

i. Network Protocols such as TCP, IP and UDP.
ii. Audio that use digital audio formats such as way, midi, avi, mpeg, mpi and voc.
iii. File and Disk that can hide and append files by using the slack space.
iv. Text files such as html and java.
v. Image files such as bmp, gif and jpg, where they can be both colour and gray-scale.

In general, the information hiding process extracts redundant bits from cover-object. The process consists of two steps:

i. Identification of redundant bits in a cover- object. Redundant bits are those bits that can be modified without corrupting the quality or destroying the integrity of the cover-object.
ii. Embedding process which selects the subset of the redundant bits to be replaced with data from a secret message. The stego-object is created by replacing the selected redundant bits with message bits.

## 5. RECOMMENDATIONS FOR PRACTICES, POLICIES AND DESIGN

Basically, the purpose of cryptography and steganography is to provide secret communication. However, steganography is not the same as cryptography. Cryptography hides the contents of a secret message from malicious people, whereas steganography even conceals the existence of the message. Steganography must not be confused with cryptography, where we transform the message so as to make its meaning obscure to malicious people who intercept it. Therefore, the definition of breaking the system is different (Klimant et al, 1998).

In cryptography, the system is broken when the attacker can read the secret message. Breaking a stenographic system needs the attacker to detect that steganography has been used and he is able to read the embedded message. In cryptography, the structure of a message is scrambled to make it meaningless and unintelligible unless the decryption key is available. It makes no attempt to disguise or hide the encoded message. Basically, cryptography offers the ability of transmitting information between persons in a way that prevents a third party from reading it. Cryptography can also provide authentication for verifying the identity of someone or something. In contrast, steganography does not alter the structure of the secret message, but hides it inside a cover-image so that it cannot be seen.

A message in a cipher text, for instance, might arouse suspicion on the part of the recipient while an "invisible" message created with stenographic methods will not. In other word, steganography prevents an unintended recipient from suspecting that the data exists. In addition, the security of classical steganography system relies on secrecy of the data encoding system. Once the encoding system is known, the steganography system is defeated.

It is possible to combine the techniques by encrypting message using cryptography and then hiding the encrypted message using steganography. The resulting stego-image can be transmitted without revealing that secret information is being exchanged. Furthermore, even if an attacker were to defeat the stenographic technique and detect the message from the stego-object, he would still require the cryptographic decoding key to decipher the encrypted message. Table 1 shows that both technologies have counter advantages and disadvantages (Isabell, 2002).

## 5. CONCLUSION

In this paper we gave an overview of steganography. It can enhance confidentiality of information and provides a means of communicating privately. We have also presented an image stenographic system using LSB approach. However, there are some advantages and disadvantages of implementing LSB on a digital image as a carrier. The advantage of LSB is its simplicity to embed the bits of the message directly into the LSB plane of cover-image and many applications use this method (Johnson et. al, 1998). Another advantage is its perceptual transparency whereby the changes made to the cover-image cannot be traced by human eye. One of the disadvantages is that LSB is not robust. It is very sensitive to any kind of filtering or manipulation of the stego-image. Another weakness is that it is tamper resistance. An attacker can easily destruct the message by removing or zeroing the entire LSB plane, however there is only very little change in the perceptual quality of the modified stego-image.

## 6. DIRECTION FOR FUTURE WORKS

Further work on this research is to enhance the system by using a password to embed the message. We will also implement another two approaches of stenographic system on a digital image. Then, a comparative study on these different approaches will be done.

## REFERENCES


1. Z. Hrytskiv, S. Voloshynovskiy & Y. Rytsar "Cryptography of Video Information In Modem Communications", Electronics And Energefics, vol. 11, pp. 115-125, 1998.
2. Chhaya Varade, Danish Shaikh, Girish Gund, Vishal Journal of advanced Reseach in Computer Science and Software Engineering, Volume 6, Issue 2, February 2016.
3. Rosziati Ibrahim and Teoh Suk Kuan "Steganography algorithm to hide secret message inside an image", Computer Technology and Application 2 (2011) 102-108.
4. Shivani Khosla, Paramjeet Kaur "Secure Data Hiding Technique using Video Steganography and Applications (0975 – 8887) Volume 95– No.20, June 2014.
5. K. Steffy Jenifer, G. Yogaraj, K. Rajalakshmi "LSB Approach for Video Steganography to Embed Images", International Journal of Computer Science and Information Technologies, Vol. 5 (1), 2014, 319-322
6. Miss. Uma Sahu, Mr. Saurabh Mitra "A Secure Data Hiding Technique Using Video Steganography", International Journal of Computer Science & Communication Networks, Vol 5(5), 348-357.
7. Obaida Mohammad Awad Al-Hazaimeh "Hiding Data in Images Using New Random Technique", International Journal of Computer Science Issues, Vol. 9, Issue 4, No 2, July 2012.
8. C . Cachin, "An Information-Theoretic Model for Steganography", in proceeding 2nd Information Hiding Workshop, vol. 1525, pp. 306-318, 1998
9. R. Chandramouli, N. Memon, "Analysis of LSB Based Image Steganography Techniques", IEEE pp. 1019-1022, 2001.
10. D. Artz, "Digital Steganography: Hiding Data within Data", IEEE Internet Compufing, pp. 75-80, May-Jun 2001
11. J. Zollner, H. Federrath, H. Klimant, et al., "Modeling the Security of Steganographic Systems", in 2nd Workshop on Informafion Hiding, Portland, April 1998, pp. 345-355.
12. N. Provos, P. Honeyman, "Detecting Steganography Content on the Internet".
13. E.T. Lin and E.J. Delp, "A Review of Data Hiding in Digital Images",
14. RA Isbell, "Steganography: Hidden Menace or Hidden Saviour", Steganography White Paper, IO May 2002.
15. N.F. Johnson & S. Jajodia, "Steganalysis of Images Created Using Current Steganography Software", in Proceeding for the Second Information Hiding Workhop, Portland 0 regon, USA, April 1998, pp. 273-289.
16. M. M Amin, M. Salleh, S. Ibrahim, M.R. Katmin, and M.Z.I. Shamsuddin - Faculty of Computer Science & Information Systems, Universiti Teknologi Malaysia. 81300 Skudai, Johor, Malaysia. J. Computer Network and Information Security, 2017, 9, 38-45