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)

Digital Image Staganography

Worthy Elijah
School of Technology
Ghana Institute of Management & Public Administration
GreenHills, Accra, Ghana
E-mail: worthyelijah2@gmail.com

ABSTRACT

In today's world, where digital media is the predominant mode for data and information sharing, it has become needful for computer security professionals to help secure this form of digital media both in transmission and at rest. Steganography has been in use since ancient times. Through computer techniques, security professionals have developed ways to apply the old steganography techniques to digital media to ensure that the confidentiality and integrity of digital media are not compromised. This paper gives a broad overview of steganography and specifically digital steganography. Then it analyses the use of Least Significant Bit techniques in digital media steganography and how we can further secure it since it is the most used steganography technique on digital media.

Keywords: Steganography, Least Significant Bit, Cybersecurity, Digital Media

Proceedings Citation Format
Worthy Elijah (2022): Digital Image Staganography. 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 175-183. www.isteams.net/ghanabespoke2022. dx.doi.org/10.22624/AIMS-/ECOWASETECH2022P35

1. BACKGROUND OF STUDY

Steganography is the act of hiding secret data within an ordinary, non-secret file or message to avoid detection; the personal data is then extracted at its destination. Using steganography combined with encryption can be an extra step in hiding the data. Steganography comes from the Greek words steganos which means to hide or cover, and graph, which means to write.(*What Is Steganography? - Definition from SearchSecurity*, n.d.) Digital media is information shared through electronic devices. This form of media can be created, viewed, modified and distributed via electronic devices. In today's world, any form of media relies on an electronic device for its creation, distribution, viewing, and storage.(*Digital Media: Definition and Example*s, n.d.)

In today's world, steganography is used to conceal almost any digital content, including text, image, video or audio. The content concealed through steganography -- hidden text -- is often encrypted before being incorporated into the innocuous-seeming cover text file or data stream. If not encrypted, the hidden text is commonly processed to increase the difficulty of detecting the secret content. The main purpose of steganography is to keep data secured from the visible eye. There are several types of steganography applied in our world today. They are listed in the diagram below:

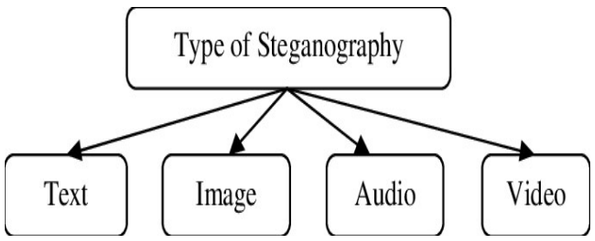

Fig 1: (*Types of Steganography*
Source: (*Types of Steganography | Download Scientific Diagram*, n.d.)

Text Steganography is the process of hiding information inside text files. It involves changing the format of existing text, changing words within a text, generating random character sequences or using context-free grammar to generate readable texts. It includes techniques such as Format Based Method, Random and Statistical Generation and Linguistic Method. Image Steganography is the act of hiding the data by making the cover object an image. Image steganography is widely used as a cover source because many bits are present in an image's digital representation(Muralidharan et al., 2022). The most common approaches to hiding data under images include Least Significant Bit Insertion, Masking and Filtering, Redundant Pattern Encoding, Encrypt and Scatter and Coding and Cosine Transformation.

In the steganographic approach to audio, the secret message is hidden in an audio signal which alters the binary sequence of the corresponding audio file(Mandal et al., 2022). Doing this in digital sound is a much more complicated process when compared to other forms of steganography. Techniques such as Least Significant Bit Encoding, Parity Encoding, Phase Coding and Spread Spectrum are used in audio steganography.

These methods hide the data in WAV, AU, and even MP3 sound files. One can hide any kind of data in digital video format. The significant advantage of video steganography is the large amount of data hidden inside a video. Moreover, it is a moving stream of images and sounds. Video steganography is a combination of image steganography and audio steganography. Two main approaches to video steganography are embedding data in uncompressed raw video, compressing it later, and embedding data directly into the compressed data stream(Cheddad et al., 2010).

2. RELATED LITERATURE

he table below presents a review of studies conducted on digital media steganography;

Authors	Work on digital steganograhy
(Mandal et al., 2022)	This article offered an extensive state-of-the-art review and analysis of some recent steganographic techniques. It included a discussion on popular steganography tools in detail with some recent challenges in deep learning-based steganography. The he article concludes by mentioning some future research directions
(Cheddad et al., 2010)	This paper provided a state-of-the-art review and analysis of the different existing steganography methods along with some common standards and guidelines drawn from existing literature. This paper concluded with some recommendations and advocated for the object-oriented embedding mechanism. Steganalysis, the science of attacking steganography, is not the focus of this survey.
(Muralidharan et al., 2022)	This article provided several taxonomies for steganography and steganalysis methods based on the approach and techniques underlying the methods, which allows us to perform the first comprehensive comparison of steganography and steganalysis methods. This comparison sheds light on the existing gaps between the two connected domains. The article identified and prioritized the steganography methods that require immediate remediation using steganalysis methods.
(Biswas et al., 2012)	The technique discussed in this paper consists of two processes: encoding and decoding. The main focus in the encoding phase is to hide the secret RGB colour image in a cover image and transmit some shares to the receiver. In the decoding phase, the main focus is to get the retrieved image back to the original image quality as much as possible from the shares in the received end.

3. FINDINGS

Least significant bit insertion is one of the essential methods of steganography implementation. In this method, the LSB bits of a byte are altered to form a bit string and represent an embedded file. Changing the LSB bits will cause minor differences in colour that are not noticeable to the human eye. After that, the image is compressed, and a text message is hidden in the image. In the LSB method, LSB bits of the covered image is altered to form embedded information. Embedding a message into the cover image will result in a stego image. The stego image will be identical to the cover image because of only minor changes in pixel values. Therefore there is no significant difference. The embedded message is sequentially placed in the covered image so a third party can recover the message by retrieving the pixels sequentially.

When converting an analogue image to digital format today, three different ways of colour representation are used;

- 24-bit colour: every pixel can have one in 2^24 colours, and these are represented as different quantities of three primary colours: red (R), green (G), and blue (B), given by 8 bits (256 values) each.
- 8-bit colour: every pixel can have one in 256 (2^8) colours chosen from a palette or a table of colours.
- 8-bit grey-scale: every pixel can have one in 256 (2^8) shades of grey.

LSB insertion modifies the LSBs of each colour in 24-bit images and 8-bit value for 8-bit images. For example, we insert the letter 'A' into an image using LSB. 'A' as a letter has the ASCII code of 65, which is 1000001 in binary. The letter 'A' will need three consecutive pixels for a 24-bit image to store.

The pixels before insertion are:

1. 10000000.10100100.10110101
2. 10110101.11110011.10110111
3. 11100111.10110011.00110011

After insertion, their values for 'A' will be:

1. 1000000**1**.10100100.1011010**0**
2. 1011010**0**.1111001**0**.1011011**0**
3. 1110011**0**.10110011.00110011

NB: The figures in bold were the ones modified.
24-bit image modification sometimes can be extended to the second or third LSBs without being visible. The most basic LSBs insertion for 24-bit pictures inserts 3 bits/pixel.

4. RESEARCH GAPS

Though LSB is good for steganography, it has some major draw backs that need to be fixed for improved security and use. One of the major draw backs with LSB insertion for stegnaograpgy is the ease of extraction. Due to this, attackers can use programs to rearrange the significant bits to be able to decode the information stored in the image. This has great implications for confidentiality.

5. RECCOMENDATIONS FOR PRACTICES, POLICIES AND DESIGN

A solution for the ease of data extraction from the steno image that had LSB applied on it is, the encoder must apply encryption to the message so that decryption can also occur when the image is received. Another added layer is by randomizing the placement of the bits using a cryptographical random function. By so doing, the message is protected by two primary keys, which affords more confidentiality to the steno image.

6. CONCLUSION

In today's world, where we use digital media for much data transmission, steganography has become an essential technique for the confidentiality and integrity of digital media transmission. Steganography techniques must therefore be robust to enhance digital media security.

7. DIRECTION.FOR FUTURE WORKS

Future works can look at more robust ways to secure the LSB approach to steganography since it is the most used technique in digital steganography.

8.0 IMPLICATIONS FOR PRACTICE, POLICY AND ONLINE SAFETY IN AFRICA

Given the context that, Africa is rising to become a continent that relies mostly on digital communication due to increase in population in the coming years, cybersecurity experts must develop new ways to further enhance the cryptographic strength of LSB's use in digital steganography. This will lead to more safe communication online and this will inform policy guidelines on the use of LSB in digital Steganography.

REFERENCES

1. Biswas, D., Biswas, S., Majumder, A., Sarkar, D., Sinha, D., Chowdhury, A., & Das, S. K. (2012). Digital Image Steganography using Dithering Technique. *Procedia Technology*, *4*, 251–255. https://doi.org/10.1016/j.protcy.2012.05.038
2. Cheddad, A., Condell, J., Curran, K., & Mc Kevitt, P. (2010). Digital image steganography: Survey and analysis of current methods. In *Signal Processing* (Vol. 90, Issue 3, pp. 727–752). https://doi.org/10.1016/j.sigpro.2009.08.010
3. *Digital Media: Definition and Examples*. (n.d.). Retrieved August 21, 2022, from https://www.copypress.com/kb/content-marketing/digital-media-definition-and-examples/
4. Mandal, P. C., Mukherjee, I., Paul, G., & Chatterji, B. N. (2022). Digital image steganography: A literature survey. *Information Sciences*, *609*, 1451–1488. https://doi.org/10.1016/j.ins.2022.07.120
5. Muralidharan, T., Cohen, A., Cohen, A., & Nissim, N. (2022). The Infinite Race Between Steganography and Steganalysis in Images. *Signal Processing*, 108711. https://doi.org/10.1016/j.sigpro.2022.108711
6. *Types of Steganography | Download Scientific Diagram*. (n.d.). Retrieved August 21, 2022, from https://www.researchgate.net/figure/Types-of-Steganography_fig4_228765086
7. *What is Steganography? - Definition from SearchSecurity*. (n.d.). Retrieved August 21, 2022, from https://www.techtarget.com/searchsecurity/definition/steganography