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)

High-Capacity Image Steganographic Model

Tseh Richard Divine
Ghana Institute of Management & Public Administration
GreenHills Accra, Ghana
E-mail: richard.tseh@st.gimpa.edu.gh / tsehdivine@gmail.com

ABSTRACT

Deep studying technology, which has emerged as an effective device in diverse packages which includes photograph steganography to shield and steady the transmitted data, has received multiplied interest recently. The essential purpose of this paper is to discover and talk diverse deep studying strategies to be had in photograph steganography field. Deep studying strategies used for photograph steganography can widely be divided into 3 categories - conventional strategies, CNN primarily based totally and GAN-primarily based totally strategies. This paper goals to assist the fellow researchers through compiling the present-day trends, demanding situations and a few future paths on this field.

Keywords: Image Steganography, Steganalysis, Stego Image, Cover Image, Embedding, GAN-based, CNN based

Proceedings Citation Format
Tseh Richard Divine (2022): High-Capacity Image Steganographic Model. 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 137-141. www.isteams.net/ghanabespoke2022. dx.doi.org/10.22624/AIMS-/ECOWASETECH2022P28

1. INTRODUCTION

In particular, the net has received extended recognition for replacing virtual media and individuals, personal companies, institutions, governments se those multimedia statistics switch techniques for replacing statistics. The maximum not unusualplace answer is statistics encryption in which the statistics is transformed right into a cipher textual content area using encryption key. Using statistics encryption, the authentic statistics isn't always seen, cipher textual content encrypted statistics is seen in a scrambled shape to human eyes main to suspicion and similarly scrutiny. A new studies topic, steganography, has received attractiveness on this context to cover the statistics that isn't always seen to human eyes. Cryptography makes the statistics unbreakable and unreadable however the cipher textual content is seen to human eyes

1.1 Background to the Study

As proven in parent 4, inputs are cowl photo and the mystery statistics which may be both textual content or photo. DL version may be both a CNN-primarily based totally or GAN-primarily based totally whilst the steganography block generates the stego photo. The steganalysis version takes the stego photo as enter to hit upon and perhaps extract the name of the game statistics. Based on the use of the name of the game media and the techniques are labeled into 3 classes as proven in parent 2. As may be visible withinside the parent 2, the foremost techniques use the textual content as the name of the game statistics.

1.2 GAN-Based Steganography Methods

Image steganography can be considered as one such image generation task where two inputs – the cover image and the secret image are given to generate and one output – stego image. The existing methods used for image steganography using a GAN architecture can be grouped into five categories - a three network-based GAN model, cycleGAN based architectures, sender-receiver architecture using GAN, coverless model where the cover image is generated randomly instead of being given as input and an Alice, Bob and Eve based model. (Jianhua et al, 2018) and (Jianhua et al, 2019) presented a GAN based image steganography with three modules - Generator, Embedding Simulator and Discriminator.

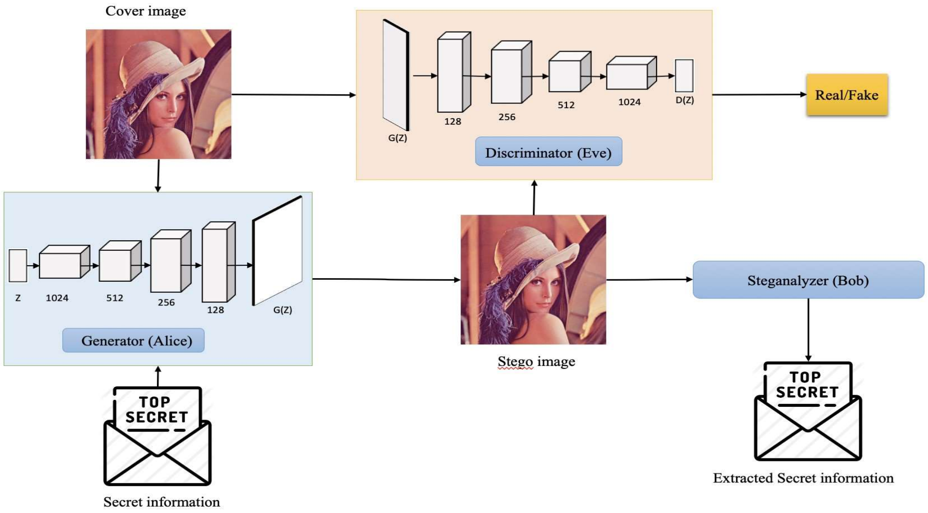

Fig 2: Image steganography technique GAN based image steganography with three modules – Generator, Embedding Simulator and Discriminator.

Concepts for Image Steganography:

Image Definition

An image is defined as a collection of numbers that represent different intensities of light in different parts of the image. The basic points that make up the grid of this numerical representation are known as pixels. Image pixels are displayed horizontally, line by line. The number of bits used for each pixel is referred to as bit depth or the number of bits in a colour scheme.

Compression of images:
Lossless and lossy compression are two types of compression used for images. GIF (Graphic Interchange File) is one format that offers lossless compression; in lossless compression, every single bit of data is recovered when the image is decompressed.

2. RELATED LITERATURE

The author of (Hemalatha S et al, 2013) has presented an Integer Wavelet Transform-based image steganography algorithm (IWT). In the suggested method, the cover is a 256x256 colour image with two 128x128 grayscale images serving as the secret message. It obtains a single level IWT of the secret message, and the resulting matrix has bands with the widths LL, LH, HL, and HH. The covert message is concealed by the LL sub bands. Through their research, the authors demonstrated how two hidden images might be concealed within a single-coloured image. In comparison to other approaches, the average PSNR values produced are substantially superior.

The author of (gowtham et al, 2012) has suggested a block complexity study for image steganography in the transform domain. An approach based on segmentation of bit plane complexity and wavelet transform has been proposed by the author. While the bit plane complexity segmentation is used as a measure of noise, the secret message is hidden by the cover's wavelet transform presentation. An image is segmented into 8x8 blocks for the wavelet representation, and the capacity of each block is calculated using BPCS. The author has also discussed a number of factors related to embedded images, such as PSNR and SSIM (Structural Similarity). By using embedding and extraction techniques, it is possible to obtain images of bit plane complexity, which demonstrates how the image quality has improved.

An image steganography and compression method for data concealment is suggested by the author in (Rahul et al, 2012). The author has suggested a method in which the processed secret data is first included into the LSBs of the cover image. During the compression process, input characters are gathered in sequence and a dictionary with single character strings corresponding to all possible input characters is formed. This dictionary is used to encode 8-bit secret data as fixed length 12-bit code. By using the suggested technique, all cover photos have a greater chance of containing the hidden data.

A reliable steganography algorithm based on DCT, Arnold Transform, and chaotic system has been proposed by the author in (Siddharth et al, 2012). The cover image is modified using the DCT during the embedding process, and data is subsequently scrambled using the Arnold transform to further strengthen security. The idea of three keys one for scrambling and two for creating chaotic sequences is presented by the author. In the extraction process, inverse DCT and Arnold transforms are applied. The experiment uses a host image that is initially divided into 4096 blocks of 8x8 each, and a 512x512 grayscale Lena, girl, and Tank image serves as the experiment's cover image. The Arnold transform is used to jumble up the logo. In contrast to previous methods, the Arnold sequence boosts security level and approach is strong against JPEG compression, noise addition, low pass filtering, and cropping operation. As a result, security is improved.

Only 0s and 1s are substituted from the lowest nibble of the byte and are taken into consideration for hiding a hidden message in an image in (Dipesh et al, 2013), among other approaches. Various ways of data concealing based on the random bits of random pixels have also been suggested by the author, including changing intermediate bits, the raster scan concept, the random Scan principle, colour-based data hiding, and shape-based data hiding. Therefore, the techniques were examined, and the results demonstrated that the factors influencing the noise in a cover image as a result of the hidden data depend on the volume of data to be concealed, the size of the cover image, the frequency of pixels present in the image, and the actual locations of the pixels.

3. RESEARCH GAPS/FINDINGS

A key finding in the research revolved around the weakness of Image Steganography technique. As such, one of the recommended strategies was to engage in testing of individual models such Integer wavelength transform, Wavelet transform coefficients, LSB, LZW (Limpel-Ziv-Welch, modified Kekre, Algorithm (MKA), DCT, Arnold transforms and chaotic sequences and Spatial domain to establish their efficiency and how to employ them in image steganography. In the process a study of Spatial domain shows that when using steganography tools, image parameters such as pixel location and intensity value are taken into account. Obtainable noise-related parameters include cover image size, pixel location physically, etc. More secure and robust systems can be created using these parameters. This steganographic model will enforce information security in terms of invisibility of the steganography algorithm, payload capacity to conceal information, robustness in the use of steganography algorithms, independent of file format to embed messages in any online file format, unsuspicious files that may prompt a warden to further examination the file and PSNR indicates a smaller discrepancy between the stego picture and cover images, it also indicates secure communication.

4. CONCLUSION

Image steganography is the method used in transmitting secret information by hiding it in plain sight inside a cover image. Most of the traditional based steganography methods use the LSB substitution and some of its variants. The hiding capacity of the traditional methods are limited as over burdening the cover image by exploiting more pixels for hiding the secret message may led to distortions. Also, the autoencoder-decoder structure with VGG as base, U-Net and Xu-Net are the most prevailing architectures used for CNN based image steganography methods. GAN based methods have proved to have better security performance and hiding capacity.

5. RECOMMENDATIONS

Steganography is a centuries-old technique for transmitting messages in a covert manner so that only the recipient is aware of their presence. At least four bits can be used for message embedding for each greyscale pixel. To maximise embedding capacity while maintaining picture authenticity, an image steganographic model based on variable-size LSB insertion is recommended. The proposed model's effectiveness and efficiency are demonstrated through experimental findings.

6. DIRECTION FOR FUTURE WORKS

Benchmarking of appropriate grayscale images for use as a cover in the suggested data hiding approach. Based on the suggested scheme, research on AVI steganography should be taken into consideration. In order to further improve the effectiveness of the CPSO method, it is recommended to research various varieties of chaotic maps and investigate their impact on pixel selection in future work.

REFERENCES

1. Johnson, Neil F., “Steganography”, 2000, URL: http://www.jjtc.com/stegdoc/index2.html
2. Ingemar J. Cox: Digital watermarking and steganography. Morgan Kaufmann, Burlington, MA, USA, 2008
3. Akhtar, N.; Johri, P.; Khan, S., "Enhancing the Security and Quality of LSB Based Image Steganography," Computational Intelligence and Communication Networks (CICN), 2013 5th International Conference on, vol., no., pp.385,390, 27-29 Sept. 2013.
4. T. Morkel J.H.P Eloff, M.S. Olivier, “An overview of Image Steganography”, information and computer Security architecture research group department of computer science, 2005.
5. Hemalatha S, U Dinesh Acharya, Renuka A, Priya R. Kamath, “a secure and high-capacity image Steganography technique” Signal & Image Processing: An International Journal (SIPIJ) Vol.4, No.1, February 2013
6. Gowtham dhanarasi and Dr.A. Mallikarjuna Prasad, image steganography using block complexity analysis, International Journal of Engineering Science and Technology (IJEST) Vol. 4 No.07 July 2012 Rahul Jain and Naresh kumar, “Efficient data hiding scheme using lossless data compression and image steganography “, International Journal of Engineering Science and Technology (IJEST), Vol. 4 No.08 August 2012
7. Siddharth Singh and Tanveer J. Siddiqui, “A Security Enhanced Robust Steganography Algorithm for Data Hiding” IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 3, No 1, May 2012
8. Dipesh Agrawal, Samidha Diwedi Sharma, “Analysis of Random Bit Image Steganography Techniques” International Journal of Computer Applications (0975 – 8887) International Conference on Recent Trends in engineering & Technology - 2013(ICRTET'2013). http://prateekvjoshi.com/2013/03/20/image-steganography/ https://www.academia.edu/14169243/A_Comparative_Study_and_Literature_Review_of_Image_Steganography_Techniques
9. Jianhua Yang, Kai Liu, Xiangui Kang, Edward K Wong, and Yun-Qing Shi. Spatial image steganography based on generative adversarial network. arXiv preprint arXiv:1804.07939, 2018.
10. Jianhua Yang, Danyang Ruan, Jiwu Huang, Xiangui Kang, and Yun-Qing Shi. An embedding cost learning framework using gan. IEEE Transactions on Information Forensics and Security, 15:839–851, 2019.