New York Science Journal

Websites:
http://www.sciencepub.net/newyork
http://www.sciencepub.net

Emails:
newyorksci@gmail.com
editor@sciencepub.net

MARSLAND PRESS
Multidisciplinary Academic Journal Publisher

STUDY ON STEGANOGRAPHY IMAGE RELATED TO DIFFERENTIATION OF ADAPTIVE PIXEL VALUE

* Prasad HM and ** Dr. Kamal Srivastava

[1]Research Scholar, Department of Computer Science, SunRise University, Alwar, Rajasthan (India)
[2]Associate Professor, Department of Computer Science, SunRise University, Alwar, Rajasthan (India)
Email: parsadworld8@gmail.com

Abstract: Nowadays, smartphones are widely used and offer powerful hardware capabilities and various communication channels. This research focuses on steganography, which involves hiding information within digital media. Specifically, we employ the Pixel Value Differencing (PVD) technique to encrypt hidden messages in the least significant bits of cover pictures. The PVD algorithm is recommended for practical purposes due to its high capacity for embedding data and low distortion rate. In this study, we provide an overview of steganography and the PVD method, followed by a detailed explanation of our implementation. Additionally, we assess the security and resilience of our method against various attacks, including statistical analysis and picture compression. Our results demonstrate that our solution remains secure and effectively retrieves concealed data even after undergoing severe compression. This research highlights the practical applications of steganography in real-world scenarios.
[Prasad HM and Dr. Kamal Srivastava. **STUDY ON STEGANOGRAPHY IMAGE RELATED TO DIFFERENTIATION OF ADAPTIVE PIXEL VALUE .** *N Y Sci J* 2024;17(3):87-90]. ISSN 1554-0200 (print); ISSN 2375-723X (online). http://www.sciencepub.net/newyork.03.doi:10.7537/marsnys170324.03.

Keywords: Steganography, Pixel Value Difference, Android, Exploiting Modification Direction.

Introduction:

The fundamental principle of the Steganography technique involves concealing confidential data or information within images, audio, or video files. It is a technology and scientific approach to hiding sensitive information by using other forms of communication or media that appear less suspicious. In our rapidly advancing technological world, the demand for data and information has increased significantly, and many functionalities rely on data as their foundation. Consequently, there is a growing need to protect messages and data that contain highly confidential content. Encryption has been the widely adopted and formal technique for achieving this goal. Encryption transforms information into a different format, and on the recipient side, the information is decrypted to its original configuration. This process is commonly known as Cryptography. Steganography, on the other hand, is viewed as an enhanced and evolved form of cryptography that focuses on hiding information within various media.

Steganography and cryptography are distinct from each other because in steganography, the code or message itself is not altered. Instead, the message is embedded within seemingly innocuous media such as images, audio, or video files, as depicted in Figure 1. This distinction gives steganography higher security implications compared to cryptography, as the hidden information is less susceptible and visible to potential intruder attacks. Various types of steganography techniques are commonly employed, including Image Steganography, Video Steganography, Text Steganography, Audio Steganography, and Network Steganography. Among these, Image Steganography, particularly using the Least Significant Bit (LSB) method, is widely utilized. In the LSB technique, the least significant parts of scattered pixels in an image are sequentially replaced with hidden messages. This method is advantageous due to its simplicity, ease of execution, and the ability to generate stego-pictures containing the secret message. However, the LSB technique has drawbacks. It is vulnerable to Steganalysis, the detection of hidden messages, and lacks any form of verification. To overcome these limitations, an alternative technique called Pixel Value Differentiation (PVD) can be used. PVD involves considering the difference between two successive pixels for message hiding. This approach is extensively used in data concealment and provides higher resistance against step analytical attacks. PVD is more effective than LSB and can conceal more data. However, it does impact the image quality more compared to LSB. Due to the distinct visual and mathematical characteristics, it is more challenging to model edges in smoother regions compared to individual pixels. Consequently, pixels located in edge regions are a better choice for concealing secret data

within an image. Changes in these regions are less noticeable, making the image appear less suspicious to potential intruders. This selection of edge regions enhances the overall security of the steganographic technique. In this paper, the provided image is converted to stego-image for hiding secret data or information within, by combining PVD technique with Canny Edge Detection [2]. This paper contributes: 1) The secret text is converted to decimal format and then further converted to binary format, ensuring an additional layer of protection. 2) Using the PVD method with the help of a modulus function, the binary representation of the secret message is embedded within the edge regions of the image. This technique makes the extraction of the embedded data more difficult [2]. 3) To extract the secret text from the image pixels, the above steps are reversed. The embedded data is retrieved by applying the reverse process, which involves utilizing the PVD method and decoding the binary representation back to the original secret message.

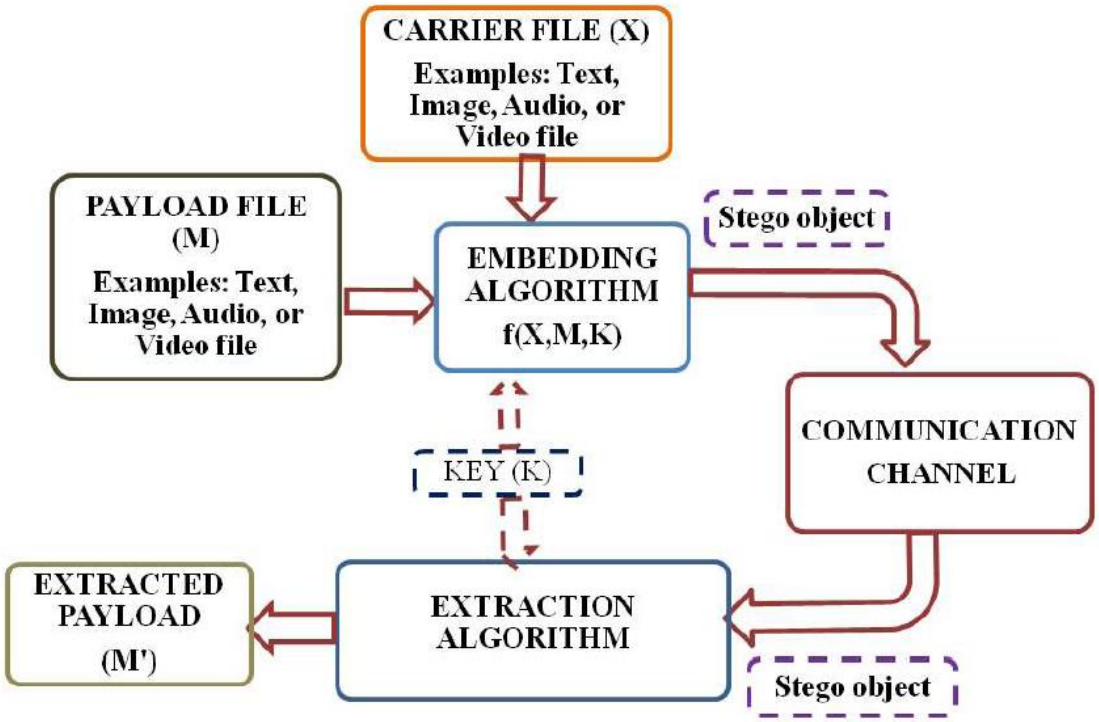

Figure 1. Basic Process of Digital Steganography

Cryptography is the technique in which encryption and decryption of secret message can be done using enciphering and deciphering algorithms. Enciphering/Encryption algorithms are used to convert plain text or secret data into an unreadable form known as cipher text. Deciphering/Decryption algorithms are used to retrieve the original plain text by deciphering the unreadable or scrambled text. Secret keys are required for both enciphering and deciphering. The strength of the cryptographic algorithm depends on the size of the key and number of iterations used in the encryption algorithm. Depending up on the nature of keys used, Cryptographic techniques can be of two types namely:- Asymmetric Cryptography and Symmetric Cryptography [2].

Symmetric Cryptography: In Symmetric cryptography, the key used for encryption as well as decryption is the same in order to maintain confidentiality. A secure key is shared among two parties in prior to communication.

Asymmetric Cryptography: In Asymmetric cryptography, two different pairs of keys are used for encryption and decryption. The keys generated are named as public and private key pairs. Then using shared public and known private key pairs, a common secret key is generated on both sender and receiver side, which will not be shared over the communication channel. Thus ensures the secrecy of common secret key calculated. Public Keys are distributed and managed by trusted public key distributors. Use of cryptographic techniques in a security system leads to

key-management problem, which is one of the major disadvantage.

Steganography has gained more and more popularity due to its versatility and its potential towards covert communication. In modern era, with the advances in computer technology, secret information can be embedded in a cover file such as digital media and the technique used is known as Steganography. It is an art and science of embedding secret payload into the contents of digital media in order to protect the data used for secret communication [5]. Digital databases that are accessed continuously by the corporate organizations over internet are not safe always and thus guaranteed the researchers to make use of Steganography techniques.

Overview of Digital Steganography

Steganography is the science or technique which embeds the secret information in a suitable multimedia carrier and further the embedded carrier file can be used for secure communication. Basic process of digital steganography is shown in figure 1.2 two inputs considered are carrier file (X) and payload data or it can be a secret message (M). The payload data is embedded inside the cover file using Steganography based encoder or data hiding/embedding algorithm considered as a function of f(X, M, K) where K is the Key used for encoding and decoding. The resulted object is called as Stego object and it can be used for secure communication. The received stego image is decoded using Steganography decoder. In General, steganography scheme consists of two phases: (a) Identifying the redundant information in carrier file. (b) Replacing or modifying the redundant bits to embed the secret message. The redundant bits are considered for the hiding process because any alterations made in these bits will not destroy the visual quality or unification of the carrier object. The strength of the steganography depends on the similarity between the resulted stego object and raw carrier object.

One of the major steganalysis tool is the human visual system that should not identify the changes in the cover file after embedding

Finally the goals of Steganography techniques are invisible secure communication with robustness and increased embedding capacity made it different from the other similar processes such as cryptography and watermarking [8]. Depending up on the way of using keys in steganography, there are three types first one is Pure Steganography where the system does not require any keys to exchange before initiating the secret communication [9]. Thus the security of pure steganography system relies on the secrecy maintained by sender and receiver. Pure steganography is preferred in many applications because it. If the hacker predicts the method of data hiding, then the system will not be secure. Second one is secret key steganography, where the communication parties exchange the secret keys in prior to begin the secret communication. In the process of transmission, the user A select a cover file and the message is embedded into cover file using embedding algorithm and the shared secret key. At the receiver side, user B decodes the received stego object using the same secret key and the decoding algorithm thus the secrecy of the system depends on communication of the secret key in a secure manner [10]. The third one is the public key steganography which does not depend on shared secret key instead it make uses the concept of public key cryptosystem where one of the keys used for the embedding purpose is published or shared among users and the other one is kept private. The algorithm designed is based on public and private key relationships [11].

Text steganography Steganography is the technique in which text files are used as cover file. The message is embedded in the text file by making certain changes in cover text file like changing the format of cover text, inserting message bits in the spaces, modifying characters of cover in an unnoticeable form and creating pseudorandom sequence of characters or make use of un conditional grammar to create readable texts. Different methods used under text steganography are Format based data hiding, Random generation of texts, statistical generation and Rhetorical techniques.

Audio steganography In this steganography, the cover file used is an audio file. The embedding process is done by changing the binary sequence of an audio signal in corresponding to payload data. The process becomes tedious when compared to other types in order to embed two different data forms that are payload and an audio signal. Kinds of audio steganography comprises of: Phase encoding, LSB parity encoding and spread spectrum techniques. In general different forms of audio file formats used for embedding are waveform audio file format, AU file format and MP3 audio file formats.

Image Steganography The type of steganography where image files are considered as cover files is called as Image Steganography. Image steganography is most popularly used because of its wide applications. Various data hiding techniques are possible using image as a cover file, and in general payload data can be embedded in two domains such as spatial domain and transform domain.

Video Steganography The type of Steganography where the cover file used is video file. The information can be embedded into digital content of video file. Since the video file is a combination of image and audio, it has enormous embedding capacity of information, which can be embedded in the moving

stream of pictures and sounds. Different types of video file formats used for data embedding are 3GP, MP-4, MPEG-1, MPEG-2, VOB, SWF and FLV.

Network Steganography Network steganography also called as Protocol Steganography, it is the method of hiding messages inside the network control protocols such as TCP/IP, User Datagram Protocol, and Internet Control Message Protocol etc. Network steganography could also be used in the covert channels of the OSI model like payload data embedded in some of the unused fields of TCP/IP protocol.

CONCLUSION

In conclusion, the purpose of this study was to investigate the efficacy of steganography as a data security method. We have proven that steganography is a practical method for protecting sensitive data by implementing and testing a steganographic algorithm. Our findings demonstrate that a cover picture may include concealed data thanks to the steganographic technique without having a substantial impact on the cover image's aesthetic appeal. We also showed that by employing the right decoding algorithms, it is possible to obtain the concealed data with great accuracy. Additionally, we assessed the steganographic algorithm's performance in terms of its capacity, resilience, and security. Our tests have demonstrated that the algorithm is capable of managing a respectable quantity of concealed data while preserving the integrity of the cover picture. The algorithm also demonstrated that it was resilient against typical operations and assaults on image processing. Overall, this effort advances the subject of data security by showcasing steganography potency as a method of protecting sensitive data. It also emphasizes how crucial it is to create reliable and secure steganographic algorithms in order to defend against future assaults. By investigating more sophisticated steganographic methods and thoroughly analyzing their efficiency in various applications and circumstances, future research might improve our findings.

REFERENCES

[1] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: survey and analysis of current methods," Signal Processing, vol. 90, no. 3, pp. 727–752, 2010.

[2] Yang C-H.2008 Inverted pattern approach to improve the image quality of information hiding by LSB substitution. Pattern Recognit. 41, 2674– 2683.

[3] Chen S-K. 2011 Amodule-basedLSBsubstitution method with lossless secret data compression. Comput. Stand. Interfaces 33, 367– 371.

[4] K. Bailey and K. Curran, "An evaluation of image-based steganography methods," Multimedia Tools and Applications, vol. 30, no. 1, pp. 55– 88, 2006.

[5] Shiv Prasad and Arup Kumar Pal "An RGB colour image steganography scheme using overlapping block-based pixel-value differencing"

[6] Islam S, Modi MR, Gupta P.2014 Edge-based steganography on coloured images. In Intelligent computing theories (eds DSHuang, Bevilacqua, JC Figueroa, P Premaratne). Lecture Notes in Computer Science, vol.7995, pp.593–600.Berlin, Germany.

[7] Wu D-C, Tsai W-H.2003 A steganographic method for images by pixel value differencing. Pattern Recognit.Lett.24, 1613– 1626.

[8] Tseng H-W, Leng H-S. 2013 A steganographic method based on pixel value differencing and the perfect square number.J.Appl.Math.2013, 189706.

[9] Liao X, WenQ-Y, ZhangJ. 2011 A steganographic method for digital images with four-pixel differencing and modified LSB substitution. J.Vis. Commun. ImageR22,1–8.

[10] Pradhan A, Sekhar KR, Swain G.2016 Digital image steganography based on seven-way pixel value differencing.

2/16/2024