Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 8, July, 2021:7471 – 7479

Research Article

Image Steganography's Challenges, Risks and Inferences in Spatial Domain

[1]K.S. Suresh, [2]Dr.T. Kamalakannan

Abstract

Steganography has found its value for a long time in digital transformation/ communications. Cryptography is the oldest method to convert a plain text into cipher text. Steganography is the art of encryption. For example, a picture is used to cover details. Steganography in the local domain plays a major role because of its compatibility with images. Steganography is a study of undetectable communication that regularly deals the methods to hide the details of existence. Normally, secret data are embedded into a text message, image, voice, audio and video. Steganography is a process of embedding private information or a message into an image commonly referred to as stego-image (image with hidden message). This paper reviews books on various forms of steganography images in the local domain for the past 5 years. The main purpose of this paper is to study the methods and its findings along with their advantage and disadvantages of existing steganography techniques. The complete configuration of steganography techniques for buildings and their structures in the local domain is reduced. Researchers have already done a lot of research on image steganography but the embedded methods may be incomplete. In this article we have explored many steganographic methods in the local domain. This paper examined various steganographic tools and covered steganography summary in its main types, classification and applications. This paper discussed various steganographic tools and techniques. Also it covers the steganographic general ideas including the impacts and applications.

Keywords: stego-image, Steganography, techniques and spatial domain.

1. Introduction

In the 15th century the name steganography was coined. Steganography is the method to hide the secret message within a known message. There are four types of Steganography namely Text, Images, Audio / Video and Protocol. The steganography process removes fragments of data with a standard pattern in a file with images, sound, text, HTML, or floppy disks with distinct, invisible particles. The purpose of steganography is a covert statement to cover communication from outsiders. There is a big difference between cryptography and

[1]Dept. of Computer Science, Rajeswari Vedachalam Government Arts College, Chengalpattu, Research Scholar, VISTAS, Chennai, India.
[2] School of Computing Sciences, Vels Institute of Science, Technology and Advanced Studies(VISTAS), Chennai, India.
[1]ksampathsuresh@gmail.com, [2]kkannan.scs@velsuniv.ac.in

Steganography. The art of encryption, includes the message unreadable by others. But it never hides the existing secret communications between them. However, this paper will treat steganography as a separate field. Other old methods of concealing information are writing tables, inscribed on the rabbit's stomach, tattooed on the head of slaves, Microdots and microfilm, the basis of war and spy movies, emerged after the invention the two are connected.

The process of steganography usually involves placing a hidden message in another form of transportation, called a manager. A secret message is embedded in the steganography site carrier. The use of steganography keys can be used to encrypt a hidden message and / or randomly in a steganography program. The basic structure of Steganography is described in the following Figure 1. The steganography process is applied and the message is removed encrypted by the image of stego when we provide the key to the unit removed by encryption.

1.1 Image Steganography

The process of steganography involves embedding a secret piece within an image is called an image steganography.

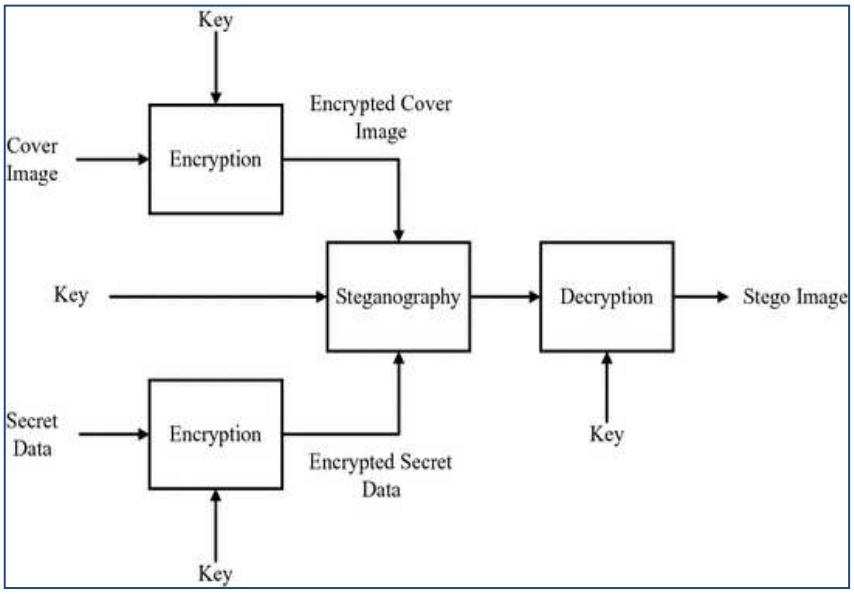

Figure -1 Basic structure of Steganography

Figure – 2 Data embedding process

Data embedding process is shown in Figure 2. The data / message were hidden inside the image in a way that prevents the embedded user from accessing the hidden data / messages.

1.2 Evaluation of cryptography and steganography :

The evaluation of crytography and steganography were done by its objectives,

Table - 1 Comparison chart between Cryptography and Steganography

S.No	Evaluation - characterstics	Cryptography	Steganography
1	Objectives	Content is protected	Secret data is communicated along with orignal data
2	Perceptual security	Easy to identify	Hard to recognize
3	Protection of announcement	It depends on privacy of key	Same as watermarking
4	Robustness	difficulty of ciphering algorithm	Detection of removing secret information
5	Key requirement	Mandatory	It depends upon the application used.
6	Yield type	"Cipher or simple text"	May be of image /text/video
7	Life time of safety	Until decoding of cipher "text"	Till secret information existence exposed
8	Medium	Data were represented in 0's and 1's (Digital)	Data were represented in 0's and 1's (Digital)
9	Recognition and Extraction difficulty	Simple and composite	"Detection and removal are complex"

1.3 Behind the Image Steganography in Spatial Domain

Steganography is used for digital communication, meaning that something is hidden in confidential information. The communication tool can be any content / controller (Fig.2), A device such as an android phone, a button or a browser-like app, Facebook that keeps confidential communications. Ways to communicate with digital files or digital data, audiovisual, network protocol and DNA. Various technical methods use the features to hide private information.

For example, the script Steganography helps to the word converter to enter the words and presently using emotional icons in a conversation to attain confidential communication. In audio steganography, it uses phase coding, spectrum distribution and low-level encryption to encrypt private information. Encryption data can be uploaded, package titles to another form such as network protocol. It uses to inform and transfer the performance of information known as "retransmission steganography". In DNA-based steganography, random features in DNA can be used to cover confidential information.

2. Background and importance

[1]Mohadad Najm Abdulwahed (Jan 2020) has released a novel version of a very important bit of exchange process, a combination of two opposing works, and a controversial map. [2]Haitao Song & Guangming Tang & Yifeng Sun & Shunxiang Yang (Jan2020) have proposed a new ADU Strategy to automatically renew the initial cost of distortion (acquired by HILL etc.) to

define interactions between multiple precision embedded fixes. [3]Ji-HweiHorng, Chin-Chen Chang and Guan-Long Li (July 2020) discuss three phases of embedding based on the AMBTC block data structure consisting of high-resolution, low-resolution and matrix in compressed image.

The [4]SerdarSolak (Sep2020) proposed algorithm uses nearby cover image pixels to encrypt confidential data with the EMSD algorithm, as well as the k-bit neutral algorithm replacement LSB. [5]Samayveer Singh (April 2019) A new data encryption system using a combination of pixel value (PVD) and low-key input (LSB) is proposed to increase data encryption capabilities.

[6]Bishwas Mandal, Anita Pradhan, Gandharba Swain (2019), proposed a new steganography procedure in place of LSB and PVD. Advances in Internet technology have created large documents and the transfer of multimedia records in the Internet. It will safeguard the documents from illegal users, the use of safety measures such as digital copy of steganography is very important.

[7]Manashee Kalita, Themrichon Tuithung & Swanirbhar Majumder (2019) proposes a local approach to the color scheme of steganography using the differentiating concept of both pixels to maximize embedding power. The proposed method takes into account the degree of tolerance of the distortion of each plane of color and the degree of variation between two neighboring pixels while taking the number of fragments that can be quoted in that pair of pixels.

[8]Nabanita Mukherjee, Goutam Paul, Saha, Debanjan Burman (2019) and Sanjoy Kumar Analyzed the Recent study about Steganography attentions on collective information without caring any signature seen on stego-media by introduce the pixel value (PVD) difference based on high power process. Embedding is not limited to two pixels of high brightness. Low-level sets are measured to increase strength. The surrounding process is also varying depends on the local variation of the pair. The encrypted information is also encrypted before embedding and the sets of pixels are randomly selected to make the path much safer. Results obtained are based on the performance of more and more images. It is evident that, the embedding process seems unpredictable and can withstand a variety of attacks. Measurement tests based on StirMark also gives the same results of the function. Assessment of results with the existing one with other modules also shows that the new method preserves a high PSNR value with improved power.

[9]Rojali, Ford LumbanGaol, Edi Abdurahman and BenfanoSoewito (June 2019) introduced a way to improve power embedding and provide unparalleled visual quality steganography and converted interval table (TFPVD).

[10] Shanti.S, R. JagadeeshKannan, Santhi.S (2018) focuses on sharing secure and confidential information in the cloud with data integrity.[11]Zhaotong Li, Ying He (2018) reviewed a system that combines pixel count separation, modulus function and particle efficiency. Differences between neighboring pixels in a network company image. The PVD function are used to embed and extract private information.

[12]Aditya Kumar Sahu. Gandharba Swain (May 2018) has studied this process based on the Pixel Transition (EC) and PSNR. The two variants are OPVDMF and OPVD. [13]Serdar solak, Umut Altinişik (oct 2018) provided the most effective way to encrypt data while transmitting secure data to an open channel. By analyzing the performance of the least Significant Bit (LSB)

and Pixel-Value Differencing (PVD) methods and comparing the Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index (SSIM) and loading values. [14]Mehdi Hussain[a,b], Ainuddin Wahid Abdul Wahab[a,*] , Anthony T. S. Ho[c] , Noman Javed[d] , Ki-Hyun Jung [e,*] (2017) introduced a data encryption system using parity-bit pixel variations and improved multi-digit recovery right. [15]Nan-I Wu & Min-Shiang Hwang (2017) described a LSB novel encryption system with very low distortion. In this program three pixels are combined as a embedded unit to hide three pieces of private data.

[16]"Weiqing Wang[1,2], Junyong Ye[1], Tongqing Wang[1], Weifu Wang[3] (2017)" An encrypted data encryption scheme based on bit-wise expansion, the proposed system rotates pixels on the cover image into two parts, that is, the highest particles (HSB) and the most important particles (LSB), and then calculate the HSB difference between adjacent pixels. Bits are added to HSBs by changing the HUMB histogram value drums. [17]Gandharba Swain (2016) A steganographic method that combines the insertion of LSB and PVD into a block, suggest a steganographic process with the existing PVD and LSB insertion with the module. The obtained value of this pixel used here is to determine the value difference of three pixels by bottom left and the top right, bottom right of the module. After that the pieces of data are hidden using these three differences in three ways. Here both vertical and horizontal lines are considered. The tables are prepared to variate the two different scores. For the first variation the PSNR has been upgraded and for the second variation the PSNR and its hiding capabilities have been upgraded.

[18]Mehdi Hussain, Ainuddin Wahid Abdul Wahab, Noman Javed" and "Ki-Hyun Jung (2016)" Hybrid Data Encryption Scheme Using Right Digit Recovery and ALSB for digital photography, First, the proposed hybrid power system improves efficiency. The use of ALSB in high-performance areas for cover images. Second, the proposed hybrid method maintains a high quality of viewing because the RMDR has a very close selection process to make the balance between stego pixels and covers. Finally, the proposed mixture process is protected from standard mathematical or single (RS) steganalysis and pixel histogram steganalysis variations.

[19]"Ismael R. Grajeda-Mar´ın, H´ector A. Montes-Venegas (B), J. Raymundo Marcial-Romero, J.A. Hern´andez-Serv´ın, and Guillermo De Ita (2016)" How to Improve TWPVD's Digital Image Steganography Method. In Digital Image Steganography, using the PVD method to avoid this problem, many additional steps can be added to correct those values, even if the pixels are considered invalid and ignored. In this paper, he adopt the Tri-way Pixel-Value Differencing method and find the correct pixel value for each pixel block designed to differentiate them with high input information and no flow or spread out pixels.

3 Inferences

Table - 2 Summary of existing Pixel Value Differencing methods

Reference	**Techniques**	**Proposed Method**	**Tool**	**Embedding capacity (bpp)**	**Visual Quality (PSNR)**db
Mohanad Najm Abdulwahed 2020	NSKA-LSB	Data hiding – using potentiality, image aspects	MATLAB	0.5	60 - 70 (avg)

		and reliability			
Haitao Song Y et al.,2020	ADU strategy	Update initial distortion cost- multiple embedding modifications	MATLAB R 2016a	0.5	26.8
Ji-HweiHorng Y et al.,2020	AMBTC	3 phases to fully leverage the AMBTC data structures	MATLAB R 2017a	0.46	30.86 (avg)
Nur Khaleeeda Mansor et al.,2020	PVD Method	Embedding methods- LSB & PVD	MATLAB	.056	40-50
Bishwas Mandal Y et al.,2019	OPVD method (modified)	steganography technique has been proposed based on the concept of adaptive Least significant bit substitution(LSB) method and PVD	MATLAB R2015a	4.025	32.63
ManasheeKalita y et al., 2019	XOR encoding technique	"color steganography method that uses a neighboring pixel pair differencing"	RS steganalysis	3.498	38.23
Pascal Maniriho, y et al., 2019	Pixel Differencing Expansion	Steganography -based on difference expansion and modulus function	Excel 7.1 Histogram	.07	56.23
SerdarSolak , UmutAltinişik 2018	PSNR, SSIM and payload performance criteria are used.	Image steganography - comparison performed by using PSNR,SSIM and payload values.	Excel 7.1 Histogram	2.7	51.656
Gandharba Swain 2018	Eight-Directional PVD Technique	steganography technique - edges in 8 directions and LSB substitution to resist	Matlab	2.37	39.31
Mehdi Hussain et al.,2017	PBPVD and iRMDR	PVD with extra parity bit used maintain visual quality (Higher range level) & iRMDR used in lower range level and maintain the steganographic security	Matlab	2.17	39.29
Muhammad et al., 2016	ALSB-MLEA	Secret data encrypted using MLE Algorithm & embedded into image using ALSB.	Excel 7.1 Histogram	1	>35

4. Research Method

Search strategy

It is a well-designed search strategy is at the heart of our step by step assessment and it will be reported in the traffic segment of my article. This technique redirects more number of papers as we will check for aptness and placement. The significance of the search strategy gives disturbs of the items which may not be available. Experts can be partners in this process.

Document Review

"The book review includes reviewing various publications in the leading database namely IEEE, Science Direct, Xplore, Scopus, ACM Digital Library, Springer, google expert, ResearchGate between 2016 and 2020."

5. Image steganography methods in spatial domain

Various Methods of obtaining the Steganography are as follows.

a) Visual detection (JPEG, BMP, GIF, etc.) b) Sound detection (WAV, MPEG, etc.) c) Statistical detection (changes in pixel patterns or LSB - Not important Bit) d) Layout Detection - View file / content properties

Other background image steganography methods are Pixel Value Difference (PVD) method, Least Significant Bit (LSB) technique, Modification Direction method(EDM), Multi-Base Notation System (MBNS), Pixel-Pair Path-based ways (PPM), Histogram-based technique, Edge-based method, Pixel Value Prediction (PVP) process, mapping method, Pixel / Block indexes, color marketing approach and machine learning approach. Steganalysis means determining the presence of a message without encrypting the message. Various steganalysis are Visual steganalysis, Statistical steganalysis, Histogram based analysis, RS steganalysis, Chi-square analysis, Bit plane analysis, Non-Structural steganalysis.

6. Challenges to Image Steganography

The power of the steganography system to encrypt data securely while it is being transferred to a network and the required supply makes it very convenient to deal with the latest features in steganography. In many areas researchers are developing a concept or specific models for career development across all local steganography. New methods have become prominent in many techniques to improve text hiding methods through image. As the use of data in photography grows day by day the image steganography techniques have been improved at a higher rate.

7. Conclusion

This article analyzed the detailed study of steganography methods at the local field for the past five years. The elementary differences between steganography and cryptography are discoursed in terms of their objectives. Examination of current embedded methods in the local domain was labeled and emphasized their benefits and functions. Steganographic performance metrics used by steganalysis are discussed. Based on the analysis, the conclusion arrived, which are represented here, may be helpful to scholars in this field.

a) Encryption of personal data before embedding is an added advantage. since it gives more safety. If a steganographic procedure is discovered by steganalysis, the invader must break the encryption to obtain confidential information.

b) As we have seen many steganographic tools, they can be illustrated by new steganalysis. But, getting encrypted records with backup encryption is costly.

c) Hybrid Steganographic Strategies: Many steganographic procedures can rise the information safety and may interfere with certain steganalysis strategies. In addition, the strengths and weaknesses of the already present models which can be used to plan a new steganographic process. The Fusion of the existing and the new steganographic model can be a good line of defense.

8. References

1. Mohanad Najm Abdulwahed (2020) An effective and secure digital image steganography scheme using two random function and chaotic map. Journal of Theoretical and Applied Information Technology, 98(1), 78-91.
2. Haitao Song & Guangming Tang &Yifeng Sun &Shunxiang Yang (Jan2020) Anisotropic distortion cost update strategy in spatial image Steganography. Multimedia Tools and Applications, 79, 1-20.
3. Ji-Hwei Horng, Chin-Chen Chang and Guan-Long Li (July 2020) Steganography Using Quotient Value Differencing and LSB Substitution for AMBTC Compressed Images. Digital Object Identifier, 8, 129347 – 129358.
4. Serdar Solak (2020), High Embedding Capacity Data Hiding Technique Based on EMSD and LSB Substitution Algorithms. IEEE Access, vol. 8, pp. 166513-166524.
5. Samayveer Singh (2020), Adaptive PVD and LSB based high capacity data hiding scheme. Multimedia Tools and Applications, 79(5).
6. Bishwas Mandal, Anita Pradhan, Gandharba Swain (2019). Adaptive LSB substitution Steganography technique based on PVD. 459-464. 10.1109/ICOEI.2019.8862579.
7. ManasheeKalita, Themrichon Tuithung &Swanirbhar Majumder (2019), An adaptive color image steganography method using adjacent pixel value differencing and LSB substitution technique. Cryptologia, 43:5, 414-437.
8. Nabanita Mukherjee, Goutam Paul, Sanjoy Kumar Saha, Debanjan Burman(2019) ,A PVD based high capacity steganography algorithm with embedding in non-sequential position. Multimedia Tools and Applications. 79, 13449–13479.
9. Rojali, Ford LumbanGaol, Edi Abdurahman and Benfano Soewito (June 2019), A High Quality Steganography Method with Twenty Five-Pixel Value Differencing. Journal of Computer Science, 15(10),1538-1545.
10. Shanthi.S ,R.JagadeeshKannan,Santhi.S(2018) ,Efficient secure system of data in cloud using steganography based crypto system with FSN. Materials Today: Proceedings, ISSN: 2214-7853, Vol: 5, Issue: 1, Page: 1967-1973
11. Zhaotong Li, Ying He (2018) Steganography with pixel-value differencing and modulus function based on PSO. Journal of Information Security and Applications, 43, 47-52.
12. Aditya Kumar Sahu .Gandharba Swain(2018) Pixel overlapping image steganography using PVD and modulus function. 3D Research, 9(3), 1-14.

13. Serdar SOLAK*, Umut ALTINIŞIK (2018) LSB Substitution and PVD performance analysis for image steganography. International Journal of Computer Sciences and Engineering. 6, 1-4.
14. Mehdi Hussain[a,b], Ainuddin Wahid Abdul Wahab[a,*] , Anthony T. S. Ho[c] , Noman Javed[d] , Ki-Hyun Jung [e,*] (2017) A data hiding scheme using parity-bit pixel value differencing and improved rightmost digit replacement. Signal Processing: Image Communication. 50.
15.Nan-I Wu[a] and Min-Shiang Hwang[b,c] (2017) A novel LSB data hiding scheme with the lowest distortion. The Imaging Science Journal, 65:6, 371-378.
16. Weiqing Wang[1,2], Junyong Ye[1], Tongqing Wang[1], Weifu Wang[3] (2017) Reversible data hiding scheme based on significant-bit-difference expansion. IET Image Processing, 11(11), 1002 - 1014.
17. Gandharba Swain (2016) A steganographic method combining LSB substitution and PVD in a block. Procedia Computer Science,85,39-44.
18.Mehdi Hussain, Ainuddin Wahid Abdul Wahab, Noman Javed and Ki-Hyun Jung (2016), Hybrid Data Hiding Scheme Using Right-Most Digit Replacement and Adaptive Least Significant Bit for Digital Images. Symmetry. *2016; 8(6):41*.
19. Ismael R. Grajeda-Mar´ın, H´ector A. Montes-Venegas(B), J. Raymundo Marcial-Romero, J.A. Hern´andez-Serv´ın, and Guillermo Delta (2016). An Optimization Approach to the TWPVD Method for Digital Image Steganography. Pattern Recognition, 9703, 125-134.