Volume 9, Issue 04, April 2024 ISSN (online): 2456-0006

International Journal of Science Technology Management and Research

Available online at: www.ijstmr.com

A Review on Image steganography

Tejaswini R. Hyalij
MSC (Computer Science)
Indira College, Malegaon

Mr. G. B. Hiray
MSC (Computer Science)
Indira College, Malegaon

Abstract-: ***Data exchange encompasses more than just personal or institutional text; it extends to digital media like images, videos, audio, and animations exchanged over the Internet. Ensuring the security and speed of transmission for such media is crucial. This study proposes a novel approach to conceal a grayscale image within a larger color image using a steganography map that integrates chaotic and random functions, each 16 bytes in size. Experimental results demonstrate the effectiveness of the method based on various metrics such as mean squared error, signal-to-noise ratio, peak signal noise rate, embedding capacity, entropy, and histogram. This technique enables swift hiding and extraction of ciphertext within grayscale images, making it challenging for attackers to discern between the original and stego images visually due to their nearly identical correlation coefficient, thus effectively concealing information on the Internet..***

Keywords: Chaotic Function, Color Image, LSB Technique, steganography

I. INTRODUCTION

Safeguarding private data transferred via networks is highly necessary. [1] [2]. These data include not only personal text information or information about institutions and the government, but also digital media via the Internet, such as everything, whether texts, images, videos or audio, and animation [3] [4]. These media need high-security protection and high speed during its transmission from one site to another [5]. The exchange of all media, whether digital or text, is highly susceptible to intrusive attacks, especially at the present time, where tools and methods that can violate privacy [6][7], data security, and safety are available. Therefore, researchers determine more complex hiding methods and discover how these algorithms suffer from easy access by attackers [8][9]. Some algorithms suffered from slowness during hiding. Thus, this research introduces a steganography method. The proposed method is better than the previous approach, where the steganography map depends mainly on merging two maps. Map1 consists of 16 numbers generated from chaotic functions, whereas map2 consists of 16 numbers generated from the randomized function that generates numbers between ranges 0 and 3. The final map is obtained after merging these maps. The final map shows gray images of different sizes, and resolutions are hidden in color images with large size. This proposed method was characterized by the fact that the method of concealment is difficult to break and has a high level of safety and protection.

II. LITERATURE SURVEY

Arshiya S. Ansari, Mohammad S. Mohammadi, and Mohammad T. Parvez [10] proposed a masking method that is suitable for various image formats, particularly for the cover image. This method has many benefits, including the application of unified security to all image formats, the ability to select the cover images that are most appropriate for the length of the data and network bandwidth. The results of this method are very effective and efficient

Yasir Ahmed Hamza, Nada Elya Tewfiq, and Mohammed Qasim Ahmed [11], along with visual coding, suggested improving image masks. Images were captured with a size of 128x128. Binary images are encrypted by sharing (2 out of 2), from which two secret participations are generated during the entry process, and the cover image is divided into three layers (RGB) with a size of 512x512. The method starts by converting the first layer of blue color through the discrete Shearlet transform (DST), resulting in the first secret participation in the first layer (blue) converted on the image masks. The criteria are applied to the experimental results, and the first image's participation is extracted from the encrypted image using the blue layer's coefficients and XORed. The second secret participation is used to create the secret logo for the original image. Then, the results obtained were in accordance with the criteria's standards. This suggested approach was coded to compare with the research from our work (EISU (DST and SSH)).

Raheem Abdul Sahib Ogla [12] proposed a method of masking based on the spiral search machine, where they used the measures of the structural index to obtain the image quality, retrieved accuracy, and improved quality. The results showed that the use of evaluation criteria, mean squared error (MSE) and peak signal-to-noise ratio (PSNR), improved the image quality by approximately 87%. Our research was compared with the suggested approach, and the proposed method was labeled and compared (SBSTUSSMFHSVCI).

Srushti S Yadahalli, Shambhavi Rege, and Dr. Reena Sonkusare [13] relied on the implementation of masking on two methods, the first (LSB) and the second (DWT). The image to be transferred was explained, encoded, and decoded using these methods, and then analyzed using image parameters. This proposed method obtained highly efficient results after applying the criteria. This suggested approach was written to compare with our work (IAAOISU LSB and DWT).

Jiaohua Qin, Yuanjing Luo Xuyu Xiang, Yun Tan, and Huajun Huang [14] covered the main areas of coverless image steganography research, which comprises more than 50 significant contributions. The study includes the underlying structures, pre-processing, feature

extraction, production of hash sequences, and mapping relationships. The potential for future study is also highlighted, along with an assessment of the current methodologies.

Muhammad Aminul Islam, Md. Al-Amin Khan Riad, and Tanmoy Sarkar Pias [15] utilized an image as the cover object, and text is used as a secret message. Images in 24-bit RGB color are utilized for coverage and hiding purposes. This approach transforms a secret image into a new image called share2 image using a new image named share1. People can typically readily obtain the secret message if they are aware of the extraction technique. Visual encryption adds an extra layer of protection by using a key that is created by somebody once. We guarantee secured image steganography by using the suggested technique.

S. Sravani and R. Raniith [16] focused on steganography utilizing the LSB method. The method entails cloaking a secret image under a cover image before sending it via the internet. Text, images, audio clips, and video files can be used with this technique. Here, steganography is designed to conceal the position of a region (for example, in the form of a map) inside a cover image and send the image over the internet. For its use in security-based applications, the performance of this approach has been examined using MSE and PSNR values.

III. SYSTEM ARCHITECTURE

In the proposed system we concentrate on finding some algorithm to hide the data inside images using steganography technique. An algorithm is designed to hide all the data inputted within the image to protect the privacy of the data. Then, the system is developed based on the new steganography algorithm This proposed system provides the user with two options encrypt and decrypt the data, in encryption the secret information is hiding in with image file, and on the other side the decryption is getting the hidden information from the stego image file, and also the user can show the image size after and before the encryption. The processes of encryption and decryption of the data file consists of: Providing security for the data to be transmitted through network using steganography. Proposing an approach for hiding the data within an image using a steganographic algorithm which provides better accuracy and quality of hiding. Microsoft Techniques is used through the .NET framework to extensively analyze the functions of the LSB algorithm in steganography. Texts and other file formats are encrypted and embedded into an image file which is then transferred to the destination

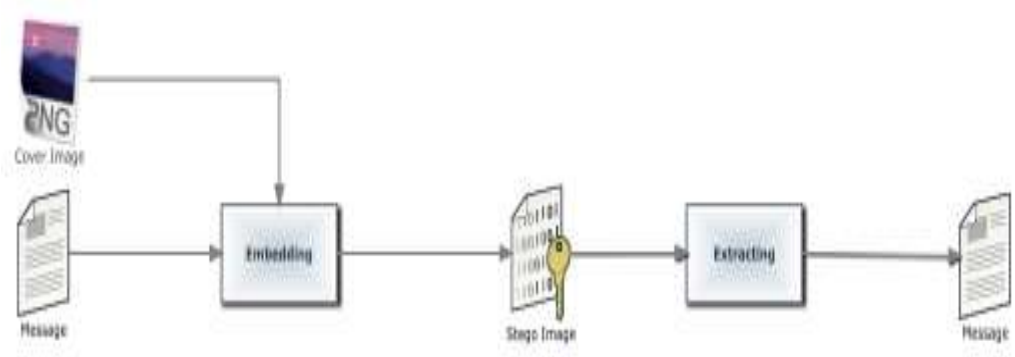

Figure 1. Basic architecture

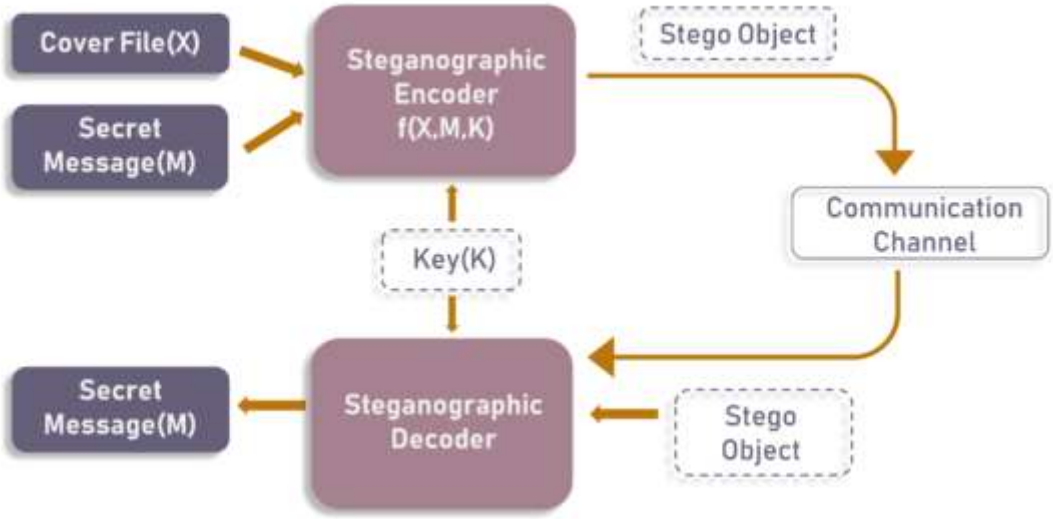

Figure 2. Detail System architecture

CONCLUSION

The secure communication of information is of much essence in today's world. Day per day eavesdropping are going on during the confidential information transmission; may it be the banking details of a bank, the call taping of people for blackmailing, the information leakage through unsecure communication media etc. Thus, concerning about these aspects, Image Steganography is the application for the organizations such as police department to hide confidential police details like strictly confidential criminal details, secret missions, police strategy etc. inside an image file. Also this technique can be widely applicable to deliver required confidential matters even through social networking sites where people will not even think that the image could hold something else. The message is highly secure since it has double-layer protection: encryption and steganography, and has wide range of applications in various sectors.

REFERENCE

1. Nandhini Subramanian, Omar Elharrouss, Somaya Al-Maadeed, And Ahmed Bouridane, "Image Steganography: A Review Of The Recent Advances", Ieee Access, Received December 27, 2020, Accepted January 7, 2021, Date Of Publication January 25, 2021, Date Of Current Version February 10, 2021. Doi 10.1109/Access.2021.3053998.
2. Dalal N. Hmood, Khamael A. Khudhia, Mohammed S. Altaei, "A Proposed Steganographic Method for Embedded Image In Audio File," International Journal of Computer Science and Security (IJCSS), Volume (6): Issue (2): 2012.
3. Shivam Ilasariya, MCT's Rajiv Gandhi Institute of Technology, Mumbai, India, Parth Patel, Vatsal Patel, and Swapnil Gharat, "Image Steganography Using Blowfish Algorithm and Transmission via Apache Kafka", IEEE, 2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT), Date Added to IEEE Xplore: 25 February 2022, Tirunelveli, India, DOI: 10.1109/ICSSIT53264.2022.9716292.
4. Juhi Singh and Mukesh Singla, "A Novel Method of high-Capacity Steganography Technique in Double Precision Images", IEEE,2021 International Conference on Computational Performance Evaluation (ComPE),12 April 2022, Shillong, India, DOI: 10.1109/ComPE53109.2021.9751905.
5. Mehdi Sharifzadeh, Mohammed Aloraini, and Dan Schonfeld, "Adaptive Batch Size Image Merging Steganography and Quantized Gaussian Image Steganography". 2019 IEEE ACCESS. DOI 10.1109/TIFS.2019.2929441.
6. Baqer A Hakim, Ahmed Dheyaa Radhi, and Fuqdan AL-Ibraheemi," An innovative and robust technique for human identification and authentication based on a secure clinical signals transmission", Int. J. Nonlinear Anal. Appl. 13 (2022) No. 1, 603-613 ISSN: 2008-6822 (electronic) ,doi.org/10.22075/ijnaa.2022.5542.
7. S. Sravani and R. Ranjith, "Image Steganography for Confidential Data Communication", IEEE, 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT),03 November 2021, Kharagpur, India, DOI: 10.1109/ICCCNT51525.2021.9579814.
8. Azhaar Akram Abdallah and Alaa Kadhim Farhan, "A Proposed Image Encryption Algorithm Based on Multi ChaoticSystem, " Iraqi Journal of Science, 2022, Vol. 63, No. 1, pp: 324-337DOI: 10.24996/ijs.2022.63.1.31.
9. Arnold Gabriel Benedict, "Improved File Security System Using Multiple Image Steganography" Publisher: IEEE, Date Added to IEEE Xplore: 29 August 2019, INSPEC Accession Number: 18958412, DOI: 10.1109/IconDSC.2019.8816946.
10. Arshiya S. Ansari, Mohammad S. Mohammadi, and Mohammad Tanvir Parvez, "A Multiple-Format Steganography Algorithm for Color Images" Publisher: IEEE, Date of Publication: 29 April 2020, DOI: 10.1109/ACCESS.2020.2991130.
11. Yasir Ahmed Hamza, Nada Elya Tewfiq and Mohammed Qasim Ahmed, "An Enhanced Approach of Image Steganographic Using Discrete Shearlet Transform and Secret Sharing", Baghdad Science Journal P-ISSN: 2078-8665 Published Online First: July 2021 2022, 19(1): 197-207 E-ISSN: 2411-798, DOI: http://dx.doi.org/10.21123/bsj.2022.19.1.0197.
12. Raheem Abdul Sahib Ogla "Symmetric- Based Steganography Technique Using Spiral-Searching Method for HSV Color Images", Baghdad Science Journal Vol.16(4) 2019, DOI: http://dx.doi.org/10.21123/bsj.2019.16.4.0948.
13. Srushti S Yadahalli, Shambhavi Rege, and Dr. Reena Sonkusare, "Implementation and analysis of image steganography using Least Significant Bit and Discrete Wavelet Transform techniques", Proceedings of the Fifth International Conference on Communication and Electronics Systems (ICCES 2020), IEEE Conference Record # 48766; IEEE Xplore ISBN: 978-1-7281-5371-1.
14. Jiaohua Qin, Yuanjing uo, Xuyu Xiag, Yun Tan,andd Huajun Huang, "overless Image Steganography: A Survey", IEEE Access,25 November 2019, DOI 1 0.1109/ACCESS.2019.2955452.
15. Muhammad Aminul Islam, Md. Al-Amin Khan Riad, and Tanmoy Sarkar Pias, "Enhancing Security of Image Steganography Using Visual Cryptography", 2021 2nd International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST), IEEE,05-07 January 2021, DOI: 10.1109/ICREST51555.2021.9331225.
16. S. Sravani and R. Raniith, "Ima Steganography for Confidential Data Communication",202 12th International Conference on Computing Communication and Networking Technologies (ICCCNT), IEEE,03 November 2021, DOI: 10.1109/ICCCNT51525.2021.9579814.
17. Rupali Bhardwaj and Vaishali Sharmab, "Image Steganography Based on Complemented Message and Inverted bit LSB Substitution," 6th International Conference On Advances In Computing & Communications, ICACC 2016, 6-8 September 2016, Cochin, India.
18. Umme Sara1, Morium Akter, and Mohammad Shorif Uddin, "Image Quality Assessment through FSIM, SSIM, MSE, and PSNR—A Comparative Study", Journal of Computer and Communications Vol.07 No.03(2019), Article ID:90911,11 pages 10.4236/jcc.2019.73002.
19. De Rosal Igantius Moses Setiadi, "PSNR vs SSIM: imperceptibility quality assessment for image steganography", Multimedia Tools and Applications, Published: 03 November 2020.
20. Tom Carter, "An introduction to information theory and entropy", Complex Systems Summer School, September 3, 2014.
21. A. K. Farhan, N. M. G. G. Al-Saidi, A. T. Maolood, F. Nazarimehr, and I. Hussain, "Entropy Analysis and Image Encryption Application Based on a New Chaotic System Crossing a Cylinder," Entropy, vol. 21, no. 10, p. 958, 2019, DOI: 10.3390/e21100958.
22. Azhaar Akram Abdallah and Alaa Kadhim Farhan, "A New Image Encryption Algorithm Based on Multi Chaotic System", Iraqi Journal of Science, 2022, Vol. 63, No. 1, pp: 324-337, DOI: 10.24996/ijs.2022.63.1.31.
23. Mohammed Mahdi Hashim and Mohd Shafry Mohd Rahim," Image Steganography Based On Odd/Even Pixels Distribution Scheme and Two Parameters Random Function". Journal of Theoretical and Applied Information Technology, 30th November 2017. Vol.95. No 22.

24. Hiba Abdel-Nabi and Ali Al-Haj, "Frequency domain-bas data hiding for encrypted medical images", Intelligent Data Security Solutions for e-Health Applications, 2020,https://doi.org/10.1016/B978-0-12-819511-6.00002-9.
25. Serdar Solak, "High Embedding Capacity Data Hiding Technique Based on EMSD and LSB Substitution Algorithms", Publisher: IEEE, 10 September 2020, ISSN: 2169-3536, DOI: 10.1109/ACCESS.2020.3023197.
26. Ammar Mohammed Ali And Alaa Kadhim Farhan ”Enhancement of QR Code Capacity by Encrypted Lossless Compression Technology for Verification of Secure E-Document, ” in IEEE Access, vol. 8, pp. 27448-27458, 2020, DOI: 10.1109/ACCESS.2020.2971779.
27. Upendra KumarAcharya and SandeepKumar, "Genetic algorithm based adaptive histogram equalization (GAAHE) technique for medical image enhancement", Optik, Volume 230, March 2021, 166273,doi.org/10.1016/j.ijleo.2021.166273.
28. Kaiser A. Reshak, Ban N. Dhannoon, and Zainab N. Sultani,” Explicit feedback-based movie recommendation system: A survey," AIP Conference Proceedings 2290, 040009 (2020), doi.org/10.1063/5.0027433.