IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Concealment Of Information In Images Using The Technique Of Steganography

Neha Dhagay

Student
Computer Science and Engineering
Institute of Aeronautical Engineering, Hyderabad, India

Abstract: In today's day and age, the art of sending and displaying hidden information, especially in public places, has proven to be essential. The topic of concealing and transferring data has been called to attention and thus faced many challenges. With the widespread of innovations in the aspect of technology and with the easy access of fast Internet, the ability for information to be distributed over the world has become quite easy and economical. This has in turn led people to worry about their privacy. The topic of steganography has been proposed to help overcome this breach. Steganography is a technique that helps prevent unauthorized users from having access to essential data. This feature helps in providing various methods with which users can encrypt and entangle their information with other information (preferably images). This process helps conceal the information you would like to stay hidden in such a way that malicious attackers fail to easily identify it. For the process of steganography, various methods have been proposed so far for hiding information in different cover media. It is a widespread knowledge through which encryption lends a hand in providing various techniques to secure channels for the aspect of communicating entities. Alas, due to the lack of covertness on the respective channels, any malicious user, such as an eavesdropper, can easily identify the encrypted streams by performing various statistical tests and entrap them for further cryptanalysis. In this paper, we have proposed a way to encrypt a piece of text in a random image on the line of hiding information on the output screen of the instrument. The image is then sent to the receiver and there is no threat of malicious activity.

Index Terms **- Information hiding, Least Significant Bit, Communication, Conceal, Secure Transmission**

I. INTRODUCTION

Communication is a desideratum in every aspect. Due to this, major developments have occurred in the field of science utilized by masses everywhere. Be as that may, complications arise with maintaining the confidentiality and vulnerability of the data communicated. Due to this, the need for information security arises. For the process of communication of data, several techniques of confidential communications using the internet or the telephone have been established. However, these techniques of protecting the data might not be up-to-par. Other methods like cryptography and/or steganography are widely trending. The process of cryptography ensures that the data is altered into a form that is encrypted using the help of an encryption key that lies only in the hands of the sender and the receiver. No other party has access to the data without the proper encryption key. Though, some altercations arise during the transmission of the information. The suspicion of an attacker is likely to be aroused in turn resulting in the interception of the data. For overcoming these frailties present in the cryptography process, we turn towards the process of steganography. The art of concealing data and transmitting the communication while camouflaging the concealed information is called steganography. Here, the data is transmitted without revealing the existence of data. This technique is a trending topic in the field of cryptography. The key point of the process is to properly communicate the data in such a manner that any third-party doesn't even have an inkling towards the presence of data being transmitted. The process of steganography stresses the topic of covertness more than its other partners like cryptography. The attackers can easily see that data is being transmitted through the communication channels in the cryptographic process but in the case of steganography, the existence is not known at all. The process works on the way of "embedding" the data into cover media – video clips, audio clips, image clips, text clips, etc. The fusion of steganography and other security protocols in the information communication channels utilized in the communication process has boosted security immensely

II. EXISTING SOLUTION

A prominent implementation of the steganography technique is digital watermarking. In this practice, the data is obscured with the help of a digital signal. The watermark created does not budge with the addition of external elements such as- audio, video, imagery or text for the purpose of maintaining the authenticity of data. The classified information then entangles with the primordial data.

The technique of digital watermarking has its implementations as well. They comprise of prevention of duplication of data (or at least the control of it), authorization of the personnel, monitoring the broadcast of the data, checking the authenticity of identity cards, keeping account of fraud and the detection of the data being tampered, medicinal approaches, etc.

In taking into account the visibility, we can classify the process into two segments- visible and invisible. In the case of visible watermarking, the watermark placed on the data is visible to all those who look upon it- let it be an image or a piece of text. More than often not, the logo of a company is placed upon the image to help recognize the owner of the data. Artists usually watermark their art when posting it to help preserve the authenticity or as an anti-theft method. This conveys that the particular information can only be used with the permission of the owner.

On the other hand, the process of invisible watermarking incorporates the elements such as audio, video, imagery or text onto the data creating an "invisible watermark" that resembles the original data. This helps in the protection against the data being copy-righted. This method is advantageous in recognizing the original creator.

A machine manipulates images as a group of picture elements called pixels, as a matter of reality. Each pixel reflects a stream of binary numbers representing the intensity or color of the pixel. Photos can be classified into two categories of images, based on color. One is a grayscale image that has 1 byte for each pixel (8 bits), and the second is a color image that has 3 bytes for each pixel (24 bits).

The 8-bit picture comprises of 256 separate palettes of gray. It will view this type of image as a black-and- white correspondent. There are three basic colors for a 24-bit image- Red, Green, and Blue (RGB). Three bytes are used to represent each pixel. Each byte relates to the RGB intensity of the three primary colors. The resultant picture formed has a good quality, and there are more than 16 million different colors in the number of palettes.

Images are split into several styles, depending on extensions, such as Joint Photographic Experts-JPEG, Bitmap-BMP, Portable Network Graphics-PNG, Graphics Interchange Format-GIF, Tagged Image File Format- TIFF, and so on. Most of these extensions use the RGB format to display pixel color strength.

Web page scripting, such as HTML, uses RGB, where one primary color is represented by two hexadecimal digits.

This suggests that there seems to be six hexadecimal digits to every pixel. For instance, the yellow color can be established with the full red color (decimal 255, hex FF) whereas the full green color can be created with the pixel value '#FFFF00' in the hexadecimal system number. Images are of variable size, relying largely on the pixel density and the bit rate in each pixel as well.

The 8-bit gray input image comprises of a 320 by 240-pixel resolution proportional to 75 kilobytes. The resolution of a full-color picture would be 225 kilobytes. When communicating via the internet, it is crucial to reduce image file sizes. Throughout recent times, numerous compression methodologies have been introduced for this function.

Lossy and lossless compressions, which are extensively included in image processing, are the 2 most frequent compression styles. In the case of BMP, GIF, and JPEG file image formats, compression processes are especially valuable. One such technique uses the Lossy compression scheme to broaden the file similar to the size of the original file utilizing JPEG images.

Lossless compression, on the other hand, is a methodology that utilizes the original image to be recovered by the implementation of some program. Two types of images that use the same framework are GIF and 8-bit BMP. The protected data called the logo will sometimes be integrated into the host data in the convolution operation to call cover data and send it to the destination

III. PROPOSED SOLUTION

Numerous steganography techniques have been put forth for the requirement of protection and extraction of data. One such technique focuses on the least significant bit of the pixels present in an image. Several enhancements were designed to increase the level of security of the LSB framework. LSB is an improperly secured technique of storing hidden messages and by allocating 8 bytes of the carrying image to store one character of the message, the mechanism of data hiding can be enforced.

The binary version of the character is necessary by LSB, and each bit of this version can be inserted in the least bit of the selected byte of the image kept. Low mean square error (MSE) values and high peak signal to noise ratio (PSNR) values are the advantages of the LSB-based methods, which make it very hard for the human eye to notice abnormalities in the holding picture.

Some scholars have theorized a color picture technique through which the encryption-decryption technique can be done with a moderate throughput and is dependent on the process of matrix reordering. One such method has been proposed in the aspect of digital color images which can be achieved by applying matrix multiplication. This strategy offers useful metrics of efficiency and a high degree of protection, but the capacity of the private encrypted data used for encryption-decryption is very vast and complex. On another note, large memory size is required for the safe storage of the image.

Instead of linear functions, certain authors gave forth a pattern of image encryption-decryption that solely depends upon an algorithm chaotic in nature utilizing power and tangent functions. The encryption method is a one-time password scheme and is more reliable than the DES algorithm (but not enough). Also, it does have low-efficient, high encryption-decryption time and low throughput.

Focusing on the utilization of a chaos-controlled operation, a technique of color image encryption-decryption was implemented. There is a low throughput for both versions of this method.

IV. METHODOLOGY

Concealing the Information onto the Image

Attempting to hide a secret message can be enforced by adopting the following measures in a covering color image:

1. Incorporating the object which is the data to be encrypted onto the image

   In this process, we first select the image which we are going to use as a base for the data to be encrypted. Then, we produce the "secret message". Following this, we decide where the message must be encrypted on the image. This is based off on the starting and ending positions of the message on the image. Lastly, we insert the message character-by-character onto the image. Doing so, we reserve a byte for each character present in the message. Finally, we then save the base image.

2. Carrying out the encryption process on the image

   Now we take the image onto which we have encrypted the message on and then transform it into a 3-dimensional matrix which maps the colors into a 2-dimensional matrix. Then, we partition the produced matrix into chunks that are of equivalent size. We then take out a 4x4 matrix (0-255) which is to be utilized as an encryption key that can be used to encrypt and decrypt the data. To get an encrypted form of the 2-dimensional matrix, we apply the operation XOR onto each and every block. After this, we re- transform the 2-dimensional matrix back into its 3-dimensional format to get the colored version of the image encrypted. Finally, we save this image.

Unsheathing the Encrypted Message

To obtain the subliminal code etched onto the image, the following steps must be acted upon:

1. Decryption based upon the color

   Procure the image which has been encrypted and transform the 3-dimensional matrix which gives color to the image into a 2-dimensional form and then partition the produced matrix into sections of 4x4 chunks. Then, the matrix which has been acting as the encryption key is procured and each block is made to perform XOR operation with the key to obtain the decrypted matrix. This matrix is in a 2-dimensional format. This must then be transformed to its 3-dimensional equivalent to show the colored image.

2. Extraction of the concealed data

   In this part, we take the base image and withthe help of the decryption key, extract and obtain the message character-by-character.

V. IMPLEMENTATION AND EXPERIMENTAL RESULTS

The technique proposed is implemented and various measures are taken. Images of varying sizes and forms are used. To demonstrate the enhancement of effectiveness, the methodology proposed is implemented in two phases- the secret is integrated and then it is extracted.

The following "HII" message, 3 characters long, is implanted by first using the selected position and then using the LSB procedure.

The message can be incorporated into the image numerous times until which the final level of security we wish to reach has been fulfilled.

The performance of the selected position method proposed is superior to the performance of the LSB method (including time and throughput of encrypting and decrypting) and the SNR and MSE values for the LSB method are better than those of the selected position method proposed. These parameters are not crucial as this second stage is the holding image encryption, so it should be MSE and PSNR.

Encryption-decryption is the second stage of hidden message hiding-extracting. Using the same images and applying the process of encryption and decryption repeatedly by segmenting the image matrix into equivalent blocks, the output of the first step is taken and the process is repeated several times. The results show a high MSE value between the holding image and the decrypted one, which is a good indicator.

VI. CONCLUSION

While the internet has many perks, it has also opened up a whole new opportunity for hackers and privacy breaches to threaten our privacy and intellectual property. Since these problems appeared, numerous approaches have been introduced the help diminish them. Steganography is one suitable tactic for guarding data via the internet.

REFERENCES

[1] Weixuan Tang, Shunquan Tan, Bin Li, and Jiwu Huang (2017) Automatic steganographic distortion learning using a generative adversarial network. IEEE Signal Processing Letters, 24(10): pp.154715

[2] D. Hu, L. Wang, W. Jiang, S. Zheng, and B. Li, ''A novel image steganography method via deep convolutional generative adversarial networks,'' IEEE Access, vol. 6, pp. 38303–38314, 2018.

[3] W. Tang, B. Li, S. Tan, M. Barni, and J. Huang, ''CNN-based adversarial embedding for image steganography,'' IEEE Trans. Inf. Forensics Security, vol. 14, no. 8, pp. 2074–2087, Aug. 2019.

[4] V. U. Sameer and R. Naskar, ''Universal wavelet relative distortion: A new counter–forensic attack on photo response non-uniformity-based source camera identification,'' in Proc. Inf. Secur. Pract. Exper. (ISPEC). Cham, Switzerland: Springer, 2018, pp. 37–49.

[5] S. Li and X. Zhang, ''Toward construction-based data hiding: From secrets to fingerprint images,'' IEEE Trans. Image Process., vol. 28, no. 3, pp. 1482–1497, Mar. 2019.

[6] M. Yang, W. Zhao, W. Xu, Y. Feng, Z. Zhao, X. Chen, and K. Lei, ''Multitask learning for cross- domain image captioning,'' IEEE Trans. Multimedia, vol. 21, no. 4, pp. 1047–1061, Apr. 2019

[7] X. Liang, Z. Hu, H. Zhang, C. Gan, and E. P. Xing, ''Recurrent topic-transition GAN for visual paragraph generation,'' 2017, arXiv:1703.07022. [Online]. Available: http://arxiv.org/abs/1703.07022

[8] X. Wang, A. Shrivastava, and A. Gupta, ''A-Fast- RCNN: Hard positive generation via adversary for object detection,'' 2017, arXiv:1704.03414. [Online]. Available: http://arxiv.org/abs/1704.03414

[9] S. Rajeswar, S. Subramanian, F. Dutil, C. Pal, and A. Courville, ''Adversarial generation of natural language,'' 2017, arXiv:1705.10929. [Online]. Available: http://arxiv.org/abs/1705.10929

[10] J. Li, W. Monroe, T. Shi, S. Jean, A. Ritter, and D. Jurafsky, ''Adversarial learning for neural dialogue generation,'' 2017, arXiv:1701.06547. [Online]. Available: http://arxiv.org/abs/1701.06547

[11] A. Cherian and A. Sullivan, ''Sem-GAN: Semantically-consistent imageto-image translation,'' in Proc. IEEE Winter Conf. Appl. Comput. Vis. (WACV), Waikoloa Village, HI, USA, Jan. 2019, pp. 1797–1806.

[12] R. Zhang, S. Dong, and J. Liu, ''Invisible steganography via generative adversarial networks,'' Multimedia Tools Appl., vol. 78, no. 7, pp. 8559–8575, Apr. 2019

[13] J. Zeng, S. Tan, B. Li, and J. Huang, ''Large-scale JPEG image steganalysis using hybrid deep- learning framework,'' IEEE Trans. Inf. Forensics Security, vol. 13, no. 5, pp. 1200–1214, May 2018, doi: 10.1109/ tifs.2017.2779446.

[14] A. Nguyen, J. Clune, Y. Bengio, A. Dosovitskiy, and J. Yosinski, ''Plug & play generative networks: Conditional iterative generation of images in latent space,'' in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR), Honolulu, HI, USA, Jun. 2017, pp. 3510–3520.

[15] Y. Jing, Y. Yang, Z. Feng, J. Ye, Y. Yu, and M. S J. Li, X. Yang, X. Liao, F. Pan, and M. Zhang, ''A game-theoretic method for designing distortion function in spatial steganography,'' Multimedia Tools Appl., vol. 76, no. 10, pp. 12417–12431, May 2016.

[16] Y. Zhang, W. Zhang, K. Chen, J. Liu, Y. Liu, and N. Yu, ''Adversarial examples against deep neural network based steganalysis,'' in Proc. 6th ACM Workshop Inf. Hiding Multimedia Secur. (IH&MMSec), 2018, pp. 67–72

[17] D. Volkhonskiy, I. Nazarov, and E. Burnaev, ''Steganographic generative adversarial networks,'' 2017, arXiv:1703.05502. [Online]. Available: http://arxiv.org/abs/1703.05502

[18] Y. Wang, K. Niu, and X. Yang, ''Information hiding scheme based on generative adversarial network,'' J. Comput. Appl., vol. 38, no. 10, pp. 2923–2928, 2018.

[19] W. Tang, S. Tan, B. Li, and J. Huang, ''Automatic steganographic distortion learning using a generative adversarial network,'' IEEE Signal Process. Lett., vol. 24, no. 10, pp. 1547–1551, Oct. 2017.

[20] G. Xu, H.-Z. Wu, and Y.-Q. Shi, ''Structural design of convolutional neural networks for steganalysis,'' IEEE Signal Process. Lett., vol. 23, no. 5, pp. 708–712, May 2016.

[21] M. Chaumont, ''Deep learning in steganography and steganalysis from 2015 to 2018,'' 2019, arXiv:1904.01444. [Online]. Available: http://arxiv.org/abs/1904.01444

[22] Alec Radford, Luke Metz, and Soumith Chintala. (2016) Unsupervised representation learning with deep convolutional generative adversarial networks. In Proceedings of International Conference on Learning Representations (ICLR)

[23] K. He, X. Zhang, S. Ren and J. Sun. (2016) Deep Residual Learning for Image Recognition. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp.770-778