

Cryptography and Steganography: New Approach

¹Hameem Mohammed, ²Vipin Vasu A. V

¹P. G. Student, ²Associate Professor
Dept. of Computer Engineering,
College Of Engineering, Thiruvananthapuram, Kerala.

Abstract: In many Internet applications, digital communication is undergoing visible and continuing development. As a result, secure communication sessions must be made available. The security of data transferred across a worldwide network has become a critical issue in network performance measurements. As a result, data confidentiality and integrity are required to prevent eavesdroppers from accessing and utilising transmitted data. Steganography and cryptography are two significant techniques used to secure networks. In this study, we examine many strategies for merging cryptography and steganography techniques in a single system. Furthermore, we discuss the contrasts between cryptography and steganography. The goal of this study is to create a novel method for hiding secret information in a picture, audio, or video by leveraging the benefits of combining cryptography and steganography. To avoid assaults, the message is encrypted using the AES technique and the key is hashed using SHA-2. Following that, we modified the LSB algorithm by adding a key to make the hiding process non-sequential. The results obtained show that our proposed strategy is promising in terms of robustness and security.

Keywords: Steganography, Cryptography, Least Significant Bit (LSB), encryption, decryption, Stego image, Color image, Random embedding.

Introduction:

Information security has become a major concern in our digital lives. The growth of new transmission technologies necessitates a specialised strategy of security procedures, particularly in the condition of data communication. The importance of network security grows with the amount of data carried across the Internet. The most important approaches for information security are cryptography and steganography. [1-3]

The value of the confidential data obtained by assaulting the system is the most crucial reason for the attacker to benefit from intrusion. Hackers can disclose the data, change it, distort it, or use it in more complicated assaults. One solution to this problem is to merge cryptography and steganography into a single system. [4-5]

Cryptography:

Cryptography is a conventional way for ensuring the privacy of communication between parties. This method is a form of secret writing in which plaintext is encrypted with a key and then passed between participants across an unsecure channel. The ciphertext can be decoded to the original plaintext with a valid key. Nobody can retrieve the plaintext unless they know the key. Many aspects required for secure communication through an unsecure channel, such as confidentiality, privacy, non-repudiation, key exchange, and authentication, rely on cryptography. [6]

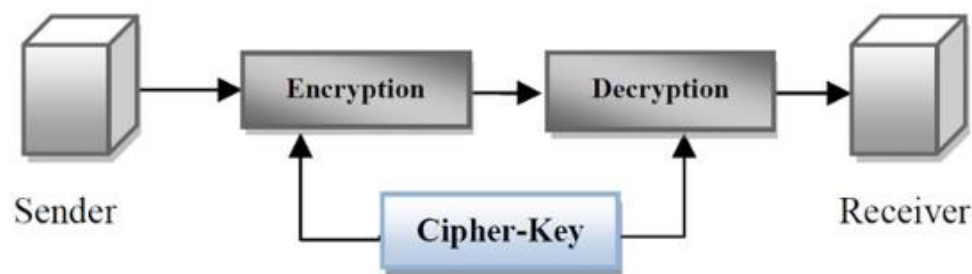


Figure 1: Cryptography System

There are two types of cryptographic algorithms for data security. The following approaches are frequently employed to achieve the goal: public-key cryptography, secret key cryptography, and hash functions. The length and kind of keys used are determined by the encryption technique.

Steganography:

Can be described as the science of concealing and conveying data through seemingly reliable carriers in order to conceal the data's existence. As a result, there is no awareness of the message's existence in the first place. If a person looks at the cover in which the information is hidden, he or she will have no idea that there is any covering data, and hence will not attempt to decode the data. [7] The stego system encoder can introduce the secret information into the cover media using a specific algorithm. A hidden message can be plaintext, an image, cypher text, or anything else that can be represented as a bitstream. After the secret date is embedded in the cover object, the cover object is referred to as a stego object, and the stego object sends to the receiver by selecting the

appropriate channel, where the decoder system is used with the same stego method to obtain the original information that the sender wishes to transfer.

There are various types of steganography:

Text Files: Text stego is the process of embedding secret data within a text. Text steganography necessitates a small amount of memory because this form of file can only store text files. It allows for the quick transfer or communication of files from sender to receiver.

Image Files: It is the process through which we embed information within the pixels of an image. As a result, the attackers will not notice any change in the cover image. The LSB method is a popular image steganography algorithm.

Audio Files: It is the process of concealing information within an audio file. There are numerous methods for concealing hidden information in audio recordings, such as Phase Coding and LSB.

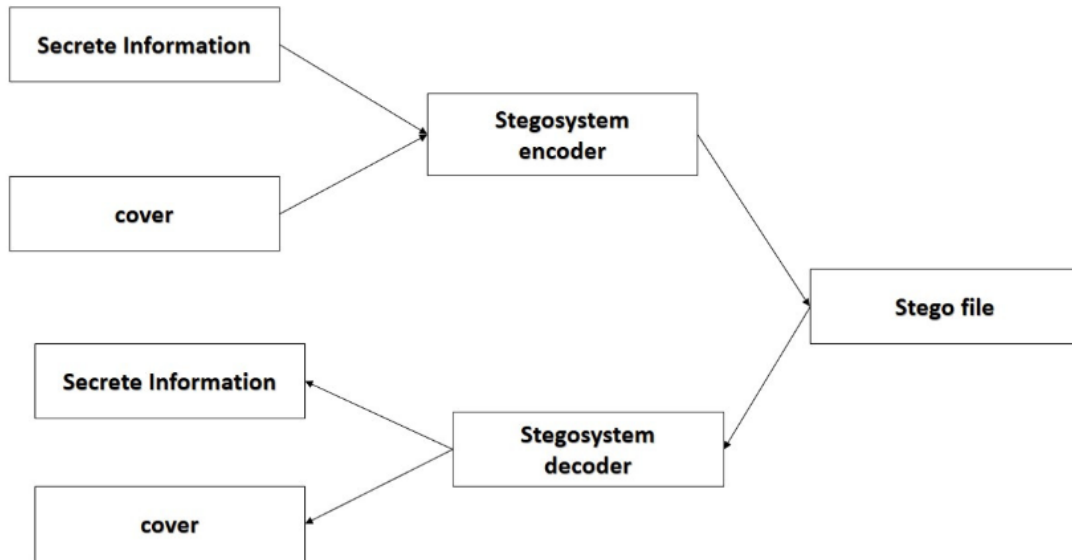


Figure 2: Steganography System

Encryption and Decryption:

We employ the MD5 technique throughout the encryption step. In MD5 algorithms, the input message is processed into 512-bit blocks, which are then separated into 32-bit sub-blocks of 16 pieces. The MD5 algorithm produces a hash value of four 32-bit blocks. While RGB Shuffling is used for picture encryption. The author created this method. The idea behind RGB Shuffling encryption is to shuffle all of the RGB elements in order to distort the image. The RGB Shuffling technique will shuffle the RGB values of each pixel in the image based on the password entered by the user. The first stage in RGB shuffling is to add an RGB element with an ASCII password, then invert and shuffle it. Figure 3 depicts the RGB shuffle process.

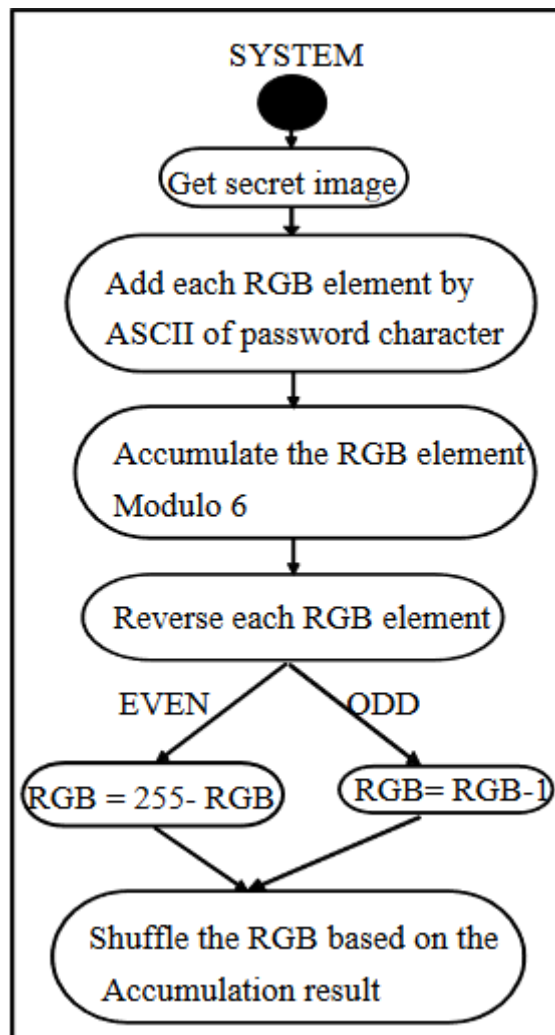


Figure 3: RGB Shuffling Process

B. Steganography Phase:

In this study, the Least Significant Bit (LSB) approach is developed to hide information. This approach will modify the bit in the rightmost location. Because the value of that bit is low, the final bit value that has been updated has little effect on the file. The LSB algorithm works by replacing non-important bits of data in the carrier with bits from sensitive or secret data. There is a most significant bit (MSB) and a least significant bit (LSB) in the arrangement of bits in a byte (1byte=8bits) (Least Significant Bit or LSB). The advantage of LSB is that the image will not change. The LSB approach processes data that has already been encrypted and converts it to binary form. If the carrier is an image, the binary of text can be stored using only one LSB utilising the LSB technique.

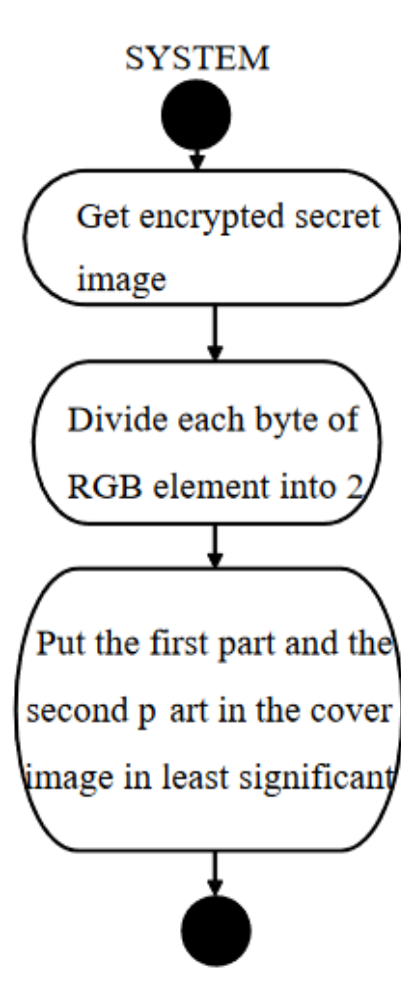


Figure 4: Least Significant Bit Process

Figure 4 depicts an LSB technique procedure for changing and storing the bit each RGB element per pixel of the encrypted secret image in the cover image.

If the carrier is audio, the first process is to initialise recognising an audio signal by generating a memory stream and binary writer, then converting it to binary. Because the data of the wave audio cannot be updated using the LSB approach if it is still in hex, the data of the wave audio needs to be transformed to binary. Then, take the information from an audio's left and right streams. So the hex of both streams will be transformed to string, and the data will be translated to char (example: from 13 14 15 16 into 1 3 1 4 1 5 1 6). The stream is then converted into binary. The message that will be embedded will be changed to char before being transformed to binary. The LSB technique is used in the following step. The wave audio signal's original left stream will be replicated and modified. Then it will count the size of the available left stream and compare it to the message size that will be buried. If it met the criterion, the LSB procedure will begin by replacing the message with the last digit of the left stream. If the left stream size is insufficient, an error notice will be displayed. Following that, the data from the changed left stream will be translated back to string and used to replace the original left stream.

Objectives:

- The goal of steganography is to conceal hidden messages in digital material.
- The major goal of cryptography is to give an additional level of protection, particularly at the message and password levels.
- To improve data security, RGB shuffling and LSB steganography are used.

Review Of Literature:

Soni, A., Jain, J., and Roshan, R. developed the fractional Fourier transform in 2013. (FrFT), Investigated as a generalisation of the classical Fourier transform, which was introduced in mathematics literature many years ago. The discrete version of the fractional Fourier transform, DFrFT, was created as an improved calculation of the fractional Fourier transform. This study shows how the discrete Fourier transform (DFrFT) outperforms other transforms for steganography in image processing. The PSNR in both domains (time and frequency) is the same, however DFrFT has the advantage of an additional stego key. This transform's order parameter. [8]

Akhtar, N.; Johri, P.; and Khan, S. implemented a version of the standard LSB (Least Significant Bit) method in 2013. The bit-inversion approach was used to increase the stego-image quality. The LSB technique improves the PSNR of the stego image. Image can be accurately obtained by saving the bit patterns for which the LSBs are inverted. To improve the stability of steganography, the RC4 technique was used to achieve randomization in hiding message image bits into cover picture pixels rather than storing them sequentially. This method randomly distributes the message bits in the cover image, making it more difficult for unauthorised

users to recover the original message. In terms of security and image quality, the offered solution outperforms the Least Significant Bit strategy. [9]

In 2013, Prabakaran, G.; Bhavani, R.; and Rajeswari P.S. investigated on Medical records as particularly sensitive patient information and suggested a multi secure and robustness of medical picture based steganography technique. This technology provides an effective storage security mechanism for digital medical images. The authors suggested a suitable steganography approach based on the Integer Wavelet Transform for protecting an MRI medical image into a single container image. The patient's medical diagnosis image was used as the secret image, and Arnold transform was used to create a scrambled secret image. The scrambled secret picture was inserted in the dummy container image in this case, and Inverse IWT was used to obtain a dummy secret image. When compared to the previous techniques, the quality parameters are enhanced with acceptable PSNR. [10]

Thenmozhi, S., and Chandrasekaran, M., presented a unique approach in 2012 that embeds data in integer wavelet transform coefficients by utilising a cropping function in an 8x8 block on the cover image. After embedding the message, the best pixel change procedure was used. The frequency domain was used by the authors to improve the resilience of our steganography technology. The integer wavelet transform avoids the wavelet filter's floating point precision issues. In terms of peak signal to noise ratio and capacity, the method outperforms the adaptive steganography methodology based on integer wavelet transform. [11]

Research Methodology :

This section will go through a potential approach for combining cryptography with steganography algorithms. In this proposed method, the message is encrypted using the Message Digest 5 (MD5) Algorithm, and the image is encrypted using RGB Shuffling. We then employ Least Significant Bit (LSB) techniques to embed the encrypted information in an image, video, or audio. The LSB technique conceals information or a file in the rightmost bit. This approach makes few changes to the carrier file, and the quality is nearly identical to the original. The difficulty with this strategy is that the message that can be buried is limited due to the bit capacity of the carrier file.

Books, educational and development magazines, government papers, and print and online reference materials were just a few of the secondary sources we examined to learn about the components, applications, and impacts of Cryptography and Steganography.

Result And Discussion:

The performance of the suggested system in this research is evaluated using the Peak Signal Noise Ratio (PSNR). Peak Signal Noise Ratio (PSNR) is used to compare the stego image and the cover image, as well as to measure the quality of the stego image; the greater the PSNR, the better the quality of the reconstructed image. Several conditions of secret image and password will be hidden by image application. The major focus of the test is the ratio of cover picture to secret image, as well as password strength, which can be measured by its length, difficulty, and change. Here are the conditions for testing the system's performance. [12]

Table 1: Processing Time

No.	Secret Image Resolution	Password Length	Time (second)
1	111x74	4	0.489
2	111x74	8	0.547
3	111x74	12	0.6
4	222x148	4	0.707
5	222x148	8	0.889
6	222x148	12	1.09
7	310x206	4	0.945
8	310x206	8	1.311
9	310x206	12	1.77

Table 1 displays the processing time required to hide the secret image in various sizes. The length of the password and the size of the secret image determine the processing time. The longer the password and the larger the size of the secret image, the longer the processing time.

The suggested approach was successfully implemented to regularly used colour images such as Lena, Baboon, and Boat colour test images in this research; the algorithm uses only one colour plane.

Table 2: Test result for 512X512X24 Colour images

Comparison of LSB and Our Algorithm	Lena		Baboon	
	LSB	Our Algorithm	LSB	Our Algorithm
PSNR(dB)	36.3	41	35.1	37
Capacity (bits)	788	812	570	598
Robustness	.8	.7	1.6	1.4

For authentication purposes, the embedding capacity can range from 512 to 1024 bits, and it can be changed by adjusting the block size for other applications. As shown later, the PSNR achieved by employing the approach is significantly higher. It should be noted that the data embedding capacity and PSNR of the marked image compared to the original image can be modified based on the password (key) [13]

Table 3. The result of encrypted image and stego image


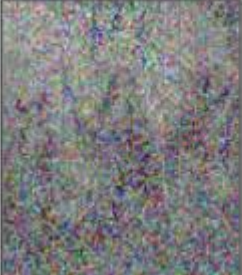
No.	Secret Image Resolution	PasswordSt length*	Encrypted Image	PSNR
1	50% cover image	Low		31.99
2	25% cover image	Low		38.00

Table 3 displays the results of the encrypted picture and the stego image. When the percentage of secret picture resolution is 12.5% and the password is Low, the PSNR is maximum; when the percentage of secret image resolution is 50% and the password is Medium, the PSNR is lowest. This PSNR value was generated using the passwords low="computing," medium="itiscomputing2012," and high="CoMpUtInG2012!". [14]

Conclusion:

Combining cryptography and steganography in terms of information encryption has proven to be extremely beneficial in terms of security analysis. Although it cannot guarantee complete data security, the additional RGB shuffling utilising the least significant bit method contributed to increasing the security of digital image information against any vulnerable assault by unauthorised access.

References:

- [1] M. K. I. Rahmani and N. P. Kamiya Arora, "A crypto-steganography: A survey," International Journal of Advanced Computer Science and Application, vol. 5, pp. 149–154, 2014.
- [2] J. V. Karthik and B. V. Reddy, "Authentication of secret information in image stenography," International Journal of Computer Science and Network Security (IJCSNS), vol. 14, no. 6, p. 58, 2014.
- [3] M. H. Rajyaguru, "Cryptography-combination of cryptography and steganography with rapidly changing keys," International Journal of Emerging Technology and Advanced Engineering, ISSN, pp. 2250–2459, 2012.

- [4] D. Seth, L. Ramanathan, and A. Pandey, "Security enhancement: Combining cryptography and steganography," *International Journal of Computer Applications (0975-8887)* Volume, 2010.
- [5] H. Abdulzahra, R. AHMAD, and N. M. NOOR, "Combining cryptography and steganography for data hiding in images," *ACACOS, Applied Computational Science*, pp. 978-960, 2014.
- [6] P. Kumar and V. K. Sharma, "Information security based on steganography & cryptography techniques: A review," *International Journal*, vol. 4, no. 10, 2014.
- [7] P. R. Ekatpure and R. N. Benkar, "A comparative study of steganography & cryptography," 2013
- [8] Soni, A.; Jain, J.; Roshan, R., "Image steganography using discrete fractional Fourier transform," *Intelligent Systems and Signal Processing (ISSP), 2013 International Conference on*, vol., no., pp.97,100, 1-2 March 2013.
- [9] 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.
- [10] Prabakaran, G.; Bhavani, R.; Rajeswari, P.S., "Multi secure and robustness for medical image based steganography scheme," *Circuits, Power and Computing Technologies (ICCPCT), 2013 International Conference on*, vol., no., pp.1188,1193, 20-21 March 2013.
- [11] Thenmozhi, S.; Chandrasekaran, M., "Novel approach for image stenography based on integer wavelet transform," *Computational Intelligence & Computing Research (ICCIC), 2012 IEEE International Conference on*, vol., no., pp.1,5, 18-20 Dec. 2012
- [12] Nikhil Patel; Shweta Meena "LSB based Image steganography using Dynamic key cryptography" 2016 International Conference on Emerging Trends in Communication Technologies (ETCT), Pages(s): 1- 5, India-2016
- [13] Khan, M.K.; Naseem, M.; Hussain, I.M.; Ajmal, A.; , "Distributed Least Significant Bit technique for data hiding in images," *Multitopic Conference (INMIC), 2011 IEEE 14th International*, vol., no., pp.149-154, 22-24 Dec. 2011
- [14] Navita Agarwal, Prachi Agarwal "An Efficient Shuffling Techniques on RGB Pixels for Image Encryption", *MIT International Journal of Computer Science & Information Technology*, 2013, Vol. 3, No. 2, pp. 77-81