http://www.jctjournals.com

ISSN(ONLINE):2278 - 3814

Volume-12, Issue-05, May 2023

JOURNAL OF COMPUTING TECHNOLOGIES (JCT)

International Journal

Page Number: 01-05

Data Hiding Through Image Steganography Using modified LSB Method:- A Review

Ramaiya Rawat [1] Prof. Prateek Singhal [2],
[1]M.Tech Student, [2]Assistant Professor
[1,2]SAM College of Engineering and Technology Bhopal

Abstract— Data is one of today's most important assets and must be handled appropriately when it comes to serious cyber security risks. In addition, every year information is stolen and changed from the internet during transmission. Therefore, there are two techniques known as cryptography and steganography to increase security during transmission. In cryptography, information is hidden in cipher text using a private key, but the existence of the information is visible to others even if it cannot be cracked. Steganography, on the other hand, stores confidential information in confidential files so that it cannot be discovered. This article presents a new method of hiding information using LSB image steganography, where only selected image pixels are used for confidential information. For this purpose, image pixel data is used to filter the entire image to identify candidate pixels, and user passwords are used to prevent LSB steganography. For better security, the AES method encrypts passwords before using steganography. In the experiment, MSE and PSNR values were measured to evaluate the quality of the synthesized steganographic images. The fact that steganographic images provide higher PSNR and smaller MSE values than other studies demonstrates the simplicity of the proposed method.

Keywords— Steganography, Encryption, Decryption, Advance encryption standard (AES) technique, least significant bit (LSB).

I. INTRODUCTION

There are several types of cover media available, where we can apply steganography. Steganography methods hide confidential information into cover media like image, audio, text, and video files (Islam et al., 2014). Figure 2 show some possible cover media where we can apply steganography easily. But the image is the most popular and fruitful medium for securing informative information. As we know, the human eye is not much sensitive to chrominance but in luminance. Therefore, Steganography exchange information by utilizing the weakness of the human eye in viewing image files. In this paper, we have used a 24-bit color image as a cover media. The image Steganography method can be classifiedinto the frequency domain and spatial domain (Kaur&Behal, 2014). In the frequency domain, the image istransformed into a new domain by manipulating thoriginal image and applying a mathematical operation (Chen & Lin, 2006). On the other hand, the spatial domain is relatively straightforward and modifies the original image directly (Lai & Tsai, 2010). The most common and simplest spatial domain steganography method is the least significant bit (LSB)method, where the LSB bit of the image pixels are substitute with the secret message bits (Ker, 2005).The LSB image steganography also can be divided into two categories, non-filtering, and filtering. In then on-filtering method, every image pixel is used for hiding secret information, but in the filtering method, not all the pixels are used for steganography. In the filtering method, image quality is considered and chooses the candidate pixels for hiding data (Sultanate al., 2018).

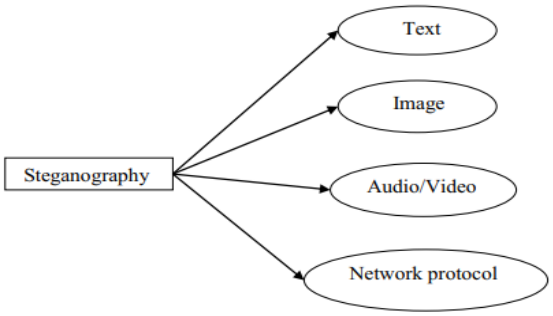

Figure .1 Types of cover media (Hussain & Hussain, 2013).

1.2 Watermarking

Watermarking could be a familiar image prototype that tone will be of darker or lighter, specifies the copy rights of specific documents. Sometimes watermarking has been utilized in administration documents, currency notes, and stamp papers for legal purpose, passports for safety features. Watermarking is tremendously obliging for characteristic the document of any licensed firm. No one else will turn out the copy of written document if copyrights are reserved. In times of yore, numerous styles of watermarks are used like Dandy roll method, Cylinder mould method, watermarks on postage stamps and stationary. In modern world, as the ways of communication has been changed or people prefer to communicate through digital media, so for secure communication, digital watermarking was introduced. The word digital was first introduced in 1992 by Andrew Trickle and Charles Osborne. Digital watermarking emerged as a solution for copyright protection, detection and maintenance of important data

II. LITERATURE SURVEY

There are lots of methods found that implement the steganography techniques on different cover media. Islam et al. (2014) have proposed a method by taking the combination of cryptography and image steganography. Here, the secret message is encrypted before embedding the image using the AES encryption algorithm. Additionally, they have used the concept of filtering, where not all the image pixels uses for hiding data. Mukhedkar et al. (2015), have proposed an approach that uses both message encryption and image hiding to hide personal information during communication for maintaining security. Image encryption has done using Blowfish Algorithm and hides message bits in LSB position. Singh et al. (2007) have proposed a method where the LSB method where secret messages hide in non-adjacent pixel locations of the selected image. As the pixels in edges may be much brighter and dimmer comparing their neighboring pixels, the intruder is unable to find the existence of message bits in the edges. Joshi and Yadav (2015) have proposed a new method that combines image steganography in the spatial domain on gray images with cryptography. In this method, the Vernam cipher algorithm is applied to encrypt the secret message. Then the encrypted data is embedded in LSB bit positions of the pixels. Also, the left shift operation and the XOR operation are Ibrahim et.al(2021) In this paper, A new set of algorithm is designed by the author for hiding data in images by means of Steganography. Here, in this algorithm binary codes and image pixels are used to hide data. In this method, for Maximizing the data storage capacity, It is firstly converted into Zip file and then to the binary codes. The application of this algorithm system is called Steganography Imaging System (SIS). Then the viability of the proposed algorithm is tested to observe, whether it is viable or not. Algorithm, when applied and tested with the naked eyes, it remains unchanged and cannot be noticed. When the stego images are tested using PSNR value. The PSNR value of those images observed higher and hence, this method of data hiding is very viable and liable for hiding our data from getting leaked [7].

Khaled Loukhaoukha et.al.(2020) A new design has been created using Rubik's cubeprinciple. In the proposed algorithm, the author has shuffled and mixed the data with itsidentical but different data using the Rubik's cube method.XOR operation is applied tointermix the image data in rows and columns by applying two secret keys. In this method ofdata encryption, the time taken for hiding data is comparatively less and the method is alsovery liable as well as viable as per the data security, data encryption and its capability todefend its data from the various attacks of data hacking. The experiment shows tremendousresults and is used in the real time application for communication applications [10].

performed. Li et al. (2008) have investigated the calibration technique that uses in the LSB steganographic method based on the pixel value. Loukhaoukha et al. (2012) have developed an image encryption algorithm based on Rubik's cube principle. After the image is scrambled, the XOR operation is performed in rows and columns. Therefore, the relationship between the original and the encrypted image becomes confused. Majeed et al. (2009) proposed a steganography method on text media. A new steganographic technique is proposed by Ghosal (2011), where the number of 1's and the number of 0's of the Red component is computed first. Then the method computes the absolute difference between these two, and the result is divided by 2. Hence, the resultant number of bits is hidden in another color component (Green and blue). Kaur et al. (2016) have proposed an approach where the upper LSB bit is used to hide data. And for optimizing the data size used LZW compression method. Ren-Er et al. (2014) have proposed the LSB image steganography method, where they use DES encryption to the confidential data before embedding. Raniprima et al. (2016) proposed a steganography method employing recounts investigation results applied in a grayscale image and an RGB image as the cover image. For more realistic security secret image is encrypted using the Rubik's cube principle that moves the pixels' position in a digital image. Phadte and Dhanaraj (2017) have proposed a method by combining Steganography and Cryptography. This method uses the chaotic theory to encrypt this resulting stego image for hiding secret information. Broda et al. (2015) have proposed a method where an image color model is used to hide data as a text form. It causes no loss of information during the conversion between RGB and YCbCr. Charan et al. (2015) have proposed a method to hide confidential information into a color image using a 3,3,2 LSB replacement algorithm. Caesar cipher technique is employed first to the private data then embed the encrypted data into the image. Khalaf and Sulaiman (2011) have proposed a method that combines both the segmenting and the data hiding technique. Two RGB channels are used to occult the confidential data concerning the third channel. By taking the advantages of one channel as an index path, the other channels calculate the number of one within the

selected index path. Emad et al. (2018) have proposed a steganography algorithm that hides a bit stream of data into the LSB bits. The method uses the approximation coefficients of the integer wavelet transform (IWT) to the grayscale images. Deeba et al. (2020) proposed a digital watermarking method using ANN and LSB method to hide the secret information. For that they use LSB method to hide a digital image into another digital image and later

K.C. Akshayet al (2018) Cloud Computing has evolved into a major technology in recent days to serve its customers in many ways. The shared pool of resources with configuration requirement needed by the customer is provided in an elegant manner. Data sharing is one of the important activities in cloud environment which requires confidentiality, integrity, authentication and nonrepudiation principles to provide data security. Providing the security and maintaining integrity of the data while it is being transferred through public channels is a challenging task. This paper attempts to answer that challenge by securing the data through image steganography. It is a modified LSB image steganographic technique using a password to hide data in an image. An analysis is performed for the techniques used and the number of characters hidden in the image. Viral Parmar et al.(2023) The rapid surge in digitalization has also increased the necessity for data security. Either in terms of storage, such as databases protected by cryptographic techniques, or in terms of individuals attempting to practice security for assorted reasons. Steganography is the process of concealing useful information within an uninteresting entity, such as an image or video that does not elicit much attention. This study focuses on the deployment of a flutter-based mobile application that enables the secure transfer of steganography-hidden images between users. The employed algorithm is RGB-based and further safeguarded by a key. The paper examines the key generation process as well as the Flutter application in detail and uses cloud-based resources to address common issues such as scalability and accessibility.

Karan Padhiyaret. Al (2022) Currently, digital data security has appeared as the largest challenge before the society. This concern has become more serious due to the data movement through the unsecured wireless medium. The text format data are mostly targeted by different attackers because of its usage in various finance and other sectors. Different advanced approaches were proposed for securing text data but security concern still remains. In the proposed method a symmetric key cryptographic algorithm is developed for securing the text data. The encryption and decryption key is generated through a set of matrix operations. The Key is generated by the multiplication of random matrices followed by a determinant operation of the same transposed and conversed matrix. The performance of the proposed method is compared with a few existing algorithms using throughput expressed in kilobytes per second. The result analysis has shown that the proposed work with both variations performed well compared to all other discussed algorithms.

Numerous proposed cryptographic algorithms utilize the similar key, which contain the intricacy of the passphrase and the difficulty of time. The suggested approach is adaptive in cases when the size of block words and keys can vary. Advanced Encryption Standard (AES) is more secure than Data Encryption Standard (DES) and DES3 due to the employment of continuous algorithms and enhanced keys. There is an efficient method for resolving performance difficulties in this symmetrical encryption-based system proposal. The primary functions of genetic algorithms are traverse and alteration. functions for encryption/encoding and decryption/decoding. One or more parent chromosomes are combined to generate a child's chromosomes. Several effective AES algorithms have been added to this method. [1]

The authors of this paper propose an innovative strategy for the process of concealing data within images by making use of steganography. The approach to data processing that is being proposed makes use of binary data as well as picture pixels. A compressed version of the file is being utilized while we wait for the binary codes to be extracted from it. This is done to ensure that the image contains the maximum amount of data possible while still maintaining its quality. When the proposed algorithm is put into action, the Steganography Imaging System, also known as SIS, is produced.

Following that, we put the system through its paces in order to ascertain whether or not the proposed strategy is actually feasible. Multiple data sizes and the PSNR (Peak signal-tonoise ratio) are being saved inside of each and every one of the photographs that are being analyzed right now. In addition, the photographs are being examined right now. The PSNR value of the stego image is noticeably superior to that of the other images in this comparison. As a direct result of this, the recently developed method of steganography is particularly helpful for the concealment of data inside of images.[2]

This work will develop and implement a new method for concealing significant amounts of data (picture, audio, and text) inside of a color Image file image. The method will be developed and implemented in this work. This work's objective is to conceal a sizeable amount of previously uncovered data. Methods such as dynamic image filtering and dynamic segmentation, in addition to the substitution of bitson the suitable pixels, were used in this process. Utilizing a novel idea that is composed of primary cases and the sub cases that correspond to them for each byte that constitutes a pixel, these pixels are selected at random as opposed to in as equential manner. This is made possible by the application of a new concept. Statistical analysis enables not only the comprehension but also the visual representation of this concept.[3]

The proliferation of cloud computing over the course of the past few years has been one of the most significant shifts that has taken place in the field of information technology. The pay-as-you-go model is widely used in the corporate world, and service-oriented computing, which offers everything as an Internet service, utilizes this model. It is gaining popularity not only for individual use but also in a

wide range of different industries, such as education, banking, healthcare, and manufacturing. This is due to the fact that it offers infrastructure and services that are flexible, scalable, and dependable. When using cloud computing, the user's primary concern should be with the security of their data throughout the entire process, including storage, retrieval, and transfer. Steganography and cryptography are just two of the many security measures that are used to ensure that user data is kept secure while it is being transferred in the cloud. Other security measures include the use of steganography and other methods.

Applications that are run on computers and connected to networks are required for cloud computing. The function of information sharing is one that must always be present in a cloud environment. Information is stored in the cloud for all types and sizes of businesses, from sole proprietorships to multinational corporations, so that the owners can save money on their monthly service fees. It has become abundantly clear that cloud computing plays a significant role in the sharing of resources and networks, as well as in the sharing of applications and data storage. As a direct consequence of this, the overwhelming majority of clients have an interest in utilizing facilities and services that are hosted in the cloud.

III. PROBLEM FORMULATION

Several Scientist and researchers have proposed encryption/decryption and Steganography algorithm to provide high security with minimum time. In Research Paper [1], Authors developed an algorithm which is uses binary codes and image pixels are used to hide data. Inland it is used for Maximizing the data storage capacity. In research paper [2] author has shuffled and mixed the data with its identical but different data using the Rubik's cubemethod.XOR operation is applied to inter mix the image data in rows and columns by applying two secret keys. In Research paper [3] Authors propose an idea to produce confusion between the original and encrypted images in most possible manner. XOR operatoris applied to rows and columns of an image in such a way that using the same key. In Research paper[4] Author apply the concept in which they replaced the Least Significant Bits (LSB) of the cover image is with the Most Significant Bits (MSB) for hiding out the communication data without actual distortion or destruction of image data property. In research paper [6] Authors again tried to use mixture of Cryptography methods and Pseudorandom number generator. In research paper [7] Authors concept is to encrypt an image by scrambling of pixels and performing XOR operations and it is decrypted in the same way.

IV. PROPOSED STATEMENT

We suggest the procedure of securely transferring the data is dependent on the complexity of processing data of enormous pixel and duplicating them with an inappropriate lattice of 90 identical sizes to generate a large number of keys. A key is chosen at random from the set of keys created and inserted in for one more encryption/encoding and decryption/decoding methods. This process is therefore believed to be based on substitution, in which a randomly selected key used to generate ciphertext/secret message, which is then deciphered. The calculation manipulates plain/input text character by character then generates random results for each individual character in succession. The method continues till the whole data has been processed.

4.2 Steps of Encryption algorithm

1. Input a key of arbitrary length
2. Generate a pseudo – random no. (RN) by using following rules.

a) Add all the ASCII Value of characters of key.
b) Divide the result by 32 and the remainder comes out is Pseudo Random No (RN)

3. Convert the key into binary format & if it's lengthy after conversion is less than 128, thenperform padding operation using following rules

a) Perform XOR operation on each bit of a key moving left to right with its RN position bit
b) Result of step
3 (a) concatenate with the key
c) Repeat above steps 3 a & 3b until becomes greater or equal to 128 bit

4. Extract Most Significant 128 bits from key, Hence the final key become of 128 key.
5. Now generate 8 different keys k[0] to k[7] by using following rules.

a).K[0]=XOR all bits by its RN position bit in key
b).K[1]= Circular left rotate K[0] by RN position
c).K[2]=XOR all bits by its RN position bit in K[1].
d) K [3] =Circular left rotate K [2] by RN position.
e) K [4] = XOR all bits by its RN position bit in K[3].
f) K [5] =Circular left rotate K [4] by RN position.
g) K [6] = XOR all bits by its RN position bit in K[5].
f) K [7] =Circular left rotate K [6] by RN position.

6. Now, Divide the plain text in bit format into 128 bits chunks, if the last chunk does not
have 128 bits then pad it by 0'S
7. Now for each chunk do the following:

a) Divide the chunk into 4 equal parts (i.e of 32 bits)[pt1,Pt2,Pt3,Pt4].
b) Repeat the following for (i=0 to i=7)
(i) Pt1=Left rotate (Pt1) by RN
(ii) Pt2=XOR all bits of Pt2 by RN bit
(iii) Pt3= Left rotate (Pt3) by RN
(iv) Pt4= XOR all bits of Pt4 by RN bits
(v) Divide key K[i] into 4 equal parts [K1, K2, K3, K4] from M.S.B.
(vi)XOR (Pt1,K1),XOR (Pt2,K2),XOR(Pt3,K3), XOR(Pt4,K4).
(vii)Pt1=XOR all bits by Pt1 by RN.
(viii) Pt2=Left rotate (Pt2) by RN.
(ix) Pt3= XOR all bits by Pt3 by RN.
(x) Pt2=Left rotate (Pt4) by RN.

8. Result of Step 7 is cipher text of given Chunk.

4.3 Steps of Steganography algorithm

Proposed Steganography algorithm is Modification of Standard LSB Method.

Steps of Steganography Algorithm

1. Select a cover image having no. Of pixels equals to 8/3 bits in cipher text
2. Hide all the bits of the Cipher text behind R, G, and B Component using LSB method.
3. Now perform the analysis Using the mentioned Example:

Let consider the bits to be hide is 1011 & Pixels of cover image are 10011110,00010111, 11111110 & 01010111.After performing LSB method, Pixel will be 10011111, 000101110, 11111111, and01010111.

It is shown from above out of 4 pixels 3 has been changed so distortion % is 75%.Now divide all the pixels into 4 groups on the basis of 6th & 7th bits are 00 thenbelongs to group 00, similarity created group 01 group 10, group 11.Now if in each group changing % is more than 50% then insert all the L.S.B pixelsof that groupAlthough in above example all pixels are belong to group11 & changing % is morethan 50% therefore insert all L.S.B of pixels hence we have10011110,00010111,11111110,01010110 & marked the gropu as inserted group sothat it can be detected at reciver end . Now compare this pixels , the distortion % is25%.

Below flowchart represent the Encryption algorithm.

V. CONCLUSION AND DISCUSSION

With the projectile like growth of technologies in the field of computers and internet, security of data is an important concern in today's life. In this thesis, I have studied lots of cryptographic algorithms and proposed an improved algorithm and analyzed it with DISEWRCP [8]. Steganography has been known and practiced for centuries. Previously, people would use manual methods for data hiding in which data is placed inside some host file or an object. But after the arrival of digital steganography, the entire method of data hiding has been modified. Digital steganography has totally overtaken the old traditional methods in recent world of computers and internet. Also with the arrival of new methods, the attackers have invented newer techniques to break the code. This in turn gives rise to invention of more secure methods which are even more complex. This paper aims to develop an algorithm which provides more security to the confidential data by first encrypt it by applying a new secure encryption algorithm and then hiding it in some text or document files abundant on the internet.

Improvisations on this work would be possible in the future in a number of ways:

Firstly, this security system encrypts and embeds confidential message into which is essentially a text document. Now if this cipher message might be further encrypted and sent as a secret message, the attacker would not be able to retrieve the original message.

Secondly, this method could also be improved to compress the original secret message file and then encrypt more than one small compressed secret message files and embed them randomly.

REFERENCES

[1] M. Matsumoto, T. Nishimura, " Marsenne Twister: A 623-dimensionally equidistributed uniform pseudo-random number generator," in ACM Transactions on Modeling and Computer Simulation, 1998..

[2] A. Westfeld, A. Pfitzmann, "Attacks on steganographic systems," in Information Hiding, LNCS, vol.1768, 1999..

[3] Fridrich, M. Goljan and R. Dui, "Reliable Detection of LSB steganography in Color and Grayscale Images", in Proc. ACM Workshop on Multimedia and Security, Ottawa, CA, 5th Oct. 2001, pp. 27-30

[4] R Chandramouli , M Kharrazi and N Memon, "Image Steganography and Steganalysis: Concepts and Practices", in Proc. 2nd Int. Workshop on Digital Watermarking, Seoul, Korea, 20-22 Oct. 2003, pp.35-49..

[5] PiyushGoel "Data Hiding in Digital Images: A Steganographic paradigm" Indian Institute of Technology Kharagpur, May,2008

[6] M. Juneja, P.S. Sandhu, "Designing of robust image steganography technique based on LSB insertion and encryption," in International Conference on Advances in Recent Technologies in Communication and Computing, pp.302-305, 27-28 Oct. 2009.

[7] Ibrahim, Rosziati, and Teoh Suk Kuan. "Steganography algorithm to hide secret message inside an image." arXiv preprint arXiv: 1112.2809 (2011).

[8] Hung-Min Sun, Chi-Yao Weng, Chin-Feng Lee, Cheng-Hsng Yang, "Anti-forensics with steganographic data embedding in digital images," in IEEE Journal on Selected Areas in Communications, vol.29, no.7, pp.1392-1403, August 2011.

[9] G. Zhang and Q. Liu, "A novel image encryption method based on total shuffling scheme," Optics Communications,vol.284, no. 12, pp. 2775–2780, 2011.

[10] Loukhaoukha, Khaled, Jean-Yves Chouinard, and AbdellahBerdai. "A secure image encryption algorithm based on Rubik's cube principle." Journal of Electrical and Computer Engineering 2012 (2012).

[11] Kilaru, Seetaiah, et al. "effective and key sensitive security algorithm for an image processing using robust Rubik encryption and decryption process."University of Birmingham, ISSN (Print) 2 (2013): 2278-8948.

[12] Devi, KshetrimayumJenita. "A secure image steganography using LSB technique and pseudo random encoding technique", National Institute of Technology-Rourkela, 2013.

[13] Kaur, Navneet, and Sunny Behal "A Surveyonvarious types of Steganography and Analysis of Hiding Techniques", International Journal of Engineering Trends and Technology 11.8 (2014): 387-91.

[14] Thakre, Ketki, and NehalChitaliya "Dual Image Steganography for Communicating High Security

Information" ,International Journal of Soft Computing and Engineering (IJSCE) 4.3 (2014).
[15] Gulve, Avinash K., and Madhuri S. Joshi. "An image steganography algorithm with five pixel pair differencing and gray code conversion." International Journal of Image, Graphics and Signal Processing 6.3 (2014)
[16] Yang Ren-er, Zheng Zhiwei, Tao Shun, Ding Shilei, "Image steganography combined with DES encryption pre-processing," in Sixth International Conference on Measuring Technology and Mechatronics Automation (ICMTMA), pp.323-326, 10-11 Jan. 2014. [17]Sirisha, M., and S. V. V. S. Lakshmi. "Pixel Transformation based on Rubik's Cube Principle.", International Journal of Science and Technology 8.S7 (2015): 228-235.
[17] Srinivasan, B., S. Arunkumar, and K. Rajesh. "A novel approach for color image, steganography using nubasi and randomized, secret sharing algorithm." Indian Journal of Science & Technology 8.S7 (2015): 228-235.
[18] G.S. Charan, Nithin Kumar, B. Karthikeyan, V. Vaithiyanathan, K. Divya Lakshmi, "A novel LSB based image steganography with multi-level encryption," in International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), pp.1-5, 19-20 March 2015.
[19] Ashwini B. Akkawar, komal B. Bijwe "Hybrid approach for Embedding Text or Image in Cover Images", International journal of innovative research and science, engineering and technology, vol. 5, Issue 5, May 2016.
[20] S. Raniprima, B. Hidayat and N. Andini, "Digital image steganography with encryption based on rubik's cube principle," 2016 International Conference on Control, Electronics, Renewable Energy and Communications (ICCEREC), Bandung, 2016, pp. 198-201.
[21] Viral Parmaret all "Efficient Data Hiding Method in Image Based on
[22] Modified LSB" 2022 IEEE 2nd International Symposium on Sustainable Energy, Signal Processing and Cyber Security (iSSSC) | 978-1-6654-9056-6/22/$31.00 ©2022 IEEE | DOI: 10.1109/iSSSC56467.2022.10051264.
[23] M. R. Islam et all "A modified LSB image steganography method using filtering algorithm and stream of password," 2020 Information Security Journal: A Global Perspective

