International Journal of Innovative Trends In Engineering (IJITE) e-ISSN: 2395-2946
Issue 125, Volume 75, Number 05, May 2023

Research Results

Data Hiding Through Image Steganography using Modified LSB Method

Ramaiya Rawat[1], Prof. Prateek Singhal [2]

[1]*M.Tech Stuent, SAM College of Engineering and Technology Bhopal*
[2] *Assistant Professor, SAM College of Engineering and Technology Bhopal*

ABSTRACT

Information security, Steganography is a vast research area of computer science that develops numerous intelligent systems for secret communication. Image steganography is the most prevailing dimension due to its frequency on the internet in this field. The objective of this research work is to provide high level of security, maximum embedding capacity, efficiency and reliability for secret communication using steganographic techniques. Same work has been done before through cryptographic techniques but with time steganography emerges as a more secure and power full technique, where as cryptography lacks in several ways. Now in modern era, steganography has come up with all the deficiencies of cryptography. In this proposed work we present an image based steganography technique that integrates Least Significant Bits (LSB) techniques and pseudo random coding technique to boost the protection of the communication. In the LSB approach, the fundamental thought is to supplant the Least Significant Bits (LSB) of the cover picture with the Most Significant Bits (MSB) of the messages to be covered up without annihilating the property of the cover picture significantly. The LSB-based procedure is the most difficult one as it is difficult to differentiate between the cover-image stego-image if few LSB bits of the cover object are supplanted. In Pseudo-Random procedure, an irregular key is utilized as seed for the Pseudo-Random Number Generator is required in the inserting procedure. This combination provides better security for hiding confidential message and formerly reduces time complexity. Finally, effectiveness of the proposed algorithm is tested using encryption time, Avalanche impact, PSNR value.

KEYWORDS

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

1. INTRODUCTION

1.2 Introduction

Information security in today's world is a sense of declaration against threats, means that important information must be secured and there risks of attacks as well as controls must be balanced. Information security actually starts with the emergence of first main frame computer. But with the introduction of information security many viruses and code breakers were also developed that breaks the security channel and damage the important information. To overcome these issues, firstly physical controls were needed to limit the access of unauthorized persons to susceptible areas. Later on department of defence's Advance research project agency (ARPA) in 1960's started to examine the viability of disused network communications. In between 1970 and 1980 ARPANET become popular but with the popularity some security issues were also raised, like there are no procedures for identification and authorization of the system while dial up connection. In 1990's computer networks become more common because of communication which results in the emergence of internet. Internet bought millions of computer into communication with each other, where many pc were unsecured. Security is a quality of being secure; it can be physical, personal, communication or network security. So security is the need of our modern world. Information security is also called as info sec; information security is a combination of art and science, no hard and fast rules nor universally accepted solutions. It is a very vast field, which covers a large area in digital communication because security is the necessity of every dept in today's era.

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.

2. LITERATURE SURVEY

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.

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 cube principle. In the proposed algorithm, the author has shuffled and mixed the data with its identical but different data using the Rubik's cube method.XOR operation is applied to intermix the image data in rows and columns by applying two secret keys. In this method of data encryption, the time taken for hiding data is comparatively less and the method is also very liable as well as viable as per the data security, data encryption and its capability to defend its data from the various attacks of data hacking. The experiment shows tremendous results and is used in the real time application for communication applications [10].

Karan Padhiyar et. 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 bits on 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 a sequential 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.

3. 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. In and 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 cube method.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 operator is 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.

4. 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, then perform 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, and 01010111.

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 then belongs 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 pixels of that group Although in above example all pixels are belong to group11 & changing % is more than 50% therefore insert all L.S.B of pixels hence we have 10011110,00010111,11111110,01010110 & marked the gropu as inserted group so that it can be detected at reciver end . Now compare this pixels , the distortion % is 25%.

Below flowchart represent the Encryption algorithm.

5. RESULT ANALYSIS

This section presents the results of evaluating the efficiency of the proposed technique that is based on selected parameters. The main aim of this research is to secure text information by proposed technique. To achieve this block cipher technique and steganography technique are combined to increase the efficiency of the proposed system. The presented experimental results show the superiority of the proposed encryption and steganography algorithm over existing algorithms in terms of processing avalanche effect and timing. In the experiments, the system encrypts/decrypt image. There are three parameters which are calculated by the proposed system one is timing and second is avalanche effect and third is security which is shown in table 5.2, 5.3 and table 5.4. The proposed system has been run hundred times approximately for the four selected text displayed below. In each time, same image are respectively encrypted by existing algorithm and proposed algorithm. Size of the selected key was same for each time for the proposed algorithm. Finally, the output are the encrypted text (Cipher Text) (produced by existing algorithm and proposed algorithm) and there timing and avalanche effect. The timing and avalanche effect are noted in numeric form and are displayed below.

Desktop machine has been used to calculate experimental results which have the following configuration:

Table 5.1: Required Configuration

Processor	Memory(Primary)	Platform	Software Application
Intel Pentium Dual Core E6700 3.20 GHz	2 GB of RAM	Window-XP SP2	Visual Studio 2005

Sample files:

S.No.	File Size
1.	1 KB
2.	5 KB
3.	10 KB

5.1.1 Tabular Analysis

All the results are presented here in the form of tables.

5.1.1.1 Timing

The core advantage of any cryptographic algorithm is the speed of encoding and decoding of data. Proposed algorithm is especially designed for this feature. Table 5.2 is showing encryption time of the proposed encryption algorithm on various files size with same key value with base paper Digital Image Steganography with Encryption based Rubik's Cube Principle [8]

File Size in KB	Encryption Algorithm (Execution Time in Second)	
	DISEWRCP [8]	Proposed Algorithm
1 KB	0.234	0.140
5 KB	0.392	0.287
10 KB	0.510	0.426

It is clear from the table 5.2 that the execution time of proposed algorithm is very low as compare to DISEWRCP [8] algorithm. Example 1KB file require 0.234second to encrypt where as proposed algorithm require 0.140 seconds.

5.1.1.2 Security (Avalanche Effect)

Encryption security considers the strength of encryption algorithm. Avalanche Effect is used to calculate the strength of any cryptographic algorithm. According to the avalanche effect, on changing the single bit in key 50% bits of cipher text must change. The algorithm close to avalanche effect is more secure against cryptanalysis. Table 5.3 shows the avalanche effectproposed algorithm.

Table 5.3: Avalanche Effect of DISEWRCP & Proposed algorithm

File Size in KB	Avalanche Effect	
	DISEWRCP [8]	Proposed Algorithm
Single bit change in key	48.63 %	49.69%

On processing different 15 images, it is found that average avalanche effect comes out between 49 to 50%. This shows the strength of proposed encryption algorithm on comparing it with DISEWRCP [8] and Proposed algorithm; it is found that avalanche effect of proposed algorithm is better than the DISEWRCP [8] algorithm.

5.1.1.3 Security (Peak to Signal ratio)

Peak signal to noise ratio is a term used to find ratio between the highest possible value of a input signal and the rate of distorting noise that affects the quality of its representation. PSNR is usually expressed in terms of decibel.

Table 6.4: Comparison of PSNR value between proposed algorithm & DISEWRCP [8] algorithm (2016)

File Size in KB	PSNR Value	
	DISEWRCP [21]	Proposed Algorithm
Single bit change in key	52.644	55.63

5.1.2 Graphical Analysis

In this results are shown in the form of graphs.

5.1.2.1 Timing

A graphical representation for the table 5.2 is shown in figure 5.1, with blue line for DISEWRCP [21] encryption/decryption algorithm and red line for proposed encryption/decryption algorithm. According to the graph, there is a leaning that for encryption/decryption algorithm execution time increases with file size. But required time for the execution of proposed encryption/decryption algorithm is much smaller than execution time of compared algorithms.

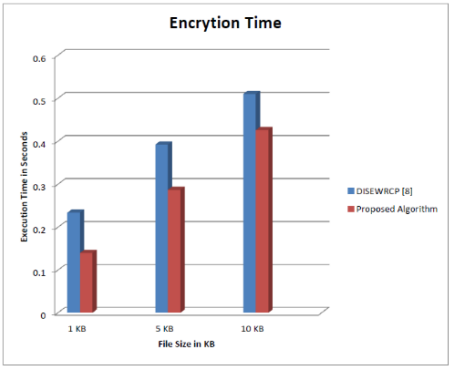

Figure 5.1: Execution time of the DISEWRCP [21] and proposed encryption algorithms in seconds

5.1.2.2 Avalanche Effect

Graphical representation of avalanche effect is shown in table 5.4 and figure 5.2. It is clearly shows that avalanche effect of proposed algorithm is more than the compared algorithm. Hence internal structure of proposed algorithm is much secure and robust.

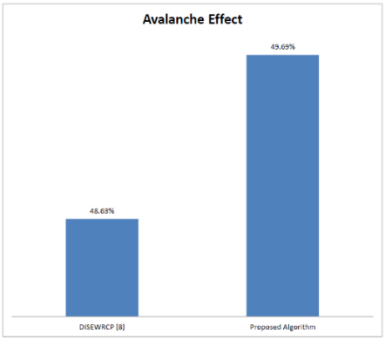

Figure 5.2: Avalanche Effect of DISEWRCP [21] algorithm and Proposed Algorithm

Here, on analyzing the avalanche effect, it is clear from table 5.3 and figure 5.2 that robustness of the DISEWRCP [8] algorithm is low as its avalanche effect is very low and our proposed algorithm is very robust.

5.1.2.3 Peak Signal to Noise Ratio

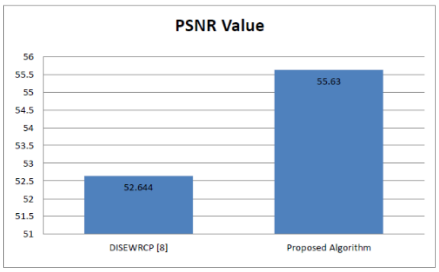

Figure 5.3 Comparison between DISEWRCP [21] and proposed algorithm.

Again, it is clearly seen from Table 6.5 and Figure 6.4 is that in Proposed algorithm PSNR for 1 KB file is higher as compared to DISEWRCP algorithm[21].

5.2 Cryptanalysis

Decryption of cipher text without prior knowledge of the key is known as Cryptanalysis [11]. In the proposed algorithm everything is done in the binary format as well as character format. Primary key is actually arbitrary bits long (in between 1-128). Although, keys and data are conveyed in character mode but keys and operations are actually applied in binary format. In this manner, it turns out to be exceptionally urgent for a Cryptanalyst to comprehend the basic organization and connection between tasks, capacities and information. Here a most dire outcome imaginable is exhibited to break the figure content, regardless of whether encryption process is known.

Conceivable number of endeavors to break the proposed Key: First of all, the interloper does not know with respect to the key, as it is discharged from information.

The effort needed to get to this arbitrary bit long key will be: $2^{128} + 2^{127} + \ldots + 2^{1} = 2^{1}(2^{128-1})$ (therefore time complexity to break the key will be $O(2^{129})$).

There are total 8 different keys that are used which are dependent on random number having range 0-32, so each key can apply 8 *32 different manners. So the time complexity will increases to $O(2^{129+3+5}) = O(2^{137})$

6.3 Summary

As this work discussed, there is a requirement to develop an algorithm which not only secure but also be time and space efficient so that it can be used for real time transmission or in ad hoc network. This work fulfill that requirement and introduces an algorithm which is time and space efficient as well as enough secure against cryptanalysis attack. Also shows that the proposed work is time and space efficient and secure by analyzing the performance with other existing algorithms.

Table 5.5: Summarized analysis between DISEWRCP [8] and Proposed algorithm

S.No	Algorithm Name	Features	Problems
1.	DISEWRCP [8]	• Secure Internal Structures	• Not space efficient • More overhead • Less robust
2.	Proposed Algorithm	• Secure • Strong Internal Structure • Strong Key Generation • Time Efficient • Less Battery Consumption • More Robust • Use for Real Time Transmission	• No Problems have been reported yet

6. CONCLUSION AND FUTURE WORK

6.1 Conclusion

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.

6.3 Future Enhancement

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

Firstly, this security system encrypts and embeds a 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] J. 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] Piyush Goel "Data Hiding in Digital Images: A Steganographic paradigm" Indian Institute ofTechnology Kharagpur,May, 2008 http://cse.iitkgp. ac.in/~abhij/facad/03UG/Report/03CS3003_Piyush_Goel.pdf

[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-Hsing 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 Abdellah Berdai. "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, Kshetrimayum Jenita. "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 Nehal Chitaliya "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.

[18] 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.

[19] 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.

[20] 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.

[21]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.

[22] Viral Parmar et all "Efficient Data Hiding Method in Image Based on 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