IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 11, Issue 5, May 2022

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.118

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 5, May 2022||

| DOI:10.15680/IJIRSET.2022.1105227 |

Information Hiding Within Image Using Image Steganography Technique

Harshada Sawant[1], Mohammed Zeeshan Shaikh[2], Praneet Waghmare[3], A.A.Shahbad[4].

U.G. Student, Department of Computer Engineering, Trinity Academy of Engineering, Kondhwa, Pune, India[123]

Associate Professor, Department of Computer Engineering, Trinity Academy of Engineering, Kondhwa, Pune, India[4].

ABSTRACT: Steganography deals with the craft of obscuring personal knowledge within a selection media. In confidential electronic communication security may be a very important issue. During this paper, we have tendancy to use a two-layer security. At first, encoding is achieved by the tactic of RSA algorithmic rule of uneven cryptography, and later the ciphered knowledge is hidden into host image by an innovative embedding technique. To cover our ciphered knowledge into host image, we have a tendancy to the present LSB technique and use a mapping operate that ensures a secure and confidential image steganography leading to resulting in a stego image. Here cryptography is mixed with steganography and provides 2 level security within the confidential knowledge transmission over the net.

KEYWORDS:LSB, Embedding, Decryption, Encryption, Steganography, Spatial Domain.

I. INTRODUCTION

Steganography may be a technique during which data may behide in to different media, the media like image, audio, video files etc. the knowledge may be straightforward text message, any image files or is also an audio clip. Steganography is that the art of concealing the fact that communication is happening, by concealing information in different information. Many various carrier file formats will be used, however digital pictures area unit the foremost widespread due to their frequency on the web. For activity secret data in images, there exist an oversized style of steganography techniques some area unit of a lot of complicated than others and every one of them have individual robust and weak points. Totally different applications have different needs of the steganography technique used.

For concealing media the antecedently LSB(Least significant Bit) methodology, is extremely straightforward technique. The formula that is employed to cover the knowledge in to the media is thought as stegoalgorithm, wherever as the un authorized way to extract the information is called stegoanalysis. Medium integrity is an important issue in stegnography, whenever because the United Nations approved thanks to extract the information is named steganalysis. Medium integrity is a vital issue in steganography, whenever one media is hidden into other the originality of canopy media shouldn't have an effect on. Steganography is outlined because the science and art of concealing a secret message in numerous files varieties, for instance: digital images files, digital audio files, digital video files, and text files. Steganography word is consists of two Greek words, namely: Stegano and Graphy. The word Stegano means that a coated, whereas Graphy means that Writing. Therefore, steganography means that a Covered Writing.

The transmission of encrypted message could simply arouse attackers suspicion, and also the encrypted message could therefore be intercepted, attacked or decrypted violently. So as to beat the shortcomings of cryptologic techniques, steganography techniques are developed. Steganography is that the art and science of communicating in such the way that it conceal the existence of the communication. Thus, steganography hides the existence of knowledge so that nobody will sight its presence. In steganography the method of concealment information content within any transmission content like image , audio, video referred as a Embedding. For increasing confidentiality of human action knowledge each techniques could combined.

II. PROBLEM STATEMENT

TheSteganography conceal the terribly existence of a message so that if winning it usually attracts no suspicion in the least. Victimization steganography, data can be conceal in carriers like images, audio files, text files, videos and knowledge transmissions. We planned a brand new framework of an image steganography system to cover a digital text of a secret message.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 5, May 2022||

| DOI:10.15680/IJIRSET.2022.1105227 |

III. RELATED WORK

M.A.Hameed [1], proposed system studies on image steganography.Steganography is the method whereby data is hidden inside other data so only the recipient can reveal hidden information after recovering the item. An Adaptive Image Steganography Method Based on Histogram of Oriented Gradient and PVD-LSB Techniques. This algorithm is effective on the security factor of secret image since the embedded checksum will validate for any unauthorized user or intruders attempt to corrupt the picture in any aspect.

In [2] system, large-scale JPEG image steganalysis using hybrid deep learning framework. We propose a generic hybrid deep-learning framework for JPEG steganalysis incorporating the domain knowledge behind rich steganalytic models. Digital image steganography using modified LSB & AES crptography. The cryptographic algorithms are AES, RSA, DES, 3DES and blowfish algorithms, & the steganography technique in LSB.

In [3] systems results improving selection-channel-aware steganalysis features. The best detectors of content-adaptive steganography are built as classifiers trained on examples of cover and stego images represented with rich media models (features) formed by histograms f quantized noise residuals. LSB based Steganography using Bit masking method on RGB planes. Steganography hides the existence of information that needs to be exchanged or transferred through some public media like the internet.

In [4] proposed system, a new LSB-S image steganography method blend with cryptography for secret communication. A method of image coding is proposed that hides the information along a selected pixel and on the next value of the selected pixel, that is, pixel + 1. International journal of advanced research in computer science & software engineering. MATLAB provides more security for secret communication.

In [5] system the LSB insertion is a common, simple approach to embedding information in a cover image. An analysis of LSB & DCT based steganography. LSB based steganography embed text message in LSB of cover image. DCT based steganography embed text message in LSB of DC coefficient.

In [6] system proposed spatial domain steganography approach to embed secret information on the conditional basis utilizing 1bit of Most Significant Bit (MSB). In addition, the cover image is decomposed to 8x8 matrix size block, whereas the first block related to cover image is embedded with the 8 bits regarding lower band and upper bound values needed to retrieve the payload at destination. The median values' mean and the difference between consecutive pixels regarding every one of the 8*8 blocks of the cover image is specified for embedding the payload in 3-bits of LSB and 1-bit of MSB on the basis of prefixed conditions. Furthermore, it has been indicated that the security and capacity is enhanced in comparison to current approaches with adequate PSNR.

IV. PROPOSED SYSTEM

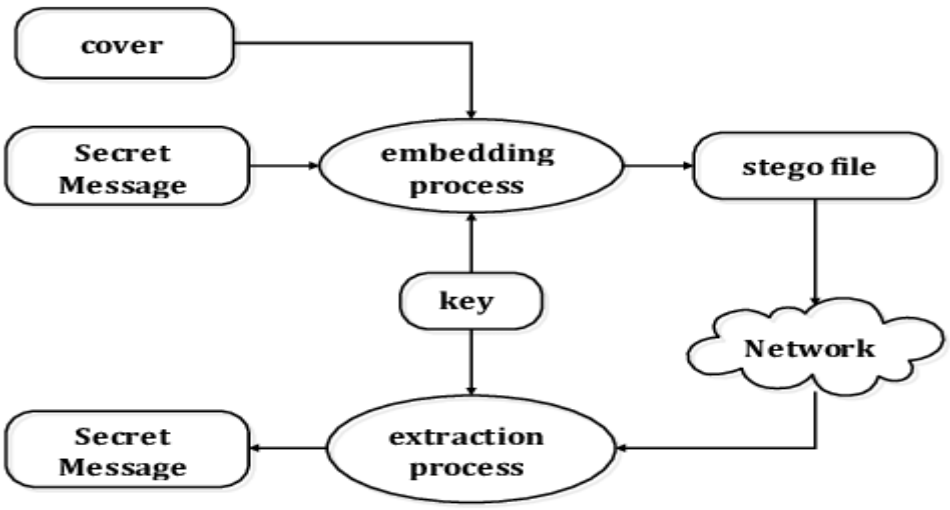


Fig. Block diagram image steganography

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 5, May 2022||

| DOI:10.15680/IJIRSET.2022.1105227 |

V. METHODOLOGY

Least Significant Bit :

This is a simple and uncomplicated technique for hiding the info or secret message in a picture. It introduce the data at right-most bit i.e. least important bit (LSB) position. Mainly there square measure 2 reasonably pictures 8-bit and 24-bit (RGB). The former support 256 colours and later support 256*256*256= concerning sixteen million completely different colours and ordinarily LSB deals with RGB image.

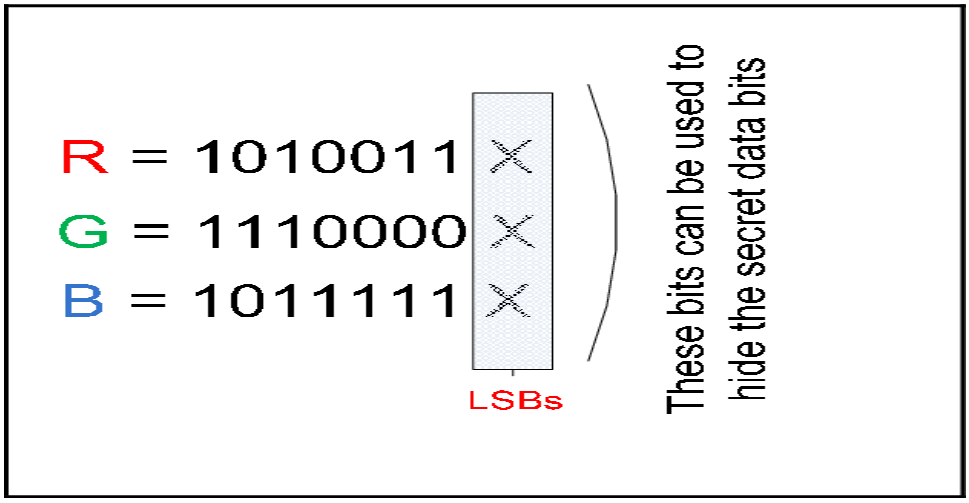


Fig. Least significant bit

E.g.Let′ s suppose that to hide the message bits 10101011 in an image whose pixel are 10110001 11001101 11101110 10001100 10001001 11111111 11001100 101010101. Then the output we will have 10110001 11001100 11101111 10001100 10001001 11111110 11001101 101010101. Here, the each single message bit are replacing rightmost value of the image pixel.

This methodology is thought as ordered LSB and it's swish and easy to implement. but it doesn't provides good payload capability thanks to just one bits of message bit per pixel. to boot, it will be detected simply by trespasser.
There are two different methods for imagesteganography:

1. Spatialmethods
2. Transformmethods

But we are using Spatial Methods

1.Spatial Domain Method :

In spatial methodology, the foremost common methodology used is LSB substitution methodology. Least significant bit (LSB) methodology could be a common, straightforward approach to embedding info in a very cowl file. In steganography, LSB substitution methodology is employed. I.e. since each image has 3 parts (RGB). This pel info is hold on in encoded format in one computer memory unit. the primary bits containing this info for each pel are often changed to store the hidden text. For this, the preliminary condition is that the text to be hold on has got to be smaller or of equal size to the image accustomed hide the text. LSB based mostly methodology could be a spatial domain methodology. however this is often liable to cropping and noise. during this methodology, the savings bank (most important bits) of the message image to be hidden ar hold on within the LSB (least important bits) of the image used because the cowl image. it's identified that the pixels in a picture ar hold on within the kind of bits. in a very grayscale

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 5, May 2022||

| DOI:10.15680/IJIRSET.2022.1105227 |

image, the intensity of every pel is hold on in eight bits (1byte). equally for a color (RGB-red, green, blue) image, every pel needs twenty four bits (8bits for every layer).

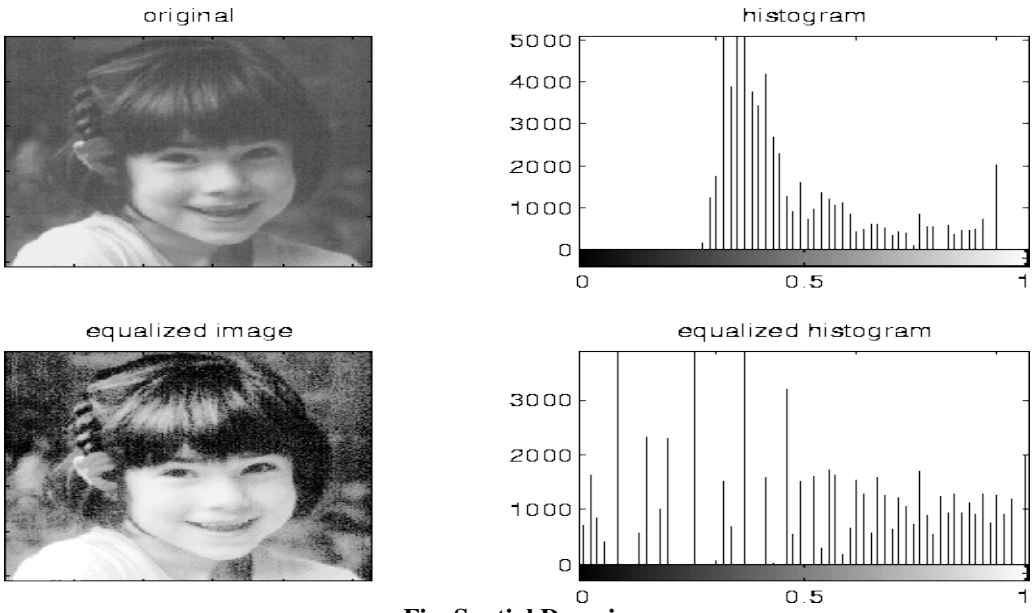


Fig. Spatial Domain

RGB-red, green, blue) image, every pel needs twenty four bits (8bits for every layer). The Human sensory system (HVS) cannot find changes within the color or intensity of a pixe. when the LSB bit is changed. this is often psycho-visual redundancy since this may be used as a plus to store info within these bits and nevertheless notice no major distinction in the image. Algorithm of LSB methodology of steganography.There can be 2 completely different phases of LSB methodology, embedding part and extracting part.
Algorithms of each of the phases square measure given below ;

1) Embedding phase Procedure:

Step 1: Extract all the pixels from the given image and store them in some array named (imagearray).

Step 2: Extract all the characters from the given text file(message file) and store it within the array known as (messagearray).

Step 3: Retrieve the characters from the Stego key and store them in an exceedingly array known as Keyarray. A stego- secret's accustomed management the concealing method thus on limit detection and/or recovery of the embedded knowledge.

Step 4: Take 1st pel and characters from Key- array and place it in 1st part of pel. If there area unit additional characters in Key array, then place rest within the 1st part of next pixels.

Step 5: Place some terminating image to point finish of the key. zero has been used as a termi- nating image during this algorithmic rule.

Step 6: Place characters of message Array in every part of next pixels by exchange it.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 5, May 2022||

| DOI:10.15680/IJIRSET.2022.1105227 |

Step 7: Repeat step six until all the characters has been embedded.

Step 8: once more place some terminating image to point finish of knowledge.

Step 9: Obtained image can hide all the characters that input.

The simplest steganography techniques introduce the bits of the message directly into least signif- icant bit plane of the duvet image in an exceedingly settled sequence. Modulating the smallest amount vital bit doesn't lead to human-perceptible distinction as a result of the amplitude of the modification is little. to cover a secret message within a picture, a correct cowl image is required. as a result of this technique uses bits of every constituent within the image, it's necessary to use a lossless compression format, otherwise the hidden info can wander off within the transformations of a lossy com- pression algorithmic program. once employing a 24-bit color image, a small amount of every of the red, inexperienced and blue color elements may be used, thus a complete of three bits may be hold on in every constituent.

For example, thefollowinggridcanbeconsideredas3pixelsofa24-bitcolorimage, using 9 bytes of memory:

(00100111 11101001 11001000)

(00100111 11001000 11101001)

(11001000 00100111 11101001)

WhenthecharacterA,whichbinaryvalueequals10000001,isinserted,thefollowinggrid results:

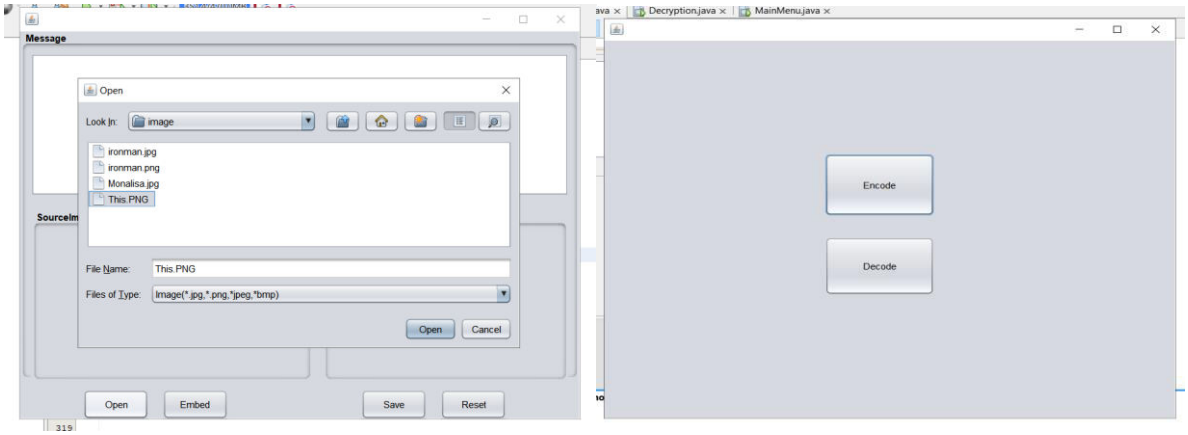
(00100111 1110100011001000)

(00100110 1100100011101000)

(11001000 0010011111101001)

VI. EXPERIMENTAL RESULT

This section we've got mentioned some experimental result, the data image and canopy image square measure chosen as true color pictures, the resultant stego image is generated, figure shows end result of the generation of stego image and extracted to original image.

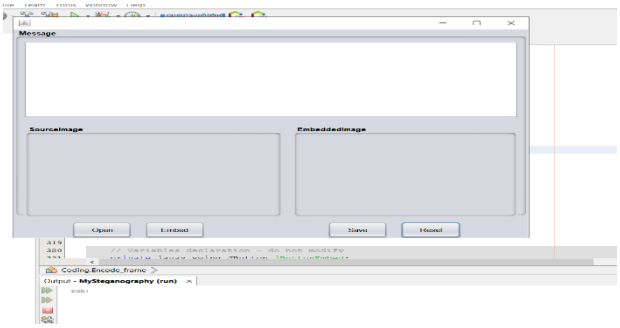


(a) Open button (b) Main menu

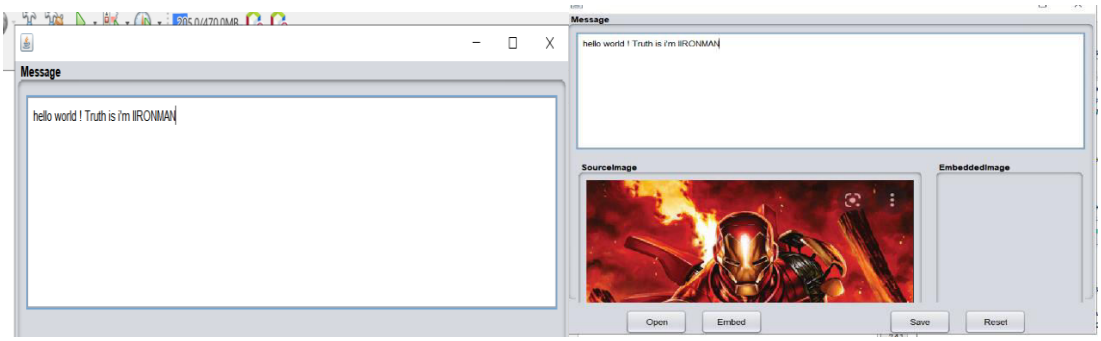
| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 5, May 2022||

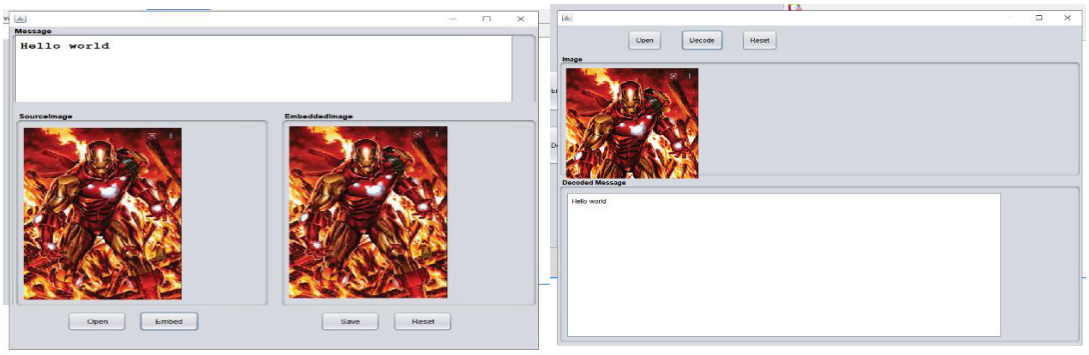
| DOI:10.15680/IJIRSET.2022.1105227 |



(c) Application UI



(d)Text Area (e) Source Image



(f) Encode Image (g) Decode Image

All figures shows how to implement the hiding information within the image using steganography technique.We have implemented the Information hiding within image using image steganography technique. Our algorithm successfully hides the information within image. We have applied our algorithm on many images and found that it successfully for concealing data in image.This is used to transfer some secret message to another person; with this technique, no one else in between will know the secret message you wanted to convey.

VII. CONCLUSION

It is discovered that through LSB Substitution Steganographic technique, the results obtained in information activity square measure pretty spectacular because it utilizes the easy incontrovertible fact that any image might be jerky to individual bit-planes every consisting of various levels of data. It's to be noted that as mentioned earlier, this technique is merely ef- fective for bitmap images as these involve lossless compression techniques. But this method can even be extended to be used for color images wherever, bitplane slicing is to be done one by one for the highest four bit-planes for every of R, G, B of the message image.

It is conjointly necessary to debate that although steganography was once unobserved, with the assorted strategies presently used, it's not solely simple to notice the presence however conjointly retrieving them is simpler.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 5, May 2022||

| DOI:10.15680/IJIRSET.2022.1105227 |

REFERENCES

[1] Ahmad Shaik, V. Thanikaiselvan and Rengarajan Amitharajan, "Data Security Through Data Hiding in Images: A Review", Journal of Artificial Intelligence, 2017, 10 (1):1-21.

[2] Rosziati Ibrahim and Teoh Suk Kuan, "Steganography Algorithm to Hide Secret Message inside an Image", Computer Technology and Application 2 (2011) 102-108.

[3] D.C. Lou, J.L. Liu, H.K. Tso, Evolution of information –hiding technology, in H. Nemati (Ed.), Premier Reference Source–***Information Security and Ethics: Concepts, Methodologies, Tools and Applications,*** New York: Information Science Reference, 2008, pp. 438-450.

[4] Odai M. Al-Shatanawi and Nameer N. El. Emam, "A NEW IMAGE STEGANOGRAPHY ALGORITHM BASED ON MLSB METHOD WITH RANDOM PIXELS SELECTION", International Journal of Network Security & Its Applications (IJNSA), March 2015 Vol.7, No.2.

[5] Ashraful Tauhid et al., "A Secure Image Steganography Using Advanced Encryption Standard and Discrete Cosine Transform", Journal of Information Security, 2019, 10, 117-129.

[6] Kamaldeep Joshi et al., "A New Method of Image Steganography Using 7th Bit of a Pixel as Indicator by Introducing the Successive Temporary Pixel in the Gray Scale Image", Hindawi, Journal of Computer Networks and Communications, Volume 2018.

[7] Dr. Ekta Walia, Navdeep and Payal Jain. ***"An analysis of LSB & DCT based Steganography."*** Global Journal of Computer Science and Technology, April 2010.

[8] Kaladharan N, "Unique Key Using Encryption And Decryption Of Image", International Journal Of Advanced Research In Computer And Communication Engineering Vol. 3, Issue 10, October 2014 ISSN (Online) : 2278-1021 ISSN (Print) : 2319-5940 Page 8102- 8104.

[9] Bhardwaj and S. Som, "Study of different cryptographic technique and challenges in future," in Innovation and Challenges in Cyber Security (ICICCS-INBUSH), 2016 International Conference on. IEEE,2016, pp. 208–212.

[10] Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," Signalprocessing, vol. 90, no. 3, pp. 727–752, 2010.

[11] J. Mandal and D. Das, "Steganography using adaptive pixel value differencing (apvd) of gray images through exclusion of overflow/underflow," arXiv preprint arXiv:1205.6775, 2012.

[12] V. L. Reddy, A. Subramanyam, and P. C. Reddy, "Implementation of lsb steganography and its evaluation for various file formats," Int. J.Advanced Networking and Applications, vol. 2, no. 05, pp. 868– 872,2011.

[13] N. Jambhekar, C. Dhawale, and R. Hegadi, "Performance analysis of digital image steganographic algorithm," in Proceedings of the2014 International Conference on Information and Communication Technology for Competitive Strategies. ACM, 2014, p. 82.

[14] D. Anandpara and A. Kothari, "Working and comparative analysis of various spatial based image steganography techniques," InternationalJournal of Computer Applications, vol. 113, no. 12, 2015.

[15] M. C. Trivedi, S. Sharma, and V. K. Yadav, "Analysis of several image steganography techniques in spatial domain: A survey," in Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies. ACM,2016, p. 84.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.118

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details