International Journal for Modern Trends in Science and Technology, 8(06): 600-607, 2022

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0806101
Available online at: http://www.ijmtst.com/vol8issue06.html

A Security Approach using Steganography, Deep Learning and Conventional Neural Networks in a Cloud Environment

P.Venkata Hari Prasad[1] | Dr.K.Gangadhara Rao[2]

[1]Research Scholar, Department of CSE,Acharya Nagarjuna University
[2]Professor, Department of CSE,Acharya Nagarjuna University
Corresponding Author Email ID: p.venkatahariprasad@gmail.com

To Cite this Article
P.Venkata Hari Prasad and Dr.K.Gangadhara Rao. A Security Approach using Steganography, Deep Learning and Conventional Neural Networks in a Cloud Environment. International Journal for Modern Trends in Science and Technology 2022, 8(06), pp. 600-607. https://doi.org/10.46501/IJMTST0806101

Article Info
Received: 12 May 2022; Accepted: 10 June 2022; Published: 27 June 2022.

ABSTRACT

Maintaining an information safe haven is a crucial limitation in the cloud computing environment. We can accomplish this using a variety of techniques, including steganography, cryptography, and watermarking. Due to the fact that information is kept by a third party from various locations and different places, those procedures are nevertheless plagued by some serious issues. Therefore, having some unique techniques that can effectively embed the information steadily is crucial. The security for data is an important parameter. Steganography is one of the prominent techniques to provide security. The introduction of steganography algorithms is based in part on the use of picture steganography. Existing picture steganography techniques insert confidential information into an image's pixels or content. Following some trails, the hacker is able to quickly find the secret information. Using steganography without the concept of embedding, this research proposes a new method for inserting secret data or images into other images. This method's foundation is a deep conventional neural network. Use one of the trained neural network techniques in this to map confidential data into a vector. With this method, a stego image can be obtained without the use of a mapping or embedding process. After the training procedure, we utilise an extractor neural network to extract data from the Stego image.Using this method, we can also integrate two distinct networks into one image. The original image is utilized to embed the hidden image via prep network. The secret image from the stego image is extracted using the reveal network. This suggested technique performed better in terms of embedding rate, extraction rate, and payload capacity after training on a variety of data types.

Index terms: Steganography, Deep Conventional Neural Networks, Steganography without Embedding, Payload capacity

1. INTRODUCTION

Data security is one of the prominent parameter in different fields. To provide security for data so many existing techniques are present. There are several methods available today for providing security for user data in a cloud setting. Steganography and segmentation are both secure methods for preserving a safe haven in those procedures unapproved users have access to user information . The process of "steganography" involvesputting data into a picture and

masking it such that the human eye cannot directly see it.Steganography is one of the traditional approaches to provide security for data. Steganography means hiding the secret data into a carrier from unauthorized persons. In this we have different techniques like Text Steganography, image steganography and audio/video steganography. The text steganography hide the secret data into text. Image steganography means hide or embed secret data into an image. In general the available data is in many forms like text/image/audio/video. This image steganography generally performed in two domains, spatial domain and transform domains.

In majority of the steganography algorithms use the concept of embedding secret data into the image. But this process is easily hacked by the hackers and loss the secret data. In order to avoid or reduce the risk from the existingalgorithms this paper prose a new technique based on the steganography without embedding and also majority of the algorithms are use to embed the data is in the form textual into the given carrier original image. This algorithm is also suitable for hiding image into an image.

Some of the algorithms are present based on the concept of steganography without embedding. In some of those algorithms the mapping process of the secret data is based on the semantic features of the natural images and also image thrashing technique [1]. In this technique use hashing process for mapping image pixels into secret information pixels and this algorithm was not suitable for larger images [2]

In this paper we proposeda new method based on the steganography without embedding technique using deep conventional neural networks. The main objectives of this proposed approach includes

1. We proposed a new technique of using deep conventional neural networks. This technique is different from already existing approaches like traditional embedding approaches of LSB embedding process and DCT coefficients embedding program. In this method we use a neural network to generate cover image according to the secret data.
2. For extracting data from the stego image we use highly trained network, extractor
3. In this proposed directly we can embed the image into another cover image with minimum noise in the cover image

The rest of the paper is organized as follows. Section II consists of various existingalgorithms in image steganography concept. Section III presents the novel proposedtechnique. Section IV consists of results and its analysis with respect to various parameters of steganography. Section V presents conclusion and its future scope this proposed work.

2. LITERATURE REVIEW:

Most of the existing steganography algorithms are based on the embedding process. In this the algorithms were broadly classified into two different environments spatial and transform domains. Majority of the existing algorithms embed the secret data or information into an image upon some parameters and conditions. All of the existing algorithms the secret data are in the form text. We cannot have proper embedding algorithm if the data is in the form of image[3].

Milmamal [4] suggested a change to the LSB method. This method involves inserting the secret information inside the original cover image's invertible pixels. When compared to many other LSB-based algorithms that are currently used in spatial contexts, this algorithm's payload capacity and embedding time were both very high.

A new embedding algorithm that is more suited for digital images was put out by Perny et al. in their proposal in [5]. The distortion function reduction is the major goal of this effort. The weight total of the difference between the feature vectors of the natural picture is used to calculate the distortion function, and those values are then subtracted from the cover image's invertible pixel values. Hou et al. [6] offer the wavelet technique to incorporate the payload in the cover picture in the more intricate texture of the true image regions. Based on the LSB non sequential embedding, Rich et al [7] proposed the most trustworthy and accurate approach for embedding secret data.

Another method for embedding protected information into an image was put out by Shital et al. [8]. The JPEG image is the best fit for the suggested scheme. To acquire the stego analysis features in this case, the Markov process was used. A method using a Markov process and discrete cosine transformation was proposed by Fridrich [9]. To extract the features from a JPEG image, both techniques are used. In order to calculate the features for steg analysis of the stego image

in the spatial domain environment, Pevyes et al. [10] presented a SPAM. To determine the difference between neighbouring pixels for the purpose of extracting more characteristics, utilise the markov technique.

Using the idea of a model with numerous submodes as the foundation, Kodovsky [17] established a fundamental technique. Steganaylsis was extended, mostly appropriate for colour images, by Goom et al. [11]. Utilizing CNN model to implant the secret data into the cover image, this technique also uses deep learning ideas for data extraction. A novel version of CNN was proposed by Qan et al. [12] with the idea of automatic feature extraction and complex pixel difference identification, which are both employed in steganography.

In steganography without embedding, there are currently two methods employed. One strategy is cover selection, and the other is cover synthesis. The cover selection method creates an image group by gathering a number of natural digital photographs, and then it establishes a connection between the original information and the secret data. The cover synthesis method uses secret data to create the cover image initially. The original cover image would change if secret data were altered.

A novel strategy was put forth by Zhous et al. [13] using the idea of SWE. Hashing is used in this case for the mapping procedure. The secret data mapping values and the original cover image were first used to generate the image database. The original image in this was split into an equal number of fragments. Each segment is mapped with the corresponding binary information mapping value. A strong hashing image steganography algorithm is what the hashing algorithm is referred to as.

Dievel[14] suggested a novel strategy built on the robust hashing method. By employing the hash function, the binary secret data is separated into segments and those segments are then mapped with the original cover picture pixel values. The image library is the key disadvantage of the cover selection-based technique. A brand-new strategy built on the cover synthesis was developed by Otori[15]. The innovative texture synthesis transformation methods were proposed by Xz et al [16]. The original input image or textual data is converted into a stego image using this method. With the use of mathematical functions, the stego texture is generated based on the real-time synthesis system, and the concealed data is recovered using the decrypterfunction[23].

3. PROPOSED METHOD:

The proposed algorithm is suitable for two different types of data i.e. textual information and image.

Case I: If the secret data is in the textual form the proposed algorithm is in different phases

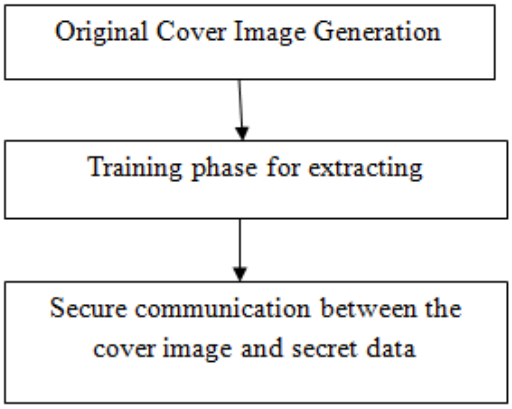

Figure 1: Phases in Proposed Algorithm

Phase I:

There are two distinct processes in the creating cover image phase. The first step is to partition the original, secret material into an even number of parts. Every data segment is represented as a DS, which maps to the noise vector Yi. The cover image is obtained in the second phase. Due to the lack of an embedding procedure in this technique, the cover image is a stego image. The multiple bits of the data segments are mapped for this mapping procedure using the noise vector ratio. The random function was used to produce those values.

$$r=random(x/2^{\sigma}-1+S\ x+1/2^{\sigma}-1-1-S) \quad (1)$$

Where the noise function's random values are created using the random function. The values of the noise vector fall between (x/2-1-1, x+1/2-1-1). The DSi/Yi is where. Figures 2 and 3 depict the phase I procedure and the mapping process in diagram form. Table I displays the relationship between the secret data and Noise values.

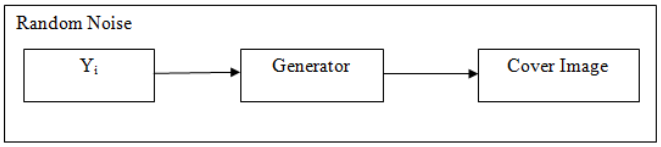

Figure 2: Generating Cover Image Process

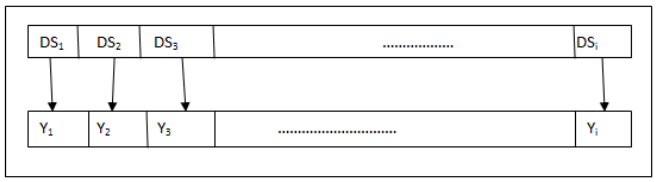

Figure 3: Mapping process Data Segments and Noise Vector

Table I: Relation of bits with noise vector

Bits	Noise values obtained from random function
000	random(-0.818,-0.651)
001	random(-0.849,-0.401)
010	random(-0.599,-0.351)
011	random(-0.249,-0.101)
100	random(0.351,0.567)
101	random(0.602,0.849)
110	random(0.689,0,899)
111	random(0.849,0.999)

Algorithm I: Generating original cover image

Input Variables: Y,X,σ

Output: Stego Image

1. Obtain the generator by using equation 1
2. t=c*X
3. n=length(Y)/t
4. Divide the secret data into nu number of segments of its length t
5. for k=1 to n do
6. for w=1 to t do
7. a=0
8. for z=w to w+ σ -1 do
9. $a=a+2^{w+\sigma-1-zY_{ij}}$
10. end for
11. for i= 1 to n
12. insert stego $_i$ into stego
13. end for
14. return stego image

Phase II:

A traditional neural network, referred known as an extractor, is designed in this phase and utilized to recover or extract data from the stego picture. This traditional neural network is created using layers. Every layer has connections to all other layers. Figure 4 depicts the structure of layered organization.

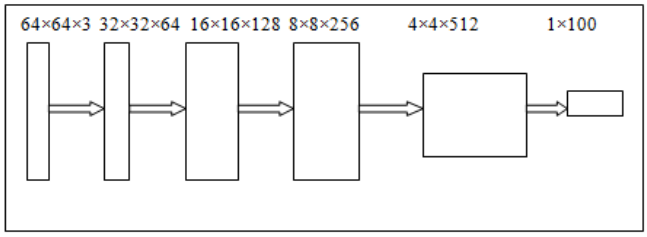

Figure 4: Layers for CNN

The original stego image is of dimensions 64×64×3 and the output secret information noise vector with 1×100 dimension. The training process of extractor is shown in Figure 5.

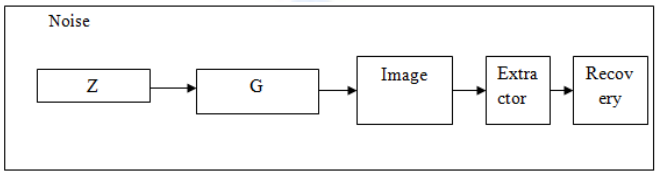

Figure 5: Extractor Process

Algorithm II: Extractor

Input : Stego Image

Output: Secret Information (D)

n=length (stego image)

for j=1 to n

Y_i= E (Stego image)

a=0

for i=1 to t do

$a=(V_{ij}+1) \times 2^{\sigma-1}j$

end for

Insert Di into D

end for

Phase III: Secret Information Communication

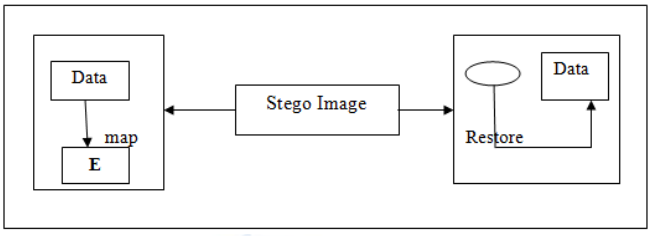

Figure 6: Process for secret communication

The data is sent to the CNN model by the transmitter, and the secret data and network parameter are received by the receiver. The sender computes the noise vector by splitting the original data into pieces. According to the mapping rules, the receiver restores the secret information after receiving the stego image and extracting the noise information.

Case II: The given data is in the form of image then the process is shown in Figure 7

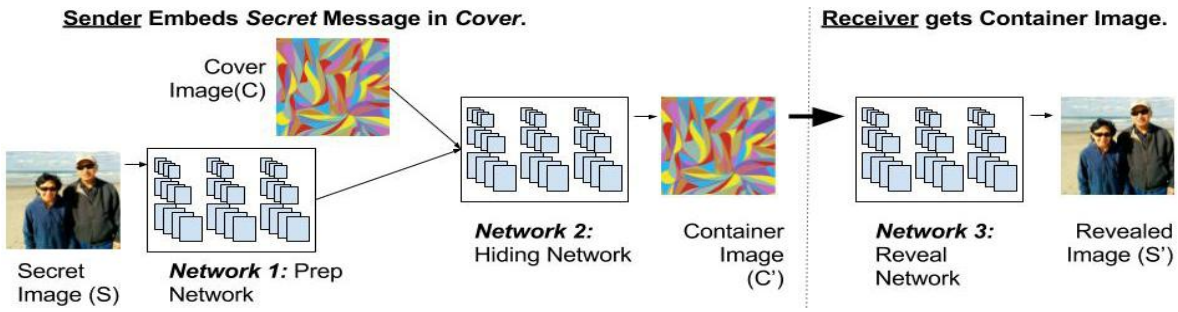

Figure 7: Process for inserting image into an image

Three essential elements make up this process. The secret image that will be hidden is prepared using the Prep network. Depending on the proportions of the cover picture and hidden image, it will automatically adjust its dimensions. It will prepare a network size equal to the size of the secret image in the first instance where the hidden image is less than the original image. The hiding network generates a container picture using the input from the cover image and the prep network. This container network features a cover picture as well as a secret image. It implies that the secret picture will be concealed within the cover image in this network. The disclosed picture is obtained by the reveal network using the input from the container image.

4. RESULTS AND ANALYSIS:

The proposed model trained on two different data sets. Dataset 1 Celebrities, which contain
300 k different, face images of the humans and Food010, which contains 75 k food images. All those two datasets are cropped into 64 × 64 size.

Case I: Insert Image into cover Image

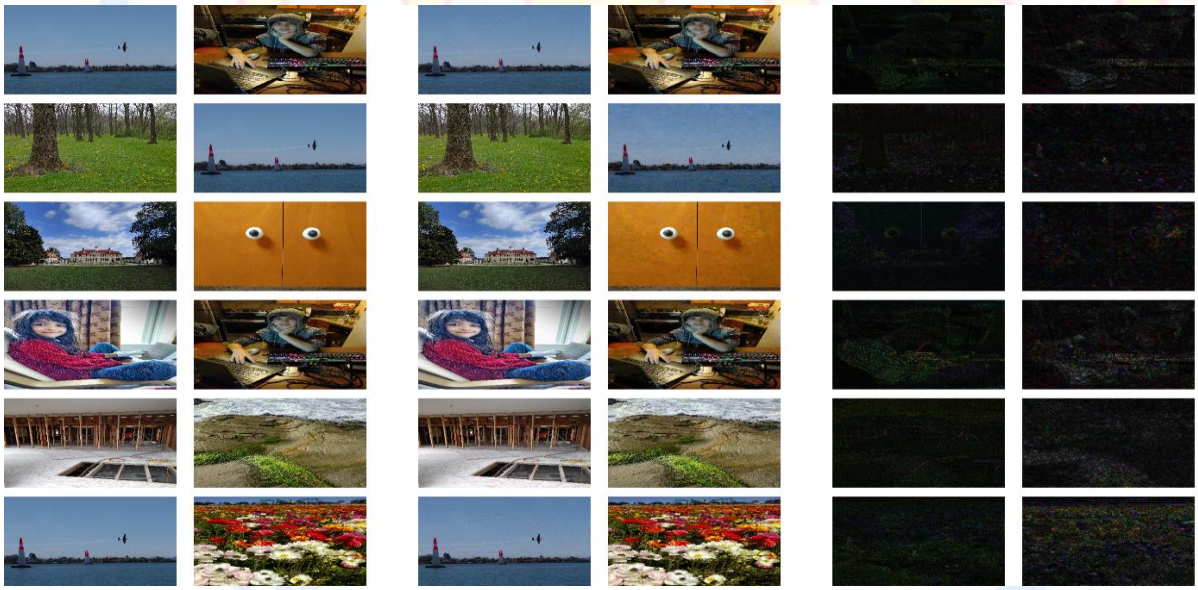

Figure 8: Hiding Results (Original image, secret image, cover image, embedding data with secret image, errors in between cover and hidden images)

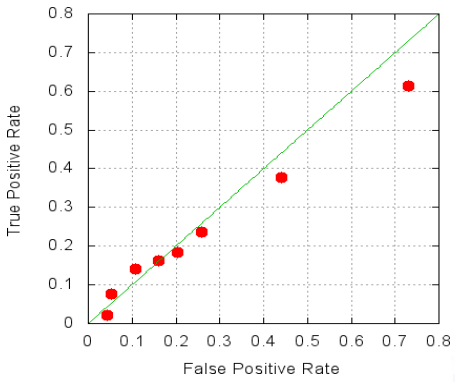

Figure 9 : ROC Curve between True and False Positive rate

Case II: Insert Textual data into cover image

In this experiment we trained with two different data set. The stego image is automatically generated by using training method and the data extracted using Conventional neural networks. The Table II shows absolute and relative capacities of various SWE existing method with proposed method

Figure 10: Cover image after Phase I

Table II: Comparison of Capacities of various SWE methods with Proposed Method

Algorithms	Capacity(Absolute)	Image Size	Capacity(Relative)
ZZHOU[18]	1.215	512 ×512	4.88 ~3
ZLHOUS[19]	2.89	480 × 480	1.32~5
S.AHANG[20]	3.72	480 ×640	7.48-6
J.XU[21]	21~98	1024 ×512	8.45 -5
WANG[22]	64×32	1024 ×1024	6.40~3
Proposed Method	>32.5	64 ×64	9.26 - 4

EVALUATION OF PSNR AND MSE

Two factors, PSNR and MSE, are considered for picture quality estimation for projected algorithms. The environment of the walked-on or altered image can be recovered to a larger extent with a higher PSNR. With the following stated expression, we can calculate this..

$PSNR=10 \log10 (MAXi^2)/MSE$ (1)

When pels are represented with 8 bits per sample, MAXi is a picture's most ideal pels value, which is 255. The MSE expresses the overall, highly developed difference between the first and trampled image. The error is proportional to the MSE calculation.$MSE=\sum X, Y [J_1 (x, y)-J_2 (x, y)]^2/X*Y$ (2)

This section compares projected security algorithms using picture steganography and image to image steganography to a variety of steganographic data concealing algorithms. It is plainly calculated and demonstrates that the projected method underwent a significant shift, making it superior to several existing image to image steganography-based algorithms. The MATLAB tools are used to evaluate various factors and determine the differences between the original cover image and the stego image. The comparison results of various current algorithm MSE values with projected

algorithm MSE are shown in Table III and Figure 11, while Table IV and Figure 12 show the comparison results of various current algorithm PSNR values with projected algorithm PSNR values.

Table III: Preceding and Projected Segmentation Method MSE scruples

Original Image	Previous MSE	Proposed MSE
Minion	0.0038	0.0036
One	0.0041	0.0032
Cameraman	0.0042	0.0034
Babo	0.0014	0.0011

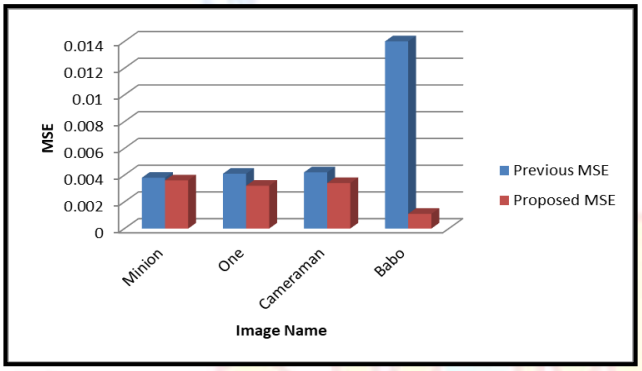

Figure 11: Comparison of Preceding and Projected Segmentation Method MSE scruples

Table IV: Preceding and Projected Segmentation Method PSNR scruples

Original Image	Previous PSNR	Proposed PSNR
Minion	68.45	75.67
One	64.53	76.89
Cameraman	78.67	83.99
Babo	75.46	84.02

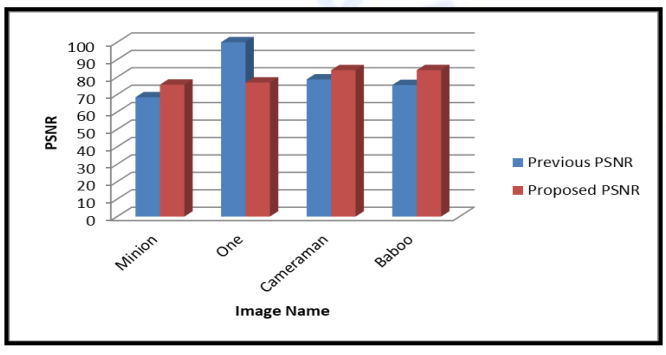

Figure 12: Evaluation of Previous and Proposed Segmentation Method PSNR values

5. CONCLUSION AND FUTURE SCOPE:

This paper proposed a new approach in image steganography without embedding methods based on the automatic generation of the cover image. This method produces stego images without encoding any data, so to speak. With the aid of the prep network, container network, and relief network, this approach is also appropriate for hiding one image within another stego image. The effectiveness of the suggested methodology is evaluated using various SWE method existing algorithms on a range of image size lengths. When an image's size is large, its storage space is just marginally sufficient. Low image size results in improved ratios for both absolute and relative capacity. Error codes can be added to this proposed solution to address the issue with higher image sizes.These problems will be left as a future work.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] Ki-Hyun Jung "A Study on Machine Learning for Steganalysis",DOI: 10.1145/3310986.3311000 Conference: the 3rd International Conference

[2] AshadeepKaur , 2Rakesh Kumar, 3Kamaljeet Kainth," Review Paper on Image Steganography" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 6, June 2018 ISSN: 2277 128X

[3] Sumit Kumar Moudgil" Steganography on Audio Wave Tenth Layer by Using Signal to Noise Ratio Test and Spectrogram Analyses International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 4 (2018) pp. 1931-1935 © Research India Publications.

[4] Harsh Kumar Verma,Milmamal ; Ravindra Kumar Singh, A hybrid approach of image steganography, 2016 International Conference on Computing, Communication and Automation (ICCCA)

[5] SwagotaBera1 ,Pernny , Dr. Monisha Sharma2 and Dr. Bikesh Singh, Feature Extraction and Analysis using Gabor Filter and Higher Order Statistics for the JPEG Steganography, International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 5 (2018) pp. 2945-2954

[6] GauravHou "Image steganography algorithm based on edge region detection and hybrid coding" International Journal of mathematical and computer modeling

[7] AmosaBabalola,Rich," Steganography Method for Hiding Data In The Name_Field of A List of Names Created by Microsoft Word" , International Journal of Scientific Research in Computer Science, Engineering and Information Technology © 2018 IJSRCSEIT | Volume 3 | Issue 1 | ISSN : 2456-3307

[8] Ankur Gupta,Shital" Image Steganography and Data Security Approaches: A Review", http://ijrar.com/, [VOLUME 5 I ISSUE 1 I JAN. – MARCH 2018]

[9] R.Keerthana,Fridrich,"Data Hiding with Adaptive Bitstream Steganography Cryptosystem",IJESC, Volume 8 Issue No.3

[10] Dr. SumathyKingslin,Peyys," Design of a Security Based Technique for Handling Secure SMS in Mobile Phones using Text Steganography", International Conference on Advancements in Computing Technologies - ICACT 2018

[11] Vandana Yadav,Goom"A New Approach for Image Steganography Using Edge Detection Method for Hiding Text in Color Images Using HSI Color Model" , 2017 IJSRSET | Volume 3 | Issue 2 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099

[12] Zhili Zhou,Qan" Coverless Image Steganography Without Embedding",International Conference on Cloud Computing and Security, ICCCS, Springer, 2018

[13] Amit Kumar, Zhupus DWT and LSB based Audio Steganography- A Review, International Journal of Engineering and Management Research Page Number: 82-84, Volume-8, Issue-1 February 2018

[14] XintaoDuan,dievel, Coverless information hiding based on Generative Model, School of Computer and Information Engineering

[15] G.Umamaheswar, Otori,A Study of Various Steganographic Techniques Used for Information Hiding, International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.6, December 2017

[16] Karthikeyan B,XZ, Gray Code Based Data Hiding in an Image using LSB Embedding Technique, International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8, Issue-1, May 2019

[17] Abdelhamid AwadAttaby,Koosvkay, Data hiding inside JPEG images with high resistance to steganalysis using a novel technique: DCT-M3, Ain Shams Engineering JournalVolume 9, Issue 4, December 2018, Pages 1965-1974

[18] AnhongzzhouWang, A Secret Image Sharing with Deep-steganography and Two-stage Authentication Based on Matrix Encoding, International Journal of Network Security, Vol.19, No.3, PP.327-334, May 2017 (DOI: 10.6633/IJNS.201703.19(3).01)

[19] Muhammad Zaheer,zzhous" Compressed Sensing Based Image Steganography System for Secure Transmission of Audio Message with Enhanced Security", IJCSNS International Journal of Computer Science and Network Security, VOL.17 No.7, July 2018

[20] Tamanna,Shang" Analysis and Refinement of Steganography Techniques", International Journal of Computer Applications (0975 – 8887) Volume 170 – No.8, July 2018

[21] J.yIsmail AbdulkarimAdamu and BoukariSouley," PERFORMANCE ANALYSIS OF TEXT AND IMAGE STEGANOGRAPHY WITH RSA ALGORITHM IN CLOUD COMPUTING", International Journal of Software Engineering & Applications (IJSEA), Vol.9, No.1, January 2018

[22] Mahdi Koohi, WANG, Practicing LSB Steganography in PCA Transform Field, International Journal of Innovative Research in Computer Science & Technology (IJIRCST) ISSN: 2347-5552, Volume-5, Issue-3, May 2017 DOI: 10.21276/ijircst.2017.5.3.5

[23] De Rosal Ignatius Moses Setiadi, Secure Image Steganography Algorithm Based on DCT with OTP Encryption,https://www.researchgate.net/publication/317401791