REVIEW PAPER ON IMAGE STEGANOGRAPHY

Vaibhavi Sushil,Abhishek Shahi

M.Tech Scholar, Department of Computer Science & Engineering, Buddha Institute of Technology GIDA , Gorakhpur, (U.P.) India.

, Assistant Professor, Department of Computer Science & Engineering, Buddha Institute of Technology GIDA , Gorakhpur, (U.P.) India

ABSTRACT

Computer based communications nowadays are at threshold of making our lives easier in the world; from exchanging electronic documents, to communicating with each other, to sharing information ,and to check bank balances and pay bills. Information security is an essential part that must be taken into consideration to ensure communication. Steganography is the technique that restricts the unauthorized users to have access to an important data. By using Steganography, the information can be hidden in the carrier items such as images, sound files, text files, videos while performing the data transmission. Therefore, this is a review paper for the various studies done on steganography. It also analyzes the work that have been conducted on steganography and clarifies the strength and weakness points on each work separately.

Keywords: *Steganography, Types of steganography, Techniques of steganography.*

Introduction

People use many different techniques to hide the elements and information they deemed valuable from past to present. Steganography of one of them. Steganography is not a new work area[1]. The first use of steganography was originated in 440 BC. Internet is generally used for data transfer. It has significantly become an important part in today's life. In fact. It has become increasingly important to secure the information exchanged while making the use of cyber space [2], for many business industries, government organization and for individuals. The reason why questions of online privacy and cyber security have raised the issue of secret writing into limelight is fact that today our social, economic and professional lives are completely dependent on emailing, net posting, e-commerce, electronic banking etc. [3]. Steganography wonders hiding the presence of secret information. It is the alternative of cryptography, where alternations are made to messages. Hence steganography and cryptography are cousins in spy craft family. In cryptography, the messages are scrambled which makes it unintelligible, while on the other hand steganography makes a message invisible by hiding it [4]. In steganography, the secret messages are kept out of sight by the use of a cover medium (i.e., carrier) before it is passed on a public communication channel. It therefore, obstruct the unauthorized access to the messages and also it protects its confidentiality. The secret messages can be encrypted or compressed before the application of steganography increases the security level and reduction in the amount of data to be embedded [1]. This paper represents the various steganography techniques that have been proposed recently for hiding the secret information within the cover-images efficiently. It is a high security technique for long data transmission. There are various kinds of methods of steganography:

1-Least significant (LSB) method

2-Transform domain techniques

3-Statistical methods

4-Distortion techniques

Steganography-

Steganography derives from the combination of Greek word "Stegano" which means sealed and "Graphy" refers to the writing which means secret writing. It is an old art of submerging the personal information into the other data by using some rules and techniques [5]. As a result, the unauthorized users will not be able to see and recognize the embedded information. While designing a steganography algorithm the two key features undetectability and embedding must be considered. There is a balance between the two features. The more bits is placed in the cover image, the more detectable tracks appear in stegonal image, which allows some stegano analysis algorithm to attack. The process is explained as follows-

By using the key the data is first hidden in a cover file transmitted to the recipient. Thus, once the message gas been received, the recipient uses the same key to read the encrypted message and thus provides unopened transmission [6]. There are following terminologies used which are as follows-

A confidential message that is transmitted securely is called a message [7].

Cover coding- It is the object that is used to hide the data. It can be an image, audio, video [7].

Stego key- this key is used to encrypt and decrypt the confidential information [7]

Stego object- the object is created after hiding the hidden message in cover image. Then the stego object is passed. At the recipient side the stego object is side processed to receive the message [8].

Embedding algorithm- this algorithm is used for hiding the message on the cover [7].

Extraction algorithm- this algorithm is used to display the message from the stego object [7].

Rules of steganography are as follows-

The information within the container should not be distorted significantly within the embedded data [9]. Embedded data must be encoded directly into the media to maintain its consistency [9].

Submerged data must be contrary to modifications, handling and attacks as possible [9].Embedded data must use the error correction codes [9].Embedded data should be self – locked [9].All embedded data must be repairable, even if only the part of the cover data is available [9].The steganography methods are explained as follows-

Insensitivity- It means that the steganographic system is not performed by the human eye. After submerging the steganographic element on the carrier element, the changes in the images should not be noticed by the human eye. The reason behind this is that the human eye is tactful to visual values such as brightness and blurr , the values should be considered.

Embedded capacity- It is recommended that you should not exceed the 51% of its maximum. Since the capacity of the important message is not greater than the carrier message. Otherwise, the element of invisibility, one of the elements of steganography is pierced.

Robustness- It refers to the level of difficulty that is required to demolish the embedded information while not damaging the cover object[10].The attacker is in the situation where it is impossible to disclose the message even if the carrier predicts a hidden message in the object. PSNR was generated from initial of the peak signal to the noise ratio**.**

Confidentiality – It means that the confidential information removed from the video should not occur without the prior consent of the intended user's password [7].

Accuracy – The removal of confidential message must be accurate and well grounded[7].

PSNR – It is the metric that is used to indicate the ratio of the maximum possible power of a signal to the power of the noise on the signal. The original data is represented by the signal and the compression- related error is represented by the noise. When comparingthe compression codes, PSNR can be considered as an approach to human quality consciousness.

PSNR=log(MAX1^2/MSE)

MSE(Average Frame Error)- It is defined as the mean square difference between the distorted image and the reference image. It is calculated by pixel-by pixel sum by summing the square difference of all pixel and dividing them by the total no. of pixels [11].

SNR(Signal to noise ratio)- It is defined as the ratio between signal strength and noise strength.

Steganography measures [7]

Invisibility- It is the steganographic process that cannot be catched with by the human eye .

Load- It shows the amount of confidential information that can be encapsulated in the cover image.

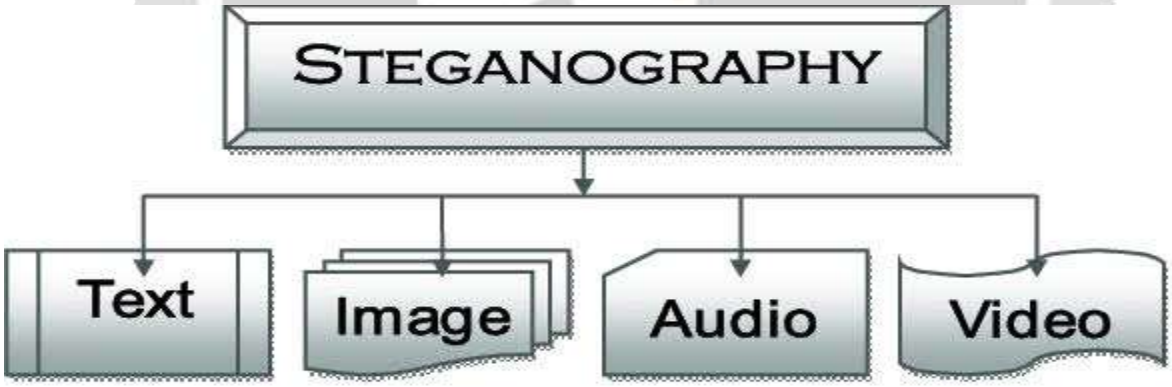
Statistical Attacks- It is the operation of extracting the confidential information from a stego object.

Security- It is defined as non – guaranteed if statistical tests cannot distinguish between cover and stegography image.

Computational cost- It is the required time failed to run that selected algorithm it is counting the minimum loops together supposing that each of it have fixed time to work.

Perceptual Quality- Increasing the load decreases the quality of the video, so the approach should be used in such a way that the quality should remain undamaged to prevent awareness.

Types of Steganography-



1- Image Steganography –

Image steganography, which is submerged In digital image poses a hazard of protecting sensitive information and gathering intelligence. It is a kind of steganographic system in which the confidential messages are hidden in a digital image by some concealment methods [12]. Many steganographic methods have been proposed to hide the hidden data in an images [13]. Some images are monochrome and grayscale in nature and they uses 8-bit per pixel. Normal digital color images usually consists of 24 bits. All these types of pixels are derived from three primary colors red, blue, green. Each primary color consists of 8 bits data.

The basic steps involved in image processing are as follows-

Image retrieval- It is used for image processing and compression [30].

Image preprocessing- An improved image acquisition process with a variety of techniques.

Image segmentation- It helps to divide the input image into sub images.

Image display- It is used for converting the input data into a computer compatible form.

2- Video Steganography –

In video steganography, the steganography sender sends the confidential message to the recipient via the video sequence. The optional value of "k" can also be used when embedding the confidential message into the cover media to reproduce "stego- video". The stego video is hand on the receiver via the common channel. On the other hand, at the receiving side, the receiver uses the secret key with the extraction algorithm to extract the confidential information from stego object.

$Sk(m,n) = Ck(m,n) + ak(m,n)\ Mk(m,n),$
$K=1,2,3,--N$

3- Audio Steganography –

It is defined as when the confidential message that is to be sent are embedded in digital audio, is termed as audio steganography. The method embeds the confidential message in WAV, AU and MP3 audio files [15]. It consists of a carrier or message, password and audio files. Here a carrier is known as a cover file that is used to hide the confidential information. Steganography requests the sender that the encrypted message should remain confidential. Text ,sound, image or any other confidential message that is to be sent to any other file can be chimney. It is important for the recipient that the corresponding decoding key must be a stego key. The cover file that contains the confidential message is known as a stego file. There are two stages in the storage process. The first step is to define the backup bits in the cover file. Second step consists of the embedding hidden data in the cover file, the backup bits in the cover file are replaced with the bits of the hidden file with the help of Human Hearing System (HAS), information can be added to the music files in voice steganography. HAS is used to recognize the additional random noise and it can also detect the complexity in an audio files. But it is not perfect.

4- Text Steganography-

It is one of the most common types of steganography. The main reason behind this is that it is most commonly used steganography in practical methods. it's importance is lost because of its ease of decoding and has less crrying capacity [16].

Text steganography is generally categorized into two categories-

Linguistic steganography – it consists of two sub parts- syntactic and semantic.
Format steganography- it consists of categories of word shift coding, open field coding, feature coding and line shift coding [17]. These techniques are used in physical text formatting as a place where text can be hidden. This technique is used to replace the existing data to hide steganographic text [18].

5- Protocol Steganography-

It is an array of rules which is used to manage the communication that is being known as protocol. UDP, TCP/IP are some of the protocols used for communication. It is used to hide the information, as with the other steganography methods. In doing this, it is also used to hide the protocol header information. Two different approaches are used for embedding and extracting the data in protocol steganography, such as the traditional embedding process used and the evolutionary removal of information [19].

Methods used in image steganography-
Of all the frameworks, the methodologies are grouped in three categories namely, traditional based image steganography methods, CNN based image steganography, and GAN based image steganography methods.
Traditional based image steganography-

It is a framework that uses the methods which are not related to the machine learning or deep learning algorithm. Most of the traditional methods uses the LSB technique. Images are of higher pixel quality, out of which not all the pixels are used. LSB methods performs the function under some assumptions that they modify a few pixel values which do not show visible changes. The secret information are converted into a binary changes. The cover are scanned that determine the least significant bit. The binary bits are then substituted in LSB of the cover image. The substitution method has to be performed deliberately as overloading the cover image may lead to visible changes leaking the presence of the secret information[25]. LSB methods are used for hiding the secret information inside the videos also which are called as video frames.

CNN- based image steganography methods-

Image steganography using CNN is heavily inspired from a encoder – decoder architecture. The two inputs – cover image and the secret image are catered as an input to the encoder to generate the steganography image and then the steganography image is given as an input to embedded secret image. The way in which the input cover image and the secret image are concatenated are also different in different approaches, while the variations in the convolutional layer, pooling layer are expected. The number of filters used, strides, activation function used and the loss function varies from method to method. One important point to be noted in the method is that the size of the cover image and the secret image has to be same, so that every point of the secret image can be distributed in the cover image.

U-Net based encoder decoder architecture are used for hiding the information and a CNN having 6-layers are used for the extraction process. The input shape of the U- Net architecture are modified to accept the 256x256 and 6 channels. The cover image and the secret image are nurtured to give the input and hence the 6 channels. The U-Net based hiding (H-net) and revealing (R-net) network are used. Also batch normalization and ReLU activation.

A separable convolution with residual block (SCR) are used to interconnect the cover image and the secret image [26]. The embedded image is given as an input to the encoder for constructing the steganography image which is given to the decoder to output the decoded secret image. ELU (Exponential Linear Unit) and batch normalization are used.

An autoencoder decoder architecture with VGG as base is used. An arbitrary image size for the secret information and using the adaptive instance normalization (AdaIN) and the output is the size of the cover image. By using the pixel distribution of the cover image are taken [27]. The secret information is then embedded in the pixel distribution evenly by reduced sampling.

There are three networks namely prep-network, hiding network, and the reveal network which are proposed by Baliya that are based on auto encoder architecture as a single model. The prep network is used for preparing the input to the hiding network , which takes the output of the prep network and the cover image to produce container image. The reveal network is used for decoding the secret image from the container image by disclosing the cover image. Two loses are calculated between the cover image and the constructed image and between the secret image and the decoded image.

Table 1: Summary of the details on the CNN-based steganography methods.

Method	Architecture	Dataset	Advantages	Disadvantages
[31]	Encoder-decoder	ImageNet	- Image is secret message	- However image size is 64 × 64 which is very small
[27]	U-Net	ImageNet	- Image is secret message - Basic and minimum architecture is used	- However image size is 64 × 64 which is very small - Input images are just concatenated
[28]	CNN	ImageNet and Holiday	- Image is secret message. Basic and minimum architecture is used - New error back propagation function is introduced to speed up training	- However image size is 64 × 64 which is very small - Input images are just concatenated
[29]	Encoder-decoder with VGG base	COCO and wikiart.org	- Domain-knowledge is not required - Highly secure as the generated image is not related to the secret information	- Computation is increased by using additional image
[25] and [26]	Encoder-decoder with SCR	ImageNet	- Highly secure and robust	- Loss used is not optimal - Visible noise can be seen in black or white regions

GAN based image steganography methods-

General Adversarial Network is a type of deep CNN introduced by Goodfellow in 2014 [28]. For the image generation task, GAN uses the game theory to train a generative model with adversarial process. The two network are used for generating a perfect image in GAN architecture- generator and discriminator. The data is given to the generator model and the close approximation of the given input image is the output. The discriminator network classifies the images generated as either fake or true. The two networks are trained in such a way that the generator model tries to imitate the input data as close as possible with minimum noise. The discriminator model is trained to effectively find out the fake images.

GANs are known for their good performance in the image generation field. Image steganography can be considered as one such image generation task. Here, the two inputs cover image and the secret image are given to generate one output – stego image. The GAN architecture can be grouped into five categories - the three network based GAN model, cycle-GAN based architectures, sender-receiver architecture using GAN, coverless model where the cover image is generated randomly instead of being as input and an Alice, Bob and Eve based model.

Generally, a GAN model consists of two main components: the generator and the discriminator. But, in context of image steganography, a new network named the steganalyzer is introduced. The main functions of these components are-

i- A generator model, G, is used to generate the stego images from the cover imahe and the random message.

ii- A discriminator model, D, is used for classifying the generated image from the generator as either real or fake.

iii- A steganalyzer model, S, is used for checking if the input image has a confidential secret data or not.

Method	Architecture	Dataset	Advantages	Disadvantages
[39]	Alice, Bob and Eve	BOSSbase and celebA	- Domain knowledge is not required for embedding	- Message is used rather than images - Grid search for selecting the embedding scheme is time consuming
[37]	Info-GAN	MNIST and celebA	- Additional security is provided by adding an extraction key along with the cover image for the generator	- Message is encrypted using extraction key generator. Both the extraction key and generator trained are publicly available which makes it prone to attacks - No privacy plans in place to avoid this attacks
[2]	DCGAN	CelebA and BOSSBase	Game-theoretic formulation is used	- Use of three components. Steganalyzer is used to provide the probability alone which leads to more computational overhead
[54]	WGAN	CelebA	- Image is secret message	- If the generative model is not working properly, the secret image will be lost
[53]	ACGAN	MNIST	- Highly Secure and robust with increased hiding capacity	- Complicated design for hiding the secret information. First images are generated as per the secret information and additionally noise to be added - A secure channel is required to pass the database of the word segment and the corresponding image
[47]	Cycle GAN	USC-SIPI	- Better performance and security than LSB methods	- Text information are hidden. The main question here is how to extract the hidden message back from the stego image. The proposed method is not complete - Convergence loss of GAN can cause mode collapse
[56]	DCGAN	DTD and COCO2017	- Secret image can be of any width and height	-Texture based images are only produced
[50]	Cycle GAN	ImageNet and Photo2Monet	- Securing of the medical data to enhance the privacy of the medical records	- Cycle GAN is used for masking the real data in IoT. The use of steganography in the place of encryption is not explained
[43]	GAN	CelebA	- Generation of unlimited number of cover images are possible	- Shared generator and discriminator. User has to choose the seed value instead of the cover image - Generated images are not natural
[38]	DCGAN	CelebA	- Generation of more realistic images - Highly secure	- The steganalyzer gives probability rather than the secret information - No explanation on how to uncover the secret message
[42]	ASDL GAN	BOSSBase	- New activation function to generate the stego images	- ASDL-GAN is still inferior to state-of-the-art hand-crafted steganographic algorithms

Table 2- Summary of the details on the GAN- based steganography methods.

Datasets used-

There are following datasets which are used in image steganography-

A. BossBase- Break Our Steganographic System (BOSS) is the first scientific challenge that is conducted to take image steganography from being a research topic to a practical application. The main aim was to develop a better steganalysis method that can break the steganographic images created by the HUGO (Highly Undetectable steGO) algorithm.

B. CELEBA- Large- scale CelebFaces Attributes dataset, also known as CelebA dataset [29] is a wide dataset with more than 200k images which can be used for face recognition, face detection, face localization, and other face related operations.

C. **IMAGENet-** It is a very large dataset containing images from the WordNet hierarchy with each node containing more than 500 to 1000 images. ImageNet do not contain any copy- rights to the image and containd only the links or thumbnails to the original image.

D. MNIST HANDWRITTEN DIGITS- Modified National Institute of Standards and Technology databse(MNIST) which can be used for various computer vision and image processing applications. It contains a training and testing set with images of handwritten digits 0 to 9. The training set consists of 60,000 images and testing set consists of 10,000 images.

E. COCO- Common Objects in Context (COCO) dataset was mainly invented for object detection, segmentation and image captioning purposes. It is a large data set with images from 80 object categories. Each class contains at least 5 images.

F. **OTHERS-** Other datasets which can be used for image steganography and steganalysis are Div2k, SZUBase, USC-SIPI, DTD, LFW, and Pascal VOC. Div2k [30] are commonly used datasets for single image resolution.

Table 3- Information of the details of the dataset used in the literature of steganography.

Dataset	Number of samples	Images format	Image Size	Purpose
BOSSBase	9074 training and 1000 testing	tiff	512 × 512 × 1	Steganography and steganalysis
CelebA	More than 200K	jpg		Face attribute recognition, face detection, landmark (or facial part) localization, and face editing and synthesis
ImageNet	More than 14M	Arbitrary	Arbitrary	Computer Vision
MNIST Handwritten Digits	60,000 training and 10,000 testing	idx	28 × 28 × 1	Image processing and computer vision
COCO	330K	jpg	640×640×3	Object detection, segmentation and image captioning
Div2K	800 training, 100 validation and 100 testing	png	1020×678×3	Single Image Super-Resolution
SZUBase	40000	-	512×512×1	Steganography and steganalysis
USC-SIPI	170	tiff	256×256×1, 512×512×1, or 1024×1024×1	Image processing, image analysis, and machine vision
DTD	5640	jpg	300×300×3 and 640×640×3	Textural analysis
LFW	13233	jpg	150×150×3	Face verification
Pascal VOC	11530	jpg	500×300×3	Object detection and classification

Steganography Techniques-

Steganographic techniques are categorized into two broad categories [27, 30] -

1- Spatial Domain Techniques- In this type of method, the carrier object pixels, such as video object and images are operated directly and changed in order to hide the secret data inside it [20,21].

i- Least Significant Bit- It is a simple strategy that is used for implementing steganography like all other steganographicmethods, it is used for embedding the data into the cover, so that it cannot be predicted by the usual observer. Generally, LSB algorithms are used for replacing the most – right bits of a cover files bytes.

Mathematically, it can be represented as-

x'i= xi-xi mod2k+mi

where

x'i is steganographic image inum

xi represents the pixel of the carrier message that is to be notified

mi is reliable data in the first block

kindictes the number of opertions to be changed in the LSB.

Mathematically, the message is-

mi= xi mod2k

Pixel 1: 11111000 11001001 00000011

Pixel 2: 11111000 11001001 00000011

Pixel 3: 11111000 11001001 00000011

LSB algorithm hides bits of letter 'A', which are 01000001, into image pixels to produce:

Pixel 1: 11111000 11001001 00000010

Pixel 2: 11111000 11001000 00000010

Pixel 3: 11111001 11001001 00000011

ii- Gray level modification(GLM)- It is defined as a technique in which the gray level values are modified in accordance with the mathematical function to present the binary data.

iii- Pixel Value Differencing(PVD)- It is defined as a scheme that uses the difference value between the two consecutive pixels to determine how many secret bits should be embedded. It is used for providing the high imperceptibility to the stego object by selecting the two consecutive pixels & is used for desigining a quantization range table to determine the payload.

2- Transform Domain Techniques- In this type of technique, the carrier objects are first transformed from spatial domain to transform domain, then it's frequencies are used to hide the secret information. After embedding the secret data it is again transformed into spatial domain.

i- Discrete Wavelet Transform (DWT)- It is defined as the accomplishment of the wavelet transform that makes the use of translation following the defined rules and a discrete set of the wavelet scales [25].

ii- Discrete Fourier Transform (DFT)- This transform is considered as the most important discrete transform which is used to carry out the fourier analysis. The samples can be values of pixels along a row or column.

iii- Discrete Cosine transform (DCT)- This transform is used to articulate a fixed sequence of data points that are oscillating at different frequencies. DCTs are important to several applications in engineering and science [26].

Distortion Techniques-

It requires the knowledge of the cover image at the time decoding process where the decoder functions to check the difference between the original cover image and the distorted cover image in order to restore the secret message. While on the other hand, the encoder adds a sequence of changes to the cover image. Therefore, the information is narrated as being stored by the signal distortion [29].

Conclusion-

In this paper, an overview of different steganography techniques which includes spatial and frequency based steganographic applications are being presented. A brief description of types of steganography method that extends to spatial application methods such as LSB, PVD, OPA and edge based embedding methods as well asd frequency application methods such as DFT, DCT &DWT are provided. Then, the variability of steganography in multimedia content such as images, audios, videos & text depending on the field pf application is also explained. Finally, the important types of steganography and classification of information starting from the steganography to the present day has also been explained in the literature.

References

1- L.M. Marvel, C.G. Boncelet, and C.T. Retter , "Spread spectrum image steganography ," in IEEE Transactions on image processing, vol.8 , no. 8, pp.1075-1083, Aug1999

2- E.S M. El-Alfy and A. A. Al –Sadi. "High capacity images steganography based on overlapped pixel differences and modulus function" in Proc. Of International Conference on Networked Digital Technologies , Springer Berlin Heidelberg , vol. 294, 2012, pp.243-252.

3- M. Conway. "Code wars: steganography , signals intelligence, and terrorism" , Technology & Policy , Springer Netherlands, vol. 169 (2) , pp.45-62, 2003.

4- N.F. Johnson and S. Jajodia. "exploring steganography : seeing the unseen". Computer ,IEEE , vol.31(2), pp. 26-34, 1998.

5- Jin-Suk , K., Yonghee, Y, &Mee Young , S. (2007, 7-9 Nov.2007) Steganography using block- based adaptive threshold , Paper presented at the Computer and information sciences ,2007 iscis 2007 22nd international symposium on.

6- N.Singh , and V. K. Yadav, "Trends in digital Video Steganography: A Survey." International Journal of Computer applications, 169(7), 1-8, 2011.

7- N. Singh , “Survey paper on Steganography” International Referred Journal of Engineering and Science (RJES), 6(1) 68-71 , 2007
8- R. M. Kirandeep, “A comparative Analysis of Steganography techniques”. The International journal of engineering and sciences (IJES), 5(4), 67-70 , 2016
9- M. I.S. Reddy , M. P. Reddy, and K. S. Reddy, “different medias of steganography- An emerging field of network security” international journal of computer sciences and information technologies, (IJCSES), 4(6), 9-25, 2013
10- C.P Sumathi, T. Santanam, and G. Umamaheshwari, “A study of various steganographic techniques used for information hiding.” International Journal of computer Science & Engineering Survey (IJCSES), 4(6), 9-25, 2013
11- J. Surana, A. Sonsale, B. Joshi, S. Sharma and N. Choudhary, “Steganography techniques.” International Journal of Engineering Development and Research, IJEDR, 5(2), 989-992,2017.
12- V. Rabara, and A. Goswami,”A Survey of image based steganography.” Internatinal Journal of computer engineering and sciences (IJCES) 1(2), 1-4, 2015
13- M. Hussain “A survey of image steganograpgy techniques.” International Journal of advanced sciences and technology, 54(1), 113-124, 2013
14- B. Chandel, and S. Jain , “Video steganography: A Survey.”. IOSR Journal of computer engineering(IOSR-JCE),18(1), 11-17, 2016.
15- Rakhi and S. Gawande, “A review on steganography methods” International Journal of advanced research in electrical , electronics and instrumentation engineering, IJAREEJE, 2(10), 4635-4638, 2013
16- A. Koyun , and H. B. Macit,”generating a stego-audio data using LSB technique and robustness test” Journal of engineering sciences and design, 6(1), 87-92, 2018
17- H. Singh, P.K. Singh and K. Saroha, “A survey on text beads steganography” Proceedings of the 3rd national conference; INDIACom, 2009
18- H. C. Wu, N. I. Wu, C. S. Tsai, M. S. Hwang, “image steganographic scheme based on pixel –value differencing and LSB replacement mthods.” IEE Proc.-Vis. Image signal process,152(5), 611-615,2005
19- M. Kumar, and a. Rani, “A short survey on steganography.” International Journal of computer science and technology, IJCST, 4(1), 181-185, 2013
20- M. H. and m. Hussain,”A survey of image steganography techniques” International Journal of Advanced Science and technology , vol54, pp. 113-124,2013.
21- N. Hamid and R. B. Ahmad,”image steganography techniques: an overview” no. 6, pp, 168-187, 2012
22- J. Kour and D. Verma ,”steganography techniques: a review paper”, Int. J. Emerg. Res. Manag. & technology, vol.9359, no. 35, pp, 2278-9359, 2014.
23- A. Miller, “least significant bit embedding implementation and detection”, 2012 International Journal of computer science and engineering.
24- E.C. Vidyasagar M. Potdar, “Grey level modification steganography for secret communication” 2014 International Journal of information technology and sciences.
25- N. F. Johnson and S. Jajodia, “Exploring steganography: seeing the unseen”computer , vol. 31. No. 2 pp. 26-34. Feb 1998
26- P. Wu, Y. Yang, and X.Li, “image-into-image steganography using deep convolutional network” in Proc. Pacific Rim Conf. Multimedia. Cham, Switzerland:Springer 2018 pp. 792-802.
27- K.Yang,K.Chen ,W.Z hang and N. Yu,”Provable secure generative stegnography based on autoregressive model,”inProc.Int.workshopDigit.Watermarking.Cham,Switzerland:Springer,2018,pp.55-68
28- A. A. Chincolkar, and D. A. Urkude,” Design and implementation of image steganography”, Journal of signal and image processing 3(3), 111-113, 2012
29- M. Kumar and A. Rani, “A short survey on steganography”, International Journal of compuer science and technology, 4(1), 181-185, 2013
30- I.Goodfellow,J.Pouget-abadie,M.Mirza,B.XuD.Warde-Farley,S.Ozair,A.Courville and Y.Bengio”Generativeadversarialnets,”in Proc.Adv.NeuralInf.Process Syst.,2014,pp.2672-2680.