iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** VII **Month of publication:** July 2021

DOI: https://doi.org/10.22214/ijraset.2021.36667

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VII July 2021- Available at www.ijraset.com

A Survey of the Various Steganography Techniques Using Soft Computing Techniques

Er. Savita Devi[1], Sumit Chopra[2]
[1, 2]*KCCEIT Nawanshahr Punjab*

Abstract: Steganography is the method of storing information by hiding that information's existence. It can be used to carry out hidden exchanges and hence can enhance individual privacy. Steganography aims at communicating the secret data in an appropriate multimedia carrier. In this paper, the various techniques used to perform Steganography in a secure way are studied and reviewed. In this the various Artificial Intelligence techniques used for steganography are reviewed and analyzed.
Keywords: Image Steganography, Steganalysis, Statistical attacks, Pixel- Value Differencing, Stego Image

I. INTRODUCTION TO STEGANOGRAPHY

The word steganography is derived from the Greek words stegos meaning cover and grafia meaning writing [1] defining it as covered writing. Image steganography the information is hidden exclusively in images. Steganography is the art and science of secret communication. It is the practice of encoding/embedding secret information in a manner such that the existence of the information is invisible. The actual files can be referred to as cover text, the cover image, or cover audio message. After inserting the secret message it is referred to as stegomedium. A stego-key has been used for hiding encoding process to restrict detection or extraction of the embedded data [2].

Watermarking and fingerprinting related to steganography are basically used for intellectual property protection needed. A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as audio or image data. It is typically used to identify ownership of the copyright of such signal. The embedded information in a watermarked object is a signature refers the ownership of the data in order to ensure copyright protection. In fingerprinting, different and specific marks are embedded in the copies of the work that different customers get. In this case, that becomes easy for the property owner to find out such customers who give themselves the right to violate their licensing agreement when they illegally transmit the property to other groups [3].One method of common Steganography technique is to hide the secret message in the least significant bits of pixels of the cover image. The image quality of stego image achieved by applying the LSB technique is very closer to the original one. But the drawback is it cannot survive image processing manipulations. One method of LSB Steganography involves manipulating the LSB plane from direct replacement of the cover image with message bits to some type of logical or arithmetic combination between two. Several examples of LSB techniques are found. This technique achieves both high capacity and low perceptibility. But it is not very sophisticated and subject to extraction by unwanted persons. Masking and filtering techniques usually restricted to 24 bits or grayscale images. These methods are effectively similar to „paper watermarks", creating markings in an image. This can be achieved for example by modifying the luminance of parts of the image. While masking does change the visible properties of an image, it can be done in such a way that the human eye will not notice the anomalies. Least Significant Bit maintains a good visual quality of stego-image, it can hide little information. Considering the drawback of LSB, some methods begin to take account of the visual identity that human eyes are insensitive to edged and textured areas when embedding secret information, such as BPCS(biplane complexity segmentation),PVD(pixel value differencing), MBNS (multiple base notational system), SOC, Side Match and WCL. The capacity of embedded information is thereby greatly improved while the quality of visual imperceptibility is maintained. As human vision sensitivity is complex, it is hard to exactly decide whether a pixel is in less sensitivity areas or not. Thus, based on the contrast and texture sensitivity, we train self-organizing map Neural Networks (NNs) trained to distinguish pixels in less sensitive areas from pixels in more sensitive areas. So, NNs trained is the secret key. Then, we use NNs trained to classify pixels, and select pixels in less sensitive areas to embed more secret data. On the receiving side, the original image is not needed for extracting the embedded data. Neural approach adds the complexity for the hackers accessing and also presents high potentiality in defense operations. Neural Steganography is a powerful tool that enables people to communicate without possible eavesdroppers even knowing there is a form of communication. Basic elements of steganography in images are shown in Figure 1. The carrier image in steganography is called the "cover image" and the image which has the embedded data is called the "stego image". The embedding process is usually controlled using a secret key shared between the communicating parties.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VII July 2021- Available at www.ijraset.com

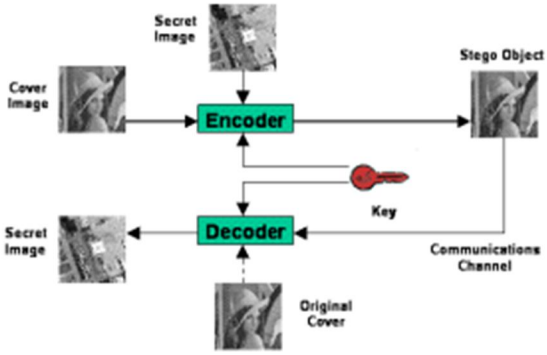


Fig. 1 Steganography System Elements

II. DIFFERENCE BETWEEN STEGANOGRAPHY AND CRYPTOGRAPHY

Steganography is an alternative to cryptography in which the secrete data is embedded into the carrier in such way that only carrier is visible which is sent from transmitter to receiver without scrambling. The combination of both cryptography and Steganography provide high level security to the secret information [6]. Cover image is called as carrier image and is the original image in which the secret data i.e., the payload has embedded. The unified image that is obtained after embedding the payload into the cover image is called the stego image. Steganography is the known as the technique of hiding the secret message within a carrier so that no one except the intended recipient is aware of its existence. The main difference between cryptography and steganography is that, it does not attract attackers to pay attention and the steganography is the best solution but cryptography is a part of a solution. These both are different techniques of hiding the message.

There are two other technologies that are very strongly related to steganography are known watermarking and fingerprinting. These technologies are mostly concerned with the safety of intellectual property; therefore the algorithms have different requirements than steganography. The requirements of a better steganographic algorithm are discussed below. Watermarking includes that all of the instances of an object are “marked” in the same way. The type of information hidden in objects when using watermarking is typically a signature to signify origin or ownership for the reason of copyright protection. While fingerprinting on the other hand includes different unique marks that are embedded in distinct copies of the carrier object that are distributed to a variety of clients [6]. This helps the academic property landlord to recognize the customers who break their licensing agreement by supplying the property to third parties. In case of watermarking and fingerprinting both, the fact includes that the information is hidden inside the files might be a public knowledge – at times it may even be visible – while in steganography the imperceptibility of the information is mainly important. The successful attack on a steganographic system consists of an adversary that observes that there is information hidden inside a file, but a successful attack on a watermarking or fingerprinting system will not be to detect the mark.

The advantage of steganography is that it can also be used to secretly pass on messages without the fact of the transmission being revealed .Frequently; using encryption might recognize the sender or receiver as somebody has a little to hide. Steganography is famous as secret writing and the idea of steganography hides the existence of a message. Cover carriers could be (video, text, audio, images, and some other digitally representative code) which will hold the hidden information. A message is the information which is being hidden and it be can be a cipher text, plain text, images, or anything that can be embedded into a bit stream. To hide the information a Stego-key is required which is additional secret information, such as password, that is required for embedding the information [7].

For example, when secret information is hidden within a cover image, the result obtained is a stego-image. The basic formula of the steganography process is represented as:

Stego –medium = cover medium + embedded message + stegokey.

III. DIFFERENT KINDS OF STEGANOGRAPHY

Several digital file formats can be used for steganography, but the most suitable formats are those that contain a high degree of redundancy. Redundancy is known as the bits of an object which provides accuracy much greater than necessary for the object’s use and display [8]. The redundant bits of an object include those bits which can be altered without any alteration being detected easily. Steganography is highly reliant on the type of media being used to hide the information.

Medium being usually used comprises of images, text and audio files, also the network protocols used in network transmissions. Image Steganography is commonly more preferred media because of its harmlessness and attraction. Furthermore exchange of greetings through digital means is on the increase throughout the increased use of the internet and ease of comfort and flexibility is sending them. The improvement in technology of design of the cameras and digital images being saved in cameras and then move to PCs has also enhanced many folds. The different kinds of file formats that can be used for steganography are Text, Image, Audio/Video, Protocol.

IV. IMAGE STEGANALYSIS

The main objective of Steganalysis is to break steganography and the detection of stego image. Steganalysis is the method of detecting hidden information inside of a file. Steganalysis is the method of identifying steganography by judging the various parameters of the stego media. Many algorithms of Steganalysis depend upon algorithms of steganography introducing statistical differences between cover and stego image. This technique depends upon unusual patterns in the media and Visual detection of the same. The main step of Steganalysis is to detect the main stego media concerned with detecting hidden information. It is very hard to detect the hidden content without having any knowledge of the tool that is used as well as of the stego key.

Apart from spatial domain as well as Transform domain, several kinds of Steganalysis tools are accessible in market similar to: Photo Title, Bench mark, Stir Mark and 2Mosaic etc. These Steganalysis tools are able to eliminate steganographic content from any image. Removal is obtained by destroying secret message via two techniques: – break apart and resample. Steg Detect, Steg Break, StegSpy discover information embedded via the following tools - Hiderman, Jsteg-shell, JPhide, and Seek, Camouflage , F5, JPHIde, JPegX and appendX. There is a scanner named Steganography Analyzer Real-Time and it is the best Steganalysis software at the moment that can analyze all network traffic to look for traces of steganographic communication. LINUX, WINDOWS are different platforms in which these tools are available [9].

V. NEED FOR STEGANALYSIS

Unfortunately with the good there comes a bad also. As Steganography is a technique that enable users to cover message from unintentional recipients, in the similar way it can also be used by criminals to hide message from authorized authorities. As of this cause the occurrence of the methods detecting Steganography is necessary. This technique is known as Steganalysis. Steganalysis is a mainly a new concept of research .Contrast to the goal of information hiding, Steganalysis is concerned with the discovering and rendering ineffective covert messages, therefore making information hiding failed. While Steganography deals with techniques for hiding information the goal of Steganalysis is to detect and estimate potentially hidden information from observed data with small or no knowledge regarding the steganography algorithm and its parameters. It is reasonable to say that Steganalysis is both an art and a science. The art of Steganalysis plays a vital role in the selection of features or characteristics a typical stego-message might exhibit while the science helps in reliably testing the selected features for the presence of hidden information. In general, extraction of the secret message generates a harder problem than mere detection.

VI. APPLICATIONS OF STEGANOGRAPHY

A. Secret Communications [10] the use steganography does not advertise secret communication and therefore avoids scrutiny of the sender side, message, and recipient. A secret, blueprint, or other sensitive information can be transmitted without alerting potential attackers.

B. Feature Tagging Elements can be embedded inside an image, as the names of individuals in a photo or locations in a map. Copy the stego-image also copies all of the embedded features and only parties who possess the decoding stego-key will be able to extract and view the features.

C. Copyright Protection Copy protection mechanisms that prevent data, generally digital data, from being copied.

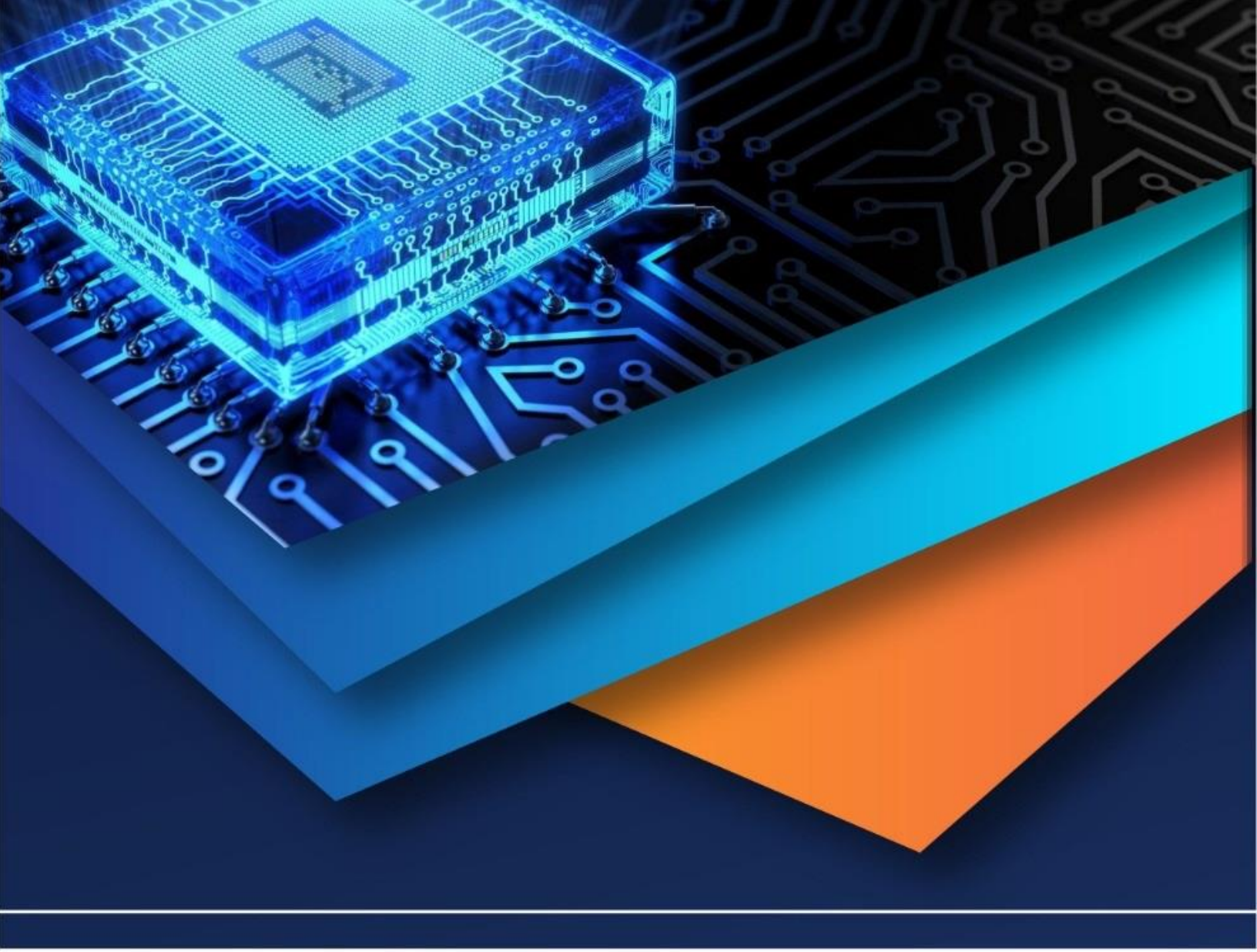
VII. CONCLUSION

Steganography is an elective way to hide sensitive information. In this paper we have reviewed the various Techniques on images to obtain secure stego-image insertion using the visual cryptography scheme for grayscale image in various platforms. The image resolution doesn't change much and is negligible when we embed the message into the image and the image is protected with the personal key. So, it is not possible to damage the data by unauthorized personnel. The algorithm is usage for both 8 bit and 24 bit image of the same size of cover and secret image. This paper focuses on the approach like increasing the security of the message and increasing PSNR and reducing the distortion rate.

Training data sets can be analyzed from the JPEG samples could be used for future research for benchmarking different methods of teaching artificial neural networks. Future analysis could be aimed on self-arranged network typology by methods of symbolic regression like Genetic Programming, Grammatical Evolution, Analytic Programming and others, i.e. superstructure of evolutionary optimization algorithms. The future work could be towards the enhancing visual cryptography scheme for grayscale image in various platforms.

REFERENCES

[1] Soni, A.; Jain, J.; Roshan, R., "Image steganography using discrete fractional Fourier transform," Intelligent Systems and Signal Processing (ISSP), 2013 International Conference on , vol., no., pp.97,100, 1-2 March 2013.
[2] Akhtar, N.; Johri, P.; Khan, S., "Enhancing the Security and Quality of LSB Based Image Steganography," Computational Intelligence and Communication Networks (CICN), 2013 5th International Conference on , vol., no., pp.385,390, 27-29 Sept. 2013.
[3] Reddy, H.S.M.; Sathisha, N.; Kumari, A.; Raja, K.B., "Secure steganography using hybrid domain technique," Computing Communication & Networking Technologies (ICCCNT), 2012 Third International Conference on , vol., no., pp.1,11, 26-28 July 2012.
[4] Weiqi Luo, Fangjun Huang, and Jiwu Huang, Edge adaptive image steganography based on LSB matching revisited, in IEEE Transactions on Information Forensics and Security, vol.5, no.2, June 2010.
[5] Lin Zhang, Jianhua Wu, Nanrun Zhou, "Image Encryption with Discrete Fractional Cosine Transform and Chaos", Fifth International Conference on Information Assurance and Security 2009 IAS '09, pp 61 – 64, 2009.
[6] El-Alfy, M. E., "Detecting pixel-value differencing steganography using Levenberg-Marquardt neural network", IEEE, Computational Intelligence and Data Mining (CIDM), pp. 160-165, 2013.
[7] Mahajan, S. and Singh, A., "A Review of Methods and Approach for Secure Steganography", International Journal of Advanced Research in Computer Science and Software Engineering, vol.2, issue 10, pp.67-70, 2012.
[8] Antony, J., "Audio Steganography in Wavelet Domain- A survey", IJCA, vol. 52, no. 13, pp. 33-37, 2012.
[9] Kaur, M. and Kaur, G., "Review of Various Steganalysis Techniques", IJCSIT, vol. 5(2), pp. 1744-1747, 2014.
[10] Phadke, A. and Mayekar, A., "Steganography Technique using Neural Network", International Journal of Computer Applications", Vol. 82, no. 7, pp. 39-42, 2013.
[11] M.P. Priyanka, E. Lakshmi Prasad and A. R. Reddy, "FPGA implementation of image encryption and decryption using AES 128-bit core", In proceeding of IEEE explore, 2017.
[12] Venkata Krishna, Pavan Kalubandi, Hemanth Vaddi, Vishnu Ramineni and Agilandeeswari Loganathan, "A novel image encryption algorithm using AES and visual cryptography", Next Generation Computing Technologies (NGCT) 2016 2nd International Conference of IEEE, 2017.
[13] Priya Deshmukh, "An image encryption and decryption using AES algorithm", International Journal of Scientific & Engineering Research, vol. 7, no. 2, February 2016.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY