Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 11, November-2019

# Information Security Through Image Processing by Utilizing Steganography

Gaurav Gupta
of (SPPU) Computer Engineering,
Dr. D.Y.Patil Institute of Engineering, Management & Research, Akurdi,
Pune, India

Shruti Patil
of (SPPU) Computer Engineering,
Dr. D.Y.Patil Institute of Engineering, Management & Research, Akurdi,
Pune, India

Piyush Varma
of (SPPU) Computer Engineering,
Dr. D.Y.Patil Institute of Engineering, Management & Research, Akurdi,
Pune, India

Ankita Raikwade
of (SPPU) Computer Engineering,
Dr. D.Y.Patil Institute of Engineering, Management & Research, Akurdi, Pune, India

Yogita Sawant
of (SPPU) Computer Engineering,
Dr. D.Y.Patil Institute of Engineering, Management & Research, Akurdi, Pune, India

***Abstract:*-Steganography is the advanced methodology for concealing secret data than the other strategies used to date. There are often cases when it is not possible to send messages openly or in encrypted form. This is where steganography play its role. While cryptography provides privacy which is intended to provide secrecy. Steganography aims to hide the secret messages and also for communication and transferring of data. So nobody aside from the licensed sender and receiver are tuned in to the existence of the key information. This paper intends to give an overview of image steganography and its uses and hiding the files (text file, audio file, video file, image file, etc.,) by using LSB and AES algorithm where AES is used for password protecting system so that if anyone can find the Stego-image they will not read the message because data is still in the encrypted form and LSB is used for hiding the data.**

***Keywords: Steganography, Cryptography, Stego image, Least Significant Bit (LSB), Advanced Encryption Standard (AES).***

## I. INTRODUCTION:

The communication is the basic necessity of each growing space in today's world. Everyone wants the secrecy and safety of their communicating data. In our daily life, we use many secure pathways like the internet or telephone for transferring and sharing information, but it's not safe at a certain level. To share the information in a concealed manner two techniques could be used. These mechanisms are cryptography and steganography. In cryptography, the message is changed in associated encrypted kind with the assistance of coding key which is known to sender and receiver only. The message cannot be accessed by anyone while not victimization the encoding key.

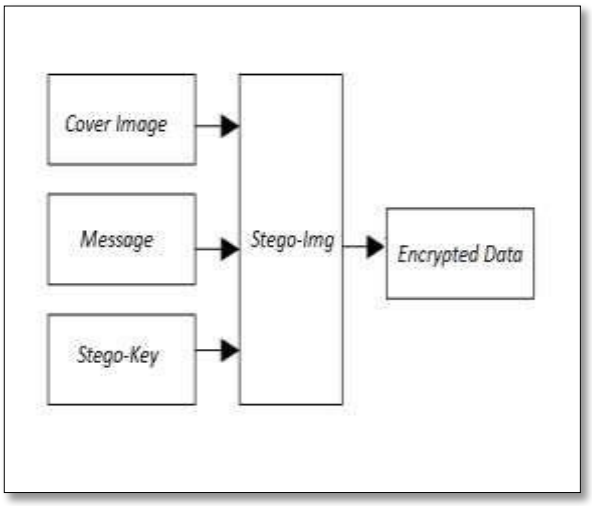
However, the transmission of encrypted messages might simply arouse the attacker's suspicion, and the encrypted message might be so intercepted, attacked or decrypted violently. To overcome the shortcomings of science techniques, steganography techniques have been developed. Steganography is the science of communicating in such a way that it hides the existence of the communication. Thus, steganography hides the existence of information so that nobody will find its presence. In steganography, the process of hiding information contained within any multimedia system content like text, image, audio, video is referred to as —"Embedding". For increasing the confidentiality of human activity information, each the techniques could also be combined.

Methods of concealing and transmission hidden info square measure typically glorious for a protracted time, around the millennium. However, the expansion of steganography as a scientific discipline emerged in recent years with the emergence of digital technologies. Steganography looks kind of like cryptography, however, there exists a basic distinction between these scientific disciplines. While cryptography resolves the safety of the content, steganography deals with the secrecy of the existence of the message herself. The suitable combination of the applying of steganography and cryptography will guarantee a high degree of confidentiality and undetectability of secret information.

## II. WHAT IS STEGANOGRAPHY?

Steganography is that the technique of concealment secret information inside a standard, non-secret, file or message to avoid detection; the key information is then extracted at its destination. The use of steganography is combined with encoding as an additional step for concealment or protective information.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 11, November-2019




The word steganography springs from the Greek words Stego (meaning hidden or covered) and therefore the Greek root graph (meaning to write). Steganography is accustomed to conceal virtually any variety of digital content, as well as text, image, video or audio content; the information to be hidden is hidden within virtually any other type of digital content. The content to be hidden through steganography -- known as hidden text -- is usually encrypted before being incorporated into the innocuous-seeming cowl computer file or information stream.

## III. TYPES OF STEGANOGRAPHY:

### *A. Text Steganography:*

The techniques in the text steganography area unit include a variety of tabs, white spaces and capital letters, rather like code is employed to realize data concealment.

### *B. Image Steganography:*

Taking the quilt object as the image in steganography is termed image steganography. In this technique pel intensities square measure accustomed hide the information. The 8 bit and 24-bit images are common. The image size is large then hides more information. Larger pictures could need compression to avoid detection and therefore the Techniques area unit LSB insertion and Masking and filtering.

### *C. Audio Steganography:*

Taking audio as carrier for data concealment is termed audio steganography. It is a very important medium due to voice over IP (VOIP) popularity. It is used for digital audio formats like WAVE, MIDI, and AVI MPEG for steganography. The methods are LSB writing, echo hiding, parity coding, etc.

### *D. Video Steganography:*

It is a method to cover any quite files or knowledge into digital video format. Video i.e. the combination of images is employed as a carrier for hidden data. The discrete cosine transform i.e. DCT amendment the values. It is used such as H.264, Mp4, MPEG, AVI or other video formats.

## IV. LITERATURE REVIEW:

In [1] authors have planned associate degree adaptive least important bit abstraction domain embedding technique. This technique divides the image pixels ranges (0-255) and generates a Stego-key. This nonpublic Stego-key has five different grey levels varies of image and every range indicates to substitute mounted range of bits to introduce in least important bits of image. The strength of the planned technique is its integrity of secret hidden info in Stego-image and high hidden capability. The limitation is to cover further bits of signature with hidden messages for its integrity purpose. It additionally planned a technique for color image simply to switch the blue channel with this theme for info concealment. This technique is targeted to realize the high hidden capability and security of the hidden message. Yang et al., in [2] planned associate degree adaptive LSB substitution based mostly knowledge concealment technique for image. To achieve higher visual quality of Stegoimage it takes care of noise-sensitive space for embedding. The proposed technique differentiates and takes advantage of traditional texture and edges space for embedding. This technique analyzes the perimeters, brightness and texture masking of the quilt image to calculate the quantity of k-bit LSB for secret knowledge embedding. The price of k is high at non-sensitive image region and over-sensitive image space k value stays tiny to balance the overall visual quality of an image. It additionally utilizes the pel adjustment technique for higher Stego-image visual quality through the LSB substitution technique. The overall result shows an honest high hidden capability, however, the dataset for experimental results are limited; there's not one image that has several edges with noise region.

In [3] anthers have proposed LSB based image hiding method. Common pattern bits (Stego-key) are accustomed to hide knowledge. The LSB's of the pel are changed counting on the (Stego-key) pattern bits and also the secret message bits. Pattern bits are a combination of M x N size rows and columns (of a block) and with random key value. In embedding procedure, each pattern bit is matched with message bit, if satisfied it modifies the 2nd LSB bits of cover image otherwise remains the same. This technique targets to realize the security of hidden messages in Stego-image employing a common pattern key. This planned technique has low hidden capability as a result of a single secret bit needs a block of (M x N) pixels.

In [4] author projected a component worth distinction (PVD) and straightforward least vital bits theme are accustomed bring home the bacon accommodative least vital bits knowledge embedding. In component worth differencing (PVD) wherever the dimensions of the hidden knowledge bits are calculable by the distinction between the

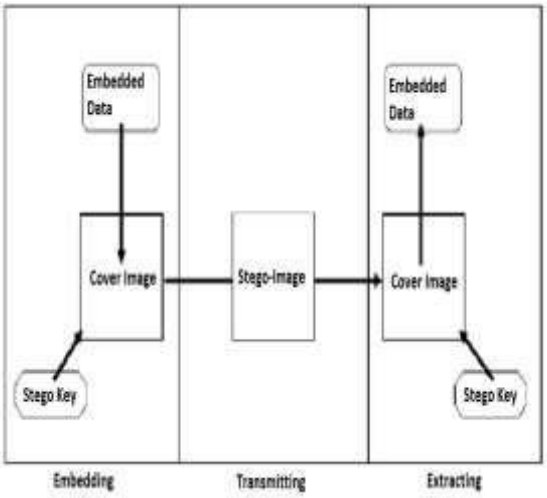
International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 11, November-2019

2 consecutive pixels in cowl image exploitation easy relationship between two pixels. PVD technique typically provides a decent physical property by calculative the distinction of 2 consecutive pixels that verify the depth of the embedded bits. The proposed technique hides giant and accommodative k-LSB substitution at edge space of image and PVD for swish region of image. So during this approach, the technique gives each larger capability and high visual quality consistent with experimental results. This technique is complicated thanks to accommodative k generation for substitution of LSB.

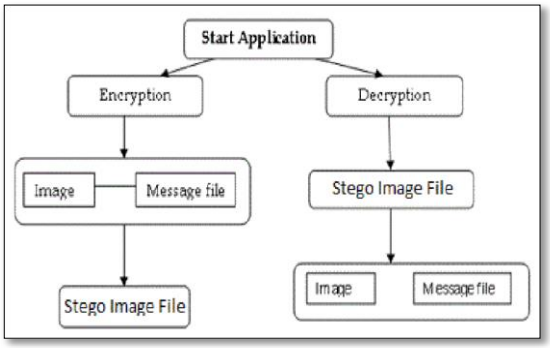
In [5] authors projected a way of Multi-Pixel Differencing (MPD) that used quite 2 components to estimate the smoothness of every component for knowledge embedding and it calculates the total of difference value of four pixels block. For small distinction worth it uses the LSB otherwise for top distinction worth it uses the MPD technique for knowledge embedding. Strength is its simplicity of algorithmic rule however experimental dataset is simply too restricted.

## V. PROPOSED METHODOLOGY:

### *A. BLOCKED DIAGRAM:*




### *B. ALGORITHMS USED IN STEGANOGRAPHY:*



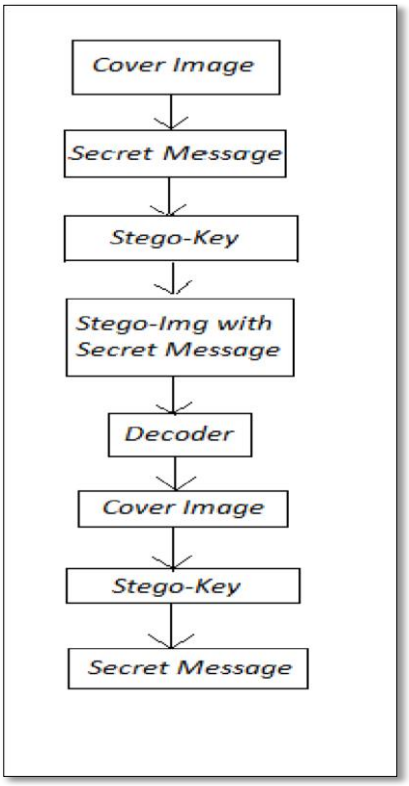

LSB:

The least significant bit (LSB) algorithm used in this paper is a spatial domain steganography in the substitution method, the principle is to exchange data within the least bit of cover image with confidential information. For a 256 grayscale cover image, the grayscale value of each element will be wont to represent an 8-bit binary, taken out a certain bit of all pixels constitute a certain bit plane, for example, the least significant bit of all the pixels constituting the least significant bit plane. The higher the bit plane, the greater the contribution of the gray value, and the lowest bit plane is similar to random noise.

AES:

AES was introduced to replace DES in commercial applications. Advanced Encryption Standard was announced by the National Institute of Standards and Technology (NIST) on November 26, 2001. AES is a symmetric-key algorithm which means that very same secret's used for each coding and encryption of data. AES is additionally referred to as RIJNDAEL that was named when the name of its inventors John Daemen and Vincent Rijmen. AES is the block cipher that uses block sizes of 128, 168, 192, 224 and 256 bits. The key sizes employed in AES are 128,192 and 256 bits. AES and DES are different from each other with some differences. DES uses a Feistel structure during which the block is split into two halves before it goes through the steps of encryption whereas, in DES, every spherical comprises a series of functions which are byte substitution, permutation, arithmetic operator over a finite field and X-OR operation with key. AES is faster than 3DES and DES.

### *C. FLOWCHART:*



International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 11, November-2019

## VI. STEGANOGRAPHY PROS:

*A. Unidirectional Hashing:*

To make sure that a 3rd party has not tampered with a sent message. This is accomplished by making a hash of the message employing a fastened character length for each item within the message, once the first things area unit in truth of variable character length. The hash is encrypted and then sent with the message. Once the recipient receives the message it's decoded. If the hash from the decoded message doesn't match the hash from the encrypted message, each the sender and recipient of the message know that it's been tampered with.

*B. Attaching Text to associate Image:*

Informative notes area unit connected to a picture. Within the health profession, this could be used once one medical workplace sends a picture to a different medical workplace. If the causing medical office has to embody informative notes of what the receiving medical workplace ought to be that specialize in, this could be accomplished with steganography. *C. Concealment Information:*

Steganography can even be wont to shield identities and valuable information from felony, unauthorized viewing, or potential sabotage by concealing the message among a trusting image.

## VII. STEGANOGRAPHY CONS:

Unfortunately most uses of steganography and analysis round the topic of steganography center around illegitimate purposes. The three biggest areas of illegitimate steganography revolve around terrorism, pornography, and data theft.

During the research, the illegitimate uses of steganography were found to get on a world scale, involved national security or were done on an academic basis to better understand the potential danger of steganography if created by people with illintentions.

## VIII. APPLICATIONS:

Steganography applies to, however not restricted to, the subsequent areas.

1) Confidential communication and secret data storing
2) Protection of data alteration
3) Access control system used for digital content distribution
4) Media Database systems

## IX. RESULT ANALYSIS:

The scope of the project is to limit unauthorized access and supply higher security throughout message transmission. To meet the requirements, we used the simple and basic approach of steganography. In this project, the planned approach finds the acceptable formula for embedding the info in a picture exploitation steganography that provides the higher security pattern for causation messages through a network. Steganography does not entirely pertain to digital photos but in addition to different media (files like voice, different text and binaries; different media like communication channels, the list can prolong and on).

## X. CONCLUSION:

Steganography is that the art and science of writing hidden message that no-one excluding the sender and receiver, suspect the existence of the message. Steganography relies on secret writing. To provide high security Steganography and cryptography area unit combined on. This technique encrypts secret information before embedding it inside the image. Steganography is not imagined to exchange cryptography but supplement it. Concealment a message with steganography ways in which reduces the chance of a message being detected. However, if that message is in addition encrypted, if discovered, it ought to even be cracked. There are a unit Associate in nursing infinite form of steganography applications.

## XI. ACKNOWLEDGMENTS:

We are grateful to our Department of Computer Science & Technology for their support and for providing us an opportunity to review such an interesting topic. While reading and searching concerning this subject we tend to learn concerning varied vital and interesting facts.

## REFERENCES:

[1] Y. K. Jain and R. R. Ahirwal, "A Novel Image Steganography methodology With adaptational variety of Least vital Bits Modification supported non-public Stego-Keys", International Journal of engineering science and Security (IJCSS), vol. 4, (2006) March 1.

[2] H. Yang, X. Sun and G.Sun, "A High-Capacity Image information concealing theme practice adaptative LSB Substitution", Journal: Radioengineering, vol.18, no. 4, (2009), pp. 509-516. [3] S. Channalli and A. Jadhav, "Steganography an Art of Hiding Data", International Journal on Computer Science and Engineering, IJCSE, vol. 1, no. 3, (2009).

[4] C.-H. Yang, C.-Y. Weng, S.-J. Wang, Member, IEEE, and H.-M. Sun, "Adaptive Data Hiding in Edge Areas of Images with Spatial LSB Domain Systems", IEEE Transactions on Information Forensics and Security, vol. 3, no. (2008) September 3, pp. 488-497.

[5] K.-H. Jung, K.-J. Ha and K.-Y. Yoo, "Image data hiding method based on multi-pixel differencing and LSB substitution methods", Proc. 2008 International Conference on Convergence and Hybrid Information Technology (ICHIT '08), Daejeon (Korea), (2008) August 28-30, pp. 355-358.

[6] R. Krakovský, R. Forgáč, I. Mokriš, "Influence of cluster center selection on clustering by hybrid neural network model", Proceedings of LINDI'2012 - 4th IEEE International Symposium on Logistics and Industrial Informatics, 2012, pp. 233 – 238

[7] M. Borda, Fundamentals in Information Theory and Coding. Springer, 2011.

[8] R. Krakovský, R. Forgáč, "Neural Network Approach to Multidimensional Data Classification via Clustering," Proceedings of SISY'2011 - 9th IEEE International Symposium on Intelligent Systems and Informatics, 2017, pp. 169-174. [9] R. Forgáč, I. Mokriš, "Feature Generation Improving by Optimized PCNN", Proceedings of SAMI'2008 - 6th International Symposium on Applied Machine Intelligence and Informatics, 2018, pp. 203-207.

[10] R. Forgáč, I. Mokriš, "Threshold Potential Optimization in the Pulse Coupled Neural Network", Proceedings of SISY'2008 - 6th International Symposium on Intelligent Systems and Informatics, 2008.

[11] USC-SIPI image database, Signal and Processing Institute, University of Southern California, http://sipi.usc.edu/database/