WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

IMAGE STEGANOGRAPHY USING LSB TECHNIQUE

Noor Mohammad[1], Raj Kumar[2], Sai Reddy[3], Brijesh Kumar Singh[4]

[1,2,3,4] Department of Electronics and Communication Engineering Madanapalle Institute of Technology and Sciences, Madanapalle (A.P.)

ABSTRACT

The word steganography means" covered in hidden writing".The object of steganography is to send a message through some innocuous carrier (to a receiver while preventing anyone else from knowing that a message is being sent to all. Computer based steganography allows changesto bemade to what are known as digital carriers such as images or sounds. The changes represent the hidden message but result if successful in no discernible change to the carrier. In steganography information can be hidden in carriers such as images, audio files, text files, and video and data transmissions.When message is hidden in the carrier a steno carrier is formed for example a stenoimage. The are used for steganography in the following way. The message may firstly be encrypted. The sender embedsthe secretmessage to be sent into a graphic file. This results in the production of what is called stego-image. Additional secret data may be needed in the hiding process e.g., a stegokey etc. This stegoimage is then transmitted to the recipient.

Keywords *- PSNR-Peak Signal To Noise Ratio. , LSB-Least Significant Bit., MSE-Mean Square Error., NCC-Normalized-Correlation Coefficient.*

1. INTRODUCTION

Digital image processing is the use of a digital computer to process digitalprocessing.Since images are defined over two dimensions (perhaps more) digital image processing may be modeled in the form of multidimensional systems.[1]

The science of steganography is the art of concealing information in data. Normally, steganography is done in such a way that anadversary would have a hard time detectingthe presence of a hidden message in otherwise benign data. The message is embedded in a piece of data that is visible to the rest of the world and looks to be harmless and normal. This is in sharp contrast to cryptography, in which the communication is scrambled to make deciphering it extremely difficult orimpossible. A ciphertext message elicits suspicion, whereas an invisible message hidden in clear text does not. This is one ofthe benefits of Steganography.[2]Steganography simply exploits human perception; human senses are not trained tohunt for files that contain information, despite the fact that software exists that canperform steganography. The most typical application of steganography is the concealment of a file within another file.Using the proposed method and an embedding intensity factor of 15, themessage picture is put on all cover images.Then, using Mean Square Error (MSE) andPeak Signal to Noise Ratio, assess the quality of the stego picture outputs (PSNR).The MSE between the cover image and thestego image is the mean error valuesquared. The lower the MSE value in the image, the higher the stego image quality.

Eq. 1 can be used to calculate the MSE value.

$$\mathbf{MSE} = \frac{1}{mn}\sum_{t=0}^{m-1}\sum_{j-0}^{n-1}(\boldsymbol{I}(\boldsymbol{i},\boldsymbol{j}) - \boldsymbol{K}(\boldsymbol{i},\boldsymbol{j}))\mathbf{2} \rightarrow [\mathbf{1}]$$

Where;m =number of image rows n=number of image columns i (i, j) =pixel value of cover image k (i, j) =pixel value ofstego image. While the NormalizedCorrelation Coefficient can be used to assess the robustness of extraction results (NCC). If the NCC value is near to 1, the likeness to the original message image is also close.PSNR is an image quality metricthat is used to compare the quality of the cover image before and after the message isplaced. To determine the PSNR, the value of must first be obtained.MSE. The higher the PSNR number, the better the stego image quality and the

$$\mathbf{PSNR}=\mathbf{10.log10}\left(\frac{\mathbf{IMAX}}{\mathbf{MSE}}\right) \rightarrow [\mathbf{2}]$$

more resembling thecover image The PSNR value can be calculated using Where: PSNR=value of PSNR image (in

dB) IMAX =the maximum value of pixels While the Normalized Correlation Coefficient can be used to assess the robustness of extraction results (NCC). If the NCC value is near to 1, the likeness to the original message image is also close. The formula for computing the value of is Eq. 6. This is a fascinating and essential meeting, as it is the first of its type. I applaud those who came up with the idea. Itcould go down in cryptology history as a watershed moment. One pixel byte is enough to hold one message byte. The rest of the bits in the pixels are unchanged. The art and science of steganography is the art and science of communicating in a non- obtrusive manner. Which conceals the communication's existence The use of steganography is crucial.In the field of information security It is the technique of concealing communication in order to communicate invisibly.

Information included within other information Steganography is a term originating from Greek. It directly translates to "covered writing"[3]. Three components make up a Steganography system. The cover image, the secret message, and the steganoimage are the three elements. A digital image is a picture that has been captured on a computer.

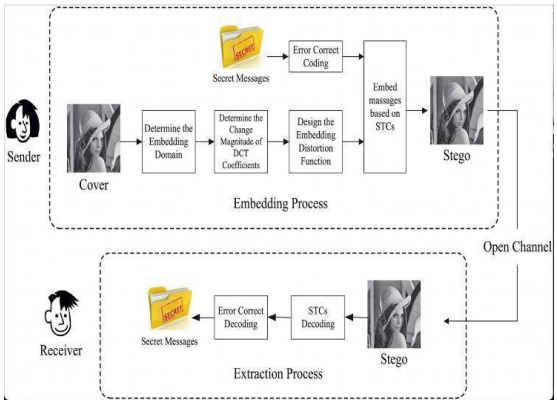


Fig: 1- (Embedded Process and Extraction Process)

Functional Requirements: Functional requirements are the requirements that defines specific behaviour or function of the system.If the username and password are correct, the login function will authenticate the sender. Otherwise, the system will be exited.File for Secret Text Messages: In this file, you must write a secret message to someone.You can either hide or pick any secret message text file.Cover Image: This is the image that will be used to hide the hidden text message.Stego Encryption.[4] An LSB implementation is used to disguise the cover picture.By swapping sections of the cover image with bits of the message, you can create a secret text message. Sender: The sender is the one who sends this stego picture file to the intended recipient.He expresses a desire to communicate. Receiver: This receiver receives the stego image and uses the decryption option to extract the hidden text message contained inside it. Non- Functional Requirements: Safety Requirements: Only the sender and receiver should use the same software to encrypt and decrypt data inside the image. Eavesdropping should be avoided by both parties. Security Requirements: We plan to create software that embeds secret text data in images. The encrypted file should only be known by the sender and receiver. The message regarding the sent image as well as the received information should not be unfolded by the user.Software Quality Attributes: Software quality is maintained to the point where only the sender and receiver can interact via picture. There's no way to know what the secret image is. Software Requirement MATLAB[5].

2. MATLAB IMPLEMENTATION

Steganography in Image: Nowadays, hiding information within an image is apopular approach. An photograph with a hidden message can quickly travel through the Internet or through newsgroups.Niles Provos, a German steganographic expert, investigated the usage of Steganography in newsgroups and developed a scanning cluster that detects the presence of hidden messages inside images that have been posted on the internet.[6] VHowever, after examining one million photos, no concealed messages were discovered, suggesting that steganography's practicalapplication is still limited. ImageSteganography is a technique for hidingdata within a picture in a way that preventsthe hidden message or data from being detected by an unwanted user.The least significant bit (LSB), masking, filtering,and modifications on the cover.[7]

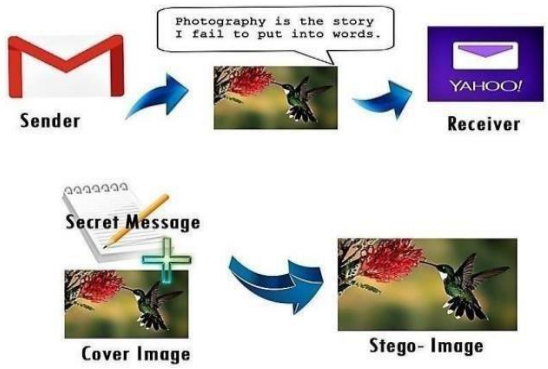


Fig:2-(Communication through Steganography)

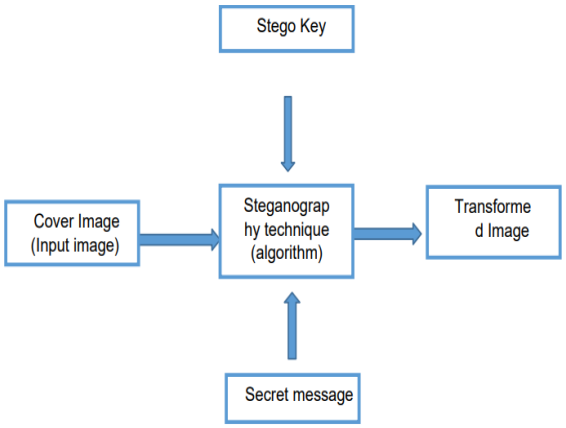


Fig:3-(encoding Process of Image Steganography)

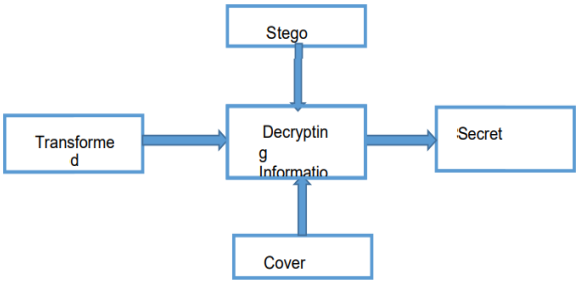


Fig:4-(Decoding Process of Image Steganography)

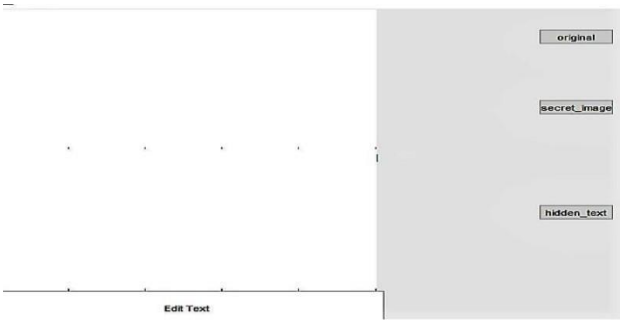


Fig:5-(Graphical user Interface)

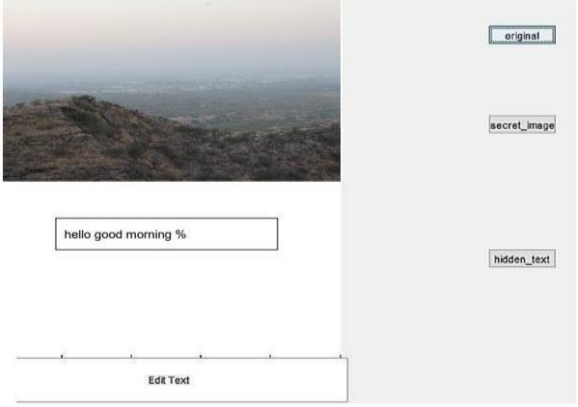
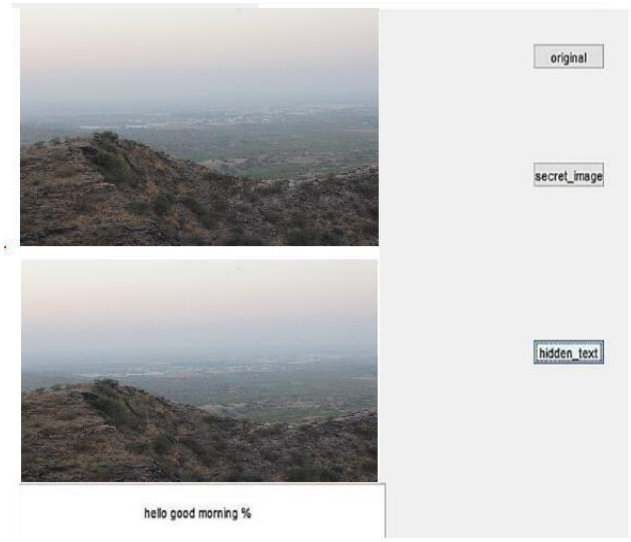


Fig:6-(Selecting Original Image)

Encoding process: Decoding process:Graphical User Interface Selecting OriginalImage. Encoded Image Decoded Message PSNR The hidden image is embedded on a carrier image, also known as a cover image, via image steganography. After that, the Steg analyzer examines the cover image formicro alterations and distortions in order to deduce the concealed messages. The stego picture and cover image are compared using metrics PSNR, MSE, Normalized Cross-Correlation (NCC), A Difference in order to measure the efficacy of thesteganography algorithm. The following are the definitions



for the performance parameters listed aboveA Signal-toNoise

Fig:7-(Encoded image)

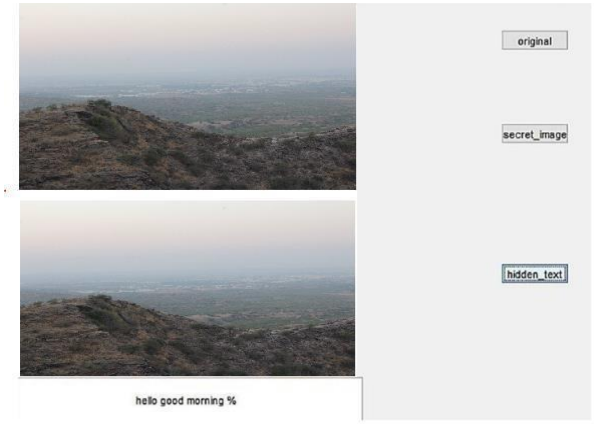


Fig:8-(Decoded image)

signal-to- noise ratio (PSNR).The lower thePSNR rate, the worse the image qualityafter embedding the hidden image; the higher the PSNR, the better the reconstructed image quality.The PSNR is calculated using the formula below.

$$\mathbf{PSNR=10.log10(\frac{IMAX^2}{MSE})} \rightarrow [3]$$

Where:PSNR =value of PSNR image (in dB) IMAX the maximum value of pixels The PSNR is estimated using the MeanSquared Error (MSE) method (MSE). MAXI is the highest pixel value that exists. If an 8-bit value is used to define pixels, theresult is 255. The MSE is the total of the differences between the embedded and cover images. Normalized Cross- Correlation (Normalized Cross- Correlation) (Normalized Cross-Core (NCC)To determine the relevance of a structure or object in a picture, the Normalized cross correlation is utilized. It is calculated using the formula

$$\mathbf{NCC=\frac{\nabla_{j=1}^{m}\sum_{k=1}^{n}(I(x,y)-I(x,\acute{y}))2}{\nabla_{i=1}^{M}\nabla_{k=1}^{n}(I(x,y))2}} \rightarrow |4|$$

Mean Squared Ratio Bean Squared Ratio Mean Squared (MSE)The MSE is the squared error between the stego and thecover picture that has been incrementally increased over time.[8] The MSE (Mean Squared Error) is determined using the formula below.

$$\mathbf{MSE}=\frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}(\boldsymbol{I}(\boldsymbol{i},\boldsymbol{j})-\boldsymbol{K}(\boldsymbol{i},\boldsymbol{j}))\mathbf{2}\rightarrow[\mathbf{5}]$$

The original image is I(i, j), while the stegoimage is K(i,j). The dimensions of the images are denoted by the letters m and n. The lower the MSE, the better the reconstructed image quality.D. Average Distinction (AD)The average difference is the difference between the two selected pixel values of the cover and stego image. The lower the average difference, the betterthe algorithm's capacity to resist noise. It iscalculated using the formula below.Table 1shows the performance parameters that have been implemented and the results thathave been collected.[9]

3. CONCLUSION

Steganography, on the other hand, is a relatively recent concept. There are ongoing improvements in the computer world, implying that steganography will advance as well. Steganalysis techniques are projected to become more efficient and sophisticated soon. Improved sensitivity to little signals is a promising benefit. Imagine how difficult it is to identify even one or two words contained in a picture, given how difficult it is to detect the presence of significant text within an image! The technology of steganalysis is expected to develop in the future, making it much simpler to discover even little signals inside a picture. Only a small portion of the science of steganography is covered in this publication. There is still a lot of study and development to be done as a new discipline. Steganography isn't simply for military or espionage purposes, as seen by the current growth of research in watermarking to protect intellectual property. Steganography, like cryptography, will play a bigger role in secure communication in the "digital world" in the future.

REFERENCES

[1] Rafael C. Gonzalez and Richard E.Woods, 2002 ‘Digital image processing’, Second Edition.

[2] Domenico Bloisi and Luca Iocchi, IEEE Conference Publication Steganography and categorization of picture steganography techniques.

[3] Monica Adriana, Emil Ioan Slusanschi, and Razvan Dobre are Dagadita, Monica Adriana, Emil Ioan Slusanschi, and Razvan Dobre. "Steganography is used to hide data." 159-166 in IEEE 12th international conference on parallel and distributed computing. 2013 (IEEE).

[4] http://www.ijetajournal.org/volume2/issue-5

[5] https://www.researchgate.net/publication/3 14116270 image steganography

[6] S. A. El Rahman, "algorithm and steganography tool to hide nuclear reactors," Comput. Electr. Eng., vol. 0, pp. 1–20, 2016.

[7] S. O. Akinola and A. A. Olatidoye, "On the Image Quality and Encoding Times of LSB, MSB, and Combined LSB-MSB Steganography Algorithms Using Digital Images," International Journal of Computer Science and Information Technology, vol. 7, no. 4, pp. 79–91, 2015.

[8] G. T. Shrivakshan and C. Chandrasekar, "A Comparison of Different Edge Detection Techniques in Image Processing," International Journal of Computer Science Issues, vol. 9, no. 5, pp. 269–276, 2012.

[9] C. H. Shreya Gupta and Akshay Kalra, "A Hybrid Technique for Spatial Image Steganography," 3rd International Conference on Computing Sustain Global Development, pp. 643– 647, 2016.