iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** V **Month of publication:** May 2018

DOI: http://doi.org/10.22214/ijraset.2018.5372

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: 6.887
Volume 6 Issue V, May 2018- Available at www.ijraset.com

Digital Image Steganography based on Combining Approach of LSB and DWT for Image Security

Shweta Agrawal[1] Dr. Neha Singh[2]
[1]*Department of Computer Science & Engineering Acropolis Institute of Technology & Research Bhopal Sikandarabad, Bhopal (M.P.), India*
Department of Computer Science & Engineering Acropolis Institute of Technology & Research Bhopal Sikandarabad, Bhopal (M.P.), India

***Abstract:** In this paper, two techniques of image steganography are hybrid in order to achieve secure transmission between sender and receiver. First is 2-bit LSB Technique and another is Discrete Wavelet Transform (DWT) Technique. In this proposed method the secret image is divided into two parts: upper half (UH) and lower half (LH).The LSB algorithm is implemented in spatial domain in which upper half of secret image is embedded into the least significant bits of cover image to derive the UH stego-image. Whereas DWT algorithm is implemented in transform domain in which the lower half secret image is embedded into the wavelet coefficient of the cover image to derive another LH stego image. Both the stego images are decomposed with wavelet transform to get final stego image. Finally an Inverse DWT (IDWT) is performed to get the stego image reconstruction. This is a unique attempt to simplify the embedding procedure and to reduce the effort of concealing the secret image in the cover image and offer better results. Finally, we have evaluated the performance of the proposed technique using Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) performance measure. The experimental result are compared with other method and found to be satisfactory.*
***Keywords:** Steganography, Embedding, Conceal, Information Hiding, DWT, LSB.*

I. INTRODUCTION

Now days, the communication is the basic necessity of each developing zone. Everybody wants the secrecy and safety of their communicating information. In our everyday life, we use numerous secure pathways like web or phone for transferring and sharing information, yet it's not safe at a specific level. With a specific end goal to share the information in a hid way two techniques could be used. These mechanisms are cryptography and steganography. In cryptography, the message is altered in an encrypted form with the assistance of encryption key which is known to sender and receiver as it were. The message can't be accessed by anybody without using the encryption key. Regardless, the transmission of encrypted message may effectively excite attacker's Suspicion and the encoded message may therefore be captured, attacked
or decoded brutally. To beat the weaknesses of cryptographic strategies steganography systems have been made. Steganography is the craftsmanship and science of communicating in such a way that it hides the existence of the correspondence. Thus, steganography hides the existence of information so that nobody can recognize its presence. In steganography the process of concealing information content inside any interactive media content like image, sound, video is referred as a ―Embedding. Steganography is the act of hiding a record, message, image, or video inside another file, message, image, or video. The word steganography combines the Greek words steganos, signifying "covered, concealed, or ensured", and graphein signifying "writing".

II. IMAGE STEGANOGRAPHY

Image steganography concerns with hiding secret information in digital images. There exists a large variety of image steganography techniques. Some of these techniques are more complex than the others, and all of them have respective strong and weak points. Image steganography techniques can be classified into spatial domain (image domain) steganography, transform domain (frequency domain) steganography, spread spectrum steganography and mode based steganography.

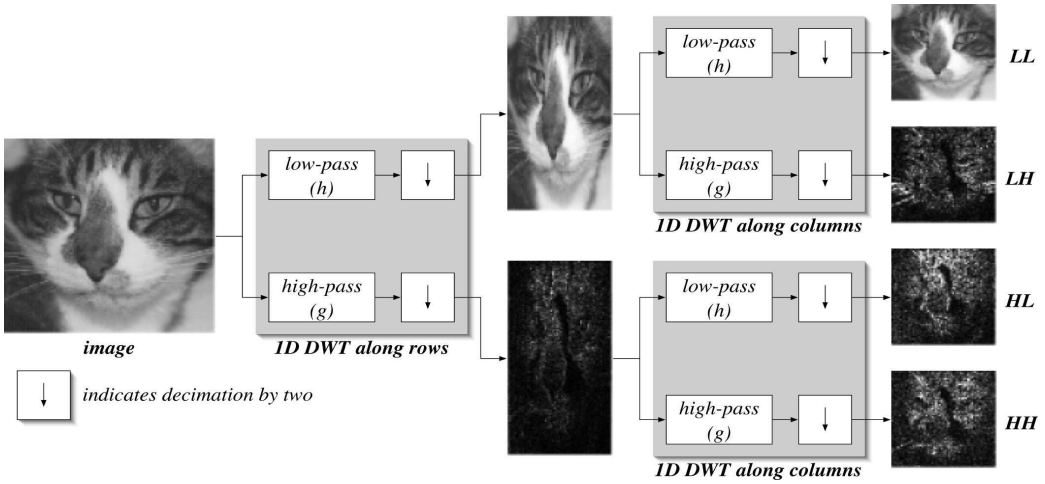
A. LSB Substitution

LSB is a simple and basic technique for covering information on cover image. Digital images can be classified as grayscale (8-bit-planes) or colored (24 bit planes) which depends on every pixel intensity levels, i.e., every pixel can be represented by 24-bits, 8-bits or indeed, even just a single piece. In case every pixel of the computerized image is accepted as n bits then the advanced image

can be made out of n quantities of 1-bit planes in the range from bit-plane zero to bit-plane n-1. For example, in a dim scale image each pixel is spoken to by eight bits, so the image can be cut onto eight cuts (bit planes) from bit-plane zero to bit-plane 7.These eight cuts are confined onto two sections: Most Significant Bits (MSE) and Least Significant Bits (LSB). LSB don't hold outwardly basic data, so that is the perfect condition for implanting watermark bits. In this technique, the way toward implanting relies upon picking a subset of cover image and applying the substitution action on them. That trades the LSB of cover image by the watermark. The LSB strategy is portrayed by simplicity, high limit, easy to understand and actualize, and can't be seen by the stripped eye. Nevertheless, the limitations of this method are that less robust (Easy control by assailants), vulnerable to noise, scaling and trimming.

B. Discrete Wavelet Transformation

Wavelet change is utilized as a part of a wide range in signal processing applications and image pressure. It isolates the signal to set of fundamental capacities which are called wavelets. Discrete Wavelet Transform (DWT) is described as an effective and exceptionally adaptable technique for breaking down signals sub bands. In instance of one-dimensional DWT, image is deteriorated into 4 bands signified by Low-Low (LL) level, High-Low (HL) level, Low-High (LH) level and High-High (HH) level, as appeared in Figure 1. Where, H symbolizes high-pass channel (High frequency) and L symbolizes low-pass channel (Low frequency).In instance of Multi-Level Discrete Wavelet Transform, as appeared in Figure 1. This speaks to the image in the wake of applying three times of DWT. The image comprises of frequency zones of LL1, LH1, HL1, and HH1. The LL1 (low frequency zone) is disintegrated onto sub-level frequency region data of LL2, LH2, HL2, HH2. By applying past decay over and over the image can be disintegrated onto N level wavelet transformation. The DWT is characterized by Imperceptibility and Robustness. In any case, the downsides of this strategy are that Long pressure time, High computational cost, Noise/obscure near edges of images.



(a)

(b)

Figure 1. 1-level DWT (a) Decomposition, (b) Reconstruction

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue V, May 2018- Available at www.ijraset.com

III. LITERATURE REVIEW

In this paper, we propose a new hybrid method for image steganography by utilizing discrete curvelet transform and least significant bit (LSB). The proposed technique is called Hybrid Curvelet Transform and Least Significant Bit (HCTLSB). In HCTLSB, the curvelet de noising is connected as a preprocessing advance keeping in mind the end goal to expel the clamor from the cover picture. The cover picture is changed by applying the discrete curvelet transform before implanting the mystery information by utilizing LSB system. Invoking the curvelet transform in the proposed strategy can handle the bend discontinuities in the cover picture to get a better quality and robustness image. [1]

Progressed watermarking has been used for keeping up copyright information of the electronic media for a long time. Automated watermarking is a technique used for embeddings copyright information in the media reports. The media record could be an image, a sound, a video, or a substance. Steganography have been used as a piece of the Digital watermarking application. Steganography has ended up being more basic due to the exponential improvement of correspondence of potential PC information on the web. Steganography fluctuates from cryptography, with the ultimate objective that cryptography covers the substance of secret message; however, steganography is tied in with disguising the message in media reasonably. This investigation article gives an outline of steganography, its applications, and difference from cryptography. This investigation article examinations execution of the Least Significant Bit (LSB), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT). [2] This paper proposes an instigated strategy for scrambling information utilizing Advanced Encryption System (AES) and camouflaging the information utilizing Haar Discreet Wavelet Transform (HDWT). HDWT means to diminish the multifaceted nature in image steganology while giving less image winding and lesser noticeable quality. One-forward of the image passing on the purposes of enthusiasm of the image in a region and other three locales passing on a more obvious components of the image then the figure content is canvassed in any occasion Significant Bits (LSB) positions in the less separated territories of the conveyor image, if the message doesn't fit in the chief LSB just it will use the second LSB. This proposed computation covers all kind of images and letters all together. There are solicitations of the figurings of steganography to progress with the farthest point or with quality, so with this procedure we went for the constrain demand to store as high as possible messages in the image with reduced effect of the idea of the image. [3] Today Security of data is of prevalent hugeness these days. Security has ended up being a champion among the most basic factor in correspondence and information advancement. Hence steganography is used. Steganography is the strength of hiding secret or sensitive information into cutting edge media like images so as to have secure correspondence. In this paper we show and discuss LSB (Least Significant Bit) based image steganography and AES encryption estimation keeping in mind the end goal to give an extra layer of security. In this paper we showed LSB based Image Steganography. LSB based image Steganography is a better than average system for introducing sensitive information behind some cover media. LSB based steganography in blend with AES will give a conventional security model to hiding data. AES is supported over DES due to its straightforwardness and its speed. [4]

IV. PROPOSED METHOD

In the proposed method, the procedure begins with the preprocessing of the input image which is known as cover image. We take another image which we have to be hide in the cover image is known as secret image. Secret image is separated into 2 sections: lowerhalf (LH) and upperhalf (UH).Upperhalf is embedded in cover image by using two bit LSB technique and another lowerhalf is decomposed by using lower 1 DWT. Wavelet Decomposition is done on upperhalf semi stego image and lowerhalf decompose image. We get stego image after the inverse DWT is performed.

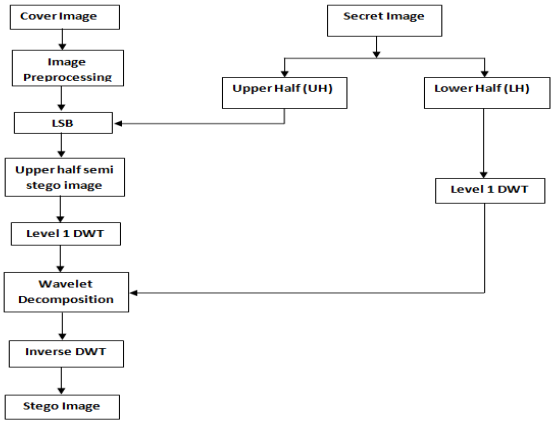


Figure 2. Proposed approach for image steganography

C. Cover Image

The Image that covers the secret message inside. The cover image is the conveyor of the secret message. A cover is regularly picked in a way that seems, by all accounts, to be more run of the mill and safe and not stimulate doubt.

D. Image Preprocessing

Preprocessing is the method in which it uses a small neighborhood of a pixel in an input image to get a new brightness value in the input image. Preprocessing was a typical name for doing tasks with the images at the most minimal level of reflection in the both info and yield were force images.

E. Secret Image

Secret image is the image which can be any type of image format. The image which hide inside the cover image is known as secret image.

F. Encoding Process

In this process two technique are proposed LSB from spatial domain and DWT form transform domain. Upperhalf of secret image is embedded by using LSB technique. The LSB conceals the message bits into the image pixels either in a successive or randomized form. It makes a way to replace the least significant bits of the image with the message bits.

Another lowerhalf of secret image is decomposed by using DWT. DWT of the image creates multi resolution representation of an image. The multi resolution representation gives a basic system for translating the digital image data.

G. Inverse DWT

When we touch base at our discrete wavelet coefficients, we require an approach to recreate them once more into the original image. So as to do this, We use the procedure known as the inverse discrete wavelet transform. The procedure is essentially reversed. The DWT coefficients are first upsampled by setting zeros in the middle of each coefficient, viably multiplying the lengths of each. These are then convolved with the remaking scaling channel for guess coefficients and the reproduction wavelet channel for the detail coefficients. These outcomes are then included to touch base at the original image.

H. Stegoimage

The Secret information is installed into cover image utilizing Hybrid approach of LSB and DWT to get stego image. Decoding process is the reverse process of encoding. We performed reverse operation of encoding process to get secret image.

V. RESULT AND ANALYSIS

Results have been assessed by estimating the image quality of original image and stego image. Normally two measures are utilized, for example, Peak Signal Noise Ratio (PSNR) what's more, Mean Squared Error (MSE).

$$MSE = \frac{\sum_{M,N} [I_1(m,n) - I_2(m,n)]^2}{M * N}$$

$$PSNR = 10 \log_{10}\left(\frac{R^2}{MSE}\right)$$

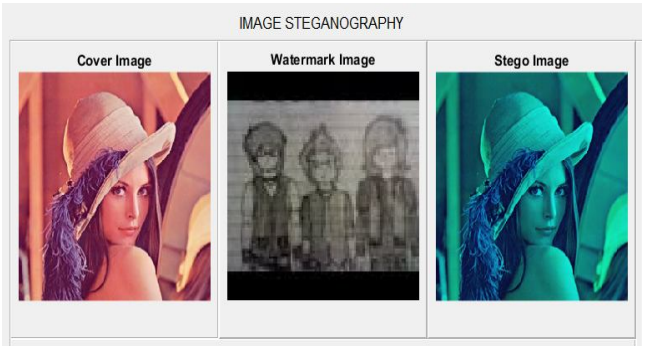


Figure 3. Watermark and stego image

Table 1 demonstrates the PSNR consequence of the cover image. PSNR is connected to quantify the nature of two images i.e. original image and stego image. A decibel (dB) is an estimation unit of PSNR.

S.no.	Image	PSNR
1	Leena	54.3828
2	Baboon	55.9755
3	Pepper	54.9232

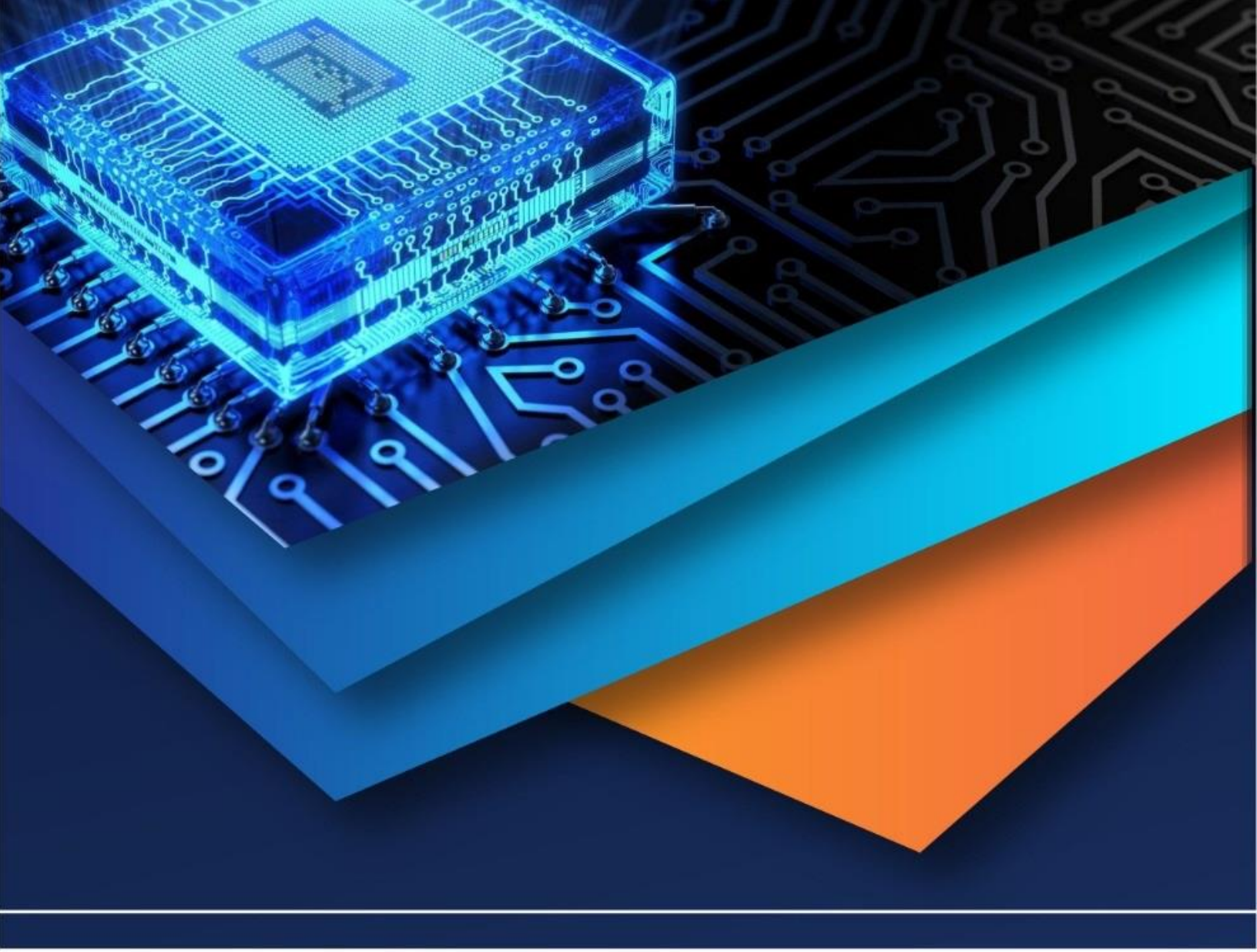
Table1. Result of Paper

V. CONCLUSION

The proposed method combines both spatial domain and transforms domain strategies of image steganography, accordingly boosting the security of data. While doing as such quality of image does not get disturbed. Most striking element is that image of all formats can be utilized for information hiding. Experimental comes about got by proposed method were promising, it demonstrated that proposed method was especially productive and secured. In future work, secret key will likewise be connected in steganography. Other sight and sound formats, (for example, video, sound) can be considered for information hiding. Considering visual cryptography with steganography and watermarking could likewise be a fascinating work.

REFERENCES

[1] Reba Mostafa, Ahmed Fouad Ali, and Ghada EI Taweal," Hybrid curvelet transform and least significant bit for image steganography", 2015 IEEE Seventh International Conference on Intelligent Computing and Information Systems (ICICIS'15)
[2] Saravanan Chandran, Koushik Bhattacharyya," Performance Analysis of LSB, DCT, and DWT for Digital Watermarking Application using Steganography", International Conference on Electrical, Electronics, Signals, Communication and Optimization (EESCO) – 2015.
[3] Essam H. Houssein ,Mona A. S. Ali and Aboul Ella Hassanien," An Image Steganography Algorithm using HaarDiscrete Wavelet Transform with AdvancedEncryption System", 978-83-60810-90-3/$25.00c 2016, IEEE.
[4] Sandeep Panghal, Sachin Kumar, Naveen Kumar "Enhanced Security of Data using Image Steganography and AES Encryption Technique",International Journal of Computer Applications (0975 – 8887) Recent Trends in Future Prospective in Engineering & Management Technology 2016
[5] Pooja Dabas , Kavita Khanna, "Efficient Performance of Transform Domain Digital Image Watermarking Technique over Spatial Domain", International Journal of Advanced Research in Computer Science and Software Engineering , Volume 3, Issue 6, June 2013 ISSN: 2277 128X.
[6] Reena Anju and Vandana "Modified Algorithm for Digital Image Wa-termarking Using Combined DCT and DWT ", International Journal of Information and Computation Technology. ISSN 0974-2239 Volume 3, Number 7 (2013), pp. 691-700 International Research Publications House .
[7] Emy V Yoyak, PG Scholar, Jaya Engineering College, Thiruvallur, India, "Three Level Discrete Wavelet Transform Based Image Steganography", International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 4, April – 2013.
[8] Th. R. Singh, Kh. M. Singh, S. Roy, "Image Watermarking Scheme based on Visual Cryptography in Discrete Wavelet Transform," IJCA, Vol. 39, No.1, Feb 2012.
[9] Qing Liu,Jun Ying(2012),"Grayscale Image Digital Watermarking Technology Based on Wavelet Analysis".
[10] X. Zhang, S. Wang, Efficient steganographic embedding by exploiting modification direction, IEEE Communications Letters 10(11)(2006) 781-783.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY