Data Hiding in Grayscale Image using Least Significant Bit Technique and Discrete Wavelet Transform

G.V.M. Praveen, E.Vishnu Priyatam, Ramaiah Challa

***Abstract:** In this paper, we present a model for data hiding using modified least Significant Bit and DWT concept to further improve the ability to embed as a picture good (EC).From the begin, each high-quality pixel produces 4 new pixels. The puzzle facts is concealed in all the four conveyed pixels. via then the pixels are fixed to improve the concept of the stego-pics. There are four separate stego-pictures crafted from the four unmistakable revised pixels. each stego-photo disguises one piece for every pixel. For Stego-photos, the typical peak signal-to-noise ratios (PSNR) the proposed procedure successfully withstand against RS-stego examination*

***Keywords :** Least significant bit (LSB), Peak signal-to-noise ratios(PSNR), pixel value difference(PVD),DWT.*

I. INTRODUCTION

Steganography has emerged over the years as a simple and conducive alternative for digital data transmission (Chedded et al.,2010).The art of secret contact is steganography. Here for examples image, sound, video, and content, the data transmission is achieved through different distributed media Picture steganography use photo to carry the facts through the all inclusive network channel .It is a beneficial approach in the fields of boundary, social safety, and banking department wherein secret's the pinnacle want (Cheddad et al., 2010). photo steganography is practiced in 2 awesome methods (1) reversible (2) irreversible (Subhedar and Mankar, 2014). The reversible philosophy ensures the recovery of poser data similarly as the primary picture at the recipient aspect. in spite of the reality that the irreversible techniques revolve simply around the successful recuperation of secret records. Our proposed work is based upon the irreversible method. A bit of the unquestionable strategies in the field of picture steganography (Hussain et al., 2018). The image quality and EC are the two parameters of the steganographic image to measure the quality of a technique of the data hiding .

The image quality depends on the stego image distortion. PSNR measures the visual quality (Bong and Khoo, 2015) of a stego-picture. The high PSNR implies that lower bending and the a different way.

The MSE considers the first and stego-picture to check the idea of stego-picture. It should be as low as would be reasonable (Bong and Khoo, 2014). Further, the WPSNR uses MSE and Noise Noise Visibility Function (NVF) to check the idea of the stego-picture. essentially, Q and SSIM are in like way used to degree the stego-image nice (Wang, et al., 2004). The Q have to reliably be at top aspect for instance round 1for the better concept of stego-photograph. The EC is the amount of mystery facts bits the picture can cowl up with out substantial relics (Hussain et al., 2018). the benefit and simplicity of the least sizable bit (LSB) photo steganography strategies made it accommodating for facts concealing. Johnson and Jajodia (1998) camouflaged the name of the game facts with the aid of superseding the LSB of the primary photograph pixel. This strategy changed into feeble to the interloper as through getting to the LSBs, the records may be effectively gotten to. Both Wu and Hwang; and Swain, 2016:Sahu and Swain,2017; Sahu et al.,2018). Making plans to cut down the mutilation of the stego-photo through self-assertively appearing +1 or - 1 to the main pixel regards if the puzzle records failed to prepare with the LSB. This system limits the introducing capacity to one piece for each pixel. Mielikainen (2006) went with a trade to the LSB approach referred to as LSB making plans got here back to. right here the puzzle bits are secured with the help of the twofold restriction and four introducing rules. The proposed strategy in like way conveys the proportionate embeddings restriction as made by way of Sharp (2001) yet it changes much less bits within the primary image. in spite of the manner that LSB approaches gigantically remodel as a long way as feasible, it's miles displayed to RS-assessment (Fridrich and Goljan, 2002). With the expectancy to manufacture the breaking factor and reducing down the turning to the stego-picture and thereafter the differentiation regard (d) between the two pixels is enrolled. The value d is mapped to the foreordained range table to perceive the number puzzle data bits to be embedded inside a square. Wang et al. (2008) found the response for falling-off boundary problem (FOBP) which existed by joining the PVD and modulus work. System improved the PSNR regard when stood out from Wu and Tsai (2003). It unearths the differentiation regard d in 3 extraordinary methods,

Revised Manuscript Received on December 30, 2019.
* Correspondence Author

Praveen Goli*, CSE Department, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, India, Email:praveengoli.1998@gmail.com@gmail.com

E.Vishnu Priyatam , CSE Department, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, India, Email:evpr768@gmail.com

Ch.Ramaiah, Computer Science And Engineering Department, Koneru Lakshmaia Education Foundation, Vaddeswaram, Guntur, India. Email: ramaiah.challa@kluniversity.in

as an instance, level, vertical and nook to nook with the aid of selecting a reference factor. Current bendy directional PVD gadget which contributed by using substantial upgradation in as a long way as viable similarly as protecting the image excellent.

There are gigantic variety of articles recorded as a difficult copy making use of systems provide more farthest factor even as PVD techniques accomplish better imperceptibility. approaches, as an example, LSB and PVD whilst solidified they outmaneuver others to as some distance as viable and imperceptibility (Khodaei and Faez, 2012; Hussain et al., 2016; Wu et al.,2005; Jung, 2018; Swain, 2018). the present photo steganographic tactics produce single stego-photo from the principle photo. The imprisonment of unmarried stego-image obliges the EC. various methodologies recorded as a tough replica made an assignment to manufacture the EC, but then, the picture best faded (Jung, 2018; Khodaei and Faez, 2012). in this paper, we present a singular multi stego-photo primarily based methodology to hide the name of the game information. The proposed device produces four stego images from one in every of a kind photograph. each pixel of the made stego-pix covers one piece.

II. PROCEDURE FOR PAPER SUBMISSION

A. Existing method

- The high PSNR implies that lower mutilation and the a different way. The MSE breaks down the first and stego-picture to check the idea of stego-picture.
- It should be as low as could be normal in light of the current situation (Bong and Khoo, 2014). Further, the WPSNR uses MSE and Noise Visibility Function (NVF) to check the idea of the stego-picture.
- In this way, Q and SSIM are furthermore used to measure the stego-picture quality.

B. Proposed method

- Encryption and decryption using DWT steganography shuffling using least significant bit of hash (HLSB) which uses hash function to create a meaningful way of incorporating data bits into LSB bits.
- Recently cryptography includes the use of advanced mathematical methods in techniques for Decoding and encryption .
- Every day ,cipher algorithms become more and more complex.

III. ALGORITHM

A. DWT :

- The Discrete Wavelet Transform can identify portions of the cover image where it is possible to hide secret data
- DWT separates data into components of high and low frequency.
- It gathers information about both frequency and position(time location).
- Wavelets are often used to describe two dimensional signs, for example objects.
- Wavelets, on the other hand ,have both frequency and position. The first, as before, complete zero cycles, and the second completes one cycle. The third and fourth ,although they have the same frequency, differ in position twice the first frequency.

B. LSB :

- In virtual steganography, sensitive messages can be concealed by manipulating and storing data in the smallest bits of an image or sound file.
- In the object context ,if the user alters the last two bits of a colour in a pixel, the colour quality can change to a maximum of +/-3 value positions from the human eye.
- The user can retrieve this information later by extracting the smallest bits of manipulated pixels to retrieve the original message.

IV. CURRENT TRENDS IN DIGITAL IMAGE-BASED DATA HIDING METHODS

Because of numerous technology included in virtual photograph steganography within the latest years, there's a exceptional fulfillment in terms of overall performance, i.e., wise algorithms permitting to comfy puzzle records have risen. considering the application territory, those counts may be very well asked into spatial space and trade (repeat) vicinity strategies. overlaying thriller statistics within the spatial sector is finished with the aid of without a doubt controlling the pixel estimations of the spread photo to acquire the suitable improvement those techniques are normally .additionally, they attain a excessive embeddings limit but they may be to a first-rate volume slanted to low nature of the stego photo. Complexity growth has become a number of the maximum excellent spatial region estimations. It engages riddle data to be secured through expanding the qualification regards determined among pixels.

A. Steganography

In the administration specialist make friends, steganography and cryptography are family. Cryptography scrambles a message by using certain cryptographic figurings for changing over the riddle data into vague structure. On the other hand, Steganography covers the message so it can't be seen [1]. In various words, we can say that steganography is the investigation of covering information. Whereas cryptography’s aim is to tangle data with an outcast, steganography’s objective is to shield information from an untouchable. The basic structure of Steganography is contained three fragments: the "spread medium", the covered message, and the key. The spread medium can be a painting,a propelled picture, a mp3, even a TCP/IP pack notwithstanding different things. The thing will „carry‟ the covered message. A key is used to decipher/interpret/discover the covered message. This can be anything from a mystery expression, a model, a blacklight, or even lemon juice. Going with condition offers a non-exclusive image of the steganographic technique bits:

Spread medium + disguised data + stego key = stego medium

In this extraordinary circumstance,the cover medium is where we conceal the information concealed ,which can be encoded similarly using the stego key.The resulting archive is the stego medium (which is clearly going to be a similar type of archive to the cover medium).The cover_medium (and, thus, the stego_medium) are normally picture or sound records. "Steganography‟s claim to fame in security is to upgrade cryptography, not replace it.

If a covered message is encoded, it ought to similarly be unscrambled at whatever point discovered, which gives another layer of security."

B. Steganalysis

Steganalysis is the path toward perceiving steganography by researching distinctive parameter of a stego media. The fundamental development of this method is to recognize a suspected stego media. After that steganalysis system chooses if that media contains disguised message or not and a while later endeavor to recover the message from it. In the cryptanalysis clearly the got message is encoded and it undeniably contains the covered message considering the way that the message is blended. Nevertheless, by virtue of steganalysis this may not be substantial. The assumed media might be with covered message. The technique of steganalysis starts with a lot of suspected knowledge flows[3]. By then the set is diminished with the help of advance quantifiable systems.

V.RESULT AND DISCUSSION

This section provides the proposed scheme's experimental results and analysis .This algorithm efficiently embedded the secret text file the image of the cover and remove it from the stego image. The simulation results suggest that the technique maintains good quality. Compared to various image processing operations, it is robust. Figure 1 displays the image of the original cover. Fig 2 shows the cover image is transferred to DWT image ,after that we embedding the secret text file by using key into the DWT image shown in the Fig 3 .In Fig 4 we are Extracting the Secret text by using key which is used before in embedding process .In Fig 5 we are validating the image and producing the PSNR and Entropy values.

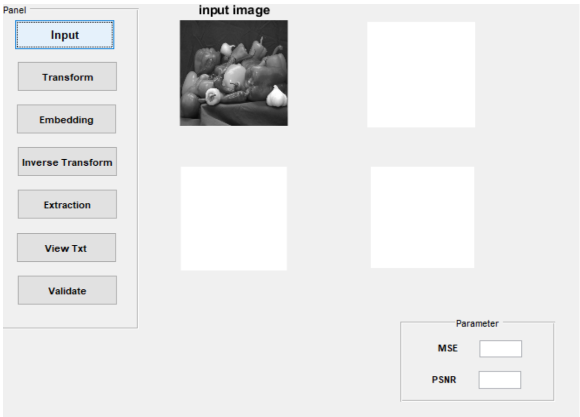


Fig .1(Cover image)

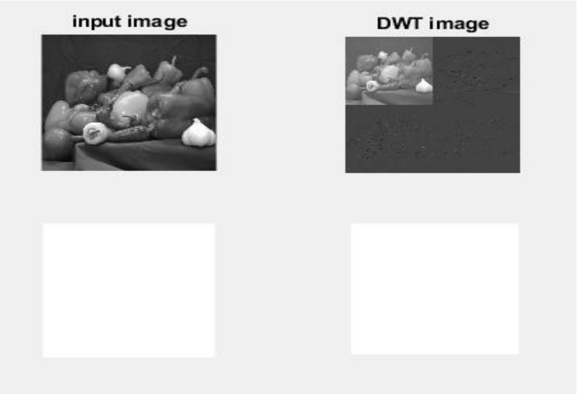


Fig.2 (DWT image)

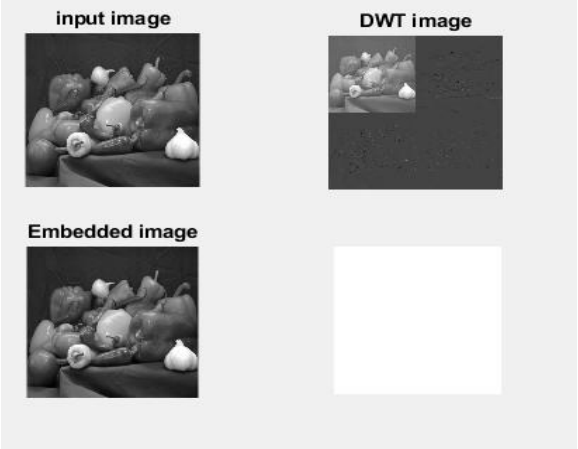


Fig .3 (Embedded image)

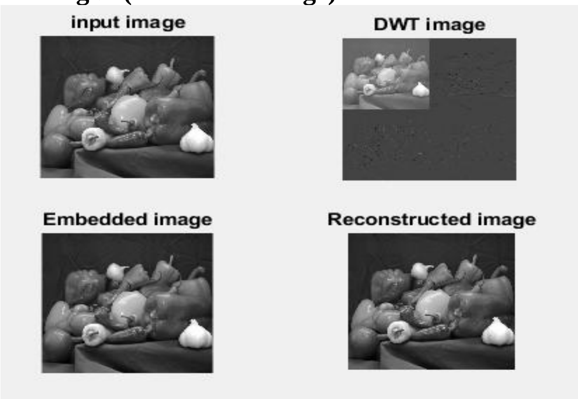
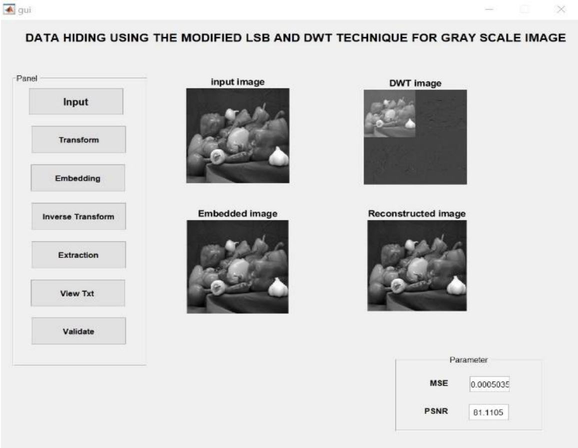


Fig .4 (Extraction image)



MSE 0.0005035
PSNR 81.1105

Fig 5.(PSNR and MSE values)

VI. CONCLUSION

This paper proposes a unique method for information protecting the use of multi stego-photographs to reap excessive farthest factor with low bowing. anyways, every pixel of the principle photo produces four pixels. The puzzle records is concealed on all of the made pixels using the changed LSB making plans machine. via then pixels are fixed to decrease the winding. Thusly, the primary photo produces four precise stego-pix and each stego-photograph disguises 1 piece for each pixel. further, the proposed technique restricts RS-assessment. For in addition improvement, the makers expect to develop a reversible steganography with the aid of enhancing the EC for the individual stego-photos by means of joining LSB making plans with PVD.

Retrieval Number: B6644129219/2019©BEIESP
DOI: 10.35940/ijitee.B6644.129219
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

REFERENCES

1. Bong, D. B. L., and Khoo, B. E. (2014). Trance photo cloud evaluation by the usage of beneficent deblur variety and histogram shape differentiate. signal Processing: image verbal exchange, 29(6), 699-710.
2. Bong, D. B. L., and Khoo, B. E. (2015). target darken evaluation reliant on pressure bumbles of neighborhood separate maps. Sight and sound tools and packages, 74(17), 7355-7378.
3. Chan, C. ok., and Cheng, L. M. (2004). Hiding facts in snap shots through direct LSB substitution. version confirmation, 37(three), 469-474
4. Chang, ok. C., Chang, C. P., Huang, P. S., and Tu, T. M. (2008). a singular photograph Steganographic method the usage of Tri-manner Pixel-cost Differencing. journal of Multimedia, three(2), 37-forty four.
5. Cheddar, A., Condell, J., Curran, ok., and Mc Kevitt, P. (2010). Propelled image steganography: Survey and exam of present day strategies. sign Processing, ninety(three), 727-752.
6. Fridrich, J., and Goljan, M. (2002, April 29). practical stegnoanalysis of reducing area pics: pinnacle tier. In safety and Watermarking of Multimedia Contents IV (Vol. 4675, pp. 1-14). San Jose, California, u.s.
7. Hameed, M. An., Aly, S., and Hassaballah, M. (2017). A capable information masking gadget reliant on adaptable directional pixel regard differencing (ADPVD). Media equipment and applications, 77, 14705-14723.
8. Hussain, M., Wahab, A. W. A., Javed, N., and Jung, okay. H. (2016). Cream statistics disguising plan using right-maximum digit substitution and adaptable least colossal piece for electronic pictures. Equalization, 8(6), 41-61.
9. Hussain, M., Wahab, A. W. A.,Ho, A. T., Javed , N., and Jung, okay. H. (2017). A statistics disguising plan the usage of balance bit pixel regard differencing and improved uttermost right digit substitution. signal Processing: picture communication, 50, 44-fifty seven.
10. Hussain, M., Wahab, A. W. An., Idris, Y. I. B., Ho, A. T., and Jung, okay. H. (2018). image steganography in spatial area: An define. signal Processing: Sixty-five, 46-sixty-six, photograph communication.

AUTHORS PROFILE

G.V.M. Praveen is pursuing his B.Tech in KL University .He is passionate about research and his area of interests are Network Security,Artificial Intelligence, Machine Learning In addition to this he is Certified salesforce Administrator.

E.Vishnu Priyatam is pursuing his B.Tech in KL University. He is passionate about research and his area of interests are Artificial Intelligence, Data mining, Network Security and Cloud Computing. In addition, he is also interested to Work in NGO.

Ramaiah Challa is working as Asst. Professor in KL University. He has done M.Tech in V R Siddhartha Engineering college. His interested areas are Networks Security and Fog computing. He has published several scopus indexed papers .