# A Review of Character Color Mapping For colored Images Using Secure LSB Steganography

[1]Nitya Khare, [2]Akanksha Singh
[1]Student, [2] Assistant Professor
[1] CSE Department,
[1] BBDU, Lucknow, India
[2] CSE Department,
[2] BBDU, Lucknow, India

*Abstract :* Steganography is an imperative region of research as of late including various applications. It is the study of inserting data into the cover picture viz., content, video, and picture (payload) without making measurably noteworthy adjustment the cover picture. Steganography can be characterized as the investigation of undetectable correspondence that ordinarily manages the methods for concealing the presence of the conveyed message. On the off chance that it is accomplished effectively, the message does not draw in consideration from spies and aggressors. The principle targets of steganography are un perceptibility, strength (protection from different picture handling strategies and pressure) and limit of the concealed information. These are the principle factors which make it not quite the same as different procedures watermarking and cryptography. This paper incorporates the critical steganography techniques and the fundamental concentrate is on the survey of steganography in computerized pictures.

***Index Terms* - Adaptive steganography, Frequency domain, Image steganography**

## I. INTRODUCTION

In this cutting edge time, web offers extraordinary accommodation in transmitting a lot of information in various parts of the world. Be that as it may, the wellbeing and security of long separation correspondence remains an issue. With a specific end goal to take care of this issue has prompted the advancement of steganography plans. Steganography is the science that imparts mystery information in a suitable sight and sound bearer, e.g., picture, sound, and video documents. Steganography is unique in relation to cryptography. The principle target of cryptography is to secure interchanges by changing the information into a shape with the goal that it can't be comprehend by a meddler. Then again, steganography systems tend to shroud the presence of the message itself, which makes it troublesome for an onlooker to make sense of where precisely the message is. There are other two advancements that are firmly identified with steganography are watermarking and fingerprinting [1]. These advancements are mostly worried about the security of licensed innovation, in this manner the calculations have unexpected necessities in comparison to steganography. In watermarking the majority of the examples of a question are "set apart" similarly. Then again, in fingerprinting novel imprints are implanted in particular duplicates of the transporter question that are provided to various clients. This empowers the protected innovation proprietor to recognize clients who break their authorizing understanding by providing the property to outsiders [1].

For quite a long time individuals have shrouded data in various ways. Steganography is a sort of concealed correspondence that actually signifies "secured expressing" (from the Greek words stegano or "secured" and graphos or "to compose"). In 1550, Jerome Cardan, an Italian mathematician, proposed a plan of mystery composing where a paper veil with gaps is utilized. The client needs to compose his mystery message in such openings in the wake of putting the veil over a clear sheet of paper. At that point evacuate the cover to fill in the clear parts of the page and along these lines the message shows up as harmless content [2].

The execution of a steganographic framework can be measured utilizing a few properties. The most vital property is the factual un perceptibility (indistinctness) of the information, which indicates that it is so hard to decide the presence of a shrouded message. Other related measures are the steganographic limit, which is the most extreme data that can securely installed in a work without having measurably perceptible items and heartiness, which alludes to how well the steganographic framework opposes the extraction of concealed information.

LSB system is actualized in spatial space while DCT and DWT strategy are executed in recurrence area. In minimum critical piece (LSB), every pixel of a picture changed into the paired esteem and information is covered up into the slightest noteworthy position of the twofold estimation of the pixels of the picture in such a way, to the point that, it doesn't obliterate the honesty of the cover picture however this plan is delicate to an assortment of picture preparing assaults like pressure, editing and so forth. The discrete cosine changes (DCT) and discrete wavelet change (DWT) are numerical capacity that changes advanced picture information from the spatial to the recurrence area. In DCT, subsequent to changing the picture in recurrence area, the information is installed at all noteworthy bits of the medium recurrence segments and is determined for lossy pressure while In DWT, mystery messages are installed in the high recurrence coefficients came about because of Discrete Wavelet Transform and give most extreme power.

## II. LITERATURE REVIEW

A novel reversible information concealing calculation, which can recoup the first picture with no bending from the stamped picture after the shrouded information have been removed, is introduced in this paper. This calculation uses the zero or the base purposes of the histogram of a picture and marginally adjusts the pixel grayscale qualities to insert information into the picture. It can insert a greater number of information than a considerable lot of the current reversible information concealing calculations. It is demonstrated systematically and indicated tentatively that the pinnacle motion to-commotion proportion (PSNR) of the stamped picture created by this technique versus the first picture is ensured to be over 48 dB. This lower bound of PSNR is significantly higher than that of every single reversible datum concealing systems detailed in the writing. The computational unpredictability of our proposed procedure is low and the execution time is short. The calculation has been effectively connected to an extensive variety of pictures, including regularly utilized pictures, therapeutic pictures, surface pictures, airborne pictures and the greater part of the 1096 pictures in CorelDraw database. Trial results and execution correlation with other reversible information concealing plans are displayed to show the legitimacy of the proposed calculation [Z Ni, YQ Shi, N Ansari, W Su - Reversible information concealing, IEEE, 2006].

Reversible watermarking empowers the installing of helpful data in a host motion with no loss of host data. Tian's distinction extension strategy is a high-limit, reversible technique for information inserting. In any case, the technique experiences unwanted contortion at low implanting limits and absence of limit control because of the requirement for installing an area outline. We propose a histogram moving method as a contrasting option to installing the area outline. The proposed strategy enhances the bending execution at low implanting limits and mitigates the limit control issue. We additionally propose a reversible information installing system called expectation blunder extension. This new system better endeavors the relationship inalienable in the area of a pixel than the distinction extension conspire. Forecast mistake development and histogram moving join to frame a successful strategy for information installing.

The trial comes about for some, standard test pictures demonstrate that forecast blunder development duplicates the most extreme inserting limit when contrasted with distinction extension. There is likewise a huge change in the nature of the watermarked picture, particularly at direct implanting limits [D.M. Thodi and J. J. Rodriguez-Expansion inserting strategies for reversible watermarking, IEEE, 2007].

K Suresh Babu, et. al.proposed a picture Steganography that can confirm the unwavering quality of the data being transmitted to the recipient. The technique can confirm whether the aggressor has endeavored to alter, erase or manufacture the mystery data in the stego-picture [14]. Atalla I. Hashad, et. al. portray the LSB addition strategy, the Discrete Cosine Transform (DCT) inclusion procedure is depicted lastly we will propose another system that uses embedding's a bit in the spatial area joined with the DCT addition technique[15]. Arvind Kumar, et. al. examines how advanced pictures can be utilized as a transporter to conceal Messages and furthermore examinations the execution of a portion of the steganography tools[16]. Vijay Kumar, et. al. means to watch the impact of installing the mystery message in various groups, for example, CH, CV and CD on the execution of stego picture regarding Peak Signal to Noise Ratio (PSNR). Experimentation has been finished utilizing six unique assaults. Test comes about uncover that the blunder piece supplanting with askew detail coefficients (CD) gives preferred PSNR over doing as such with different coefficients [17]. Ali Al-Ataby, et. al. proposed a changed high-limit picture steganography system that relies upon wavelet change with adequate levels of subtlety and contortion in the cover picture and abnormal state of general security[18]. T. Narasimmalou, et. al. Proposed an ideal discrete wavelet change (DWT) based steganography. Examinations demonstrate that the pinnacle flag commotion proportion PSNR) produced by the proposed strategy is better[19]. Neda Raftari, et. al. proposed a novel picture steganography system that consolidates the Integer Wavelet Transform (IWT) and Discrete Cosine Transform (DCT) is proposed which installs mystery picture in recurrence area of cover picture with high coordinating quality[20].

## III. METHODS OF HIDING DATA IN DIGITAL IMAGE

Framework Steganography is utilized for incognito correspondence. The mystery picture which is conveyed to the goal is inserted into the cover picture to infer the stego picture. In this area assessment parameters and proposed implanting and recovery procedures are examined.

**a) Least significant bit substitution technique(LSB)**

In LSB steganography, the slightest critical bits of the cover media's advanced information are utilized to disguise the message. The easiest of the LSB steganography methods is LSB substitution. LSB substitution steganography flips the last piece of each of the information esteems to mirror the message that should be covered up. Consider a 8-bitgrayscale bitmap picture where every pixel is put away as a byte speaking to a dark scale esteem Suppose the initial eight pixels of the first picture have the accompanying dim scale esteems [4]:

11010010
01001010
10010111
10001100
00010101
01010111
00100110
01000011

To hide the letter C whose binary value is10000011, we would replace the LSBs of these pixels tohave the following new grayscale values:
11010011
01001010
10010110
10001100
00010100
01010110
00100111
01000011
Note that, all things considered, just a large portion of the LSBs need to change. The contrast between the cover (i.e. unique) picture and the stego picture will be not really observable to the human eye. Be that as it may, one of its real constraints is little size of information which can be installed in such sort of pictures utilizing just LSB. LSB is greatly helpless against assaults. LSB strategies actualized to 24 bit designs are hard to identify in opposition to 8 bit organize [8]. Another case of LSB method is : Consider a lattice for 3 pixels of a 24-bit picture and the number 300 is to be installed utilizing LSB procedure. The subsequent lattice is as per the following:
PIXELS: (01010101 01011100 11011000)
(10110110 11111100 00110100)
(11011110 10110010 10110101)
C: 10000011
(01010101 01011100 11011000)
(10110110 11111100 00110100)
(11011111 10110011 10110101)
Here the number C was embedded into the first8 bytes of the grid, only the 2 bits needed to be changed according to the embedded message .On average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size.

**b) Discrete Cosine Transform Technique(DCT)**

DCT coefficients are utilized for JPEG pressure [10][12]. It isolates the picture into parts of varying significance. It changes a flag or picture from the spatial area to the recurrence space. It can isolate the picture into high, center and low recurrence parts. In low recurrence sub-band, a great part of the flag vitality lies at low recurrence which contains most vital visual parts of the picture while in high recurrence sub-band, high recurrence segments of the picture are normally evacuated through pressure and clamor assaults [13]. So the mystery message is implanted by adjusting the coefficients of the center recurrence sub-band, with the goal that the perceive ability of the picture won't be influenced.

**c)Discrete Wavelet Transform Technique (DWT)[5]**

The frequency domain transform we applied in this research is Haar-DWT, the simples tDWT[18][19]. A2-dimensional Haar-DWT consists of two operations:
One is the horizontal operation and the other is the vertical one. Detailed procedures of a 2-D Haar-DWT are described as follows:
Step 1: At first, scan the pixels from left to right in horizontal direction. Then, perform the addition and subtraction operations on neighboring pixels. Store the sum on the left and the difference on the right as illustrated in Figure 1. Repeat this operation until all the rows are processed. The pixel sums represent the low frequency part (denoted as symbol L) while the pixel differences represent the high frequency part of the original image (denoted as symbol H).

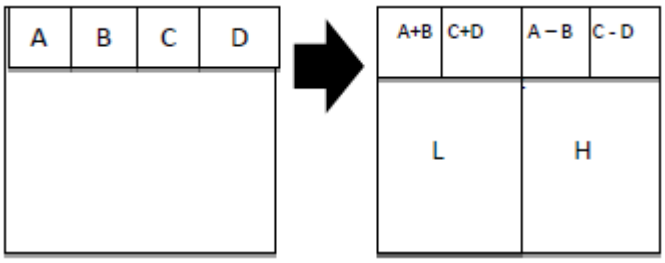

Figure 1 The horizontal operation on first row[5]

**4. Algorithm of Steganography**

**a)LSB Based Steganography[12]**

Algorithm to embed text message:-
Step 1: Read the cover image and text message which is to be hidden in the cover image.
Step 2: Convert text message in binary.
Step 3: Calculate LSB of each pixels of cover image.
Step 4: Replace LSB of cover image with each bit of secret message one by one.
Step 5: Write stego image.
Step 6: Calculate the Mean square Error (MSE), Peak signal to noise ratio (PSNR) of the stego image.
Algorithm to retrieve text message:-

Step 1: Read the stego image.
Step 2: Calculate LSB of each pixels of stego image.
Step 3: Retrieve bits and convert each 8 bit in to character.

**b)DCT Based Steganography:[12]**

Algorithm to embed text message:-
Step 1: Read cover image.
Step 2: Read secret message and convert it in binary.
Step 3: The cover image is broken into 8×8 block ofpixels.
Step 4: Working from left to right, top to bottom subtract128 in each block of pixels.
Step 5: DCT is applied to each block.
Step 6: Eachblock is compressed through quantizationtable.
Step 7: Calculate LSB of each DC coefficient andreplace with each bit of secret message.
Step 8: Write stego image.
Step 9: Calculate the Mean square Error (MSE), Peaksignal to noise ratio (PSNR) of the stego image.

Algorithm to retrieve text message:-
Step 1: Read stego image.
Step 2: Stego image is broken into 8×8 block of pixels.
Step 3: Working from left to right, top to bottom subtract128 in each block of pixels.
Step 4: DCT is applied to each block.
Step 5: Each block is compressed through quantization table.
Step 6: Calculate LSB of each DC coefficient.
Step 7: Retrieve and convert each 8 bit into character.

## 5. Steganography In Image Spatial Domain

Steganography procedures that alter the cover picture and the mystery picture in the spatial space are known as spatial area techniques. It includes encoding at the LSBs level. Minimum Significant Bit Substitution (LSB) [3] is the most usually utilized stenographic strategy. The fundamental idea of Least Significant Bit Substitution incorporates the implanting of the mystery information at the bits which having least weighting with the goal that it won't influence the estimation of unique pixel. Another steganographic strategy to conceal a mystery message into a dark - esteemed cover picture was proposed [4]. For inserting a mystery message, a cover picture is apportioned into non-covering squares of two back to back pixels. In each piece, a distinction esteem is figured from the estimations of the two pixels. At that point that distinction esteem is supplanted by another incentive to insert the estimation of the mystery message. This technique creates a more impalpable outcome than those acquired from basic minimum noteworthy piece substitution strategies. The installed mystery message can be removed from the subsequent stego-picture without referencing the first cover picture.

Iuon-Chang Lin [5] proposed a Data concealing plan with mutilation resilience which utilizes spatial area for concealing information. This technique gives twisting resistance and gives better nature of handled picture. This plan gives powerful outcomes than different plans as far as twisting resilience. As LSB inclusion is more straightforward and useful for steganography, we can attempt to enhance one of its real disadvantages: the simplicity of extraction. We don't need that a busybody have the capacity to peruse all that we are sending.

## 6. Adaptive Staganography

Versatile steganography is a unique instance of the spatial and change strategies. In addition, it is presented as insights mindful inserting and veiling. Worldwide factual attributes of the picture are essentially utilized before any endeavor to manage its recurrence changed coefficients. These measurements choose what changes can be made. An arbitrary versatile choice of pixels really describes this technique, depending on the cover picture and the choice of pixels in a square with a vast standard deviation (STD). The last is planned to dodge regions of uniform shading, for example, smooth zones. This procedure is known for misusing pictures with existing or intentionally included clamor and with pictures that show shading multifaceted nature [12-15]. A versatile minimum noteworthy piece (LSB) steganographic strategy was proposed [16]. This strategy incorporates pixel-esteem differencing (PVD) which utilizes the distinction estimation of two back to back pixels to gauge what number of mystery bits will be implanted into the two pixels. The PVD approach is utilized to separate the smooth and edge territories. A k-bit LSB substitution strategy is utilized for concealing information in the pixels situated in the edge zones. The scope of distinction esteems is adaptively isolated into three unique levels that are bring down level, center level, and more elevated amount. This strategy brings about bigger payload limit and high picture quality. Another strategy which makes utilization of all the more encompassing pixels around an objective pixel to locate the most proper limit an incentive keeping in mind the end goal to enhance subtlety was presented [17]. As contrast with other steganographic methods which utilize either three or four adjoining pixels around an objective pixel, this strategy can use each of the eight nearby neighbors, which enhances the impalpability esteem.

## 7. Conclusion

Steganography is the workmanship and art of composing concealed messages such that nobody, aside from the sender and proposed beneficiary, associates the presence with the message. This paper looked into the fundamental steganographic methods. Each of these systems tries to fulfill the three most critical components of steganographic plan (subtlety or imperceptibility, limit, and strength). LSB systems in a spatial space have a high payload limit, yet they regularly neglect to counteract measurable assaults and are along these lines effortlessly distinguished. The promising strategies, for example, DCT, DWT and the versatile steganography are not inclined to assaults, particularly when the concealed message is little. They alter the coefficients in the change area, along these lines brings about least picture twisting. By and large, such methods have a tendency to have a lower

payload when they are contrasted with the spatial area calculations. The tests on the discrete cosine change (DCT) coefficients have presented some encouraging outcomes and afterward they have redirected the scientists' consideration towards JPEG pictures. Working at some level like that of DCT turns steganography considerably more capable and less inclined to factual assaults. Inserting in the DWT space uncovers a kind of valuable outcomes and outflanks DCT installing.

## 8. References


[1] J.R. Krenn, "Steganography and Steganalysis",January 2004.Deshpande Neeta, KamalapurSnehal, Daisy Jacobs, "Implementation of LSB Steganographyand its Evaluation for VariousBits", 2004.

[2] K.B.Raja, C.R.Chowdary, Venugopal K.R, L.M.Patnaik, "A Secure Image Steganography using LSB, DCT and Compression Techniques on RawImages", IEEE-0-7803-9588-3/05/$20.00 ©2005.

[3] Vijay KumarSharma, Vishalshrivastava, "ASteganography Algorithm for Hiding Images by improved LSB substitution by minize detection." Journal of Theoretical and Applied Information Technology, Vol. 36 No.1, ISSN: 1992-8645,15thFebruary 2012.

[4] Po-Yueh Chen and Hung-Ju Lin, "A DWT Based Approach for Image Steganography", International Journal of Applied Science and Engineering 4, 3:275-290, 2006.

[5] Chen Ming, Zhang Ru, NiuXinxin, Yang Yixian,"Analysis of Current Steganography Tools:Classifications & Features",International Conferenceon Intelligent Information Hiding andMultimedia Signal Processing (IIH-MSP'06),IEEE-0-7695-2745-0/06 $20.00 © 2006.

[6] AneeshJain,IndranilSen. Gupta, "A JPEGCompression Resistant Steganography Scheme forRaster Graphics Images",IEEE-1-4244-1272-2/07/$25.00©2007.

[7] BeenishMehboob and Rashid Aziz Faruqui, "ASteganography Implementation", IEEE -4244-2427-6/08/$20.00 ©2008.

[8] Hassan Mathkour, Batool Al-Sadoon, AmeurTouir,"A New Image Steganography Technique",IEEE-978-1-4244-2108-4/08/$25.00 © 2008.

[9] NageswaraRaoThota, Srinivasa Kumar Devireddy,"Image Compression Using Discrete CosineTransform",Georgian Electronic Scientific Journal:Computer Science and Telecommunications, No.3(17), 2008.

[10] MamtaJuneja,Parvinder Singh Sandhu, "Designingof Robust Image Steganography Technique Basedon LSB Insertion and Encryption", InternationalConference on Advances inRecent Technologies in Communication and Computing, 2009.

[11] Dr. EktaWalia, Payal Jain, Navdeep, "An Analysis ofLSB & DCT based Steganography", Global Journal of Computer science & technology, Vol. 10 Issue 1(Ver 1.0), April 2010.

[12] K.B.ShivaKumar,K.B.Raja, R.K.Chhotaray,SabyasachiPattnaik, "Coherent Steganography5967-4/10/$26.00 ©2010.

[13] K Suresh Babu, K B Raja, Kiran Kumar K, ManjulaDevi T H, Venugopal K R, L M Patnaik,"Authentication of Secret Information in Image Steganography" .

[14] Arvind Kumar, Km. Pooja, "Steganography-A DataHiding Technique",International Journal ofComputer Applications (0975 –8887), Volume 9,No.7, November 2010.

[15] Atalla I. Hashad,Ahmed S. Madani, "A RobustSteganography Technique Using Discrete CosineTransform Insertion".

[16] Vijay Kumar, Dinesh Kumar, "PerformanceEvaluation ofDWT Based Image Steganography",IEEE-978-1-4244-4791-6/10/$25.00_c 2010.

[17] Ali Al-Ataby and Fawzi Al-Naima, "A Modified HighCapacity Image Steganography Technique Basedon Wavelet Transform" The International ArabJournal of Information Technology, Vol. 7, No. 4,October 2010.

[18] T. Narasimmalou, Allen Joseph .R, "OptimizedDiscrete WaveletTransform based Steganography",IEEE International Conference on AdvancedCommunication Control and Computing Technologies(ICACCCT),2012.

[19] NedaRaftari and Amir MasoudEftekhariMoghadam, "Digital Image Steganography Basedon Assignment Algorithm and Combination of DCTIWT",Fourth International Conference on ComputationalIntelligence, Communication Systems andNetworks, 2012.

[20] AnkitaSancheti, "Pixel Value Differencing ImageSteganography Using Secret Key"InternationalJournal of Innovative Technology and ExploringEngineering(IJITEE), ISSN: 2278-3075, Volume-2,Issue-1 and December 2012.

[21] NehaBatra&PoojaKaushik, "Implementation ofModified 16×16 Quantization Table Steganographyon Color Images", InternationalJournal of AdvancedResearch in Computer Science and SoftwareEngineering,ISSN: 2277 128X,Volume2, Issue 10,October 2012.

[22] ElhamGhasemi, JamshidShanbehzadeh, NimaFassihi, "High Capacity Image Steganography usingWavelet Transform and Genetic Algorithm", proceedings of international multi conference of engineers & computer science, IMECS-VolumeI, March 16-18, 2011.

[23] Gurmeet Kaur and Aarti Kochhar, "A Steganography Implementation based on LSB &DCT", "International Journal for Science and Emerging, Technologies with Latest Trends" 4(1),ISSN No. (Online): 2250-3641, ISSN No. (Print):2277-8136, 35-41 (2012).