Security for Color Image with Message using Steganography and Watermarking Technique

Gaurav Gadge[1], Prof. Satyarth Tiwari[2]
M. Tech. Scholar, Department of Electronics and Communication, Bhabha Engineering Research Institute, Bhopal[1]
Guide, Department of Electronics and Communication, Bhabha Engineering Research Institute, Bhopal[2]

Abstract— In the normal feeling of the world, the word 'security' signifies the condition of being safe and the measures taken to guarantee security. In any case, wellbeing isn't an objective or an outright thing in light of the fact that regardless of utilizing a considerable lot of the security systems accessible there is no 100 percent security. Individuals have been making and utilizing numerous wellbeing strategies since antiquated occasions to secure their lives. Before, just things with physical nearness required insurance and security (physical security); for instance: a house was utilized to get security against the brutality of nature, watches were utilized to secure spots, and weapons were utilized to ensure people, watchtowers, doors, channels, locks, and different types of insurances. This paper present digital watermarking (DW) and steganography based secured technique to secure the text and image. The proposed technique is implemented MATLAB software and calculates MSE and PSNR.

Keywords— DST, SVD, PSNR, MSE

I. INTRODUCTION

With the popularization of the Internet of things (IoT) and various artificial intelligence-enabled smart devices, a large volume of digital data is stored and shared on open platforms such as LinkedIn, Facebook, Twitter, and Flickr [1]. Images are the most frequently used data-sharing method on these platforms [2]. However, research show that data sharing may bring issues of privacy leakage, copyright protection, identity theft, and vulnerable data, which can be tampered by intruders [3]. Color image watermarking is a commonly used method to protect media content by invisibly concealing a secret mark or marks into the host media. This advantage makes watermarking appropriate for various practical applications such as smart healthcare, judicial imaging, privacy protection, military communication, broadcast monitoring, chip and hardware security, practices in the insurance and movie industries, etc. [4]. A popular set of watermarking applications are shown in Fig. 1. Compared with similar schemes such as cryptography, steganography, and digital rights management, watermarking [5] is the most useful for digital data security. Table 1 summarizes the differences between the related concepts. There are three mutually restricted properties in a watermarking scheme: invisibility, robustness, and watermark capacity, between which a good relationship is hard to maintain. Although security and computational complexity are other significant properties, it is very hard to achieve along with other properties of a watermarking scheme.

Two essential strategies are accessible to secure the information and data in transmission state or instead of changeless stockpiling: Cryptography and Steganography, Cryptography is a strategy used to change the characters structure from the clear structure to mixed up structure, in this system the interloper can know whether there is figure content or then again not on the grounds that the characters are adjusted [4]. Steganography is a method used to conceal the characters or any media in other media, in this strategy the interloper can't know whether there is a figure content or not on the grounds that the characters are covered up in other media, so unapproved client can't see the characters in light of the fact that the characters are installed in another media. Steganography is known as "undetectable" correspondence [5], in light of the fact that it hides a media in other media.

Steganography is a concealing media process over secured media and fundamental target is to impart and move significant data from one spot to another in a safe secure and imperceptible way. Actually importance writing in a spread is the act of concealing messages inside different messages so as to disguise the presence of the first. Steganography demonstrates to the mystery message or any computerized media record which has been covered up inside another computerized media document like picture, content, video or sound record [5].

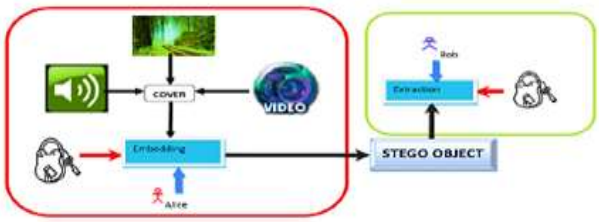

Figure 1: General schematic description

Steganography is a helpful procedure for concealing information behind the transporter record such as picture, sound, video and so forth and that information safely moved from sender to recipient. Cryptography is likewise another method which is utilized for securing data. Joining encryption strategies for cryptography and steganography empowers the client to transmit data which is concealing within a document on display. This will give greater security to moving information [6] Cryptography and Steganography are the most generally

utilized for mystery interchanges. Steganography is a science and craftsmanship to shroud mystery information in other information.

Be that as it may, Cryptography is likewise science and workmanship to of changing the information structure from comprehensible to confused structure. At the end of the day, Steganography is a concealing procedure of the information in other information, while Cryptography is a changing appearance procedure to change the information from discernible and significant to mixed up and meaningful [7].

Cryptography method is separated into two principle systems. Symmetric skeleton cryptanalysis and Asymmetric skeleton cryptanalysis is present. In Symmetric key cryptanalysis, there is just one key which is utilized by the sender to vicissitude over the flatland gratification to figure gratification and in the opposite side a similar key is utilized by the recipient to change over the figure gratification into flatland message [8], so the key is mystery and shared between the sender and the recipient. In Asymmetric skeleton cryptanalysis, there are two distinctive skeleton, a skeleton(s) is utilized by the sender to change over the plain message into the figure gratification and an alternate key(s) is utilized by the recipient to change over the figure gratification into the flatland message [9].

II. STEGANOGRAPHY USING LSB ALGORITHM

This Algorithm shrouds the mystery message in the Least Significant Bit (LSB) as per the accompanying advances:

- The initial seven bits of the LSB are the Steganography procedure type, in light of the fact that this calculation is the principal strategy the Steganography type is (1), the number (1) is spoken to in twofold esteem by seven bits to be (0000001). This double esteem is inserted in the initial seven bits of the LSB of the picture pixels.

- The twenty bits of the mystery message after the seven bits in the LSB are spoken to the mystery message length (from the eighth situation to 27th position). For instance, the mystery message length is (950 bits), it is spoken to by twenty bits as (00000000001110110110). The greatest size of the mystery message length is (11111111111111111111) that mean (1048575) bits or (149796) characters [10].

The steganography method involves masking concealed data into every single pixel's LSB in an image. Built on the LSB procedure, an 8 or 24-bit color image algorithm is established to boost the stego-image accuracy of the color object proficient in generating a hidden concealed object that is fully imperceptible to the human eye [1]. The small, important parts of each pixel can be employed to entrench the hidden communication in the concealment medium. This approach increases adjustment sensitivity but degrades the stego image quality [4].The LSB entrenching procedure implies that images could be concealed in the LSB of the concealment object so that the people's vision won't detect the concealed image in the concealment object [5]. This approach could as well be employed to conceal text in 24-bit or 8-bit or grayscale form. This research was, however, used to embed medical information into color cover file formats such as .bmp,.png, and .jpeg using a modified LSB steganography technique called Circular Shift LSB steganography algorithm. This paper also presents comprehensive LSB-built image steganography knowledge in various image forms.

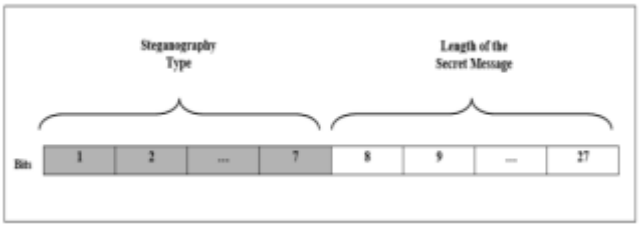

Figure 2: The reserved bits of the image Steganography using LSB algorithm

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
1	0	1	1	0	0	1	0	0	0	1	0	0	1	1	1	1	1	0	1	0	1	1	1

Figure 3: Steganography using LSB to hide the text "WHO"

III. PROPOSED METHODOLOGY

Watermarking Embedding procedure:

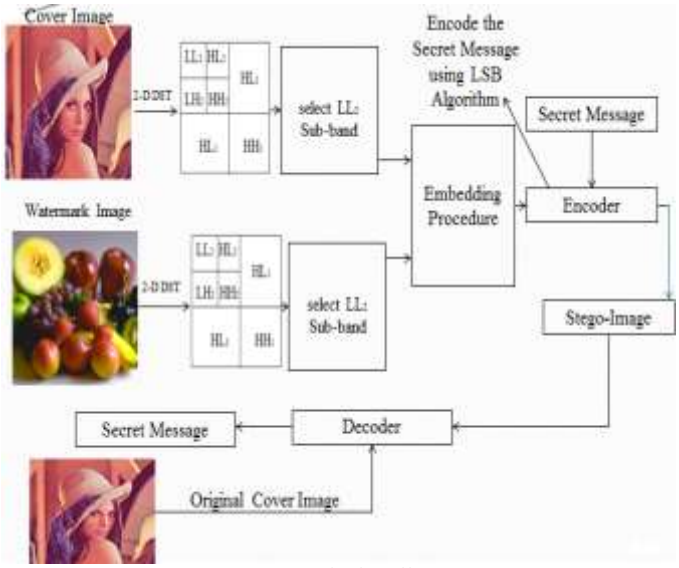

Figure 4: Flow Rough Draft of Proffered Manner

Contrivance for Watermark Ingrain

Step 1: Input Spread Oneself image, Take cover image (CI).

Step 2: Apply 2-D DST on CI to disintegrate it into four standby-bands.
Step 3: Eclectic standby-band LL2 of CI.
Step 4: Take watermark image (WI)
Step 5: Apply 2-D DST on WI to disintegrate into four standby -bands.
Step 6: Eclectic standby -band LL2 of WI.
Step 7: Embedding Process
Step 8: Enter Secret Message
Step 9: Apply LSB technique for Encoder
Step 10: Find Stego Image
Step 11: Apply Decoder Process
Step 12: Finally get secret message and watermarked image

IV. SIMULATION TOOL

MATLAB is a significant level specialized registering language and calculation advancement instrument that can be utilized in a few applications, for example, information perception/investigation, numerical examination, signal handling, control structure, and so forth.
The mean square error (MSE) is defined as,

$$MSE = \frac{1}{MN}\sum_{R=1}^{S}\sum_{C=1}^{S}[O(R,C) - I(R,C)]^2 \quad (1)$$

Where O(R, C) is the output image and I (R, C) is the input image, R: Row and C: Column
The peak signal to noise ratio (PSNR) is defined as

$$PSNR = 10\log_{10}\frac{S \times S}{MSE} \quad dB \quad (2)$$

Where S is size of row and column in original image.

V. SIMULATION RESULT

The first picture of 512×512 pixel worth is appeared in figure 5.6. This consider partitioned along with four sections. In initial segment the first arbitrary picture is resize of the 512×512, the resize picture is going through the 2-D discrete shearlet transform (DST) and get low recurrence picture is going to installing process. Second part demonstrates the watermark picture 512×512 pixel esteem, the watermark picture is going through the 2-D DWT and get low recurrence watermark picture is going to inserting process. Unique picture and watermark picture are going through the implanting preparing and get without commotion assault watermarked picture appeared in third part.

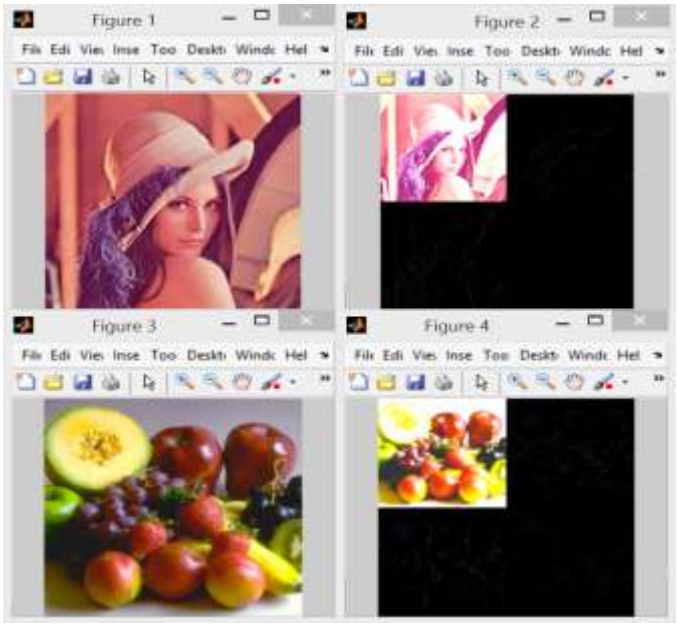

Figure 5: Original Color and Watermark Image

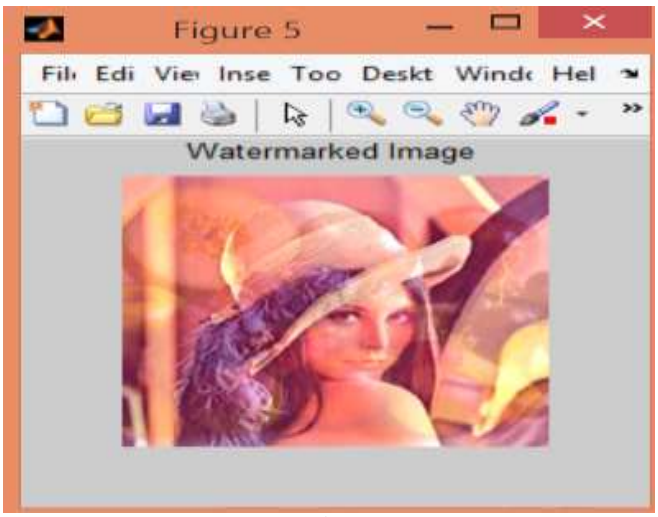

Figure 6: Embedding Processing of Watermark and Original Image

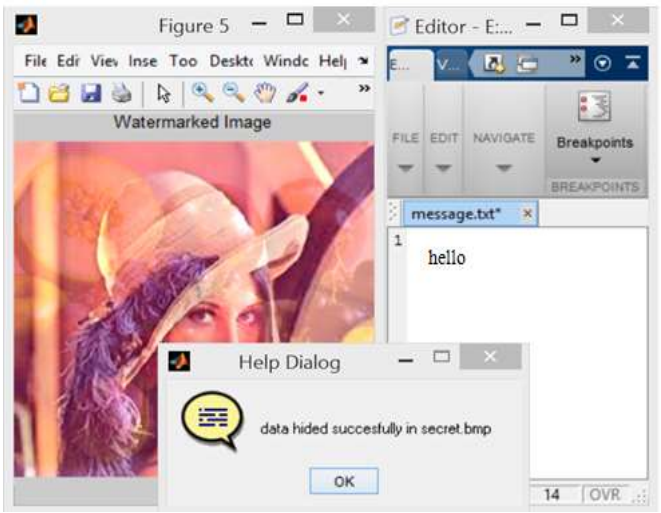

Figure 7: Data Hidden for Watermarked Image using Embedding LSB Stenography Technique

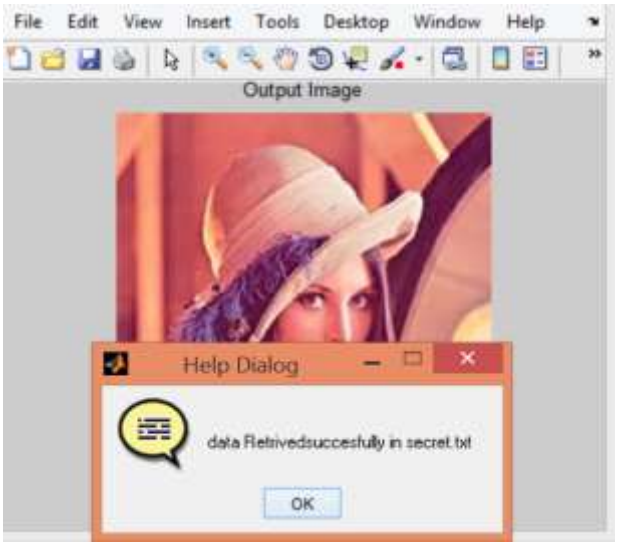

Figure 8: Received Output Image with Retrieved Message

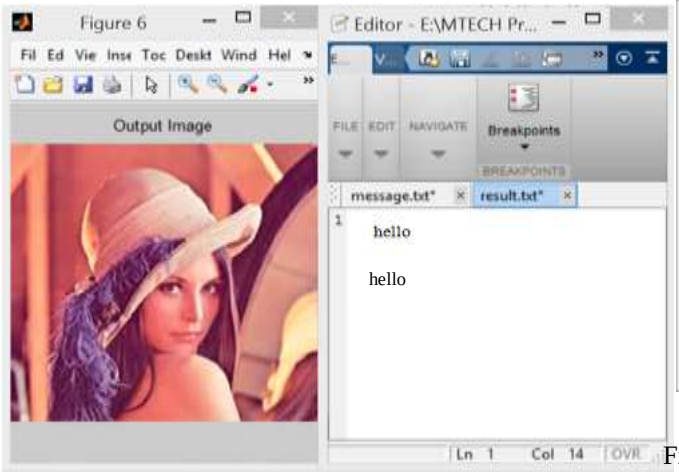

Figure 9: Received Message

Table I: Comparison Result for PSNR (dB)

	Previous Algorithm		Proposed Algorithm
Image	**DCT Technique**	**SVD Technique**	**DST-SVD Technique**
Lena Image	42.65	41.24	61.959
Baboon Image	41.37	38.89	58.618
Pepper Image	42.65	41.38	54.242

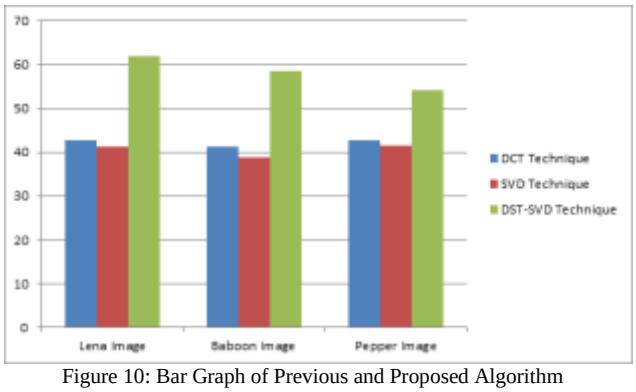

Figure 10: Bar Graph of Previous and Proposed Algorithm

Figure 10 demonstrates the graphical representation of the presentation of proposed strategy talked about in this exploration work in term of PSNR. From the above graphical portrayal it very well may be gathered that the proposed calculation gives the best execution for Lena pictures.

Table II: Comparison Result for MSE

	Previous Algorithm		Proposed Algorithm
Image	**DCT Technique**	**SVD Technique**	**DST-SVD Technique**
Lena Image	0.0056	0.0036	0.0017
Baboon Image	0.0049	0.0032	0.0014
Pepper Image	0.0073	0.0029	0.0012

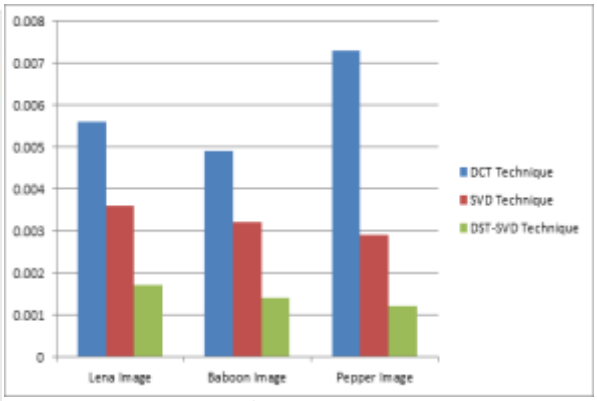

Figure 11: Bar Graph of Previous and Proposed Algorithm

Figure 11 demonstrates the graphical representation of the presentation of proposed strategy talked about in this examination work in term of MSE. From the above graphical portrayal it very well may be construed that the proposed calculation gives the best execution for Pepper pictures.

VI. CONCLUSION

It has been shown that the usage of DST-LSB with mix procedure has rehabilitated the safekeeping of the watermarking plan. Explicit thought is inclined to the proposed arrangement to guaranty impregnable watermark fasten and straightforward extrication. A comparison between the PSNR and MSE got from this study was compared and the result was also evaluated with previous concealment image formats used by other researchers. The following outcomes were deduced from this study: Firstly, it was illustrated that this modified LSB method called circular shift algorithm performed better than previous researches when compared with them. Secondly, it was deduced that concealment image with .png format is more robust in masking textual information that is it hides textual information better when compared with other image formats because it had the highest PSNR and the lower MSE which are the two metrics used in evaluating the performance of the system.

REFRENCES

[1] Wenguang He, Zhanchuan Cai and Yaomin Wang, "High-fidelity Reversible Image Watermarking Based on Effective Prediction Error-Pairs Modification", IEEE Transactions on Multimedia, IEEE 2020.

[2] Awdhesh K. Shukla, Akanksha Singh, Balvinder Singh and Amod Kumar, "A Secure and High-Capacity Data-Hiding Method using Compression, Encryption and Optimized Pixel Value Differencing", IEEE Access, October 8, pp. 51130-51139, 2018.

[3] A. Bose and S. P. Maity, ''Spread Spectrum Image Watermark Detection on Degraded Compressed Sensing Measurements with Distortion Minimization,'' Multimedia Tools Appl., vol. 77, no. 16, pp. 20783–20808, Aug. 2018.

[4] Nazir A. Loan, Nasir N. Hurrah, Shabir A. Parah, Jong Weon Lee, Javaid A. Sheikh, and G. Mohiuddin Bhat; Secure and Robust Digital Image Watermarking Using Coefficient Differencing and Chaotic Encryption; Information Security Solutions for Telemedicine Applications, Vol. 6. No. 3. pp. 19876-19 897. IEEE, 2018.

[5] Baharak Ahmaderaghi, Fatih Kurugollu, Jesus Martinez Del Rincon, Ahmed Bouridane; Blind Image Watermark Detection Algorithm based on Discrete Shearlet Transform Using Statistical Decision Theory; IEEE Transactions on Computational Imaging, Vol. 4, No. 1. pp. 46–59. IEEE, 2018.

[6] W.-H. Ko B. Satchidanandan P. R. Kumar; Theory and implementation of dynamic watermarking for cybersecurity of advanced transportation systems; Proc. IEEE Conf. Commun. Netw. Security (CNS) pp. 416-420, IEEE 2016.

[7] M. Hosseini T. Tanaka V. Gupt; Designing optimal watermark signal for a stealthy attacker; Proc. Eur. Control Conf. (ECC) pp. 2258-2262 Jun. 2016.

[8] Ahmed, F. and Moskowitz, I.S.; Composite Signature Based Watermarking for Fingerprint Authentication; ACM Multimedia and Security Workshop, pp. 137-142. 2005.

[9] Y.-H. Fung and Y.-H. Chan; Tone-dependent noise model for high-quality halftone; Journal Electron. Image, Vol. 22, No. 2, IEEE 2013.

[10] Bidyut Jyoti Saha, Kunal Kumar Kabi and Arun; Non Blind Watermarking Technique using Enhanced One Time Pad in DWT Domain; International Conference of Digital Signal and Processing, IEEE, 2014.

[11] M. Kim, D. Li, S. Hong; A Robust Digital Watermarking Technique for Image Contents based on DWT-DFRNT Multiple Transform Method; International Journal Multimed. Ubiquitous Eng., Vol. 9. No. 1, pp. 369-378, 2014.

[12] Baharak Ahmaderaghi , Jesus Martinez Del, Rincon Fatih, Kurugollu Ahmed Bouridane; Perceptual Watermarking for Discrete Shearlet Transform; 5th European Workshop on Visual Information Processing (EUVIP), IEEE, 2014.

[13] Jiann-Shu Lee and Fei-Hsiang Huang; A New Image Watermarking Scheme using Non-dominated Sorting Genetic Algorithm II; International Symposium on Biometrics and Security Technologies, IEEE, 2013.