Security for Image with Message using Watermarking and Steganography Technique

Deepali Paswan[1], Prof. (Dr.) Vikas Gupta[2]
M. Tech. Scholar, Department of Electronics and Communication, TIT, Bhopal[1]
Prof. & Head, Department of Electronics and Communication, TIT, Bhopal[2]

Abstract— Increased Internet usage and the availability of high-speed digital data networks have induced exponential growth of online transmission and distribution of multimedia content over the Web. Security, authentication, and copyright protection of multimedia data have become a major concern, because it can be duplicated, modified, and re-transmitted easily. Watermarking is a mechanism to address these issues by embedding copyright information, slightly altering the content in such a manner that the change is unnoticeable to the human visual system. The embedded information can be detected and extracted at any time for authentication, ownership identification, copy protection, and control. The application of chaotic systems in digital watermarking schemes enhance the security in an efficient way due to the inherent properties of sensitivity to initial conditions and parameters, topological transitivity, and periodic point of chaotic systems. Imperceptibility and robustness are two primary contradicting characteristics by which watermarking algorithms are evaluated. 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— DWT, SVD, PSNR, MSE

I. INTRODUCTION

Information Security, also known as InfoSec, is the practice of protecting the information from unauthorized access, modification, destruction and disruption. In the recent years, there has been a tremendous increase in the use of online systems for every need from utility bill payments, online shopping to Income-Tax filing. There are lot of secure information travelling around the internet and the sophistication and persistence of cyber-attacks on these online data keeps growing. There has been an alarming increase in data theft as a result of these sensitive private data travelling around the web. As the attack on the sensitive online data increases, so do government regulations to protect the data. Therefore, data or information security is no longer optional but has become an essential factor. There are various techniques or approaches currently being used for protecting data, like whole database encryption, Database column encryption, Application level encryption and Shuffling. The traditional or conventional approaches to data protection have many weaknesses like heavy implementation cost, no security within networks and applications, weak or breakable encryption. The weaknesses in the conventional approach to data protection lead to 'The Data-centric Approach'. This approach targets to directly protect the data rather than the devices and storage areas of the organization. The security is built into the data itself and the data is protected as soon as it is acquired and stays in the protected form, irrespective of the subsystem that uses it. Information is always protected, when stored in the database or when transferred to another system through network. The data is decrypted and processed, only when applications require it. The Data-centric approach uses Encryption, Tokenising and Masking techniques to protect data. According to John Kindervag, Senior Analyst, Forrester Research, "Encrypting or tokenizing data is the future of data security. These technologies effectively "kill" data-making it useless to the attackers. Cybercriminals cannot monetize tokenized or encrypted data. Further, breached data that a security professional has tokenized or encrypted may not be subject to state or industry breach laws or regulations."

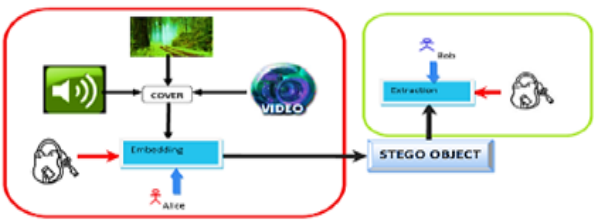

Figure 1: General schematic description

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.

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.

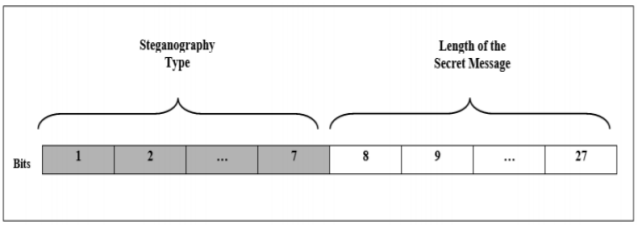

Figure 2: The reserved bits of the image Steganography using LSB algorithm

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

DWT-singular value decomposition (SVD)-based hybrid watermarking technique has been developed by Lai & Tsai (2010). In this scheme, the cover image is decomposed using single-level Haar DWT, and vertical-level frequency (LH) and horizontal-level frequency (HL) sub-bands are chosen for watermark embedding. The watermark image is divided into two parts, which are embedded into these two sub-bands following separate computation of the SVD of the two parts so as to obtain the watermarked image. The robust semi-blind reference watermarking scheme introduced by Bhatnagar & Raman (2009a) is based on DWT and SVD. In this method, a reference image is obtained from the original image by applying n-level DWT decomposition and calculating the directive contrast of all high-frequency components. SVD is applied to the reference image as well as the watermark image, so as to obtain the reference watermarked image. Finally, the watermarked image is obtained by updating the selected sub-band of the host image by matching with the subband of the reference watermarked image.

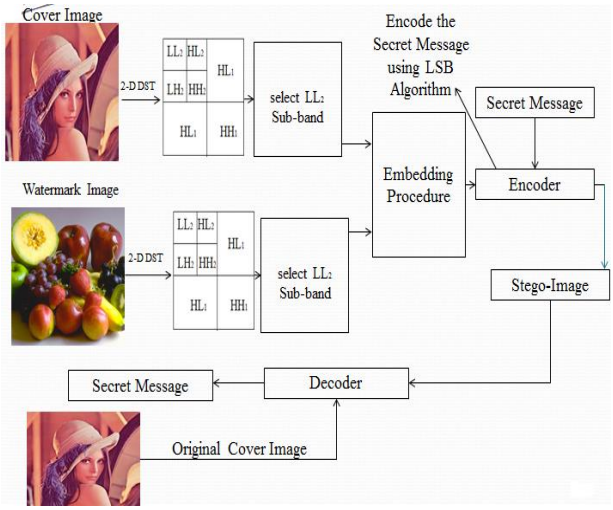

Figure 4: Flow Rough Draft of Proffered Manner

DWT

DWT is a commonly used transformation in watermarking algorithms. Kashyap & Sinha (2012) have proposed a robust image watermarking algorithm using the DWT for copyright protection. In this scheme, the 3rd -level low-frequency (LL) sub-band of the watermark image is embedded in the 3rd -level LL sub-band of the cover image using the alpha blending technique. Those authors demonstrated that the algorithm exhibits superior performance when applied to the 3rd level, compared to 2nd -level and 1st -level DWT. A DWT-based watermarking scheme has also been developed by Daren et al. (2001), in which watermark sequences are first embedded in the LL sub-bands, followed by embedding of the remaining sequences in the high-frequency (HH) sub-bands. Those researchers have reported that different embedding formulas should be applied to each of the sub-bands. Further, strong watermarks can be embedded

into the LL sub-bands as they have larger perceptual capacity than HH sub-bands.

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 wavelet transform (DWT) 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.

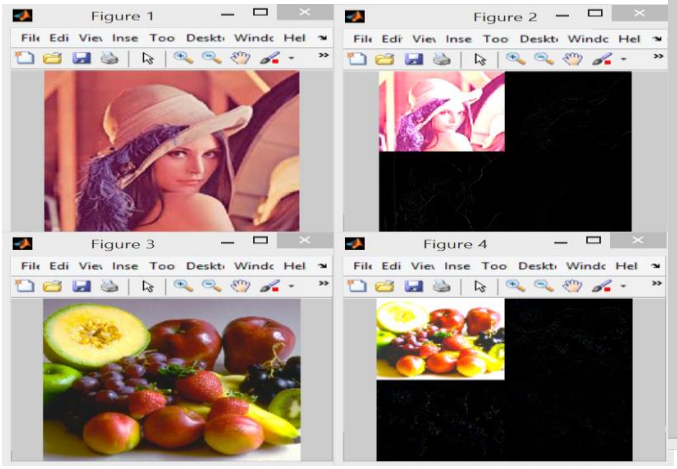

Figure 5: Original Color and Watermark Image

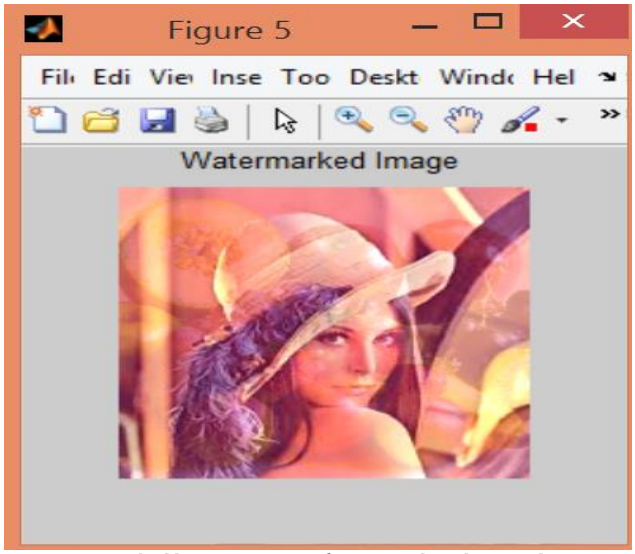

Figure 6: Embedding Processing of Watermark and Original Image

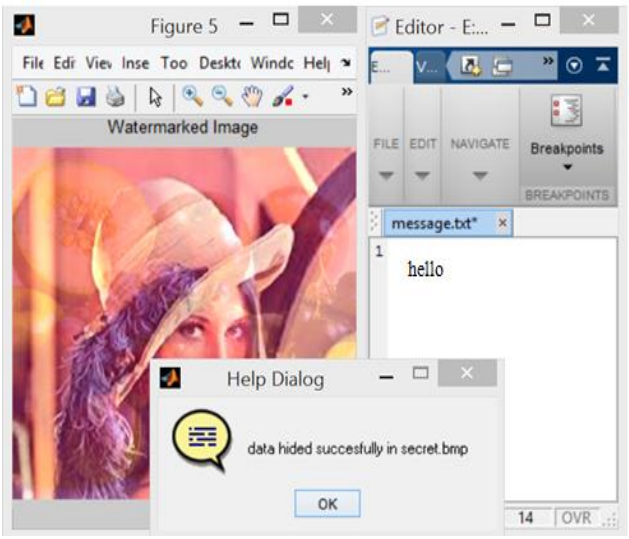

Figure 7: Data Hidden for Watermarked Image using Embedding LSB Stenography Technique

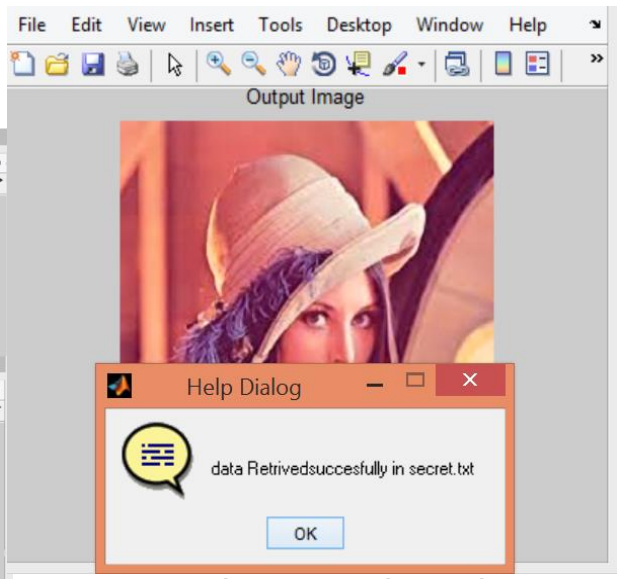

Figure 8: Received Output Image with Retrieved Message

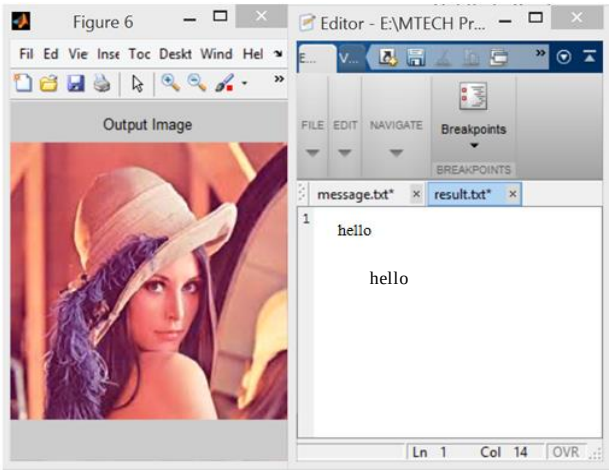

Figure 9: Received Message

As shown in table 1 the PSNR, MSE, NAE and computation time result are obtained for the proposed DWT-SVD technique. From the analysis of the results, it is found that the proposed DWT-SVD technique gives superior performances.

Table 1: Result for Different Image in Without Noise Attack

Image	PSNR (dB)	MSE	NAE	Computation Time (ns)
Lena Image	35.289	77.561	18.652	4.674
Flower Image	44.206	12.334	2.376	4.682
Home Image	34.069	28.519	10.005	4.093
Sky Image	34.436	94.581	25.512	4.532

The proposed DWT-SVD technique gives a highest PSNR 35.289 dB for Lena image and lower PSNR 33.862 dB for Sky image.
As shown in table 2 the peak signal to noise ratio (PSNR) result is obtained for the proposed DWT-SVD technique. From the analysis of the results, it is found that the proposed DWT-SVD technique gives superior performances for Home image. The proposed algorithm is gives 57.993 for Home image at 0.01 noise density and 45.032 for flower image at 0.05 density.

Table 2: Result for Lena Image in Gaussian Noise Attack

PSNR (dB)				
Noise Density	Lena Image	Flower Image	Home Image	Sky Image
0.01	56.432	57.321	57.993	56.932
0.02	54.942	55.032	54.065	53.904
0.03	51.903	53.032	51.435	50.905
0.04	47.903	49.954	47.043	46.903
0.05	44.932	45.032	44.903	43.904

As shown in table 3 the peak signal to noise ratio (PSNR) result is obtained for the proposed DWT-SVD technique. From the analysis of the results, it is found that the proposed DWT-SVD technique gives superior performances for Home image. The proposed algorithm is gives 57.993 for Home image at 0.01 noise density and 45.032 for flower image at 0.05 density.

Table 5.3: Result for Lena Image in Salt and Pepper Noise Attack

PSNR (dB)				
Noise Density	Lena Image	Flower Image	Home Image	Sky Image
0.01	55.743	55.032	54.943	55.932
0.02	53.965	52.987	51.032	51.432
0.03	51.982	50.321	49.032	48.032
0.04	48.932	47.043	46.032	45.983
0.05	44.098	44.932	43.904	43.321

VI. CONCLUSION

It has been shown that the usage of DWT-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. Information Security is a methodology and technique practiced for securing the confidential data that is being transmitted across the insecure anonymous network. It makes the data more secure from different active and passive attacks that constantly happen during transmission. Nowadays Internet is the fast and effective way of communication in this digital era. With the growth of technology, Internet has become less expensive and easily accessible that makes it more vulnerable to malicious intruders.

REFRENCES

[1] Seddeq. E. Ghrare, A. Adim Mohamad Alamari and Hajer Abdulhkim Emhemed, “Digital Image Watermarking Method Based on LSB and DWT Hybrid Technique”, IEEE 2nd International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA), IEEE 2022.

[2] 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”, Received January 4, 2018, accepted February 7, 2018, date of publication March 16, 2018, date of current version April 25, 2018.

[3] 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, Volume: 4 , Issue: 1, Page s: 46 – 59, IEEE 2018.

[4] Aleksei Zhuvikin, "Selective Image Authentication using Shearlet Coefficients Tolerant to JPEG Compression", Page s: 681 – 688, IEEE 2017.

[5] Etti Mathur and Manish Mathuria, "Unbreakable Digital Watermarking using combination of LSB and DCT", International Conference on Electronics, Communication and Aerospace Technology ICECA 2017.

[6] Morteza Heidari1, Nader Karimi, and Shadrokh Samavi, "A Hybrid DCT-SVD Based Image Watermarking Algorithm", Iranian Conference on Electrical Engineering (ICEE), IEEE 2016.

[7] N. Senthil Kumaran, and S. Abinaya, "Comparison Analysis of Digital Image Watermarking using DWT and LSB Technique", International Conference on Communication and Signal Processing, April 6-8, 2016, India.

[8] Ranjeet Kumar Singh, Dilip Kumar Shaw and M. Javed Alam," Experimental Studies of LSB Watermarking With Different Noise", Eleventh International Multi- Conference on Information Processing-2015 (IMCIP-2015).

[9] 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.

[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. ICCCNT. 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. Ubiauitous Eng.*, vol. 9, no. 1, pp. 369-378, Jan. 2014.

[12] 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.

[13] Baloshi Mathews and Madhu S. Nair, "Modified BTC Algorithm for Gray Scale Images using max-min Quantizer", Automation, Computing, Communication, Control and Compressed Sensing, PP. 01-05, 2013 IEEE.

[14] Wang Santosh, U. V. S. Sitarama Varma, K. S. K Chaitanya Varma, Meena Jami, V. V. N. S Dileep, "Absolute Moment Block Truncation Coding For Color Image Compression," International Journal of Innovative Technology and Exploring Engineering (IJITEE), Volume-2, Issue-6, PP. 53-59, May 2013.

[15] Lee, J. S., Huang, F. H., & Kuo, H. C., "A New Image Watermarking Scheme Using Non-dominated Sorting Genetic Algorithm II," In Biometrics and Security Technologies (ISBAST), International Symposium, pp. 56-61, IEEE 2013.