IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-11, Nov 2018 E-ISSN: 2347-2693

High Security Text and Image Message for Steganography and Watermarking Through Modified Least Significant Bits Technique

Bhawna Ahirwar[1*], Sanjay K. Sharma[2]

[1]M. E. Scholar, Department of Electronics and Communication, UIT-RGPV, Bhopal, India
[2]Department of Electronics and Communication, UIT-RGPV, Bhopal, India

Available online at: www.ijcseonline.org

Accepted: 18/Nov/2018, Published: 30/Nov/2018

***Abstract*—**"Steganography" is a technique that thwarts unauthorized users to have access to the crucial data, to invisibility and payload capacity using the different technique like discrete cosine transform (DCT) and discrete shearlet transform (DST).The available methods till date result in good robustness but they are not independent of file format. The aim of this research work is to develop a independent of file format and secure hiding data scheme. The independent of file format and secure hiding data scheme is increased by combining DST and least significant bits (LSB) technique. Accordingly an efficient scheme is developed here that are having better MSE and PSNR against different characters.

***Keywords*—** Discrete Shearlet Transform, SVD, PSNR, MSE

I. INTRODUCTION

Recent growth of digital image content over internet has increased the need for the protection of digital media. The image transmitted through internet and wireless communication channels can suffer various threats. One of the major threats is the threat of confidentiality. This threat represents the possibilities of accessing the audio data via unauthorized channels. Another issue is the threat of integrity, where the resource can be altered, by unauthorized entities, without any detection. Threat of availability is possession of a confidential audio content through some illicit channels. Various other threats include replication of digital data without any information loss and manipulations of the same without any detection. A feasible solution is required, for telecommunication, consumer electronics and information technology industries, to provide secure transmission of content without sacrificing their security rights [1]. Emerging technologies for audio security has three main objectives: secure content transmission, authentication of audio information and copy control to protect audio data from illegal distribution and theft [2]. Cryptography has been established as a technology of fundamental importance for securing digital transfers of data over unsecured channels. By providing encryption of digital data, cryptography enables trustworthy point-to-point information exchange and transactions. Once the recipient validates and decrypts the data, the product can be subsequently stripped from any content identification, proof-of-ownership or other descriptive information. This might lead to further duplication and re-distribution leaving the rights holders powerless and royalty-less [3]. To enhance the security of audio data, digital watermarking and steganography techniques complement cryptography for protecting content even after it is deciphered [4].

The study of multimedia security [5] therefore includes not just encryption but also watermarking and steganography. Steganography and Watermarking almost interchangeably, refers to hiding secondary information into the primary multimedia source. The primary multimedia sources can be audio, image, and video. There are unique techniques associated with each type of primary perceptual sources depending on their inherent redundancy and perceptual properties. These techniques have been proposed as alternative methods to enforce the intellectual property rights and protect digital media from tampering [6]. In this thesis work the primary multimedia source is image.

The word steganography was originated from Greek which means covered writing. Steganography is the oldest form of covert channel. A famous illustration of steganography is Simmons' Prisoners' Problem [7]. Audio Steganography is the act of embedding a secret message within a larger message so that others cannot discern the presence of the secret message [8]. Steganography can be used to hide a message intended for later retrieval by a specific individual or group. Audio watermarking involves a process of embedding into host audio signal a perceptually transparent digital signature, carrying a message about the host data in order to mark its ownership. The aim in watermarking systems is to ensure the robustness of the hidden message; the presence of the embedded message itself does not have to be secret [9].

The watermark is always present in the signal, even in illegal copies of it and the protection that is offered by the watermarking system is therefore of a permanent kind. Although the process of watermark embedding and steganography are similar, there are some basic differences between the two techniques. Steganography methods assume that the existence of the covert communication is unknown to third parties and are mainly used in secret one-to-one communication between authorized users. On the other hand, watermarking is to hide message in one-to-many communications. Steganography methods usually do not need to provide strong security against removing or modification of the hidden message. Whereas, watermarking methods need to be very robust to attempts to remove or modify a hidden message.

II. DIGITAL WATERMARKING

Watermarking basically refers to information hiding. Information or digital signal in the form of images, audio, video or text is hidden or inserted. This information to be hidden is termed as Watermark. The watermark can be hidden in cover/host/carrier signal. The host popularly can be text file, image, audio file or video file. Depending on the type of host, watermarking can be categorized as:

- Text watermarking
- Digital image watermarking,
- Digital audio watermarking and
- Digital video watermarking

To have efficient copyright protection, watermarking algorithms must possess certain characteristics. Depending on the application requirement different characteristics can be primary objectives. The most desirable characteristics [2] are listed below:

Robustness- Robustness refers to difficulty in removing or destroying watermark from host image when watermarked image is subjected to image processing attacks.

Imperceptibility- Imperceptibility dictates the inability to notice the existence of watermark in host image and retained visual quality of host image after embedding watermark into it.

Capacity- Capacity refers to amount of information that can be embedded in host image. Capacity depends on the application and the image.

Security- Watermarking algorithm is secure if knowing the algorithm to embed and extract the watermark does not help an unauthorised party to detect the presence of watermark.

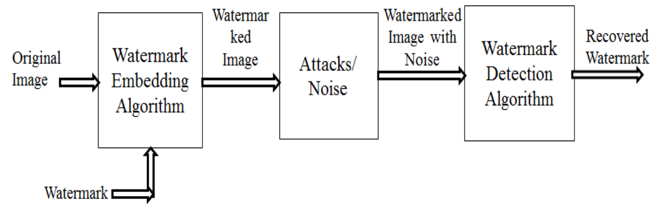

Figure 1: General digital watermark life-cycle phases with embedding-, attacking-, and detection and retrieval functions

All these characteristics cannot be achieved simultaneously as there is always a trade-off between them. For example, robustness and imperceptibility are contradictory to each other. Watermarking algorithm having high robustness usually sacrifices imperceptibility and vice versa. For higher robustness increased capacity is desired. But increased capacity leads to compromising imperceptibility. Watermarking methods introduced in proposed work aim to provide higher robustness as well as imperceptibility.

III. DISCRETE SHEARLET TRANSFORM

Shearlet transform is an affine function containing a single mother Shearlet function that is parameterized by scaling, shear and translation parameters with the shear parameter capturing the direction of the singularities [8]. An important advantage of this transform over other transforms is due to the fact that there are no restrictions on the number of directions for the shearing. There are also no constraints on the size of the supports for the shearing, unlike, for instance, directional filter banks [9] where using a small window size would result in a performance loss. Therefore, the Shearlet transform is designed to deal with directional and anisotropic features, typically present in images, and has the ability to effectively capture the geometric information of edges.

In relation to its application for image watermarking, the DST ability to better represent directional features as claimed in [10], may allow watermark embedding to adapt to the diagonal features in the host image more efficiently. In this section, a new DST-based watermarking framework for blind watermarking is developed in order to explore the possible improvements on DST performance against signal processing, geometric and compression based attacks. In addition, this proposed new blind watermark detection scheme for DST coefficients is optimal for non-additive schemes relying on the statistical decision theory.

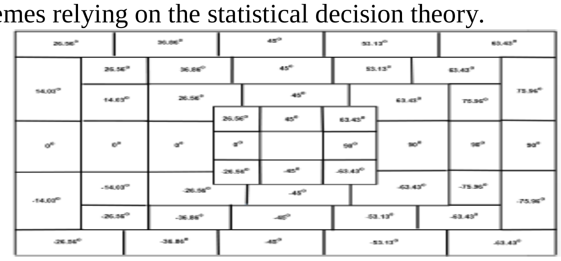

Figure 2: 2- Levels for DST.

The DST of the first flag is then gotten by connecting all coefficients beginning from the last level of decay (staying two examples, for this situation). The DST will then have an indistinguishable number of coefficients from the first flag.

IV. PROPOSED METHODOLOGY

DST involves decomposition of image into frequency channel of constant bandwidth. This causes the similarity of available decomposition at every level. DST is implemented as multistage transformation. Level wise decomposition is done in multistage transformation.

S is a diagonal matrix of singular values in decreasing order. The fundamental thought behind SVD strategy of watermarking is to discover SVD of picture and the modifying the particular incentive to insert the watermark. In Digital watermarking plans, SVD is used due to its basic properties:

A s mall aggravation incorporated the photo, does not cause tremendous assortment in its singular characteristics. The particular esteem speaks to inborn logarithmic picture properties [3].

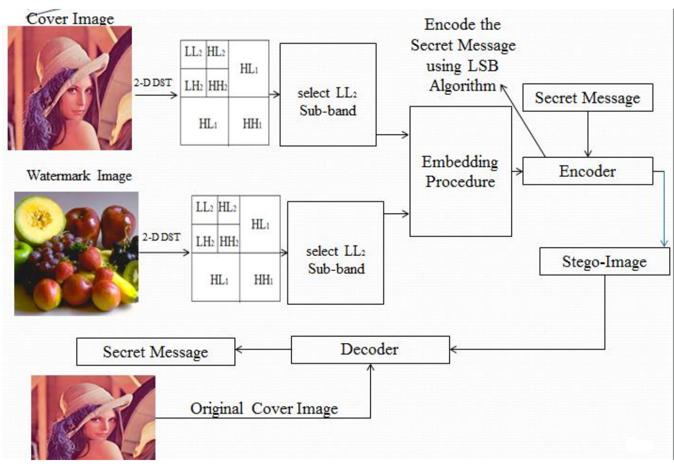

Figure 3: Flow Chart of Proposed Methodology

Algorithm for Watermark Embedding

Step 1: Take host image as input and convert it into Rearrange image original (RIO).

Step 2: Apply 2-D DST on rearranged image original (RIO) to decompose it into seven sub-bands.

Step 3: Select sub-band LL_2 of RI.

Step 4: Then apply SVD to sub-bands LL_2 to get UR, ΣR and V^TR.

Step 5: Take watermark image as input and convert it into Rearrange image watermark (RIW). Apply 2-D DWT on rearranged image watermark (RIO) to decompose into seven sub-bands.

Step 6: Select sub-bands LL_2 of Wi.

Step 7: Then apply SVD to sub-bands LL_2 to get UW, ΣW and V^TW.

Step 8: Modify UR, ΣR and V^TR by using equation

$UR^* = UR + (0.10^*UW);$

$\Sigma R^* = \Sigma R + (0.10^* \Sigma W);$

$V^TR^* = V^TR + (0.10^* V^TW);$

Step 9: Construct modified SVD matrix UR*, ΣR* and V^TR^*.

Step 10: Apply inverse SVD.

Step 11: Apply inverse DST and finally get watermarked image WI.

LSB Technique:-

This technique works best when the file is longer than the message file and if image is grayscale.

When applying LSB technique to each byte of a 24 bit image, three bits can be encoded into each pixel.

If the LSB of the pixel value of cover image C(i, j) is equal to the message bit SM of secret message to be embedded C(i, j) remain unchanged; if not, set the LSB of C(i, j) to SM.

Message embedding procedure is given below:

S(i, j) = C(i, j)-1, if LSB (C(i, j)) = 1 and SM = 0

S(i, j) = C(i, j)+1, if LSB (C(i, j)) = 0 and SM = 1

S(i, j) = C(i, j), if LSB (C(i, j)) = SM

Where LSB (C(i, j)) stand for LSB of cover image C(i, j) and "SM" id the next message bit to be embedded. S(i, j) is the Stego image.

The proposed method follows a directional embedding technique for achieving maximum image quality in the stego image. The proposed method performs a selection of suitable direction for secret byte embedding so as to minimize the bit changes in the cover image when a secret data is embedded.

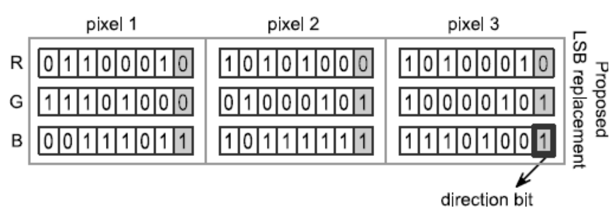

Figure 4: LSB embedding of the byte 11110000 in the cover image using the proposed method.

As you can see in Fig. 4, the byte 11110000 is embedded in a reverse order (00001111) in the original cover image for minimizing the number of alterations. Here also, we take three consecutive pixels (say *p*1, *p*2 and *p*3) for embedding a byte of information. Firstly, the red channels of *p*1, *p*2 and *p*3 are replaced with secret bits, followed by their green and blue channels. A direction bit is added at the 9-th bit which indicates that the preceding data is in stored in a reverse order. A value for the direction bit indicates a normal forward direction of storing data while a value 1 for the direction bit indicates that the data is stored in reverse direction.

V. SIMULATION RESULT

The digital sherlet transform are scalable in nature. DST more frequently used in digital image watermarking because of its excellent spatial localization and multi resolution techniques. The excellent spatial localization property is very convenient to recognize the area in the cover image in which the watermark is embedded efficiently.

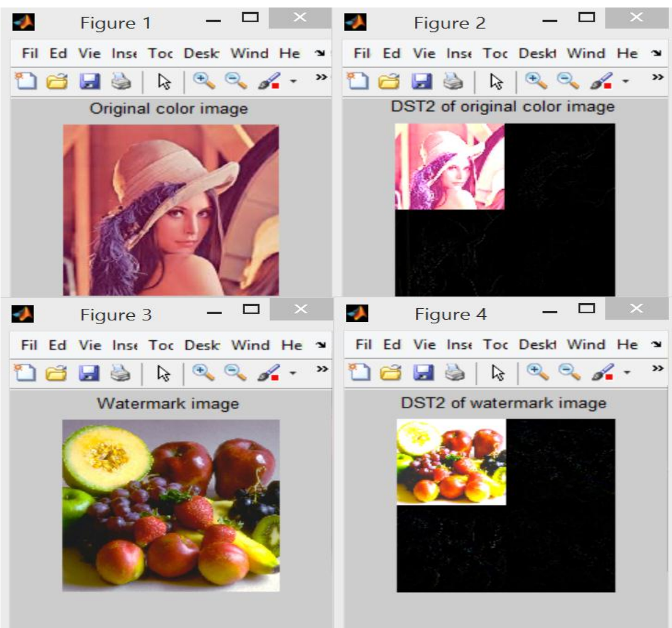

Figure 5: Original Color and Watermark Image

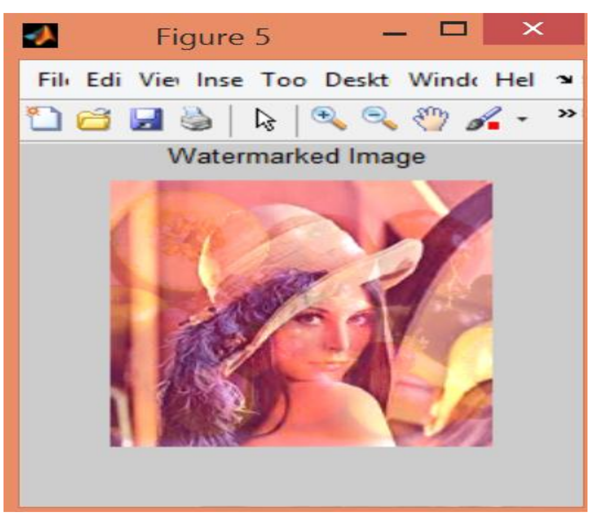

Figure 6: Embedding Processing of Watermark and Original Image

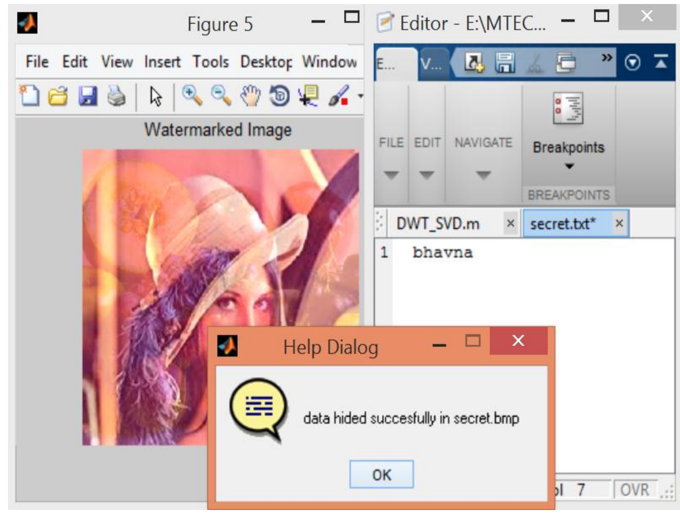

Figure 7: Data Hidden for Watermarked Image using Embedding LSB Stenography Technique

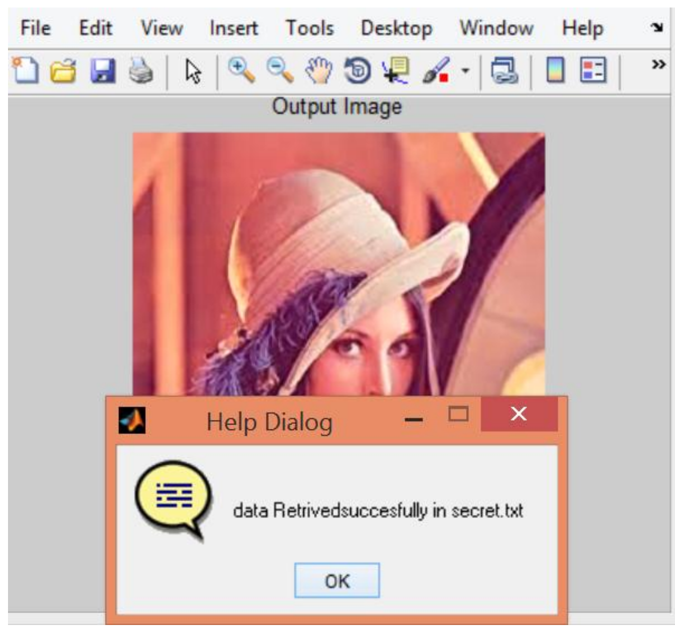

Figure 8: Received Output Image with Retrieved Message

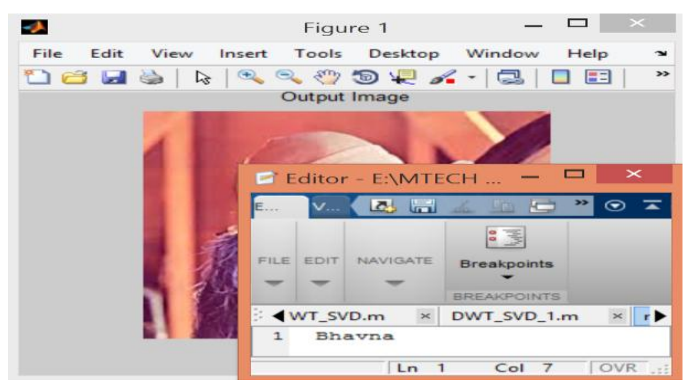

Figure 9: Received Message

Table 1: Comparison Result for PSNR

	Previous Algorithm		Proposed Algorithm
Image	Scheme-I [1]	Scheme-II [1]	PSNR (dB)
Lena Image	42.65	41.24	61.959
Baboon Image	41.37	38.89	58.618
Pepper Image	42.65	41.38	54.242

VI. CONCLUSION

It has been proved that the use of DST-SVD with fusion method has improved the security of the watermarking scheme. Particular attention is given to the proposed scheme to from the above descriptions, it have been shown that using Stenography and Watermarking can ensure a secure message. Besides, it is examined by applying different attacks and the performance is assessed by various factors included PSNR and MSE. The proposed Algorithm successfully analyzed in different image file format. The results have confirmed the effectiveness of the introduced method with and without the attacks.

REFRENCES

[1] 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.

[2] 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.

[3] Aase, S.O., Husoy, J.H. and Waldemar, P. (2014) A Critique of SVD-Based Image Coding Systems, IEEE International Symposium on Circuits and Systems VLSI, Orlando, FL, Vol. 4, Pp. 13-16.

[4] Ahmed, F. and Moskowitz, I.S. (2014) Composite Signature Based Watermarking for Fingerprint Authentication, ACM Multimedia and Security Workshop, New York, Pp.1-8.

[5] Akhaee, M.A., Sahraeian, S.M.E. and Jin, C. (2013) Blind Image Watermarking Using a Sample Projection Approach, IEEE Transactions on Information Forensics and Security, Vol. 6, Issue 3, Pp.883-893.

[6] Ali, J.M.H. and Hassanien, A.E. (2012) An Iris Recognition System to Enhance E-security Environment Based on Wavelet Theory, Advanced Modeling and Optimization, Vol. 5, No. 2, Pp. 93-104.

[7] Al-Otum, H.M. and Samara, N.A. (2009) A robust blind color image watermarking based on wavelet-tree bit host difference selection, Signal Processing, Vol. 90, Issue 8, Pp. 2498-2512.

[8] Ateniese, G., Blundo, C., De Santis, A. and Stinson, D.R. (1996) Visual cryptography for general access structures, Information Computation, Vol. 129, Pp. 86-106.

[9] Baaziz, N., Zheng, D. and Wang, D. (2011) Image quality assessment based on multiple watermarking approach, IEEE 13th International Workshop on Multimedia Signal Processing (MMSP), Hangzhou, Pp.1-5.

[10] Bao, F., Deng, R., Deing, X. and Yang, Y. (2008) Private Query on Encrypted Data in Multi-User Settings, Proceedings of 4th International Conference on Information Security Practice and Experience (ISPEC 2008), Pp. 71-85, 2008.

[11] Barni, M. and Bartolini, F. (2004) Watermarking systems engineering: Enabling digital assets security and other application, Signal processing and communications series, Marcel Dekker Inc., New York.

[12] Barni, M., Bartolini, F. and Piva, A. (2001) Improved Wavelet based Watermarking Through Pixel-Wise Masking, IEEE Transactions on Image Processing, Vol. 10, Pp. 783-791.

