ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 8, August 2019

High Security Text and Image Message for Discrete Shearlet Transform and Modified Least Significant Bits Technique

Sandeep Kumar Singh, Dr. Paresh Rawat

M. Tech. Scholar, Department of Electronics and Communication, SISTech., Gandhinagar, Bhopal, India

Head of Department, Department of Electronics and Communication, SISTech., Gandhinagar, Bhopal, Bhopal, India

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 modified 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

The basic concepts and requirements of Data Security, different methods used with merits and demerits, different types of classification of watermarking techniques and requirements of each technique are discussed in this chapter. Data/Information security is a process of protecting information from an unauthorized access, use, disclosure, disruption, modification, or destruction. The terms information security, computer security and information assurance are frequently used interchangeably. These fields are interrelated and share the common goals of protecting the confidentiality, integrity and availability of information, with some subtle differences between them [1]. The use of digital data has become more and more commercialized. This is especially true for digital images, where proof of origin and content integrity is an important issue. [2]. Multimedia signal processing has the goal of [3] high quality, highly efficient compression, security related issues, error resilient transmission and interactivity.

There are two widely used methods of information security: one being the data encryption or cryptography and the other being the data hiding [4]. In data encryption, a particular user with private key can recover the encrypted message. Even if an attacker gets access to the encrypted message, it is difficult to find its content, without knowing the key. Unfortunately, this method is unsafe if it is tampered. Encryption protects contents during the transmission of data from the sender to receiver, but the data is no longer protected once the data is decrypted. To overcome this problem, a secret data is hidden into a meaningful host data to distract the attention of the observers. This technique is called as Data hiding. Since internet is given public access, the transmitted material is exposed to all types of users. To protect the data against illegal access, encryption technique is used. But it has the disadvantage that the encrypted message usually looks noisy. It may seek the attention of the attackers during transmission activity and hence increase the risk. Data hiding is used as an alternative, which is an art of concealed communication, aiming at sending message under the cover of some carrier signals.

The embedded data is the message that has to be sent secretly. It is usually hidden in an innocuous message referred as a cover-text, or cover-image or cover-audio producing the stego-text or other stego-object. In image Steganography the information is hidden exclusively in an image which is called the cover image. After embedding the secret image, the cover image is called the stego-image. It must provide imperceptible data hiding and should be able to convey the

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 8, August 2019

meaning after extraction. Key is an additional secret data that may be required in the process of hiding. If the same key is used at both embedding and extraction, it is called as symmetric. The embedded data in Steganography is no way related to the cover media, but in case of watermarking the embedded data called as watermark is one of the attribute of cover media. Steganography is more concerned about bandwidth of the hidden message but the watermarking concerns more about robustness. Fingerprinting is the process of adding fingerprints to an object and recording them, or identifying and recording fingerprints that are already intrinsic to the object. Digital fingerprinting produces a metafile that describes the contents of the source file [5].

II. DIGITAL WATERMARKING

Watermarking scheme should resist destruction from standard image processing and malicious attacks. For example, watermarked images may be compressed before transmitting or storing it. Thus, the watermarked image has to survive the legitimate usage such as lossy compressions, conversions, re-sampling, and other non-malicious operations. On the other hand, the watermarked image may be involved in several of the intentional or the unintentional attacks trying to remove the embedded watermark. A watermarking scheme must be robust in the following areas:
Common signal processing: The watermark should be unaffected and retrievable even if some of the common signal processing operations such as resampling, requantisation (dithering and recompression), digital-to-analog and analog-to-digital conversion are applied.

Common geometric distortions: watermarked image should be immune to geometric operations such as rotation, translation, cropping and scaling.

Collusion and forgery attacks: watermark should be robust to combining copies of the same data set to destroy the watermarks. Further, if a digital watermark is to be used in litigation, it must be impossible for colluders to combine their images to generate a different valid watermark with the intention of framing a third party.

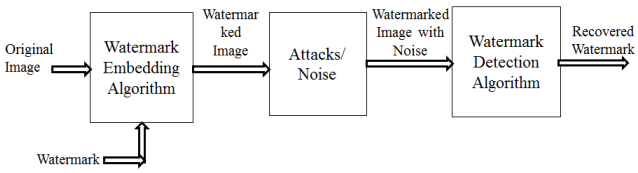

Figure 1: General digital watermark life-cycle phases with embedding-, attacking-, and detection and retrieval functions

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.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 8, August 2019

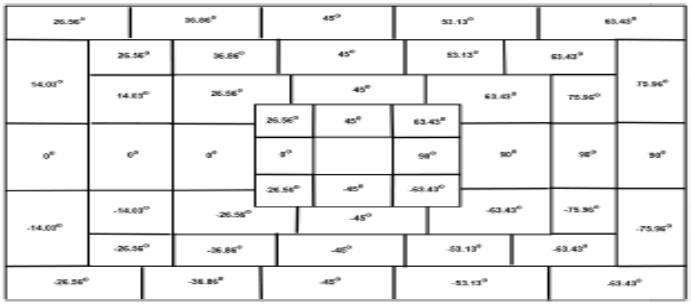

FIGURE 2: 2- LEVELS FOR DST.

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.
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

A watermark can be embedded into an image as either visible or invisible. The visible watermark is perceptible and is just like noise. It can be removed by a noise removing process. In order to decrease the risk of cracking, most of the proposed watermarking schemes are invisible [50]. On the other hand, the quality of the watermarked image is also important. If the watermark embedding process seriously affects the quality of the watermarked image, the watermarked image will draw the attention of attackers or even lose its value.

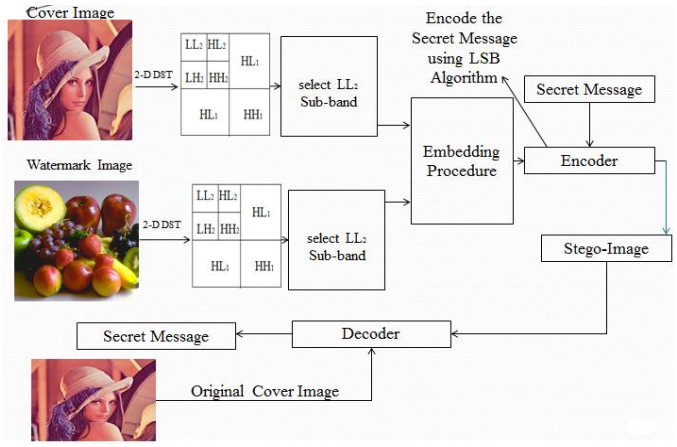

Figure 3: Flow Chart of Proposed Methodology

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 8, August 2019

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.

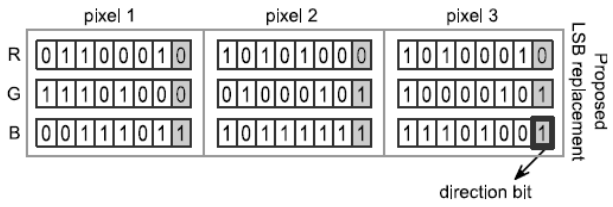

Figure 4: LSB embedding of the byte 11110000 in the cover image using the proposed method.

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.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 8, August 2019

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.

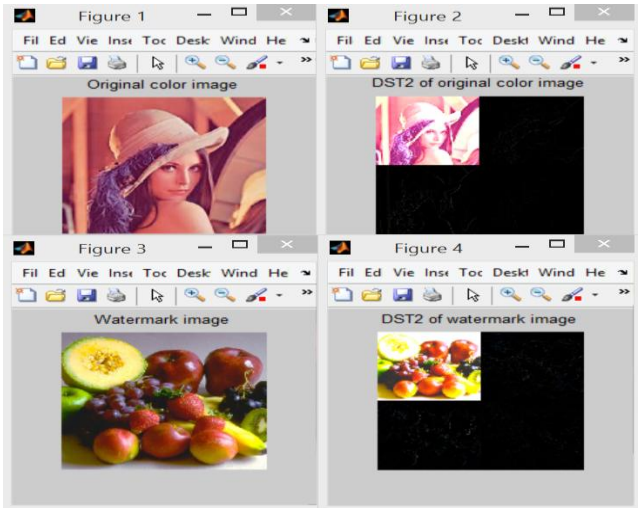

Figure 5: Original Color and Watermark Image

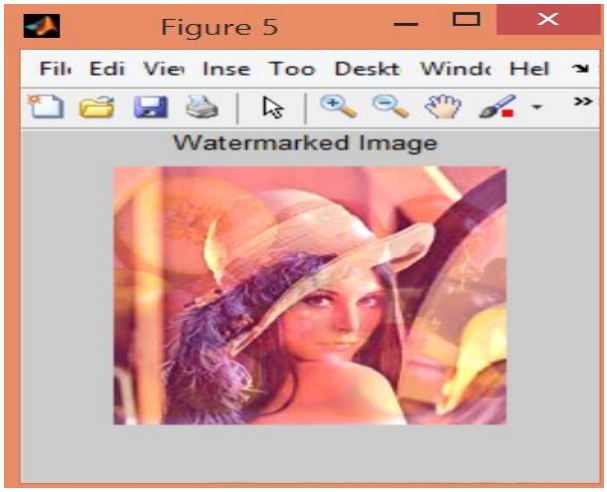

Figure 6: Embedding Processing of Watermark and Original Image

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 8, August 2019

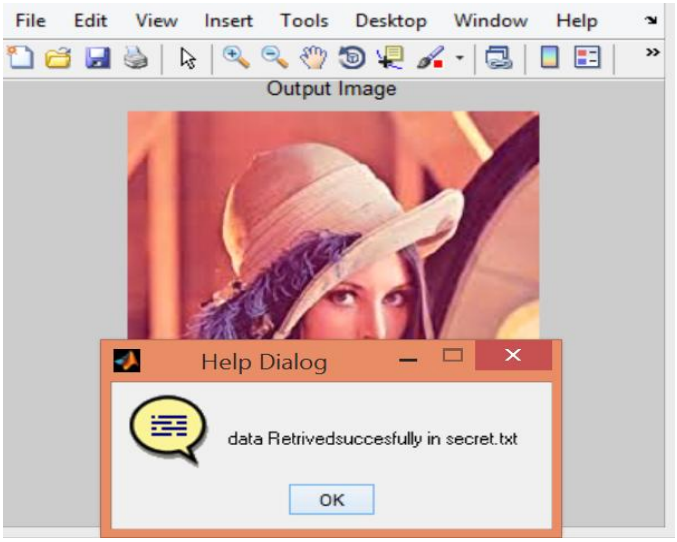

Figure 7: Received Output Image with Retrieved Message

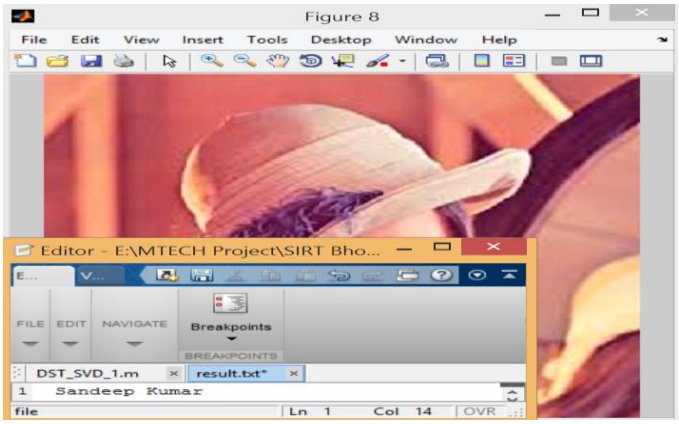

Figure 8: Received Message

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	55.743
Baboon Image	41.37	38.89	55.032
Pepper Image	42.65	41.38	54.943

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 8, August 2019

VI. CONCLUSION

A watermark is said to be private if only authorized readers can detect it. In other words, in private watermarking a mechanism is envisaged that makes it impossible for unauthorized people to extract the watermark. Indeed, blind techniques are by themselves private, since only authorized users can access the original data needed to read the watermark. Privateness may be achieved by assigning to each user a different pseudo-random key whose knowledge is necessary to extract the watermark from the host document. The results have confirmed the effectiveness of the introduced method with and without the attacks.

REFRRENCES

[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.