IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-6, June 2019 E-ISSN: 2347-2693

Optimization of Secure Data for Steganography and Digital Watermarking Scheme

Avinash Rai [1*], Vivek Todkar[2]

[1,2]Dept. of Electronics and Communication Engineering, UIT-RGPV, Bhopal

Corresponding Author: avinashrai@rgtu.net

DOI: https://doi.org/10.26438/ijcse/v7i6.10361040 | Available online at: www.ijcseonline.org

Accepted: 08/Jun/2019, Published: 30/Jun/2019

***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 wavelet transform (DWT).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 in increased by combining DWT 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 Wavelet Transform, SVD, PSNR, MSE

I. INTRODUCTION

In the recent few years, there is a serious problem about unauthorized and illegal access and manipulation of multimedia files over internet. Everybody can obtain copies of copyrighted multimedia openly. So we need to generate a robust method in order to protect the copy rights of media. Digital watermarking provides copyright protection of data. It is done by embedding additional information called digital signature or watermark into the digital contents such that it can be detected, extracted later to make an assertion about the multimedia data. [1, 2] For picture watermarking, the calculations can be sorted into one of the two spaces: spatial area or change area. [1, 2] In Spatial area the information is installed specifically by altering pixel estimations of the host picture, while change space plans insert information by adjusting change area coefficients. Algorithms used for special domain are less robust for various attacks as the changes are made at least Significant Substitution (LSB) of original data. While in the transform-domain the watermark is embedded by changing the magnitude of coefficients in a transform domain with the help of discrete cosine transform, discrete wavelet transform (DWT), and singular value decomposition (SVD) techniques[3, 5]. This provide most robust algorithm for many common attacks. [7] In this paper we proposed a hybrid watermarking using DWT and SVD technique in order to achieve high robustness and transparency.

Therefore we decided to design watermarking schemes such that an inherent nature in can be embedded to guarantee that at least one serious attack having most financial implications cannot be conducted on watermarked images**.** If owner identification applications place the same watermark in all copies of the same content, then it may create a problem. If out of n number of legal buyer of content, one starts to sell the contents illegally, it may be very difficult to know who is redistributing the contents without permission. Allowing each copy distributed to be customized for each legal recipient can solve this problem. This capability allows a unique watermark to be embedded in each individual copy.

This particular application area is known as fingerprinting and thus has numerous financial implications. The most serious attack for fingerprinting is the "collusion attack". On the off chance that assailant approaches in excess of one duplicate of watermarked picture, he/she can anticipate/evacuate the watermark information by conniving them. Analysts chipping away at "fingerprinting" basically center around the "plot assault".

Along these lines, while planning a watermark plot, we chose that our proposed plans must be outlined such that plans are intrinsically conspiracy assault safe. In this manner this proposal displays another term "ICAR (Inherently Collusion Attack Resistant)" as a necessity for a watermarking framework. The other 3 issues are considered while building up the watermarking plans.

The primary section is given to the presentation of the watermarking territory. Information concealing foundation is spoken to and the related phrasings are clarified. At that

point different application territories of watermarking are spoken to and what may the key necessities of a fruitful watermarking framework are talked about. Since watermarking can be grouped on different parameters, the different kinds of watermarking are spoken to in view of various arrangements.

ISSUE 1: Till now there is no "Nonspecific" nature in the watermarking calculations accessible. All the more correctly, if certain approach is appropriate for a dark level picture, a similar approach does not work for alternate configurations of a picture.

ISSUE 2: Regardless of whether dark shading picture watermarking calculations are stretched out for RGB shading pictures, the most extreme work has been improved the situation BLUE shading channel simply because human eyes are less delicate to distinguish the adjustments in BLUE shading channel. No assault affect examination, i.e, which shading channel might be influenced by a specific assault, has been completed.

In this way, aside from picking computerized Image Watermarking as a noteworthy issue, we have distinguished the appropriateness of a shading channel as for assault (assuming any) for multicolor channel pictures (True shading windows BMP, uncompressed JPEG). We likewise chose to investigate the ways with the end goal that assault effects might be limited before the watermark inserting process.

ISSUE 3: In most of the research papers, once the watermarking scheme is finalized, it is applied to all test images. Since each image is different and has certain characteristics and after embedding the watermark data by a particular watermarking scheme, its performance against a particular attack may not be similar with other image. No study is conducted to make the embedding scheme based on some image characteristics.

II. DIGITAL WATERMARKING

The data to be installed in a flag is known as an advanced watermark, in spite of the fact that in a few settings the expression computerized watermark implies the distinction between the watermarked flag and the cover flag. The flag where the watermark is to be installed is known as the host flag. A watermarking framework is generally partitioned into three particular advances, installing, assault, and identification. In implanting, a calculation acknowledges the host and the information to be inserted, and delivers a watermarked flag.

At that point the watermarked advanced flag is transmitted or put away, typically transmitted to someone else. On the off chance that this individual makes an alteration, this is called an assault. While the change may not be pernicious, the term assault emerges from copyright insurance application, where outsiders may endeavor to expel the computerized watermark through adjustment. There are numerous conceivable adjustments, for instance, lossy pressure of the information (in which determination is lessened), trimming a picture or video, or purposefully including clamor.

Location (frequently called extraction) is a calculation which is connected to the assaulted flag to endeavor to extricate the watermark from it. In the event that the flag was unmodified amid transmission, at that point the watermark still is available and it might be removed. In powerful computerized watermarking applications, the extraction calculation ought to have the capacity to deliver the watermark accurately, regardless of whether the alterations were solid. In delicate computerized watermarking, the extraction calculation ought to come up short if any change is made to the flag.

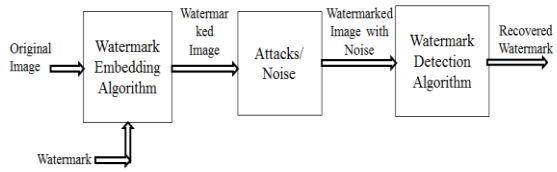

Figure 1: General digital watermark life-cycle phases with embedding-, attacking-, and detection and retrieval functions

III. DISCRETE WAVELET TRANSFORM

The model utilized as a part of [5] to actualize the tree structure of Direct Wavelet Transform (DWT) depends on the separating procedure. Figure 1 portrayed a total 2-level Direct WT. In this figure G and H is the high pass and low pass channel separately.

Calculation period is the quantity of the information cycles for one time creates yield tests. In general, the computation period is M= for a j-level DWT. The period of the 2-level computation is 8. Figure 1, The Sub band Coding Algorithm As an example, suppose that the original signal X[n] has N-sample points, spanning a frequency band of zero to π rad/s. At the first decomposition level, the signal passed through the high pass and low pass filters, followed by subsampling by 2. The output of the high pass filter has N/2- sample points (hence half the time resolution) but it only spans the frequencies π/2 to π rad/s (hence double the frequency resolution).

The output of the low-pass filer also has N/2- sample points, but it spans the other half of the frequency band, frequencies from 0 to π/2 rad/s. Again low and high-pass filter output passed through the same low pass and high pass filters for

further decomposition. The output of the second low pass filter followed by sub sampling has N/4 samples spanning a frequency band of 0 to π /4 rad/s, and the output of the second high pass filter followed by sub sampling has N/4 samples spanning a frequency band of π/4 to π/2 rad/s. The second high pass filtered signal constitutes the second level of DWT coefficients. This signal has half the time resolution, but twice the frequency resolution of the first level signal. This process continues until two samples are left. For this particular case there would be 3 levels of deterioration, each having a large portion of the quantity of tests of the past level.

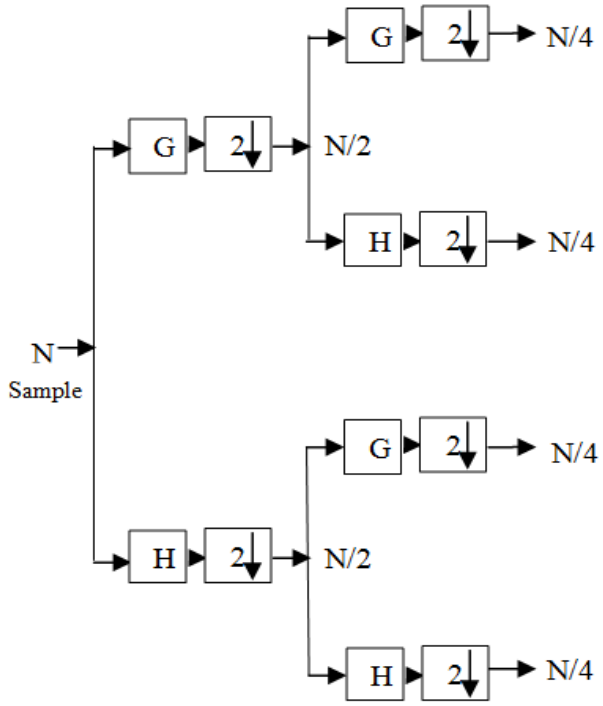

Figure 2: 2- Levels for DWT. Where G, H are the high-pass and low-pass filter coefficient

The DWT 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 DWT will then have an indistinguishable number of coefficients from the first flag.

IV. PROPOSED METHODOLOGY

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

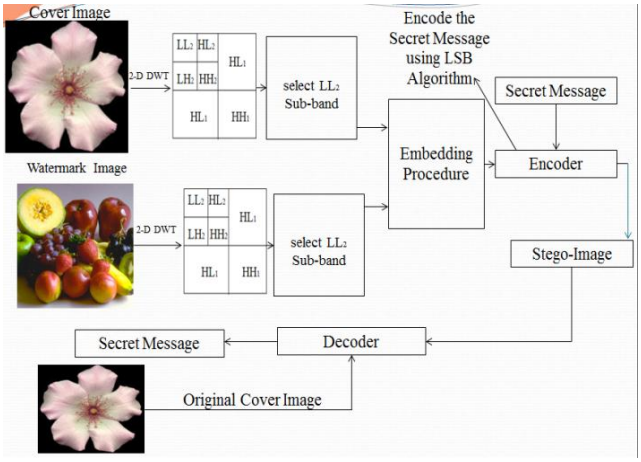

Figure 3: Flow Chart of Proposed Methodology

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].

Algorithm for Watermark Embedding

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

Step 2: Apply 2-D DWT 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 DWT 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.

V. SIMULATION RESULT

Discrete Wavelet Transform (DWT): The digital wavelet transform are scalable in nature. DWT 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 4: Experiment Result for Steganography and Watermarking

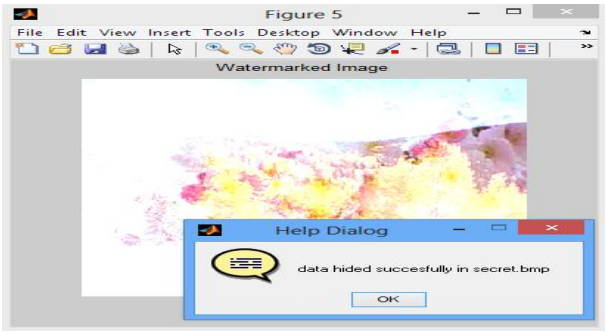

Figure 5: Data hidden successfully with watermarked image

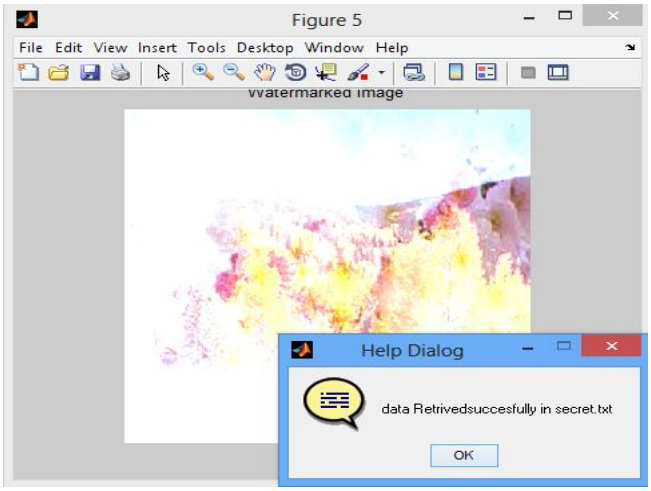

Figure 6: Experiment Result for Steganography and Watermarking

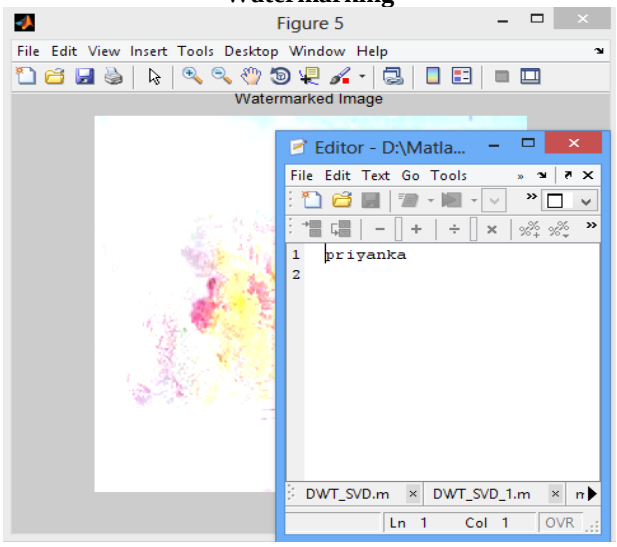

Figure 7: Experiment Result for Steganography and Watermarking

Table 1: Comparison Result

Image	PSNR (dB)	MSE	RMSE	NAE	Computation Time (ns)
College Image	29.864	25.7597	8.3286	9.241	4.451
Flower Image	28.765	19.4129	5.2992	4.962	5.347
Lena Image	30.654	22.543	6.954	3.654	4.332
Tree Image	31.432	25.782	8.543	3.576	3.667

VI. CONCLUSION

It has been proved that the use of DWT-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, MSE, RMSE, NAE and Computation Time. 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. Remarkably, the method is more robust and secure compared with previous technique.

REFERENCES

[1] 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.

[2] 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.

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

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

