IJASEM

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

Examining the Robust Watermarking Performance of DWT-SVD and RDWT-SVD

[1] Mrs.Mohammad Rubeena, [2] Mrs. S. Mounika, [3] G.Nagaraju

[1,2,3]Asst. Professor, Department of ECE, Balaji Institute of Technology & Science, Warangal-Narsampet Rd,

Laknepally, Madhira D, Telangana 506330

Abstract:

When it comes to digital watermarking, DWT and RDWT are two of the most well-known methods. The DWT method's main drawbacks are its shift variance characteristic and the fact that the size of the initial picture decreases with each successive breakdown level. Due to these constraints, the watermarking system's data output is reduced. RDWT is effective at overcoming DWT's limitations. To boost the efficiency of digital watermarking, SVD is another method that has been widely discussed in the literature. Two such mixed methods, DWT-SVD and RDWT-SVD, are presented in this article. Data from the observational study Assistant Professor Rd. Shaifali M. Arora, Electrical and Electronics Engineering, MSIT Janakpuri New Delhi India In shaifali04@msit.in domain watermarking, time domain actions are applied to the pixels of the host picture to alter them in accordance with the watermark. While relatively straightforward, this version does not hide the watermark, making it vulnerable to various assaults on picture processing, and reducing its overall resilience [10]. RDWT-SVD outperforms the other superior method, in which the host picture is changed in the frequency domain, according to the parameters of the frequency domain.

Keywords: Digital Watermarking, Robust Watermarking, DWT-SVD, RDWT-SVD.

INTRODUCTION

Digital data production and modification have reached unprecedented levels thanks to the widespread availability of the internet and the advent of powerful computing devices like computers, iPads, and mobile phones. To counteract malevolent actors' ability to make unauthorized changes, there is a wide variety of methods at their disposal. Due to its effectiveness in concealing digital data, digital watermarking has distinguished itself among other data concealment methods. In digital watermarking, a piece of data (a watermark) is superimposed on the data that needs to be protected, typically a picture, text, or emblem. There are two phases to the watermarking process: encoding the watermark and decoding it. Both the host data and the watermark data must be provided for the watermark placement procedure to proceed. Using a reader to determine whether a watermark is present in the retrieved data, the embedded watermark is removed during the extraction procedure [1-2]. The validity of a file is determined by comparing its signature to the one used to create the file. Both reliability and invisibility in use are crucial for any watermarking device. If the watermark can withstand common image processing and geometry assaults like scaling, shrinking, sharpening, fading, adding noise, etc., then the watermarking method is durable. All geometry and picture processing attacks must fail on the marking. The watermarking scheme's imperceptibility is measured by how well it conceals itself within the watermarked picture. Other key limitations to think about in watermarking system design include computational expense, watermark security, watermark instability, and data content provided by the scheme. Both frequency domain and spatial domain techniques can be used to superimpose a digital stamp on top of the source picture. In a geographicalSince SVD (singular value decomposition) has proven to be relatively effective in digital watermarking uses, it has recently been combined with various transform domain methods to increase its resilience and undetectability. In this work, we introduce two mixed domain watermarking, in which time domain operations are applied directly to the pixels of the host picture to alter them in accordance with the watermark. While relatively straightforward, this version does not hide the watermark, making it vulnerable to various assaults on picture processing, and reducing its overall resilience [10]. Another effective method involves a frequency domain transformation of the host picture and the use of watermarking apps' frequency domain coefficients, which are both more secure and undetectable. Some of the methods that have been used to transform data include the discrete cosine transform, discrete Fourier transform, discrete wavelet transforms, discrete fractional transform, linear wavelet transform, etc. [10–14]. The DWT-SVD and RDWT-SVD techniques have been introduced, and their performance in terms of mean square error (MSE), peak signal to noise ratio (PSNR), and structural similarity index (SSIM) has been assessed. The article is organized as follows: Part II provides an overview of the transform domain methods (discrete wavelet transform [DWT], radial basis function [RDF] transform [SVD], and spectral vector decomposition [SVD]). In Section III, we described the suggested method,

and in Section IV, we presented the acquired findings. Metrics like mean squared error, pseudo-signal-to-noise ratio, and SSIM have been used to assess the efficacy of the integrated algorithm. In Section V, we summarize our findings from testing the two algorithms and comment on their relative effectiveness.

TRANSFORM DOMAIN TECHNIQUES

In the realm of digital watermarking, DWT has become the most popular change method. DWT can be used to conduct picture segmentation on an N-level granularity. Several high pass filters are applied to the picture in sequence to meet the breakdown criteria. High pass filters are used to remove 50 percent of an image's frequency content. As a consequence, the original picture dimension is cut in half. These filters can break a picture down into its component colours. It is possible to view the one-level 2-D DWT procedure as a combination of two 1-D decompositions. The picture is split in half horizontally using a single 1-D translation procedure applied to the image collection. The other kind of disintegration splits the picture in half vertically. Decomposition is carried out repeatedly until the required granularity is reached. The LL, LH, HL, and HH sub bands that come from a one-level subdivision. Any one of these sub bands can be broken down even further depending on the task at hand. Figures 1 and 2 depict the one-level breakdown of a 2-D DWT and a woman's picture, respectively.
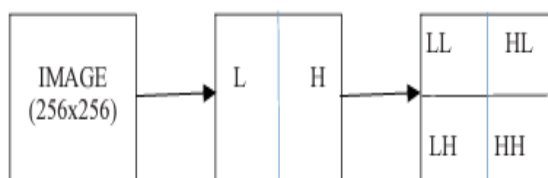

Fig.1 The process of one level 2

Fig. 2 An one level 2-D DWT decomposition of Woman image (LL, LH, HL, and HH=128x128)

SVD (Singular Value Decomposition)

The SVD is a linear algebraic method. The application of SVD will not degrade the visual clarity of a picture because single values in digital images tend to be stable. By performing the SVD procedure to any digital picture, the image's algebraic characteristics can be recovered; the singular vectors will reflect the image's mathematical elements, and the singular values will indicate the image's luminosity. SVD application is numerically costly, but merging with a frequency domain method has shown significant efficiency gains. Decomposing a picture into a 2-dimensional matrix is a prerequisite to implementing SVD to that image. After it, SVD can be inferred. Three matrices, U, S, and V, are produced as a consequence of the SVD operation on a picture [13, 14]. In fig. 3, we see the steps involved in the breakdown of a Mx picture.
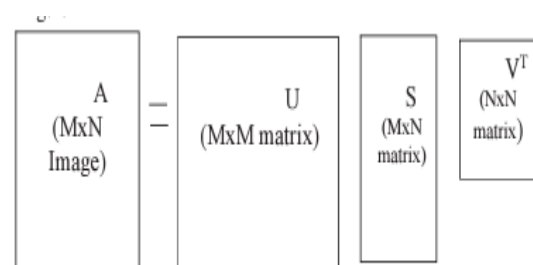

Fig. 3 SVD process

RDWT (Redundant Discrete Wavelet Transform)

Inhibited in DWT are terrific patio-frequency localisation characteristics, making it a great tool for identifying the host picture areas suitable for embedding an undetectable stamp. Because of this quality, DWT has become one of the most popular transformation techniques for digital watermarking. The shift variation feature is a significant drawback of DWT. When a picture is filtered multiple times, its parameters will alter slightly at each stage due to down sampling. The accuracy of watermark retrieval suffers as a result of these alterations. A shift-invariant transform, RDWT, has been developed to address this issue [16].
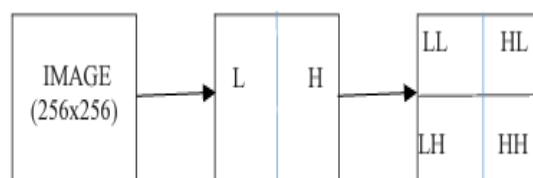

Fig.4 The process of I level 2-D RDWT decomposition process (LL, LH, HL, and HH =256x256)
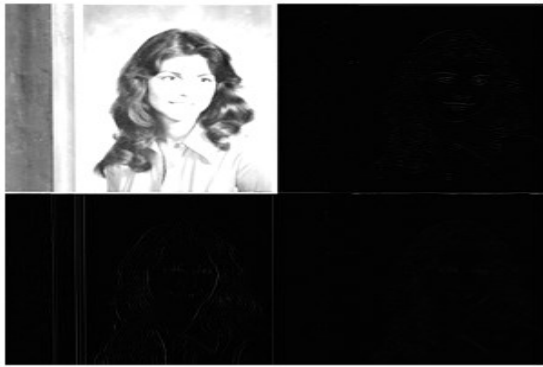
Fig. 5 An one level 2-D RDWT decomposition of Woman image (LL, LH, HL, and HH =256x256)

Down sampling and up sampling of factors are destroyed by RDWT. As a result, the picture dimension remains unchanged when using this technique. As a result, the image's size is increased compared to when using DWT. RDWT based watermarking methods have been shown to be more resilient in contrast to the DWT method [14], thanks to the increase in frame that enhances resilience with regard to the inclusion of noise. Figures 4 and 5 show examples of 1-level 2-D RDWT decompositions, along with their sub-band breakdowns.

PROPOSED ALGORITHM

This part has introduced the DWT-SVD and RDWT-SVD watermarking algorithms that have been suggested. Both methods use the same steps to embed and remove watermarks.

- Implement the transformation (DWT and RDWT for DWT-SVD algorithm and RDWT-SVD algorithm respectively), on the host image to acquire decomposed sub bands.
- Choose LL sub band to apply SVD to get Singular values.
- Apply transformation technique DWT and RDWT for DWT-SVD algorithm and RDWT-SVD algorithm respectively on Watermark image.
- Decompose watermark image to retrieve sub bands, use LL sub band to apply SVD to get Singular values.
- Embed watermark as: $S + \alpha$
- Alpha is scaling factor
- To get watermarked image perform DWT^{-1} for DWT-SVD and $RDWT^{-1}$ for RDWT-SVD technique.

B. The Extraction Algorithm

- The steps followed for extraction process are as follows:
- Apply DWT and RDWT for DWT-SVD algorithm and RDWT-SVD algorithm respectively on Watermarked image (possible distorted by attack).
- Apply SVD to LL sub band.
- Calculate

$$WMy = Uw * Swrec * Vw' \qquad (1)$$

- Perform DWT^{-1} and $RDWT^{-1}$ to reconstruct the extracted watermark.

EXPERIMENTAL RESULTS

An implementation of two hybridized algorithms DWT-SVD and RDWT-SVD has been presented in this work. Five images have been taken as images that are to be watermarked and one image has been taken as watermark image (tiff format). To evaluate the performance of both schemes MSE, PSNR and SSIM are calculated.

To test robustness, different attacks like blurring, cropping, resizing, addition of salt & pepper noise, addition of additive guassian noise have been imposed on the watermarked image. The standard 256x256 images have been used from SIPI database. Fig.6 (a-f) shows original host images and the watermark image.
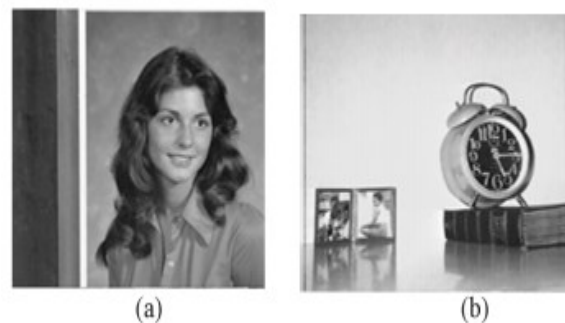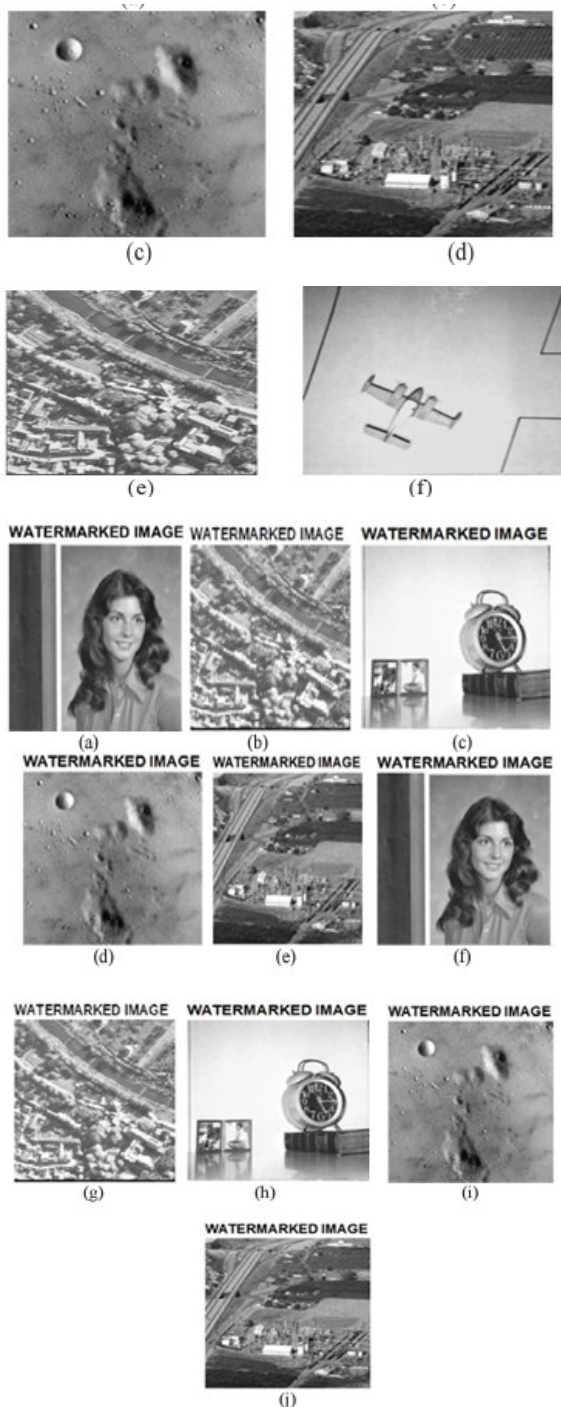
Fig. 7 DWT-SVD (a-e) and RDWT-SVD (f-j) watermarked images.

V. CONCLUSION

We present two new blind watermarking techniques in this work: DWT-SVD and RDWT-SVD. In tests against both geometric and nongeometric attacks, RDWTSVD has performed better than its predecessors except for spinning and cutting. The findings graph for RDWT-SVD shows that both the MSE and PSNR have improved. The lower MSE and PSNR values show that RDWT-SVD is less noticeable, and the better results for SSIM suggest that it is more robust. Combining the two random methods results in an unbreakable watermarking technique.

REFERENCES

[1] Cox, Ingemar J., Joe Kilian, F. Thomson Leighton, and Talal Shamoon. "Secure spread spectrum watermarking for multimedia." IEEE transactions on image processing 6, no. 12 (1997): 1673-1687. [2] Kutter, Martin, and Fabien AP Petit colas. "Fair benchmark for image watermarking systems." Security and Watermarking of Multimedia Contents 3657 (1999): 226-239.

[3] Cox, Ingemar J., and Matt L. Miller. "The first 50 years of electronic watermarking." EURASIP Journal on Advances in Signal Processing 2002, no. 2 (2002): 820936.

[4] Cox, I. J., and M. L. Miller. "J. ABloom, "Digital watermarking," Chapter 5—Watermarking with Side Information." (2001).

[5] Lie, Wen-Nung, Guo-Hsiang Lin, Chih-Liang Wu, and Ta-Chun Wang. "Robust image watermarking on the DCT domain." In Circuits and Systems, 2000. Proceedings. ISCAS 2000 Geneva. The 2000 IEEE International Symposium on, vol. 1, pp. 228-231. IEEE, 2000.

[6] Verma, Vivek Singh, and Rajib Kumar Jha. "Improved watermarking technique based on significant difference of lifting wavelet coefficients." Signal, Image and Video Processing 9, no. 6 (2015): 1443-1450.

[7] Singh, D., and Singh, S.K., 2017. DWT-SVD and DCT based robust and blind watermarking scheme for copyright protection. Multimedia Tools and Applications, 76(11), pp.13001-13024.

[8] Arora, Shaifali M. "A DWT-SVD based Robust Digital Watermarking for Digital Images." Procedia Computer Science132 (2018): 1441-1448.

[9] Thakkar, F.N. and Srivastava, V.K., 2017. A blind medical image watermarking: DWT-SVD based robust and secure approach for telemedicine applications. Multimedia Tools and Applications, 76(3), pp.3669-3697.

[10] http://sipi.usc.edu/database/database.php

[11] Bhatnagar, Gaurav. "A new facet in robust digital watermarking framework." AEU-International Journal of Electronics and Communications 66, no. 4 (2012): 275-285.