

DFT-SVD based Digital Image Watermarking

Ningombam Jimson¹, Kattamanchi Hemachandran²

^{1,2}*Department of Computer Science, Assam University, Dorgakona, Silchar-788011*
(E-mail: ¹jimson123@gmail.com, ²khchandran407@gmail.com)

Abstract— In the present era where the number of person using the computer network is increasing and the owner of the digital content has control over how the digital data is being used or manipulated, thus violating the intellectual properties rights of the digital data. Digital watermarking provide a possible solution for the protection of the digital data. In the presented paper we presented a digital image watermarking scheme in which a binary watermark is embedded into a cover image blockwise using both DFT and SVD is proposed. The scheme is a non-blind watermarking scheme in which the original image required for watermark extraction or detection. To test the scheme we used StirMark benchmarking tools and some common image processing attacks. Expiremental shows the scheme is robust against some of the common attacks involve in digital image watermarking.

Keywords— Discrete Fourier Transfrom (DFT), Singular value Decompostion(SVD), Peak signal to Noise ratio(PSNR), NC(Normalised Correaltion), SSIM(Structutal Similarity Index). Introduction

I. INTRODUCTION

The development of computer network such as internet has resulted in the high rate of digital data exchange among many person who has excess to it. Digital data in the form of image, audio and video can be created, manipulated, duplicated and stored without anyloss in the quality. Due to this reasons digital data owner or copyright holder has major concern of the about the copyright violation, ambiguity ownership of digital data and the digital data has been used in the way they intended. One way of preventing the unauthorized usage of digital data is by using Cryptography. Cryptography scramble the digital data in such a way that the information is meaningless to the unauthorized person by using a key. A person with valid key can unscramble the data. One major drawback of cryptography is that, once the digital content is decrypted, the owner of the digital content has no control over the decrypted data which can be later misused by unauthorized users [1]. Digital watermarking can be considered as a possible solution for protecting digital data, by adding information to a digital data. The information to be added can be in the form of text, logo etc and contain ownership information or copyright information of the digital data. Digital Steganography and digital watermarking are closely - both added additional information to a digital content. The main difference between the two is regarding robustness. In steganography, how the data is hidden into the digital content

is the main concern, and once the presence of the hidden information is known, steganography fails, but in case of digital watermarking, even if the presence of information is known, the watermark or information cannot be removed. Another difference between steganography and watermark is that in case of steganography, information hidden in digital content may or may not be related to the content itself. Steganography is a way of secret communication between two parties. In digital watermarking, the information embedded or hidden is related to the content itself. The information can be copyright information, description of owner etc. Robustness, Capacity, transparency are the major concerned in digital watermarking [2]. Robustness, as mentioned before, the watermark embedded should not remove from the digital content and it should survive from various intentional and unintentional attacks. Capacity is the amount of information that can be added or embedded into a digital data. Imperceptivity mean that the addition of digital watermark should cause any visual artefact or distortion to the digital data which mean both the watermarked data and original data should have same perceptual quality. In this paper we mainly deals with digital image watermarking. In digital image watermarking, a watermark or information can be added in the pixels level or in frequency domain, based on this digital image watermarking can be categories into spatial domain watermarking and transform domain watermarking. Transform or frequency domain digital watermarking are more robust compared to the spatial domain watermarking. On the other hand spatial domain watermarking have less computational complexity, low system requirement. In this paper we proposed a transform domain watermarking using Discrete Fourier Transform (DFT) and Singular value decomposition (SVD). The paper is organized as follows. In section I, we presented a brief introduction of digital watermarking in section II we present related work regarding digital watermarking using SVD is presented. In section III we present a theoretical background on DFT and SVD. In section IV we present our proposed algorithm, and finally conclusion of our proposed algorithm is given in section V.

II. RELATED WORKS

Ganic et al. [3] recommended a double SVD watermarking scheme by inserting a watermark twice. In their scheme, two watermark are added one by using block based approach and another by treating the entire cover image as one block. The watermark embedded by using block based approach allows flexibility in the amount of watermarking data and the watermark added using the second methods gives additional

robustness. Lee et al[4] proposed image content authentication using SVD. They insert a watermark into the blocks which are ordered randomly, by modifying the greatest singular value of each block in order to enhance the security. The proposed scheme was robust against Vector Quantization (VQ) attacks and histogram analysis. Calanga et al.[5] also proposed watermarking using SVD, in their approach, the cover image is divided into blocks and SVD is applied in each block and the watermark is integrates to the non- zero singular value of each block according to the local characteristics of the cover image to balance the embedding capacity with distortion. The scheme was robust against typical attacks, including low-pass and high-pass filtering, as assessed by the benchmarking tool. Mohan and Kumar [6] introduced a robust multimedia copyright image watermarking technique in SVD domain and using dither quantization to insert the watermark into the SVD acquired matrices (U and V). They stated that their method adjusts the largest singular value of the cover image and U matrix coefficients to embed the watermark. In Basso et al [7] scheme, the watermark is embedded in each block of the cover image by modifying the right singular vectors of the block. The proposed scheme is resistant to common signal processing and attack operations while maintaining original image quality. Lai and Tsai[8] proposed a watermark scheme using DWT and SVD. In their scheme, the watermark is embedded into the singular value of the cover image DWT sub-bands. In Agarwal et al [9] scheme the singular value of the binary watermark is embedded into the singular value of the LL3 subbands using multiple scaling factors which were optimized using firefly algorithm with an objective function which combined imperceptibility and robustness in linear basis. Ali et al [10] proposed a hybrid block based watermarking scheme by using differential evolution in DCT and SVD. In this scheme, the cover image is divided into blocks and DCT is performed in each block. The DC component of each block is collected to construct a low resolution image and SVD is applied to this image. The watermark is embedded by modifying the singular value of the estimated image with the singular values of the watermark. Makbol and Khoo[11] used integrated wavelet transform and SVD to embed the watermark. In this scheme, the challenge regarding the false positive faced by most of the SVD based algorithm has been solved by using a digital signature in the watermarked image. The ownership is authenticated by the digital signature embedded before extracting the watermarking. Later, Makbol et al[12] proposed a Block-based watermarking system based on the singular value decomposition (SVD) and human visual system in the discrete wavelet transformation (DWT) domain. The proposed method, entropy, and edge entropy as is used as HVS characteristics to select important blocks for embedding the watermark, a binary watermark logo. The blocks of the lowest entropy values and the edge entropy values are selected as the best watermark regions. After the first decomposition level of the DWT, the SVD is performed on the LL subband to modify several elements in its U matrix according to predefined conditions. Singh et al[13] proposed a hybrid watermarking scheme utilizing DWT, DCT and SVD. In this

scheme, the cover image is first decomposed using DWT and low-frequency component (LL) of the DWT is transform using DCT and SVD. The watermark image is also transformed using DCT and SVD. The S element of the watermark image is embedded in the S element of the cover image. Applying inverse SVD using the modified S element and original U and V and then inverse DCT and DWT is performed to get the watermarked image. Lai[14] scheme utilized SVD and DCT to embed the watermark into a cover image. The scheme presented is a block-based approach in which the cover image is divided into a non-overlapping block and using HVS characteristic the scheme select an appropriate block and then DCT is applied into the selected blocks and SVD is again applied to the DCT transform block and watermark information is embedded into the U matrix of the SVD transformed. Inversed SVD and DCT are applied to the selected block to get the watermarked image. Rastegar et al[15] utilized Radon transform and SVD to embed the watermark. In this scheme, Finite radon transform is performed on the cover image and they apply 3 level DWT to the transformed image and Perform SVD transform on approximation and all the detail parts in the third level of wavelet transform. The watermark is embedded by modifying the singular value of the cover image with the singular value of the watermark. Zhang et al [16] proposed SVD based watermarking scheme in the spatial domain. In this scheme, a binary watermark is embedded into the largest singular value of the spatial block of the cover image. Natu et al proposed a scheme which utilized DCT-Walsh hybrid transform and SVD. In this scheme, the DCT-Walsh hybrid transform is applied to the cover image and 30 coefficient is selected as low frequency and SVD is applied to selected low-frequency component to obtain the singular value. The watermark is also transformed using DCT-Walsh hybrid transform and SVD is also applied to transformed watermark image and 30 singular value is selected for embedding. The cover image singular values are replaced by the obtained watermark image singular value. Taking inverse SVD and inverse DCT-Walsh hybrid transform to get the watermarked image.

III. THEORITICAL BACKGROUND

In this section we present a brief theoretical background of Discrete Fourier Transform and Singular value decomposition of image.

A. Discrete Fourier Transform(DFT)

The DFT $F(u, v)$ of an image $f(x, y)$ of size $M \times N$ is given by[18][19][20]

$$F(u, v) = \frac{1}{MN} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x, y) \exp^{-j2\pi\left(\frac{xu}{M} + \frac{yv}{N}\right)} \quad (1)$$

And the inverse DFT is given by

$$f(x, y) = \frac{1}{MN} \sum_{x=1}^{M-1} \sum_{y=1}^{N-1} F(u, v) \exp i2\pi \left(\frac{ux}{M} + \frac{vy}{N} \right) \quad (2)$$

The DFT of an image is a complex value image and divided into phase (ϕ) and magnitude (M) and is given by equation (3) and (4) respectively.

$$\text{Phase, } \phi = \angle F(u, v) = \tan^{-1} \left[\frac{I(u,v)}{R(u,v)} \right] \quad (3)$$

And

$$M(u, v) = |F(u, v)| = \sqrt{R^2(u, v) + I^2(u, v)} \quad (4)$$

Where R and I are the real and imaginary part of the complex valued output of DFT.

B. Singular value Decomposition(SVD)

The SVD is a general linear algebra technique for a variety of application including the solution of least square problem, computing pseudo-random inverse of a matrix and multiplicative analysis. In addition SVD has been utilized in image processing application such as image coding, noise estimation and recently in watermarking.

A digital image X of size MXN, with $M \geq N$, can be represented by SVD defined by [21]

$$X = USV^T = \sum_{i=1}^N \sigma_i u_i v_i^T \quad (5)$$

Where U is a MXM orthogonal matrix and V is a NXN orthogonal matrix, S is an MXN matrix with the diagonal elements representing the singular values, σ_i of X. The matrix S has structure of the form

$$S = \begin{bmatrix} \sigma_1 & 0 & \dots & 0 \\ 0 & \sigma_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \sigma_n \end{bmatrix} \quad (6)$$

The column of the orthogonal matrix U is called the left singular vectors and column of the orthogonal matrix V are called the right singular vector. The left singular vectors of X are eigenvector of XX^T and the right singular vector are the eigenvectors $X^T X$.

IV. PROPOSED SCHEME

The proposed scheme is block based approach in which one binary bit is embedded in one non-overlapping block of the image. The details embedding algorithm is given below:

Input: Cover-image, Watermark

Output: Watermark Cover image.

1. The input cover image is divided into non overlapping block of 8X8.
2. Since one bit of data is going to be inseted into each non-overlapping block, we perform a check whether a

watermark can be inserted to this cover image by using the equation (7)

$$\text{Size} = \frac{M * N}{\text{Blocksize}^2} \quad (7)$$

3. DFT is performed in each non overlapping block and magnitude and phase is computed.

4. Magnitude block of the DFT is taken and SVD is applied to this magnitude block, the diagonal matrix(S) is computed.

5. The matrix S is used for watermark embedding the watermark by using equation (8)

$$S' = S_0 + \alpha W \quad (8)$$

Where S' is modified diagonal matrix and S_0 is the original diagonal matrix of SVD and α is the watermarking strength and W is the watermarking bit.

6. Perform inverse SVD using the modified diagonal matrix and U and V to get modified magnitude of the DFT.

7. Inverse DFT is performed on the modified magnitude and original phase to get the watermarked image.

In watermark extraction process the original image is required. The input of the watermark extraction process are - the poissibly watermarked image, the original cover image. The details steps of the watermark extraction process are given below.

1. The original cover image and possibly watermarked image are divided into non-overlapping block of 8X8.
2. DFT is performed on both the image blocks to get the magnitude and phase of both image.
3. Using only the magnitude block of both the images. SVD is applied to the respective diagonal matrix.
4. The diagonal element matrix of both the cover and watermarked image is used for decoding the watermark bit and is achieved by using the following equation.

$$W^* = \frac{(S^* - S)}{k} \quad (8)$$

Where is S^* is the diagonal matrix of the watermarked image and S is the diagonal matrix of the original image and k is the embedding strength.

V. RESULT AND DISCUSSION

The scheme was implemented in matlab. We performed expirement to verify the performance of the scheme. We use Peak Signal to Noise Ratio (PSNR) and Structural Similarity Index (SSIM) to measure the similarity between the original and watermarked image. and is defined as

$$PSNR = 10 \log_{10} \left(\frac{MAX^2}{MSE} \right) \quad (9)$$

Where MAX is the maximum possible pixel value of the original image MSE is known as Mean Square Error and is given by equation 10

$$MSE = \frac{1}{MN} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} [I(i, j) - I'(i, j)]^2 \quad (10)$$

Where I and I' are the original and watermarked image respectively of size $M \times N$. If the PSNR is greater than 30dB, the watermark image is acceptable [26]. An image quality metric that assesses the visual impact of three characteristics of an image: luminance, contrast and structure [22]. We used Normalised Correlation (NC) to compute the similarity between the original and extracted watermark and can be calculated using equation 11.

$$NC = \frac{\sum_{i=1}^M \sum_{j=1}^N W(i, j)W^*(i, j)}{\sqrt{\sum_{i=1}^M \sum_{j=1}^N W^2(i, j)} \sqrt{\sum_{i=1}^M \sum_{j=1}^N W^{*2}(i, j)}} \quad (11)$$

Where W and W^* are the original and extracted watermark. The NC value ranges from 0 to 1 and 1 is achieved when the original and extracted watermark are same and $NC \geq 0.75$ is considered to be a reasonable result.

To test the robustness of the watermarked image against geometric transform we use SURF features to estimate the scale and angle of rotation of the watermarked image.

- Read the original and watermarked image and detect the surf feature.
- Find the matching SURF between the two images and matched the feature using their descriptor.
- Features points are located in each image.
- Estimate the transformation using M-estimator Sample Consensus (MSAC algorithm, Matlab inbuilt function *estimateGeometricTransform()*).
- Find the scale and angle by using geometric transform, TFORM, since we computed the transformation from watermarked image to original image, we need to compute the inverse to recover the distortion.

Let $sc = scale * \cos\theta$ and $ss = scale * \sin\theta$

$$\text{Then } T_{inv} = \begin{bmatrix} sc & -ss & 0 \\ ss & sc & 0 \\ tx & ty & 1 \end{bmatrix}$$

Where tx, ty are x and y translation respectively

- Restore the watermarked image by resizing and rotating the image with the scale and angle.

In the experiment several standard grey scale image of size 512×512 were used (Fig. 1) as a cover image and a binary image (Fig. 2) was used as a watermark.



Fig. 1: Cover images Used



Fig. 2: Watermark Used

Keeping the embedding strength $k = 50$, the binary watermark is embedded into the cover image and Fig. 3 shows the watermark image and corresponding extracted watermark. It was observed that, greater the embedding strength k , lesser the PSNR value of the watermarked image and got a better NC of the extracted for all the images used as cover image. The SSIM value can take a value ranging from 0 and 1. From the Fig 3 we can say that, the SSIM value of all the watermarked image compared with the original image is almost 1.

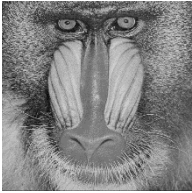


	CS
PSNR =41.5117 SSIM = 0.99174	NC =1
	CS
PSNR =41.9815 SSIM =0.97389	NC =1
	CS
PSNR =41.5581 SSIM =0.97128	NC =1



Fig. 2. Performance against Common Attacks of digital image watermarking and corresponding extracted watermark are shown

Fig 7 shows the results of the watermarking scheme against common digital watermarking attacks like JPEG compression, Salt and Pepper, Gaussian, Speckle Noise addition median filtering, imager sharpening average filtering attacks and from the result obtained we can say the scheme perform fairly well against this type of attacks. We compared our scheme with some of the existing scheme and the results obtained are shown in Table 1. The Scheme was able to achieve high PSNR value in compared to the previous two method. Except for the Gaussian Noise, Speckle noise and JPEG compression the propose scheme achieved a better robustness than the previous two scheme.

TABLE I COMPARISON OF NC VALUE OF EXTRACTED WATERMARK I IMAGE LENA UNDER DIFFERENT ATTACKS

Attack	Jain et al[24]	Guo and Prasetyo[25]	Proposed
PSNR(dB)	21.10	39.26	41.9815

No Attacks	0.9948	0.9814	1
Salt and Pepper (0.001)	0.9033	0.8442	0.99419
Salt and Pepper (0.005)	0.6383	0.5441	0.98428
Guassian Noise (0.0001)	0.9598	0.9303	0.94205
Guassian Noise (0.0005)	0.8426	0.7737	0.86075
Median Filter(3X3)	0.2306	0.7351	0.88501
Average (3x3)	0.2535	0.5192	0.84513
Image Sharpening	0.9411	0.8545	0.96157
JPEG (Q=90)	0.9591	0.9743	0.90825
JPEG (Q=80)	0.9244	0.9565	0.97224
JPEG (Q=70)	0.8930	0.9176	0.90487
Speckle Noise (0.0001)	0.9845	0.9660	0.95893
Speckle Noise (0.0005)	0.9474	0.9098	0.92577

VI. CONCLUSIONS

A DFT-SVD based image watermarking proposed in this paper in which the watermark information is added into the diagonal matrix of SVD. In this scheme, a binary watermark is embedded in the diagonal element of the SVD of Magnitude of DFT. A binary bit is embedded in every diagonal element. The scheme proposed is not a blind watermarking scheme, the original cover image is required for watermark extraction process. The attack watermark is also pre-process by finding the scaling factor and angle of attacked watermarked image using SURF features in order to restore the attacks image from geometric transformation. From the experimental results, the proposed scheme is able to achieve robustness against some of the common attacks involve in digital watermarking. The scheme also outperform some of the existing scheme. The scheme suffer from JPEG compression attacks, but it is able to achieve good results regarding common image processing attacks.

REFERENCES

- [1] Mohanty, S. P., Sengupta, A., Guturu, P., & Kougiianos, E. (2017). Everything You Want to Know About Watermarking: From Paper

- Marks to Hardware Protection: From paper marks to hardware protection. *IEEE Consumer Electronics Magazine*, 6(3), 83-91.
- [2] Chandramouli, R., Memon, N., & Rabbani, M. (2002). Digital watermarking. *Encyclopedia of Imaging Science and Technology*, 10, 0471443395.
- [3] Ganic, E., Zubair, N., & Eskicioglu, A. M. (2003, December). An optimal watermarking scheme based on singular value decomposition. In *Proceedings of the IASTED International Conference on Communication, Network, and Information Security (Vol. 85)*.
- [4] Lee, S., Jang, D., & Yoo, C. D. (2005, March). An SVD-based watermarking method for image content authentication with improved security. In *Acoustics, Speech, and Signal Processing, 2005. Proceedings.(ICASSP'05). IEEE International Conference on (Vol. 2, pp. ii-525)*. IEEE.
- [5] Calagna, M., Guo, H., Mancini, L. V., & Jajodia, S. (2006, April). A robust watermarking system based on SVD compression. In *Proceedings of the 2006 ACM symposium on Applied computing (pp. 1341-1347)*. ACM.
- [6] B.C. Mohan, S.S. Kumar, A robust image watermarking scheme using singular value decomposition, *J. Multimedia* 3 (1) (2008) 7–15.
- [7] Basso, A., Bergadano, F., Cavagnino, D., Pomponiu, V., & Vernone, A. (2009). A novel block-based watermarking scheme using the SVD transform. *Algorithms*, 2(1), 46-75.
- [8] Lai, C. C., & Tsai, C. C. (2010). Digital image watermarking using discrete wavelet transform and singular value decomposition. *IEEE Transactions on instrumentation and measurement*, 59(11), 3060-3063.
- [9] Mishra, A., Agarwal, C., Sharma, A., & Bedi, P. (2014). Optimized gray-scale image watermarking using DWT-SVD and Firefly Algorithm. *Expert Systems with Applications*, 41(17), 7858-7867.
- [10] Ali, M., Ahn, C. W., & Pant, M. (2014). A robust image watermarking technique using SVD and differential evolution in DCT domain. *Optik-International Journal for Light and Electron Optics*, 125(1), 428-434.
- [11] Makbol, N. M., & Khoo, B. E. (2014). A new robust and secure digital image watermarking scheme based on the integer wavelet transform and singular value decomposition. *Digital Signal Processing*, 33, 134-147.
- [12] Makbol, N. M., Khoo, B. E., & Rassem, T. H. (2016). Block-based discrete wavelet transform-singular value decomposition image watermarking scheme using human visual system characteristics. *IET Image Processing*, 10(1), 34-52.
- [13] Singh, A. K., Dave, M., & Mohan, A. (2014). Hybrid technique for robust and imperceptible image watermarking in DWT-DCT-SVD domain. *National Academy Science Letters*, 37(4), 351-358.
- [14] Lai, C. C. (2011). An improved SVD-based watermarking scheme using human visual characteristics. *Optics Communications*, 284(4), 938-944.
- [15] Rastegar, S., Namazi, F., Yaghmaie, K., & Aliabadian, A. (2011). Hybrid watermarking algorithm based on singular value decomposition and radon transform. *AEU-International Journal of Electronics and Communications*, 65(7), 658-663.
- [16] Zhang, H., Wang, C., & Zhou, X. (2017). A robust image watermarking scheme based on SVD in the spatial domain. *Future Internet*, 9(3), 45.
- [17] Natu, S., Natu, P., & Sarode, T. (2017, December). Improved robust digital image watermarking with SVD and hybrid transform. In *Intelligent Communication and Computational Techniques (ICCT), 2017 International Conference on (pp. 177-181)*. IEEE.
- [18] Qidwai, U., & Chen, C. H. (2009). *Digital image processing: an algorithmic approach with MATLAB*. Chapman and Hall/CRC.
- [19] O'Ruanaidh, J. J., & Pun, T. (1997, October). Rotation, scale and translation invariant digital image watermarking. In *Image Processing, 1997. Proceedings., International Conference on (Vol. 1, pp. 536-539)*. IEEE.
- [20] Gonzalez, R. C., Woods, R. E., & Eddins, S. L. (2004). *Digital image processing using MATLAB (Vol. 624)*. Upper Saddle River: Pearson-Prentice-Hall.
- [21] Sadek, R. A. (2012). SVD based image processing applications: state of the art, contributions and research challenges. *arXiv preprint arXiv:1211.7102*.
- [22] Wang Zhou, Bovik, Alan C., Sheikh, Hamid R., and Simoncelli, Eero P. Image Quality Assessment: From Error Visibility to Structural

Similarity. *IEEE Transactions on Image Processing*, Volume 13, Issue 4, pp. 600–612, April 2004.

- [23] Bay, H., A. Ess, T. Tuytelaars, and L. Van Gool. "SURF: Speeded Up Robust Features." *Computer Vision and Image Understanding (CVIU)*. Vol. 110, No. 3, 2008, pp. 346–359.
- [24] Jain, C., Arora, S., & Panigrahi, P. K. (2008). A reliable svd based watermarking schem. arXiv preprint arXiv:0808.0309.
- [25] Guo, J. M., & Prasetyo, H. (2014). False-positive-free SVD-based image watermarking. *Journal of Visual Communication and Image Representation*, 25(5), 1149-1163.
- [26] Chang, C. C., Hu, Y. S., & Lu, T. C. (2006). A watermarking-based image ownership and tampering authentication scheme. *Pattern Recognition Letters*, 27(5), 439-446.