Optimized SVD based Image Watermarking Using Optimal Pixel Adjustment

[1]Nitin kumar, [2]Vijay kumar sharma, [3]Kapil Dev Sharma
[1] Research Scholar, (nitinshan.nitin88@gmail.com)
[2]Assistant Professor,(vijaymayankmudgal2008@gmail.com)
[3]Associate Professor(shkapil@yahoo.com)
Department of Computer Science & Engineering,
Rajasthan Institute of engineering & Technology, Jaipur, India

Abstract— Digital image watermarking refers to embedding a digital data into a cover image to later prove the ownership or authentication of the document. Image watermarking find its applications in a number of areas including copyright protection, authentication, scientific analysis, medical analysis etc. to name a few. There are two important issues that watermarking algorithms need to address. Firstly, watermarking schemes are required to provide trustworthy evidence for protecting rightful ownership; Secondly, good watermarking schemes should satisfy the requirement of robustness and resist distortions due to common image manipulations (such as filtering, compression, etc.). In addition to these two requirements, the watermarking must be embedded in such a way so that the perceptible quality of the image will not go below a certain threshold. In past years, a number of image watermarking algorithms have been proposed, based on LSB, DFT, DCT, DWT etc. In this dissertation, a watermarking algorithm is presented to embed watermark in transform domain using SVD transform. SVD transform is a type of compression in which singular values of a matrix are approximated, thereby implementing a lossy compression at the cost of image quality. In this dissertation, U matrix is used for watermark embedding, by redundantly embedding the watermark bits in the 4X4 non overlapping blocks of the image. Thus, the effect of 4 bits of payload data is scattered to 10 pixels of the cover watermark image thereby giving a smooth embedding with high fidelity.

Keywords: Image watermarking, SVD, Orthogonally.

I. INTRODUCTION

For digital image watermarking systems, geometric attacks, such as rotation, scaling and translation, do not distort or remove the embedded watermark, but instead geometrically and globally modify the watermarked image to make the watermark decoder (or detector) unable to re-synchronize the received image. Most existing robust watermarking systems are block based and/or rely on the correct synchronization of the image to extract the embedded watermark. Geometric attacks destroy the synchronization and render the extracted embedded watermark incorrect or the extraction process impossible, thus making the watermark undetectable. Robust image watermarking systems, which are used to address security concerns, such as copyright protection or copy control, should guarantee resistance to geometric attacks [1]. Exhaustive search techniques try all possible combinations of the geometric distortion and can be computationally costly or infeasible. Therefore, robustness against geometric attacks still remains one of the difficult challenges in image watermarking research [1, 2]. Watermarking is something related to steganography but the main difference here is to types of data protection. Watermarking is used to copyright protection in the media files, whereas the steganography is used to protect the top important or secret data. Watermarking is similar, but has a completely different purpose. Watermarking is the process of embedding a message on the multimedia data. A watermark can be either visible or invisible.

I. RESEARCH METHODOLOGY

3. 3.1 SVD Based watermarking Illustration

The SVD based watermarking is one of the most widely accepted technique for watermarking image. The SVD watermarking in U and V matrices can be illustrated by taking the example of a 4 X 4 matrix as shown:

$$A = \begin{bmatrix} A_1 & A_2 & A_3 & A_4 \\ A_5 & A_6 & A_7 & A_8 \\ A_9 & A_{10} & A_{11} & A_{12} \\ A_{13} & A_{14} & A_{15} & A_{16} \end{bmatrix} = \begin{bmatrix} a_1 & a_2 & a_3 & a_4 \\ a_5 & a_6 & a_7 & a_8 \\ a_9 & a_{10} & a_{11} & a_{12} \\ a_{13} & a_{14} & a_{15} & a_{16} \end{bmatrix} \begin{bmatrix} b_1 & 0 & 0 & 0 \\ 0 & b_2 & 0 & 0 \\ 0 & 0 & b_3 & 0 \\ 0 & 0 & 0 & b_4 \end{bmatrix} \begin{bmatrix} c_1 & c_5 & c_9 & c_{13} \\ c_2 & c_6 & c_{10} & c_{14} \\ c_3 & c_7 & c_{11} & c_{15} \\ c_4 & c_8 & c_{12} & c_{16} \end{bmatrix}$$

Further simplification yields

The following interpretations can be derived from the above equations:

1. Changing the value of a_1, a_2, a_3 and a_4 affects the corresponding pixels of the image block. Change in the value of any of these four will result in a change in all the first row pixels. The same argument holds for all rows of a . However, changing the other rows of the U matrix alone does not have any effect on the first row of the pixels. This is true for all the rows of U matrix.
2. Changing any value of the D matrix has effect on all the pixels of A. Thus, a single change in the value of any of b_1, b_2, b_3 or b_4 changes all the pixels of the image block.
3. Change in the value of any of c_1, c_2, c_3 or c_4 (the column vector of V^T) changes the pixels of the first column of the image block. This is true for all the column vectors of V^T correspondingly.

3.2 Optimal policy of watermark embedding in the U D V^T matrix of SVD

The effect of D matrix is profound over all the pixels of the image block. This is because a change in the value of any element of the D matrix has an effect on all the pixels of the image block, thereby providing a smooth watermarking of the entire block. The effect of a change in the values of any row of U matrix changes the corresponding row of the image pixel matrix, thus providing a comparatively visible watermark, however reducing the mean square error between watermarked and the cover image. The same argument holds true of any column vector of the V^T matrix.

Consider the image block corresponding to a hypothetical gray scale image block.

$$I = \begin{bmatrix} 251 & 252 & 253 & 254 \\ 245 & 246 & 247 & 248 \\ 239 & 240 & 241 & 242 \\ 233 & 234 & 235 & 236 \end{bmatrix}$$

The SVD decomposition of this image block takes the following values:

U = -0.5183 0.6568 -0.5477 0.0001

-0.5060 0.2098 0.7304 0.4081

-0.4937 -0.2373 0.1824 -0.8165

-0.4813 -0.6843 -0.3651 0.4083

First Two Columns of Resultant Matrix

D = 974.3798 0 0 0

0 0.1232 0 0

0 0 0.0000 0

0 0 0 0.0000

V^T= -0.4969 0.6731 0.5000 0.2237

-0.4990 0.2259 -0.4999 -0.6709

-0.5010	-0.2213	-0.5001	0.6708
-0.5031	-0.6685	0.5000	0.2235

As both U and V are orthogonal matrices, modification of the values of any of these matrices will destroy the orthogonality property of these matrices.

The effect of changing the sign of the first column of elements of the U matrix can be depicted as shown in the following figure.

U =

+0.5183	0.6568	-0.5477	0.0001
+0.5060	0.2098	0.7304	0.4081
+0.4937	-0.2373	0.1824	-0.8165
+0.4813	-0.6843	-0.3651	0.4083

The sign of the determinant of this matrix is now reversed in view of the general property of the determinants which says that the determinant can be expanded across any of the row or column.

Also, one important property of the orthogonal matrix is that its determinant is always a -1 or 1. Any change in the values of elements of U or V will affect the orthogonlity property and therefore not recommended in view of the perceptibility of watermark. However, as it is clear that the singular values of the matrix D will have the effect on the perceptual quality of the image. Various levels of an image are given corresponding the level of the rank in the singular matrix.

3.3 Proposed Watermark Embedding Algorithm

As a rule, it is the largest singular values that exert the most influence on a given matrix I. In particular, when I contains the grayscale values for an image, manipulations of the smaller singular values and their corresponding singular vectors have no perceptible effect on the image. It is this mathematical principle that the proposed embedding technique is designed to exploit the visual perceptiveness of the image.

The technique for embedding watermarking bits has been given for matrices of any dimension having the values in the range 0 to 255. This represents the gray scale image. However, the proposed technique can be extended to color images by considering any or two or all the color planes of the RGB matrix of the color image. The proposed algorithm for watermark embedding works as follows:

1. A given image is partitioned into non-overlapping segments of the dimension nXn. If the given image does not have dimensions which are integer multiples of n, then the extra pixels can be ignored.
2. Each segment is then decomposed using SVD transformation. Let A be such a partition. Then the SVD decomposition of A is obtained given three matrics of dimension nXn using the following formula:

$$A = U.\ S\ .\ V^T$$

3. Here, each block of nXn will hold certain bits of payload data. The U matrix is utilized for watermark embedding. The proposed algorithm uses this 4X4 element block to hold 4 bits of payload data as per the subsequent steps:
4. Consider a 4X4 image block as shown

A =

234	200	190	189
178	134	235	139
216	101	87	23
102	206	211	119

The SVD transform of the image block is :

U = -0.6113 0.1130 0.4580 0.6354

-0.5254 **-0.1327** **0.3750** -0.7522

-0.3393 **0.8073** **-0.4631** -0.1363

-0.4849 -0.5638 -0.6597 0.1092

S = 662.1581 0 0 0

0 143.9075 0 0

0 0 64.6681 0

0 0 0 62.4121

V = -0.5427 0.8319 0.1020 -0.0559

-0.4936 -0.2069 -0.6313 0.5614

-0.5610 -0.4060 -0.0672 -0.7183

-0.3837 -0.3169 0.7659 0.4071

The 2X2 inner matrix of U matrix, (shown in red) have the values the symbols of which represents the watermark bits row-wise.

Consider the watermark bits [1,0,1,1] to be embedded in the U matrix. Recall that to embed a zero, the sign of the element must be negative and vice versa.

The modified matrix U, termed U^W can be obtained as follows:

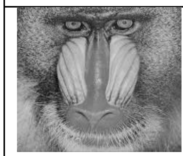
U^W = -0.6113 0.1130 0.4580 0.6354

-0.5254 **0.1327** **-0.3750** a1

-0.3393 **0.8073** **0.4631** a2

-0.4849 a3 a4 a5

Image	Watermark Data Stream Embedded	Mean Square Error (MSE)	Peak Signal to noise Ratio (PSNR in db)
 (lena)	1,1,0,1,0,1,1,0,1,1,0,1,0,1,1,0,1,1,0,1,1,0,0,1,0,1,1,0,1,1,0,1, 0,1,1,0,1,1,0,1,0,1,1,0,1,1,1,0,1,1,0,1,1,0,1,1,0,1,1,0,1,0,1,1, 0,1,1,0,1,1,0,1,1,1,0,1,1,0,0,1,1,0,1,1,0,1,1,0,1,1,0,1,1,1,0,1, 1,0,1 (total 99 bits)	594.1875	20.39157

 (old woman)	-do-	620.234	20.20525
 (baboon)	-do-	580.121	20.49562
 (camera man)	-do-	650.346	19.99936

. Table 1.1 images with watermark data stream embedded (PSNR and MSE)

Here, the values of the variables a1 to a5 needs to be obtained so as to maintain the orthogonality of the U^W matrix

This can be done by solving the following set of equation:

$$U^W *(U^W) = I$$

where I is the identity matrix.

The values of a1 to a5 can be obtained by solving the pair of linear homogeneous equations.

This gives

U^W = -0.6113 0.1130 0.4580 0.6354

-0.5254 **0.1327** **-0.3750**-0.79937

-0.3393 **0.8073** **0.4631**-2.10861

-0.4849 -0.85113-1.30775-1.54057

In this proposed algorithm, a 4X4 pixel block of the image can hold 4 bits of data, thereby providing an embedding capacity of 4/16 = 25 %.

The pixel matrix obtained with this modified value of u is

I = 250.9994 252.0238 252.9976 254.0220

245.0071 246.0309 247.0054 248.0292

287.4316 288.6596 289.8296 291.0575

232.9739 233.9965 234.9721 235.9947

Rounding off the pixel values to the nearest decimal value yields

$$I_w = \begin{matrix} 251 & 252 & 253 & 254 \\ 245 & 246 & 247 & 248 \\ 287 & 289 & 290 & 291 \\ 233 & 234 & 235 & 236 \end{matrix}$$

whereas the original image matrix is

$$I = \begin{bmatrix} 251 & 252 & 253 & 254 \\ 245 & 246 & 247 & 248 \\ 239 & 240 & 241 & 242 \\ 233 & 234 & 235 & 236 \end{bmatrix}$$

There by producing mean square error 97.50385.

The Peak Signal To Noise ratio for this hypothetical image block can be computed as per the given formula.

$$PSNR_{dB} = 10 * log_{10} \frac{255 * 255}{\sum_{i=1}^{M} \sum_{j=1}^{N} \quad [I(i,j) - I_w(i,j)]^2}$$

The value of PSNR for the image block is 20.39157.

The results for Lena image for various image block sizes, step function, and watermark message bit stream.

2 Message Embedding in U matrix

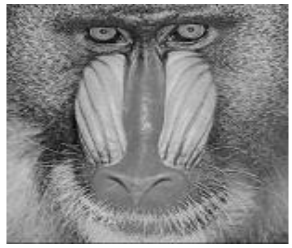
Consider the images of size 256 X 256 as shown in the table given below. For a total of 256*256 elements in the U matrix, 128 bits can be embedded in the matrix thereby providing an embedding capacity of 255/(256*256) = 25 %.

The values of MSE and the PSNR can be tabulated as shown in the table 1.1

3 Comparison with previous work

The SVD based watermark embedding proposed by Seema Rana et.al. [22], uses approximation matrix of the third level of image in DWT domain is modified with SVD to embed the singular value of watermark to the singular value of DWT coefficient. The results of the proposed work with those corresponding to the previous work[22] are investigated on different types of images using the PSNR values [23][24]. The comparison is given in table 1.1 below:

Leena.jpg



Baboon.jpg

Camera man.jpg

Fig 4.10 images with comparison lena, baboon and camera man

The PSNR metric of the above three images are illustrated as shown:

Table 1.2 The PSNR and MSE metric of the above three images with SVD values

Images	Lena		Baboon		camraman	
SVD Values	MSE	PSNR	MSE	PSNR	MSE	PSNR
1	110	27.7168	90	28.5888	140	26.6692
2	115	27.5233	114	27.5616	154	26.2556
3	117	27.4484	129	27.0241	160	26.0896
4	120	27.3389	132	26.9256	166	25.9292
5	122	27.2671	135	26.8277	170	25.8261
6	140	26.6692	140	26.6692	180	25.5788
7	160	26.0896	147	26.4573	193	25.2753
8	170	25.8261	159	26.1163	204	25.0345
9	175	25.7002	168	25.8771	220	24.7068
10	200	25.125	190	25.3437	233	24.4574

Conclusion

A conclusion section A robust blind watermarking technique is proposed that embeds and extracts the watermark information effectively. In the proposed method, a watermark data is embedded in the U matrix of the SVD transform. The proposed watermarking technique gives high embedding capacity with high PSNR as the 4 bit information is marked in 16 pixels of the cover image. The watermarking process provides qualities like imperceptibility, robustness and security. The efficiency and robustness of the watermarking scheme is evaluated with common image processing attacks such as noising, filtering, intensity adjustment, histogram equalization, JPEG compression. Experimental results shows that the watermark is robust against these attacks. The simulation results of currently devised method are compared with that of previous work [2], and the results obtained show that the proposed technique is highly robust against attacks such as JPEG compression. As a future scope of the process, it is proposed to devise techniques do that watermarking process will be robust against cutting and cropping effects using redundant embedding in the image segments..

References

1. Hai Tao, Li Chongmin, Jasni Mohamad Zain, Ahmed N. Abdalla "RobustImage Watermarking Theories and Techniques: A Review", *Journal of Applied Research and Technology*, Volume 12, Issue 1, Pages 122-138.

2. Afrin Zahra Husaini & M. Nizamuddin. "Challenges and Approach for a Robust Image Watermarking Algorithm"International Journal of Electronics Engineering, 2(1), 2010, pp. 229-233.

3. Deepa Mathew K, Karunya University,Coimbatore, India."SVD based Image Watermarking Scheme",IJCA Special Issue on "Evolutionary Computation for Optimization Techniques" ECOT, 2010.

4. Shubham Srivastava, Arun Kumar."Image Enhancement in Digital Image Watermarking Using Hybrid Image Transformation Techniques".IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) e-ISSN: 2278-2834,p-ISSN: 2278-8735.Volume 11, Issue 2, Ver. II(May-Jun.2016), PP 116-121.

5. Abdelhamid Benhocine and Lamri Laouamer, Anca Christine Pascu,Laurent Nana,"New Images Watermarking Scheme Based on Singular Value Decomposition".Journal of Information Hiding and Multimedia Signal Processing, 2013 ISSN 2073-4212,Ubiquitous International Volume 4, Number 1, January 2013.

6. Shreya Tayal , SPS Chauhan. "An Optimal Digital Image Watermarking based on SVD and Genetic Algorithm".International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064.

7. Chih-Chin Lai,"An improved SVD-based watermarking scheme using human visual characteristics", Elsevier Optics Communications 284 (2011) 938–944.

8. Dr. Swati Sherekar, Dr. V.M.Thakare & Dr. Sanjeev Jain."Attacks and Countermeasures on Digital Watermarks:Classification, Implications, Benchmarks",International Journal Of Computer Science And Applications Vol. 4, No. 2, June July 2011 ISSN: 0974-1003.

9. Mr.Mitesh Patel. "The study of various attacks on Digital watermarking technique". International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 3 Issue 5, May 2014.

10. S. S. Sudha, K. K. Rahini. "Prevention of Watermarking Attacks using Cryptography Method".International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 2, February 2014, ISSN (Online) : 2278-1021 ISSN (Print) : 2319-5940.

11. Mansi &Navneet Verma . " An Analytical Review on Various Watermarking Techniques".International Journal For Advance Research In Engineering And Technology. Volume 4, Issue IV, April 2016 ISSN 2320-6802.

12. Pragya Jain &Anand S. Rajawat. "Fragile Watermarking for Image Authentication: Survey".International Journal of Electronics and Computer Science Engineering ISSN- 2277 1956.

13. Kiranyaz, S. & Ince. T. & Gabbouj M. "Multidimensional Particle Swarm Optimization for machine learning & Pattern Recognition" Springer 2014, ISBN 978-3-642-37845-4.

14. JM Brick and G Kalton. "Handling Missing Data in Survey Research", Statical Methods in Medical Research 1996, p5, 215-238.

15. Y. Shantikumar Singh , B. Pushpa Devi and Kh. Manglem Singh. "A Review of Different Techniques on Digital Image Watermarking Scheme",A Review of Different Techniques on Digital Image Watermarking Scheme. (ISSN : 2319-6890) 01 July 2013.

16. Pracheta Bansal and Dr. Anamika Bhargava, "A Study of Digital Image Watermarking techniques. ICSTM, University of Delhi(DU), Conference Center New Delhi (India) 27 September 2015.

17. Mr.Manjunatha Prasad.R and Dr.Shivaprakash Koliwad, "A Comprehensive Survey of Contemporary Researches in Watermarking for Copyright Protection of Digital Images", IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.4, April 2009.

18. Amit Mehto & Neelesh Mehra, "Techniques of Digital Image Watermarking: A Review" International Journal of Computer Applications (0975 – 8887) Volume 128 – No.9, October 2015

19. Mr. D.G.Vaghela, Mr. V.P.Gohil, Prof. Ramlal Yadav, "Digital Watermarking: Combining DCT and DWT Techniques",Journal of Information, Knowledge And Research In Computer Engineering. ISSN: 0975 – 6760| NOV 12 TO OCT 13 | VOLUME – 02, ISSUE – 02 p-467.

20. Emir Ganic and Ahmet M. Eskicioglu, " A Dft-Based Semi-Blind Multiple Watermarking Scheme for Images". January 2004.

21. Mrugesh Prajapati . "Transform Based Digital Image Watermarking Techniques for Image Authentication". International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 5, May 2014.

22. Seema, Sheetal Sharma. "DWT-SVD Based Efficient Image Watermarking Algorithm to Achieve High Robustness and Perceptual Quality". International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 2, Issue 4, April 2012

23. Sharma V.K., Srivastava D.K. (2017) Comprehensive Data Hiding Technique for Discrete Wavelet Transform-Based Image Steganography Using Advance Encryption Standard. In: Vishwakarma H., Akashe S. (eds) Computing and Network Sustainability. Lecture Notes in Networks and Systems, vol 12. Springer, Singapore.

24. Vijay Kumar Sharma, Dr. Devesh Kr Srivastava and Dr. Pratistha Mathur, "A Study of Steganography Based Data Hiding Techniques", International Journal of Emerging Research in Management & Technology, ISSN: 2278 - 9359 (Volume - 6, Issue -4), April 2017.