ISSN 2229-5518

Increase Security of Images from Attacks Using Watermarking Technique

Ankita Durge, Prof.Alka Jaiswal

Abstract: Digital watermarking is used to hide the information inside a signal, which cannot be easily extracted by the third party. Its widely used application is copyright protection of digital information. It is different from the encryption in the sense that it allows the user to access, view and interpret the signal but protect the ownership of the content. One of the current research areas is to protect digital watermark inside the information so that ownership of the information cannot be claimed by third party. With a lot of information available on various search engines, to protect the ownership of information is a crucial area of research. In recent year, several digital watermarking techniques are presented based on discrete cosine transform (DCT), discrete wavelets transform (DWT) and discrete fourier transforms (DFT). In this paper, we proposed an algorithm for digital image watermarking technique based on singular value decomposition; both of the L and U components are explored for watermarking algorithm. This technique refers to the watermark embedding procedure and watermark extracting procedure. Digital image watermarking techniques for copyright protection is robust. The experimental results prove that the quality of the watermarked image is good and that there is strong resistant against many attacks. The image watermarking techniques help to achieve artificial intelligence. Digital image watermarking is the most effective solution in this area and its use to protect the information is increasingly exponentially day by day.

Index Terms – ***Digital image watermarking copyright protection; Singular value decomposition; Watermark embedding procedure; Watermark extracting procedure.***

---

1 INTRODUCTION

Digital watermarking is a technique that embeds data called watermark into a multimedia object such that watermark can be detected to make an assertion about the objects. It can be categorized as visible or invisible. Example of visible watermarking is the logo visible superimposed on the corner of television channel in a television picture. On the other hand, invisible watermark is hidden in the object, which can be detected by an authorized person. Such watermarks are used for suit the author authentication and detecting unauthorized copying. The novel technology of digital watermarking has been sponsored by many consultants as the best method for such multimedia copyright protection problem [1, 2], O digital watermarking will have a variety of useful applications such as digital cameras, medical imaging, image databases, and video on demand systems, and many others. In recently years, many digital watermarking techniques have been proposed in the literature which is based on spatial domain technique and frequency domain technique. These techniques are used in watermark embedding algorithm and watermark extracting algorithm [3]. In 2005, Chen [4] proposed a singular value decomposition scheme that based on components of D and U. Without using DWT, DCT and DFT transforms. They showed that quality of watermarked image is good on their schemes. In 2007, Patra [5] introduced a novel digital watermarking method, which is based on single key image for extracting different watermarks. In this method, they used Arnold transform technique in watermark embedding and extraction, which is based on DWT and DCT algorithm. With the popularity of internet and availability of large storage devices, storing and transferring an image is simple and feasible. They showed that robustness of the algorithm against many signal processing operations. In 2010, Cox [6] suggested two blind, imperceptible and robust video watermarking algorithms that are based on singular value decomposition. Each algorithm integrates the watermark in the transform domain. They used the components of matrices such as U and V. Their schemes are shown to provide very good performance in watermarked video as compared to Chan [4].

Most of the domain transformation watermarking techniques works with DCT and DWT. However singular value decomposition (SVD) is one of the most powerful numeric analysis techniques and used in various requirements. These requirements can be organized and described as follows [7, 8]. In this paper, we will describe a digital image watermarking algorithm which is based on singular value decomposition technique. This paper is organized as follows. In Section 2, we introduce the SVD watermarking techniques briefly. In Section 3, we propose the embedding and extraction procedure. In Section 4, we evaluate the performance of watermark image. In section 5, we show the experimental results and Section 6 conclude the paper.

2 A review of related work

Singular value decomposition (SVD) is a mathematical technique based on linear algebra and used by factorization of a real matrix or complex matrix, with many useful applications in signal processing and statistics [9].

2. A. Singular Value Decomposition (SVD)

Singular value decomposition is one of a number of valuable numerical analysis tools which is used to analyze matrices. It can be appeared at from three jointly compatible points of view. On the other hand, we can see it as a method for transforming correlated variables into a set of uncorrelated ones that better expose the various relationships among the original data items. At the same time, SVD is a method for identifying and ordering the dimensions along which data points demonstrate the most variation. This attach the third way of viewing singular value decomposition, which accepted the most variation, it's possible to find the best approximation of the original data points using less dimensions. Hence, SVD can be seen as a method for data reduction. In SVD transformation, a matrix can be decayed into three matrices that are having the same size as the original matrix. It is useful to establish a contrast with Gaussian elimination and its equation. Given A is a n x n square matrix, this matrix can be decomposed into three components, L, D and U, respectively such that.

$$[L\ D\ U] = \text{SVD}(A),\ A = LDU^{1}$$

$$L^{-1} \text{ where } A = LDU.$$

$$= \begin{pmatrix} l_{1,1} & l_{1,2} & l_{1,n} \\ l_{2,1} & l_{2,2} & l_{2,n} \\ l_{3,1} & l_{3,2} & l_{3,n} \end{pmatrix} \begin{pmatrix} \sigma_{1,1} & \sigma_{1,2} & \sigma_{1,n} \\ \sigma_{21} & \sigma_{2,2} & \sigma_{2,n} \\ \sigma_{3,1} & \sigma_{3,2} & \sigma_{3,n} \end{pmatrix}$$

$$\begin{pmatrix} u_{1,1} & u_{1,2} & u_{1,n} \\ u_{21} & u_{2,2} & u_{2,n} \\ u_{3,1} & u_{3,2} & u_{3,n} \end{pmatrix} \qquad (1)$$

$$= \sum_{i=1}^{n} \sigma_i l_i u_i^{T}$$

.

Where the L and U components are real unitary matrices or complex matrices with small singular values, and the D component is an n x n diagonal matrix with larger singular value or eigen vector values entries which specify o_u» °2.2..... «k,k, k+i= ..... o_n.n = 0- Z $^{\text{are non zero}}$ matrix by diagonals of A. Reduced singular value decomposition is the mathematical technique underlying a type of document retrieval and word semblance method. These are also known as Latent Semantic Indexing or Latent Semantic Analysis.

. the section title are not indented. Only the initial, introductory paragraph has a drop cap.

In this way, the three components of matrices L, D, and U specify AUJ = O; li and $Hj^{T}A = OjUi^{7}$.

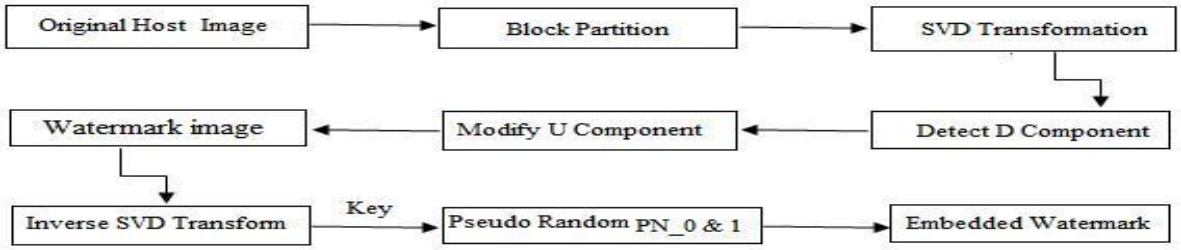
Digital image watermarking techniques has some advantages that used singular value decomposition. Firstly, SVD transformation from the size of memory is not fixed and can be represented by a rectangle or a square. Secondly, SVD are increase in accuracy and decrease the memory requirement. Thirdly, digital images in singular values are less affected if general image watermark is executed. Fourth, singular value decomposition include by algebraic properties.

3 PROPOSED WATERMARKING TECHNIQUES

We proposed a singular value decomposition technique and quantization - based watermarking technique. The watermarking techniques can be represented by three components, L, D and U. It relies on row operations and column operations. Row operations involve pre-multiplying matrix and column operations involve post-multiplying matrix. The D component can be explored with a diagonal matrix. These techniques depend upon the watermark embedding procedure and watermark extraction procedure.

3. A. Watermark Embedding Procedure

The digital watermarking procedure can be followed by singular value decomposition techniques, which involve the characteristics of the D and U components. In the embedding procedure, the largest coefficients in D component were customized and used to embed a watermark. The adjustment was determined by the quantization method. We will start the procedure by applying SVD transformation on original image and to reconstruct the watermarked image. Because the largest coefficients in the D component can oppose with general image processing, the embedded watermark was not really affected. In this way, the quality of the watermarked image can be decomposed by quantization method. In our inspection, two important features of the D and U components are found. In the first feature, the number of non zero coefficients in the D component could be used to determine the complexity of a matrix. Commonly, the greater number of the non-zero coefficient can be specified by greater complexity. In the second feature, the relationship between the coefficients in the first column of the L component could be sealed, when usually image processing was presented as shown in figure 2. The watermarks embedding algorithm can be described as follows.



Step 1: Read the original image blocks.

Step 2: Apply singular value decomposition (SVD) transformation.

Step 3: Extract the largest coefficient D (1, 1) from each D component and quantize by using a predefined quantization coefficients A. Suppose that S = D (1,1) mod A.

Step 4: Perform embed the two pseudo-random sequences PNO,

PN1, that is applied to the mid-band coefficients. If A is the matrix of the mid band coefficients of SVD transformed block, then embedding is done as follows:
If the watermark bit is 0 then, D '(1, 1) = D (1, 1) + K/4 -A. so that [A< 3K/4] Otherwise, if the watermark bit is 1 then, D'(1,1) = D(1, l)-k/4+A so that [A<K/4]
Step 5: Apply the inverse of singular value decomposition transformation to reform the watermarked image.

3. B. Watermark Extracting Procedure

The watermark extracting procedure is similar to the watermark embedding procedure. Extraction procedure is the same as embedding one and pre-filtering is used before applying SVD transform to superior split watermark information from original image. The watermark extraction procedure is performed as described by the following steps. The first three steps of the watermark extracting procedure are same as the watermark embedding procedure except that the original image is replaced with the watermarked image previously, an embedded block is detected according to the feature of the D component and PRNG, the relationship of the U component coefficients is observed. If a positive relationship is detected, the extracted watermark has assigned a bit value of 1. Otherwise, the extracted watermark has assigned a bit value of 0. These extracted bit values convert the original image SVD from the extracted watermark. The extracted watermark can be specified by original watermarked image and as shown in figures.

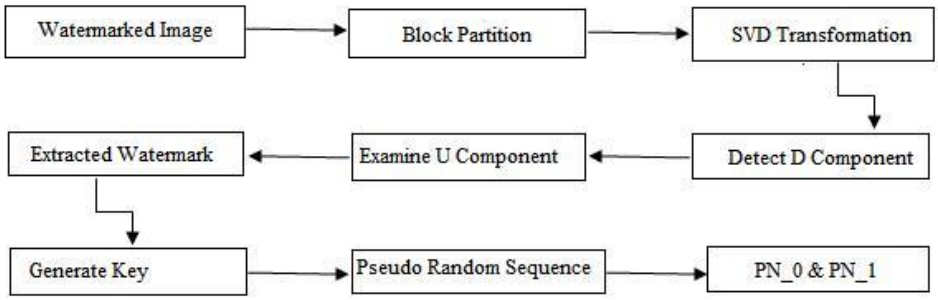


Figure 3. Watermark Extraction Algorithm

Step 1: Read the watermarked image into blocks.

Step 2: Apply the SVD transformation.

Step 3: Extract the largest coefficients D> (1, 1) from each D component and quantize by using a predefined quantization coefficients A. Suppose that S = D (1,1) mod A.

Step 4: Regenerate the two pseudo random sequences number using the same key, which is used in the watermark embedding procedure.

Step 5: For an extraction watermark bit valued of zero, if A<K/2. On the other hand, the extraction watermark bit value of one, if A>k/2.

Step 6: The watermark is restructured using the extracted watermark bits, and compute the similarity between the original watermark and extracted watermarks.

In this technique, the steady property of the largest D component coefficients resists the image processing was preserved. More trix in which only a small number of the coefficients could be used. In addition, the modification of the largest coefficients would cause a largest measure of image humiliation.

4. PERFORMANCE EVALUATION

We evaluated the performance of the SVD image watermarking algorithms. The performance of the watermarking methods can be measured by imperceptibility and robust capabilities. Imperceptibility means that the superficial quality of the original image should not be distorted by the presence of watermark image. On the other hand, the robustness is a measure of the intentionally attacks and unintentionally attacks. It was found that the image quality measured by peak signal to noise ratio among the watermarked images was larger than 42 db. This peak signal to noise ratio is defined as;

$$PSNR=10log_{10}\{\mathbf{MAX}^2/\mathbf{MSE}\} \quad (2)$$

$$=20log_{10}\{\mathbf{MAX}/\sqrt{\mathbf{MSE}}\}$$

The PSNR is employed to evaluate the difference between an original image and watermarked image. For the robust capability, mean absolute error (MSE) measures the difference between an original watermark W and corresponding extracted watermark W^1 as shown by equation.

Generally, if PSNR value is larger than 40db the watermarked image is within acceptable degradation levels, i. e the watermarked is almost invisible to human visual system. A lower mean absolute error reveals that the extracted watermark W resembles the W^1 more closely. The strength of digital watermarking method is accessed from the watermarked image, which is further degraded by attacks and the digital watermarking performance of proposed method is compared with that of Chen [4]. If a method has a lower MSB (W, W^1), it **is** more robust.

5 EXPERIMENTAL RESULTS

The experimental results are simulated with the software MATLAB 7.10 version. We are using a 256x256 'Lena', 'facial', and 'Moon' as the gray scale original host image, and (3) a 256x256 grey-scale image of the watermark image. The three images are shown in Fig. 4, 5 and 6 respectively. In the proposed method, we select the largest complexity of blocks; the original images can be separated into blocks of 4^{x} 4 pixels. Each block can be transformed into L, D, and U components by singular value decomposition. And then, a set of blocks with the same size as the watermark was selected, according to the feature of the D component. For an embedding watermark block, the relationship between the L component coefficients can be examined and the coefficients were modified, according to the watermark to be embedded. In our experiment, the original images and watermarked image quality shown by figure 4.

Figure 4. Three original images of 256 × 256 pixels (a) The original Lena Image (b) The original Facial Image (c) The original Moon Image.

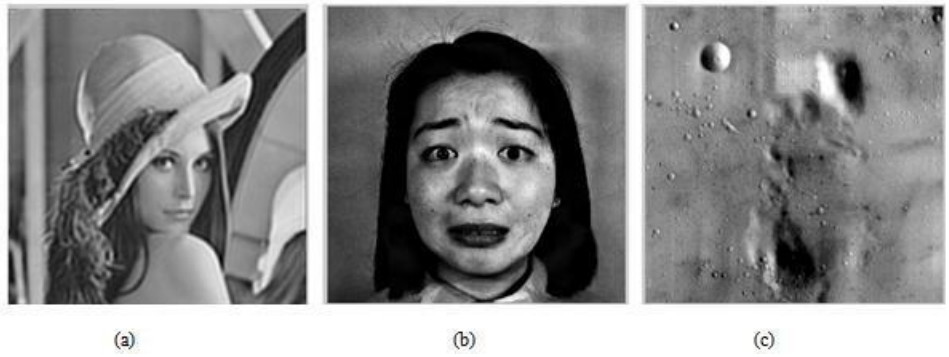


Figure 5.Three watermarked images of 256×256 pixels (a) The watermarked Lena Image (b) The watermarked Facial Image (c) The watermarked Moon Image.

Table 1. The parameter values of attacked embedded watermarked image

Parameters	NO Attacks	Cropping Attacks	Pyramid Attacks	Rotation Attacks	Noise Attacks	Blurring Attacks	PSNR (DB)
E1	45.59	67.49	81.76	48.15	40.16	45.59	$\alpha = 0.3$
E2	51.67	57.77	84.01	51.97	43.34	51.67	$\alpha = 0.3$
E3	37.97	59.61	76.00	40.10	43.28	37.97	$\alpha = 0.3$

Table2. The parameter values of attacked extraction watermarked image

Parameters	NO Attacks	Cropping Attacks	Pyramid Attacks	Rotation Attacks	Noise Attacks	Blurring Attacks	PSNR (DB)
E1	35.50	48.20	59.81	36.33	33.46	29.27	$\alpha = 0.4$
E2	39.70	48.19	64.07	40.66	35.57	39.70	$\alpha = 0.4$
E3	35.68	49.89	59.83	36.75	35.50	35.68	$\alpha = 0.4$

The simulation results recommend that this algorithm can be robust against many different types of attacks such as no attacks, rotation attacks, noise attacks, and cropping attacks.

Figure 6. A similarity between quality of original image and Watermarked Image: (a) E1 (45.59 db), (35.50 db), E2 (51.67 db), (39.70 db), E3 (33.97 db), (35.68 db)

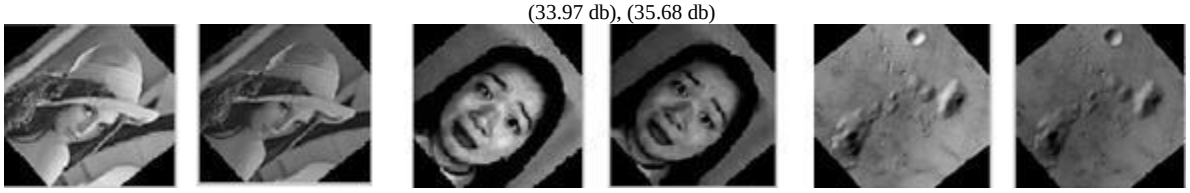


Figure 7. A similarity between quality of original image and Watermarked Image: (a) E1 (48.15 db), (36.33 db), E2 (51.97 db), (40.66 db), E3 (40.10db), (36.75db)

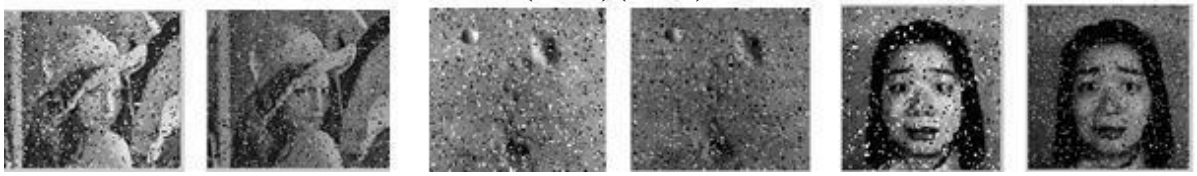


Figure 8. A similarity between quality of original image and Watermarked Image: (a) E1 (40.16 db), (33.46 db), E2 (51.67 db), (35.57 db), E3 (37.97 db), (35.50 db)

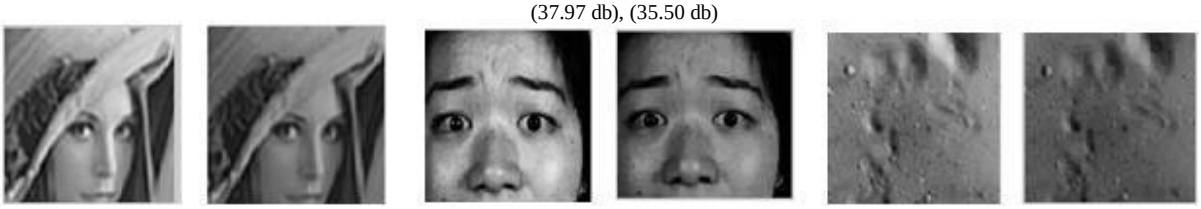


Figure 9. A similarity between quality of original image and Watermarked Image: (a) E1 (67.49 db), (48.20 db), E2 (57.77 db), (48.19 db), E3 (59.61 db), (49.89 db)

From the other data in table1 and table2, we can see the performance of our algorithm against the different geometrical attacks. Thus the proposed digital image watermarking algorithm can be used for protecting the copyrights of digital images.

6 CONCLUSION

We introduced a digital image watermarking algorithm based on singular value decomposition. Digital image watermarking is one crucial area of research. Researchers have proposed various security techniques for to protect the ownership of digital information. It is used in security tools, security features and security parameter. We presented a technical discussion on digital watermarking techniques such as cropping attacks, rotation attacks, noise attacks and filter attacks. Digital watermarking can be utilized for aunthication of data, copyright protection and communication process. It provides a consistent performance on different original image and watermarked image in all the experiments.

The Experimental results prove that the quality of the watermarked image is better. Furthermore, the extracted watermark can be easily identified.

REFERENCES

[1] M. Barni and B. Bovid, "Digital Watermarking-for Copyright Protection: A Communication Perspective, IEEE Communication Magazine, vol.
39, no. 8, pp. 90-91,2001.

[2] A. Kumar and V. Santhi, "A Review on Geometric Invariant Digital Image Watermarking Techniques", International Journal of Computer Applications, vol. 12, no. 14, pp.31-36, 2010.

[3] F. Petitcolas, R. Anderson and M. Kuhn, "Attacks on Copyright Marking Systems in Information Hiding", LNCS, Berlin, vol. 1524, pp. 218-238, 1998.

[4] C. C. Chang and P. Tsai, "SVD-based Digital Image Watermarking Scheme", Pattern Recognition Letters, vol. 26, pp. 1577-1586,2005.

[5] T. V. Nguyen and J. C. Patra, "A Simple ICA based Digital Image Watermarking Scheme", Digital Signal Processing, vol. 18, pp. 762-776, 2007.

[6] I. J. Cox and J. P. Linnartz, "Some General Methods for Tampering With Watermark", IEEE Journal on Selected Areas in Communications, vol. 16, pp. 587-593, 2010.

[7] Z. Bojkovic and D. Milovanovic, "Multimedia Contents Security :Watermarking Diversity and Secure Protocols", 6th International Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Service, TELSIKS, vol. 1, no. 3, pp. 377-383, 2003.

[8] S.J. Lee, S. H. Jung, "A Survey of Watermarking Techniques Applied to Multimedia", IEEE Transactions on Industrial Electronics, vol. 12 pp. 272-277,2001.

[9] Y. Trank and W. Frank," Robust Image Watermarking in The Spatial Domain", Signal Processing, vol. 13, no 14, pp. 385-403, 1997.

[10] E. Koch and J. Zhao, "Robust Labels into Images for Copyright
Protection", International Congress on Intellectual Property Rights for Specialized Information, Knowledge and New Technologies, Vienna, pp. 1064-1087, 1985.