IJASRM International Journal of Advanced Scientific Research and Management, Vol. 2 Issue 8, August 2017.
www.ijasrm.com
ISSN 2455-6378

A SVD and Adaptive Quantization Based Robust Digital Image Watermarking Technique

Usha Devi [1] and Singh Rajeev Kumar [2]
[1] Research Scholar, Bhagwant University,
Ajmer, Rajasthan,. India

[2] Associate Professor, Bhagwant University,
Ajmer Rajasthan India

Abstract
Digital Watermarking is a technology, to facilitate the authentication, copyright protection and Security of digital media. The objective of developing a robust watermarking technique is to incorporate the maximum possible robustness without compromising with the transparency.

Singular Value Decomposition (SVD) using Adaptive Quantization provides this objective of an optimal robust watermarking technique. In this paper watermarking technique has been developed using Adaptive Quantization and Singular Value Decomposition Technique (SVD). In this quantization step has been used and after that PSNR value is calculated and compare with the PSNR values of watermarked image designed by using Singular Value Decomposition technique.

Keywords: *SVD, DWT, PSNR, Adaptive Quantization, Quantization Step.*

1. Introduction

The development and growth of the internet has created new challenges to protect digital data from piracy [1]. Digital watermarking technique provides a superior and robust solution for ownership problem. It becomes much important to maintain the copyright of the digital data which is a form of intellectual properties. Digital watermarking technique embeds copyright information or watermark in to original host image. The embedded information should be imperceptible. These watermarks are difficult to remove by altering or damaging the original host image. The digital image watermarking is a process of embedding watermark in to audio signal to show authenticity and ownership proof. The watermark is permanently embedded in to the digital image and embedding should not degrade the quality of digital image.

The term digital watermarking [1], first came into existence in 1993 when Tirkel presented watermarking techniques to hide the watermark data in the image. Due to the rapid growth in computer and communication industry, cost effective and popular digital recording and storage devices made it possible to copy, and have unauthorized access of the original digital multimedia contents. Digital watermarking has evolved as a solution to these problems of copyright protection, authorization, illegal modifications and distributes the data in an effortless ways without having legal permission of the author. Digital watermarking provides a way to imperceptibly embed digital signal or information into the digital multimedia content. The watermarking is done by embedding a watermark signal into the host data for the purpose of copyright protection, access control. Broadcast monitoring etc. A watermark can be a signal, a tag or a label. The embedding process should be in such a way that the watermark image can be extracted from the watermarked image any perceptible loss of quality of the host image. Watermarking techniques can be classified according to domain, visibility and permanency.

According to domain, watermarking is classified as spatial domain and transform domain [2]. In spatial domain, watermark is embedded directly into the pixel value of the original image. In transform domain, the watermark is embedded by modulating the coefficients in a transform such as discrete cosine transforms (DCT), discrete Fourier transform (DFT), discrete wavelet transform (DWT). The transform domain provides more robust and secure watermarking which has attracted many researchers to work in this domain. The main advantage of working in the transform domain is the fact that when the image is inverse transformed the watermark is distributed irregularly over the host image which makes the attacker difficult to modify and copy the host image.

The singular value decomposition (SVD) [3] is a kind of transform domain technique. SVD divides a N x N matrix into three matrices:

$A=USV^T$, where S is an N x N diagonal matrix. U and V^T are N x N orthogonal matrices, whose column vectors are u_i's and v_i's, respectively. The important property of the singular values is that any modifications done on these values do not show any change in the respective matrix. Based on this property, the singular values are modified with the singular values of the watermark image. An N x N image can have N singular values that reveal various tolerances to modifications [4]. As there is no idea of the sensitivity of the image to various scaling factors. Therefore, an optimization algorithm [5] is needed to obtain optimum scaling factors [6] that can give highest possible robustness and transparency. For this purpose, firefly algorithm [7] is used, which is a metaheuristic algorithm for optimization problems. The algorithm is based upon the flashing behavior of fireflies. Randomly generated solutions are treated as fireflies. It has two basic components- brightness and attractiveness. Attractiveness is directly proportional to the brightness but decreases with distance. Brightness is computed on the basis of an objective function. Thus the basic rule is that the brighter firefly will attract the more fireflies and if no such brighter firefly is present then the firefly will move in random direction [8]. This random movement may decrease the brightness depending on direction. As a consequence the overall performance of the algorithm is decreased in that particular iteration. Now if we change this property of random movement by moving in a particular direction in which its brightness increases then it will not degrades the performance in that iteration. If such direction does not exist then the firefly will remain at its current position. Hence the modified singular values (SV) by the watermark values will be more robust and secure. Also it will enhance the overall watermarking scheme and decreases the trade-off between robustness and transparency and less vulnerable to various attacks. The paper is organized in the following manner: Section II elaborates the description of Singular Value Decomposition (SVD); Section III is for Adaptive Quantization. The proposed model is being given in Section IV. Section V gives the implementation results of the proposed model. Section VI gives the conclusion of the paper.

2. Singular Value Decomposition (SVD)

Singular value decomposition (SVD) comes under the category of transform domain technique of digital image watermarking, which is akin theory of diagonalizing of symmetric matrix in linear algebra. SVD decomposes a matrix into three sub-parts: U, S and V. U and V are the orthogonal matrices while S is the diagonal matrix. These diagonal elements are called the singular values of the corresponding matrix.This decomposition can be illustrated as:

$$A = USV^T \quad (1)$$

Where A is a matrix of dimension m x n. U is made up of the eigen vectors of AA^T and is called left singular vector. V is formed by the orthogonal vectors of A^TA and is called right singular vector. S contains the square roots of either U or V in descending order in its diagonal being a diagonal matrix. Let the rank of the matrix A be r (r<n), then the diagonal elements of S will follow the following relation:

$$\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_r > \alpha_{r+1} = \alpha_{r+2} \ldots = \alpha_n = 0 \quad (2)$$

Now can be derived as:

$$A = \sum_{i=1}^{r} \alpha_i \, u_i v_i \quad (3)$$

Where α_i is the diagonal element of matrix S at i^{th} position. The singular values gives the luminance of the image at each i^{th} position, whereas singular vectors gives the geometrical property.The most important property of SVD is that if any changes are applied to the singular values then will be no significant changes seen on the given matrix. Using this property the watermark image is modified by applying change in its singular values and embedded into the singular values of the host image without getting any distortions and any perpetual change.

A. Properties of SVD:

1. Singular values preserve the energy as well as prevent the image from attacks.
2. The matrix in SVD can be variable. It need not be always scalar.
3. The singular values α_i are unique in the matrix S.
4. The rank of the matrix is given by the the non-zero elements in the diagonal matrix, S.

3. Adaptive Quantization

To compress the maximum value into minimum or we can say in single value, defined as Quantization. In quantization precision is reduced. It is lossy compression. Adaptive Quantization is a linear quantization. In this step size is not fixed it varies so as to analyze the variance. Adaptive quantization [5] combine with SVD has been used to improve the quality of an image. With this scheme, high transparent and more robust watermarked image has been formed. Algorithm is as follow using Adaptive Quantization:-

1. Standard deviation (σBk) is calculated for each block (Bk).
2. Maximum value (σM) and minimum value (σm) for all σBk.
3. Quantization step (dk) is calculated for different blocks. k= 1, 2 ……. N N is number of blocks, dm and dM are minimum and maximum quantization step. In our calculation, dm and dM is taken as 9 and 54.

4. Proposed Watermarking Model

Let the host image be H and watermark image be W of size N x N, then the following are the steps of the algorithm by which this model works:

Embedding algorithm using SVD –

1. Read original image and watermark image.
2. Check image is RGB then, Convert to gray scale and go to step Otherwise, Go to step 3.
3. Segment image into blocks of size w * w.
4. Compute i1 = || v || + 1, where k = 1, 2……N

$$v = (\lambda_1^k, \lambda_2^k, \ldots, \lambda_w^k),$$

5. Compute integer number s = floor (i1 / dk).
6. Convert watermark image into black and White image. Embedding one bit of watermark image If b=1 then If s is odd number, then s=s+1 Else s remain unchanged If b=0 then If s is even number, then s=s+1 Else s remain unchanged
7. Calculate nvd = dk * s + dk / 2
8. Compute matrix

$$\widetilde{B}_k = \sum_{i=1}^{w} \gamma_i^k U_i(k) V_i^T(k).$$

9. Calculate PSNR value of watermarked image in comparison to original image PSNR = 10 * log10 (255 * 255 / MSE) Here, v is known as the vector of singular values. nvd is used to calculate modified singular values. dk is quantization step for i1 corresponding to block. MSE is mean square error.

The extracting algorithm is describes as follows:

1. Segment the watermarked image into block Of size w * w.
2. Compute nv= || u || + 1, Where u is formed by singular values of each block that has been divided of watermarked image.
3. Compute S1 = floor (nv / dk) 4. If S1 is even Then embedded bit is 1 Otherwise, Embedded bit is 0

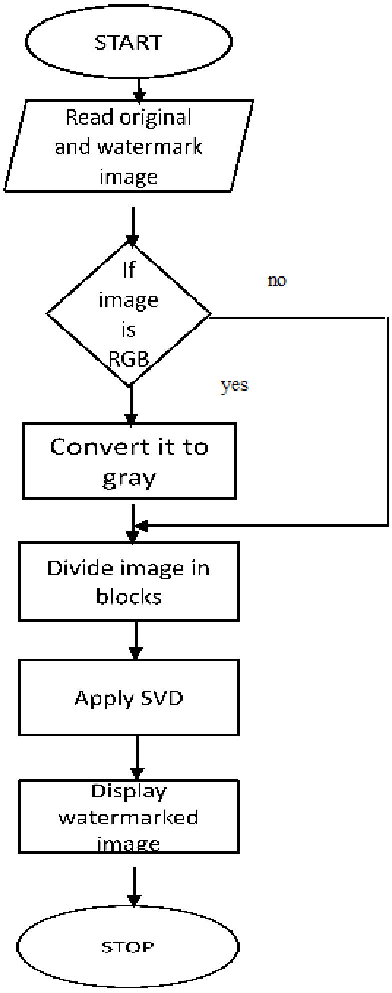


Fig 1: flowchart for embedding process

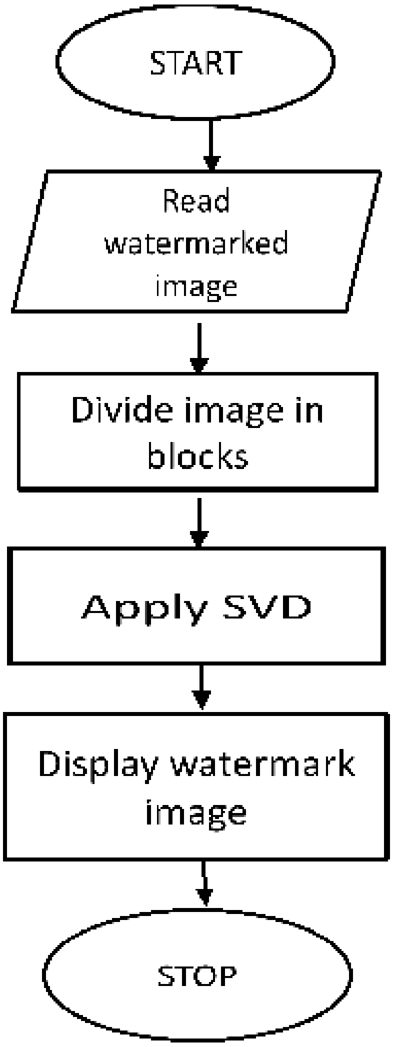


Fig 2: Flowchart for extraction process

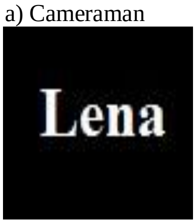
5. Implementation Results

The implementation is carried out on the MATLAB platform. By using the SVD with adaptive quantization technique and PSNR values have been calculated of different images at different quantization step. If the PSNR values of a watermarked image are highest then we can say that hidden message or image cannot be seen in the cover image and it fulfills security parameter.

The images that have been used for calculating the PSNR values using different techniques are:

IJASRM
International Journal of Advanced Scientific Research and Management, Vol. 2 Issue 8, August 2017.
www.ijasrm.com
ISSN 2455-6378

a) Cameraman b) Lena c) Baboon



(d)

Fig 3: (a)-(c) Original Images
(d) Watermark image

With the help of SVD technique watermark image is embedded in a cover image an after that PSNR values are calculated at different quantization step i.e. d_k = 9,27 using the images in fig 3.

IMAGE	PSNR		
	$d_k = 9$		$d_k = 27$
Lena	43.9947	34.1596	28.3588
Camera man	43.8491	34.0087	28.4308
Baboon	44.8076	35.0587	29.1219

Table 1: PSNR values using SVD

The adaptive quantization technique is used with the help of SVD and PSNR values are calculated with quantization step range i.e. 9 and 54 using the images in fig 3.

IMAGES	PSNR
Lena	38.8821
Cameraman	38.9887
Baboon	36.6784

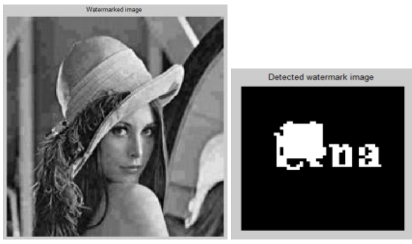
Table 2: PSNR values using Adaptive Quantization

Figure 4 shows the effects of different signal processing attacks.

- When Gaussian noise is applied

(a)

- When Cropping is applied



(b)

- When Rotation is applied

(c)

- When Med filter is applied

(d)

Fig 4: Recovered Watermarks After Application of different attacks

6. Conclusion

According to the work done in this paper result has been concluded that PSNR values of watermarked image using SVD with Adaptive Quantization technique is better than the SVD technique. By using this technique image quality has become better. As we compare that if we use SVD with Adaptive Quantization the PSNR value is more while using only SVD with Quantization Step 27 and 54. In future Block Truncation Coding [14] method will be used for the compression of the image and different attacks have been applied on watermarked image like cropping, blurring etc and then PSNR value is calculated of watermarked image.[7][8] From that we can conclude that which technique is better after applying different attacks on watermarked image and.

References

[1] Hartung, F., and Kutter, M. 1999. Multimedia Watermarking Techniques, Proceeding of IEEE, 87(7) 1079-1107, July 1999.

[2] Liu, F., & Liu, Y. (2008). "A watermarking algorithm for digital image based on DCT and SVD." In IEEE Congress on image and signal Processing (Vol. 1, pp. 380-383). Sanya, Hainan, China.

[3] Lai, C.-C. (2011). "A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm." Digital signal processing. Elsevier. 522-527.

[4] Ghazy, R., El- Fishawy, N., Hadhoud, M., Dessouky, M.m& El-Samie, F. (2007). "An efficient block by block SVD based image watermarking scheme." In proceedings of the 24th national radio science conference (pp. 1-9), Cairo, Egypt

[5] K. VijayaDurga, G.Mamatha, Ch.HimaBindu (2015) "SVD Based Image Watermarking With Firefly Algorithm". In International Conference on Computer Communication and Informatics, Coimbatore, INDIA

[6] VeyselAslantas (2009). "An optimal robust image watermarking based on SVD using differential evolution algorithm". In Optics communications Elsevier 769-777.

[7] Jain, C., Arora, S., &Panigrahi, P.K., (2008). "A reliable SVD based watermarking scheme," adsabs.harvad.edu/abs/2008arXiv 0808.0309J.

[8] Chandra, D. (2002). "Digital image watermarking using singular value decomposition." In proceedings of the IEEE 45th Midwest symposium on circuits and systems (Vol.3, pp. 264-267). USA: Oklahoma State University.

[9] SurafelLulesegedTilahun and Hong ChoonOng.,(2012). "Modified Firefly Algorithm". In Hindawipublishing corporation, journal of applied mathematics volume 2012, article 467631.

[10] P. Surekha and Sumathi (2011). "Implementation of genetic algorithm for a dwt based image watermarking scheme". ICTACT journal on soft computing:special issue on fuzzy in industry and process automation, volume 02, issue 01.

[11] S. Lee, D. Jang, C.D. Yoo, AN SVD-based watermarking method for image content authentication with improved security, in: Proc. ICASSP05, 2005, pp. 525–528.

[12] Yuan, Q.; C. Li; and Y. Zhong. 2007. Adaptive DWT-SVD domain image watermarking using a human visual model, Proceedings of the 9th Advanced Communication Technology Conference 3: 1947-1951.

[13] B. Kim, J. G. Choi and D. Min, "Robust Digital Water-marking Method Against Geometric Attacks," *Real Time Imaging Processing*, Vol. 9, No. 2, 2003, pp. 139-149.

[14] J. Z. K. H. F. L. Shuhua Xiong, "A Multipurpose Image Watermarking Method Based on Adaptive Quantization," in IEEE First International Multi-Symposiums on Computer and Computational Sciences , 2006.