International Journal of Engineering Research and General Science Volume 2, Issue 3, April-May 2014
ISSN 2091-2730

A Novel Blind Hybrid SVD and DCT Based Watermarking Schemes

Samiksha Soni[1], Manisha Sharma[1]

[1]Bhilai Institue of Technology Durg, Chhattisgarh

Email- samiksha.soni786@gmail.com

ABSTRACT – — In recent years SVD has gained wide importance in the field of digital watermarking. In this paper the fundamental of SVD and quantization based watermarking algorithm is discussed and a modified hybrid algorithm is proposed. In this work cascade combination of DCT and SVD is applied to design a robust watermarking system. This work exploits the features of both DCT and SVD. We implemented the same algorithm in three variants where these variation lies in the embedding procedure of watermark bit '1'. Simulation result shows that minor change in embedding formula has significant impact on robustness of the system. To check the robustness of the proposed work it is subjected to variety of attacks and robustness is measured in terms of normalized correlation and bit error rate.

Keywords— DCT, SVD, watermarking, quantization, embedding, extraction, singular value, diagonal, orthogonal.

INTRODUCTION

In today's era, the internet has subverted the way we access information and share our ideas. The internet provides excellent means for sharing digital multimedia object. It is inexpensive, eliminates warehousing and delivery, and is almost instantaneous. But with the advent of information technology there is threat to duplication and authentication of multimedia data. Watermarking is a branch of information hiding which is used to embed proprietary information in digital multi media.The conceptual model [1] of the watermarking system is explained in Fig. 1 and Fig. 2. Which comprise of two basic modules, embedding module and extraction module. Original image acts as the carrier which is to be secured. The watermark embedding module embeds the secondary signal in to the original image. This secondary signal providing the sense of ownership or authenticity is called watermark. The optional key is used to enhance the security of the system. Extraction module estimates the hidden secondary signal from the received image with the help of key and original image if required. Channel noise or illegitimate access may degrade quality of watermarked image during transmission. But embedding system should be strong enough in such a manner that no manipulation can detach the watermark from its cover except the authentic user.

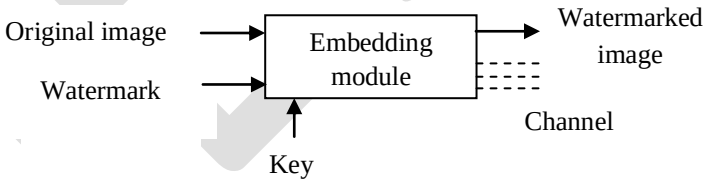


Fig. 1 Watermark Embedding Module

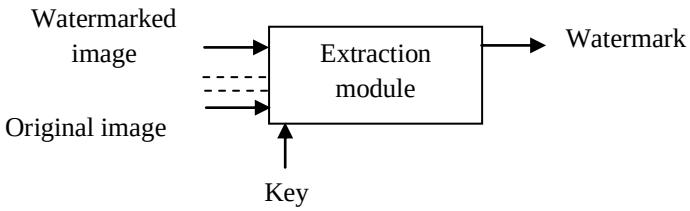


Fig. 2 Watermark Extraction Module

An effective watermarking scheme [2] should satisfy the following basic requirements

- Transparency: The watermark embedded in the original signal should not be perceivable by human eye and watermark should not distort the media being protected.
- Security: A watermarking scheme should also ensure that no one can generate bogus watermarks and should provide reliable evidence to protect the rightful ownership.
- Robustness: It refers to the property of survival of watermark against various attacks such as filtering, geometric transformations, noise addition, etc.

Image watermarking techniques proposed so far can be broadly categorized according to the basis of how to embed the watermark as: First category is spatial domain technique [3] which adds the digital watermark on the image directly in terms of a certain algorithm. Second category is transform domain technique which embeds the watermark into the transformed image [4-6]. The former technique has an easier algorithm and faster computing speed, but the disadvantage is that its robustness is not stronger; the latter one has better robustness and resilient to image compression, common filtering and noise, but its problem lies in computing speed. However, because of its better robustness, transform domain technique has gradually been applied to digital watermarking development and research.

In the recent years, singular value decomposition based watermarking technique and its variations have been proposed. SVD is a mathematical technique used to extract algebraic features from an image. The core idea behind SVD based approaches is to apply the SVD to the whole cover image or, alternatively, to small blocks of it, and then modify the singular values to embed the watermark. Gorodetski *et al.* in [7] proposed a simple SVD domain watermarking scheme by embedding the watermark to the singular values of the images, to achieve a better transparency and robustness. Proposed method is not image adaptive and fails to maintain transparency for different images. Liu *et al.* in [8] presented a scheme where a watermark is added to the singular value matrix of the watermarking image in spatial domain. This scheme offers good robustness against manipulations for protecting rightful ownership. But since the scheme is designed for the rightful ownership protection, where the robustness against manipulations is desired, it is suitable for authentication. Makhloghi *et al.* in [9] presents singular value decomposition and discrete wavelet transform based blind robust digital image watermarking. In the proposed work the wavelet coefficients of the host image are modified by inserting bits of singular values of watermark image.

In [10] a digital image watermarking scheme based on Singular Value Decomposition using Genetic Algorithm (GA) is proposed. The proposed scheme is based on quantization step size optimization using the Genetic Algorithm to improve the quality of watermarked image and robustness of the watermark. Zhu *et al.* [11] method can deal with the rectangle matrices directly and can extract better-quality watermarks. It takes little time to embed and extract the watermark in large images. This method can avoid some disadvantages such as the distortion caused by the computing error then extracting the watermark in the diagonal direction. Modaghegh *et al.* [12] proposed an adjustable watermarking method based on SVD, the parameters of which were adjusted using the GA in consideration of image complexity and attack resistance, and by the change of the fitness function, watermarking method can be converted to each of robust, fragile, or semi-fragile types. Abdulfetah *et al.* [13] proposed a robust quantization based digital image watermarking for copy right protection in DCT-SVD domain. The watermark is embedded by applying a quantization index modulation process on largest singular values of image blocks in the DCT domain. To avoid visual degradation of, they have designed adaptive quantization model based on blocks statistics of the image.

Horng *et al.* [14] proposed an efficient blind watermarking scheme for e-government document images through a combination of the discrete cosine transform (DCT) and the singular value decomposition (SVD) based on genetic algorithm (GA). DCT, in this case, is applied to the entire image and mapped by a zigzag manner to four areas from the lowest to the highest frequencies. SVD, meanwhile, is applied in each area and then the singular value of DCT-transformed host image, subsequently, is modified in each area with the quantizing value using GA to increase the visual quality and the robustness. The host image is not needed in the watermark extraction and it is more useful than non blind one in real-world applications.

SVD BASED WATERMARKING ALGORITHM

Sun *et al.* [15] proposed an SVD and quantization- based watermarking scheme. The diagonal matrix property is exploited to embed the watermark. To embed the watermark largest coefficient of diagonal matrix is selected. The modification was determined by the

quantization means. After that, the inverse of the SVD transformation was performed to reconstruct the watermarked image. Because the largest coefficients of diagonal matrix can resist general image processing, the embedded watermark was not greatly affected. Also, the quality of the watermarked image can be determined by the quantization. Thus, the quality of the watermarked image can be maintained. To extract the watermark, the SVD transformation was employed and the largest coefficients in the S component were examined. After that, the watermark was extracted.

The watermark embedding and extracting procedures can be described as follows.

- watermark embedding procedure

In first step partition the host image into blocks. In second step perform SVD transformation. In third step extract the largest coefficient $S_i(1,1)$ from each S component and quantize it by using a predefined quantization coefficient Q.

Let $Y_i = S_i(1,1) \bmod Q$

In fourth Step embed watermark bit as follows

When $W_i = 0$ it will be embedded as follows:

if $Y_i < 3Q/4$,then $S'_i(1,1) = S_i(1,1) + Q/4 - Y_i$ else $S'_i(1,1) = S_i(1,1) + 5Q/4 - Y_i$

When $W_i = 1$ it will be embedded as follows:

if $Y_i < 3Q/4$,then $S'_i(1,1) = S_i(1,1) - Q/4 + Y_i$ else $S'_i(1,1) = S_i(1,1) + 3Q/4 - Y_i$

In step five perform the inverse of the SVD transformation with modified S matrix and U, V matrix of original image to reconstruct the watermarked image.

- Watermark extraction procedure

In first step partition the watermarked image into blocks. In second step perform SVD transformation. In third step extract the largest coefficient S'(1, 1) from each S component and quantize it by using the predefined quantization coefficient Q. Let Z = S'(1, 1)modQ.

In fourth step check if Z < Q/2, the extracted watermark has a bit value of 0. Otherwise, the extracted watermark has a bit value of 1.

In the proposed work we implemented three variants of quantization based blind embedding [] which differs minutely from one another. Difference lies in the embedding step for watermark bit to be '1'. This minor difference creates significant change in robustness.

PROPOSED SCHEME

In the proposed work we provide modification in the existing method by cascading it with DCT. DCT operation is performed on original image to obtain its frequency components. Then reordering of DCT components is done in zigzag manner. After that block SVD operation is performed on scanned DCT coefficients then watermark is embedded inside the largest SV's of each block.

- Watermark embedding procedure:

In first step convert the original color image in to gray scale. Then apply 2-D DCT to the gray scale image and perform the zigzag scanning operation on DCT coefficients shown in Eq. (1) and Eq. (2). Let the gray scale image be A

$$A_d = \mathrm{DCT2}(A) \quad (1)$$

$$Z_d = \mathrm{Zigzag}(A_d) \quad (2)$$

In next step two dimensional matrix is formed from the zigzag scanned vector

$$M = \mathrm{Con2\_matrix}(Z_d) \quad (3)$$

After that Matrix M is fractioned in to smaller blocks depending on the payload size $(m_1, m_2, \ldots\ldots, m_n) =$ divi(M) where n is equal to watermark length, then using Eq. (4) SVD operation is performed on this blocks

$$[U_i S_i V_i] = \text{svd}(m_i) \qquad (4)$$

Where i=1,2,3,4…….,n

After applying DCT SVD operation on original image the binary watermark is inserted by the following ways:

Modify the largest singular value of each block as

$$Y_i = S_i(1,1) \bmod Q$$

Where Q is predefined quantizing value, Q must be selected with the specification of an image both to obtain a maximum resistance towards attack and to obtain the minimum perceptibility.

- First Embedding Procedure:

When $W_i = 0$ it will be embedded as follows:

if $Y_i < 3Q/4$,then $S'_i(1,1) = S_i(1,1) + Q/4 - Y_i$ else $S'_i(1,1) = S_i(1,1) + 5Q/4 - Y_i$

When $W_i = 1$ it will be embedded as follows:

if $Y_i < Q/4$,then $S'_i(1,1) = S_i(1,1) - Q/4 - Y_i$ else $S'_i(1,1) = S_i(1,1) + 3Q/4 - Y_i$

- Second Embedding Procedure:

When $W_i = 0$ it will be embedded as follows:

if $Y_i < 3Q/4$,then $S'_i(1,1) = S_i(1,1) + Q/4 - Y_i$ else $S'_i(1,1) = S_i(1,1) + 5Q/4 - Y_i$

When $W_i = 1$ it will be embedded as follows:

if $Y_i < 3Q/4$,then $S'_i(1,1) = S_i(1,1) - Q/4 + Y_i$ else $S'_i(1,1) = S_i(1,1) + 3Q/4 - Y_i$

- Third Embedding Procedure:

When $W_i = 0$ it will be embedded as follows:

if $Y_i < 3Q/4$,then $S'_i(1,1) = S_i(1,1) + Q/4 - Y_i$ else $S'_i(1,1) = S_i(1,1) + 5Q/4 - Y_i$

When $W_i = 1$ it will be embedded as follows:

if $Y_i < 3Q/4$,then $S'_i(1,1) = S_i(1,1) - Q/4 + Y_i$ else $S'_i(1,1) = S_i(1,1) + 3Q/4 + Y_i$

Next step is to perform inverse SVD operation on blocks to obtain modified DCT coefficients $m'_i = \text{ISVD}(U_i S'_i V_i)$ and smaller blocks are recombined by $M' = \text{merg}(m'_1, m'_2, \ldots, m'_n)$, then after inverse zigzag operation is performed on M' to map DCT coefficients back to their position $A'_d = \text{IZigzag}(M')$. Last step is to perform inverse DCT operation on A'_d using Eq. (5) to obtain watermarked imageA'.

- Watermark extraction procedure

The first step of the watermark-extraction process is to apply DCT to the watermarked image as shown in Eq. (5)

$$A'_{dr} = DCT2(A') \quad (5)$$

In Step two, using Eq. (6) scan the DCT coefficients in the zigzag manner

$$Z_{dr} = Zigzag(A'_{dr}) \quad (6)$$

After that two dimensional matrix is formed from scanned vector using Eq. (7)

$$M_r = Con2\_matrix(Z_{dr}) \quad (7)$$

In step three matrix M_r is fractioned in to smaller blocks depending on the payload size $(m_{r1,}m_{r2,\ldots\ldots,}m_{rn}) = divi(M_r)$ where n is equal to watermark length, then SVD operation is performed on this blocks as shown in Eq. (8)

$$[U_{ri}\,S_{ri}\,V_{ri}] = svd(m_{ri}) \quad (8)$$

Where i=1, 2, 3, 4……., n. In step four get the largest singular values from each block and extract the watermark

$$Y_{ri} = S_{ri}(1,1) \bmod Q$$

- Extraction mechanism for first and second embedding procedure:

If $Y_{ri} < Q/2$, then $W_{ri} = 0$, else $W_{ri} = 1$, these extracted bit values are used to construct the extracted watermark.

- Extraction mechanism for third procedure:

If $Y_{ri} \leq Q/2$, then $W_{ri} = 0$, else $W_{ri} = 1$, these extracted bit values are used to construct the extracted watermark.

EXPERIMENTAL RESULTS

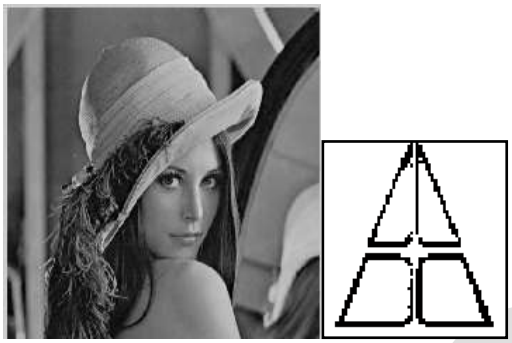
To verify the performance of the proposed watermarking algorithm, MATLAB platform is used and a number of experiments are performed on different images of size 512×512 and binary logos of size 64×64.Here we provide the comparative result for host image Lena and binary logo shown in Fig. 3 (a) and Fig. 3 (b).Extracted watermark of three procedure is shown in Fig. 4 (a)(first procedure) , Fig. 4 (b)(second procedure), Fig. 4 (c)(third procedure) The watermarked image quality is measured using PSNR (Peak Signal to Noise Ratio) given by Eq. (9).To verify the presence of watermark, two parametric measures are used to show the similarity between the original watermark and the extracted watermark. These two parameters are normalized correlation and bit error rate given by Eq. (9) and (10)

$$PSNR = 10Log_{10}\left[\frac{\sum_{i=1}^{N}\sum_{j=1}^{N}(A'(i,j))^2}{\sum_{i=1}^{N}\sum_{j=1}^{N}(A(i,j)-A'(i,j))^2}\right] \quad (9)$$

$$NC = \left[\frac{\sum_{i=1}^{N}\sum_{j=1}^{N}(w(i,j)-w_{mean})(w'(i,j)-w'_{mean})}{\sqrt{\sum_{i=1}^{N}\sum_{j=1}^{N}(w'(i,j)-w'_{mean})^2\sum_{i=1}^{N}\sum_{j=1}^{N}(w(i,j)-w_{mean})^2}}\right] \quad (10)$$

$$BER = \frac{\sum_{i=1}^{N}\sum_{j=1}^{N}w(i,j)\oplus w'(i,j)}{N\times N} \quad (11)$$

Where w(i, j) be the original watermark image and the extracted watermark be w'(i, j) original watermark image and the extracted watermark be w'(i, j).



(a) (b)

Fig.3 Host image and watermark image

(a) (b) (c)

Fig.4 Extracted watermark

In order to check the robustness of the proposed watermarking scheme the watermarked image is attacked by a variety of attacks namely Average and Median Filtering, Gaussian noise, Random noise, JPEG Compression, Cropping, Resize, Rotation, Blur. After these attacks on the watermarked image, the extracted logo is compared with the original one.

- Filtering

The most common manipulation in digital image is filtering. In filtering watermarked image is attacked by applying Mean(3×3), Median (3×3) and Gaussian low pass (5x5) filter.

- Addition of noise

Noise addition in watermarked image is another way of checking the robustness of the system. Noise addition leads to degradation and distortion of the image. Which effects the quality of extracted watermark. Here robustness is checked against salt and pepper noise and random noise.

- JPEG compression

Another most common manipulation in digital image is image compression. To check the robustness against Image Compression, the watermarked image is tested with JPEG100 and JPEG2000 compression attacks.

- Cropping and resizing

Cropping is the process of selecting and removing a portion of an image to create focus or strengthen its composition. Cropping an image is done by either hiding or deleting rows or columns. In the proposed work three variants of cropping is performed they are row column blanking, row column copying, cropping 25% area (right bottom corner). To fit the image into the desired size, enlargement or reduction is commonly performed and resulted in information loss of the image including embedded watermark. For this attack, first the size of the watermarked image is reduced to 256×256 and again brought to its original size 512×512.

- Rotation

In this work watermark is subjected to very minor rotation i.e. of 0.2, 0.3 and result are obtained. When rotation of larger degree is provided watermark fails to resist the attack. However if the effect of rotation is reverted by some way watermark can be successfully extracted.

- General image processing attacks

We employed motion blur with pixel length 3 and angle 45^0 on watermarked image to check its robustness

TABLE I
NORMALIZED CORRELATION VALUE OF THREE IMPLEMENTED SCHEMES

Types of attacks	First Embedding	Second Embedding	Third Embedding
Without attack	0.9927	0.8956	0.5352
Random noise	0.5930	0.4070	0.3028
Low Pass Filtering	0.5218	0.3854	0.2160
Rotation	0.6316	0.4624	0.2951
Blurred	0.6831	0.5229	0.3064
Average Filtering	0.6004	0.4499	0.2630
Median Filtering	0.7333	0.5805	0.3437
Crop	0.7396	0.5904	0.1906
JPEG 100	0.9546	0.7606	0.4903
JPEG2000	0.9912	0.9004	0.5340
Salt & Pepper	0.7439	0.5786	0.3917
Row Column	0.7550	0.6306	0.4232
Row Column Copying	0.7984	0.7535	0.4320
Resizing	0.8328	0.5130	0.4185

TABLE III
PSNR VALUE OF THREE IMPLEMENTED SCHEMES

Types of attacks	First Embedding	Second Embedding	Third Embedding
Without attack	47.5090	47.5671	38.8217
Random noise	33.9449	33.9422	32.8873
Low Pass Filtering	33.6067	32.5978	32.1208
Rotation	37.4609	37.4382	35.5961
Blurred	35.4630	35.4561	34.3489
Average Filtering	32.7986	32.7889	32.2431
Median Filtering	35.9154	35.9007	34.6384
Crop	11.4074	11.8670	11.3010
JPEG 100	44.0591	44.3251	38.2187
JPEG2000	46.3709	47.2910	38.5917
Salt & Pepper	32.0481	32.1717	31.4888
Row Column	24.1098	26.2981	23.9875
Row Column Copying	28.9098	33.3551	27.0656
Resizing	34.5344	37.9656	33.5479

TABLE IIIII
BER VALUE OF THREE IMPLEMENTED SCHEMES

Types of attacks	First Embedding	Second Embedding	Third Embedding
Without attack	0.0037	0.0510	0.4304
Random noise	0.1848	0.2253	0.4614
Low Pass Filtering	0.2261	0.2607	0.5028
Rotation	0.1768	0.2146	0.4695
Blurred	0.1528	0.1868	0.4983
Average Filtering	0.1951	0.2275	0.5029
Median Filtering	0.1328	0.1599	0.4870
Crop	0.2554	0.1406	0.5012
JPEG 100	0.0225	0.0896	0.4579
JPEG2000	0.0044	0.0496	0.4255
Salt & Pepper	0.1240	0.1587	0.4475
Row Column Blanking	0.1277	0.1365	0.4412
Row Column Copying	0.1030	0.0923	0.4380
Resizing	0.0840	0.2795	0.4882

Conclusion

In this paper three variants of quantization based blind watermarking scheme is discussed. Experimental result shows that performance of first embedding procedure is better is terms of NC, PSNR and BER. Proposed technique shows resilience towards a variety of attacks but it fails to withstand histogram equalization, contrast enhancement attacks and rotational attacks of higher degree. Since embedding procedure for inserting watermark bit '0' is common in all the procedure and variation exists in insertion of watermark bit '1' only. This variation plays significant impact on watermark retrieval which is clearly identified by the NC, BER and PSNR of three embedding procedure shown in Table I, II and III.

REFERENCES:

[1] C.I.Podilchuk and E.J.Delp, "Digital Watermarking: Algorithms and Applications," *IEEE Signal Process.Magazine*, pp.33-46, July 2001.
[2] Fernando PCrez-Gonz6lez and Juan R. Hernbdez, " A TUTORIAL ON DIGITAL WATERMARKING, " IEEE Trans. on Information Forensics Security, 1999;
[3] Dipti Prasad Mukherjee, Subhamoy Maitra , Scott T. Acton ,"Spatial Domain Digital Watermarking of Multimedia Objects for Buyer Authentication", IEEE Transactions on multimedia, VOL. 6, NO. 1, FEBRUARY 2004.
[4] J. R. Hernansez, M. Amado, and F. Perez-Gonzalez, "DCT-domain watermarking techniques for still images: Detector performance analysis and a new structure," IEEE Trans. Image Process., vol. 9, pp. 55–68, Jan. 2000.
[5] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," IEEE Trans. Image Processing, vol. 6, pp. 1673–1687, Dec. 1997.
[6] P. Meerwald, "Digital Watermatrking in the Wavelet Transform Domain," Master's, Dept. Sci. Comput., Univ. Salzburg, Austria, 2001.
[7] V. I. Gorodetski, L. J. Popyack, and V. Samoilov, "SVD-based approach to transparent embedding data into digital images," in Proc. International Workshop, MMM-ACNS, St. Petersburg, Russia, pp. 263–274, May 2001.
[8] R. Liu and T. Tan, "A SVD-Based Watermarking Scheme for Protecting Rightful Ownership", IEEE Trans. on Multimedia, Vol. 4, pp.121-128, March 2002.
[9] M. Makhloghi, F. Akhlaghian, H. Danyali, Robust digital image watermarking using singular value decomposition, in: IEEE International Symposium on Signal Process. and Information Technology, pp. 219–224, 2010.
[10] B.Jagadeesh, S.Srinivas Kumar, K.Raja Rajeswari, "Image Watermarking Scheme Using Singular Value Decomposition, Quantization and Genetic Algorithm", International Conf. on Signal Acquisition and Process., IEEE Computer Society, pp.120-124, 2010.
[11] Xinzhong Zhu, Jianmin Zhao and Huiying Xu ," A Digital Watermarking Algorithm and Implementation Based on Improved SVD"The 18th International Conf. on Pattern Recognition ,2006

[12] H. Modaghegh, R.H. Khosravi, T. Akbarzadeh, " A new adjustable blind watermarking based on GA and SVD", Proceeding of International Conf. on Innovations in Information Technology in, pp. 6–10, 2009.
[13] A. Abdulfetah, X. Sun and H. Yang, "Quantization Based Robust Image Watermarking in DCT-SVD Domain". Research Journal of Information Technology, Vol 1, pp. 107-114, 2009.
[14] Shi-Jinn Horng , Didi Rosiyadi, Tianrui Li a, Terano Takao , Minyi Guo , Muhammad Khurram Khan," A blind image copyright protection scheme for e-government", Pattern Recognition Letters, pp.1099–1105 ,2013.
[15] Sun, R., Sun, H., Yao, T., "A SVD and quantization based semi-fragile watermarking technique for image authentication", Proc. IEEE International Conf. Signal Process., pp. 1592-95, 2002.