IJCSC 0973-7391 Volume 7 • Number 1 Sept 2015 - March 2016 pp.89-94 available online at www.csjournalss.com

A Singular Value Decomposition Based Robust Image Watermarking Scheme

Deepti Varshney
Assistant Professor, Department of Comp Engg, SRCOE, Pune

Abstract: The growth of new imaging technologies has created a need for techniques that can be used for copyright protection of digital images. Copyright protection involves the authentication of image content and/or ownership and can be used to identify illegal copies of an (possibly forged) image. One approach for copyright protection is to introduce an invisible signal known as a digital watermark in the image. Several techniques have been introduced. Finally the experimental analysis is performed and results are compared with the other work which shows the watermarking in Singular Value Decomposition domain is better. We developed a new watermarking scheme in which double watermarking techniques in SVD domain to increase the robustness of the images.
Keywords: Singular Value Decomposition, PSNR, Digital Watermark, Correlation, Intellectual property rights.

I. INTRODUCTION

The idea of communicating secretly is as old as communication itself. The earliest allusion to secret writing in the West appears in Homer's Iliad. Steganographic methods made their record debut a few centuries later in several tales by Herodotus, the father of history. The origin of steganography is biological and physiological. The term "steganography" came into use in 1500's after the appearance of Trithemius' book on the subject "Steganographia"

The recent growth of networked multimedia systems has increased the need for the protection of digital media. This is particularly important for the protection and enforcement of intellectual property rights.

One way to improve one's claim of ownership [1] over an image, for instance, is to place a low-level signal directly into the image data. This signal, known as a *digital watermark*, uniquely identifies the owner and can be easily extracted from the image. Digital watermarking technology is an emerging field in computer science, cryptography, signal processing and communications.

In this work we present algorithms for image authentication and forgery prevention known as watermarks. And also present the mathematical model to implement digital watermarking.

II. CURRENT STATE OF ART

A. Embedding process

Let us denote an image by *I*, a watermark by $S = s_1, s_2, \ldots$ and the watermarked image by $\hat{I}$. *E is* an encoder function, it takes an image *I* and a watermark *S*, and it generates new image which is called watermarked image $\hat{I}$, mathematically

$$E(I, S) = \hat{I} \quad (1)$$

It should be noted that the watermark S may be dependent on image *I*. In such cases, the encoding process described by Eqn.(1) still holds. Following figure illustrates the encoding process.

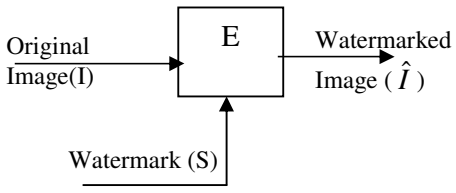


Fig 1: Encoder

B. Extraction process

A decoder function *D* takes an image *J* (*J* can be a watermarked or un-watermarked image, and possibly corrupted) whose ownership is to be determined and recovers a watermark *S´* from the image. In this process an additional image *I* can also be included which is often the original and un-watermarked version of *J*. This is due to the fact that some encoding schemes may make use of the original images in the watermarking process to provide extra robustness against intentional and unintentional corruption of pixels. Mathematically,

$$D(J,I) = S' \quad (2)$$

The extracted watermark S' will then be compared with the original watermark by a comparator function C_δ and a binary output decision generated. It is 1 if there is match and 0 otherwise, which can be represented as follows.

$$C_\delta(S', S) = \begin{cases} 1, c \le \delta \\ 0, \text{otherwise} \end{cases} \quad (3)$$

Where C is the correlator, $x = C_\delta(S', S)$. c is the correlation of two signatures and δ is certain threshold. Without loss of generality, watermarking scheme can be treated as a three-tupple (E, D, C_δ). Following figures 2 and 3 demonstrate the decoder and the comparator.

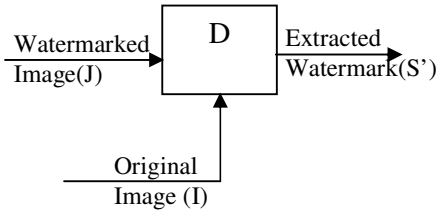


Fig 2: Decoder

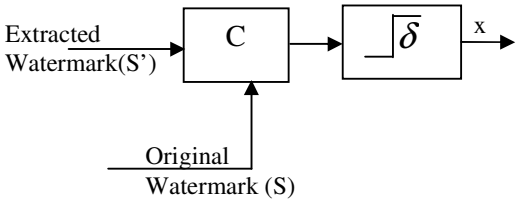


Fig 3: Comparator

III. EXISTING SYSTEM

Liu and Tan [13] proposed an SVD-based watermarking scheme for rightful ownership protection. Without loss of generality, I and W are assumed to be $N \times N$ square matrices. Their algorithm consists of the following three steps:

- Perform SVD on the original un-watermarked image $I = USV^T$ (4)
- Add the watermark image W to S and obtain the reference watermark S_n as $S_n = S + \beta W$ (5)
- Then perform SVD on the reference watermark S_n as

$$S_n = S + \beta W = U_W S_W V_W^T \quad (6)$$

- Obtain the watermarked image I_w as $I_W = US_W V^T$ (7)

Here, β is a scale factor that controls the strength (energy) of the embedded watermark.

To extract the watermark from a possibly distorted watermarked image I_W^*, their algorithm proceeds as follows

- Perform SVD on the possibly distorted watermarked image I_W^* as $I_W^* = U^* S_W^* V^{*T}$ (8)
- Use U_W, V_W; $S^* = U_W S_W^* V_W^T$ (9)

- Get the possibly distorted watermark W^* as $$W^* = \frac{1}{\beta}(S^* - S) \quad (10)$$

This algorithm requires U_W , *S*, and V_W to be available for detection.

Zhang and Li [1] have shown that this algorithm is fundamentally flawed. This is because it only embeds the diagonal matrix S_W . The detection algorithm simply extracts a possibly distorted diagonal matrix S^*_W . After that, the detection algorithm utilizes (does not extract) the singular vectors of the reference watermark (U_W and V_W) Zhang and Li [1] have shown that, by using the reference watermark SVD pair (U_W, V_W) in the detection stage, false-positive detection will have a probability of one. In other words, using the singular vectors of any fake watermark in the detection stage, one can always claim that this watermark was the embedded one. Hence, he can claim ownership of the watermarked image. We propose a variation on this teechnique. As opposed to their algorithm, the proposed algorithm overcomes the problem of false-positive detection. Also if first watermark is degraded or destroyed due to some reason we can detect second one. In addition, the proposed algorithm is robust and noninvertible.

IV. PROPOSED METHODOLOGY AND IMPLEMENTATION OF WORK

The following three steps summarize the embedding algorithm:

- Perform SVD on the original image *I*: $$A = \bigcup \Sigma V^T \quad (11)$$
- Add the watermark image *W* to $\sum$, with a scale factor α as $$\Sigma_n = \Sigma + \alpha W \quad (12)$$
- Obtain the watermarked image I_w : $$A_W = \bigcup \Sigma_n V^T \quad (13)$$

The main difference between this technique and that of Liu and Tan is that their algorithm only embeds the singular values of $\sum_n$ while our algorithm embeds $\sum_n$. As was shown in [1], this is why Liu and Tan's algorithm turned out to be flawed. Notice also that while Liu and Tan's algorithm performs two SVD decompositions for *A* and $\sum_n$, our algorithm performs one SVD for *A* only. This means that our algorithm saves up to $15(N)^3$ computations (Flops).

We use double watermarking by embedding the text into the watermark image using following process:

1. Read the Watermarked image
2. Read the message which is to be embed
3. And the watermarked image with message.
4. Resultant image is called double watermarked image

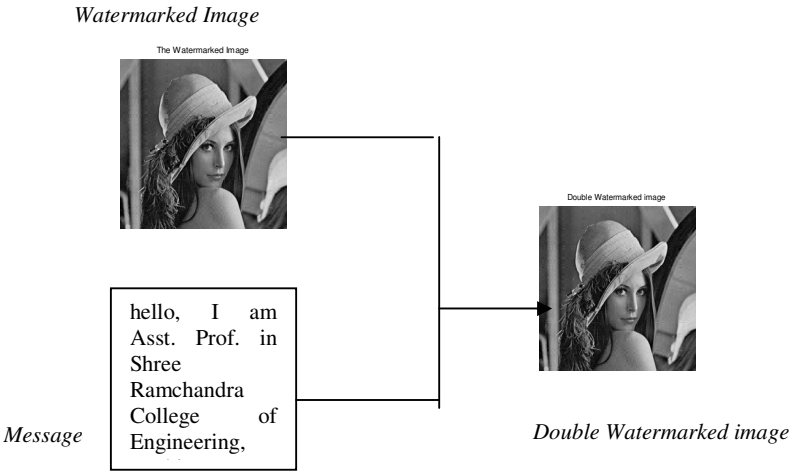


Fig 4: producing double watermarked image Process

Fig 4 illustrates the process of embedding the message in the watermarked image.

Given the SVD components of the original un-watermarked image $A = \bigcup \Sigma V^T$ and a possibly corrupted double watermarked image A_w^{**}, the extraction sequence proceeds as follows:

- Extract the text and get the watermarked image A_w^*
- Obtain the corrupted matrix $\sum_n^*$ as

$$\sum_n^* = \bigcup^T A_w^* V \tag{14}$$

- Reverse step 2 of the embedding procedure to get a possibly distorted watermark W^* as follows:

$$W^* = \frac{1}{\alpha}\left(\sum_n^* - \Sigma\right) \tag{15}$$

$$A_W = \bigcup \sum_n V^T \tag{16}$$

Note that, only the original cover image or its SVD components U, $\sum$, and V need to be available for extraction. This is another difference with Liu and Tan's algorithm. Their algorithm uses both the cover image and the singular vector's matrices of $\sum_n$ for extraction.

V. EXPERIMENTAL RESULTS AND ANALYSIS

In this section, some experimental results have been shown to demonstrate the effectiveness and success of the digital watermarking technique for the embedding and extraction of watermark image with the original (digital) image in SVD domain. Also, we investigate the robustness of the proposed SVD algorithm against different attacks.

MCK

hello, I am Asst. Prof. in Shree Ramchandra College of Engineering, working as head of the department

Fig 5: Input images for watermarking: (a) original image of Lena, (b) original watermark image (c) Sample Text

(a) (b) (c) (d)

Fig 6: Output of algorithm with scaling factor α =0.02: (a) watermarked image, (b) Double Watermarked image (c) Image after text extraction (d) extracted watermark image.

(a) (b) (c) (d)

Fig 7: Output of algorithm with threshold α=0.1: (a) watermarked image, (b) Double watermarked image (c) Image after text extraction (d) extracted watermark image.

In order to measure the similarity between the original watermark W and the extracted watermark W^*, we calculate the correlation between W and W^*. For simplicity, W and W^* are converted to one-dimensional row vectors X and X^*. Eqn (22) defines the correlation coefficient $C(W, W^*)$ as

$$C(W,W^*) = \frac{XX^T}{\sqrt{XX^T}} \tag{22}$$

Another method for measuring similarity between W and W^* is using the peak signal-to-noise ratio (PSNR) given by

$$PSNR(W,W^*) = 10\log_{10} L\frac{Maximum(X(t)^2)}{\sum_{t=1}^{L}(X(t)-X^*(t))^2} \tag{23}$$

where L is the length of the vectors X and X^*. Actually, one can use any similarity measure.

As opposed to Liu and Tan's algorithm, this algorithm does not suffer the false-positive detection problem. Table-1 and Table-2 show the performances of our algorithm. On different threshold values for each type of attack, Table-1 and Table-2 give the PSNR, the correlation coefficient, and the extracted watermark for the proposed SVD-based method. As can be seen from the extracted watermark, our algorithm proved to be much more robust than other methods.

Table 1: Quality rates under various executions at scaling factor α =0.02

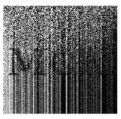
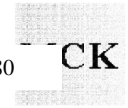
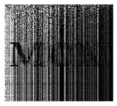
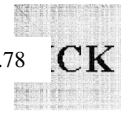
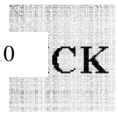
Attack type	PSNR	Correlation coefficient	Extracted watermark
No attack	34.32	97.71	
Low pass filter (only watermarked image is filtered)	25.60	11.24	
Gaussian noise	33.36	48.49	
Salt and Paper	33.76	66.80	
Rotation by 30^0	8.87	0.34	
Rotation by 360^0	34.32	97.71	

Table 2: Quality rates under various executions at scaling factor α =0.1

Attack type	PSNR	Correlation coefficient	Extracted watermark
No attack	20.89	85.10	
Low pass filter (only watermarked Image is filtered)	23.30	15.99	
Gaussian noise	20.86	81.48	
Salt and Paper	20.87	83.78	
Rotation by 30^0	8.75	0.69	
Rotation by 360^0	20.89	85.10	

Due to its computationally efficient modeling of the HVS, the proposed SVD method offers perhaps the most promising environment for robust watermarking. The algorithm does not offer any problem for retrieving the small watermark from the watermarked image along with only minimal degradation of the cover image during embedding.

The algorithm described here is one of the simplest ones available in the SVD domain, and yet the results are excellent. These results tend to reinforce the common belief in SVD domain as the most promising domain for digital watermarking.

VI. CONCLUSION

.

Double watermark are embedded by SVD method. First of all we have embedded an watermark image by SVD method in the cover image and then its robustness is improved by embedding another watermark *i.e.* text watermark into the embedded watermarked image so that if one watermark gets lost due to some reason another one can be extracted to prove the rightful ownership.

Only the original cover image or its SVD components U, $\sum$, and V need to be available for extraction whereas other algorithms uses both the cover image and the singular vector's matrices of $\sum_n$ for extraction.

This method can be extended in future to choose the scaling factor that is used to control the strength of the embedded watermark.

REFERENCES

[1] X. Zhang, K. Li, Comments on an SVD-based watermarking scheme for protecting rightful ownership, IEEE Trans. Multimedia 7 (3) (April 2005), pp. 593–594.

[2] R. B. Wolfgang and E. J. Delp, "Overview of image security techniques with applications in multimedia systems," Proceedings of the SPIE International Conference on Multimedia Networks: Security, Displays, Terminals, and Gateways, November 4-5, 1997, Dallas, Texas, vol. 3228, pp. 297-308.

[3] M. D. Swanson, M. Kobayashi, and A. H. Tewfik, "Multimedia data embedding and watermarking technologies," to appear in Proceedings of the IEEE, 1998.

[4] I. J. Cox and M. L. Miller, "A review of watermarking and the importance of perceptual modeling," Proceedings of the SPIE International Conference on Human Vision and Electronic Imaging II, Feb. 10-13, 1997, San Jose, CA, USA, pp. 92-99.

[5] M. Kutter and F. Hartung, "Image watermarking techniques," to appear in Proceedings of the IEEE, Special Issue on Identification and Protection of Multimedia Information, 1999.

[6] I. J. Cox, "Spread-spectrum techniques for image watermarking," to appear in Proceedings of the IEEE, Special Issue on Identification and Protection of Multimedia Information, 1999.

[7] M. Kutter, F. Hartung, "Introduction to Watermarking Techniques" in Information Techniques for Steganography and Digital Watermarking, S.C. Katzenbeisser et al., Eds. Northwood, MA: Artec House, Dec. 1999, pp 97-119.

[8] H. Inoue, A. Miyazaki, T. Katsura "An Image Watermarking Method Based on the Wavelet Transform", Kyushu Multimedia System Research Laboratory.

[9] I.J. Cox, M.L. Miller, J.M.G. Linnartz, T. Kalker, "A Review of Watermarking Principles and practices" in Digital Signal Processing for Multimedia Systems, K.K. Parhi, T. Nishitani, eds., New York, New York, Marcel Dekker, Inc., 1999, pp 461-482.

[10] F.A.P. Petitcolas, "Watermarking Schemes Evaluation" ", in IEEE Signal Processing Magazine, Vol 17, pp 58-64, September 2000.

[11] S.P. Mohanty, et al.,"A Dual Watermarking Technique for Images", Proc. 7th ACM International Multimedia Conference, ACM-MM'99, Part 2, pp 49-51, Orlando, USA, Oct. 1999.

[12] I. J. Cox, "Spread-spectrum techniques for image watermarking," to appear in Proceedings of the IEEE, Special Issue on Identification and Protection of Multimedia Information, 1999.

[13] R. Liu, T. Tan, A SVD-based watermarking scheme for protecting rightful ownership, IEEE Trans. Multimedia 4 (1) (March 2002), pp. 121–128.

[14] Xiangyang Luo, Zongyun Hu, Can Yang, Shanqing Gao "A Secure LSB Steganography System Defeating Sample Pair Analysis Based on Chaos System and Dynamic Compensation" IEEE Feb. 20-22, 2006, pages-1014-1019

[15] Ahmad A. Mohammad, Ali Alhaj, Sameer Shaltaf , An improved SVD-based watermarking scheme for protecting rightful ownership, ELSEVIER (March 2008) P. 2158-2180.