Semi-Blind Gray Scale Image Watermarking Algorithm based on hybrid SVD-DWT using HVS Model

D.Y. Thorat, Shiv K Sahu, Amit Mishra

Abstract: ***To achieve good imperceptibility and robustness, a hybrid image watermarking algorithm based on discrete wavelet transform (DWT) and singular value decomposition (SVD) is proposed using the characteristics of human visual system model for copyright protection and authenticity. In the proposed watermarking algorithm, one level DWT is applied to selected image blocks to obtain four sub-bands of each block and then the S component of low frequency sub-band (LL) obtained after SVD transformation is explored under different threshold values for embedding and extracting the watermark. The experimental results show that HVS model based hybrid image watermarking scheme is imperceptible and robust against several image processing operations like JPEG compression, median filtering, sharpening, cropping and addition of Gaussian noise. Peak signal to noise ratio (PSNR) and bit correction rate (BCR) are used to measure the quality of watermarked image and extracted watermark respectively.***

Keywords: Singular value decomposition, Discrete wavelet transform, Image watermarking, Copyright, Human Visual Model

I. INTRODUCTION

As the electronic media is get popular for communication, the secure communication is the important task in electronic media. Now a days there are large techniques available with different technologies. Among them authentication is the important task for secure communication. On the basis of authentication we can able to find out the authorized user, image or data.

There are number of existing technique which provides the authentication on which we can find the authorized data. The most important technique used for digital data authentication is encryption i.e. public key encryption which is also called traditional method of authentication. Another technique available is watermarking. Digital watermarking is a technique which hide some logo or data in the given image so that we prevent copyright, integrity and/or the authenticity of the original data [1-2]. Usually, a robust watermarking is used to protect the copyright while a fragile or semi-fragile watermarking is used to verify the authenticity[3-4]. Authentication of image data is a challenging task. Content modification or tampering is defined as an object appearance or disappearance, a modification to an object position, or changes to texture, color or edges. Image watermarking algorithm used to detect tampering has several essential properties. First is transparency.

Revised Version Manuscript Received on May 20, 2016.

D.Y.Thorat, M.Tech. Scholar, Department of Information Technology, Technocrats Institute of Technology, Bhopal (M.P). India.

Dr. Shiv K Sahu, Assoc. Prof. & Head, Department of Information Technology, Technocrats Institute of Technology, Bhopal (M.P). India.

Amit Mishra, Asst. Prof. Department of Information Technology, Technocrats Institute of Technology, Bhopal (M.P). India.

The embedding processing should not degrade the quality of the original digital media and should be perceptually invisible to maintain its protective secrecy and sensitivity.

The embedded watermark is robust to resist normal image processing (such as JPEG compression) while it is fragile to malicious tampering to image content. The watermark is embedded in a secure way and it can't be removed illegally [5-10].

We propose the new technique of authentication in which we can use the watermark which is generated from the same cover image. Watermark is generated with the help of SVD-DWT method for the contour image and apply the Arnold transform for the given image. The watermark which is generated is stored into LH or HL band so we get the standard result.

This paper is organized as follows: Section 1 introduces related works. Section 2 details the system diagram & workflow steps. Section 3 details the detailed steps. Experiments are presented in section 4. Finally, conclusions are drawn in section 5.

II. SYSTEM ARCHITECTURE

The design of given system is basically divided into the two steps. In this first is watermark embedding and second watermark extraction. As we are going in detailed we found some properties of image make the watermark embedding as easy task

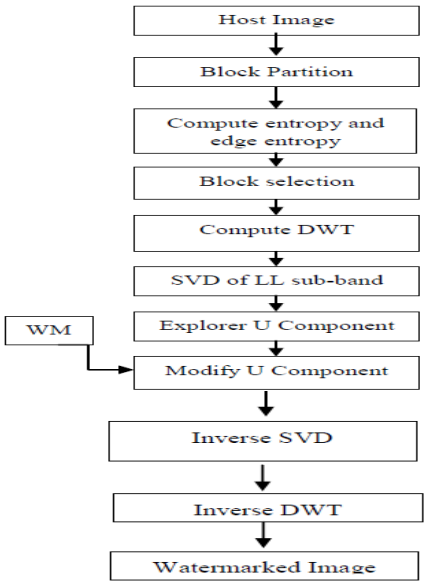

Figure 1: Watermark embedding process

The above diagram for the watermark embedding and details of the diagram are given in the mathematical model.

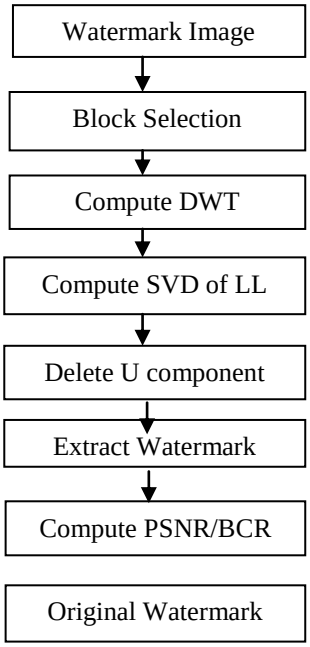

Figure 2: Watermark Extraction Process

III. DETAILED DESIGN

1. Watermark Embedding Process

Step 1: The original image is divided into non-overlapping blocks of size 2*2, 4*4, 8*8.
Step 2: Compute the sum of visual entropy and edge entropy of each block and arrange the blocks in ascending order to select the appropriate number of blocks equal to number of watermark bits.
Step 3:Perform two level DWT to selected blocks of host image to obtain four sub-bands, the approximate sub-band cA , the horizontal detail component cH , the vertical detail component cV and detail of diagonal component cD .
Step 4: Apply SVD to low frequency sub-band cA to decompose the cA into three components U, S and V i.e.
cA' =U' *S *V'
where U and V are components of unitary matrices and S is a diagonal matrix of singular values arranged in descending order.
Step 5: The watermark is a binary image which is embedded into selected coefficients of first column of the U component according to the formula:
If watermark bit is 1 then

$$U'(2,1) = -\left|\,|U(2,1)| + \left(T - \frac{Diff}{2}\right)\right|$$

$$U'(3,1) = -\left|\,|U(3,1)| - \left(T - \frac{Diff}{2}\right)\right|$$

If watermark bit is 0 then

$$U'(2,1) = -\left|\,|U(2,1)| - \left(T - \frac{Diff}{2}\right)\right|$$

$$U'(3,1) = -\left|\,|U(3,1)| + \left(T - \frac{Diff}{2}\right)\right|$$

where T is the threshold value, Diff $|U(2,1)| - |U(3,1)|$and U' is the watermarked component.
Step 6: Perform inverse SVD to each block used for embedding the watermark bit to obtain the watermarked low frequency sub-band i.e.
cA' = U ' *S *V '
where cA' is the watermarked approximate sub-band.
Step 7:Perform inverse DWT to obtain the watermarked image.
Step 8:Compute PSNR value between watermarked image and host image to evaluate the quality and imperceptibility of watermarked image.

2.Watermark Extraction Process

Step 1: The watermarked image is divided into non-overlapping blocks of size 2*2, 4*4, 8*8.
Step 2:Select the appropriate number of blocks used in embedding process using human visual characteristics.
Step 3: Apply two level DWT to each selected block of watermarked image to obtain the approximate sub-band cA', the horizontal detail component cH', the vertical detail component cV ' and detail of diagonal component cD'.
Step 4:Apply SVD to cA' of each selected block to decompose cA' into three components U', S ' and V ' i.e.
[U' S ' V ']= svd (cA')
Step 5:The second and third co-efficient of first column of U' is examined to obtain the extraction of watermark bits. If $(|U(2,1)| - |U(3,1)|) > 0$ then the extracted watermark bit is one otherwise zero.
Step 6: The watermarked bits obtained in step5 forms a vector which is converted into matrix to obtain the watermark image.
Step 7: Peak signal noise ratio (PSNR) is computed to evaluate the visual quality of watermark.

IV. EXPERIMENTAL RESULTS

The experiments in this paper are tested with MATLAB 7.0. The original image used to test is a 512×512 image.
1. PSNR
The PSNR rates for all three images are calculated. From the results we found that 8x8 block shows good authentication results. Also if we go for compression the PSNR rate is decreases.

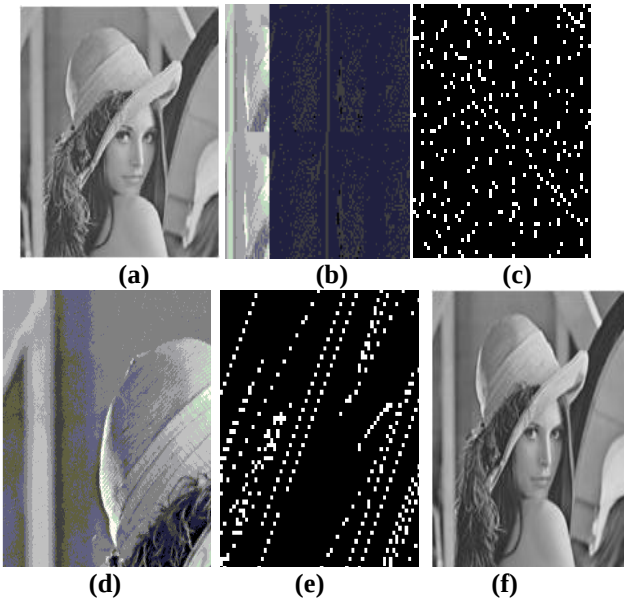

Figure 3: Perceptibility Test (a)Original Image (b) 2-level DWT (c) Contour Image (d) Selected area (e) Inverse DWT (f) Watermarked Image

TABLE1: Comparison of PSNR Using Dwt

Block size	Watermark Region	PSNR
2x2	LH or HL	47.94
4x4	LH or HL	58.36
8x8	LH or HL	65.07

TABLE2: Comparison of PSNR using SVD

Block size	Watermark Region	PSNR
2x2	LH or HL	82.38
4x4	LH or HL	89.51
8x8	LH or HL	95.47

Comparison of PSNR in dB with existing watermarking algorithm for image size 512x512 with watermark size 32x32

TABLE3: Comparison of PSNR using Our Method & Various Authors

Paper/Image	Lena	Pepper
Hi jinn horng	44.25	43.60
Byun .lee	41.95	44.37
E.Li H.Liang	40.60	42.60
Charkari	51.70	46.43
Chin chin li	48.58	47.94
Rajash m[16]	51.06	50.72
Our method	63.69	52.39

V. CONCLUSION

In this paper we used SVD-DWT transform method for watermark embedding. Also due to Arnold transform space relativity is get reduced. From the above result we can say that algorithm which is proposed here is good as compared to previous one. In this particular algorithm we can use any logo or another image as the watermark to embed in the given region. So it is easy to improve the result by such experiment.

REFERENCES

1. J. Cox, M. L. Miller and J. A. Bloom, Digital Watermarking, New York: Academic Press , 2002.
2. Cox, J. Kilian, F. T. Leighton and T. Shamoon, "Secure spread spectrum watermarking for ultimedia," IEEE Transactions on Image Processing, vol. 6, pp. 1673-1687, December 1997.
3. S. Walton, “Authentication for a slippery new age,” Dr. Dobb’s Journal, vol. 20, no. 4, pp. 18-26, April 1995.
4. C. Lu and H. Liao, “Multipurpose watermarking for image authentication and protection,” IEEE Transactions on Image Processing, vol. 10, no. 10, pp. 1579- 1592, October 2001.
5. C. Y. Lin and S. F. Chang. “Semi-fragile watermarking for authenticating JPEG visual content,” Proceedings of the SPIE International Conference on Security and Watermarking of Multimedia Contents II, San Jose, USA, vol.3971, pp.140-151, 2000.
6. S. Yang, Z. Lu and F. Zou. “A Novel Semi-fragile Watermarking Technique for Image Authentication,” ICSP Proceedings, pp. 2282–2285, 2005.
7. J. Huang, Y. Shi and W. Cheng, "Image watermarking in DCT: An embedding strategy and algorithm," Acta Electronica Sinic, vol.28, no.4,pp.57-60, 2000. (in Chinese)
8. X. Li, "Blocked DCT and quantization based blind image watermark algorithm," Computer Engineering, vol.32, no.21, pp.139-144, 2006. (in Chinese)
9. J. Zhang and C. Zhang, “Semi-fragile watermarking for JPEG2000 image authentication,” ACTA Electronica Sinica, vol.32, no.1, pp.157-160, 2004. (in Chinese)
10. X. Wang, L. Meng and H. Yang, “Geometrically invariant color image watermarking scheme using feature points,” Sci China Ser F-Inf Sci, vol.52, no.9, pp.1605-1616, September
11. Daxing Zhang, Zhigeng Pan” A Contour-based Semi-fragile Image Watermarking Algorithm in DWT Domain” IEEE2010 Second International Workshop on Education Technology and Computer Science
12. P. Fakhari, E. Vahedi, and C. Lucas, “Protecting patient privacy from unauthorized release of medical images using a bio-inspired wavelet-based watermarking approach,” Digital Signal Processing, vol. 21, no. 3, pp. 433 – 446, 2011. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1051200411000170
13. Liu Bo, Yang Zhaorong. “Image Compression Based on Wavelet Transform” IEEE publication on 2012 International Conference on Measurement, Information and Control (MIC)
14. Sachin Mehta, Rajarathnam Nallusamy, Ranjeet Vinayak Marawar, Balakrishnan Prabhakaran. “A Hybrid Semi-Blind Gray Scale Image Watermarking Algorithm Based on DWT-SVD using Human Visual System Model” IEEE 2013 International Conference on Healthcare Informatics.
15. Ye Xueyi ,ang yunglu ,Zhang jing “A Robust DWT-SVD blind watermarking algorithm based on Zernike moment” ieee 2014 conference communication security
16. Naderahmaderin Y. Beheti .S“Robustness of wavelet domain watermarking against scaling attack”IEEE 2015 international conference on CCECE

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication