International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075, Volume-8 Issue-4S2 March, 2019

Development of Reversible Video Watermarking Algorithm based on Hybrid DWT-SVD

Neha Patil , V. R. Udupi

Abstract*: *The research work aimed to develop a reversible DWT-SVD. We reviewed different methods for reversible video watermarking which gives linear response for data integrity, authentication and content protection. Spatial domain methods are normally fragile adversary-based attacks. Thus, for developing robustness and fragility balanced technique, research work is carried out in the transform domain. DWT has the excellent capacity of localization of special-frequency and multi-resolution characteristics. This is suitable to identify areas where watermark can be invisibly embedded. In case of small perturbation, singular values do not give large variation, also intrinsic algebraic properties are represented by singular values. SVD is computationally expensive, therefore hybrid DWT-SVD method is developed to embed the watermark on video by modifying diagonal singular value coefficients of LL sub-band with scaling factor 0.10 and watermark itself. This method decreases computational cost and shows high robustness and fragility balance. Dynamic access code (DAC) is generated for authentication purpose, so that at the receiving stage the original video or transmitted data is available only to the specified user. Benchmarking of software written in MATLAB, by selecting different videos and watermark on it. Experimental results give the efficiency of proposed algorithm with reference to visual effects and analysis of qualitative and quantitative measures for PSNR and CC. The proposed method can be implemented in the area of military applications, medical image analysis, law enforcement, healthcare.

Index Terms*: *Reversible Watermarking, Information Hiding, DWT, SVD, Multimedia Data.

I. INTRODUCTION

In recent years, use of multimedia data has been increased. This leads to issues such as copy protection, vulnerability, copyright violation. Conventional watermarking technique can cause to permanent distortion of input image. Thus, an exact recovery of watermark at receiver side is not possible. This is intolerable in the field of military applications, medical image analysis, law enforcement, healthcare. Reversible watermarking allows full extraction of embedded watermark along with restoration of the input image in original form. This is also called as lossless watermarking.

The basic reversible watermarking scheme shown in figure 1. Robust, fragile and semi-fragile are three classes based on watermarking properties.

In robust watermarking scheme, the watermark survive in different image processing operations such as adversary based attack. This is suitable in copyright protection applications. A fragile watermarking scheme is used for authentication, which loses watermark in case of tempering. In a semi-fragile watermarking scheme, the watermark survives against user level operations.

According to the watermark embedding domain, these techniques are categorized in two domains. In special domain, watermark embeds into image pixels directly. This is easy to implement and less complex. However, special domain methods are normally fragile to attacks. In transform domain, watermark embeds in the image by modulating the magnitude of coefficients. This balances the robustness and fragility and take invisibility into account but leads to high computational cost. In order to achieve a high-performance watermarking technique should meet some characteristics such as robustness and fragility balance, invisibility, versatility, security. Thus, we carried out further work in transform domain.

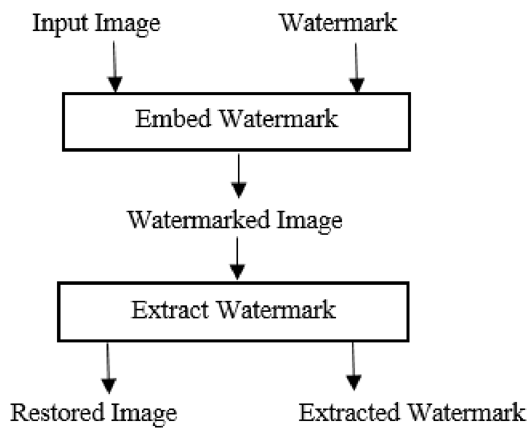


Figure 1. Basic Reversible Image Watermarking Scheme

Widely used transform domain techniques are DCT, DWT, DFT. Discreet wavelet transform (DWT) decompose image into different bands and has excellent capacity of localization of spatial-frequency and multi resolution characteristics. This is suitable to identify areas where watermark can be invisibly embedded. Visual perception of input image cannot be affected by a slight variation in singular values. This singular value decomposition (SVD) helps

Revised Manuscript Received on December 22, 2018.

Neha Patil, Computer Science & Engineering Department, Gogte Institute of technology, VTU University, Belagavi, India.

Dr. V. R. Udupi, Electronics and Communication Engineering Department, Maratha Mandal Engineering College, VTU University, Belagavi, India

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

to get better transparency. As SVD is computationally expensive, we have developed a hybrid DWT-SVD watermarking scheme which require less computational cost.

II. METHODOLOGY

A. Embed Watermark Algorithm

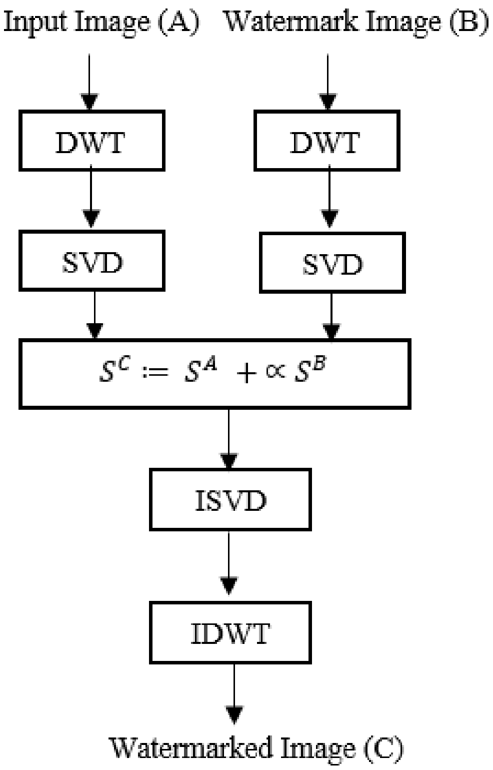


Figure 2. Mathematical Model for Embedding Process

Input: Original Video and Watermark Image

Output: Watermarked Video

1. Generate dynamic access code (Ks) for transmission security.

2. Read video and divide the video into frames and store these frames sequentially.

3. DWT is applied on Red, Green, Blue planes of the input image which decomposes image into four sub-bands using the haar wavelet transform.

4. Select LL sub-band of input image & implement SVD.

$$A = U^A\ S^A\ V^A \tag{4}$$

5. DWT is applied on Red, Green, Blue planes of the watermark image which decomposes image into four sub-bands using the haar wavelet transform.

6. Select LL sub-band of the watermark and implement SVD.

$$B = U^B\ S^B\ V^B \tag{5}$$

7. Diagonal singular value coefficients for LL sub-band are modified with the scaling factor and the watermark itself.

$$S^C = S^A + \propto S^B \tag{6}$$

where α is the scaling factor. S^A and S^B are the diagonal coefficient of the input and the watermark image respectively.

8. LL sub-band is reconstructed for each red, green, blue planes.

$$C = U^A\ S^C\ V^A \tag{7}$$

9. Inverse DWT is implemented to obtain the watermarked image.

10. Create watermarked video by combining watermarked images. Thus we get the watermarked video for transmission.

B. Extract Watermark Algorithm

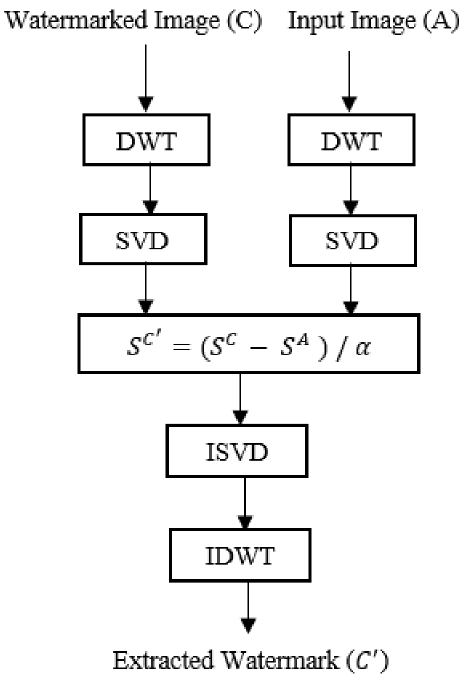


Figure 3. Mathematical Model for extraction process

Input: Watermarked Video

Output: Extracted Watermark Image

1. Enter dynamic access code (Kr) and compare it with Ks. If Kr == Ks, then user is authenticated and allowed to extract the watermark from selected video.

2. Get watermarked video and divide it into frames and store frames sequentially.

3. DWT is applied on Red, Green, Blue planes of the watermarked image which decomposes image into four sub-bands using the haar wavelet transform.

4. Select LL sub-band of the watermarked image and implement SVD.

$$C = U^C\ S^C\ V^C \tag{5}$$

5. DWT is applied on Red, Green, Blue planes of the input image which decomposes image into four sub-bands using the haar wavelet transform.

6. Select LL sub-band of input image & implement SVD.

$$A = U^A\ S^A\ V^A \tag{6}$$

7. Diagonal singular value coefficient for the extracted watermark is constructed using the diagonal singular value coefficient of watermarked image, input image and scaling factor 0.10

$$S^{C'} = (S^C - S^A)/\propto$$

(7)

8. LL sub-band is

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

reconstructed for each red, green, blue planes.

$$C' = U^C \; S^{C'} \; V^C \tag{8}$$

9. Inverse DWT is applied to obtain the watermark.
10. The original watermark compared with the extracted watermark. If average CC ≥ threshold value 0.98 then the data integrity achieved.

III. PERFORMANCE MEASURE

A. PSNR : Watermarked image quality is estimated with respect to original image using PSNR.

$$PSNR = 10 \; log_{10} \; \frac{Z_{max}^2}{\frac{1}{MN} \sum_{i,j} [\, q(i,j) - p(i,j)]^2} \tag{9}$$

where $Z_{max} = 255$

$p(i,j)$ is intensity values of input image

$q(i,j)$ is intensity values of the watermarked image.

B. Coefficient of Correlation (CC) : Quality analysis of the watermark and the restored watermark is checked using coefficient of correlation.

$$CC = corr2(A,B) \tag{10}$$

where, A and B are matrices or vectors of the same size.

IV. RESULTS AND DISCUSSIONS

Performance is evaluated by selecting five videos (video 1 to video 5) and five watermarks (W1 to W5). A scaling factor chosen is 0.10. Average PSNR and CC are calculated and shown in Table 1 and Table 2.

Calculation of Threshold Value:

=(0.9847+0.9854+0.9887+0.9820+0.9864)/5

= 0.9854≈0.98

Threshold value for coefficients of correlation is considered as 0.98 for every video. As shown in Table 2, Video 1 to Video 5 gives an average coefficient of correlation greater than Threshold value 0.98. This data integrity is achieved. Experimental results give the efficiency of proposed algorithm with reference to visual effects and analysis of qualitative and quantitative measures for PSNR and CC.

Figure 4. Input Image

Figure 5. Watermark Image

Figure 6. Watermarked Image

Figure 7. Extracted Watermark

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

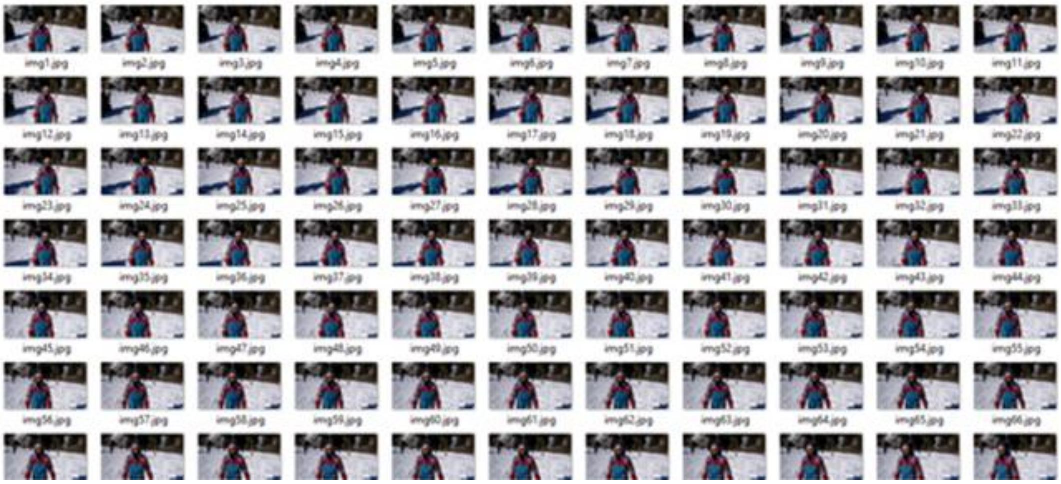


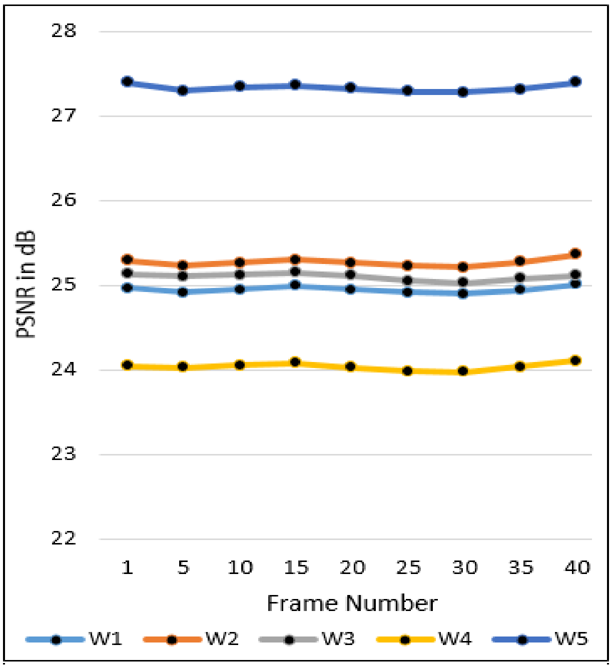
Figure 8. Video divided into number of frames

Table 1. Calculation of Average PSNR between the Original and Watermarked Video

	 **W1**	 **W2**	 **W3**	 **W4**	 **W5**	**Average PSNR**
Video 1	24.8905	25.2652	24.8986	24.0906	27.5810	**25.3482**
Video 2	24.9419	25.2625	25.0944	24.0335	27.3267	**25.3318**
Video 3	23.8897	24.2144	24.0474	23.2493	26.5049	**24.3811**
Video 4	25.2314	25.1542	26.1673	24.1000	27.5849	**25.6476**
Video 5	24.8780	25.0970	24.9799	23.8799	27.3677	**25.2405**

Table 2. Calculation of Average CC between the Original and Extracted Watermark

	 **W1**	 **W2**	 **W3**	 **W4**	 **W5**	**Average CC**
Video 1	0.9843	0.9838	0.9840	0.9885	0.9831	**0.9847**
Video 2	0.9857	0.9851	0.9897	0.9841	0.9826	**0.9854**
Video 3	0.9897	0.9894	0.9889	0.9888	0.9868	**0.9887**
Video 4	0.9802	0.9848	0.9816	0.9829	0.9807	**0.9820**
Video 5	0.9886	0.9870	0.9855	0.9850	0.9860	**0.9864**



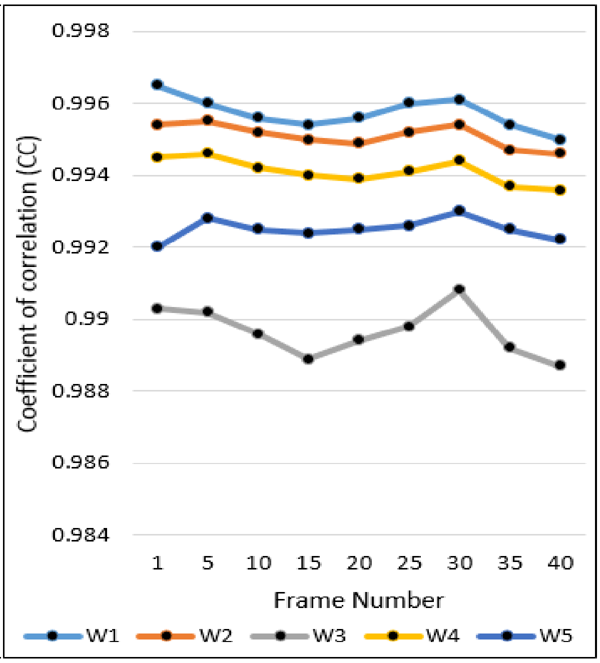


Figure 9. PSNR between original & watermarked video frames. **Figure 10.** CC between the original & extracted watermark.

V. CONCLUSION

We have developed a new reversible watermarking technique based on hybrid DWT & SVD. On sender side, video is converted into the number of frames. DWT is applied to Red, Green, Blue planes which decomposes each plane into four sub-bands using the haar wavelet transform. This is first level decomposition. Diagonal singular value coefficients of LL sub-band are modified with scaling factor and watermark. Then LL sub-band is reconstructed for each Red, Green, Blue planes and watermarked image is obtained by applying Inverse DWT. On receiver side, diagonal singular value coefficients for the extracted watermark is constructed using the diagonal singular value coefficient of watermarked image, input image and scaling factor 0.10. Threshold value 0.99 is defined to check data integrity. Dynamic access code (DAC) is generated for authentication purpose, so that at the receiving stage the original video or transmitted data is available only to the specified user. This method decreases the computational cost and shows high robustness and fragility balance. Benchmarking of software written in MATLAB by selecting different videos and watermarks. Experimental results give the efficiency of proposed algorithm with reference to visual effects and analysis of qualitative and quantitative measures for PSNR and CC.

REFERENCES

1. Youcai Gao, Yun-Qing Shi, Jinwei Wang, "Dynamic multi-watermarking and detecting in DWT domain", Journal of Real-Time Image Processing, pp. 1–12, 14 Aug 2018.
2. Poonam, Shaifali M. Arora, "A DWT-SVD based Robust Digital Watermarking for Digital Images", Procedia Computer Science, vol. 132, pp. 1441-1448, 2018.
3. Vedvyas J. Dwivedi, Rohit M. Thanki, Komal R. Borisagar, "Multibiometric Watermarking Technique Using Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT)", Multibiometric Watermarking with Compressive Sensing Theory, pp. 91-113, 04 Jan 2018.
4. Xiao-bing Kang, Ya-jun Chen, Fan ZhaoGuang-feng Lin, "A novel hybrid of DCT and SVD in DWT domain for robust and invisible blind image watermarking with optimal embedding strength", Multimedia Tools and Applications, vol. 77, pp. 13197–13224, Jun 2018.
5. Amir Anees, Abdulmohsen Algarni, Iqtadar Hussain, Muhammad Aslam, "A Robust Watermarking Scheme for Online Multimedia Copyright Protection Using New Chaotic Map", Security and Communication Networks, vol. 128, pp. 20, 28 Jun 2018.
6. Sampath Kiran, P. Rajesh Kumar, Deepika Sanku, Tamirat Tagesse Takore, "Digital Image Watermarking in RGB Host Using DWT, SVD, and PSO Techniques", Proceedings of 2nd International Conference on Micro-Electronics, Electromagnetics and Telecommunications, vol. 434, pp 333-342, 07 Sept 2017.
7. Somanshi Ojha, Rekha Chaturvedi, Abhay Sharma, "Centric-Oriented Novel Image Watermarking Technique Based on DWT and SVD", Soft Computing: Theories and Applications, vol 583, pp 217-225, 25 Nov 2017.
8. Irshad Ahmad Ansari, Millie Pant, "Multipurpose image watermarking in the domain of DWT based on SVD and ABC", Pattern Recognition Letters, vol. 94, pp. 228-236, 2017.
9. Amit Mehtoa, Neelesh Mehra, "Adaptive Lossless Medical Image Watermarking Algorithm Based on DCT & DWT", Procedia Computer Science, vol. 78, pp. 88-94, 2016.
10. Beijing, Jianbin, "An Identity-Based One-Time Password Scheme with Anonymous Authentication", Networks Security, Wireless Communication and Trusted Computing, vol. 2, pp. 864–867, 2009.
11. Kuan-chieh Liao, "A One-Time Password Scheme with QR-Code Based on Mobile Phone", IEEE, INC, IMS, IDC, pp. 2069-2071, 2009.
12. Harris, J. A., "OPA: a one-time password system", IEEE in Parallel Processing Workshop, Proceedings, pp. 25-29, 2002.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication