Asian Journal of Computer Science and Technology
ISSN: 2249-0701 (P) Vol.8 No.S3, 2019, pp.85-89
© The Research Publication, www.trp.org.in
DOI: https://doi.org/10.51983/ajcst-2019.8.S3.2079

A Robust Watermarking Scheme Using DWT and SVD

B. Gopi[1] and T. Sudha[2]
[1]Research Scholar, Department of Computer Science, Vikrama Simhapuri University, Andhra Pradesh, India
[2]Professor, Department of Computer Science, Sri Padmavati Mahila ViswaVidhyalayam, Andhra Pradesh, India
E-Mail: gopikrishnavarma@gmail.com

(Received 20 April 2019; Revised 30 April 2019; Accepted 11 May 2019; Available online 20 May 2019)

***Abstract* - Singular value decomposition is in use quite recently in many applications. The SVD is being used for many applications along with other techniques. In this paper a robust watermarking scheme was proposed by using SVD along with wavelet transform. In addition to normal hiding scheme a random signature was used to improve its robustness against spurious intruders. The unitary matrices are used to generate a signature which is going to be embedded into the fourth level decomposition of cover image. After extracting the watermark at the other end, it will be checked with the signature embedded. If these signatures are matched the unitary matrices will be used to extract watermark from watermarked image. Different attacks are considered and the simulation results have shown that the extraction of watermark after attacks have shown minor effect only.**

***Keywords:* SVD, Attacks, Watermarking, Authentication**

I. INTRODUCTION

In contemporary years, fast growth of network multimedia systems and other numerical technologies have been observed. This requires an increasing cognizance of how simple it is to imitate the data. The comfort with which flawless replicas can be made may lead to significant illegal copying, which isa great concern to the audio, video, text, and software distributing businesses. Because of this concern over copyright issues, a number of technologies are being developed to protect against illegal copying. One of these techniques is the use of digital watermarks. Watermarking embeds an ownership signal directly into the data. In this way, the signal is always present with the data. Watermarking is the technique of embedding a secret imperceptible signal directly into the original data in such a way that always remains present. Existing watermarking schemes can be divided into two categories: spatial domain schemes and transform domain schemes. Spatial domain schemes embed data by directly modifying pixel values of the host image, while transform domain schemes embed data by modifying transform domain coefficients.

The major benefit of transform domain approaches is their extreme robustness to common image distortions. DCT (Discrete cosine transforms) and DWT (Discrete wavelet transform), which are utilized in image compression standards JPEG and JPEG2000, are two main transform techniques used in frequency domain watermarking. As wavelet transform decomposes images into four parts, DWT-based watermarking systems can embed data in any frequency band separately. This process result in robustness to a wide range ofattacks for embedding in low and high frequency bands are complementary. Symmetrical attacks such as scaling, rotation, and translation are simple to apply and may result many watermark detectors to total failure due to loss of synchronization among the embedded and the correlating watermarking. Numerous watermarking techniques resilient to geometric attacks have been proposed in the literature [1][2]. The secret information should be embedded in secure and robust manner such that it remains resistive to malicious attempts of removal [3]. Usually the watermark is the information about the digital content it intends to protect. A watermark should be embedded in such a way that it remains detectable as long as the perceptual quality of the digital content stays at an acceptable level [4].

In general, any watermarking scheme contains the following parts: Watermark image, Cover image, Encoding and decoding sections. The theoretical model of the watermarking system is described in [5]. The encoder embeds the watermark into the cover image. The watermark can be a pseudorandom number, any binary sequence or more practically a confidential data. An optional key is used to improve the security of the scheme. Decoder section predicts the watermark from the received watermarked image with the help of key and cover image if need be. Watermarked image is subjected to various forms of attacks on cover image. The watermarking methods can be categorized based on the presence and absence of original content at the time of watermark extraction.

1. *Non-Blind:* It needs original content during watermark extraction.
2. *Blind:* It does not need the original content during extraction of the watermark.

In the earlier days non-blind watermarking systems were prevalent as they were more robust than blind systems. It is because of the fact that in watermarking model the original content is considered as a noise source to watermark, which is the signal of interest. The presence of original content at the receiver cancels the effect of this noise effect. However, the non-blind systems suffer from two different short comings.

1. *Security Compromise:* Non-blind extraction does not assure unambiguous claim of ownership by the content originator. Attacker can easily fool the system, may

claim the ownership by inserting another watermark in the content.

2. *Practical Constraints:* It is impossible to ensure presence of original content during extraction for every watermarking application.

In this research a blind watermarking scheme is considered. The rest of the paper is organized as follows. In the next section the related work is presented, the third section discusses the SVD. In the fourth and fifth sections the watermarking scheme using SVD and proposed techniques are presented. In the sixth section the simulation results are presented and section VII concludes the paper.

II. RELATED WORK

In the literature many watermarking systems have been proposed with the intents of improving robustness and perceptual quality. Raval and Rege proposed a DWT based multiple watermarking systems [6]. Image was decomposed in two levels and watermarks were inserted in LL and HH bands. The scheme has shown good results against different attacks like compression, noise addition, and histogram equalization but almost failed at rotation, scaling and print-scan attacks.

Kasmani and Naghsh-Nilchi proposed a combination of DWT and DCT to embed the binary watermark [7]. They have implemented a 3-level DWT decomposition and then applied DCT to embed the watermark. Simulation results showed a good watermark extraction against many attacks but this scheme takes more execution time. Furthermore, it had a non-blind extraction. In recent times singular value decomposition became very prevalent in watermarking systems because of its attractive mathematical properties. SVD is popular for the watermarking [8][9] because of the following reasons.

1. Few singular values can represent large portion of signal energy,
2. SVD can be applied to square as well as rectangular images,
3. The SVs (singular values) of an image have very good noise immunity, i.e., SVs don't change significantly when a small perturbation is added to an image intensity values,
4. SVs represent intrinsic algebraic properties.

Most of the previous procedures based on SVD embeds watermark straightaway into SVs. For instance, Liu and Tan presented an algorithm in which watermark was embedded into the SVD domain and the extraction was blind [10]. Results shown that scheme proved to be robust against filtering, compression, cropping but fails against rotation, print-scan and scaling attacks. Ghazy *et al.*, separated the image into non-overlapping parts and then applied SVD to these blocks [11]. SVs of these parts were used to embed the watermark. This system have shown good results against compression, filtering, noise addition but failed against cropping and geometric attacks. With an aim to increase the robustness of watermarking scheme Bhandari *et al.*, used spread spectrum along with SVD [12].

They have utilized two watermarks during embedding; one was embedded using spread spectrum technique and other by using pure SVD. Spread spectrum methods provided robustness against compression, rotation, filtering, scaling, print and scan attack, while, SVD offered good robustness against noise addition and histogram equalization. Hence, these two complementary techniques covered wide range of attacks however, scheme was non-blind in nature. The SVD schemes which are using transform domain coefficients for decomposition are called hybrid SVD schemes. DCT, DWT, FFT are among popular frequency transforms. A hybrid method based on DCT and SVD has been proposed by Quan and Qingsong [13]. They applied DCT to the cover image and coefficients are mapped to frequency bands using zig-zag scanning.

SVD was then applied to each band. SVs of the DCT transformed visual watermark are then utilized to change the SVs of each band of the host image. Resulted robustness against compression, filtering and cropping but watermark cannot survive against geometrical attacks and print-scan attack. The scheme was computationally expensive and non-blind in nature. An SVD based algorithm using DWT has been presented by Ganic and Ahmet Eskicioglu [14] which is very similar to the algorithm by Quan and Qingsong [13]. The host image is decomposed using DWT into four sub bands. SVD is applied to each sub band and also to the watermark. Singular values of the cover image are modified using the singular values of the watermark during embedding process. This scheme gives comparatively good results when compared to all the schemes discussed so far.

III. SVD

A common problem is that the response matrix is singular or close to singular, so it has no well-defined inverse. Of the various algorithms that have been developed to deal with this problem, singular value decomposition (SVD) has emerged as the most popular. Any matrix can be represented with SVD as follows:

$$M \qquad {}_{k\ \ 1}^{\ \ n} \vec{u}_k w_k \vec{v}_k^{T}$$

Where v_k is a set of orthonormal steering magnet vectors, u_k is a corresponding set of orthonormal BPM vectors, and w_k are the singular values of the matrix M. Given the SVD of a matrix, the matrix inverse is:

$$M^{\ 1} \qquad {}_{k\ \ 1}^{\ \ n} \overset{r}{v}_k \frac{1}{w_k} \overset{r}{u}{}_{k}^{T}$$

which follows from the ortho normality of the two vector sets. It is immediately apparent from the singular value decomposition if the response matrix is singular one or more of singular values, w_k, are zero. Physically, a zero w_k

implies that there is some combination of steering magnet changes, v_k, which gives no measurable change in orbit. The orbit shift from this v_k is zero at all the BPMs. Removing the terms with zero w_k from the sum in the above equation produces a pseudo inverse for orbit correction which generates no changes in the steering magnet strengths along the corresponding eigenvectors v_k.

IV. THE STANDARD DWT-SVD WATERMARKING ALGORITHM

In this paper a basic watermarking based on cascading DWT with SVD is proposed. By using DWT the cover image is decomposed into four frequency bands: LL, HL, LH, and HH bands. LL band characterize slow frequency, HL and LH characterize middle frequency and HH characterizes high frequency bands, correspondingly. The LL band signifies approximate details, HL band horizontal details, LH vertical details and HH band diagonal details of the image. In this scheme, HH band was selected to embed the watermark image because it comprises of finer details and contributes immaterially to the image energy. Therefore embedding of watermark will not affect the perceptual fidelity of cover image. Furthermore, high energy LL band coefficient cannot be pinched way from certain point as it will harshly impact perceptual superiority. Also, Raval and Rege [6] observed that watermark image inserted in HH band lasts certain image processing operations or attacks like noise addition, intensity manipulation and limitation of the human visual system (HVS) can be exploited by inserting watermark into HH band.

The HVS fails to distinguish variations made to HH band. Thus the proposed scheme is based on the idea of replacing singular values of the HH band with the singular values of the watermark. It is observed that singular values lie between 84 and 173 for most of the standard images. If a watermark is selected such that its singular values lies within the given range, then the energy of the singular values of watermark image will be roughly equal to the energy of the SVs of the HH band. Thus the replacement of the singular values will not affect perceptual quality of image as well as the energy content of HH band. Watermark image used for experimentation in this work is preprocessed to have singular values within the range of 0–150 and it closely matches the singular values of the given test images.

A. Algorithm for Watermark Embedding

1. Watermark ‘W’ is decomposed using SVD, $W = U_w * S_w * V_w^T$
2. Apply wavelet (in this work ‘haar’) and decompose cover image into four sub bands: LL, HL, LH, and HH.
3. Apply SVD to HH band. $H = U_H * S_H * V_H^T$
4. Substitute the SVs of the HH band with that of the watermark.
5. Apply inverse SVD to obtain the modified HH band. $H' = U_H * S_w * V_H^T$
6. Apply inverse DWT to produce the watermarked image.

B. Algorithm for watermark extraction

1. Using the haar wavelet, decompose the (noisy) watermarked image into four sub-bands: LL, HL, LH, and HH.
2. Apply SVD to HH band. $H = U_H * S_H * V_H^T$
3. Extract the SVs from HH band.
4. Reconstruct the watermark using SVs and orthogonal matrices U_w and V_w acquired using SVD of original watermark.
   $W_E = U_w * S_H * V_w^T$

This constitutes a blind decoding as the extraction process don’t need original cover image for extracting the watermark image at the receiver.

V. AUTHENTICATION MECHANISM IN THE PROPOSED SCHEME

Zhang and Li [15] observed an authentication problem in the basic SVD based approaches proposed by Zhou and Chen [9], and Ganic and Ahmet Eskicioglu [14]. This section discusses the common problem with most of SVD-based schemes in the state-of-art techniques. To make evident the problem assume that two different watermark images were embedded in an image separately as shown in fig.1 using the standard SVD system. The watermark images were embedded by changing the SVs of cover image with the SVs of the watermark images. Decoder guesstimates the watermark by merging SVs extracted from one watermarked image and using orthogonal matrices of other watermark. Fig. 2 shows that the decoder extracted SVs from watermarked image-2 and combines them with orthogonal matrices (U1 and V1*)* for watermark extraction. As a consequence, watermark-1 is extracted in place of watermark-2.

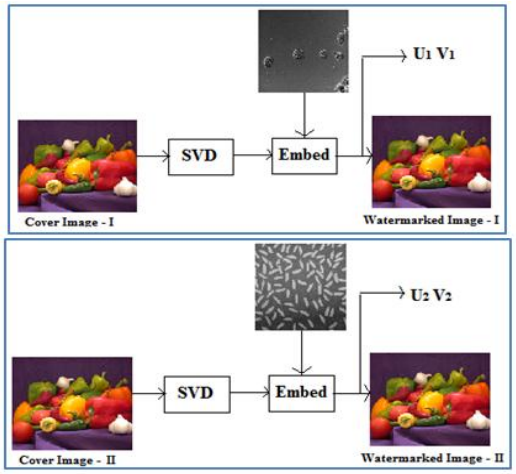

Fig. 1 embedding of watermark

Zhang and Li in [15] shown that the orthogonal matrices U and V preserve most of the datas they characterize Eigen vectors of the respective SVs. When inverse SVD is applied, Eigen vectors play a significant role in extraction. Thus if any singular matrix is utilized along with Eigen vectors it will produce the correlated output as an alternative of the actual output. The correlation will be high if the unmatched SVs will be roughly equal to the original SVs. So it gives rise to large number of false-positives during watermark detection and also presents a security hazard.

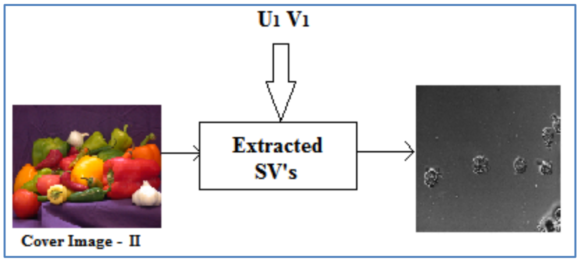

Fig. 2 Extraction of watermark

This risk can be seen as problem of unauthorized embedding wherever an attacker may use his own set of Eigen vectors throughout watermark extraction and claims false possession. To overcome these disadvantages, a signature-based authentication tool for U and V matrices was presented in this paper. Orthogonal matrices (U and V) are authenticated before combining them with SVs to generate watermark image.

A unique signature conforming to the orthogonal matrices are created and embedded into the cover image along with the watermark. The decoder extracts these signatures, authenticates orthogonal matrices and then proceeds with the extraction of watermark. This will safeguard a correct mapping among the SVs and orthogonal matrices.

A. Generation of Signature: Digital signature of the orthogonal matrices is a unique binary string made through a hashing function. In addition, the digital signature must be random, so that an attacker can’t predict them. Digital signature for the orthogonal matrices is generated as follows.

1. Proposed Algorithm

a. Add the column of orthogonal matrices and create 1-D array.
b. Based on the threshold, map the array values into corresponding binary digits.
c. By XORing the binary digits make the signature for the given orthogonal matrices.

Threshold value plays an important role while mapping and it is used to randomize the mapping, improving the security.

B. Proposed authentication scheme: Embedded signature should remain robust against processing manipulation. Alteration in signature bits at decoder roots authentication to miscarry. Therefore, signature bits must be embedded into high-energy region for better robustness. The length of the signature is kept small to minimize changes in the high energy coefficients. Signature should persist robust against wide range of attacks hence one set of signature bits are embedded into LL4 and another set is embedded intoHH4 band to ensure retrieval from at least one of the band. The algorithm for embedding and extracting the signature is given below.

1. Signature Embedding

a. Produce the signature of N bits for the U and V matrices of watermark.
b. Using Haar wavelet, decompose the cover image into 4 sub-bands: LL, HL, LH, and HH. Further decompose LL band to the 4th level.
c. Select N random coefficient from LL4 and HH4 band with the help of secret key. Convert the integer part into the binary code of L bits.
d. Replace the n^{th} bit of the coefficient with signature bit and then convert the binary code to its decimal representation.
e. Apply the inverse DWT with modified LL4 and HH4 band coefficients.

2. Signature Extraction

a. Using DWT, decompose the watermarked image into 4 sub-bands: LL, HL, LH, and HH with help of Haar wavelet and further decompose LL band to the 4th level.
b. Select N random coefficient from LL4 and HH4 band with the help of shared secret key. Convert the integer part of selected coefficient into the binary code of L bits.
c. Extract the n^{th} bit from the coefficient to extract the signature.
d. Generate signature using U and V matrices of the original watermark at the receiver and compare it with extracted signature. If they match, authenticate U and V matrices and use them in watermark estimation.

In this work an 8-bit signature is produced for the authentication. Certain coefficients from LL4 and HH4 were changed to 16 bit binary number and 10th most significant bit position is replaced with signature bits. This authentication mechanism is employed in parallel with the watermarking scheme. Fig. 4a and b show the block diagram of the proposed scheme. The encoder will embed the watermark and signature bits according to the proposed scheme. The decoder extracts the signature and matches it with the regenerated signature for authentication of U and V matrices. If matching criteria is satisfied, then decoder will continue estimating watermark.

VI. SIMULATION RESULTS

In this section the simulation results of the proposed technique is presented. The images in fig. 3 are considered as the cover image and watermark respectively.

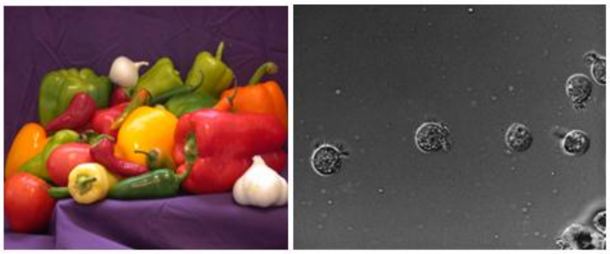

Fig. 3 Cover image and Watermark

The proposed technique is used to hide the watermark in the cover image. On the watermarked image different attacks are applied and the watermark was extracted. The attacks considered in this work are noise effects of Gaussian, Poisson, Speckle and Salt & Pepper, compression and blurring. In the figure 4 the extracted images with different attacks are shown along with the PSNR and MSE values.

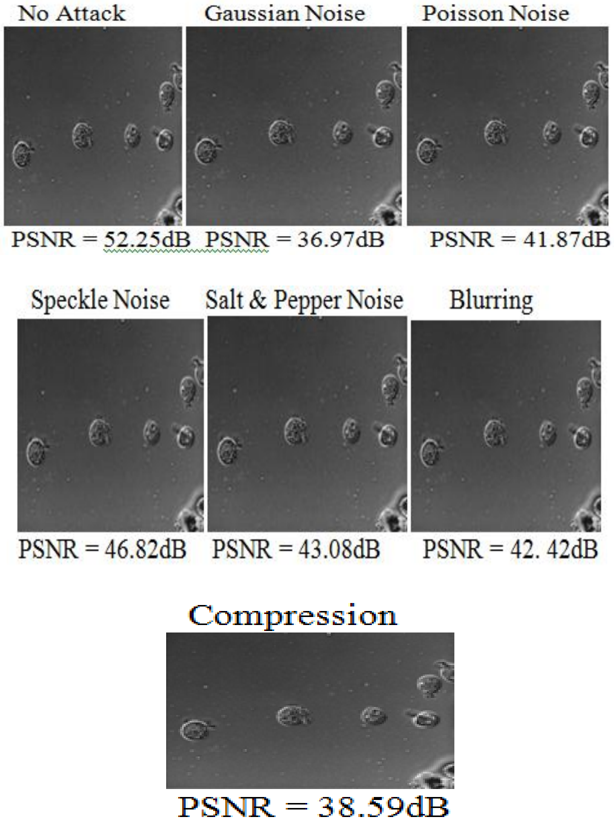

Fig. 4 Extracted watermark after different attacks

VII. CONCLUSION

In this paper a novel robust watermarking scheme was proposed using DWT and SVD. A standard DWT-SVD based watermarking scheme was used. The HH sub-band was used to hold the watermark. In the standard DWT-SVD based watermarking scheme the authentication problem was explained. A signature based resolution to the authentication problem was proposed. The signature developed in this algorithm was specific to the SVD coefficients at the instant. The signature was embedded into the fourth level decomposition of LL of the cover image. Based on a secret key four coefficients are selected and then replaced with the signature. By using similar steps on watermarked image the signature will be extracted. If the signature is matched then U and V will be used to extract the watermark from the watermarked image. The simulation results have shown that the watermark was sustained a number attacks.

REFERENCES

[1] J. O Ruanaidh and T. Pun, “Rotation, scale and translation invariant spread spectrum digital image watermarking,” *Signal Processing*, Vol. 66, No. 3, pp. 303–317, May 1998.

[2] C.Y. Lin, M. Wu, J.A. Bloom, I.J. Cox, M.L. Miller, and Y.M. Lui, “Rotation, scale and translation resilient watermarking for images,” *IEEE Trans. Image Processing*, Vol. 10, No. 5, pp. 767–782, May 2001.

[3] Katzenbeisser Stefan and A. Petitcolas Fabien, “Information hiding techniques for steganography and digital watermarking”, *Norwood, MA, USA, Artech House, Inc., 2000.*

[4] Lee Sin-Joo and Jung Sung-Hwan, “A survey of watermarking techniques applied to multimedia”, *Industrial electronics. Proceedings. ISIE 2001. IEEE International Symposium*, pp. 272–277, 2001.

[5] C.I. Podilchuk and E.J. Delp, “Digital watermarking: Algorithms and applications”, *Signal Process. Mag. IEEE.* Vol. 18, No.4, pp.33–46, 2001.

[6] M.S. Raval and P.P. Rege, “Discrete wavelet transform based multiple watermarking scheme”, *TENCON, Conference on Convergent Technologies for Asia-Pacific Region*, Vol. 3, No. 1, pp. 935–938, 2003.

[7] S.A. Kasmani and A. Naghsh-Nilchi, “A new robust digital image watermarking technique based on joint DWT-DCT transformation”, in *Proc. Convergence and Hybrid Information Technology ICCIT ‘08 Third International Conference*, pp. 539–544, 2008.

[8] H.C. Andrews and C.L. Patterson, “Singular value decomposition (SVD) image coding”, *IEEE Trans. Commun.,* Vol. 24, No.4, pp. 425–432, 1976.

[9] B. Zhou and J. Chen, “A geometric distortion resilient image watermarking algorithm based on SVD”, *Chin. J. Image Graphics*, Vol. 9, No. 1, pp. 506–512, 2004.

[10] R. Liu and T. Tan, “A SVD-based watermarking scheme for protecting rightful ownership”, *IEEE Trans. Multimed.,* Vol. 4, No. 1, pp. 121–128, 2002.

[11] R.A Ghazy, N. AEl-Fishawy, M.M. Hadhoud, M.I. Dessouky and F.E. AEl-Samie, “An efficient block-by-block SVD-based image watermarking scheme”, *Radio Science Conference*, NRSC 1–9, 2007.

[12] Bhandari Kunal, K. Mitra Suman and Jadhav Ashish, “A hybrid approach to digital image watermarking using singular value decomposition and spread spectrum”, *Pre MI*, pp. 272–275, 2005.

[13] Quan Liu and Qingsong Ai, “Combination of DCT-based and SVD-based watermarking scheme”, in *Signal Processing Proceedings, ICSP ‘04, 7th International Conference*, pp. 873–876, 2004.

[14] Ganic Emir and M. Ahmet Eskicioglu, “Robust DWT-SVD domain image watermarking: Embedding data in all frequencies”, in *Proceedings of the workshop on Multimedia and Security*, pp. 166–174, 2004.

[15] Zhang Xiao-Ping and Li Kan, “Comments on-An SVD-based watermarking scheme for protecting rightful ownership”, *IEEE Trans. On Multimedia*, Vol. 7, No.3, pp. 593–594, 2005.