A NOVEL SVD-BASED WATERMARKING SCHEME USING DWT

Dr. M. Sushanth Babu
Professor, Matrusri Engineering College, Hyderabad,
Telanagana, India

Abstract: In this paper, a watermarking system is proposed by using SVD (Singular Value Decomposition) and DWT (Discrete Wavelet Transform). Along with additional methods in literature, SVD is used for various applications. In addition to usual hiding arrangements a random moniker is utilized to increase its heftiness in contradiction to unnecessary burglars. The unitary matrices are utilized to produce a moniker which is going to be embedded into the fourth level decomposition of shield image. After extraction, an image is checked with the Moniker embedded. If these Monikers are harmonized the unitary matrices will be used to excerpt watermark from the watermarked image. Diverse attacks are well-thought-out and the simulation outcomes show that the extraction of watermark after attacks had minor effect only.

Index Terms: **Keywords: Encryption, Authentication, Moniker, SVD, Watermarking**

I. INTRODUCTION

The security of data transmitted from one place to other using regular wired or wireless network is a major concern in the current era. A large amount of secret information is being sent using a regular network it may be wired or wireless. Most of the networks will not employ additional security measures on how the data is being transferred from one place to other. Hence the users of these kinds of networks are themselves responsible to take care of their data. An attempt to transmit images safely was made in this paper. The components of a digital watermarking system are embedded and extracted. Depending on domain of shield image used to embed the watermark, literature identifies many watermarking systems proposed in spatial and transform or frequency domain.

The main pro of transform domain tactics is their extreme sturdiness to common image falsifications. DCT (Discrete cosine transform) technique which was used widely for image processing and image compression. Later, the revolution of wavelet is extended to other applications. Compared to the effective representation of the image, DWT provides a means to enable different mechanisms by which different image processing tasks can ease their implementations and improves the performance of their task. The interesting feature of the wavelet transform is that it separates the image in terms of the frequency with multiple levels. Some of the levels are playing a vital role in reconstruction and other a minor role.

Least Significant Bit (LSB)based technique in spatial domain has similarity with above technique[1], but LSB concentrates on hiding the message bits in the LSB locations of the cover image. The original LSB bits will be lost and as any change in bits leads to only one bit variation, the effect felt on the display will be very less. In addition to the said watermarking scheme, numerous watermarking techniques robust to symmetrical attacks have been proposed in the literature [2][3]. The wavelet-based watermarking schemes are found to be robust against multiple attacks like compression, blurring, salt and pepper noise and many other [4].

To sustain and mitigate many attacks, watermarking techniques provide secured transmission to the destination. Cover image, which is usually large enough for the watermarking scheme to embed the watermarking. Embedding means a process of hiding the watermark in the cover image. An attack is an act of modifying the effective appearance or the effective pixel value plane to a different set. The extraction is the process of separating the watermark from the watermarked image [5].

In the literature, a number modifications and improvements have been made to the watermarking schemes. In [6], Mohammad Ali *et. al* presented a blind digital watermarking scheme based on quantization of Eigenvalues in Wavelet domain. In the literature, fuzzy and artificial neural networks based techniques [7]-[9], SVD based techniques [10][11], hybrid techniques [12][13], Biometric template based techniques [14], Evolutionary algorithm based techniques [15], Quadtrees based techniques [16], GEP based techniques [17] and video watermarking schemes [18][19] are proposed. A large number of surveys are also being conducted [20][21].

In this paper, a watermarking scheme is proposed which is a modified version or improved version of traditional SVD-DWT based watermarking scheme. The rest of the paper is organized as follows. In section-II, the basic or standard DWT-SVD based watermarking scheme was presented. In section-III the authentication issue of the standard DWT-SVD based technique is described. Section-IV is concerned the solution of the authentication problem. Section-V presents the simulation results and the last section concludes the paper.

II. THE STANDARD DWT-SVD WATERMARKING ALGORITHM

The standard DWT-SVD watermarking scheme considers the cascade of DWT and SVD as the main building block for the watermarking scheme. The DWT will be applied to the cover image or the carrier image. The DWT usually decomposes the cover image into four frequency bands: Low-Low, Low-High, High-Low, and High-High. The Low-Low band characterizes low frequency, High-Low, and Low-High bands describe the middle frequency and High-High band characterizes high-frequency bands, respectively. The Low-Low band signifies approximate details, High-Low band horizontal details, Low-High vertical details and High-High band diagonal details of the image.

These different bands contain different grades of information in it. The cover image in Low-Low band contains all the small variations which crucial in determining the boundary of different objects present in the image. Similarly, the Low-High and High-Low has some useful information in reconstruction than that of a High-High band of frequency. Hence the High-High frequency band was selected as the candidate to store the information related to the secret data. To provide additional security the SVD is applied to the High-High band of cover image as well as to the watermark. The concept of this scheme is to replace the singular values obtained after applying the SVD of cover image with the singular values of the watermark. For standard images, it is noticed that, singular values varies from 85 to 175.

a. ***Embedding of Watermark:***

i. Decompose the watermark using SVD decomposition

$$W = U_w * S_w * V_w^T$$

ii. Apply DWT('Haar' wavelet was used in this work) and decompose carrier image into four subbands: Low-Low, High-Low, Low-High, and High-High.

iii. Applying SVD to a High-High band.

$$H = U_H * S_H * V_H^T$$

iv. Substitute the Singular values of the High-High band with that of the watermark.

v. Apply inverse SVD to obtain the modified High-High band.

$$H' = U_H * S_w * V_H^T$$

vi. Apply IDWT to produce the watermarked image.

b. Extraction of watermark:

i. Using the DWT, decompose the watermarked image which is the outcome of an attack (if any) into four sub-bands: Low-Low, High-Low, Low-High, and High-High.

ii. Apply SVD to a High-High band.

$$H = U_H * S_H * V_H^T$$

iii. Extract the SVs from a High-High band.

iv. Reconstruct the watermark using SVs and orthogonal matrices (OMs)U_w and V_w acquired using SVD of original watermark.

$$W_E = U_w * S_H * V_w^T$$

III. AUTHENTICATION ISSUE IN THE DWT-SVD BASED TECHNIQUE

In the literature, different DWT-SVD based techniques are proposed. The fundamental and which assumed to perform well on different attacks are Zhou and Chen [22], and Ganic*et. al* [23]. Zhang *et.al* identified an authentication difficulty of the basic Singular value decomposition based methods [24].Figure 1, shows that the watermark's singular values are embedded into the cover image. In the figure, the orthogonal matrices are indicated as U_1 and V_1 are also generated when SVD is applied to the cover image. In figure 1 two such systems are shown by considering same cover image but with a different watermarking. In the second case, the orthogonal matrices are assumed to be U_2 and V_2.

Zhang *et.al* shown that, the orthogonal matrix contains the most of the data as they characterize the Eigenvectors of the respective singular values [15]. In figure 2, it is shown that the decoder extracted singular values from the second watermarked image and combine them with orthogonal matrices of the first cover image (U1 and V1*)* for watermark extraction. As a consequence, the first watermark is extracted. Thus if any singular matrix is utilized along with Eigenvectors it will produce the correlated output as an alternative to the actual output. The similarity is high if the unmatched SVs will be roughly equal to the original SVs. So it gives rise to the large number of false-positives during watermark detection and also presents a security hazard.

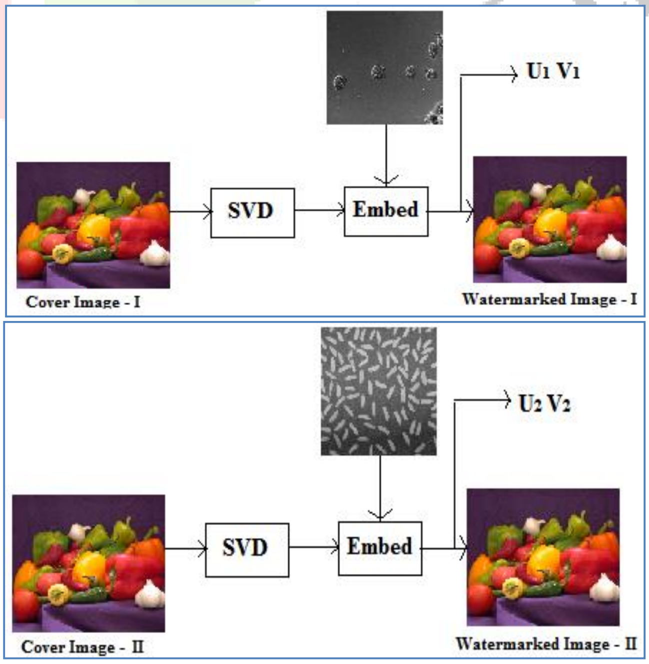

Figure 1, Embedding of a watermark.

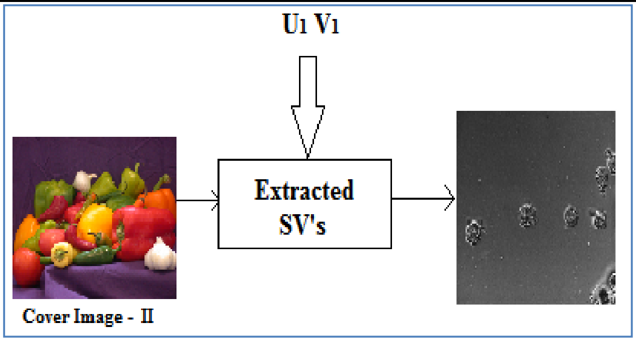

Figure 2, Extraction of a watermark.

IV. PROPOSED WATERMARKING SCHEME

In the standard SVD based watermarking schemes, if the attacker generates a sample orthogonal matrix that somehow approximates the orthogonal matrices of the cover image, then by using the Eigenvectors the watermark it can be extracted. In order to overcome the above threat in this paper a new mechanism was introduced, in which a moniker will be generated to improve the security levels to further levels. In the generation of the above-said moniker hashing function was utilized. The moniker is a unique string of 1's and 0's and random. Here the inputs for the generation of the moniker are the orthogonal matrices.

a. Moniker Generation

a. First, add the column wise number and get a 1D array.
b. By using a threshold value assign the 1D array to binary values 0's or 1's.
c. Now on performing the Exclusive-OR, the manifestation of moniker finishes.

b. Proposed authentication scheme

The moniker devised must be preserved even after the usual manipulation tasks on the image. Hence a safeguard measures must be taken so that the moniker does not lose in the manipulations. Also, the moniker is duplicated and placed at two locations. The first in the Low-Low of second level decomposition of cover image by wavelet transform designated as Low-Low4. The second in the High-High of second level decomposition of cover image by wavelet transform designated as High-High4. The procedure of embedding the moniker is given below.

Moniker Embedding:

- First, decompose the cover image wavelet transform.
- Now Decompose the Low-Low band further into Low-Low4, Low-High4, High-Low4, and High-High4.
- As the plan is to embed the moniker in two locations, select randomly, N coefficients from High-High4 and Low-Low4.
- Here, the selection may be done by a simple key or a polynomial.
- If higher order polynomial is used the robustness increases further but the embedding becomes complex.
- Now place the moniker bits in some or all of the bits of selected coefficients.
- Then, apply inverse wavelet transform.

***Moniker Extraction*:**

The extraction of the moniker from the watermarked image is crucial, because the moniker identifies the orthogonal matrices to be used as well as not to be used. The procedure of moniker extraction is as follows.

- First, decompose the received watermarked image using wavelet transform.
- Then, apply the wavelet transform on a Low-Low band as the moniker was embedded in the Low-Low4 and High-High4 of Low-Low.
- Use the key or polynomial to identify the coefficients in which the moniker bits are embedded.
- Then, extract the corresponding bits of the coefficients where the moniker bits are embedded, and form the moniker.

IV. SIMULATION RESULTS

This section is concerned with the simulation results of the proposed schemes. Figure 3 shows the carrier image and the watermark.

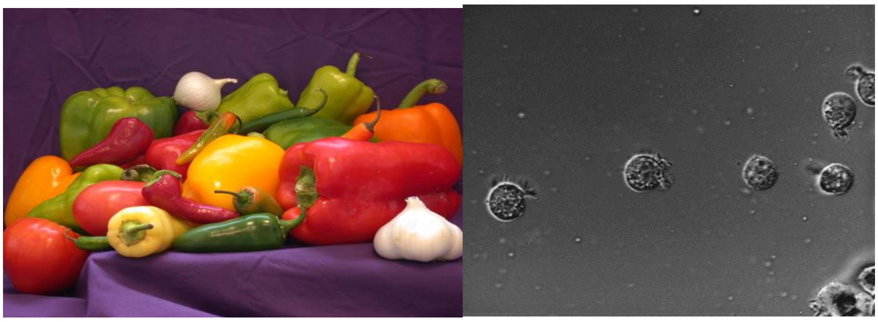

Figure 3, Carrier image and Watermark

The proposed technique is used to hide the watermark in the carrier 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 figure 4, the extracted images with different attacks are shown along with the PSNR and MSE values.

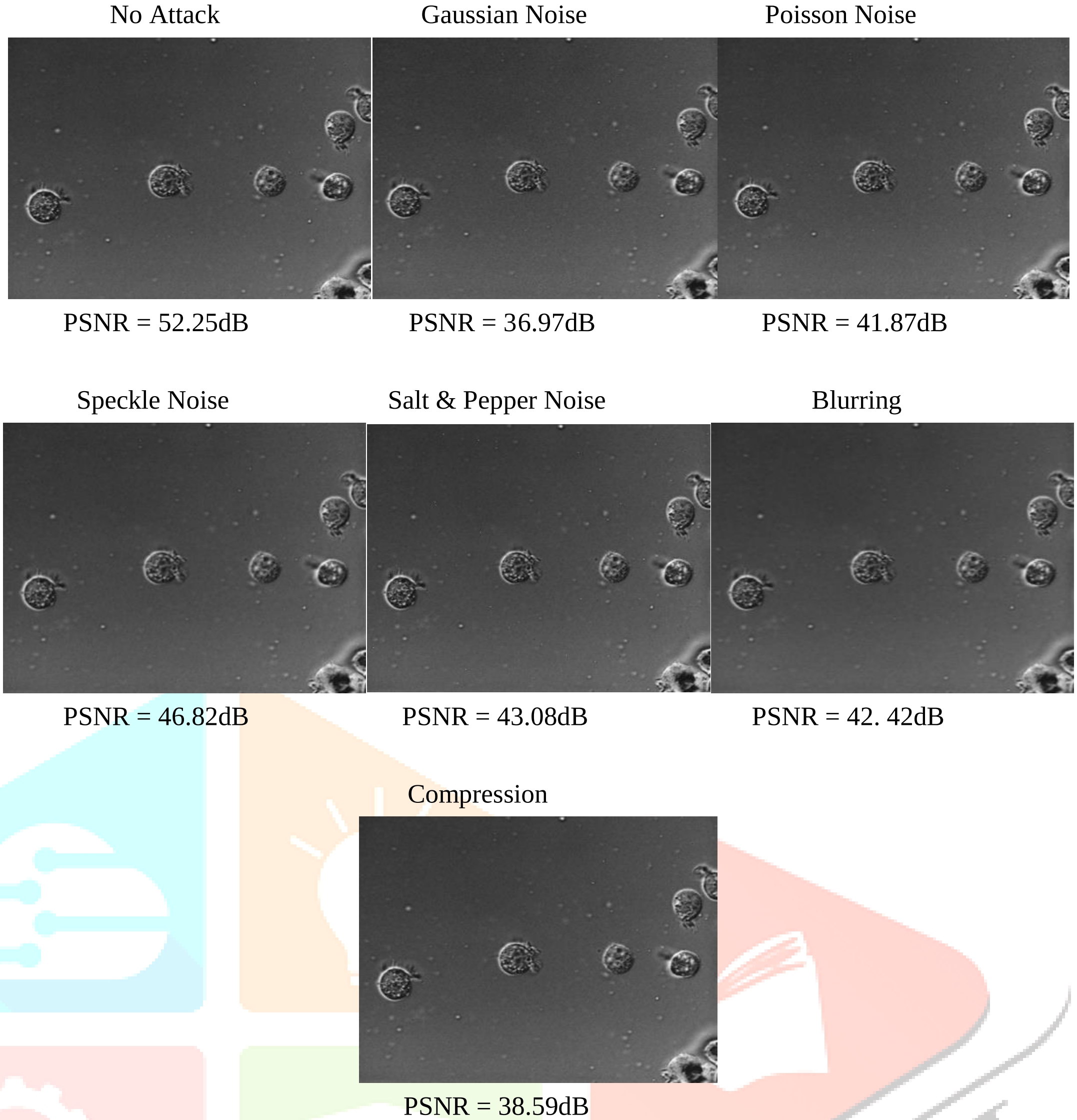

Figure 4, Output images after extraction with different attacks

V. CONCLUSIONS

The conventional SVD based watermarking schemes are popular and are used in many modern applications. The SVD based watermarking schemes calculate the singular values and unitary matrices associated with the shield image. The unitary matrices associated with the shield image will be modified in accordance with the watermark image. But when a dummy image is used to extract the watermark it associates with a fair amount of correlation with the watermark. Hence the intruders may grab the secret data. To combat the issue in the SVD based watermarking schemes, a novel scheme was proposed in this paper. In the proposed technique, a moniker will be formed using the shield image. At the time extraction, the watermarked image will be authenticated by checking the moniker. Hence unauthorized or false watermarked images are not allowed for further process in extraction. On the other hand, different attacks are considered. The simulation results with corresponding attacks are presented.

REFERENCES

[1] Siva Sankar, Dr.T. Jayachandra Prasad, Dr.M.N.Giriprasad, “LSB based Image Steganography using Polynomials and Covert Communications in Open Systems Environment for DRM”, Proc. International Conference & Workshop on Emerging trends in - Technology, ICWET-2011, Mumbai.
[2] J.O. Ruanaidhet. al., “Rotation, scale and translation invariant spread spectrum digital image watermarking,” Signal Processing, May 1998.
[3] C.-Y. Lin, et. al.," Rotation, scale and translation resilient watermarking for images," IEEE Transactions on Image Processing, May 2001.
[4] Katzenbeisser Stefan, et. al., “Information hiding techniques for steganography and digital watermarking”, Norwood, MA, Artech House, 2000.
[5] Podilchuk C I et. al., “Digital watermarking: Algorithms and applications”, *Signal Processing Magazine IEEE*, 2001.
[6] Mohammad Ali Nematollahi, S.A.R. Al-Haddad, FaranehZarafshan, “Blind digital speech watermarking based on Eigen-value quantization in DWT”, Journal of King Saud University – Computer and Information Sciences, 27, 58–67, 2015.
[7] Charu Agarwal, Anurag Mishra, Arpita Sharma, "A novel gray-scale image watermarking using hybrid Fuzzy-BPN architecture", Egyptian Informatics Journal,16, 83–102, 2015.
[8] Jose Aguilar, Juan Anderson, “A Neural Watermark Approach”, Electronic Notes in Theoretical Computer Science, 281, 35–50, 2011.
[9] MohammadRezaKeyvanpour, FarnooshMerrikh-Bayat, “An Effective chaos-based image watermarking scheme using fractal Coding”, WCIT 2010, Procedia Computer Science, 3,89–95, 2011.

[10] Li Xufang, Hu Min, "Digital Watermark Based on W-SVD Method in Copyright Protection of E-Service", 2012 International Conference on Solid State Devices and Materials Science, Physics Procedia, 25, 743 – 748, 2012.

[11] D.Vaishnavi, T.S.Subashini, "Robust and Invisible Image Watermarking in RGB Color space using SVD", International Conference on Information and Communication Technologies, Procedia Computer Science, 46, 1770 – 1777, 2015.

[12] JianhuaSonga, JianweiSongb ,YuhuaBao, "A Blind Digital Watermark Method Based on SVD and Chaos", 2012 International Workshop on Information and Electronics Engineering (IWIEE 2012), Procedia Engineering, 29,285-289, 2012.

[13] Abhilasha Sharma, Amit Kumar Singh and S P Ghrera, "Secure Hybrid Robust Watermarking Technique for Medical Images", 4th International Conference on Eco-friendly Computing and Communication Systems, ICECCS 2015, Procedia Computer Science, 70, 778 – 784.

[14] GauravBhatnagar, Q.M. Jonathan Wu, Balasubramanian Raman, "Biometric Template Security based on Watermarking", ICEBT 2010, Procedia Computer Science, 2, 227–235, 2010.

[15] WidiAstuti, Adiwijaya, "Graph Coloring Based on Evolutionary Algorithms to Support Data Hiding Scheme on Medical Images", International Conference on Graph Theory and Information Security, Procedia Computer Science, 74,173 – 177, 2015.

[16] Nidaa A. Abbas, "Image watermark detection techniques using quadtrees", Applied Computing and Informatics, 11, 102–115, 2015.

[17] Anil Kumar Shaw, SwanirbharMajumder, SouvikSarkar, Subir Kumar Sarkar, "A novel EMD based watermarking of fingerprint biometric using GEP", International Conference on Computational Intelligence: Modeling Techniques and Applications (CIMTA) 2013, Procedia Technology, 10, 172 – 183, 2013.

[18] DivjotKaurThind, Sonika Jindal, "A Semi Blind DWT-SVD Video Watermarking", International Conference on Information and Communication Technologies, Procedia Computer Science, 46, 1661 – 1667, 2015.

[19] Nisreen I. Yassin, Nancy M. Salem, Mohamed I. El Adawy, "QIM blind video watermarking scheme based on Wavelet transform and principal component analysis", Alexandria Engineering Journal, 53, 833–842, 2014.

[20] S. Anu H. Nair, P. Aruna, "Comparison of DCT, SVD and BFOA based multimodal biometric watermarking systems", Alexandria Engineering Journal, 54, 1161–1174, 2015.

[21] Lee Sin-Jooet. al., "A survey of watermarking techniques applied to multimedia", Industrial electronics *Proceedings, IEEE International Symposium*, 2001.

[22] Zhou B et. al., "A geometric distortion resilient image watermarking algorithm based on SVD", *China Journal on Image Graphics*, 2004.

[23] Ganic Emir et. al., "Robust DWT-SVDdomain image watermarking: Embedding data in all frequencies", *Proceedings of the workshop on Multimedia and Security* 2004.

[24] Zhang Xiao-Ping et. al., "Comments on-A SVD-based watermarking scheme for protecting rightful ownership", *IEEE Transactions on Multimedia*, 2005.