A Hybrid Approach for SVD and Neural Networks Based Robust Image Watermarking

Mokhtar Hussein[#1], Dr. B. Manjula [*2]
[#]*Computer Science Department - Kakatiya University*
Warangal – India.

Abstract

In the digital world, a lot of digital watermarking techniques for copyright protection of multimedia data have been proposed to avoid their misuse. Implementation of these watermarking schemes requires main focus on robustness, trustworthiness and imperceptibility. In this paper, a new SVD and Neural Network based robust image watermarking method is proposed. The proposed method is supposed to offer better quality and robustness for the image under different types of attacks and under copy move forgery attacks.

Keywords*: Digital Image Watermarking, SVD, Neural Networks.*

I. INTRODUCTION

Information technology has eased the duplication, manipulation and distribution of digital data in recent times which has resulted in the demand for safe ownership of digital images. The solution to the problem of copyright protection and content authentication is digital watermarking. However, a single watermarking method can only serve a limited number of purposes. To overcome the limitations of single watermarking, a hybrid watermarking method is a good choice. As we know that Singular value decomposition (SVD) is a very powerful numerical analysis tool used to analyze the matrices. For that, SVD of a matrix with real complex entries is considered as one of the fundamental tools of mathematics.

Along with that, Neural Network (NN) is knows as a mathematical model or computational model that is inspired by the structure and/or functional aspects of biological neural networks. A neural network consists of an interconnected group of artificial neurons, and it processes information using a connectionist approach to computation. They are usually used to model complex relationships between inputs and outputs one algorithm introduced copyright protection for images with a full counter propagation neural network. In addition, Neural Network is having the ability to learn.

All these characteristics of SVD and NN makes the useful for embedding watermark, and this type of algorithms has proven to be robust in watermarking systems. In existing methods, the watermarked image is almost the same as the original cover image. Most of attacks would degrade the quality of the extracted watermark image. A robust watermarking technique should prevent a watermark attack against geometric distortions, ensures the synchronization of watermark before and after embedding and ensures watermark resilience to common image processing attacks as well as desynchronization attacks.

Geometric attacks induce synchronization errors between the original and the extracted watermark during the detection process, which mean that the watermark still exist in the watermarked image but its positions have been changed. For that, creation and enforcement of synchronization errors correction of such frameworks is to be dealt.

In this research paper, watermark image embedding is proposed with singular value decomposition (SVD) and Neural Networks (NN) classifier method. Firstly we take the cover image and create the watermark image using fusion of SVD and probabilistic neural networks method. SVD is connected to each block. A bit of the watermark is inserted through slight alterations of the value of singular quality (SV framework in every block. The proposed method supposed to provide better image quality and more robustness under Geometrical attack (GA), Compression attack (CA), noise attack (NA), it is also supposed to offer better image quality and more robustness under Copy move forgery attacks.

Security is also the main concern of our research. Encryption is a conspicuous and secure technique to converse data into a scrambled code that can be distributed and deciphered through a private or public network. It is clear that, in both research and application fields, encryption and cryptographic algorithms serve copyright owners as an approach to protect the secure transmission of confidential multimedia data between a distributor or publisher and the purchaser of the multimedia data over public channels.

Encryption of watermark image ensures the security of watermark from unauthorized attacks. Without the key information watermark cannot be decrypted. The watermark is extracted from the possible corrupted watermarked image using the host

image, by applying the inverse procedure at each resolution level to obtain an estimate of the watermark. The estimates for each resolution level are averaged to produce an overall estimate of the watermark. Here SVD has been used along with encryption and error control coding and back propagation neural networks to enhance the performance. Till date a lot of digital watermarking techniques, for copyright protection of multimedia data, have been proposed to avoid their misuse. Implementation of these watermarking schemes requires main focus on robustness, trustworthiness and imperceptibility. In a broader sense, the embedding of watermark for any multimedia data (audio, video or image) is either in spatial or in the transform domain. In the spatial domain, embedding of watermark is implemented by directly adding it to the data in terms of any particular algorithm. It is faster than the latter, due to its simpler operations and implementation. Here SVD has been used along with encryption & error control coding and back propagation neural networks to enhance the performance. The Singular Value Decomposition (SVD) technique is a generalization of the Eigen-value decomposition, used to analyze rectangular matrices. This mathematical technique has been used in various fields of image processing. The main idea of the SVD is to decompose a rectangular matrix into three simple matrices (two orthogonal matrices and one diagonal matrix). It has been widely studied and used for watermarking by researchers for long.

When SVD is undergone on an image ($I_{M \times N}$) matrix it produces three matrices ($U_{M \times M,}$ $S_{M \times N}$ and $V_{N \times N}$). The main image characteristics are in the S. U and V contain the finer details respective to the Eigen values at S. where U is column-orthogonal matrix of size m x m , S is the diagonal matrix with positive elements of size m x n and transpose of n x n orthogonal matrix V. The important property of SVD based watermarking is that the large of the modified singular values of image will change by very small values for different types of attacks. By using any rank R, the $U_{M \times M}$ becomes $U_{M \times R}$ and $S_{M \times N}$ becomes $S_{R \times R}$ and $V_{N \times N}$ becomes $V_{N \times R}$. Their resultant operation is image $I'_{M \times N}$, where I' is the image generated from $U_{M \times R}$, $S_{R \times R}$ and $V_{N \times R}$. This I' does have approximately similar features as I for optimum value of R. Here SVD is used to hide the logo for watermarking, in its Eigen values. To improve the robustness error control coding is applied, for which the convolution encoder is used.

A long with the SVD and the error control coding scheme with encryption the next important technique employed is the back propagation algorithm based neural network. This is because among different learning algorithms, back-propagation algorithm is a widely used learning algorithms in Artificial Neural Networks. The Feed-Forward Neural Network architecture is capable of approximating most problems with high accuracy and generalization ability. This algorithms is based on the error correction learning rule. Error propagation consists of two passes through the different layers of the network, a forward pass and a backward pass. In the forward pass the input vector is applied to the sensory nodes of the network and its effect propagates through the network layer by layer. Finally a set of outputs is produced as the actual response of the network. During the forward pass the synaptic weight of the networks are all fixed. During the back pass the synaptic weights are all adjusted in accordance with an error-correction rule. The actual response of the network is subtracted from the desired response to produce an error signal. This error signal is then propagated backward through the network against the direction of synaptic conditions. The synaptic weights are adjusted to make the actual response of the network move closer to the desired response.

A robust digital image watermarking method based on neural network (NN) and adaptively identify watermarking embedding location and strength and uses trained NN to help watermarking embedding and extracting. Experimental results show that the existing method has better performance than the similar method in countering common image process, such as Jpeg compression, noise adding, filtering and so on. The fusion of Singular value decomposition and probabilistic neural networks can be used to resolve gap issues. Here SVD has been used along with error control and back propagation neural networks to enhance the performance at the cost of algorithmic complexity.

Embedding watermark on a single coefficient may not sustain robustness against attacks but group of coefficients when used for data embedding has higher probability to show robustness. Also, improvement on these watermarking schemes is required to carry variable payloads for adjustability requirement with imposed security.

Information technology has eased the duplication, manipulation and distribution of digital data in recent times which has resulted in the demand for safe ownership of digital images. The solution to the problem of copyright protection and content authentication is digital watermarking. However, a single watermarking method can only serve a limited number of purposes. As reported earlier, DWT, DCT and SVD are the popular transform domain techniques used for watermarking. To overcome the limitations of single watermarking, a hybrid watermarking method is a good choice.

In most of the research papers, once the watermarking scheme is finalized, it is applied to all test images. Since each image is different and has

certain characteristics and after embedding the watermark data by a particular watermarking scheme, its performance against a particular attack may not be similar with other image. No study is conducted to make the embedding scheme based on some image characteristics. Thus, the issue is to explore the relationship between the performance of watermarking scheme and the cover image characteristics itself.

II. PROPOSED METHOD

In our proposed method, host image and logo image analyzed and logo image is encrypted for the security concerns, which protect the image from various attacks and distortions. After that SVD (singular value decomposition) is applied to both the image and Eigen values are calculated. This process gives the 3 matrices. The whole process from analyzing images to obtaining decomposed matrices is undergone through the neural network training and then logo image is embedded to host image by watermark embedding algorithm. The neural network model consists of an input layer, more or less hidden layers as well as an output layer. Each connection connecting neurons has a distinctive weighting value. In training the network, the nodes in the neural network obtain input information from exterior sources, and then go by to hidden layer which is an interior information processing layer and is answerable for the information conversion, and then the nodes in the output layer supply the required output information. After that, the backpropagation of error is transported by distinct the actual output with wanted output. Once the network weights and biases are preliminary, the linkage is prepared for training. The preparation process necessitates a group of instances for proper network behavior, such as network inputs p and destination outputs t. For the duration of training the weights as well as biases of the network are iteratively adjusted to minimize the network performance function. The number of hidden layer is always difficult to determine in ANN creation. It is generally agreed that one hidden layer is sufficient for most of purposes.

When embedding is done once again neural network is applied for checking the watermarked image and to calculate new image values. Finally, if the watermarked image looks like the original image then the image is properly watermarked otherwise the watermark is not embedded properly. The reverse process is applied for watermark extraction.

III. WATERMARK EMBEDDING ALGORITHM

The prerequisites for image watermarking are the subjective watermark (logo image) and the host image for data concealment. After generation of encrypted or compressed version of watermark, it is passed through the decomposition process for singular value decomposition (SVD). The SVD of host image as well as watermark is performed to obtain the matrices U, S, and V. The S matrix consisting of the diagonal values is converted to one dimension via zig zag scan, done in order to add the logo near the most significant Eigen values. This leads to a matrix S *. Since the number of bits in S is greater than that of the logo, number of bits in S* is same as that of S.

The following algorithm explains each step in detail:

1) Read the Host image of size N x N.
2) Read the watermark.

Apply neural network to train

3) Analyze the host image for any distortion or for presence of already embedded watermark.
4) Apply Encryption on logo image to protect the logo from various attacks.
5) Applying SVD to host image and the watermark image.
6) Obtain 3 matrices U*, S*, and V T for both the images by calculating Eigen Values.
7) The cover image and watermark are then supplied to the input layer of probabilistic neural network, followed by training the network to produce watermarked image and desired watermark at the output layer. In this step through the trained neural network reconstruction of the watermarked image is done.
8) Verifying the quality of resultant watermarked image to check the authenticity of embedding process. Find the difference between input values and trained values. The resultant values are accepted as watermark.

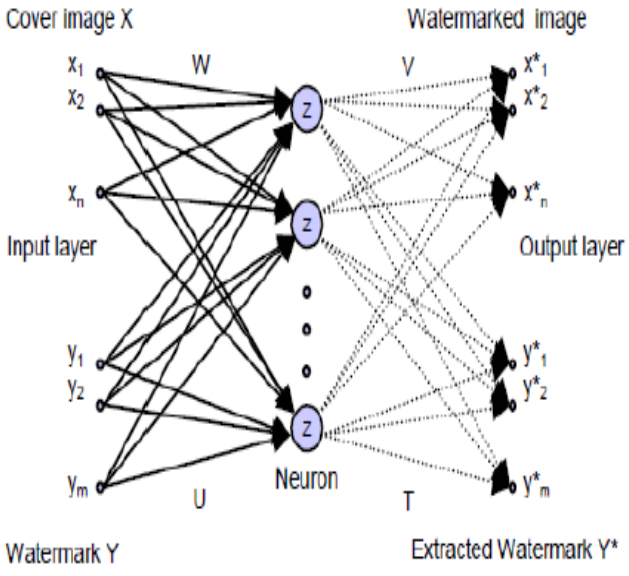

Figure 1 Image watermarking through neural network

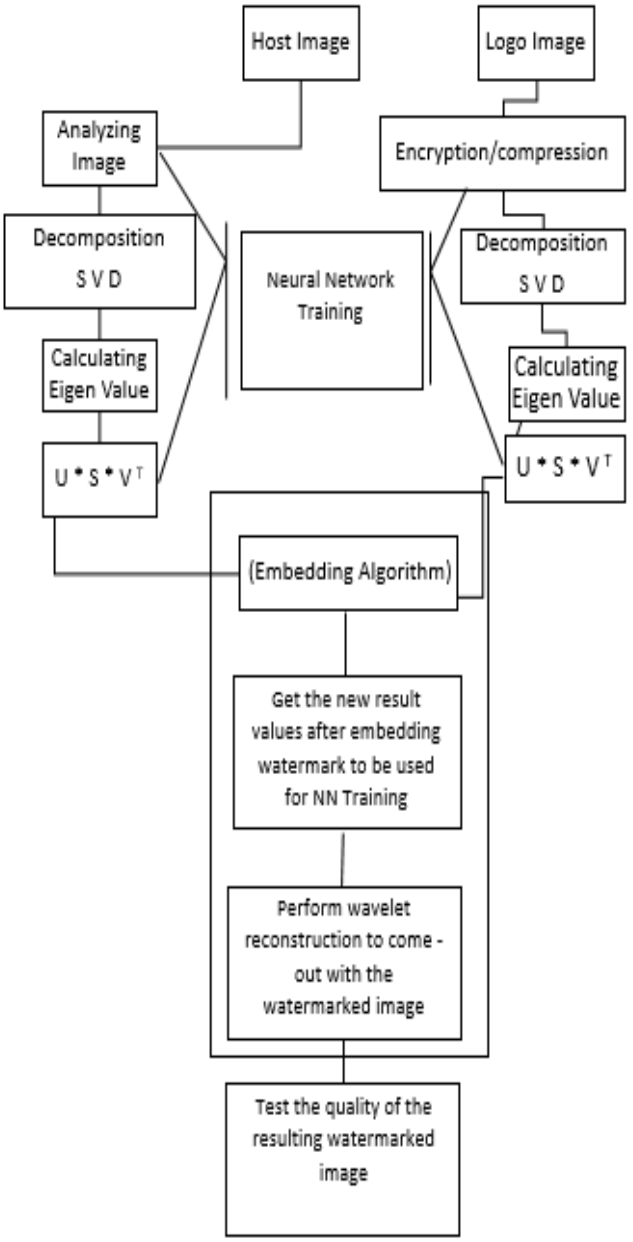

Figure 2 Watermark Embedding using SVD and Neural Network

IV. WATERMARK EXTRACTION ALGORITHM

The owner of the watermarked image should have the authenticity whenever the image gets duplicated without his consent. The author should retrieve the watermark from the watermarked image which has undergone the image processing techniques.

The detection of the watermarked logo from the host image is just the opposite of the embedding method. This is of non-oblivious type, where the host image I'W (due to malicious attacks IW turns to I'W) is received instead of IW. Therefore, SVD is applied on the key image IK to obtain to obtain U1, S1 and V1 and the distorted watermarked image I'W to obtain U2, S2 and V2.

Watermark Extraction algorithm steps are explained in detail as follows:

1) Read the watermarked image.
2) Perform the SVD on watermarked image, as well as on key image.
3) Compare the Eigen values extracted from both the images, identify distortions and errors.
   Apply neural network to train
4) Apply the watermark extraction Algorithm for detecting and extracting watermark from the host image.
5) Apply the decryption on the watermark image to obtain original logo, if not attacked the image, returns the similar watermark as it is embedded.
6) Reconstructing the watermark image by applying neural network.
7) Verifying the quality of watermark image for proving that image has not attacked by the malicious user.

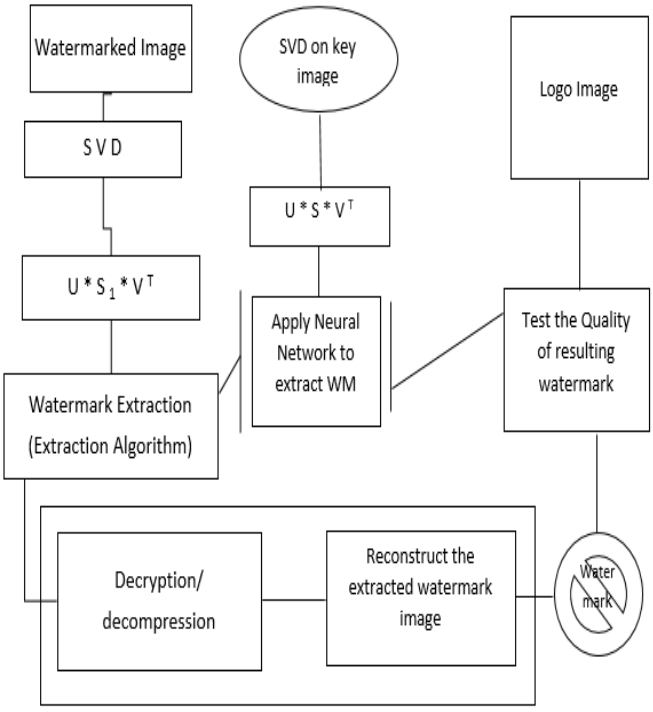

Figure 3 Watermark Extraction using SVD and Neural Network

V. CONCLUSION

In this paper, we assumed a new SVD and Neural network which supposed to offer better quality and robustness for the image.

In extraction panel, watermarked image is uploaded nad neural network is applied to obtain extracted watermark. A parameter evaluation will be done using PSNR, MSE, BCR, BER and NCC. These parameters are used to check the quality of the

watermarked image. Different attacks must be applied on the watermarked image to check the robustness. The proposed scheme is should be implemented in MATLAB. Verification on the receiver's side, the same robust bits extraction and watermark detection methods are performed and the image is considered as integrity. Block based verification techniques can also be used which reduces the burden of the network.

REFERENCES

[1] Potdar, Vidyasagar M., Song Han, and Elizabeth Chang. "A survey of digital image watermarking techniques. "In Industrial Informatics, 2005.INDIN'05.2005 3rd IEEE International Conference on, pp. 709-716. IEEE, 2005.

[2] C-S. Lu, S-K. Huang, C-J. Sze and H-Y. Liao A new watermarking technique for multimedia protection, Multimedia Image and Video Processing (2001) pp. 507{530}.

[3] Chen Yongqinang, Zhang Yanqing, and Peng Lihua, ― A DWT Domain Image Watermarking Scheme Using Genetic Algorithm and Synergetic Neural Network‖, Academy Publisher, pp. 298- 301, 2009.

[4] heng-Ri Piao, Seunghwa Beack, Dong-Min Woo, and SeungSoo Han, ― A Blind Watermarking algorithm Based on HVS and RBF Neural Network for Digital Image‖, Springer-Verlag Berlin Heidellberg, pp. 493-496, 2006.

[5] S. Bounkong, B. Toch, David Saad, David Lowe, ― ICA for Watermarking Digital Images‖, Journal of Machine Learning Research 4 (2003) 1471-1498.

[6] Huo-Chong L, Raphael C, Phan W, Swee-Huay H (2011) On an optimal robust digital image watermarking based on SVD using differential evolution algorithm. Opt Commun 284:4458– 4459.

[7] Chen Yongqinang, Zhang Yanqing, and Peng Lihua, ― A DWT Domain Image Watermarking Scheme Using Genetic Algorithm and Synergetic Neural Network ‖ , Academy Publisher, pp. 298- 301, 2009.

[8] Quan, L.; Jiang, X.: Design and Realization of a Meaningful Digital Watermarking Algorithm Based on RBF Neural Network. Proceedings of the Sixth World Congress on Intelligent Control and Automation, WCICA. vol. 1, pp. 2878 2881, 2006.

[9] Mohamad Vafaei, and Homayoun Mahdavi-Nasab, ―A Novel Digital Watermarking Scheme Using Neural Networks with Tamper Detection Capability, ‖, J. Basic. Appl. Sci. Res., 3(4)577-587, 2013.

[10] Hieu V. Dang and Witold Kinsner, ‖An intelligent digital color image watermarking approach based on wavelet transform and general regression neural network,‖ in Proc. of the 11th IEEE Intern. Conf. on Cognitive Informatics and Cognitive Computing, ICCI*CC 2012, (Kyoto, Japan; August 22-24, 2012), pp. 115-123, 2012.

[11] Zhang G, Patuwo BE, Hu MY (1998) Forecasting with artificial neural networks: the state of the art. Int J Forecast 14:35–62.

[12] Akram Zeki, Adamu Abubakar and Haruna Chiroma, ―An intermediate significant bit (ISB) watermarking technique using neural networks‖, SpringerPlus (2016) 5:868 DOI 10.1186/s40064-016-2371-6.

[13] Abdullatif M, Zeki AM, Chebil J, Gunawan TS. Properties of digital image watermarking. In: IEEE 2013 Signal Processing and Its Applications, 9th International Colloquium; 8–10 March 2013; Kuala Lumpur, Malaysia. New York, NY, USA: IEEE. pp. 235-240.

[14] Singh YS, Devi BP, Singh KM. A review of different techniques on digital image watermarking scheme. Int J Eng Res 2013; 2: 193-199.

[15] Nguyen TH, Duong DM, Duong DA. Robust and high capacity watermarking for image based on DWT-SVD. In: IEEE RIVF 2015 Computing & Communication Technologies-Research, Innovation and Vision for Future International Conference; 25–28 January 2015; Can Tho, Vietnam. New York, NY, USA: IEEE. pp. 83-88.

[16] Lagzian S, Soryani M, Fathy M. A new robust watermarking scheme based on RDWT-SVD. Int J Intell Inform Process 2011; 2: 27-35.

[17] Radouane M, Boujiha T, Messoussi R, Touahni R. A robust method for digital image watermarking based on combination of SVD, DWT and DCT using optimal block. J Theor Appl Inform Technol 2014; 59: 297-303.

[18] Lou DC, Liu JL, Hu MC. Adaptive digital watermarking using neural network technique. In: IEEE 2003 Security Technology Proceedings of the 37th Annual International Carnahan Conference; 14–16 October 2003; Taipei, Taiwan. New York, NY, USA: IEEE. pp. 325-332.

[19] Aslantas V. A singular-value decomposition-based image watermarking using genetic algorithm. Int J Elec Commun 2008; 62: 386-394.

[20] Mokhtar Hussein, Manjula, " A Survey Study on Singular Value Decomposition and Genetic Algorithm Based on Digital Watermarking Techniques", Proceedings of the First International Conference on Computational Intelligence and Informatics pp 7-16. vol 507. Springer, Singapore