Secure Data for Digital Image Watermarking Using DWT and SVD Technique

Richa Kumari[1], Prof. Rakesh Kumar Verma[2]

[1]*M. Tech. Scholar,* [2]*Assistant Professor*

[12]*Department of Computer Science and Engineering, IES Collage, Bhopal*

Abstract—In order to improve the robustness and imperceptibleness of the algorithm, a new embedding and extracting method with DWT-SVD is proposed. The approximation matrix of the third level of image in DWT domain is modified with SVD to embed the singular value of watermark to the singular value of DWT coefficient. The proposed embedding and extracting method was employed to accelerate the hybrid DWT-SVD watermarking and to avoid the leak of watermark. This hybrid technique leads to optimize both the fundamentally conflicting requirements. The experimental results show both the good robustness under numerous attacks and the high fidelity. The time needed to perform the program is greatly decreased.

Keywords— Discrete Wavelet Transform, SVD, PSNR, MSE.

I. INTRODUCTION

In the recent few years, there is a serious problem about unauthorized and illegal access and manipulation of multimedia files over internet. Everybody can obtain copies of copyrighted multimedia openly. So we need to generate a robust method in order to protect the copy rights of media. Digital watermarking provides copyright protection of data. It is done by embedding additional information called digital signature or watermark into the digital contents such that it can be detected, extracted later to make an assertion about the multimedia data. [1, 2] For image watermarking, the algorithms can be categorized into one of the two domains: spatial domain or transform domain. [1, 2] In Spatial domain the data is embedded directly by modifying pixel values of the host image, while transform domain schemes embed data by modifying transform domain coefficients. Algorithms used for special domain are less robust for various attacks as the changes are made at least Significant Substitution (LSB) of original data. While in the transform-domain the watermark is embedded by changing the magnitude of coefficients in a transform domain with the help of discrete cosine transform, discrete wavelet transform (DWT), and singular value decomposition (SVD) techniques[3, 5]. This provide most robust algorithm for many common attacks. [7] In this paper we proposed a hybrid watermarking using DWT and SVD technique in order to achieve high robustness and transparency.

Therefore we decided to design watermarking schemes such that an inherent nature in can be embedded to guarantee that at least one serious attack having most financial implications cannot be conducted on watermarked images**.** If owner identification applications place the same watermark in all copies of the same content, then it may create a problem. If out of n number of legal buyer of content, one starts to sell the contents illegally, it may be very difficult to know who is redistributing the contents without permission. Allowing each copy distributed to be customized for each legal recipient can solve this problem. This capability allows a unique watermark to be embedded in each individual copy.

This particular application area is known as fingerprinting and thus has numerous financial implications. The most serious attack for fingerprinting is the “collusion attack”. If attacker has access to more than one copy of watermarked image, he/she can predict/ remove the watermark data by colluding them. Researchers working on “fingerprinting” primarily focus on the “collusion attack”.

So, while designing a watermark scheme, we decided that our proposed schemes must be designed in such a way that schemes are inherently collusion attack resistant. Therefore this thesis presents a new term “ICAR (Inherently Collusion Attack Resistant)” as a requirement for a watermarking system. The other 3 issues are taken into account while developing the watermarking schemes.

The first chapter is devoted to the introduction of the watermarking area. Data hiding background is represented and the related terminologies are explained. Then various application areas of watermarking are represented and what may the key requirements of a successful watermarking system are discussed. Since watermarking can be classified on various parameters, the various types of watermarking are represented based on different classifications.

ISSUE 1: Till now there is no “Generic” nature in the watermarking algorithms available. More precisely, if certain approach is applicable for a gray level image, the

same approach does not work for the other formats of an image.

ISSUE 2: Even if gray color image watermarking algorithms are extended for RGB color images, the maximum work has been done for BLUE color channel only because human eyes are less sensitive to detect the changes in BLUE color channel. No attack impact analysis, i.e, which color channel may be affected by a particular attack, has been carried out.

Therefore, apart from choosing digital Image Watermarking as a major problem, we have chosen to identify the suitability of a color channel with respect to attack (if any) for multicolor channel images (True color windows BMP, uncompressed JPEG). We also decided to explore the ways such that attack impacts may be minimized before the watermark embedding process**.**

ISSUE 3: 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.

II. LITERATURE REVIEW

Senthil Kumaran et al. [1], Image security is a relatively very young and fast growing. Security of data or information is very important now a day in this world. In this paper proposed to advantages and that working functionalities. This algorithm is verified on different watermarking images. And it's providing robust and secure results. To measure the effectiveness of this algorithm is provide embedding and extracting images. PSNR and MSE also calculated the embedding watermarking images. In this DWT watermarking embedding result images provide the good, secure and robust. In this paper proposed to how to process LSB technique.

Aase et al. [2] briefly discussed the issue of watermarking digital images as part of a general survey on cryptography and digital television. The authors provided a description of a procedure to insert a watermark into the least significant bits of pixels located in the vicinity of image contours. Since it relies on modifications of the least significant bits, the watermark is easily destroyed. Further, their method is restricted to images, in that it seeks to insert the watermark into image regions that lie on the edge of contours.

Ahmed et al. [3] described a method that adds or subtracts small random quantities from each pixel. Addition or subtraction is determined by comparing a binary mask of bits with the LSB of each pixel. If the LSB is equal to the corresponding mask bit, then the random quantity is added, otherwise it is subtracted. The watermark is subtracted by first computing the difference between the original and watermarked images and then by examining the sign of the difference, pixel by pixel, to determine if it corresponds to the original sequence of additions and subtractions. This method does not make use of perceptual relevance, but it is proposed that the high frequency noise be pre-filtered to provide some robustness to low-pass filtering. This scheme does not consider the problem of collusion attacks.

Akhaee et al. [4], digital watermarking has been investigated deeply for its technical and commercial feasibility in all media types like, digital photographic image, printed materials or document images and video. It is a proven method for reducing content piracy and improving the ability to identify, tract and manage digital media. It is widely used in applications like rights management, remote triggering, filtering/classification and e-commerce. It is a technique that is used to balance the need for content security with best possible consumer experience to enable media and entertainment industries to adapt the advanced facilities of the modern digital revolution while reducing the threat of content theft.

Ali et al. [5], proposed two schemes where the first was fragile watermarking and was used to authenticate the digital content, while the second was used to reconstruct the region where the integrity verification fails.

The watermark embedding procedure even though efficient reduced the quality of the reconstructed image when the strength of attack was increased. Different decomposition levels grant the tamper detection within the image in localized spatial and frequency domain. The aim is to present an authentication technique that hides watermark into some wavelet sub-bands of the to-be-authenticated image. This scheme is capable of detecting malicious and incidental manipulations. Furthermore, security is of particular concern that is often overlooked. It is extremely difficult for an attacker to create a faked image that appears to be authentic.

III. DIGITAL WATERMARKING

The information to be embedded in a signal is called a digital watermark, although in some contexts the phrase digital watermark means the difference between the watermarked signal and the cover signal. The signal where the watermark is to be embedded is called the *host* signal. A watermarking system is usually divided into three distinct steps, embedding, attack, and detection. In embedding, an algorithm accepts the host and the data to be embedded, and produces a watermarked signal.

Then the watermarked digital signal is transmitted or stored, usually transmitted to another person. If this person

makes a modification, this is called an attack. While the modification may not be malicious, the term attack arises from copyright protection application, where third parties may attempt to remove the digital watermark through modification. There are many possible modifications, for example, lossy compression of the data (in which resolution is diminished), cropping an image or video, or intentionally adding noise.

Detection (often called extraction) is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If the signal was unmodified during transmission, then the watermark still is present and it may be extracted. In robust digital watermarking applications, the extraction algorithm should be able to produce the watermark correctly, even if the modifications were strong. In fragile digital watermarking, the extraction algorithm should fail if any change is made to the signal.

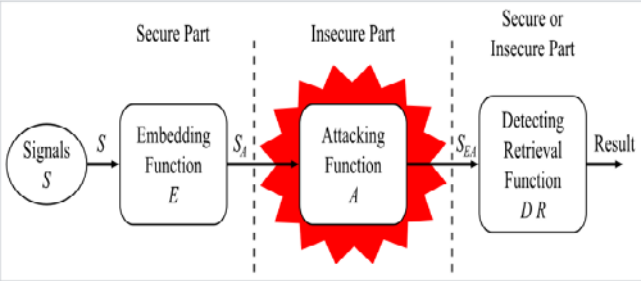

Figure 1: General digital watermark life-cycle phases with embedding-, attacking-, and detection and retrieval functions

IV. DISCRETE WAVELET TRANSFORM

The model used in [5] to implement the tree structure of Direct Wavelet Transform (DWT) is based on the filtering process. Figure 1 depicted a complete 3-level Direct WT. In this figure G and H is the high pass and low pass filter respectively.

Computation period is the number of the input cycles for one time produces output samples. In general, the computation period is M= for a j-level DWT. The period of the 3-level computation is 8. Figure 1, The Sub band Coding Algorithm As an example, suppose that the original signal X[n] has N- sample points, spanning a frequency band of zero to π rad/s. At the first decomposition level, the signal passed through the high pass and low pass filters, followed by subsampling by 2. The output of the high pass filter has N/2- sample points (hence half the time resolution) but it only spans the frequencies □/2 to □ rad/s (hence double the frequency resolution).

The output of the low-pass filer also has N/2- sample points, but it spans the other half of the frequency band, frequencies from 0 to □/2 rad/s. Again low and high pass filters for further decomposition. The output of the second low pass filter followed by sub sampling has N/4 samples spanning a frequency band of 0 to □/4 rad/s, a the output of the second high pass filter followed by sub sampling has N/4 samples spanning a frequency band of □/4 to □/2 rad/s. The second high pass filtered signal constitutes the second level of DWT coefficients. This signal has half the time resolution, but twice the frequency resolution of the first level signal. This process continues until two samples are left. For this specific example there would be 3 levels of decomposition, each having half the number of samples of the previous level.

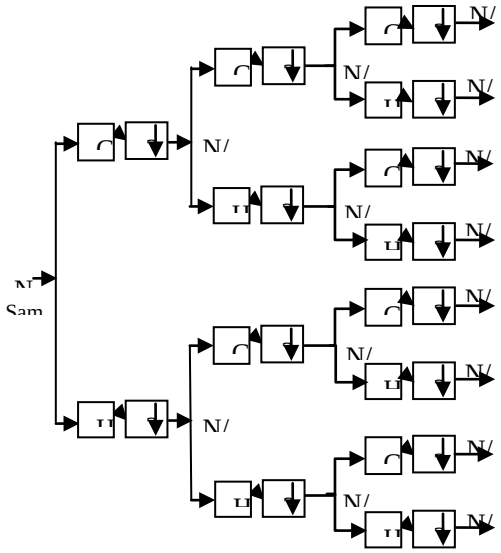

Figure 2: 3- Levels for DWT.
Where G, H are the high-pass and

The DWPT of the original signal is then obtained by concatenating all coefficients starting from the last level of decomposition (remaining two samples, in this case). The DWT will then have the same number of coefficients as the original signal.

V. PROPOSED METHODOLOGY

DWT involves decomposition of image into frequency channel of constant bandwidth. This causes the similarity of available decomposition at every level. DWT is implemented as multistage transformation. Level wise decomposition is done in multistage transformation.

S is a diagonal matrix of singular values in decreasing order. The basic idea behind SVD technique of watermarking is to find SVD of image and the altering the singular value to embed the watermark. In Digital watermarking schemes, SVD is used due to its main properties:

1) A s mall agitation added in the image, does not cause large variation in its singular values.

2) 2) The singular value represents intrinsic algebraic image properties. [3]

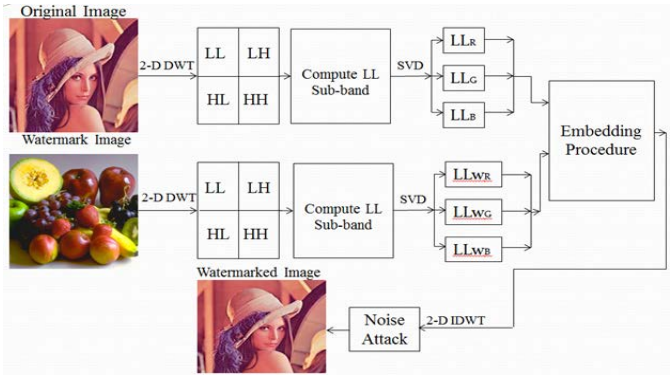

Figure 3: Flow Chart of Proposed Methodology

VI. CONCLUSION

In this paper DWT is proposed to overcome the drawback of DWT-SVD based watermarking scheme. The redundancy in the DWT provides the robustness to the watermarked image. As the embedding of watermark image occurs in all sub-bands, more information can be transferred and principal components help to avoid the false positive problem. Thus the proposed scheme can satisfy the capacity, robustness and imperceptibility.

REFRENCES

[1] N. Senthil Kumaran, and S. Abinaya, "Comparison Analysis of Digital Image Watermarking using DWT and LSB Technique", International Conference on Communication and Signal Processing, April 6-8, 2016, India.

[2] Aase, S.O., Husoy, J.H. and Waldemar, "A Critique of SVD-Based Image Coding Systems", IEEE International Symposium on Circuits and Systems VLSI, Orlando, FL, Vol. 4, pp. 13-16, 2014.

[3] Ahmed, F. and Moskowitz, I.S., "Composite Signature Based Watermarking for Fingerprint Authentication", ACM Multimedia and Security Workshop, New York, pp.1-8, 2014.

[4] Akhaee, M.A., Sahraeian, S.M.E. and Jin, C., "Blind Image Watermarking Using a Sample Projection Approach", IEEE Transactions on Information Forensics and Security, Vol. 6, Issue 3, pp.883-893, 2013.

[5] Ali, J.M.H. and Hassanien, A.E., "An Iris Recognition System to Enhance E-security Environment Based on Wavelet Theory", Advanced Modeling and Optimization, Vol. 5, No. 2, pp. 93-104, 2012.

[6] Al-Otum, H.M. and Samara, N.A., "A robust blind color image watermarking based on wavelet-tree bit host difference selection", Signal Processing, Vol. 90, Issue 8, pp. 2498-2512, 2009.

[7] Ateniese, G., Blundo, C., De Santis, A. and Stinson, D.R., "Visual cryptography for general access structures, Information Computation", Vol. 129, Pp. 86-106, 1996.

[8] Baaziz, N., Zheng, D. and Wang, D., "Image quality assessment based on multiple watermarking approach", IEEE 13th International Workshop on Multimedia Signal Processing (MMSP), Hangzhou, Pp.1-5, 2011.

[9] Bao, F., Deng, R., Deing, X. and Yang, Y., "Private Query on Encrypted Data in Multi-User Settings", Proceedings of 4th International Conference on Information Security Practice and Experience (ISPEC 2008), Pp. 71-85, 2008.

[10] Barni, M. and Bartolini, F., "Watermarking systems engineering: Enabling digital assets security and other application", Signal processing and communications series, Marcel Dekker Inc., New York 2004.

[11] Barni, M., Bartolini, F. and Piva, A. "Improved Wavelet based Watermarking through Pixel-Wise Masking", IEEE Transactions on Image Processing, Vol. 10, Pp. 783-791, 2004.