

Comparative Analysis of Non Blind DWT Based Multiplicative SVD Watermarking Algorithm with Additive Approach

Pawan Singh Shekhawat

Assistant Professor

Maharishi Arvind Institute of Engineering & Technology, Jaipur

Corresponding author's email id: shekhawatpawansingh@gmail.com

Abstract

Watermarking technology insert ownership information in suitable form inside any media like audio, video, image etc, so that owner of the object will claim his/her ownership when anyone claims his/her false ownership on that object. Proposed work, proposes a new algorithm for watermark insertion and extraction named as “Non Blind DWT Based Multiplicative SVD Watermarking algorithm” which is new version of the algorithm proposed by Bhargava [8] in his paper “Digital Image Authentication System Based on Digital Watermarking” .In this paper he is utilizing additive approach for watermark embedding and extraction algorithm and proposed algorithm utilize the multiplicative approach also he embeds watermark in one sub-band i.e. approximation sub-band and proposed algorithm utilize all four sub-bands for watermark embedding.

Keywords: Watermark, Non-Blind, SVD, Multiplicative, Additive, Embedding, Extraction, hentication.

INTRODUCTION

Media objects like Images, audios or videos or any object which is present on the internet can be copied and stored easily in this internet world. So, for preventing this type of illegal copying and distribution of media objects we need copy right

protection rule and regulation with a method for proving the belongingness of the object.

LITERATURE SURVEY

A survey on the history of watermark is done by reading various research paper

and various articles on the watermark, after reading all that the main points about watermarking history are shown below.:

- i. Oldest watermarked paper found in archives dates back to 1292, in Fabriano, Italy. Watermarks were made by adding thin wire patterns to the paper molds. These paper would be slightly thinner where the wire was and hence more transparent [1].
- ii. At the end of 13th century about 40 paper mills were sharing the paper market in Fabriano and producing paper with different format, quality and price [2].
- iii. Digital Watermarking became famous only in the early of 1990 the idea of digital watermarking. This was due to the growth of the Internet.
- iv. Digital watermarking first publication year is 1993, when Tirkel et al 1993 presented technique to hide data in image [4]. The method based on modification to the least significant bit (LSB) of the pixel values. Since then worldwide research activities have been increasing in digital watermarking [1].

- v. Zhang [3] explained the importance of digital watermarking in comparison of other technology in three important aspects: First importance is that, the watermarks and the host image in which they are embedded in are inseparable, Even if the watermarked image converted into other file formats, the watermarks will not be removed. Second importance says that encryption degrade the visibility aspect of secured image i.e. it is not imperceptible but, watermark is imperceptible i.e. the quality of watermarked image not degraded visibly. Last one is, the watermarks will have exactly the same transformation experience as the host image have, that means you can get the information about transformation technique by looking at the watermarks [3].

WATERMARKING PROCESS

Process for Digital Watermarking has two parts. In first part the watermark is embedded in the host image for embedding identity of owner in the any one form, from these four i.e. image, text, audio, video and in second part the embedded watermark is extracted back from the watermarked image as a proof of the identity of the owner.

Complete digital watermarking system will work in two basic modules as shown in Figure 1 and 2:-

1. Watermark embedding process:-

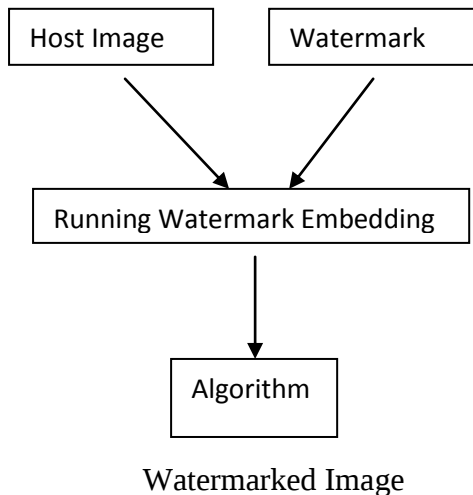


Figure 1 Watermark embedding process

Figure 1 explains the watermark embedding process in which host image is embedded with the watermark of any form of data, such as numeric, text, and image. Sometimes key is also used with the watermark embedding which is not shown in the diagram.

2. Watermark detection and extraction process:-

Watermark detection and extraction process is used to examine whether the host image contains the embedded watermark or the watermark can be extractable or not. In extraction process, inputs are watermarked data and output of extraction process is a watermark or some

kind of credibility value. The watermark detection and extraction process is as shown in Figure 2 [7].

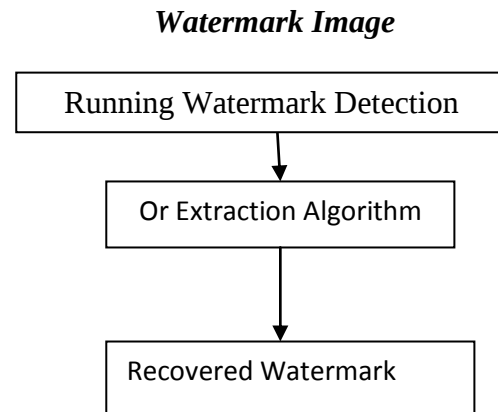


Figure 2 Watermark detection and extraction process

WATERMARKING RESEARCH DIRECTION

Research in watermarking nowadays is achieving new heights and for researching in digital watermarking we have to choose a particular research direction from various research directions as explained below :-

Research Directions of Watermarking

To propose some research in the digital watermarking field, a researcher must be aware of four research directions from which a scholar/researcher can perform his/her research work as shown below:

Study on Evaluation System of Watermarking Technology

Most of the watermarking system evaluation are empirical, so it is necessary to improve the theoretical evaluation system of watermarking technology, establish the watermark testing and evaluation standards, and design an evaluation system for fair comparison and evaluation of various watermarking algorithms [3].

Study on Watermark Attack

The relationship between watermark attack and watermarking algorithm is the same as spear and shield; they restrict each other and promote each other as well. To develop the technologies combined with cryptography, authentication and digital signature is probably the direction of resistance development to various attacks [3].

Study on Watermarking Theory

The lack of standards, interoperability problems, as well as a suit of accurate and realistic requirements to watermarking system, is still hindering the development of digital watermarking technology. Although there are many published articles on watermarking, the current watermarking technology can't yet fill the actual requirements of most users. There

are still many problems to be resolved. In order to be more widely used, digital watermarking should establish a series of standards or agreements, such as the standards of watermark embedding, detection and certification. Different watermarking algorithm has different compatibility, and that is obviously not conducive to promoting the application of digital watermarking [3].

Study on Watermarking Algorithm

Digital watermarking technology processing contains two cores: watermark embedding algorithm and detection algorithm. Robustness, imperceptibility, invisibility and security of digital watermarking are generally the focus of the requirements [3].

Decision: We selected proposed research direction as —Study on Watermarking Algorithm where the proposed work will try to develop and improve a watermarking algorithm for watermark embedding and extraction.

PREVIOUS WORK

During literature survey we found a research paper by Bhargava [8] in which a algorithm proposed by Bhargava[8] in his paper named as —Digital Image

Authentication System Based on Digital Watermarking.

In this paper he is utilizing additive approach for watermark embedding and extraction algorithm and also he embeds watermark in one sub-band i.e. approximation sub-band.

Bhargava algorithm for digital watermark embedding and extraction:-

1. Watermarking domain: Frequency Transform Domain.
2. Host image Decomposition Technique:
 - Discrete Wavelet Transformation with one level of decomposition of the host image. In this algorithm the red component of the host image is separated from RGB and only this red component is watermarked with the watermark data.
3. Host image sub-band selection: - Only Approximation sub-band selected for embedding the watermarked data
4. Watermark Selection: - An image with some predefined text is utilized as watermark.
5. Watermark weight assigning: - Weight is assigned in such a way such that the

watermark is visible after embedding the watermark as shown in the paper.

6. Watermark Embedding Strategy: - In this algorithm additive embedding strategy is utilized for watermark embedding inside the host image.
7. Watermark extraction: - Non blind method is utilized for extraction of the watermark
8. Attack Analysis: - No attack analysis is performed on the watermarked image as shown in the paper.
9. Measuring Terms utilized for evaluation: - PSNR value, SNR value and Correlation coefficient are calculated for evaluation of the algorithm robustness.

After surveying and analyzing all the aspect of Bhargava watermark embedding and extraction algorithm. We decided to improve this algorithm in some best way by doing various experiment and research on it.

PROPOSED ALGORITHM

Previous Algorithm

Bhargava [8] had Implemented Digital Watermarking using discrete 2-D wavelet

transform and Input image is watermarked with single value decomposition of the from RGB i.e. only red component is chosen for watermark data embedding using additive embedding rule and extraction of the watermark is Non Blind. Up to my best knowledge this algorithm is available for embedding and extraction of the watermark and can be improved for, attack analysis for proving the robustness and imperceptibility algorithm.

Also we can improve it by applying multiplicative embedding rule and embedding the watermark in all sub-bands to the single component of the RGB.

Proposed Watermark embedding algorithm Embedding algorithm is described as follows:-

- 1) Original Image to be watermarked is read from source and stored in an array using Matlab.
- 2) Single Value Decomposition: RGB components are broken down in individual form and then only red component of the original image is selected for watermarking.
- 3) Image transformation:- Red component of the image is transformed into signals by utilizing 2D Discrete Wavelet Transform for image

decomposition up to level 1 utilising the haar wavelet filter.

- 4) Choosing the Watermark:- Image is used as a watermark, where ownership information is written as text message. Image used for watermarking is read from source and stored in an array.
- 5) Weight of Watermark is assigned:- In Proposed algorithm the weight of the watermark is adjusted such that the watermark is invisible after embedding.
- 6) Coefficient Selection:-All four sub-bands are selected for the inserting the watermark data to the single component of RGB separated for watermarking.
- 7) Embedding rule:-Multiplicative embedding is utilized for watermark embedding as shown in the below formula [9]:-

$$Y = y.(1 + c.*I)$$

Y= watermarked image

y=original image

c= weight of watermark

I=watermark

8) Watermarked image display:- The red component signal embedded with the watermark applied with 2D Inverse Discrete Wavelet transformation to reconstruct the image decomposed and embedded with watermark by DWT .

Watermark weight is chosen in such a way such that it gives robustness to the watermarked data and also does not degrade the signal (data) quality. Table 1 shows the test image watermark and watermarked image.

1) Single Value Decomposition of original image: RGB components of original image are broken down in individual form and then only red component of the original image is separated.

2) Decompose the red component of the original image utilizing the 2D Discrete Wavelet Transformation utilizing the Haar wavelet filter and assign the decomposed image a 2x 2 matrix as shown below:-

3) $z=[ca \ ch \ ; \ cv \ cd];$

$z= 2 \times 2$ matrix for the level 1 sub-bands of red component of original image decomposed by DWT.

ca = Approximate sub-band of decomposed red component of original image.

ch = Horizontal sub-band of decomposed red component of original image.

cv = Vertical sub-band of decomposed red component of original image.

cd = Diagonal sub-band of decomposed red component of original image.

4) Input the original watermark image:-
The original watermark image utilized for the watermarking the original image is read from source and stored in an array.

5) Input the watermarked image: - The watermarked image is read from source and stored in an array.

6) Single Value Decomposition of watermarked image: RGB components of watermarked image are broken down in individual form and then only red component of the watermarked image is separated.

7) Decompose the separated red component of the watermarked image with 2D Discrete Wavelet Transformation utilizing the Haar wavelet filter and assign the

decomposed image a 2x 2 matrix as shown below:-

$$f=[w_a \ w_h ; w_v \ w_d];$$

f = 2x2 matrix for the level 1 sub-bands of red component of watermarked image decomposed by DWT.

w_a =Approximate sub-band of decomposed red component of watermarked image.

w_h = Horizontal sub-band of decomposed red component of watermarked image.

w_v =Vertical sub-band of decomposed red component of watermarked image.

w_d = Diagonal sub-band of decomposed red component of watermarked image.

8) Subtract the components of decomposed red component of watermarked image and the red component of original image by the following formula [9]:-

$$R_w=f-(z.*(1 + c.*N))$$

R_w =Extracted watermark.

N = Original Watermark.

c = Weight of watermark where $c=1$;

f = 2x2 matrix for the level 1 sub-bands of red component of watermarked image decomposed by DWT.

z = 2x2 matrix for the level 1 sub-bands of red component of original image decomposed by DWT.

CONCLUSION AND FUTURE SCOPE

Proposed watermarking algorithm uses Multiplicative embedding rule for watermark embedding, invisible and non blind watermarking algorithm. This algorithm is applicable for colour images by which you can easily embed and extract the watermark. Future scope of the this algorithm is that it can further modified and improved for the attack analysis on the watermarked image for testing robustness and imperceptibility of proposed algorithm.

REFERENCES

- I. Yusnita Yusof and Othman O. Khalifa, Member, IEEE," Digital Watermarking For Digital Images Using Wavelet Transform", in Proceedings of the 2007 IEEE International Conference on Telecommunications and Malaysia International Conference on Communications, Penang,

- Malaysia, 14-17 May 2007, pp.665 – 669.
- II. Mehemed Bashir Aliwa, Tarek El-Ahmady El-Tobely, Mahmood M.Fahmy et.al, —Fidelity and Robust Digital Watermarking Adaptively Pixel based on Medial Pyramid of Embedding Error Gray Scale Images,|| in International Journal of Computer Science and Network Security, VOL.10 No.6, pp. 284-314, June 2010.
- III. Yanqun Zhang, —Digital Watermarking Technology: A Review,|| in ETP International Conference on Future Computer and Communication, 2009, pp 250 –
- IV. Prof. Manoj Ramaiya, Richa Mishra, — Digital Security using Watermarking Techniques via Discrete Wavelet Transform|| in National Conference on Security Issues in Network Technologies (NCSI-2012), pp 1-8, August 2012.
- V. Martin Zlomek, —Video Watermarking,|| Master Thesis, Dept. of Software and Comp. Science Education, Charles university, Prague, Czech Republic, 2007.
- VI. Elinor Mills(2011 March 1), Watermark tap old trick for mobile media (1st ed.) [Online]. Available: http://news.cnet.com/8301-27080_3-20037532-245.html.
- VII. Jiang Xuehua, —Digital Watermarking and Its Application in Image Copyright Protection||, in IEEE International Conference on Intelligent Computation Technology and Automation - 2010, 2010, pp 114-117.
- VIII. Dr. Neeraj Bhargava, Dr. M. M. Sharma, , Abhimanyu Singh Garhwal, Manish Mathuria, ||Digital Image Authentication System Based on Digital Watermarking||, in International Conference on Radar Communication and Computing (ICRCC-2012), Dec 2012. Available Online: [http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6450573&content_Type=Conference+Publications&sortType%3Dasc_p_Sequence%26filter%3DAND%](http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6450573&content_Type=Conference+Publications&sortType%3Dasc_p_Sequence%26filter%3DAND%26)

28p_IS_Number%3A6450525%29
%26pageNumber%3D2.

- IX. Peter Meerwald, —Thesis on digital image watermarking using wavelet transformation,|| diploma thesis, Dept. of Computer Science, University of Salzburg, Salzburg, Austria, 2001.
- X. Mitra Abbasfard —Digital Image Watermarking Robustness: A Comparative Study,|| MSc thesis, Dept. of Electrical Engineering, Delft University of Technology, Delft, Netherland, 2009.
- XI. Nikita Kashyap, G. R. Sinha, —Image Watermarking Using 3-Level Discrete Wavelet Transform (DWT)||, I.J.Modern Education and Computer Science, pp 50-56, April 2012.