www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 6 June, 2014 Page No. 6804-6806

An Improved Approach of Digital Watermarking in Frequency Domain

Kirti[1], Vikram Nandal[2]
[1]M.Tech student, CSE Dept, R.N College of Engineering & Management
[2]Assistant Professor, CSE Dept, R.N College of Engineering & Management
[1]Kirtinandal3@gmail.com, [2]vikramcselive.com

Abstract: Digital watermarking is the processing of combined information into a digital signal. A watermark is a secondary image, which is overlaid on the host image, and provides a means of protecting the image. It acts as a digital signature, giving the image a sense of ownership or authenticity. Digital watermarking technique is very impressive for image authentication or protection for attacks. This paperproposes an approach to robust digital watermarking in frequency domain. The approach is divided in two parts: one is watermark embedding and another is watermark extraction. For watermarking SWT transformation is performed. MSE and PSNR are calculated for the extracted watermark.The robustness of different digital watermarking algorithms in frequency domain is evaluated by applying different attacks and by calculating PSNR. In this paper comparison is also performed between the proposed technique and DCT, DFT and DWT.

Keywords: digital watermarking, frequency domain, MSE, PSNR.

I. INTRODUCTION

Digital watermarking is the embedding or hiding of information within a digital file without noticeably altering thefile itself. Now digital image watermarking is increasing attention due to the fast developing in the internet traffic.Digital watermarking achieved is popularity due to its significance in content authentication and copyright protection for digital multimedia data. It is inserted invisible in host image so that it can be extracted at later times for the evidence of rightful ownership [1].The large use of networked multimedia system has created the need of "Copyright Protection" for different digital medium as images, audio clips, videos etc. The term "Copyright Protection" involves the authentication of ownership and identification of illegal copies of digital media. Though digital media provides various efficient facilities like distribution, reproduction and manipulation of images, audio clips and videos, they increase illegal copying of digital

media. The solution for this problem is to add the visible or invisible structure to digital media which is to be protected from copyright. These structures are known as "Digital Watermarks" and the process of adding digital watermarks to digital media is known as "Digital Watermarking". Digital watermarking is created by inserting a digital signal or pattern into digital content. Digital watermarking is nothing but process of conveying information by imperceptibly embedding it into digital media. The purpose of embedding the information depends upon application and need of user of digital media. Digital watermarking provides the solution for difficult problem of providing guarantee to organizer and consumer of digital content about their legal rights. Copyright protection for multimedia information is nothing but a golden key for multimedia industry.

Characteristics of Watermarking [2]:

There are many characteristics that watermarking hold are as follows:

5.1 Invisibility

An embedded watermark is not visible. Invisible watermark is hidden in the content. It can be detected by an authorized agency only. Such watermarks are used for content or author authentication and for detecting unauthorized copier.

5.2 Computational Complexity

Computational complexity indicates the amount of time watermarking algorithm takes to encode and decode. Toensure security and validity of watermark, more computational complexity is needed. Conversely, real-timeapplications necessitate both speed and efficiency.

5.3 Robustness

Piracy attacks or image processing should not affect the embedded watermark. Even if the visible watermark isremoved (by an attack), there is the invisible one as the backup. The visible watermark is inserted into the originalimage while the invisible water mark is added to it. Therefore, it is a watermark within a watermark creating a dualwatermarked image. This is another method of developing robust watermarking techniques. For robustness we can also add watermark at more than one position in the image, if one or two are removed then the other is there.

5.4 Fidelity

Fidelity can be considered as a measure of perceptual transparency or imperceptibility of watermark. It refers to the similarity of un-watermarked and watermarked images. This perspective of watermarking exploits limitation of human

vision. Watermarking should not introduce visible distortions as it reduces commercial value of the watermarked image.

5.5 Data Payload

Data payload is also known as capacity of watermarking. It is the maximum amount of information that can be hidden without degrading image quality. It can be evaluated by the amount of hidden data. This property describes how much data should be embedded as a watermark so that it can be successfully detected during extraction.

5.6 Non-perceptibility

Watermark cannot be seen by human eye or not be heard by human ear, only be detected through special processing or dedicated circuits.

5.7 Verifiability

Watermark should be able to provide full and reliable evidence for the ownership of copyright-protected information products. It can be used to determine whether the object is to be protected and monitor the spread of the data being protected, identify the authenticity, and control illegal copying.

II. Digital Watermarking inFrequency Domain

Watermark to be distributed over the whole domain of the cover image and is achieved by using transformation to the original image. These methods are based on the usage of some invertible transform (DFT), discrete wavelet transform (DWT)[8] etc. to the host image. Embedding of a watermark is made by modifications of the transform coefficients, accordingly to the watermark or its spectrum. Finally the inverse transform is applied to obtain the marked image. This approach distributes irregularly the watermark over the image pixels after the inverse transform, thus making detection or manipulation of the watermark more difficult.These methods are more complicated and require more computational power.

Our proposed technique is divided into two steps. Watermark insertion and watermark extraction. The goal of proposed technique is to improve the robustness of watermarked image. The embedding process takes as input a watermark (the data to be embedded in the image), a carrier signal (the digital image into which the watermark will be embedded), and a key, similar to the keys used in cryptographic systems. The output of the embedding process is a new digital image which contains the watermark. The reverse process, watermark extraction, is not the same for all watermarking systems. The extraction process, as a minimum, takes the watermarked image and the key as inputs.

Our proposed approaches for insertion and extraction are based on following algorithms.

ALGORITHM (WATERMARK EMBEDDING)

(a) Read original image and watermark image
(b) Generate a pseudorandom number sequence
(c) Perform SWT2 transformation on original image and watermark image, we get a coefficient matrix.
(d) XOR the pseudorandom sequence with watermark image and the resultant image is modified watermarked image.
(e) Watermark embedding can be done as:

0←swtc x mwi
O = output coefficient matrix
Swtc = transformed coefficient matrix
Mwi = modified watermark image

(f) Apply inverse discrete stationary wavelet transformation to get watermarked image.

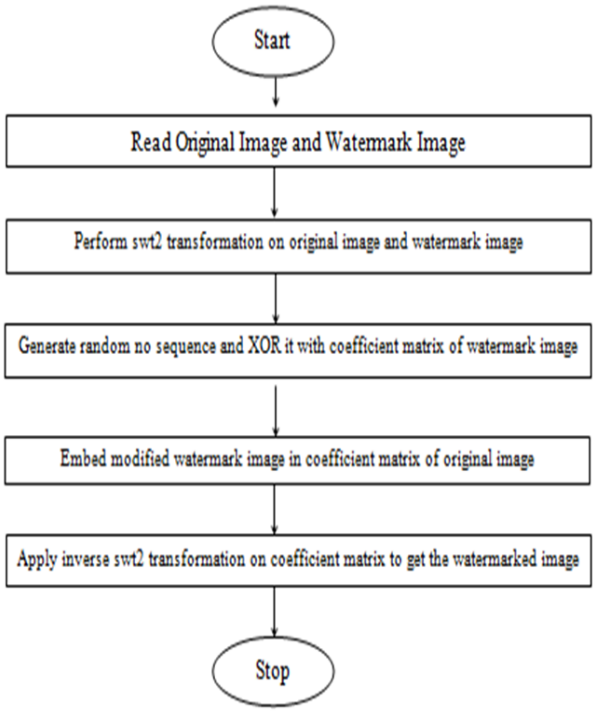

Fig1. Flow chart of watermark embedding

ALGORITHM (WATERMARK EXTRACTION)

(a) Read the watermarked image and original image.
(b) Perform SWT2 transformation on original image and watermarked image, we get coefficient matrix.
(c) Watermark extraction can be done as:

W← swtc / oi
oi = Original Image
swtc = transformed coefficient matrix
W = watermark coefficient matrix

(d) XOR the above pseudo random sequence with extracted watermark image
(e) Apply inverse discrete stationary wavelet transformation to get original watermark image.

Flow Chart of Watermark Extraction is shown below:

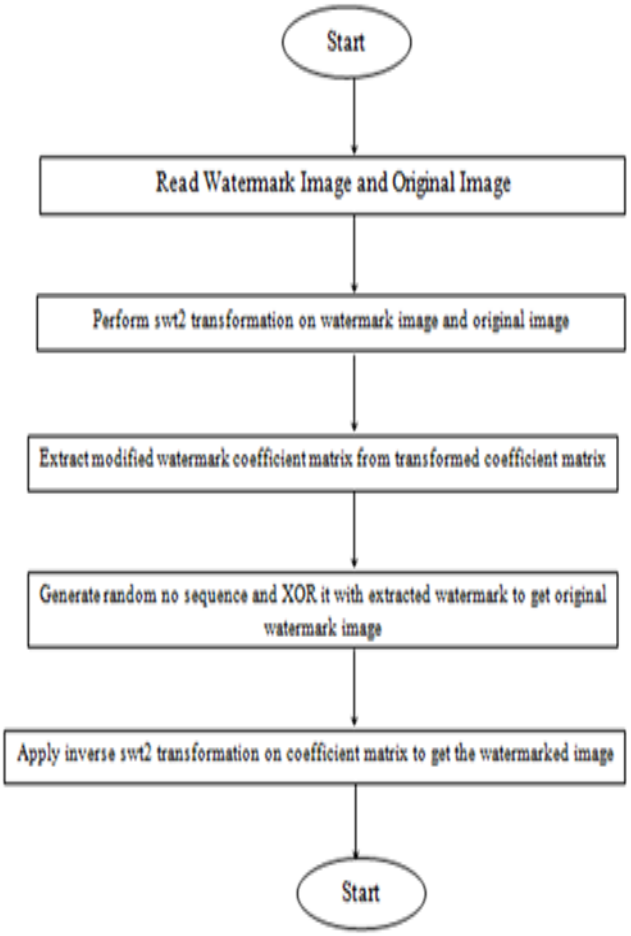

Fig 2. Flow chart of extraction process

III. RESULTS

To calculate the impact of our proposed approach, simulation is done using MATLAB. Table 1 shows PSNR of DCT, DWT, DFT and proposed technique against various attacks.

Attacks	PSNR (DCT)	PSNR (DWT)	PSNR(DFT)	PSNR (Proposed Technique
Watermarked Image	34.2423	24.9588	13.4119	48.0546
Poisson Attack	29.7157	28.9580	17.7461	25.1827
Speckle attack	22.0836	21.5686	17.7988	26.6995
Gaussian attack	19.2978	19.1260	21.1228	23.9778

Table 1 PSNR comparison

The effectiveness, efficiency and robustness of the designed and existing methods for digital watermarking in frequency domain against various attacks is reflected in table 1 by calculating PSNR value through simulation.

IV. CONCLUSION& FUTURE WORK

Digital watermarking is the embedding or hiding of information within a digital file without noticeably altering the file itself. In this paper we have proposed an improved approach of Digital Watermarking in Frequency Domain. We have shown results for existing techniques and made comparison with our proposed technique. Simulation results shows that by usingxor operation on the watermark image before embedding in proposed approach,made it more efficient and robust against existing approaches.

Digital watermarking, in its multitude of forms, has been in use literally for thousands of years. With the advancement in technology improvements are done on digital watermarking techniques. So we will focus to develop more secure and robust digital watermarking techniques which are easy to implement and which are more robust from security point of view. In this regards, future work is to introduce a new approach that works on frequency domain using 3-dimensional images

V. REFERENCES

[1]. Literature Survey on Digital Image Watermarking Er - Hsien Fu EE381K-Multidimensional Signal Processing 8/19/98.

[2]. I. J. Cox and M. L. Miller, "Electronic watermarking: the first years". Fourth, IEEE Workshop on Multimedia Signal Processing, 2001, pp. 225-230.

[3]. F. A. P. Petitcolas, R.J. Anderson, R. J. and M. G. Kuhn," Information hiding - A survey," Proceedings of the IEEE, Volume 87, Issue 7, 1999, pages 1062-1078.

[4]Ming-Shing Hsieh, Din-Chang Tseng, Member, IEEE, and Yong-Huai Huang "Hiding Digital Watermarks Using Multi resolution Wavelet Transform", IEEE Transactions on Industrial Electronics, Volume 48, Issue 5, pages 875-882, Oct.
2001.

[5]Sin-Joo Lee, Sung-Hwan Jung, "A Survey of watermarking techniques applied to multimedia", IEEE Transactions on Industrial Electronics, Volume 1, pages 272- 277, 2001.

[6] Muharemagic and BorkoFurht "Survey OfWatermarking Techniques And Applications".

[7] G. Coatrieux, L. Lecornu, Members, IEEE, Ch. Roux, Fellow, IEEE, B. Sankur, Member, IEEE'a review of digital image watermarking in health care'.

[8]D. Kilburn. Dirty linen, dark secrets.Adweek, 1997.20. Santa Agreste, Guido Andaloro, Daniela Prestipino, LuigiaPuccio, "An Image Adaptive Wavelet Based Watermarking of Digital Images", Science Direct Journal of Computational and Applied Mathematics, 2006, pp. 1-9.

[9]J. Fridrich, "Image watermarking for tamper detection," in Proc. IEEE Int. Conf. Image Processing, Chicago, IL, Oct. 1998, pp. 404-408

[10]. Keshav S Rawatet. al. / Indian Journal of Computer Science and Engineering Digital watermarking scheme for authorization against copying or piracy of color image volume. 1 No. 4 295-300.

[11]. EdinMuharemagic and BorkoFurht "a survey of watermarking techniques and applications" 2001