ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

Hybrid Digital Watermarking Technique based on DWT-DCT-SVD algorithms.

[1] Riya Naik, [2] Manisha Naik Gaonkar
[2] Professor
[1][2][3] Department of Computer Science & Engineering, Goa College of Engineering, Farmagudi, India

Abstract: Digital watermarking is a developing technology which ensures and facilitates security, authentication and copyright protection of digital data. Digital watermarking is the method of hiding digital data in any form of multimedia data such as image, audio, video, etc. This paper performs a comparative analysis of different hybrid image watermarking techniques. The watermarking techniques based on a combination of DCT and DWT is implemented. These methods use Singular Value Decomposition (SVD) of the cover image and watermark for embedding the watermark. Different attacks are applied on the watermarked image in order to analyze the robustness of each algorithm.

Index Terms— Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Singular Value Decomposition (SVD), least significant bit (LSB).

I. INTRODUCTION

Digital watermarking technique is a solution to the copyright protection problem of digital media. The digital watermarking was developed as a variation of steganography. Watermarks are traditionally used in currencies, paper and postage stamps to prevent fraud and forgery. In most recent scenario watermarking is used in the exchange of digital data. Digital watermarking is the process of hiding a digital data into another digital data. It is applied to digital data such as image, audio, video, etc. Digital watermarking find its applications in the field of image processing, cryptography, signal processing and communications. Due to the increased usage of digital data and their exchanges through the Internet, it is necessary to provide security measures for this data in order to gain copyright protection and ownership rights. Researches based on achieving the security of digital images while exchanging them through the internet are happening widely nowadays. At the time of transmission through the channel, this image can get accessed by a third party and he can fraud or tamper the data and resend it to the destination. Using a watermark this can be prevented. Any tampering on the image will also affect the watermark. By extracting and analyzing the watermark the receiver can understand that it is not the actual image that was transferred by the sender. Watermarking can also be considered as method for secret communication. Invisible watermarks will help for this secret data passing. A confidential data or image can be watermarked into a host image using a key and send to the receiver. The receiver who has the actual key is only able to extract the watermark with the help of that key.

The watermark can be visible or invisible. Invisible watermarks have wide range of applications today. The watermark image can be a simple image, a logo of the company or the owner of the company to indicate ownership, fingerprint or signature of the owner which are unique, etc. Unique data such as signatures faces and other biometric identifiers are efficient to indicate ownership because these cannot be reproduced by a third party. Signature is unique but they can be easily imitated and forged. The watermark embedding technique is done on spatial domain and frequency domain. In this paper a comparison between the robustness of different frequency domain watermarking techniques are done, which are DCT, DWT, DCT + SVD, DWT + SVD, DWT + DCT + SVD methods. The paper is organized as follows: section II covers the related works based on frequency domain watermarking, section III, IV defines the proposed watermarking techniques, section V defines experimental results on an image and VI gives the conclusion drawn from the analysis.

II. RELATED WORK

The least significant bit (LSB) [1] [2] a spatial domain technique uses simple operation to embed information in a cover image. In LSB technique inside of a cover image pixels are changed by bits of the secret message where LSB of the original image carries watermark information. On the average, only half of the bits in an image will need to be modified to hide a secret message using a cover image. These changes cannot be perceived by the human. But, a passive attacker can easily extract the changed bits, or manipulate the bits therefore spatial domain methods are considered as less robust and suffer from signal compression.

Discrete Cosine Transform (DCT) [3] is a Fourier Transform, it represents data in terms of frequency space rather. DCT based watermarking techniques are robust compared to spatial domain techniques. DCT divides the image into three bands namely low frequencies, middle frequencies and high frequencies. Low frequencies are related to illumination condition. High frequencies represents noise and middle frequencies contain useful information and basic structure of an image. Middle frequencies are chosen to embed watermark as it does not scatter the watermark information.

Another method proposed by Gu Tianming [4] DWT corresponds to processing the image by 2-D filters in each dimension. The filters decomposes the input image into four non-overlapping multi-resolution sub-bands LL1, LH1, HL1 and HH1. To obtain coarser wavelet coefficients, the sub-band LL1 is further divided the watermark is embedded into final low frequency area. The proposed algorithm is robust against many image distortions.

The method introduced by Justin Varghese [5] divides the host image using DCT and reference image. SVD [7] is applied to both reference image and watermark. And singular values of reference image is manipulated using singular values of watermark image. Singular Value Decomposition (SVD) is more robust to potential attacks and rank high due to its simplicity and compactness [6]. Prasanah shah et.al [8] proposed a technique which is combination of DWT and SVD. It forms four band data with decomposition level called LL, HL, LH and HH sub bands. Proposed watermarking algorithm initially decomposes the host image into sub bands; next it determines the singular values of each sub band and modifies these with the watermark by scaling with the scaling factors. Method shows. Improvement in robustness under different wavelet function.

III. DWT-DCT-SVD WATERMARKING

In this watermarking scheme, DCT, DWT and SVD based hybrid watermarking scheme is devised by utilizing their salient features. First one level DWT is applied to original cover image. To achieve imperceptibility LL band is select for second level decomposition and LL_ HH band is selected. It is divided into 4X4 sub blocks. DCT is applied to each sub blocks and first DC coefficient of each block is selected and formed it in matrix. SVD is applied to this matrix and singular values are modified with singular values of watermark. Inverse SVD, inverse DCT and inverse DWT is performed to get watermarked image.

A. Embedding of watermark

The embedding process is summed up in following steps:

1. Consider I1 as input image of size N x N. Select Color channel.
2. Apply DWT to decompose it into four sub-bands LL, HL, LH and HH.
3. Select LL band and Apply DWT to decompose it further Into LL_LL, LL_HL, LL_LH and LL_HH.
4. Select LL_HH band, divide it into 4 X 4 blocks and apply DCT to get coefficient matrix M.
5. Apply SVD to M, M=U1*S1*V1T, and obtain U1, S1 and V1.
6. Let I2 be watermark image of size N/16 x N/16. Apply SVD to it, I2= W_U*W_S*W_V'.
7. Obtain W_U, W_S and W_V.

6. Modify S1 with watermark such that S=S1 + α* W_S.
7. Obtain M* using M*= U*S*VT.
8. Apply inverse DCT (IDCT) to M* to get LL_HH*.
9. Apply inverse DWT (IDWT) to LL_LL, LL_HL, LL_LH and LL_HH* to get matrix LL*.
10. Apply inverse DWT (IDWT) to LL*, HL, LH and HH to get watermarked image IW.

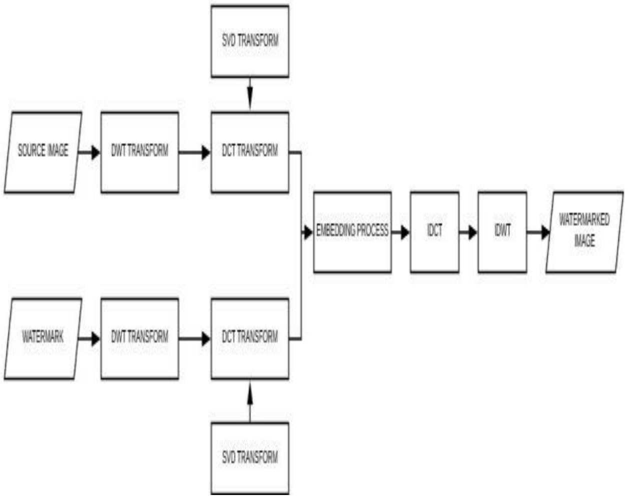

Figure 1: Embedding process.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

B. Watermark Extraction Process

The extraction process is summed up in following steps:

1. Select color channel and apply DWT to IW to get LL*, HL, LH and HH.

2. Apply DWT again to get LL_LL, LL_HL, LL_LH and LL_HH*

3. Select LL_HH* band and divide it into 4X4 square Blocks.

4. Apply DCT to each block of sub band LL_HH*,to get matrix M1.

5. Apply SVD to M1, M1= WU*WS*WVT and obtain WU, WS, WV.

6. Obtain SW=(S-WS) /α.

7. Obtain EW= WU*SW*WVT

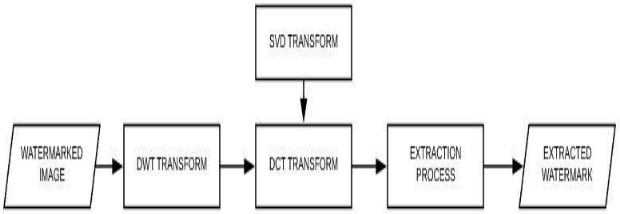

Figure 2: Extraction Process.

IV. EVALUATION PARAMETERS

The PSNR value was used to evaluate the quality and imperceptibility, i.e. the similarity between two images. The peak signal-to-noise ratio (PSNR) is most commonly used as a measure of quality of reconstruction in image compression [lsb1]. It is defined via the Mean Squared Error (MSE) which for two m X n images I and K where one of the images is considered as a noisy approximation of the other (in other words, one is the original and the other is the watermarked image). MSE is defined as the following equation (1) and the PSNR is defined in equation (2).

$$\text{MSE} = \frac{1}{m*n}\sum_{i=0}^{m-1}\sum_{i=0}^{n-1}[I(i.j) - K(i,j)]^2 \quad (1)$$

Where I is the original image and K is the watermarked image.

$$\text{PSNR}=10 * \log 10\left(\frac{max}{MSE}\right)$$

$$20 * \log 10\left(\frac{max}{\sqrt{MSE}}\right) \quad (2)$$

Where MAX is equal to 255 in grayscale images, MSE is the mean square error.

A good imperceptibility means that the watermarked image looks nearly identical to the original image, and thus, the host image is barely affected by the embedding process.

V. EXPERIMENTAL RESULTS

Results are calculated on the basis of Experiment done in MATLAB R2017a. The watermarking algorithms are tested for the various host and watermark images. The originality of the image taken should not be affected with the watermarking algorithm. Calculated PSNR and MSE values for Sample image taken are shown in the table.

For evaluating the robustness the implemented scheme has been tested for cover images of size 512 x 512 pixels, and the watermark of size 64 x 64 pixels. The three watermarking algorithm on were experimented on 04 different cover images and a single image is used as common watermark.

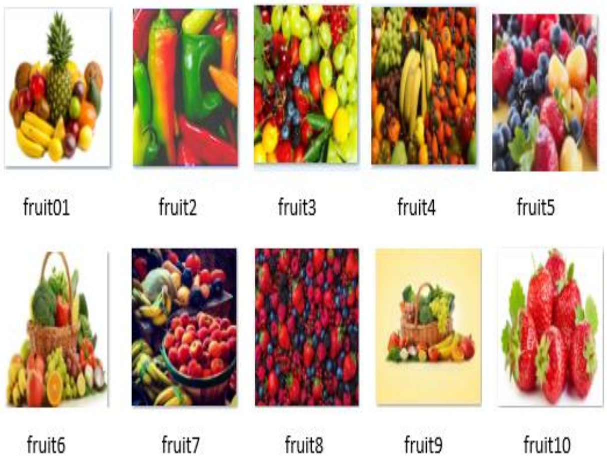

Figure 3: Cover images

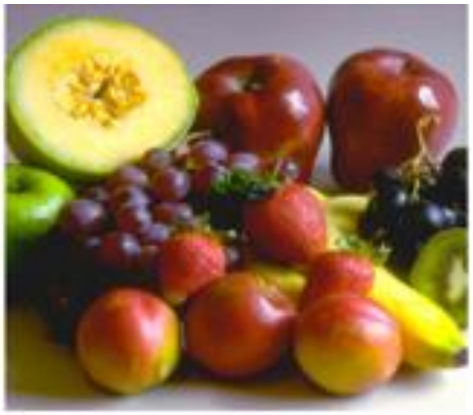

Figure 4: Watermark Image.

IMAGES	LSB	DCT	DWT	DCT-SVD	DWT-SVD	DWT-DCT-SVD
Fruits01	34.33	36.85	35.40	36.70	35.95	35.98
Fruits02	29.57	29.47	35.27	32.50	35.05	35.33
Fruits03	34.70	34.29	39.49	40.29	44.35	42.64
Fruits04	36.89	36.08	40.46	41.43	47.03	47.42
Fruits05	38.08	36.61	41.21	39.69	47.14	44.33
Fruits06	39.36	37.63	40.18	39.40	38.20	38.87
Fruits07	34.84	34.72	39.05	40.14	44.46	42.29
Fruits08	32.65	32.39	38.62	38.77	43.23	43.77
Fruits09	37.72	36.70	39.43	38.57	34.98	35.83
Fruits10	32.17	32.00	36.89	36.76	36.00	37.22

Table I: PSNR values of Watermarked Images

IMAGES	LSB	DCT	DWT	DCT-SVD	DWT-SVD	DWT-DCT-SVD
Fruits01	20.65	19.07	23.18	20.12	18.54	20.26
Fruits02	17.35	17.39	23.66	19.34	20.47	19.31
Fruits03	18.70	18.29	23.27	22.45	21.58	22.56
Fruits04	19.46	18.59	27.79	24.22	26.14	26.47
Fruit05	20.41	19.04	27.79	20.21	27.10	27.87
Fruits06	21.07	19.22	23.07	20.09	18.69	21.34
Fruits07	18.99	18.79	23.99	19.70	24.14	23.87
Fruits08	18.05	18.01	23.12	21.27	23.69	24.84
Fruits09	19.84	19.11	25.31	20.44	17.18	17.08
Fruit10	17.88	17.69	21.22	19.54	19.01	18.68

Table II: MSE values of Watermarked Images.

CONCLUSION

In this experiment, performance analysis of LSB, DCT, DWT DCT-SVD, DWT-SVD and DWT-DCT-SVD methods is successfully completed and experimental results are discussed. The MSE and PSNR values are compared for the algorithms. The PSNR value shows the quality of image after embedding the data. From the experiment results it is observed that the PSNR of DWT-DCT-SVD is high as compared to the other algorithms. Thus, the experiment concludes the DWT-DCT-SVD algorithm is more suitable for the steganography application.

REFERENCES

[1] Abdullah Bamatraf, Rosziati Ibrahim and Mohd. Najib Mohd Salleh, "_ A New Digital Watermarking Algorithm Using Combination of Least Significant Bit (LSB) and Inverse Bit," Journal of computing, volume 3, Issue 4, April 2011, ISSN 2151-9617.

[2] Etti Mthur, Manish Mathuria, "Unbreakable Digital Watermarking using combination of LSB and DCT" International Conference on Electronics, Communication and Aerospace Technology ICECA 2017

[3] Syed Ali Khayam, "The Discrete Cosine Transform (DCT): Theory andApplication", March 10th 2003.

[4] Gu Tianming ,Wang Yanjie, "DWT-based Digital Image Watermarking Algorithm", The Tenth International Conference on Electronic Measurement & Instruments ICEMI'2011 978-1-4244-8161-3/11/$26.00 ©2011 IEEE.

[5] Justin Varghese, Saudia Subash, Omer Bin Hussain, "An Efficient DCT - SVD based Algorithm for Digital Image Watermarking "978-1-4799-3532-1/14$31.00©2014 IEEE.

[6] Mengmeng Li, Chao Han,"A DCT-SVD Domain Watermarking for Color Digital Image Based on Compressed Sensing Theory and Chaos Theory" Seventh International Symposium on Computational Intelligence and Design 978-1-4799-7005-6/14 $31.00 © 2014 IEEE.

[7] Rashmi Agarwal, "Block Based Digital Watermarking using Singular Value Decomposition on Color Images", International Conference on Computing, Communication and Automation (ICCCA2015) ISBN:978-1-4799-8890-7/15/$31.00 ©2015 IEEE.

[8] Prasanna Shah, Toshanlal Meenpal, Ankit Sharma, Vivek Gupta, Amit Kotecha, "A DWT-SVD Based Digital Watermarking Technique for Copyright Protection", International Conference on Electrical, Electronics, Signals, Communication and Optimization (EESCO) – 2015.

[9] Shabir A. Parah, Shazia Ashraf, Ayash Asharf "Robustness Analysis of a Digital Image Watermarking Technique for Various Frequency Bands in DCT Domain ", IEEE International Symposium on Nanoelectronic and Information Systems 2015.