A FEATURE BASED SEMI-FRAGILE WATERMARKING MECHANISM FOR GRAY-SCALE DIGITAL IMAGE AUTHENTICATION.

Ms. Hiral A. Patel

Abstract-As the use of internet increases day by day, the authentication as well as integrity issues are also increased. This paper proposed the semi fragile watermarking algorithm which discriminate the malicious and non-malicious attacks and work accordingly. The algorithm is designed in such a way that the watermark is generated from the original image. The features of the image are extracted using DWT and canny edge detection method. These features' image is worked as watermark image. To embed this watermark in original image the combination of DWT, DCT and SVD transforms are used. Using the advantages of the hybrid transform, the algorithm can achieve good result. With this algorithm, the imperceptibility which is measured using PSNR is increased as compare to other researchers' system. To check the robustness of the algorithm, numbers of attacks are applied on watermarked image. The experimental outputs show that the algorithm is robust with JPEG compression, Gaussian Noise, Salt and Pepper, Sharpen Image, Median Filter. For the authentication of the image, the proposed algorithm is preferable.

Keywords- Gray Image Content Authentication, DCT, DWT, SVD, Semi Fragile Watermarking, Digital Watermarking

I. INTRODUCTION

As the use of internet increases day by day, the use of digital assets like text, image, audio and video files also increases. Because of the telecommunication network, user can easily pass these files from one location to another through electronic way. There is a need to make file authentic so no one can integrate the file and also the authentication of original file can be done anytime. This paper is concern only with the digital image. Watermarking is the method which can embed the information about the image inside the original image in such a way that the size of the image is not changed and make this watermarked image invisible by unauthorized users. Authentication to image is possible using Fragile Watermarking and Semi-Fragile Watermarking.

Fragile watermarking is strict to authentication which doesn't allow a single bit change in image. Semi-fragile watermarking is content oriented authentication which tolerates content preserving manipulation and detects any manipulations that change the image content [12]. It is mainly used to discriminate between malicious and non-malicious attacks [13]. Feature based watermarking generates the watermark by extracting the features of original image and embeds this watermark

in original image. Using this feature, the integrity can be compared whenever requires [14].

The rest of the paper is organized as follows: Section 2 describes the related work which was done earlier by researchers, Section 3 expresses the proposed algorithm, Section 4 shows the experimental results and finally the conclusion is shown in Section 5.

II. RELATED WORK

The published work related to the image content authentication shows that the authentication issue solved using fragile watermarking as well as semi fragile watermarking. Many researchers worked on Semi fragile watermarking for authentication and achieved their target. Some of the researchers work progress towards the semi fragile watermarking is discussed below. In [1] S.S.Sujatha et. al. used DWT and Arnold scrambling for more security and achieved the result with PSNR 59.1168 and tolerated JPEG Compression up to 10% with Similarity ratio 0.8158. The watermark size was 256 X 256. In [2] Woo Chaw Seng et. al. embedded the watermark using DWT method, got 85.09 PSNR and tolerated JPEG Compression up to 85% and noise with density 0.03.

In [3] Chaitanya Kommini et. al. worked with colour images, used DWT and secret key for more security, achieved PSNR up to 34.16 and tolerated JPEG Compression up to 80%. In [4] Lintao LV et. al. embedded the watermark using DWT and achieved the PSNR up to 44.2936. They tolerated the JPEG Compression up to 50%. In [5] Md. Moniruzzaman et. al. embedded the watermark of size 85 X 85 using DWT and Secret code. They used XOR for scrambling, achieved PSNR 44.60 and tolerated JPEG Compression up to 80%. In [6] Chitra Arathi embedded the watermark using SVD method but the system was less imperceptible and not robust. In [7] Buddhika Madduma et. al. had worked with feature based watermark and generated watermark from original image using Sobel Edge detection and Zernike Movement Megnitude, embedded the watermark using DCT and DWT which tolerated JPEG Compression up to 40% and Gaussian noise up to 0.3.

In [8] Nidhi Divecha et. al. embedded watermark of size 128 X 128 using DCT, DWT and SVD method and was robust for many attacks. In [9] Mohammad Ibrahim Khan1 et. al. used DCT, DWT and SVD to embed the watermark of size 256 X 256, tolerate JPEG Compression up to 75% and Gaussian noise up to 0.001. In [10] Tanmay Bhattacharya worked with colour images, embedded the watermark of size 64 X 64 using DWT and achieved the PSNR up to 34.5409. In [11] Nidhi Divecha et. al. had

worked with colour images and embedded watermark of size 32 X 32 using DCT, DWT and SVD methods. They suggested two algorithms and achieved the PSNR up to 53.00. Archana Tiwari et. al. [16] had worked with gray scale image. It used cover and watermark images. Two watermarks were used among these one is used for robustness and another is used for semi-fragility. Watermark was embedded within 4X4 blocks and vector quantization method used. Calculate variance and embed the watermark based on the threshold value. The achieved the PSNR up to 41.79dB. System also tested different non-malicious attacks. Nazir A. Loan et. al. [17] had developed system for gray scale as well as colour image. The proposed system for gray scale image used separate image as a watermark. Scrambling is applied to the watermark image using Arnold transform. XOR is used to encrypt the data. Watermark is embedded within cover image based on the bock based DCT. The PSNR is achieved up to 42.65dB.

Based on this reviews following challenges are faced by existing techniques:

i. There is need to improve imperceptibility of watermarked image.

ii. Embedment done in perceptual significant coefficient brings distortion; there is a need to fill this gap.

iii. Diagonal line problem in SVD should be taken care.

iv. There is a need to improve the robustness of the existing techniques.

v. The improvements in robustness of the existing systems with wide range of attacks are required.

vi. Amalgamation of transform should be done in the way so higher imperceptibility, capacity and protection for variety of attacks can achieve.

III. PROPOSED ALGORITHM

The proposed work is trying to solve the above mentioned challenges. The proposed algorithm is divided into three parts: Generating Watermark, Embedding Watermark and Extracting Watermark. Each one is discussed further in detail.

a. Generating watermark:

The feature based watermarking means the feature of original image is extracted from the image and this feature is considered as watermark.

Input: Original Image

Output: Watermark

The feature of original image is extracted using following steps:

Let IM is the original image of size 512 X 512.

Apply Haar Wavelet transform to decompose the image into four sub bands LL1, LH1, HL1 and HH1 of size 256 X 256.

Again apply DWT of LL1 sub band to get LL2, LH2, HL2 and HH2 of size 128 X 128.

Select LL2 sub band and apply the canny edge detection method to get 128 X 128 sized logical image (WM).

Consider this WM as watermark image of size 128 X 128.

b. Embedding Watermark:

The embedding watermarking process is divided into following steps:

Input: Original Image, Watermark

Output: Watermarked Image

Follow the 1st, 2nd and 3rd steps of generating watermark process.

Select the LL2 sub band and apply DCT on it to get DCT co-efficient matrix B.

Apply SVD on B to get U, S and V.

Now apply SVD on WM (Watermark) to get U_W, S_W and V_W.

Modify the singular values S with S_W using scaling factor (α) using (1). Here the value of (α) is 0.01.

$$S\_NEW = S + \alpha * S\_W \quad (1)$$

Apply inverse SVD using (2).

$$iB = U * S\_NEW * V'. \quad (2)$$

Apply inverse DCT of iB to produce iLL2.

Apply inverse DWT to iLL2, LH2, HL2 and HH2 to get iLL1.

Apply inverse DWT to iLL1, LH1, HL1 and HH1 to get watermarked image (WMD).

c. Extracting Watermark:

For extracting watermark, the original image is required so this algorithm is of non-blind watermarking.

Input: Watermarked Image, Original Image

Output: Extracted watermark

The watermark extracting process from watermarked image is as follow:

Apply DWT to WMD to get LL1, LH1, HL1 and HH1.

Apply DWT to LL1 to get LL2, LH2, HL2 and HH2.

Calculate DCT of LL2 to get DCT co-efficient matrix A.

Apply SVD on A to get WU, WS and WV.

Obtain the singular values using (3).

$$SR = (WS - S)/ \alpha. \quad (3)$$

Apply inverse SVD using (4) to extract the embedded watermark..

$$WM\_E= U\_W * SR * V\_W' \quad (4)$$

IV. EXPERIMENTAL RESULTS

The algorithm is applied in MATLAB R2017a. The original image is of size 512 X 512 and the generated watermark is of size 128 X 128. The efficiency of the algorithm is tested using Gray scale images which are displayed in Fig. 1.

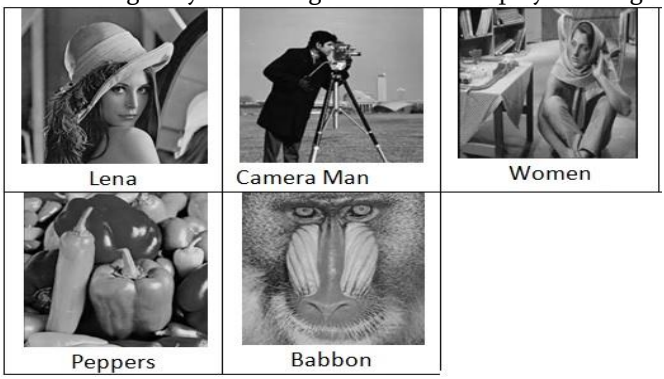


Fig. 1 Image Database

The original image, generated watermark, watermarked image and extracted watermark are demonstrated in Fig. 2.

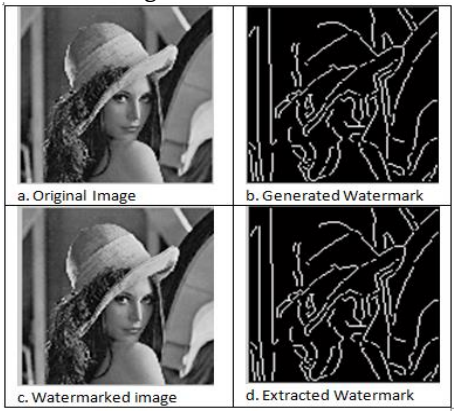


Fig. 2 Result without attack

To compare the imperceptibility of watermarked image, the system uses Peak Signal Noise Ratio (PSNR). Following is the formula to calculate the PSNR.

$$PSNR = 10\log_{10}\left(\frac{255\times 255}{MSE}\right)$$

where

$$MSE = \frac{1}{M \times N} \sum_{m=1}^{M} \sum_{n=1}^{N} [I(m,n) - I_w(m,n)]^2$$

Higher the PSNR value means the watermarked image is closer to the original image. To compare the robustness of the extracted watermark, NCC means Normalized Correlation Coefficient is calculated. NCC is calculated using following formula:

$$NC = (\sum_{i=0}^{M} \sum_{j=0}^{N} OW * EW) / (\sum_{i=0}^{M} \sum_{j=0}^{N} OW * OW)$$

NCC value is 1.0000 when the original watermark and extracted watermark are exactly matched. The comparison for the imperceptibility of the proposed algorithm with other researchers is shown in Table I. As Lena is the standard image, the comparison is done based on this image. The PSNR of proposed system is comparatively higher than the others.

Table I: PSNR comparison with existing systems

Authors	Year of publishing	PSNR Value
Proposed System		90.4665
Archana [16]	2018	41.92
Nazir [17]	2018	42.65
Arya [18]	2015	51.45

Table II shows the PSNR values which are near to 90dB with all images and NCC values are exactly 1 before applying attacks for all tested images.

Table II: PSNR and NCC values for different images.

Std. Images	PSNR	NCC
Lena	90.4665	1
Camera Man	91.3541	1
Women	88.9376	1
Peppers	90.5322	1
Babbon	88.5594	1

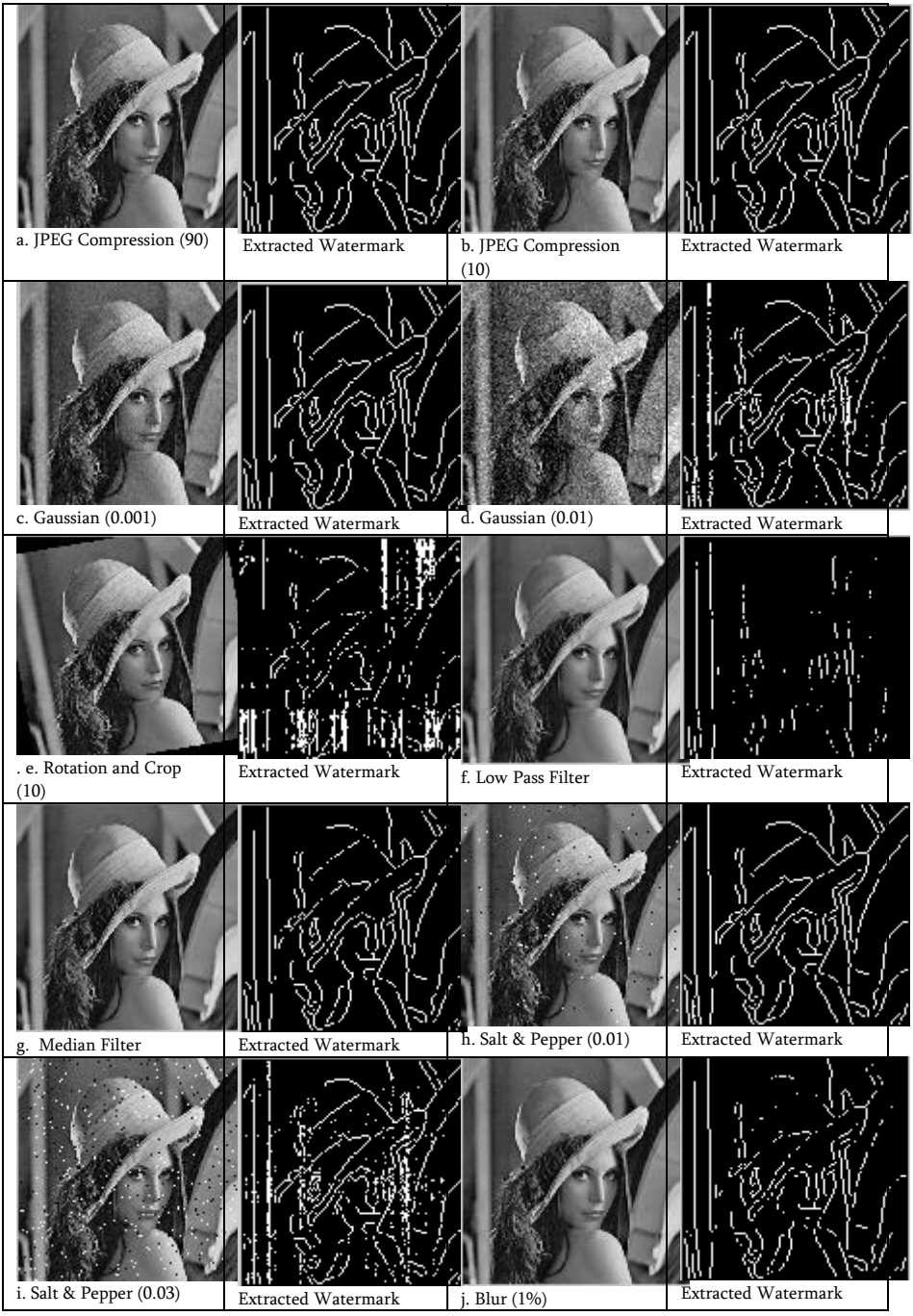
To check the robustness and the fragility, different attacks like JPEG compression, Gaussian noise, Salt & Pepper, Low Pass filter, Rotation, Blurring are applied with algorithm and the NCC results with image database are observed which are shown in Table III. As per the NCC result with different attacks, it is found that with JPEG compression, Gaussian noise, Median Filter, Salt & Pepper and Sharpen attacks proposed algorithm is robust where as with other attacks, it is fragile.

Table III: NCC values of proposed system with different attacks

Attacks	Lena	Camera man	Women	Peppers	Babbon
JPEG Comp					
90	1	1	1	1	1
50	1	1	1	1	1
10	1	1	1	1	1
Gaussian					
0.001	1	1	1	1	1
0.01	0.9517	0.7532	0.9972	0.9271	1
0.03	0.7603	0.5777	0.8401	0.756	0.9893
Low Pass Filter	0.3788	0.2123	0.5016	0.2977	0.2307
Rotation & Crop	0.6388	0.8598	0.7644	0.2095	0.8247
Median Filter	0.9275	0.9575	0.9582	1	0.7344
Salt & Pepper					
0.01	0.9987	0.9792	1	0.9927	1
0.03	0.8419	0.6931	0.8535	0.8282	0.9667
0.04	0.7792	0.6106	0.7556	0.7706	0.9339
Blur (1%)	0.8086	0.8013	0.9187	0.9761	0.8395
2%	0.3083	0.1771	0.3344	0.2095	0.1507
Sharpen	0.9941	1	0.9954	0.9993	0.9959
Motion Blur	0.2632	0.1426	0.3073	0.2122	0.2213

Fig. 3 Results with attacks

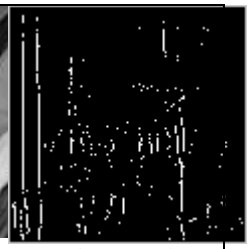
Fig. 3 demonstrated the attacked images and extracted watermarks. From Fig.3 it is revealed that with JPEG compression, Median Filter, Sharpen Image, Gaussian noise, Salt & Pepper attacks the watermark can be extracted properly where as with Blurring, Low Pass Filter, Rotation attacks it fails.


a. JPEG Compression (90)
Extracted Watermark
b. JPEG Compression (10)
Extracted Watermark
c. Gaussian (0.001)
Extracted Watermark
d. Gaussian (0.01)
Extracted Watermark
. e. Rotation and Crop (10)
Extracted Watermark
f. Low Pass Filter
Extracted Watermark
g. Median Filter
Extracted Watermark
h. Salt & Pepper (0.01)
Extracted Watermark
i. Salt & Pepper (0.03)
Extracted Watermark
j. Blur (1%)
Extracted Watermark


k. Sharpen Image


Extracted Watermark


l. Motion Blur


Extracted Watermark

V. CONCLUSION

In the paper, the system is proposed for authentication of the image. As per the results shown here, the PSNR is 90.4665 which show the imperceptibility of the watermarked image. Also the watermark is generated based on the original image so there is no need of extra cover image. The original image is used to embed the features of it which can further extracted whenever authentication as well as integrity needs to check. To check the robustness and the fragility, different attacks are applied on the algorithm and the results demonstrated that the proposed algorithm is robust with JPEG Compression, Median Filter, and Sharpen Image. With Gaussian noise, the algorithm is robust till the variance is less than 0.03. With Salt and Pepper noise, it resists till the density is less than 0.04. It is not robust with Rotation and cropping, Low pass filter, blurring and motion blur. This algorithm requires original image for extracting watermark so in future authors will try to solve the same with blind watermark. This algorithm is implemented and is worked only with Gray scale images so in future they will try to modify the algorithm for color images.

VI. REFERENCES

[1] Sathik, M. M., and S. S. Sujatha. "Authentication of digital images by using a semi-fragile watermarking technique." Int. J. Adv. Res. Computer.Sci. Softw.Eng 2.11 (2012): 39-44.

[2] Seng, Woo Chaw, Saied Ali Hosseini, and Leong Lai Fong. "Semi-fragile watermarking for gesture authentication." Open Systems (ICOS), 2011 IEEE Conference on. IEEE, 2011.

[3] Kommini, Chaitanya, Kamalesh Ellanti, and E. Harshavardhan Chowdary. "Semi-Fragile Watermarking Scheme based on Feature in DWT Domain."International Journal of Computer Applications 28.3 (2011).

[4] LV, LINTAO, et al. "A semi-fragile watermarking scheme for image tamper localization and recovery." Journal of Theoretical and Applied Information Technology 42.2 (2012): 287-291.

[5] Moniruzzaman, Md, et al. "Wavelet based watermarking approach of hiding patient information in medical image for medical image authentication."Computer and Information Technology (ICCIT), 2014 17th International Conference on. IEEE, 2014.

[6] Arathi, Chitla. "'A Semi Fragile Image Watermarking Technique Using Block Based SVD"." International Journal of Computer Science and Information Technologies 3.2 (2012): 3644-3647.

[7] Madduma, Buddhika, and Sheela Ramanna. "Content-based image authentication framework with semi-fragile hybrid watermark scheme." Man-Machine Interactions 2. Springer Berlin Heidelberg, 2011. 239-247.

[8] Divecha, Nidhi H., and N. N. Jani. "Image watermarking algorithm using DCT, DWT and SVD." IJCA Proceedings on national conference on innovative paradigms in engineering and technology NCIPET. Vol. 10. 2012.

[9] Khan, Mohammad Ibrahim, et al. "Digital Watermarking for Image AuthenticationBased on Combined DCT, DWT and SVD Transformation."arXiv preprint arXiv:1307.6328 (2013).

[10] Bhattacharya, Tanmay, Sirshendu Hore, and SR Bhadra Chaudhuri. "A Semi-Fragile Blind Digital Watermarking Technique for Medical Image File Authentication using Stationary Wavelet

[11] Transformation." International Journal of Computer Applications 104.11 (2014).

[12] Divecha, Nidhi, and N. N. Jani. "Implementation and performance analysis of DCT-DWT-SVD based watermarking algorithms for color images." Intelligent Systems and Signal Processing (ISSP), 2013 International Conference on. IEEE, 2013.

[13] Vartak, Reshma, et al. "Survey of Digital Image Authentication Techniques." (2014).

[14] Saha, Shilpi, Debnath Bhattacharyya, and Samir Kumar Bandyopadhyay. "Security on fragile and semi-fragile watermarks authentication." Int. J. Comput. Applicat 3.4 (2010): 23-27.

[15] Rey, Christian, and Jean-Luc Dugelay. "A survey of watermarking algorithms for image authentication." EURASIP Journal on Applied Signal Processing 6 (2002): 613-621.

[16] Wu, Xiaoyun, et al. "Secure Semi-Fragile Watermarking for Image Authentication Based on Parameterized Integer Wavelet." Journal of computers 17.2 (2006): 27-36.

[17] Archana Tiwari, and Manisha Sharma. "An Efficient Vector Quantization Based Watermarking Method for Image Integrity Authentication." Progress in Intelligent Computing, 2018.

[18] Loan, Nazir A., et al. "Secure and Robust Digital Image Watermarking Using Coefficient Differencing and Chaotic Encryption." IEEE Access 6 (2018): 19876-19897.

[19] Arya, Ranjan Kumar, Shalu Singh, and Ravi Saharan. "A Secure Non-blind block based Digital Image Watermarking technique using DWT and DCT." Advances in Computing, Communications and Informatics (ICACCI), 2015 International Conference on. IEEE, 2015

AUTHOR'S PROFILE

Ms. Hiral Patel is working as an Assistant Professor at SUTEX Bank College of Computer Applications and Science, Surat. She is a M.Phil. and GSET qualified faculty having more than 18 years of academic experience. She is currently pursuing Ph.D. from SPU, VV Nagar, Gujarat. Her area of interest includes Digital Image Processing especially Watermarking, Security and Networking etc. She has attended many conferences and seminars.