International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue IX, September 2017- Available at www.ijraset.com

A Robust Hybrid Non Blind Watermarking Algorithm Based On RDWT-DCT-SVD and Arnold Transform

Vikas Sharma[1], Rajvir Singh[2], Ajmer Singh[3]
[1]*M. Tech scholar,* [2,3]*Assistant Professor, Computer Science Department, D.C.R.U.S.T., Murthal*

Abstract*: With the increasing growth of internet, digital information can be retrieved anywhere anytime effortlessly. But this information also needs security from illicit and unauthorized usage and to protect copyright owners rights. Thus security becomes one of the significant problems to protect this information. The information can be in any form image, audio, video. Digital watermarking is the process of embedding a secret message or data into the original content to protect it from unauthorized access .In this paper we use RDWT-DCT-SVD based hybrid technique on colored image. The blue channel of the host image is processed with 3-level RDWT which results in 4 frequency sub bands. As higher frequency band provides better imperceptibility so we used HH2 sub band and then DCT is applied. The singular values of host image modified with the singular values of watermark image. The experimental performance is evaluated by applying different attacks on the watermarked image. The results demonstrated that the proposed method is more imperceptible and robust compared to existing hybrids.

Keywords: Singular value decomposition, redundant discrete wavelet transform, Discrete Cosine Transform, Arnold Transform, non-blind, RDWT, DCT, SVD, PSNR, NCC.

I. INTRODUCTION

With the increasing reachability of internet, protection of multimedia data is seeking more attention. The rapidly increasing capability and accuracy of image processing softwares enabled unauthorized users to violate owners copyrights and make illegal distributions or piracy without the owner's consent. There are various solutions proposed to handle the copyright problem like steganography, DRM, encryption techniques and watermarking. Digital watermarking provides the best solution to protect owner's rights and secure from piracy.

Digital watermarking is the technique of hiding secret information related to owner identification in the multimedia data such that no one is able to detect any thing hidden by viewing the multimedia data. The multimedia data may be image, audio or video and the secret information can be text, image or sequence of numbers. Various application of watermarking are covert communication, owner identification, Transaction tracking, broadcast monitoring and copy control[1]. Every watermark should satisfy some desirable and necessary properties. Some of the properties are conflicting to each others and we are forced to accept some tradeoffs between them. The first most important property is imperceptibility. If the human eye cannot identify the difference in original image and watermarked image, the image is said to be imperceptible. It should be high as much as possible. Second property is robustness. It refers to watermark ability to withstand various geometric attacks, noise and compression attacks[3]. Payload size refers to the amount of watermark data that can be embedded in the host image. All three properties stated above are conflicting to each other. Besides these some more properties are security, false positive rate, effectiveness etc.

II. WATERMARKING TYPES

According to human perception the watermark can be categorized as visible and invisible watermarks. Visible watermark are those which are visible to human eyes and invisible watermark are hidden from human eyes.

According to application, the watermark can be categorized as fragile, semi-fragile and robust watermarks. The fragile watermark destroys from little modifications thus help in detecting tampers. The semi-fragile watermarks destroys if threshold exceeds. The above two methods ensures integrity and authentication. Robust watermark can't be broken easily as these can withstand any of the attacks.

According to user's authorization, the watermarks are of two types- public and private watermarking. In public watermarking user is authorized to detect the watermark and in private users are not authorized.

According to information required to extract watermark, the watermarks are of 3 types- blind watermark which do not require original image during extraction, semi blind requires some special information to detect watermark and non-blind which requires original image to extract[2].

III. WATERMARKING METHODS

Watermarking techniques can be divided into two domains- spatial domain and transform domain. In spatial domain embedding is done directly to the pixel locations. The spatial domain techniques are simple to implement but very poor against geometric attacks. The spatial domain techniques are LSB, Texture mapping coding, patchwork and additive technique. The transform domain watermarking also known as frequency domain watermarking embeds the watermark into the transform coefficients after applying transform. The transform domain watermarking distributes the changes introduced by watermark in all of the locations as compared to spatial domain. The transform domain watermarking techniques are DWT (Discrete wavelet transform), DCT(Discrete cosine transform), SVD(Singular value decomposition), RDWT(Redundant discrete wavelet transform).

DCT is an orthogonal transform which transforms the image in terms of cosine transforms[4]. The DCT divides the image into low, middle and high frequency components. In DCT maximum energy is concentrated in low frequency. So if higher frequency components are thrown away we can reduce the data required thus compression can be achieved. The DCT is robust against compression attacks and less complex. But it is less resistant against geometric attacks.

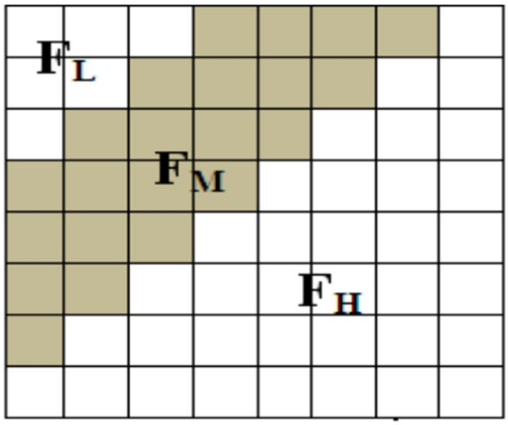

Fig. 3.1: DCT on 8x8 block

DWT transforms the image in terms of wavelets. A wavelet is a small wave of limited duration and varying frequency. It provides excellent spatial localization and multi resolution property. But it suffers from shift invariant. Thus a little change in image pixels can lead to major change in transform coefficients. It is more robust than DCT also it models the human visual model more perfectly than DCT. It decomposes the image into 4 sub domains- LL(Approximation), LH(Vertical), HL(Horizontal), HH(Diagonal). The lower sub domains(LL) contains the more significant components and higher subdomains(LH,HL,HH) contains least significant components. If higher components are considered for embedding imperceptibility increases but robustness decreases and if lower components are considered robustness increases and vice versa[5].

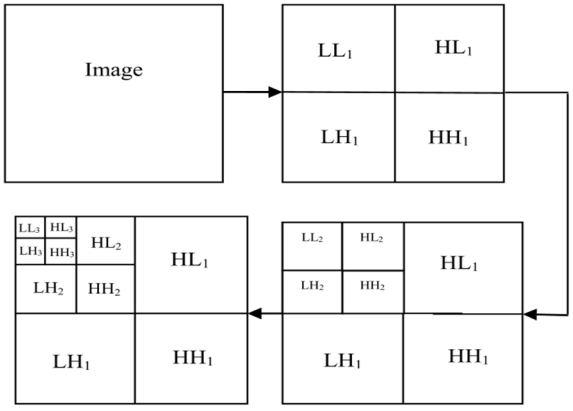

Fig. 3.2: DWT 3-level decomposition into subbands

RDWT[6] was proposed to overcome the limitations of DWT shift invariance. It removes the downsamplers and upsamplers in the DWT. Thus redundant information is stored in RDWT. It performs better in Affine transform but less efficient in rotation and blur attacks against DWT.

SVD is a mathematical tool which divides the matrix into 3 orthogonal matrices U,S and V where U is MxM matrix known as left singular value and S is a MxN diagonal matrix and V is a NxN right singular vector. SVD vectors have good stability, having algebraic properties and SVD vectors change very little even after major modifications. Thus SVD offers high robustness against geometric attacks. SVD is used in combination with other techniques[6].

Arnold transform is a simple and periodic technique of image scrambling. It restores the image to its original after certain number of iterations. The number of iterations can be used as key. The iterations needed directly proportional to image size[7].

IV. PROPOSED WATERMARKING ALGORITHM

Watermarking system consists of two modules namely- watermark embedding module and watermark extraction/detection module. As RDWT is shift invariant and offer better robustness and good imperceptibility we have used RDWT in this technique. DCT is used because of its energy compaction and robustness against compression attacks. SVD is used because of its stability and robustness against geometric attacks.

A. Watermark embedding Algorithm

It includes following steps-

1) Select Host image of size MxM and split it into RGB channels.
2) Apply 3 level RDWT to the Blue channel as shown in fig. 3.2 The HH2 subband is used for embedding.
3) Then apply DCT to the HH2 sub band.
4) Select watermark image of same size as that of host image and split it into RGB channel repeat steps 1-2 to watermark image.
5) Apply Arnold transform to watermark DCT.
6) Then apply SVD to host image DCT and watermark scrambled image.
7) Embed the singular vectors of watermark with singular vectors of host image by

$$S^* = S + \alpha * S_w \quad (1)$$

where α is embedding factor, S is singular of host image and S_w is singular of watermark image.

8) Apply Inverse DCT and inverse 3-level RDWT.
9) Combine all the colors to get the watermarked image.

B. Watermark Extraction Algorithm

It has following steps-

1) Split the colors of watermarked image, original image and watermark image.
2) Apply 3-level RDWT to the blue channel of watermarked image and original and watermark image.
3) Then apply 3 level RDWT to all the three images.
4) Then apply DCT to HH2 sub band of all three images.
5) Then apply SVD to all 3 images and extract singular values of watermark by

$$S_w = (S^* - S)/\alpha \quad (2)$$

6) Then SVD is reconstructed with watermark singular values.
7) Apply inverse Arnold transform and inverse DCT.
8) Then apply inverse 3 level RDWT is applied to get extracted watermark.
9) Merge all the colors of the extracted watermark.

V. EXPERIMENTS AND RESULTS

In the performed experiments, we have used peppers as cover image and fruits as watermark image of size 515x512. Also baboon and lena of same size are experimented with watermark image of fruits. For performance measurement PSNR and NCC parameters are used.

$$PSNR = 10 \log 10 \left(\frac{MAX(A(i,j))^2}{MSE} \right) \quad (3)$$

Where, NxN is the size of the image, and MSE is the Mean Square Error between the original O (i, j) and the watermarked image WM (i, j), can be written as:

$$MSE = \frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}[\,A(i,j) - W(i,j)\,]^2 \quad (4)$$

To find out the similarity between the original and extracted watermark, normalized correlation coefficient (NCC) is calculated. Its formula is:

$$NC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} W(i,j)\ W^*(i,j)}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N} W(i,j)^2}\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N} W^*(i,j)^2}} \quad (5)$$

Where, W (i, j), W* (i, j) are the original watermark image and the extracted watermark image respectively. NCC is a value between 0 and 1. The larger the NCC value, the higher the watermark robustness and similarly higher the PSNR, higher is the imperceptibility.

Fig. 5.1: (a) Host image(peppers) (b) watermark image(fruits)

Fig.5.2: (a) cover image(lena) (b) cover image(baboon)

The value of embedding factor is taken as 0.05. The tolerance level for NCC is 0.85. If the watermark NCC is greater than tolerance than the image is robust. To check the robustness, various Attacks are performed on watermarked images. The attacks can be geometric attacks, compression attacks, noise attacks. The watermarked image and host image PSNR is equal to 1 and NCC is infinite. Thus imperceptibility is perfect. Also under No attack the PSNR is greater than 65.

Fig. 5.3: watermarked image pepper

The performance results under different attacks are presented in below table-

Table 5.1: PSNR of watermark fruits with different cover images of different intensity

ATTACKS	Baboon	Lena	Peppers
No attack	66.53	66.53	66.53
Speckle noise	51.21	46.81	55.17
Gaussian Noise	43.05	37.99	37.08
Salt & Pepper	49.46	44.77	40.34
Cropping	42.08	54.28	53.77
Rotation	44.15	50.31	56.90
JPEG compression	45.75	49.70	55.44
Blur	34.23	42.20	48.37

Also we have compared our results with similar type of hybrid algorithm of RDWT-DCT-SVD.

Table 5.2: PSNR and NCC comparison with existing proposed RDWT-DCT-SVD hybrid

Attacks	Proposed Method(peppers and fruits)		Previous Work(1-RDWT-DCT-SVD) Based	
	PSNR	NCC	PSNR	NCC
Speckle noise	55.17	0.999	26.91	0.986
Gaussian Noise	37.08	0.999	33.36	0.996
Salt & Pepper	40.34	0.998	24.96	0.978
Cropping	53.77	0.997	45.94	0.999
JPEG	55.44	0.991	48.46	0.999
Blur	48.37	0.990	45.11	0.997

VI. OBSERVATIONS

The results shows that the PSNR lies in the range 35-55 for various types of attacks. Also the NCC is greater than 0.90 against different types of attacks. In case of Gaussian and blur result is almost equal to existing hybrid method.

VII. CONCLUSION

This paper has proposed a hybrid image watermarking algorithm which embeds watermark image of same size as host image. The technique results good PSNR and NCC against different types of attacks and with different types of host images of varying intensity. The technique also provides security to watermark as Arnold transform is used and period is used as the key for Arnold transform. In future this algorithm can be improved further for varying watermark size and for other multimedia types.

REFERENCES

[1] Qureshi, M. A., & Tao, R. (2006). A comprehensive analysis of digital watermarking. Information Technology Journal, 5, 471-475.
[2] Potdar, V. M., Han, S., & Chang, E. (2005, August). A survey of digital image watermarking techniques. In Industrial Informatics, 2005. INDIN'05. 2005 3rd IEEE International Conference on (pp. 709-716). IEEE.
[3] Cox, I. J., Miller, M. L., Bloom, J. A., & Honsinger, C. (2002). Digital watermarking (Vol. 1558607145). San Francisco: Morgan Kaufmann.
[4] Cox, I. J., Kilian, J., Leighton, F. T., & Shamoon, T. (1997). Secure spread spectrum watermarking for multimedia. IEEE transactions on image processing, 6(12), 1673-1687.
[5] Lin, Q., Liu, Z., & Feng, G. DWT based on watermarking algorithm and its implementing with DSP. In 2009 3rd International Conference on Anti-counterfeiting, Security, and Identification in Communication.
[6] Bajaj, A. (2014, August). Robust and reversible digital image watermarking technique based on RDWT-DCT-SVD. In Advances in Engineering and Technology Research (ICAETR), 2014 International Conference on (pp. 1-5). IEEE.
[7] Wang, Y., & Li, T. (2010, October). Study on image encryption algorithm based on arnold transformation and chaotic system. In Intelligent System Design and Engineering Application (ISDEA), 2010 International Conference on (Vol. 2, pp. 449-451). IE