I J C T A, 9(41), 2016, pp. 53-57 ISSN: 0974-5572

DWT, DCT and SVD based Digital Image Watermarking

Manie Kansal, Divya Deora, Harpreet Singh Bedi* and Shekhar Verma

ABSTRACT

Since Internet is a public transmission way and it is widely applied in many applications, we can send and receive digital data, such as images, by connected networks, with the recent growth of communication technologies. However, many new issues such as security of digital information transmission and copyright protection of digital products also emerge in the meantime. A watermarking algorithm consists of the watermark structure, an embedding algorithm, and an extraction or detection algorithm. In this paper, digital image watermarking algorithm based on DWT, DCT and SVD has been proposed in which chaotic system has been applied to watermark image in order to ensure the watermark robustness. Logistic mapping is used to find the hiding position information to extract DC, which are used to construct zeros-watermark. Binary image is selected as watermark image so that the watermarks of existing zeros watermarking algorithm are no longer invisible and meaningless and watermark security is also analyzed. The experimental result based on this algorithm have shown that the watermarking is robust to the common signal processing techniques including JPEG compressing, adding noise, median filter, cropping and so on.

Keywords: DCT, DWT, SVD, PSNR, MSE, NC.

1. INTRODUCTION

One of the biggest technological events of the last two decades was the invasion of digital media in an entire range of everyday life aspects. Digital data can be stored efficiently and with a very high quality, and it can be manipulated very easily using computers. Furthermore, digital data can be transmitted in a fast and inexpensive way through data communication networks without losing quality. Copying is simple with no loss of fidelity and a copy of a digital media is identical to the original. One solution would be to restrict access to the data using some encryption technique. However, encryption does not provide overall protection. Once the encrypted data are decrypted, they can be freely distributed or manipulated. The above problem can be solved by hiding some ownership data into the multimedia data, which can be extracted later to prove the ownership. This idea is implemented in bank currency notes. In bank currency notes, a watermark is embedded which is used to check the originality of the note. The same "watermarking" concept may be used in multimedia digital contents for checking the authenticity of the original content. So, Watermarking is adding "ownership" information[1] in multimedia contents to prove the authenticity. This technology embeds a data, an unperceived digital code, namely the watermark, carrying information about the copyright status of the work to be protected. So embedding of watermark in the host image can be done by using various techniques and also the watermark can be extracted at the other end. Attacks like jpeg compression, noises and filtering etc. are being performed on the watermarked image in order to ensure the robustness and imperceptibility of the algorithm, which can further be measured by performance evaluation parameters like PSNR and NC. Thus, watermarking techniques may be relevant in various application areas including Copyright protection, Copy protection, Temper detection, Fingerprinting etc. On the other hand, information hiding techniques hides the message into a meaningful multimedia data.

* Assistant Professor, Department of Electronics and Communication, Lovely Professional University, Jalandhar, India, *Emails: manie.15692@lpu.co.in, divya.16864@yahoo.co.in, harpreet.17377@lpu.co.in, Shekhar.14572@lpu.co.in*

The requirements for digital watermarks in these scenarios are different, in general. Identification of the origin of content requires the embedding of a single watermark into the content at the source of distribution. To trace illegal copies, a unique watermark is needed based on the location or identity of the recipient in the multimedia network. In both of these applications, non-blind schemes are appropriate as watermark extraction[2] or detection needs to take place in special laboratory environment only when there is a dispute regarding the ownership of content.

2. NEED OF WATERMARKING

Watermarking methods are based on the human visual [3]system in which it cannot be recognized due to tiny difference. In these techniques, the cover-image is used to hide the secret information and the stereo-image is the cover- image with the secret data embedded inside. It hides the secret information in general files secretly first and then transmits these files through network, because they look the same as general files, they can escape from the attention of illegal interceptors easily and therefore the secret information is not easy to be attacked.

3. METHODS USED

The various methods used for watermarking embedding and its extraction are:

3.1. Discrete Wavelet Transform (DWT)

DWT is a partial transform and has the ability to multiscale analysis. The original image[4] is decomposed into four sub-band images by DWT: three high frequency parts (HL, LH and HH, named detail sub-images) and one low frequency part (LL, named approximate sub-image). The detail sub-images contain the fringe information while the approximate sub-image is the convergence of strength of original image. Therefore, watermark is embedded into approximate sub-image to gain a better robustness.

3.2. Discrete Cosine Transform (DCT)

The discrete cosine transform (DCT) helps separate the image into parts (or spectral sub-bands) of differing importance (with respect to the image's visual quality). The DCT is similar to the discrete Fourier transform: it transforms a signal or image from the spatial domain to the frequency domain. It has been widely used because of its good capacity of energy compression[5] and decorrelation. DCT is faster than DFT because its transform kernel is real cosine function while it is complex exponential in DFT.

3.3. Singular Value Decomposition(SVD)

If a *m*n* image is represented as a real matrix *A,* it can be decomposed as:

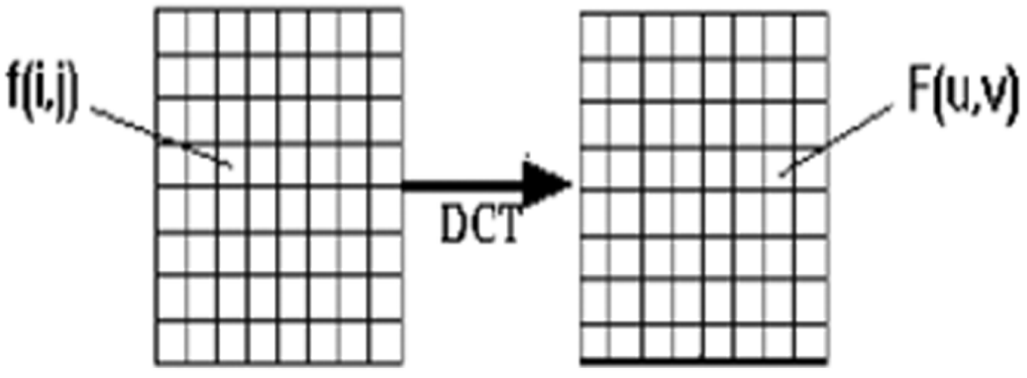

Figure 1: Discrete Cosine Transform of an image

$$A = U\ S\ V^T$$

It is called a singular value decomposition of *A*. Where *U* is a *m*m* unitary matrix, *S* is a *m*n* matrix with nonnegative numbers on the diagonal and zeros on the off diagonal, and V^T denotes the conjugate transpose of *V,* an *n*n* unitary matrix. The nonnegative components of *S* represent the luminance value of the image. Changing them slightly does not affect the image quality and they also don't change much after attacks, watermarking algorithms make use of these two properties.

3.4. Chaos

Watermarks generated using chaotic functions have received increasingly interest recently. Numerous chaotic functions have been studied for this purpose and the generated watermark sequence can be easily controlled in order to create a sequence with particular spectral properties. There are advantages of using these ones over the more common pseudorandom ones. Chaotic system ensures watermark's security.

4. WATEMARKING ALGORITHM

4.1. Watermark Embedding Scheme for Digital Image Watermarking

The embedding process is divided into 6 steps and is briefly described as follows:

1) The cover image of size 512*512 is taken. DWT is applied to decompose it into four sub bands.
2) LL is divided into 8*8 square blocks, DCT is applied to each block, collect the DC value of each DCT coefficient matrix C(m, n) together to get a new matrix D of size 32*32.
3) SVD is applied to D, $D = U1S1V1^T$ to obtain U1, S1 and V1.
4) W of size 32*32 to represent the watermark image is taken. Then modify S1 with W, and apply SVD to it, $S1 + kW = U2S2V2^T$ and obtain U2, S2 and V2.
5) For the coefficient matrix C(m,n) in above step[6], change each DC value to D*(m, n), obtain the new coefficient matrix C*(m,n).
6) Apply chaos key = 0.5 to create a sequence with particular properties so that watermark is in utter confusion.

4.2. Watermark Extraction Scheme for Digital Image Watermarking Using DCT, DWT, SVD.

The extracting process of our method is divided into 4 steps[7] and is briefly described as follows:

1) DWT is applied to I, obtain LL*, HL, LH and HH.
2) Divide LL* into 8*8 square blocks, apply DCT to each block. Collect the DC value to get the 32*32 matrix D**.
3) Apply SVD to D**, $D^{**} = U1^*S2V1^T$, and obtain S2*.
4) Associating S2* with U2, and V2, obtain $E = U2S2V2^T$, in the end we can obtain the watermark according to W* = (1/k)*(E-S).
5) Apply chaotic reverse sequence also in order to extract watermark.

5. EXPERIMENTAL RESULTS

Results with the Arnold transform shows that the algorithm improves the robustness[8]. Also, chaotic system ensures watermark's security. The results are shown below after applying the attacks on the watermarked[9] image.

5.1. Results with Chaotic system

Table 1
Effect of Jpeg Compression on PSNR

Jpeg compression	*PSNR*
10 PER	35.48
20 PER	40.01
30 PER	41.83
40 PER	43.68
50 PER	45.25
60 PER	46.20
70 PER	48.67
80 PER	55.31
90 PER	58.01

Gaussian Noise

Figure 2: Watermarked Image (Gaussian Noise)

Table 2
Effect of Gaussian Noise on PSNR:

Variance	*PSNR*
0.01	29.04
0.02	29.01
0.03	23.45
0.04	22.13

Salt and Pepper Noise

Figure 3: Watermarked Image (Salt and Pepper Noise)

Table 3
Effect of Salt and Pepper Noise on PSNR:

Variance	*PSNR*
0.01	30.45
0.02	28.00
0.03	27.80
0.04	26.89
0.05	25.78
0.06	26.78
0.07	24.00

Gaussian Filter

Table 4
Effect of Gaussian Filter on PSNR:

Size	*k*	*PSNR*
[3 3]	0.6	50.05
[5 5]	0.7	47.78
[7 7]	0.8	44.12

6. CONCLUSION

The algorithm has a good performance on imperceptibility[10] and robustness. It is non-blind watermarking method of which can be used to embed copyright information in the form of a visual watermark. Furthermore, the algorithm is robust to the common image process such as JPEG compression and other attacks like

noise (Gaussian, salt and Pepper) and filters (Gaussian). The PSNR value is very high in case of Jpeg compression

REFERENCES

[1] Kintak U, Shengdun Hu, Dongxu Qi, Zesheng Tang, "A Robust Image Watermarking Algorithm Based On Non-Uniform Rectangular Partition And SVD" Pacific-Asia Conference On Knowledge Engineering And Software Engineering, 2009.

[2] Navas K A , Ajay Mathews Cheriyan , Lekshmi.M, Archana Tampy. S, Sasikumar M, "DWT-DCT-SVD Based Watermarking".

[3] Daxing Zhang, Zhigeng Pan, "A Novel Watermarking Algorithm in DCT Domain to Authenticate Image Content", 2009.

[4] Wang Na, Wang Yunjin, Li Xia, "A Novel Robust Watermarking Algorithm Based On DWT And DCT", International Conference on Computational Intelligence and Security, 2009.

[5] Xianyi Cheng, Liu Ding, Fei Gao, "Adaptive Robust Watermarking Algorithm Based On Dct-Domain", 2009.

[6] Kuang Hang, "Design Of Image Watermarking Algorithm Resistant To Copy Attack", International Conference On Digital Image Processing, ICDIP.2009.93.

[7] Yixin Yan, Wei Cao, Shengming Li, "Block-Based Adaptive Image Watermarking Scheme Using Just Noticeable Difference", International Workshop On Imaging Systems And Techniques, 2009.

[8] Deng Jianghua, "Color Image Digital Watermarking Algorithm Based on Singular Value Decomposition", International Conference on Multimedia Information Networking and Security, 2009.

[9] A. Al–Gindy, H. Al-Ahmad. R. Qahwaji and A. Tawfik, "A High Capacity Digital Watermarking Technique for the Authentication of Colour Images", 2009.

[10] Wei Song**,** Jianjun Hou, Zhaohong Li, Liang Huang, "A novel zero-bit watermarking algorithm based on Logistic chaotic system and singular value decomposition", 2009.