DWT, DCT and SVD Based Digital Image Watermarking

Conference Paper · September 2012

DOI: 10.1109/ICCS.2012.28

Gursharanjeet Singh Kalra
CT Group of Institutions

DWT, DCT and SVD based Digital Image Watermarking

Manie Kansal[1]
Assistant Professor, Department of Electronics and Communication,
Lovely Professional University, Jalandhar,India
manie_kansal27@yahoo.com

Gursharanjeet Singh[2]
Assistant Professor, Department of Electronics and Communication,
Lovely Professional University, Jalandhar,India
gursharanjeet.singh@lpu.co.in

B V Kranthi[3]
Assistant Professor, Department of Electronics and Communication,
Lovely Professional University, Jalandhar,India
bvkranthi@gmail.com

Abstract: **With the rapid development of multimedia and computer technology, images, audio, text and video can be more easily produced, processed as well as stored by digital devices in recent years. To conceal data in transmitting message for preventing the illegal copying or to protect the secret is very important. Data encryption and information hiding schemes are developed to protect the secret data. In this paper, digital image watermarking algorithm based on DWT, DCT and SVD has been proposed in which Arnold transform has been applied to watermark image in order to ensure the watermark robustness. Experimental results show the algorithm is robust to the common image process such as JPEG compression and other attacks like noise and filters.**

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

I. INTRODUCTION

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. At the end of the 20th century, information network technology was widely used all over the world and it was greatly convenient for resource sharing and exchange between people. However, it was followed by many serious problems. However, many new issues such as security of digital information transmission and copyright protection of digital products also emerge in the meantime. How to prevent digital products from copyright infringement, piracy and alteration without permission have become many nations' concerns needing to be resolved urgently. Data encryption methods make the secret data into meaningless bits. On the other hand, information hiding techniques hides the message into a meaningful multimedia data.

Watermarking is the process of embedding data into a multimedia element such as an image, audio or video file for the purpose of authentication . This embedded data can later be extracted from, or detected in, the multimedia for security purposes. A watermarking algorithm consists of the watermark structure, an embedding algorithm, and an extraction or detection algorithm. Watermarks can be embedded in the pixel domain or a transform domain. In multimedia applications, embedded watermarks should be invisible, robust, and have a high capacity. In the classification of watermarking schemes, an important criterion is the type of information needed by the detector. 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 or detection needs to take place in special laboratory environment only when there is a dispute regarding the ownership of content.

II. NEED OF WATERMARKING

Watermarking methods are based on the human visual 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 stego-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.

III. WORKING DOMAINS

Currently, there are two most popular digital watermarking technologies including the Methods in Time Domain and Methods in Transformation Domain. Methods in the former one can be implemented more simply, but the robustness is poorer, while methods in the latter one are more popular with their stronger anti-attack functions. The typical Transformation-Domain Methods are mostly based on the domain of Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT), etc. Recently, some researchers began to make use of Singular Value Decomposition (SVD) to embed a watermark[1]. SVD is a compression technique that can be used in a wide range of applications where data may be organized in a matrix representation. With the increasing use of SVD, the digital watermarking

978-0-7695-4817-3/12 $26.00 © 2012 IEEE
DOI 10.1109/ICCS.2012.28

technology in transform domain has been greatly developed. Based on DWT, DCT and SVD, a new watermarking algorithm for digital image shows that this algorithm combines the advantages of these three transforms. It can satisfy the imperceptibility and robustness very well. Furthermore, the algorithm is robust to the common image process such as JPEG compression, noise, filtering, cutting, rotation, and contrast enhance. Applying the Arnold transform to the watermark improves the robustness greatly. Compared with the SVD and the DCT+SVD algorithms, the proposed algorithm has stronger robustness and faster speed in embedding and extracting. Some works are reported in the frequency domain watermarking using Single Value Decomposition (SVD). The two most commonly used methods are based on DCT-SVD and DWT-SVD. The commonly present disadvantages in traditional watermarking techniques such as inability to withstand attacks are absent in SVD based algorithms. They offer a robust method of watermarking with minimum or no distortion. DCT based watermarking techniques offer compression while DWT based compression offer scalability. Thus all the three desirable properties can be utilized to create a new robust watermarking technique.

The DCT coefficients of the DWT coefficients are used to embed the watermarking information. This method of watermarking is found to be robust and the visual watermark is recoverable without only reasonable amount of distortion even in the case of attacks. Thus the method can be used to embed copyright information in the form of a visual watermark or simple text.

In all frequency domain watermarking schemes, there is a conflict between robustness and transparency. If the watermark is embedded in perceptually most significant components, the scheme would be robust to attacks but the watermark may be difficult to hide. On the other hand, if the watermark is embedded in perceptually insignificant components, it would be easier to hide the watermark but the scheme may be less resilient to attacks. In image watermarking, two distinct approaches have been used to represent the watermark. In the first approach, the watermark is generally represented as a sequence of randomly generated real numbers having a normal distribution with zero mean and unity variance.

IV. METHODS USED

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

A. Discrete Wavelet Transform (DWT)

DWT is a partial transform and has the ability to multiscale analysis. The original image 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. Relative to the detail sub-images, approximate sub-image is much more stable, since the majority of image energy concentrates here. Therefore, watermark is embedded into approximate sub-image to gain a better robustness.

B. 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 and decorrelation. DCT is faster than DFT because its transform kernel is real cosine function while it is complex exponential in DFT.

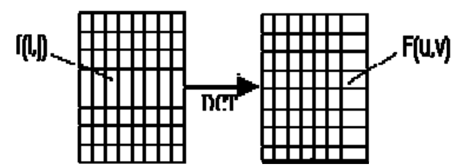

Figure 1. Discrete Cosine Transform of an image

C. Singular Value Decomposition(SVD)

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

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

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.

D. Arnold Transform

Actually, Arnold transform is the position shift of one-to-one point. This transformation can be iterated. Note that, Arnold transform is cyclical, that is, when iterate to certain step, it will get the original image. Dyson and Falk analyzed the cyclicity of discrete Arnold transform and gave the cycle of arbitrary Arnold transform. After been transformed, the image can not be distinguished by eye so that encryption is been implemented, hence it break the correlation between watermarks data and reduce the errors that may be caused in the process of transmission and extraction.

E. 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.

V. WATEMARKING ALGORITHM

A. 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 256*256 sub-bands LL, HL , LH and HH.
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, $D=U_1S_1V_1^T$ to obtain U_1, S_1 and V_1.
4). W of size 32*32 to represent the watermark image is taken. Then modify S_1 with W , and apply SVD to it, $S_1+\alpha W= U_2S_2V_2^T$ and obtain U_2, S_2 and V_2.
5). For the coefficient matrix C(m,n) in above step, change each DC value to D*(m,n), obtain the new coefficient matrix C*(m,n) , and apply inverse DCT to each C*(m,n) to produce the watermarked low frequency band LL* .
6). Apply chaos key = 0.2 to create a sequence with particular properties so that watermark is in utter confusion.
7). Apply inverse DWT to LL* , HL , LH and HH to get the watermarked image I* .

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

The extracting process of our method is divided into 4 steps 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**, $D^{**}=U_1{}^*S_2V_1T$, and obtain $S_2{}^*$.
4). Associating $S_2{}^*$ with U_2, and $V_{2,}$ obtain $E=U_2S_2V_2^T$, in the end we can obtain the watermark according to $W^*=(1/\alpha)^*(E-S)$.
5). Apply chaotic reverse sequence also in order to extract watermark.

VI. EXPERIMENTAL RESULTS

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

A. Results with Arnold Transform

JPEG Compression

Figure 2. Original Image

Figure 3. Watermark [32 32]

Figure 4. Watermarked Image (Jpeg Compression)

TABLE1: EFFECT OF JPEG COMPRESSION ON PSNR

Jpeg compression	PSNR
10 PER	34.48
20 PER	39.20
30 PER	41.83
40 PER	43.68
50 PER	45.25
60 PER	46.67
70 PER	48.67
80 PER	51.31
90 PER	56.01

The plots of Jpeg compression with PSNR is shown:

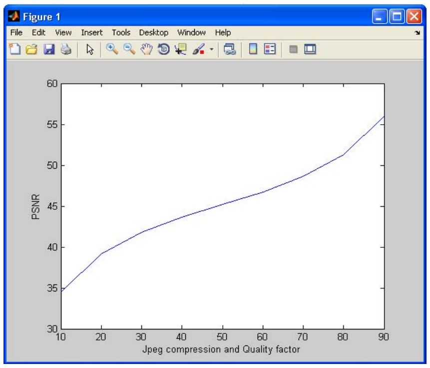

Figure 5. Jpeg compression with PSNR

Gaussian Noise

Figure 6. Watermarked Image(Gaussian Noise)

TABLE 2: EFFECT OF GAUSSIAN NOISE ON PSNR

Variance	PSNR
0.01	28.04
0.02	25.01
0.03	23.33
0.04	22.13

The plots of Gaussian noise with PSNR is shown:

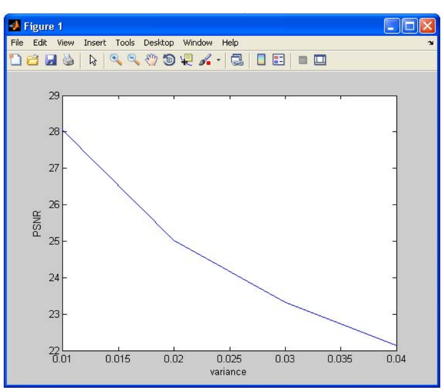

Figure 7. Gaussian Noise with PSNR

Salt and Pepper Noise

Figure 8. Watermarked Image (Salt and Pepper Noise)

TABLE 3: EFFECT OF SALT AND PEPPER NOISE ON PSNR

Variance	PSNR
0.01	33.06
0.02	29.76
0.03	28.06
0.04	26.68
0.05	25.78
0.06	24.95
0.07	24.26

The plots of salt and pepper noise with PSNR is shown:

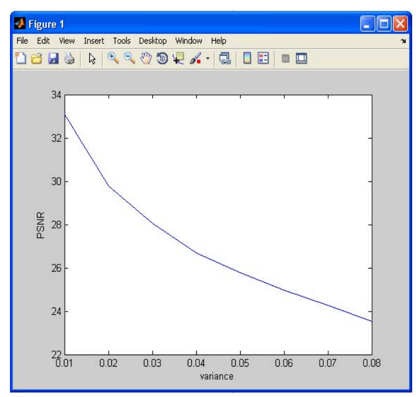

Figure 9. Salt and pepper noise with PSNR

Gaussian Filter

TABLE 4: EFFECT OF GAUSSIAN FILTER ON PSNR

Size	Sigma	PSNR
[3 3]	0.5	49.23
[5 5]	0.6	49.14
[7 7]	0.7	43.21

B. CONCLUSION

The algorithm has a good performance on imperceptibility 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.

Results with the Arnold transform shows that the algorithm improves the robustness greatly as the PSNR value is highest at 90 PER Jpeg compression i.e. 56.01. As the compression factor increases and Quality factor reduces i.e at 10 PER Jpeg compression, the PSNR value is obtained 34.48. Even after the other attacks like noise (Gaussian, salt and Pepper) and filters (Gaussian) the PSNR value is obtained between 22 and 34 which shows the robustness of the algorithm.

Chaotic system ensures watermark's security as the PSNR value at this is 56.05. As the compression factor increases and quality factor reduces i.e at 10 PER Jpeg compression, the PSNR value is obtained 34.48. Even after the other attacks like noise (Gaussian, salt and Pepper) and filters (Gaussian) the PSNR value is obtained between 22 and 34 which shows the watermark's security against the attacks.

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]. Manie Kansal, Gursharanjeet Singh, B V Kranthi, "Digital Image Watermarking Techniques " published at National Conference on "Impact of Management and Technological Advancements in Technical Education and Industrial Sector", JSSIET, Patiala (Pb), India, February 18-19, 2011

[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 DigitalWatermarking Algorithm Based on Singular Value Decomposition", International Conference on Multimedia Information Networking and Security,2009.

[9]. Saraju P. Mohanty, "Digital Watermarking", Indian Institute of Science, Bangalore,1999.

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

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