http://infor.seaninstitute.org/index.php/infokum/index
INFOKUM JOURNAL, Volume10, No.5, December 2022 ISSN : 2302-9706

APPLICATION OF THE COX METHOD TO DIGITAL IMAGES FOR COPYRIGHT PROTECTION

Abdul Sani Sembiring[1], Pandi Barita Nauli Simangunsong[2]

Universitas Budi Darma[1], Politeknik LP3I Medan[2]
gurkiy@gmail.com[2], Simangunsong.pandi@gmail.com[2]

Article Info
Received 16/11/22
Revised 02/12/22
Accepted 08/12/22

Abstract

All these digital products can be downloaded easily. And can be exchanged with services such as e-mail. One way to protect multimedia copyrights is to embed information into the multimedia data (watermarking) as a digital signature of the legal owner of the multimedia product. Thus, the embedded watermark does not damage the protected digital data. So that the person who opens the multimedia product knows about the ownership of the maker. Digital data that will be applied in this research is only data in the form of digital images. Currently there are several watermarking methods that can be applied to digital images, such as: Least Significant Bit Coding, Patchwork (introduced by Bender), Pitas and Kaskalis, Caroni, Cox, Randomly Sequenced Pulse Position Modulated Code (RSPPMC), and others. However, the authors are interested in methods that utilize the characteristics of the Discrete Cosine Transform (DCT).

Keywords: COX Method, Digital Image, Protection, Copyright.

1. INTRODUCTION

One of the protected intellectual works is multimedia. Both in the form of text, music (in MP3 or WAV format), pictures or images, and digital video. So far, the duplication of digital products has been carried out freely and freely. The result of doubling is exactly the same as the result. The copyright holder of the digital product is of course disadvantaged because he does not receive royalties from the copying effort. Copyright abuse in the multimedia field is not only about copying and distributing it, but also about ownership labels. Most of these digital products do not include who the copyright holder is. even if there is proof of ownership, usually the ownership information is included on the cover which explains that the multimedia product belongs to the manufacturer. whereas the current distribution of multimedia products is not only done offline, but can also be done via the internet. On websites on the internet, information can be found in the form of text, images, sound and video. All these digital products can be downloaded easily. And can be exchanged with services such as e-mail. One way to protect multimedia copyrights is to embed information into the multimedia data (watermarking) as a digital signature of the legal owner of the multimedia product. Thus, the embedded watermark does not damage the protected digital data. So that the person who opens the multimedia product knows about the ownership of the maker. On websites on the internet, information can be found in the form of text, images, sound and video. All these digital products can be downloaded easily. And can be exchanged with services such as e-mail. One way to protect multimedia copyrights is to embed information into the multimedia data (watermarking) as a digital signature of the legal owner of the multimedia product. Thus, the embedded

watermark does not damage the protected digital data. So that the person who opens the multimedia product knows about the ownership of the maker. On websites on the internet, information can be found in the form of text, images, sound and video. All these digital products can be downloaded easily. And can be exchanged with services such as e-mail. One way to protect multimedia copyrights is to embed information into the multimedia data (watermarking) as a digital signature of the legal owner of the multimedia product. Thus, the embedded watermark does not damage the protected digital data. So that the person who opens the multimedia product knows about the ownership of the maker. One way to protect multimedia copyrights is to embed information into the multimedia data (watermarking) as a digital signature of the legal owner of the multimedia product. Thus, the embedded watermark does not damage the protected digital data. So that the person who opens the multimedia product knows about the ownership of the maker. One way to protect multimedia copyrights is to embed information into the multimedia data (watermarking) as a digital signature of the legal owner of the multimedia product. Thus, the embedded watermark does not damage the protected digital data. So that the person who opens the multimedia product knows about the ownership of the maker.

Digital data that will be applied in this research is only data in the form of digital images. Currently there are several watermarking methods that can be applied to digital images, such as: Least Significant Bit Coding, Patchwork (introduced by Bender), Pitas and Kaskalis, Caroni, Cox, Randomly Sequenced Pulse Position Modulated Code (RSPPMC), and others. other. However, the authors are interested in methods that utilize the characteristics of the Discrete Cosine Transform (DCT). This is because the change in the DCT value in an image has a smaller effect than the change in the pixel value of the image. The watermarking method that will be used in this research is the Cox method proposed by Ingemar J. Cox, Joe Kilian, Tom Leighton, and Talal Shamoon, because this method utilizes the characteristics of the Discrete Cosine Transform (DCT) in the method of inserting and extracting copyright labels. This method supports robustness to signal operations (such as digital-analog and analog-digital conversion, resampling, requantization, and signal enhancement), robustness to geometric operations (such as rotation, translation, etc.), and resistance to attack (Cox et al. al, 1997).

2. METHODS

2.1 Digital Watermarking

*Digital watermarking*is a technique that allows an individual to add hidden copyright notices or other verification messages to documents or audio, video, or image signals. Watermarks actually first appeared in the form of handmade paper 700 years ago. After the invention, watermarks were widely used throughout Europe.

2.2 Various*Domain*for the Application of Watermarking

*Watermarking*in its application to digital data, it can be applied to various domains. This means that the application of watermarking to digital data such as text, image, video and audio, is carried out directly on the type of digital data (eg for images and video in the spatial domain, and audio in the time domain) or it is first transformed into another domain.

Various transformations are known in digital signal processing such as:

1. FFT (Fast Fourier Transform),
2. DCT (Discrete Cosine Transform),
3. *Wavelet Transform*, etc.

2.3 Discrete Cosine Transform (DCT)

*Watermarking*to digital images can be applied to various domains. There is something that is done directly on these types of digital data or it is first transformed into another domain. One of the transformations used is the Discrete Cosine Transform (DCT) which converts digital data into a frequency domain form.

2.4 Cox's method

This method supports resistance to signal operations (such as digital-analog and analog-digital conversion, resampling, requantization, and signal enhancement), resistance to geometric operations (such as rotation, translation and others) and resistance to attacks.

2.5 Copyright

In Law of the Government of the Republic of Indonesia No. 19 of 2002, copyright (international symbol: ©) is an exclusive right for creators or recipients of rights to announce or reproduce their creations or give permission for it without reducing restrictions according to applicable laws and regulations. Basically, copyright is "the right to copy a work".

3. RESULTS AND DISCUSSION

Problem Analysis

PUnauthorized duplication and distribution creates problems with intellectual property rights (IPR). This problem can be overcome by using digital watermarking. Digital watermarking is a technique for embedding information stating ownership labels (called watermarks) into digital data. Digital watermarking has many applications, including proof of ownership, authentication, copyright protection, fingerprinting and tamper proofing.

The watermarking process in this study was carried out on digital images that became cover images in BMP format but the copyrights that were inserted were text which became watermarks. On each image that becomes the cover, the process of inserting a watermark with a label, namely 'LittleBaby.bmp' in RGB format and text copyright with a value ofαon different Cox methods.

Logo insertion process as*watermark*in the frequency domain using the DCT (Discrete Cosine Transform) transformation. This process is based on the frequency domain, namely by embedding a number of sequences of real numbers along n in the main image.

Watermark Extraction

The watermarked image extraction process aims to detect the presence of copyright in the embedded image and separate the copyright from the image. There are two ways that can be done in this process, namely, extraction without the need for the original image (blind watermarking) and extraction requiring the original original image (non-blind watermarking). In the extraction process that will be carried out, the author will use a non-blind watermarking extraction process. Thus, it is necessary to use the original original image before inserting a copyright which will be useful for comparing changes in the DCT value of the original image with the watermarked image.

Insertion of Copyright

For example, a 24-bit V main image with dimensions of 512 x 512 will be inserted with a copyright in the form of the letter A. The V image will undergo a DCT transformation and the copyright in the form of the letter A will only convert the binary value.

Figure 1. Cover Image

The V image will be divided into several blocks, each block size is 10 x 10. These blocks have 3 color values for RGB. Each block is transformed by DCT using equation 2.1 or Matlab 6.1. Suppose V1 is one of the pixel blocks taken from image V to be transformed by DCT.

$$V1 = \begin{bmatrix} 216 & 212 & 217 & 218 & 218 & 219 & 220 & 221 & 221 & 221 \\ 129 & 124 & 133 & 133 & 134 & 138 & 140 & 142 & 142 & 142 \\ 131 & 137 & 138 & 133 & 134 & 136 & 138 & 139 & 139 & 139 \\ 132 & 139 & 140 & 138 & 140 & 142 & 142 & 142 & 142 & 142 \\ 136 & 142 & 141 & 141 & 145 & 146 & 145 & 143 & 142 & 142 \\ 136 & 139 & 139 & 142 & 145 & 145 & 144 & 144 & 145 & 145 \\ 136 & 138 & 138 & 142 & 142 & 141 & 140 & 143 & 144 & 144 \\ 135 & 136 & 139 & 145 & 144 & 142 & 140 & 140 & 141 & 141 \\ 135 & 132 & 134 & 140 & 140 & 138 & 136 & 134 & 135 & 135 \\ 134 & 126 & 125 & 129 & 127 & 125 & 123 & 122 & 120 & 117 \end{bmatrix}$$

The first is to change the V image and the copyright in the form of the letter A to be binary. The binary value for A is 10000011. Because the number of binary digits for A is only 8 bits, the required number of pixels for the RGB image is 8 bits.

$$V1 = \begin{bmatrix} 216 & 212 & 217 & 218 & 218 & 219 & 220 & 221 & 221 & 221 \\ 129 & 124 & 133 & 133 & 134 & 138 & 140 & 142 & 142 & 142 \end{bmatrix}$$

131	137	138	133	134	136	138	139	139	139
132	139	140	138	140	142	142	142	142	142
136	142	141	141	145	146	145	143	142	142
136	139	139	142	145	145	144	144	145	145
136	138	138	142	142	141	140	143	144	144
135	136	139	145	144	142	140	140	141	141
135	132	134	140	140	138	136	134	135	135
134	126	125	129	127	125	123	122	120	117

Image pixels	Letter A
2 = 00000010	1
1 = 00000001	0
6 = 00000110	0
2 = 00000010	0
1 = 00000001	0
2 = 00000010	0
2 = 00000010	0
1 = 00000001	1

The DCT transformation process for the watermarked image and the original image is carried out the same as the DCT transformation process for the embedding process.

Image pixels		Letter A
2 = 00000010	←	1
1 = 00000001	←	0
6 = 00000110	←	0
2 = 00000010	←	0
1 = 00000001	←	0
2 = 00000010	←	0
2 = 00000010	←	0
1 = 00000001	←	1

So as to produce image pixels as follows:

Changed image pixels

2 = 00000011

1 = 00000000

6 = 00000110

2 = 00000010

1 = 00000000

2 = 00000010

2 = 00000010

1 = 00000001

Overall after inserting the letter A only 4 pixels have changed, so the image changes to:

V1 =

306	202	217	218	218	219	220	221	221	221
129	124	133	133	134	138	140	142	142	142
131	137	138	133	134	136	138	139	139	139
132	139	140	138	140	142	142	142	142	142
136	142	141	141	145	146	145	143	142	142
136	139	139	142	145	145	144	144	145	145
136	138	138	142	142	141	140	143	144	144
135	136	139	145	144	142	140	140	141	141
135	132	134	140	140	138	136	134	135	135
134	126	125	129	127	125	123	122	120	117

It appears that the pixels that change are only ± 1 in intensity, so to the naked eye this doesn't really matter. In addition, not all pixels experience a change in intensity.

After getting the value, each block will be compared. Differences or differences in values will definitely be found in a number of image coefficients because there has been an insertion process. The number of different coefficients, n shows the number of logo bits that have been inserted. If the coefficient of a watermarked image is greater than the coefficient of the original image, then the binary value copyright 1 is inserted into that coefficient which adds to the coefficient of the original image. Conversely, if the coefficient value of the watermarked image is smaller than the coefficient value of the original image, then the coefficient has been inserted with a copyright binary value of 0 and reduced the coefficient value of the original image.

After the n difference in the value of the watermarked image and the original image is obtained, change the value from {0.1} to the binary value {1.1}. If the binary value has been obtained, convert the binary value to a decimal value (RGB value) using the parseInt(Strings) function in Java.

4. CONCLUSIONS

The conclusion of this research is that the Cox method can be applied to digital images in .BMP format. The existence of copyright protection applications, especially digital images, makes it easier for users to secure their copyrights in the form of images

REFERENCE

[1.] Nugroho, R. D. A. (2019). PERANCANGAN APLIKASI STEGANOGRAFI PADA CITRA DIGITAL DENGAN MENGGUNAKAN METODE TWOFISH. Informasi dan Teknologi Ilmiah (INTI), 6(2), 269-274.

[2.] Anugrah, R. (2022). SISTEM PENDUKUNG DIAGNOSA IRIDOLOGI DENGAN MENGGUNAKAN PENGOLAHAN CITRA DIGITAL METODE TRANSFORMASI HOUGH. Insan Pembangunan Sistem Informasi dan Komputer (IPSIKOM), 9(2).

[3.] Anugrah, R. (2020). SISTEM PENDUKUNG DIAGNOSA IRIDOLOGI DENGAN MENGGUNAKAN PENGOLAHAN CITRA DIGITAL METODE SEGMENTASI BERBASIS REGION. Insan Pembangunan Sistem Informasi dan Komputer (IPSIKOM), 8(2).

[4.] Anugrah, R. (2019). Sistem Pendukung Diagnosa Melalui Iris Mata dengan Menggunakan Pengolahan Citra Digital Metode Jarak Euclidean. Insan Pembangunan Sistem Informasi dan Komputer (IPSIKOM), 7(2).

[5.] HAFIZHANA, Y., SAFITRI, I., NOVAMIZANTI, L., & IBRAHIM, N. (2020). Image Watermarking pada Citra Medis menggunakan Compressive Sensing berbasis Stationary Wavelet Transform. ELKOMIKA: Jurnal Teknik Energi Elektrik, Teknik Telekomunikasi, & Teknik Elektronika, 8(1), 43.

[6.] Asroni, O., & Serumena, D. R. (2021). Pengamanan Hak Cipta Citra Digital dengan Teknik Watermarking Menggunakan Metode Hybrid SVD dengan DWT. Jurnal Syntax Admiration, 2(11), 2145-2157.

[7.] Imami, F. S., Putra, R. R. J., & Rahman, E. F. (2019). DIGITAL SIGNATURE MENGGUNAKAN METODE SPREAD SPECTRUM SEBAGAI PERLINDUNGAN HAK CIPTA PADA CITRA DIGITAL MPEG-4. Jurnal Aplikasi dan Teori Ilmu Komputer, 3(1), 35-41.

[8.] WIDIYONO, W., WIBOWO, A. P., & DARMAWAN, A. S. (2021). TEKNIK WATERMARKING MENGGUNAKAN METODE LEAST SIGNIFICANT BIT PADA CITRA UNTUK PERLINDUNGAN HAK CIPTA MOTIF BATIK. Jurnal INSTEK (Informatika Sains dan Teknologi), 6(1), 37-45.

[9.] Ikromina, F. I. (2020). Invisible Watermarking Citra Digital Menggunakan Kombinasi Metode Discrete Cosine Transform Dan Discrete Wavelet Transform. Jurnal Nasional Pendidikan Teknik Informatika: JANAPATI, 8(3), 261-271.

[10.] Malese, L. P. (2021). Penyembunyian Pesan Rahasia Pada Citra Digital Dengan Teknik Steganografi Menggunakan Metode Least Significant Bit (Lsb). Jurnal Ilmiah Wahana Pendidikan, 7(5), 343-354.