Digital Image Watermarking in Color Models Using DCT Transformation

Rastislav HOVANČÁK, Dušan LEVICKÝ

Dept. of Electronics and Multimedia Telecommunications, Technical University of Košice, Park Komenského 13 Košice, Slovak Republic

Rastislav.Hovancaka@tuke.sk, Dusan.Levicky@tuke.sk

Abstract. *In recent years, an access to multimedia data has become much easier due to the rapid growth of the Internet. While this is usually considered an improvement of everyday life, it also makes unauthorized copying and distributing of multimedia data much easier, therefore presenting a challenge in the field of copyright protection. Digital watermarking, which is inserting copyright information into the data, has been proposed to solve the problem. In this paper two original watermarking schemes based on DCT transformation for ownership verification and authentication of color images were proposed. Some color models in process of watermarks embedding and extracting are described too.*

Keywords

Watermark; digital watermarking, watermark embedding and extraction.

1. Introduction

The rapid growth of the Internet increases an access to multimedia data tremendously. Multimedia and computer networking have known rapid development and expansion. These facts, combined with more powerful image processing software present a challenge to copyright protection of multimedia data as unauthorized copying and distributing of digital images, video, etc. also become easier. Watermarking is a potential method for protection of ownership rights on digital data.

Digital watermarking is a concept that emerged in the digital signal processing community in early 1990. It is a process of embedding information directly into the digital data, also called original data, by making small modifications to them. The embedded information is called watermark. Depending on the application, the watermark itself may be a string of characters, a number, an image, a piece of sound, or just a 1-bit piece of information to indicate if the data has been watermarked.

The watermarks can be perceptually visible or invisible. We focus on invisible watermarks in this paper. With the detection/extraction of the watermark from the watermarked data, it has been claimed that digital watermarks can be used to identify the rightful owner, as well as the authenticity of digital data. In general, there are two most common requirements of invisible watermarks. The watermarks should be perceptually invisible, i.e., they should not interfere with the media being protected. They should also be robust to common signal processing and intentional attacks.

Attacks on digital watermarking schemes have two effects: either they reduce the effective channel capacity or fully disable the detection of the embedded watermark. Because it is not possible to enumerate all possible attacks, it is very difficult or even impossible to assess if a given system is robust in the general sense [4].

This paper deals with color image watermarking by using two different methods. Digital watermarks have a form of binary images which are embedded into different color models of original images.

2. Methods of Embedding and Extracting

In digital watermarking many different approaches and techniques for watermarks embedding can be used. A very important technique is digital watermarking based on two-dimensional discrete cosine transformation (2D DCT) [2], [3].

Embedding rules operating in the DCT domain are often more robust to JPEG and MPEG compression, thus the watermark designer can prevent JPEG/MPEG attacks more easily. Watermarking in the DCT domain offers the possibility of direct realization of the embedding operator in the compressed domain in order to minimize the computation time.

In the field of digital watermarking two basic methods are used:

- a method using an original image for the extraction of a watermark from an image under test,
- a method without using an original image for the extraction of a watermark from an image under test.

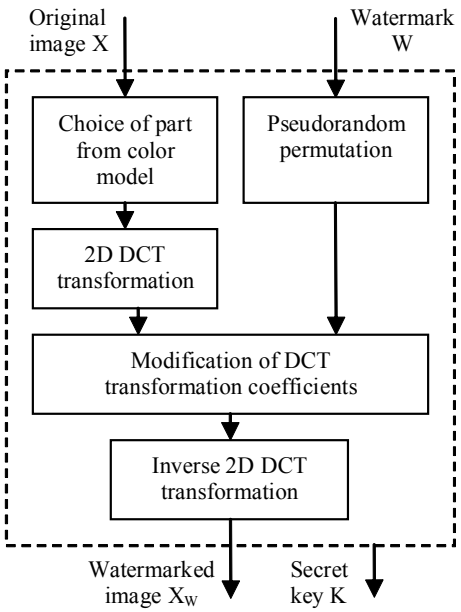

Fig. 1. Embedding process.

In Fig.1 the embedding process which uses both methods is shown. As we can see, the embedding process contains two-dimensional discrete cosine transformation of an original image, permutation of a watermark, modification of transformation coefficients and finally inverse 2D DCT of modified coefficients. Inputs of the embedding process are an original image X of size (N_1xN_2) and a watermark W of size (M_1xM_2). Outputs of this process are a watermarked image X_W with size (N_1xN_2) which is different from the original image and a secret key. The secret key contains information about changed DCT transformation coefficients, permutation random vector, size of watermark etc. Before modification of coefficients, two-dimensional pseudorandom permutation of watermark is used to disperse its spatial relationship. Permutation is used for increasing security for all watermarking method.

2.1 Method 1: DCT Method using an Original Image for Extraction of a Watermark

The original image X is divided into blocks of 8x8, and each block is DCT transformed independently. Only (($64xM_1xM_2$)/(N_1xN_2)) coefficients are selected out of the 64 DCT coefficients for each 8x8 image block. Those selected coefficients are then mapped into reduced image blocks of size (M_1x8/N_1)x(M_2x8/N_2). The coefficients selected from the image of size (N_1xN_2) are collected to compose a reduced block of coefficients. This block has the same size (M_1xM_2) as the binary watermark. We denote watermark's coefficient as $w(x,y)$ and $c(x,y)$ as DCT coefficient. Modified coefficients can be expressed in the form:

$$m(x,y) = c(x,y) + \alpha \quad if \quad w(x,y) = 1, \tag{1}$$

$$m(x,y) = c(x,y) - \alpha \quad if \quad w(x,y) = 0 \tag{2}$$

where α is a real number.

The extracting process is shown in Fig.2. After transformation of the image under test and the original image we compute differences between coefficients as follows:

$$if \quad m(x,y) - d(x,y) \geq 0 \;\Rightarrow\; w'(x,y) = 1, \tag{3}$$

$$if \quad m(x,y) - d(x,y) < 0 \;\Rightarrow\; w'(x,y) = 0 \tag{4}$$

where $m(x,y)$ is a watermarked coefficient, $d(x,y)$ is an original coefficient and $w'(x,y)$ is a coefficient of the extracted watermark.

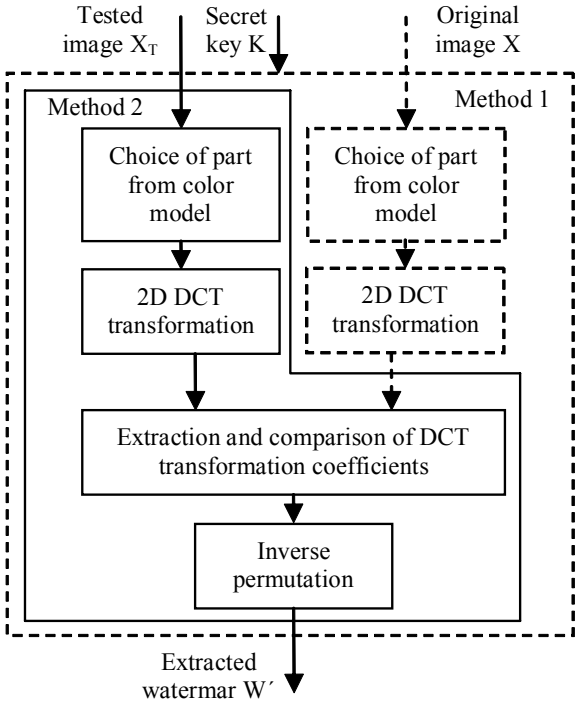

Fig. 2. Extracting process.

2.2 Method 2: DCT Method without Using an Original Image for the Extraction of a Watermark

The method 2 has the main advantage opposite to the Method 1: it doesn't need an original image in extracting process. As is shown in Fig.3, one bit of a watermark for 3 DCT coefficients is used, therefore the number of necessary coefficients from each block of 8x8 DCT coefficients for the whole watermark is 3x(($64xM_1xM_2$)/(N_1xN_2)). Extracted coefficients are compared each other (L-low, M-medium, H-high). It stands to reason, there exist 3^3=27 combinations, but some combinations are not used. All combinations, which represent embedding of a watermark bit 0 or 1 are in Tab.1. The embedding of a watermark means changing an arbitrary combination to the required combination in this method. If the extracted combination doesn't correspond to a combination from Tab.1 we have to change this combination. The embedding process for bit

"0" of a watermark is described in Tab.2. Firstly the extracted combination is compared with combinations representing bit "0" of the watermark, and from this comparison the type (sequence) of choice of DCT coefficients is obtained (Fig.2). Finally extracted coefficients are changed using constant α.

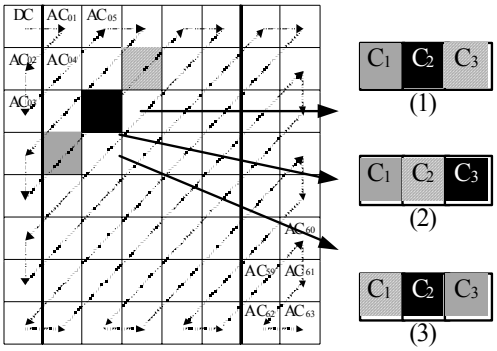

Fig. 3. The choice of DCT coefficients

Bit of watermark	Combinations		
	C_1	C_2	C_3
	L	M	H
0	M	L	H
	L	L	H
	M	H	L
1	H	M	L
	H	H	L

Tab. 1. Combinations represents embedded bit 0 and 1

"0"	Change of combination	Type of choice	C_{W1}	C_{W2}	C_{W3}
1.	LMH	1	C_1-α	C_2	C_3+α
2.	MLM	1	C_1	C_2-α	C_3+α
3.	LLH	1	C_1-α	C_2-α	C_3+α
4.	MHL⇒MLH	2	C_1	C_2+α	C_3-α
5.	HML⇒LMH	3	C_1+α	C_2	C_3-α
6.	HHL⇒HML⇒LMH	3	C_1+α	C_2	C_3-α
7.	MMM⇒LMH	1	C_1-α	C_2	C_3+α
8.	LHL⇒LLH	2	C_1-α	C_2+α	C_3-α
9.	LHH⇒LMH	1	C_1-α	C_2	C_3+α
10.	LHM⇒LMH	2	C_1-α	C_2+α	C_3
11.	HLL⇒LLH	3	C_1+α	C_2-α	C_3-α
12.	HLH⇒MLH	1	C_1	C_2-α	C_3+α
13.	HLM⇒MLH	3	C_1+α	C_2-α	C_3

Tab. 2. The modification of the transformation coefficient if the bit of the watermark is 0

For the extraction of the watermark, at first DCT coefficients using information about the type of choice are extracted. The results of this operation are the combinations (LMH, etc.), which are compared with the combinations from Tab.1. If the extracted combination is identical with one of the first three combinations (for example MLH), then the extracted bit of the watermark is "0". The extracting process for bit "1" is the same. If the extracted combination is not in Tab.1, then the extraction of bit is failed [3], [4].

3. Color Models

In color image processing two basics aspects are important. The first one is a specification of a basic set of colors; the second one is how these basic colors are combined. The two methods of color mixture are known:

- additive color mixture,
- subtractive color mixture.

A set of basic colors, a method of color mixture and rules of alternating color characteristics characterize the color models. In all watermarking methods the following color models are used:

- RGB model (Red, Green, Blue),
- CMY model (Cyan, Magenta, Yellow),
- YUV model (Y-luminance primary, U,V-chrominance primary),
- YCBCR model (Y-luminance primary, CB,CR - blue, red primary).

4. Experimental Results

For our experimental results pictures lenna, montage and camera (256*256*24b) and two digital watermarks (32*32*1b) were used. Four different groups of attacks can be identified: removal attacks, geometrical attacks, cryptographic attacks, and protocol attacks [2]. Watermarked images were tested under some types of attacks, e.g.: increasing and decreasing of brightness, adding noise ("Gaussian", "salt & pepper"), a loss of a part of a watermarked image, JPEG quantization, scaling, rotation, gamma correction, etc.

Primary G from model RGB gives the best results of robustness of extracted watermarks for both methods. Similarly, the best results are obtained if watermarks are embedded to primary M from the color model CMY. The most suitable primary for embedding to the model YUV is primary Y as is shown in Tab. 3.

The method 1 compared with the method 2 has better robustness in most cases because the method 2 in contrast to the method 1 changes three times more coefficients from each block and attacks cause more damages of watermarked images. The results show that luminance primary Y from the color models YUV and primary G from the color model RGB are the best for both methods of color image watermarking from the point of view of robustness to all type of attacks.

Color Model	Primary	Method	Attacks / MSE of extracted watermarks						
			loss ¼ of image	JPEG kvantizat. Q=50	Gamma correction (+0,5)	Gauss.noise mean=0; var.=0,01	'salt & pepper' density=0,05	Scaling (resize to1/2)	Rotation 0,5°
RGB	R	1	**0.1230**	0,0098	0,0068	0,0889	0,1514	0,0410	**0.1279**
		2	0,2578	0,1914	0,0400	0,3330	0,3516	0,1426	0,2139
	G	1	0,1299	**0**	**0**	**0,0811**	**0,1133**	**0,0391**	0,1387
		2	**0,2539**	**0,1240**	**0,0244**	**0,2793**	0,3340	**0,0967**	**0,1738**
	B	1	0,1279	0,3428	0	0,0869	0,1230	0,0449	0,1387
		2	0,2568	0,2275	0,0303	0,3242	**0,3311**	0,1465	0,1982
CMY	C	1	0,1260	0,0039	0,0088	0,0957	0,1387	0,0469	**0,1416**
		2	0,2598	0,1934	0,0430	0,3262	0,3330	0,1348	0,2002
	M	1	0,1240	**0,0010**	**0**	**0,0820**	0,1357	0,0488	0,1465
		2	0,2539	**0,1104**	0,0381	**0,2852**	**0,3066**	**0,1152**	**0,1377**
	Y	1	**0,1230**	0,3379	0	0,0918	**0,1299**	**0,0430**	0,1533
		2	**0,2520**	0,2314	**0,0225**	0,3428	0,3564	0,1309	0,1611
YUV	Y	1	0,1240	**0**	0,0127	0,1455	0,1953	0,1074	0,1904
		2	**0,2559**	**0,1104**	**0,0391**	**0,2510**	**0,2891**	**0,1143**	**0,1768**
	U	1	0,1260	0,5078	**0**	**0,1191**	0,1494	0,0068	0,1035
		2	0,3242	0,3789	0,2646	0,4619	0,4795	0,2197	0,2617
	V	1	**0,1074**	0,4873	0	0,0986	**0,1465**	**0,0029**	**0,0791**
		2	0,3105	0,3770	0,3477	0,4326	0,4863	0,2607	0,2744

Tab. 3. Experimental results

5. Conclusions

In this paper a comparison of two original methods using DCT transformation for the invisible embedding digital watermark into the still color images is presented. Experimental results show that both methods have advantage in few points of view in opposite to other methods. Primary G gives usually the best results from the color model RGB and Y primary from models YUV. Better robustness and effectivity are obtained by using combination of proposed methods i.e. using multiembedding of watermarks or consecutive multiembedding also called hybrid watermarking.

Acknowledgements

The work presented in this paper was supported by the Grant of the Ministry of Education and the Academy of Science of the Slovak Republic VEGA under No. 1/1057/04.

References

[1] LEVICKÝ, D., HOVANČÁK, R., KLENOVIČOVÁ, Z. Digital watermarking. Principles, systems and applications. (in Slovak) *Slaboproudý obzor*, Czech Republic, p. 1-5.

[2] HOVANČÁK, R. DCT Watermarking Algorithm without Using Original Image for Extraction. In *II. PhD conference and ŠVOS*, Košice, 2002, p. 33-34.

[3] HOVANČÁK, R., LEVICKÝ, D. Comparison of watermarking methods using DCT transformation. *RADIOELEKTRONIKA 2003*, 13th International Czech - Slovak Scientific Conference, Brno, Czech Republic, 2003, p. 403-406.

[4] PETITCOLAS, F. A. P., ANDERSON, R. J., KUHN, M. G. Attacks on copyright marking systems. In *Proceedings of the Second International Workshop on Information Hiding.* Portland, 1998, p. 218-238.

About Authors...

Rastislav HOVANČÁK was born in Prešov (Slovak Republic) in 1977. He received the M.S. degree at the Technical University in Košice and now he is PhD. student at the Department of Electronics and Multimedia Communications, Technical University in Košice. His research interests include digital image processing, digital image watermarking and cryptography.

Dušan LEVICKÝ was born in Slanec (Slovak Republic) in 1948. He received the M.S. and PhD. degrees at the Technical University in Košice and now he is professor at the Department of Electronics and Multimedia Communications, Technical University in Košice. His research interests include digital image processing, multimedia communications and cryptography.