IOSR Journal of Electronics & Communication Engineering (IOSR-JECE)
ISSN(e) : 2278-1684 ISSN(p) : 2320-334X, PP 05-09
www.iosrjournals.org

Watermarking Moble Phone Color Images With Error Correction Codes

Praseeja P S[1],Thamizharasi A[2]

[1]*MTech CSE Student,MCET*

[2]*Assistant Professor,CSE,MCET*

ABSTRACT : *This paper proposes a scheme for embedding phone numbers into color images captured by a mobile phone camera. Firstly, the phone number digits are transformed using BCD encoder and the generated binary vector is appended by the phone number checksum represented in binary format. Then, this binary vector is encoded before inserting it in the DCT blocks of the image. The coded watermark information are embedded into a predefined low frequency coefficient in the DCT domain. The proposed algorithm is found to be robust against JPEG compression and different image manipulation algorithms.*

Keywords - *Watermarking, DCT, Error detection, color image, scrambling*

I. INTRODUCTION

Watermark coefficient selection for color images, and the amount of inserted data in a human visual system have problems in robustness and invisibility among watermark requirements. As the technique that inserts watermarks uniformly in every image in different color spaces causes color alterations and image quality deterioration, watermarks should be selectively inserted in visually less sensitive places. In addition, watermark insertion is needed in devices with various features such as computers, PDAs and mobile phones as users want to use multimedia services on those devices. This paper suggests a watermark insertion technique for color images by selecting frequencies to insert watermarks in Y components that correspond to spatial locations, which are less sensitive to chrominance signals, and creating insertion keys that consider properties of frequency coefficients in multi-level structures. Therefore, insertion, invisibility and robustness of watermarks against JPEG compression for multimedia contents in devices with various performances can be guaranteed.

A digital watermark is a technique to hide the information in a multimedia content, in such a way that it is imperceptible to a human observer which is identified by a computer. By this, the watermark is inseparable from the content. This technique was initially used to measure the authenticity in paper and currency. In earlier days encryption is used for data protection. During data transmission, Encryption protects the content. Though, the datum is not protected after receipt and decryption. Watermarking stabilizes encryption.The literature survey reveals that mostly DCT based schemes differ either in these two steps (third and fourth). The remaining steps involves embedding the watermark by modifying the selected coefficients and finally applying inverse DCT transform on each bloc. This paper consists of 4 sections. The new algorithm is discussed in Section 2. Results and comparison with other algorithms are presented in Section 3. Finally, the concluding remarks are introduced in Section 4.

II. THE PROPOSED ALGORITHM

The phone number plus the international country code is used as the watermark. The summation of the decimal digits is added to the number to make it 16 decimal digits. This is useful to check that the extracted number is correct or not. A special procedure is applied if the summation exceeds 99. Its worth mentioning that the maximum summation that can be achieved is 126 when a mobile phone with 14 digits all nines is entered, in such a case the check sum digits as shown in figure 1 will hold 12 and 6 instead of 6 and 3 respectively. Then each one of the 16 decimal digits is converted to a 4 bit binary number. Therefore, we will end up with 64 binary bits. Figure 1shows an example for a UAE mobile number.

In the proposed watermark casting algorithm, the image is partitioned in 8 x 8 pixel blocks similar to the JPEG algorithm. The watermarking algorithm consists of two steps. The first step selects certain blocks according to a Gaussian network. In the selected blocks we modify DCT coefficients such that they full a given constraint. The parameters of the Gaussian functions and of the imposed constraints on the DCT coefficients make up the watermark code. In the detection stage we first check for the DCT constraints and afterwards for the respective block location. The processing blocks for watermark embedding and detection are shown in Figure 2.The DCT block consists of 8×8 coefficients. The 16 lower frequencies are screened to find the coefficient with the highest magnitude and register its location. This process is repeated for all DCT blocks. The location which is repeated more is selected. This location will vary from one image to another according to the spatial frequency contents of the image. One binary bit of the watermark will be embedded in this location. A flow graph of the DCT coefficients selection (DCS) process is shown in figure 3.

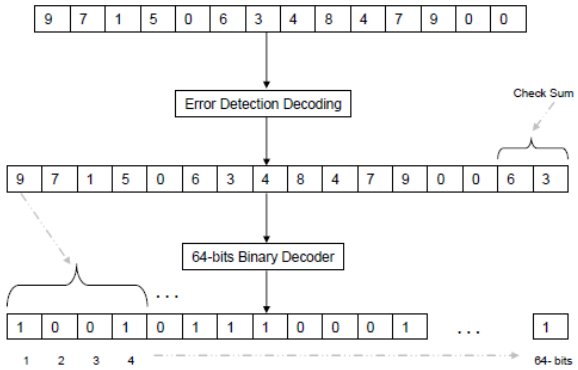

Figure 1 Phone number encoder

2.1 The Embedding Process

The proposed watermarking scheme is based on the possibility of embedding multi copies of the binary watermark (i.e. 64 bits) in the host image. Let us assume that $f(i, j)$ is the host image of size h Z pixels and let $w(i, j)$ be the binary phone digits of size w Z bits which is usually much smaller in size compared to the size of the host image. For simplicity, let us assume that the host image size could accommodate integer copies of the watermark image. The watermark is converted to 1D vector and the host image is divided to HB N no overlapping 8×8 sub-blocks. The number of watermark copies n that can be embedded in the host image is given

$$n = N_{HB} / N_{wB} \qquad (1)$$

Where N_{wB} is the number of the watermark bits.

The binary mobile number digits are randomly scrambled using a secret key. This scrambling process is essential to reduce the spatial correlation between the host image and the embedded watermark. After the scrambling process, the shuffle scheme is applied for each copy of the binary mobile number to shift the binary digits before the embedding process. The shift operation is carried out in a cyclic way. The number of shifted watermark bits depends on the host image size and the watermark size. It can be calculated as follows:

$$W_{SB} = Z_w/n \qquad (2)$$

Where W_{SB} is the number of shifted watermark bits.The frequency component $F(2,1)$ is used to embed only one bit. Since it is a low frequency component it will survive most of the attacks on high frequency components such as JPEG attack or low pass filtering. Standard images with 512x512 pixels were used to test the algorithm therefore only 64x64 bits can be embedded.Finally individual insertion of the binary mobile phone digits is applied into the host image using the embedding equation as follows:

$F_1(i,j)=DCT\{f_1(m,n)\}; \quad 1 \le l \le N_{HB}$

If $(w(i,j)==1)$

$$\text{If} \left[\text{mod} \left[\text{round} \left[\frac{F_1(2,1)}{\Delta} \right], 2 \right] == 1 \right]$$

$F_1(2,1)= F_1(2,1)+ \Delta$

Else $F_1(2,1)= F_1(2,1)$

$$\text{else if} \left[\text{mod} \left[\text{round} \left[\frac{F_1(2,1)_l}{\Delta} \right], 2 \right] == 1 \right]$$

$F_1(2,1)= F_1(2,1)$

else $F_1(2,1)= F_1(2,1)+ \Delta$

Where $1 \le x, y \le 1$, and *Qe* is the quantization to the nearest even number and *Qo* is the quantization to the nearest odd number, Δ is a scaling quantity and it is also the quantization step used to quantize either to an even or an odd number. All the previous watermarking steps are described graphically in the diagram as shown in Figure 2. It is important to note that the watermark is embedded several times in the host image depending on the sizes of the host image and the watermark image.

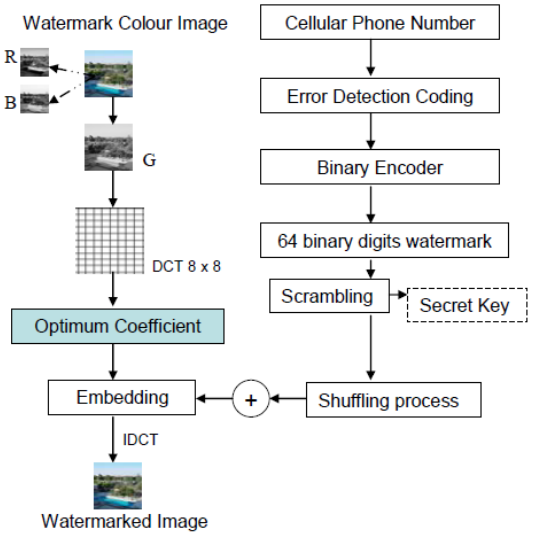

Figure 2 Graphical illustration of the embedding process

2.2 The Extraction process

The embedded watermarks information can be extracted by performing 8×8 DCT transform for the G channel of the watermarked host image and then indicating the same coefficient of the host image that carries the bits of the embedded watermarks using the required secret key. It is worth mentioning that although the proposed scheme is blind, it requires information such as the sizes of both the host and watermark images and the watermark embedding strength Δ. The extraction formula defined in equation is used to produce the scrambled watermark. According to the key in the initial scrambling operation, the scrambled watermark is descrambled to retrieve the original watermark. A reverse shuffling process is implemented for each reconstructed watermark. Simply, the recovery function is the inverse of all the watermarking embedding steps. Each predefined frequency coefficient is quantized by Δ and rounded to the nearest integer. The extracted formula is defined as follows:

If $Q(F_k(x,y)/\Delta)$ is odd then w(I,j)=0

If $Q(F_k(x,y)/\Delta)$ is odd then w(I,j)=1

Where Q is rounded to the nearest integer

. Δ has a value that is equal to the value used for the embedding process. The averaging process has managed to reduce the error of the extracted watermarks. A visual representation for the extraction process is shown in Figure 3.

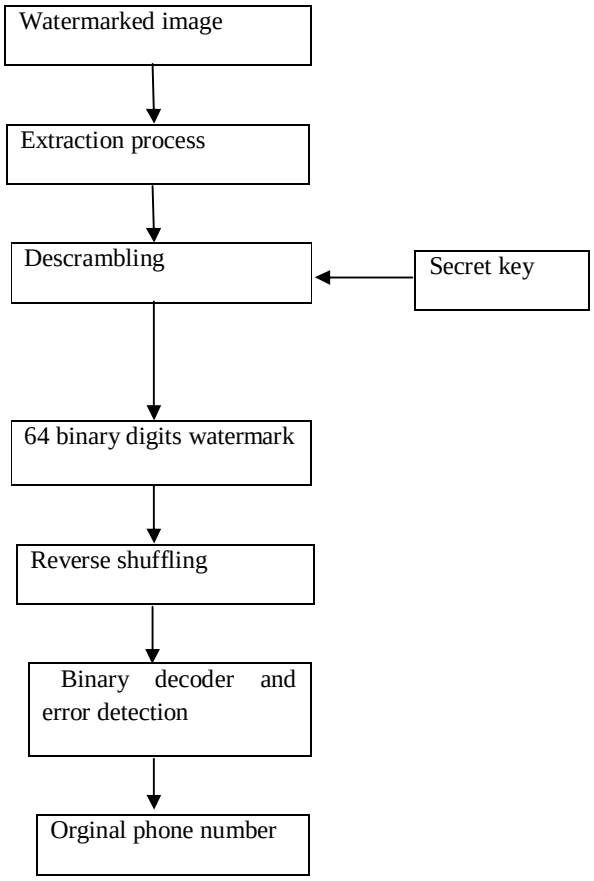

Figure 3 Graphical representation for extraction steps

III CONCLUSION

This paper suggests a secure blind watermarking algorithm of colour images using mobile numbers. A DCT coefficient selection (DCS) process has been applied to increase the invisibility qualities, this process managed to find the coefficient with the maximum magnitude. Different embedding location depending on the spatial frequencies of the host image was selected. The proposed algorithm is robust.

REFERENCES

[1] S. Katzenbeisser and F. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking. London: Artech House,2000.

[2] COX I. J., MILLER M., BLOOM J.: Digital Watermarking. Morgan-Kaufmann, 2002. 4] K. Krasavin, J. Parkkinen, and T. Jaaskelainen, "Digital watermarking on mobile devices," in International Conference on Information and Communication Technologies: From Theory to Applications, Damascus, Syria, 2004, pp. 319-320.

[5] PETITCOLAS F., KUHN M.: Information hiding: A survey.IEEE Special Issue on the Protection of Multimedia Content87, 7 (July 1999), 1062–1077.

[6] J.-S. Sohn, S.-l. Lee, and D.-G. Kim, "Image adaptive watermarking technique for digital phone," in International Conference on Computational Intelligence and Security, Guangzhou, China, 2006, pp.1190 - 1194.

[7] A. Al-Gindy, H. Al-Ahmad, R. Qahwaji & A. Tawfik, “A new watermarking scheme for colour images captured by mobile phonecameras,” International Journal of Computer Science.