Int. J. Electron. Commun. (AEÜ) 69 (2015) 1074–1084

Contents lists available at ScienceDirect

International Journal of Electronics and Communications (AEÜ)

journal homepage: www.elsevier.com/locate/aeue

QR code based blind digital image watermarking with attack detection code

Pillai Praveen Thulasidharan*, Madhu S. Nair

Department of Computer Science, University of Kerala, Kariavattom, Thiruvananthapuram 695581, Kerala, India

ARTICLE INFO

Article history:
Received 29 October 2013
Accepted 31 March 2015

Keywords:
Blind watermarking
QR code
Data hiding
Distortion detection
Image registry code

ABSTRACT

A QR code based blind digital image watermarking technique with an attack detection feature is described here. The technique describes a key based framework to incorporate image, server port address or website address as watermark data; which increases the extended usability of the embedded data and the adaptability of the verification application. The watermarking problem is formulated as a signal communication problem with watermark data representation, embedding of watermark and attack detection as a source encoding, channel encoding and attenuation detection problems respectively. The mathematical aspects of the respective signal processing problems are extended to digital image watermarking with sufficient background support. The use of QR code ensures extended usability, while the application specific watermark data achieves adaptability of the verification application. The QR code is embedded into the attack resistant HH component of 1st level DWT domain of the cover image and to detect malicious interference by an attacker, a unique image registry code generated from the high frequency structural components of the stego-image is used. The key based approach and the attack resistant embedding domain makes this method robust against visually invariant attacks. The testing results show the compliance of the method with all the proposed aspects.

1. Introduction

Watermarking is a form of Steganography, which uses information hiding techniques as a means to protect the ownership of a digital document; commonly referred as copyright protection in today's digital world. In the study of watermarking, digital image watermarking finds a significant place owing to the challenges encountered in efficiently representing the watermark data on a size limited, noise sensitive and tightly bounded data domain represented by the image intensity values. Image watermarking procedure begins by embedding some secret information by the owner into the original image, which is retrieved at the receiver for owner identification or verification. The main focus is on imparting minimal image perceptual distortion and protecting the embedded data from deliberate data removal attacks. [1–4] have given a detailed study on the types of watermarking, embedding techniques, attacks and the counter measures that can be deployed to minimize the attack impact. These techniques rely on the statistical information within the image representation, viz. spatial [Least Significant Bit (LSB)] and frequency domain [Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT)] of the original image for watermarking. Some of the domain specific watermarking techniques have been described in [5–7]; however none of the techniques cover the entire watermarking problem domain nor discuss the extended usability of the extracted data. They attempt to find optimal balanced values for robustness, invisibility and embedding capacity, which are considered to be the three mutually orthogonal [2] performance features of the watermarking problem illustrated in Fig. 1.

Theoretically, Moulin and O'Sullivan [8] formulated watermarking as a communication problem with certain side information at both the encoder and decoder. They proposed a mathematical model for watermarking as depicted in Fig. 2, and formulated an upper bound hiding capacity. They suggested that hiding capacity is a game between the hider and the attacker; the optimal hiding strategy is the solution to a channel coding problem whereas the optimal attack strategy is the solution to a particular rate-distortion problem. In image watermarking the optimal solution to a rate distortion problem would be the maximum distortion (increase or decrease in pixel values) that can be applied to the stego-image (original image with hidden data) such that the cover-image (original image without hidden data) can be approximately reproduced without much perceptual variation, i.e. the attacker

* Corresponding author. Tel.: +91 9745329961.
E-mail addresses: praveentpillai@gmail.com (P.P. Thulasidharan), madhu_s_nair2001@yahoo.com (M.S. Nair).

http://dx.doi.org/10.1016/j.aeue.2015.03.007
1434-8411/

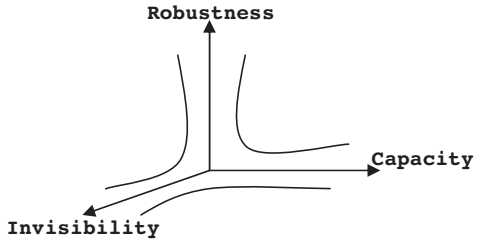

Fig. 1. Tradeoffs between robustness, invisibility and capacity.

tries to maintain the perceptual quality while removing the hidden data to disguise his attack and make it effective. This concludes that the attacks such as cropping, noise addition and geometrical distortion that would affect the perceptual features can be given the least importance in the design of watermarking techniques with more emphasis on increasing the usability information within the watermark data. As opposed to these facts, most of the work in this area focus either on a specific type of watermark data or a particular embedding scheme with much less focus on the adaptability of the watermark technique to different forms of data or application.

In this paper, we present a novel watermarking technique which introduces some new conceptual ideas toward watermark data representation and attack detection for digital image watermarking. At present there are not any known standard techniques which deploy the same concepts for digital image watermarking. The proposed technique enables to represent the watermark data in an adaptive manner and thereby creates a framework which can be easily integrated into any sort of application structure for automated accomplishment of tasks. This framework can be described as a key based blind watermarking method which emphasis on the watermark data representation that results in more information representation with minimal encoding overhead and the extended usability of the extracted data by other application technologies. To attain this we formulate the watermarking problem as a communication problem with watermarking data representation as a sub-problem called source encoding. QR Code, a matrix coding scheme is used for watermark data representation and the DWT domain of the image as the data carrier domain which can sustain most of the attacks. For the detection of malicious interference by an attacker we use a key based image registry code derived from the attack sensitive features of the watermarked image. The key based approach and the DWT domain features makes this technique robust against most of the visually invariant attacks discussed in [4]. Section 2 describes watermarking as a communication problem and Section 3 gives a detailed description about the method, followed by the results and other discussions.

2. Watermarking as a communication problem

Communication in general can be viewed as the delivery of any sort of information from one point to another through a medium. In signal processing, communication is a result of two processes viz. source encoding; determining the representation form of the sender's data and channel encoding; determining the representation form of the carrier signal to include the encoded sender's data. A simple instance of this is the representation of data as 0's and 1's (source encoding) and representation of these bits by a low and high voltage over a conductor (channel encoding). When we extend this perspective to digital image watermarking; the process can be viewed as a communication problem where the watermark data can be considered as the sender's data represented by a source encoding process and the cover image as the communication channel into which the watermark data is embedded using channel encoding methods. Both the encoding processes should ensure error free reproduction of the source data at the receiver end even in the presence of noise. The re-construction of the source data is achieved by applying the reverse form of the channel and source encoding processes in sequence. In case of attenuation of signal during electrical transmission, certain types of signal boosters designed considering the basic properties of the transmitted signal is used to regenerate the signal; which facilitates in the recovery of transmitted information (to some extend). To extend this concept to digital watermarking process, we design an image code describing the basic structural aspects of the stego-image, which is known to the decoder as side information and can be used to determine any attenuation to the image due to transmission errors or deliberate attacks. Based on the analysis of the image code corrective measures can be applied to recover the watermark data. However we limit our discussion up-to construction of the image code; its analysis and corrective strategies can be considered as a further area of research. The following sections describe the mathematical and other parameter selection aspects of the different processes with respect to watermarking process.

2.1. Source encoding

Source encoding process consists of a generator which at a given time 't', generates a character sequence from an alphabet '$\sum$'; which are then encoded by the encoder into another sequence of characters from the alphabet '£'. Mathematically we represent the generator and encoder by two functions $S(t)$ and $F(X)$ respectively, where the output of $S(t)$ is the input to $F(X)$. $S(t)$ generates a character sequence 'X' (Eq. (1)) independent of any factors and is assumed to follow an Independent and Identical Probability distribution model. On the other hand, $F(X)$ generates a character sequence 'Y' (Eq. (2)) from £ depending on X.

$$S(t) : \sum^{*} \rightarrow X \tag{1}$$

$$F(X) : £^{*} \rightarrow Y \tag{2}$$

$F(X)$ defines the representation form of the source data and uses two strategies for this purpose; constructing Y either with fewer characters than X or having some additional error correction characters using which we can recover X during transmission errors. Representing X with fewer bits is a part of data compression theory governed by Shannon's information entropy equation $-P_i \log(P_i)$,

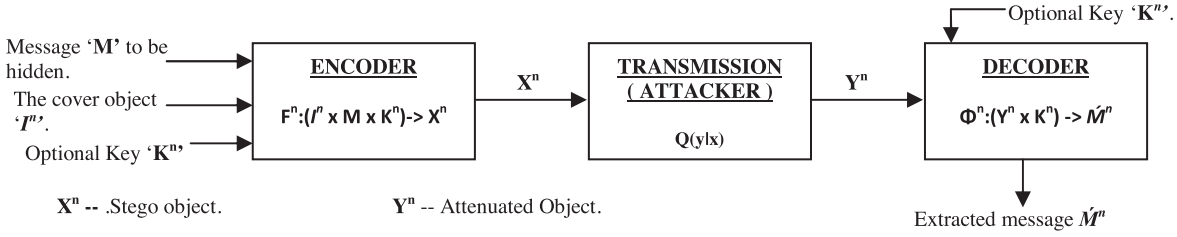

Fig. 2. Watermarking as a communication problem as proposed in [8].