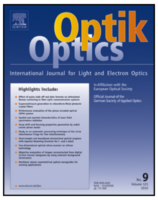
Optik 125 (2014) 2918–2922

Contents lists available at ScienceDirect

Optik

journal homepage: www.elsevier.de/ijleo



# Demosaicking authentication codes using adaptive step via color difference estimation

Guorui Feng*, Zifeng Zuo, Haiyan Zhang

*School of Communication and Information Engineering, Shanghai University, Shanghai 200444, China*

ARTICLE INFO

*Article history:*
Received 21 June 2013
Accepted 1 December 2013

*Keywords:*
Color filter array
Data hiding
Pseudo host
Edge-sensinginterpolation
Color difference

ABSTRACT

In this paper, data hiding is used for raw images instead of the full-resolution color version. Among various color filter array patterns, we choose the most popular Bayer pattern and cover authentication codes in the pseudo host from original sampling in terms of high correlation within red, blue and green channels. pseudo host is based on a transient image that is created by interpolating in this pattern by selecting the key. This procedure confirms the security, in the meantime, and less brings the artifact of embedding codes. This process exploits spatial correlations both red and blue channel to adaptively tune quantization scale parameter and suppresses visual distortion. Core structure presents a watermarking to jointly resist to demosaicking and JPEG compression approach. It can carry visual distortion as small as possible. The simulations test the robustness and transparency after some demosaicking methods and JPEG compression. These results imply that hiding data accompany with less demosaicking traces and the better robustness via various demosaicking methods.

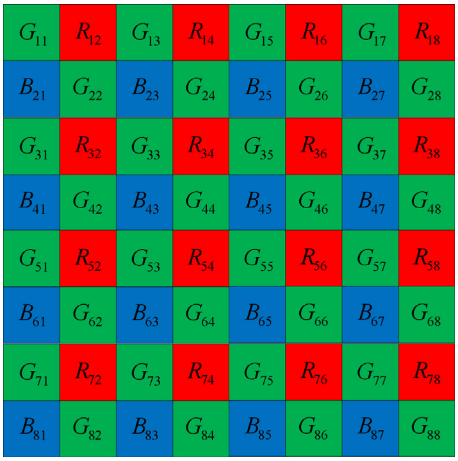
## 1. Introduction

In many consumer electronics systems, digital imaging devices have widely been embedded instead of film cameras for capturing and processing the digital image to provide the user with a viewable image [1]. A full-color image is usually composed of three color planes, accordingly, these information are desired from three separate sensors to measure an image, but to reduce the cost, a usual approach choose only sensor to receive different color components. Meanwhile, the step of imaging is the exposure of sensor, i.e. the light reaches the sensor through the camera optical system via the predefined instrument. It achieves the conversion from optical to digital representation using a sensor. The majority of these digital devices use monochromatic sensors covered with a color filter array (CFA). Fig. 1 shows the most widely used Bayer CFA pattern. The sensor allows only one color to be measured each pixel. It is necessary to estimate two missing color values each pixel, and the process was called CFA interpolation or demosaicking [5]. High correlation between all pairs of primary color channels measured over benchmark images indicates a commonly exploited property to devise the interpolation method. This interpolation process is known as color demosaicking. Recently, multiple demosaicking algorithms were reported in refs. [5,8–11].

As mentioned before, the authentication security of color images pictures plays an important role in images released. It can tolerate acceptable data manipulations by authentication codes. Unfortunately, color authentication cannot be considered as a simple RGB decomposition because of imaging from CFA widely used. For the sake, camera raw image should be separately considered aiming to content security. An early result was suggested by embedding visible watermarks at CFA data acquisition level [2]. This approach embedded in CFA is considered with direct spread spectrum (DSSS), derived from enhanced secure features of raw images. Post-processing images are easily available for the storage or distribution. After down-filtering, the watermark embedded in the low-resolution raw data led to better performance at the cost of the complex implementation [3,12]. This scheme allowed the watermarking information survive to the demosaicking and postprocessing pipeline of the camera. In nature, this type of watermarking scheme was called 1-bit watermark and only denotes the presence (and a 0 the absence) of a watermark. Another technique for combined demosaicking and watermarking in a digital camera pipeline was also presented in [13]. It ignored the impact of JPEG compression. Despite a variety of applications, the essential attributes were relatively featured as: transparency, payload, robustness, security, detectability [4]. In these attributes, the perceptual measure was more emphasized since the effect of

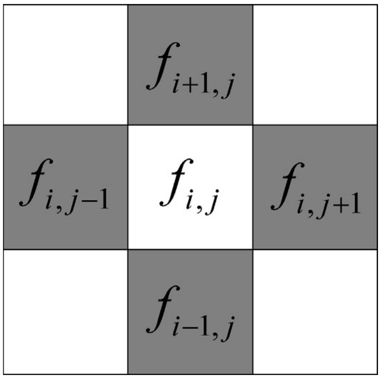
* Corresponding author.
*E-mail addresses:* fgr2082@aliyun.com, fgr2082@yahoo.com.cn (G. Feng).

http://dx.doi.org/10.1016/j.ijleo.2013.12.084
0030-4026/© 2014 Elsevier GmbH. All rights reserved.



| | | | | | | | |
|---|---|---|---|---|---|---|---|
| $G_{11}$ | $R_{12}$ | $G_{13}$ | $R_{14}$ | $G_{15}$ | $R_{16}$ | $G_{17}$ | $R_{18}$ |
| $B_{21}$ | $G_{22}$ | $B_{23}$ | $G_{24}$ | $B_{25}$ | $G_{26}$ | $B_{27}$ | $G_{28}$ |
| $G_{31}$ | $R_{32}$ | $G_{33}$ | $R_{34}$ | $G_{35}$ | $R_{36}$ | $G_{37}$ | $R_{38}$ |
| $B_{41}$ | $G_{42}$ | $B_{43}$ | $G_{44}$ | $B_{45}$ | $G_{46}$ | $B_{47}$ | $G_{48}$ |
| $G_{51}$ | $R_{52}$ | $G_{53}$ | $R_{54}$ | $G_{55}$ | $R_{56}$ | $G_{57}$ | $R_{58}$ |
| $B_{61}$ | $G_{62}$ | $B_{63}$ | $G_{64}$ | $B_{65}$ | $G_{66}$ | $B_{67}$ | $G_{68}$ |
| $G_{71}$ | $R_{72}$ | $G_{73}$ | $R_{74}$ | $G_{75}$ | $R_{76}$ | $G_{77}$ | $R_{78}$ |
| $B_{81}$ | $G_{82}$ | $B_{83}$ | $G_{84}$ | $B_{85}$ | $G_{86}$ | $B_{87}$ | $G_{88}$ |

**Fig. 1.** Bayer sample pattern. (For interpretation of the references to color in the text, the reader is referred to the web version of this article.)



| | | |
|---|---|---|
| | $f_{i+1,j}$ | |
| $f_{i,j-1}$ | $f_{i,j}$ | $f_{i,j+1}$ |
| | $f_{i-1,j}$ | |

**Fig. 2.** Local interpolation structure.

demosaicking process. The aforementioned methods were absent of some key attributes to fit for certain applications.

This paper provides a type of mechanism that content authentication can be detected when the received multimedia signal suffer demosaicking and JPEG compression. It generates a slight difference from original version. We propose a set of securely pseudo-host scheme using in the non-overlapped block of the host after the local map. This quantization-based watermarking can adaptively tuning the step by means of the estimation between red and blue component spectral. The security of whole scheme is supported by the high correlation of sampled levels, which is controlled by the key. The rest of manuscript is organized as follows. Section 2 describes the related background of a kind of pseudo host generated. The detailed transfom-domain watermaking algorithm is presented in Section 2.4. As a special issue, adaptive quantizer scale parameter will be highlighted. The experimental results and conclusion are drawn in Section 3 and Section 4, respectively.

## 2. CFA data hiding

By far, information hiding may be mainly divided into spatial and transform domain algorithms. The mechanism devises over the pseudo host by the key, but neither runs over the CFA sample pattern directly. This model can confirm the security. Because attackers have not known the main body of schemes, this algorithm satisfies the Kerckhoffs principle of the cryptography.

### 2.1. Security mechanism

In this section, a secure watermarking framework is briefly introduced. Accordingly, the mathematical expression during the watermarking embedding phase is defined by

$$F_w = E(F, W, K), \qquad (1)$$

where $F_w$ is the watermarked image, $W$ denotes watermarking information and $K$ is the key. Many transform-domain methods ignore the security. Their security of whole scheme is supported by encrypting watermarking bits instead of encrypting the embedding algorithm. At this time, the equation mentioned becomes

$$F_w = E(F, \hat{W}), \qquad (2)$$

where $\hat{W} = S(F, W, K)$. The proposed method overcomes this obviously drawback. The main body of the technique satisfies Kerckhoffs principle. The decrypting party must have access to the private key associated with the same key utilized to encrypt the body of this algorithm. It aims to avoid potential malicious process and improves the system scalability. The inverse process deals with the extraction of useful data.

$$(F, \tilde{W}) = D(F_w, K). \qquad (3)$$

It is desired that $\tilde{W} = W$. To say the least, $\tilde{W} \approx W$.

### 2.2. CFA pseudo-host pattern

In order to recover missing samples of the CFA, a color demosaicking algorithm has to rely on some additional statistical properties about input color signals. In our approach, we propose a pseudo-host-based embedding algorithm to enable the platform to cover hiding information. First of all, we assume that the sampling gray values are the corresponding the green, red and blue components of the CFA pattern. The gray image from Bayer pattern can be generated using edge-sensing interpolation. Like downsample pattern in four subimages [6], CFA pattern can also treated as a specific downsample model.

To carry out precise measurement of each pixel, adaptively tuning weight parameters system becomes more and more important. Next section presents a flexible and valid method for calibrating system interpolation parameters, which overcomes difficulty of traditional fixed weighting methods. According to real values of surrounding pending point as a reference framework, the relative orientation and position can be quickly determined with constraint of the similar features through simple algebraic algorithm.

In general, we assume $\tilde{f}_{i,j} = \sum_k w_k f(x_k)$, where $f_k$ is in the neighborhood of $f_{i,j}$ and $w_k$ is the weight shown in Fig. 2. A reasonable assumption is that $w_k$ is smaller when $f_k$ has more difference with $f_l (l \neq k)$. In [14], the edge sensing weight coefficients utilized in each above sub-procedure. For convenience sake of the formula, we re-demonstrate new four weights $w_k$, $(k = 1, 2, 3, 4)$ regardless which image area it is as following, i.e.

$$w_k = \frac{u_k}{\sum_{l=1}^{4} u_l}, (k = 1, 2, 3, 4) \qquad (4)$$

$$u_k = \left(1 + \exp\left(\sum_{l=1}^{4} |f(x_k) - f(x_l)|\right)\right)^{-\tau}, (k = 1, 2, 3, 4) \qquad (5)$$

where $x_1 = x_{i,j-1}$, $x_2 = x_{i-1,j}$, $x_3 = x_{i,j+1}$, $x_1 = x_{i+1,j}$.

Note that $\tau$ can control weighting effect of the membership function and be set the key. For an outlying value $x_k (k = 1, 2, 3, 4)$ that is highly dissimilar to the rest of the values, the aggregate distance will approach infinity and the corresponding $\mu_i$ will close to zero. Note that the pixel's contribution to itself is zero. This method preserves edge-information by calculating the trend of near pixels.