ARTICLE IN PRESS

Information Sciences xxx (2014) xxx–xxx

Contents lists available at ScienceDirect

Information Sciences

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

Data hiding method in binary images based on block masking for key authentication

Ki-Hyun Jung [a,1], Kee-Young Yoo [b,*]

[a] School of Computer Information, Yeungjin College, 35 Bokhyun-Ro, Buk-Gu, Daegu 702-721, Republic of Korea
[b] School of Computer Science and Engineering, Kyungpook National University, 80 Daehak-Ro, Buk-Gu, Daegu 702-701, Republic of Korea

ARTICLE INFO

Article history:
Received 3 March 2008
Received in revised form 1 June 2011
Accepted 4 February 2014
Available online xxxx

Keywords:
Data hiding
Block masking
Digital watermark
Key authentication

ABSTRACT

This paper proposes a new data hiding method for binary images that relies on block masking to distribute keys to two parts and then authenticates the right authorized part. The proposed method divides a cover image into small sub-blocks and designs key pairs that determine both where the bit is to be embedded and whether it is possible to embed it there. Furthermore, the key pairs are required to extract the secret data from the stego-image. Experimental results demonstrate a higher capacity and less distortion compared with previous methods since almost all data are hidden in the edge areas.

1. Introduction

Digital watermarking and data hiding techniques have attracted considerable attention from the viewpoint of applications to copyright protection, copy control, annotation, and authentication in order to keep up with the continued proliferation of digital media, including images, audio, and video. A general data hiding system does not require any information is required to initiate the communication process. The security of such a system thus depends entirely on its secrecy. Fundamentally, then this is not a truly secure practice because it violates Kerckhoffs' principle [1]. Therefore, the security of a data hiding system should rely on some secret information exchanged between the sender and receiver, such as a stego-key. Without knowledge of this key, no one should be able to extract secret data from a stego-image.

Many data hiding techniques have been proposed for applications to digital color and grayscale images. Most such techniques are based on either least significant bit (LSB) substitution or pixel-value differencing in the spatial domain. LSB substitution is a common and well-known technique for hiding data in grayscale and color images. In these methods, secret data are embedded into an image by replacing either a fixed or a variable length of bits. On the other hand, the pixel-value differencing method can be used to embed a large length of bits, and it offers good security. However, both these types of methods cannot be directly applied to binary images. This is because embedding different bits leads to changes in pixel values, and such changes lead to irregularities that are particularly noticeable in a binary. Therefore, hiding data in binary images is more challenging as compared to doing so in other types of images [2]. Generally, only some of the above mentioned types of techniques can be directly applied to binary images.

[*] Corresponding author. Tel.: +82 53 950 5553; fax: +82 53 957 4846.
E-mail addresses: hyunny.jung@gmail.com, kingjung@paran.com (K.-H. Jung), yook@knu.ac.kr (K.-Y. Yoo).
[1] Tel.: +82 53 940 5527; fax: +82 53 940 5299.

http://dx.doi.org/10.1016/j.ins.2014.02.016
0020-0255/© 2014 Elsevier Inc. All rights reserved.

Please cite this article in press as: K.-H. Jung, K.-Y. Yoo, Data hiding method in binary images based on block masking for key authentication, Inform. Sci. (2014), http://dx.doi.org/10.1016/j.ins.2014.02.016

On the other hand, very little research has been done on data hiding in binary images. The binary image is common and often appears in newspapers, faxes, and magazines. Hiding is difficult for binary images since their black or white pixels require only one-bit representation. There are two primary methods of data hiding for these images: sub-block modification and single-pixel manipulation. The first method modifies sub-blocks, which is divided into a group of pixels. Matsui and Tanaka embedded secret data in dithered images by manipulating the dithering patterns; they also embedded data in fax images, by manipulating the run lengths [3]. Low et al. changed the line spacing and character spacing to embed secret data in textual images, for bulk electronic publications [4,5]. These methods are used for some special types of binary images. The second approach modifies a single pixel, from black to white or vice versa: some special single pixels in the image are changed to embed the secret data. Koch and Zhao proposed a data hiding method by forcing the ratio of black and white pixels in a block to be larger or smaller than one [6]. However, there is some difficulty with this approach. Only a limited number of bits can be embedded, since the enforcing method has trouble dealing with blocks that have a significantly low or high percentage of black pixels. Wu et al. embedded bits in image blocks, selected by calculating a characteristic value and finding a pattern [7]. Liu et al. partitioned the binary image into blocks of 2 × 2 pixels and embedded a bit 0 or 1 in the block. This method can hide one bit per block by modifying 0.5 pixels on average [8]. Wu and Liu manipulated the flappable pixels to embed secret data into shuffled blocks. The shuffling of the blocks before embedding ensures the equalization of the embedding capacity from region to region without causing noticeable visual effects [9]. Venkatesan et al. proposed using the parity of blocks. The cover image is partitioned into small blocks, in which one bit information is stored. Unfortunately, if all of the pixel values belong to 0 or 1, a secret bit cannot be hidden [10]. Pan et al. proposed a data hiding method by partitioning into 4 × 4 blocks, where each block was repartitioned into overlapping sub-blocks [11]. Most of them do not include a stego-key, so this is less safe than other methods that adopt a stego-key [12–14]. Some methods are performed to authenticate for binary images with small distortion and image recovery [15–18].

In this paper we propose a new data hiding method in binary images using block masking to distribute the stego-key to two parts and then authenticates the right authorized part. By determining the location of embedding and selecting the edge areas, the image quality of the stego-image can be maintained at a high level quality with relatively low computational complexity.

This paper is organized as follows. In Section 2, our proposed data hiding method is described in more detail. In Section 3, our experimental results are presented and discussed. Our conclusions are presented in Section 4.

2. The proposed method

In this section, we present a detailed consideration of how data are embedded and extracted. To begin with, a binary image is made up of black and white pixels. Only a single bit is used to represent each pixel, say 0 or 1.

Let C be a cover image of $W \times H$ pixels and S be the s-bit secret data. For each $p(i,j)$ pixel value in image C, the new pixel value is $p'(i,j)$.

2.1. Data embedding

Fig. 1 presents a block diagram of the embedding and distribution process. The cover image is divided into sub-blocks and then key pairs are generated. These key pairs decide the embedding position and determine whether it is possible to embed a secret bit that position. The generated stego-image and key pairs can be distributed across other parts. In this situation, there can be various applications. For example, an encryption algorithm can be used to generate the key pairs and send key pairs more than two parts.

A given cover image is partitioned into $M \times N$ blocks. Data hiding is achieved by modifying some bits in the sub-blocks. The total number of sub-blocks, T generated

$$T = \frac{W \times H}{M \times N}. \tag{1}$$

Here, the embedding capacity, E is less than or equal to T bits.

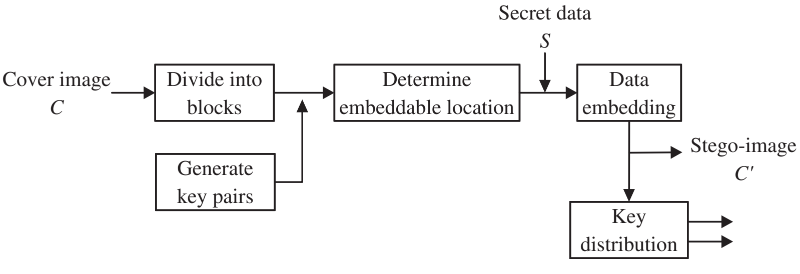

Fig. 1. Block diagram of embedding and distribution process.

Please cite this article in press as: K.-H. Jung, K.-Y. Yoo, Data hiding method in binary images based on block masking for key authentication, Inform. Sci. (2014), http://dx.doi.org/10.1016/j.ins.2014.02.016