Information Sciences 181 (2011) 2189–2208

Contents lists available at ScienceDirect

Information Sciences

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

Probabilistic visual secret sharing schemes for grey-scale images and color images

Daoshun Wang [a,*], Feng Yi [a], Xiaobo Li [b]

[a] Tsinghua National Laboratory for Information Science and Technology (TNlist), Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China
[b] Department of Computing Science, University of Alberta, Edmonton, Alberta, Canada T6G 2E8

ARTICLE INFO

Article history:
Received 13 August 2009
Received in revised form 10 January 2011
Accepted 12 January 2011
Available online 20 January 2011

Keywords:
Visual secret sharing
Visual cryptography
Image secret sharing
Relative difference
Contrast

ABSTRACT

Visual secret sharing (VSS) scheme is an encryption technique that utilizes the human visual system in recovering the secret image and does not require any cryptographic computation. Pixel expansion has been a major issue of VSS schemes. A number of probabilistic VSS schemes with minimum pixel expansion have been proposed for binary secret images. This paper presents a general probabilistic (k,n)-VSS scheme for grey-scale images and another scheme for color images. With our schemes, the pixel expansion can be set to a user-defined value. When this value is 1, there is no pixel expansion at all. The quality of reconstructed secret images, measured by average contrast (or average relative difference), is equivalent to the contrast of existing deterministic VSS schemes. Previous probabilistic VSS schemes for black-and-white images can be viewed as special cases in the schemes proposed here.

1. Introduction

Visual secret sharing (VSS) schemes have been proposed to encode a secret image onto n "shadow" images ("shares"). In a (k,n)-VSS scheme, the secret can be visually reconstructed only when k or more shares are available. Each pixel of the secret image is "expanded" into m sub-pixels in each share. In the reconstruction process, the stacking of the sub-pixels is a Boolean "OR" operation. VSS schemes were primarily designed for black-and-white (binary) images [14] by Naor and Shamir and based on this definition, Verheul and Van Tilborg [19] gave a more general definition. Directly based on black-and-white schemes, VSS schemes for grey-scale images (called GVSS) with pixel expansion m_g are proposed [1,11,13], and VSS scheme for color images (called CVSS) with pixel expansion m_c are proposed [19,25]. All these VSS schemes are "deterministic" since every pixel in the secret image can be exactly reconstructed, but each share is m times larger than the original. For example, when a $(3,3)$-GVSS scheme proposed in [1,11,13] is used to code an image with 256 grey-levels, m_g is as large as 1020. This heavy space requirement makes it impractical in many applications. To solve this pixel expansion problem, Ito et al. [12] introduced firstly a novel approach to encode a black and white image into the same size shares as the secret image. Yang [23] proposed an elegant probabilistic VSS (Prob. VSS) schemes for binary images with no pixel expansion ($m = 1$). Small areas, instead of individual pixels, of the secret image can be correctly reconstructed. Yang's Prob. VSS scheme has the same contrast level as the conventional VSS schemes. The size of the recognized area is also analyzed in [23]. Cimato et al. [8] extended the probabilistic binary VSS model [23] that allows $m \geqslant 1$ and discussed the relation between probabilistic schemes and deterministic schemes. Hsu et al. [10] used the concept of probability to construct an optimization model for general

* Corresponding author. Tel.: +86 10 62785636.
E-mail address: daoshun@mail.tsinghua.edu.cn (D. Wang).

0020-0255/$ - see front matter © 2011 Elsevier Inc. All rights reserved.
doi:10.1016/j.ins.2011.01.019

Table 1
The proposed (k,n)-VSS schemes and related probabilistic schemes.

	Prob. VSS scheme in [23]	Prob. VSS scheme in [8]	Prob. GVSS scheme proposed here	Prob. CVSS scheme proposed here
Image type	Binary	Binary	Grey-scale	Color
Pixel expansion	1	$1,\ldots,m$	$1,\ldots,m_g$	$1,\ldots,m_c$
Region size	Analyzed	Not analyzed	Analyzed	Analyzed
Average contrast	α	Computation equations[1]	$\alpha^{(i+1,i)}$, $i = 0,\ldots,g-2$	$\alpha^{(i,i)}$, $i = 0,\ldots,c-1$

access structures. Yang and Chen [24] introduced a satisfactory framework that prioritizes the pixels with different pixel expansions to enhance the image contrast for practical use. So far, all existing probabilistic VSS schemes [8,10,12,22,23] are for binary images. Wang et al. [21] proposed a probabilistic $(2,n)$ secret sharing scheme for binary images based on Boolean XOR and AND operations. The binary $(2,n)$-secret sharing scheme has been extended to grey-scale image and color image $(2,n)$-VSS schemes [3,4,18]. Those schemes in Refs. [3,4,18,22] are not VSS schemes, since they use XOR operations directly to construct a secret sharing scheme. Chen et al. [5] proposed a multiple-level (n,n)-VSS scheme without image size expansion based on basis matrices of VSS scheme, applying XOR operations to reconstruct secret image. Wang et al. [20] proposed a (n,n)-VSS scheme for grey-scale image based on the results of Ref. [21], which are not based on a corresponding deterministic scheme. Tsai et al. [17] proposed a novel (n,n)-secret image sharing scheme for true-color image with size constraint, through combination of neural networks and variant VSS, the quality of the reconstructed secret image and camouflage images are visually the same as the corresponding original images.

In this paper, we propose two probabilistic VSS schemes, one for grey-scale images and one for color images. As in [8], the pixel expansion can be set for a particular value $m \geqslant 1$, and the size of a recognizable area in [23] is analyzed in detail. Table 1 lists the proposed schemes and related probabilistic schemes. In this table and the rest of the paper, we include the pixel expansion value and the secret image type into the name of each scheme. In this notation, g is the number of distinct grey-levels in the secret image, c is the number of distinct colors in the secret image. The parameters m, m_g and m_c are the pixel expansions for basic binary VSS scheme, grey-scale image GVSS scheme and color image CVSS scheme, respectively. The quality of the reconstructed secret image is measured by the "contrast" that is the relative difference between consecutive grey-levels. The detailed definition of this measurement is given in Sections 2 and 5. Section 2 of this paper gives the background and basic notation. Section 3 presents our probabilistic VSS scheme for grey-scale images. The analysis of the size of the recognized area for this scheme is in Section 4. In Section 5, we introduce an approach to construct a color probabilistic VSS scheme for color images. The size of the recognized area for a color probabilistic CVSS scheme is presented in Section 6. Finally conclusions are given in Section 7.

In Table 1, value α is the contrast of deterministic black-and-white VSS schemes. The value $\alpha^{(i+1,i)}$ is the contrast between the ith and the $(i+1)$th grey-levels of deterministic GVSS schemes, here$i = 0,\ldots,g-2$. The value $\alpha^{(i,i)}$ $(i = 0,\ldots,c-1)$ is the contrast of the reconstructed color i in a deterministic CVSS schemes. The superscript 1 represents that the average contrast of binary Prob. VSS scheme in Ref. [23] has been given while value of pixel expansion is 1.

2. Background and basic notations

Pixel expansion in a deterministic VSS schemes is constant, however pixel expansion is variable in our presented probabilistic schemes. Although pixel expansion of deterministic VSS schemes is constant, the value of pixel expansion of binary VSS, grey VSS and color VSS is not the same. Throughout the paper, (k,n,m)-VSS scheme denotes that pixel expansion is m in binary (k,n)-VSS scheme. We write (k,n,m_g)-GVSS scheme to indicate that pixel expansion of grey-scale (k,n)-VSS is m_g. (k,n,m_c)-CVSS scheme denotes that pixel expansion is m_c in a colored (k,n)-CVSS scheme. Appendix A gives a list of all variables for easy lookup.

2.1. Binary (k,n)-VSS schemes

In a black-and-white VSS, the secret image consists of a collection of black-and-white pixels and each pixel is subdivided into a collection of m black-and-white sub-pixels in each of the n shares. The collection of sub-pixels can be represented by an $n \times\ m$ Boolean matrix $S = [s_{ij}]$, where the element s_{ij} represents the jth sub-pixel in the ith share. A white pixel is represented as a 0, and a black pixel is represented as a 1. When we Xerox a share onto a transparency on an overhead projector, white sub-pixels allow light to pass through while black sub-pixels stop light. $s_{ij} = 1$ if and only if the jth pixel in the ith share is black. Stacking shares $i_1,\ldots,i_r$ together, the grey-level of each pixel ($m$sub-pixels) of the combined share is proportional to the Hamming weight (the number of 1's in the vector V) $H(V)$ of the OR-ed ("OR" operation) m-vector $V = \mathrm{OR}(i_1,\ldots,i_r)$ where $i_1,\ldots,i_r$ are the rows of S associated with the shares we stack. Verheul and Van Tilborg [19] extended the definition of Naor and Shamir's scheme [14]. The formal definition of binary VSS scheme is given below.

Definition 1 (*[19]*). A solution to the k out of n visual secret sharing scheme consists of two collections of $n \times m$ Boolean matrices C_0 and C_1. To share a white (resp. black) pixel, the dealer randomly chooses one of the matrices in C_0 (resp. C_1). The chosen matrix defines the color of the m sub-pixels in each one of the n transparencies. The solution is considered valid if the following three conditions are met.