布林與餘數運算在影像分享之研究

研究生：趙崑源　　指導教授：林志青　博士

國立交通大學　　資訊學院　　資訊科學與工程研究所

摘要

本論文使用布林運算或餘數運算提出了三種影像分享的方法。在影像的儲存和傳輸上，影像分享是一種可用來保護數位影像之技術。傳統上，這個技術將一張機密影像轉換成數張稱之為分存(shadows 或 shares)的影像。之後，當收集到的分存張數達到指定的數量時，就可以恢復被分解的影像。

在機密影像分享上，多項式機密分享技術在日後的影像解碼上會需要很高的計算量。而另一種依據視覺編碼技術的方法，雖然解碼快速，卻常常因為分存影像放大的特性而需要很大的儲存空間。在此論文，我們先使用布林運算提出一個可容錯的 n 取 k 方法；它同時具有快速解碼能力和可以接受的分存影像大小。這個方法使用提供的機密彩色(或灰階或黑白)影像 A 產生出 n 張極為雜亂的分存影像；日後，使用這 n 張分存內任何 k 張就可以無失真地恢復 A。恢復 A 的每一個彩色(或灰階或黑白)像素平均只需要三個 24-bit(或 8-bit 或 1-bit)的 XOR 運算。因此，此新方法擁有非常快的解碼速度；而且它的像素

放大率總是可以被接受(0<像素放大率<2)。

在使用上，有些影像分享方法可產生友善的(視覺可辨認的)分存影像；換句話說，每一個分存影像看起來像原始影像在視覺畫質上被降低的版本，而不是看起來像完全無意義的亂碼雜訊圖。這個特性使得分存影像的管理，可以很容易地透過視覺辨認而方便地達成。除了分存影像的視覺可辨認外，漸進式解碼也是一個很方便的功能。在解碼會議上，對中度敏感性的影像，它提供了一個很方便的展示方法。最近，Fang 在他所提出的 ["Friendly progressive visual secret sharing," *Pattern Recognition* 2008, Vol. 41, pp. 1410-1414] 內，就結合了視覺可辨識分存影像和漸進式解碼這兩種方便的功能。然而，因為他的分存影像太大，他的方法在電腦上執行會造成記憶體空間的浪費。為了節省記憶體，我們在這裡根據餘數運算提出一個新的方法。這個新方法保留了以上兩個方便功能，而且分存影像大小為 Fang 的 1/2 到 1/4 倍；另外，其視覺可辨認的分存影像的視覺品質可以用一個簡單的公式來控制。

為了改善多張機密影像分享方法的效能，本論文提出的第三個方法是一個可以同時分解 n ($n \geq 2$)張機密影像成為 n 張分存影像的新方法。之後，在收集到所有 n 張分存影像時， n 張機密影像都可以無失真地恢復。只要缺少其中任一張分存，則所有機密影像都無法被洩漏出來。所產生的 n 張分存影像的大小總和會等於原來所有 n 張輸

入影像的大小總和；因此，這個新方法不會浪費儲存空間。任何一張機密影像內每一個像素的重建，只要使用一個布林、一個餘數和兩個數學算術運算量。所以，在大量機密影像的恢復上，這個新方法也是個十分快速的方法。

A Study of Image Sharing Using Boolean and Modulus Operations

Student : Kun-Yuan Chao Advisor : Dr. Ja-Chen Lin

Institute of Computer Science and Engineering
College of Computer Science
National Chiao Tung University

Abstract

In this dissertation, we propose three techniques in image sharing by using Boolean operations and modulus operations. Image sharing is a popular technology to secure digital images in storage and transmission. Traditionally, the technology transforms one secret image to several images called shadows or shares. Later, when the number of collected shadows reaches a specified threshold value, then the decomposed image can be reconstructed.

In image sharing, polynomial interpolation approach has heavy computational load to retrieve the shared image. To the contrary, visual cryptography approach is fast in decoding but is often needs larger storage space due to pixel expansion property. By using Boolean operations, we propose a missing-allowable (k, n) scheme that is fast and with a reasonable pixel expansion rate (per). The scheme generates n extremely noise-like shadow images for the given secret color (grayscale/binary) image A, and any k out of these n shadows can recover A loss-freely. In average, to decode a color (grayscale/binary) pixel of A, the retrieval uses only 3 exclusion-OR operations among 24-bit (8-bit/1-bit) numbers. Hence, the new method has very fast decoding speed, and its pixel expansion rate is always acceptable ($0<per<2$).

In application-oriented approaches, a few reported methods produced user-friendly (i.e. visually-recognizable) shadows; in other words, each shadow looks like a visual-quality-reduced version of a given image, rather than completely meaningless random noise. This facilitates visual management of shadows. Besides visually-recognizable shadows, progressive decoding is also a convenient feature in some applications: it provides the decoding meeting a convenient manner to view a moderately-sensitive image. Recently, Fang combined both conveniences of visually-recognizable shadows and progressive decoding in ["Friendly progressive visual secret sharing," *Pattern Recognition* 2008, Vol. 41, pp. 1410-1414]. But his method was space-wasting to implement on a computer because his shadows were too big. In order to save memory space, we propose here a novel technique based on modulus operations. It still has both conveniences, but our shadows are 2 to 4 times smaller than Fang's; and our visual quality of each shadow is controllable by a simple formula.

To improve the efficiency of secret sharing of multi-images, the third proposed technique is a new sharing approach to transform n ($n \geq 2$) secret images into n shadows. Later, after gathering all n shadows, all n secret images can be retrieved error-freely. No secret image is revealed if one shadow is absent. The total size of n generated shadows is identical to the total size of n input secret images; hence, this approach does not waste storage space. Each pixel in each secret image is reconstructed using only one Boolean, one modulus and two mathematical operations. Therefore, it is also fast to reconstructing many secret images. Comparisons are included.

Acknowledgements

I would like to express my sincere appreciation to my advisor, Professor Ja-Chen Lin for his kind guidance and patience throughout the course of this dissertation as well as the invaluable training during my study.

Thanks are also given to Professor Jen-Hui Chuang and Professor Zen-Chung Shih for their helpful discussion and suggestions. Appreciations are also extended to all colleagues in the Computer Vision Laboratory at National Chiao Tung University for their assistance and helps.

Final, I earnestly thank my parents for their love, encouragement and support. The thesis is dedicated them.

Table of Contents

List of Figures

List of Tables