向量量化型秘密影像分享及修復

研究生 ： 蘇瑋凱　　指導教授 ： 林志青　博士

國立交通大學　　電機資訊學院　　資訊科學研究所

摘要

本論文包含兩個大主題：影像分享及影像修復。在影像分享的主題中，我們提出了兩種向量量化型秘密影像分享。第一種是容錯式分享，第二種是漸進式分享。其中在容錯式分享內，我們利用碼簿(codebooks)及一些運算產生碼簿的交錯資訊，藉由這些資訊使得我們能達到(r, n)門檻值式的效果。當收集到任意 r 張分存影像時，使用者便能利用擷取出來的碼簿及索引值(code indices)來還原秘密影像。然而若收集到的分存影像未超過門檻值 r，則無法得到關於秘密影像的任何資訊。無失真漸進式分享是影像分享主題內的第二個部分，當收集到越多的分存影像時，還原出來的秘密影像品質會更好。除此之外，使用者不需要在意他拿到哪些分存影像，唯一要在乎的只有拿到的分存影像的數量。若收集到所有分存影像時，使用者便能還原出無失真的秘密影像。在本論文的第二個主題中，我們介紹了利用 search-order coding(SOC)的秘密影像錯誤修正方法。藉由一張額外的 SOC 影像，我們可以將受到損害的秘密影像修復成品質較好的影像。值得一提的是我們無法從單獨一張 SOC 影像得到秘密影像的資訊。因此 SOC 影像比起直接複製秘密影像要安全的多。此外，我們也提出一種 SOC 影像的進階版本。根據使用者是否擁有雜湊表(hash table)，SOC 影像提供兩種不同的影像修復方法。這兩種方法都擁有相當程度的修復能力。最後我們結合 SOC 影像與向量量化式的分享，實驗結果證明 SOC 影像不但能修復索引值，也能改善漸進式影像分享的還原品質。

VQ-style Secret Image Sharing and Recovery

Student: Wei-Kai Su Advisor: Dr. Ja-Chen Lin

Department of Computer and Information Science
College of Electrical Engineering and Computer Science
National Chiao Tung University

Abstract

This thesis includes two parts: the image sharing part and the image recovery part. In the first part, two methods of secret image sharing of VQ-style are proposed. One is the fault-tolerant sharing and the other is the progressive sharing. In the method of fault-tolerant sharing, we achieve the (r, n) threshold scheme by the mixed information of the codebooks. The mixed information is generated by some operations. When collecting any r shadows, the user can retrieve the codebooks and the code indices of the secret image from these r shadows, and use the codebooks and the code indices to reconstruct the secret image. However, no information of the secret image can be achieved when there are insufficient number of shadow images being collected. In the second part of image sharing, a lossless progressive image sharing method is proposed. The more the shadow images being gotten, the better the quality of the secret image being recovered. The user does not need to care about *which* shadow images he/she gets, and just needs to care about *how many* shadow images he/she collects. After receiving all shadows, the user can reconstruct a lossless secret image. In the second part of this thesis, we introduce an error correction method of secret image by search-order coding (SOC). By an additional image called SOC-image, we can repair the damaged image to a better one. Notably, the

SOC-image alone reveals nothing about the secret image. Thus the SOC-image is safer than duplicating the secret image directly. Besides, we also modify the SOC-image to an advanced version one. The advanced version of the SOC-image can repair the damaged image by two different ways according to the availability of the hash table. Both two ways are useful in the correction. Finally, we combine the SOC-image and the VQ-style sharing. The technique of the SOC-image error correction can not only repair the damaged code indices, but also improve the recovery quality of the progressive sharing.

Acknowledgements

I would sincerely thank my advisor, Professor Ja-Chen Lin for his teaching and instruction. He guided me patiently and kindly during my study of the Master's degree. Without him, it is impossible for me to complete this thesis.

Besides, the whole group of the Computer Vision Laboratory at Nation Chiao Tung University gave me much help and suggestions. Thanks are also given to them.

Finally, I cordially thank my parents for their wholehearted support to my study. This thesis dedicated to them.

Table of Contents

List of Figures

List of Tables