逢 甲 大 學
資訊工程學系博士班
博 士 論 文

嵌入機密影像的可驗證且無失真之多元影像共享機制

Verifiable Lossless Multi-Image Sharing Schemes for Secret Image Embedding

指導教授：張真誠

研 究 生：Ngoc-Tu Huynh

中 華 民 國 一 百 零 四 年 六 月

ACKNOWLEDGEMENT

This thesis is the result of my research carried out during my PhD program at Feng Chia University. It is my pleasure to thank all those who have helped me.

First, I would like to express my deep appreciation to my academic and thesis supervisor, Professor Chang Chin-Chen, who has been vigorously supervising my studies, supporting my research, and constantly involved in guiding me towards my goal. This thesis would not have been possible without his academic and financial support and insightful advices. It is fortunate for me to have him as my advisor.

I also express my sincere gratitude to Professor Lee Jung-San for his kindness and support. The classes he conducted broadened my knowledge in the field of cryptography. I learned a lot from the classes.

I am thankful to Professors and staffs of Department of Information Engineering and Computer Science. I would like to thank Mrs. Chen Ya-Chen for her administrative help.

I wish to express my heartfelt gratitude to my families for their love, encouragement and support.

Finally, I would like to send my thanks to my seniors, my juniors, my friends and my classmates in MSN lab, who have helped me during the time I stayed in Taiwan.

FCU e-Theses & Dissertations (2015)

中文摘要

相較於傳統的方法利用密鑰加密來保護數據，secret sharing 是將機密訊息切割成不同的區塊並分享到多張 shadow images 中以確保訊息在傳輸過程中的安全性；由於機密資訊可由多人持有，因此可避免機密訊息被蓄意或無意的丟失。常見的 secret sharing 有下列幾種問題：shadow images 被偵測到藏入的機密訊息、shadow images 遭受攻擊、機密訊息藏入後 shadow images 的再擴張以及一次分享有限個數的 secret images。雖然現有的算法能夠補救以上的問題，但這些處理過程的計算複雜度還有待商榷。

在本論文中，我們提出五種方案來解決上述問題。提出的方案皆滿足以下特性:安全性，準確性，計算複雜度和 shadow images 的大小。此外，每個方案都針對不同以存在的問題而設計。第一個方案旨在分享無限的 secret images，且不需檢索所有的 shadow images 就可取出特定的 secret images，可節省執行時間及計算成本。第二個方案產生高質量的 shadow images，以防禦特定攻擊。而第三個方案能夠偵測出 shadow images 上被竄改的區域，第四個方案當 shadow images 被攻擊後仍然能取出原始的機密訊息。最後一個方案能夠偵測所有疊合的 shadow images 是否有被竄改過。此外，本論文的另一目標在於確保視覺秘密共享機制適用於真實生活中。

關鍵詞：視覺秘密共享，視覺密碼學，像素擴展，無失真，多圖像共享，中國餘數定理，強韌性，可逆性

FCU e-Theses & Dissertations (2015)

Abstract

Contrary to conventional protecting data such as cryptographic techniques which encrypt the data with a secret key, secret sharing takes an approach to ensure well protection of transmitted information by allowing a secret message *M* to be divided into *n* pieces. Secret message *M* can be held by *n* participants to avoid the secret from incidentally or intentionally being lost. In a secret sharing scheme, leaking secret information from shadows, attacking on shadow image, enlarging shadow size, and the limitation of the number of secret image are existing issues which have arisen when developing an algorithm. Although existing algorithms provide remedies for such problems, the computational complexity of existing algorithms is still questionable. In this study, we propose five schemes to solve above-mentioned issues. These schemes first satisfy four general criteria of a secret image sharing algorithm: security, accuracy, computational complexity and shadow size. Moreover, each scheme has its specific features to tackle some existing problems. The first scheme aims to share and construct unlimited number of images. In addition, since the scheme is able to retrieve any secret image without revealing all other images, it can save execution time and computational cost. The second scheme generates very high quality of shadows to avoid suspicion of attackers on shadows. While the third scheme is capable of detecting and localizing tamper on shadow images, the fourth scheme is able to recover the secret even when attacks occurred. The final scheme solves the problem of cheating on given shadows. Furthermore, another major objective of this study is the visual secret sharing schemes which are suitable for real-time applications.

Keywords: visual secret sharing, visual cryptography, pixel expansion, lossless, multi-image sharing, Chinese Remainder Theorem, robustness, reversibility

FCU e-Theses & Dissertations (2015)

Table of Contents

Contents

FCU e-Theses & Dissertations (2015)

FCU e-Theses & Dissertations (2015)

FCU e-Theses & Dissertations (2015)