招生學年度	104	招生類別	碩士班
系所班別	資訊工程學系碩士班（資工乙組）		
科目名稱	英文		
注意事項	以科技英文為主		

1. **[English to Chinese Translation]** In the followings, each question shows the title of a scientific article adopted from computer magazine. Also, a description about this title is given. Please translate the title and its corresponding description to Chinese.

   (1-a) Title: Cloud Streaming Brings Video to Mobile Devices **(5%)**

   Description: Cloud streaming promises to let resource-constrained mobile devices handle computer-intensive applications like interactive video streaming and gaming.

   (1-b) Title: Gestural Interaction in Vehicular Applications **(5%)**

   Description: In-vehicle gestural interfaces are easy to use and increase safety by reducing visual demand on the driver. Prototype capacitive proximity sensing and depth-camera-based systems can recognize finger and hand gestures of varying complexity.

   (1-c) Title: Adapting Server Systems for New Memory Technologies **(7%)**

   Description: After decades of a cache, DRAM, and disk data storage hierarchy, new memory technologies are promising nonvolatility, high endurance, and fine-grained data access--all of which could, with some preparation, enable a new storage paradigm in server systems.

   (1-d) Title: E-health Demystified: An E-government Showcase **(7%)**

   Description: E-health, a priority for governments worldwide, involves multiple stakeholders and requires a complex framework designed for interoperability on legal, organizational, technical, and semantic levels, as the Croatian National Healthcare System exemplifies. Successful implementation suggests a model for e-government more broadly.

2. **[Reading Test]** In the following scientific research article, you will read an introduction for a paper about digital watermarking. Questions (2-a)-(2-e) refer to this article. Please answer for each question and mark the letter (A), (B), (C), or (D) on your answer sheet.

Protection of the intellectual property of multimedia data has become a challenge in the digital age where an enormous amount of digital images and videos are daily generated by persons who use different kinds of consumer electronic devices, such as computers, television sets, mobile phones, digital cameras and so on. Furthermore, the rapid development of the digital technology and the widespread diffusion of the communication over the Internet makes it extremely easy to distribute and exchange digital data, using different available and in some cases very popular channels, such as social networks.

For these reasons, controlling the diffusion of source multimedia data is a very difficult task, requiring an increasing set of sophisticated methodologies. From one side, technology advancements made all users capable to access different facilities for the production of digital information and for image processing techniques at lower costs. On the other side, the same nature of digital information, easily duplicable without any distinction from the original, or easily subjected to tampering, makes it possible the easily creation of novel images starting from a modified original image (infringing the copyrights of the owner).

Digital watermarking schemes have been introduced in modern digital right management systems as primitives allowing the resolution of disputes on the copyright of a given object. Usually, such schemes enable the possibility of inserting some extra information into the original data in such a way that the watermarked image is not affected too much (imperceptibility), and removal attempts are sufficiently contrasted (robustness). The presence of a valid watermark in an illegitimate copy can be easily tested and possible disputes on the ownership of the image resolved. Some state-of-the-art watermarking schemes, providing different features and characteristics, have been presented in the previous literatures.

The cryptographic technique for the visual sharing of secret images, denoted as visual cryptography (VC) or Visual Secret Sharing (VSS) has been firstly proposed by Naor and Shamir in 1994. Visual cryptography enables distributing sensitive visual materials to involved participants to the scheme, through public communication channels, as the produced random looking shares do not reveal any information if they are not combined as prescribed. Indeed, only qualified sets of participants are enabled to reconstruct the image by simply stacking together the shares they own. The attractiveness of this paradigm consists in the fact that the reconstruction phase does not require any computation, but it is performed directly by the human visual system.

Deviating a little bit from the main goal of the original schemes, visual cryptography has been exploited in many applications as a means to protect a secret image. Considering a (2, 2) VC scheme,

招生學年度	104	招生類別	碩士班
系所班別	資訊工程學系碩士班（資工乙組）		
科目名稱	英文		
注意事項	以科技英文為主		

where the original image is shared into two random looking shares, it is possible to freely distribute one of the shares, while the other can be used as a key, that is necessary to reconstruct the original image and can be provided only to a legitimate user. More in general, in a (n, n) VC scheme, where all the shares are needed to reconstruct the original image, it is possible to hide one share from the other participants in order to protect the visually shared secret. In this sense, the hidden share can be seen as a key for the "decryption" of the protected image. Under this perspective, VC has been considered as a natural way to achieve the protection of the watermark in combined schemes, where one of the share is needed to correctly reconstruct the embedded watermark, and in this case resolve any dispute on the image ownership.

In literature different schemes combining watermarking techniques with visual cryptography schemes have been presented. Usually, in such schemes, a visual cryptography scheme is used to process the watermark and obtain one or multiple shares; the shares are then merged with the host image in order to produce a watermarked image that can be freely distributed. The presented schemes consider both black & white images and color images, and can be classified on the basis of the watermarking technique used to encode the original image and of the visual cryptographic scheme needed to process the watermark.

In this paper we try to provide a general model in which most of the proposed watermarking systems based on the combination with VC schemes can be classified. Furthermore, we show how it is possible to prove the robustness gained from the adoption of a VC scheme, since the reconstruction of the watermark could be performed successfully even when some errors, randomly generated during the transmission, or induced by an attacker, are introduced into the watermarked image. We consider then some extension to the proposed model using different kinds of combined VC scheme, including for example a larger number of participants. We devise a possible utilization and new application scenarios for combined schemes using (2, n) and (k, n) VC schemes.

(2-a) To give a title for this scientific research article, which is the better title? **(3%)**
- (A) Protecting Multimedia security by Watermarking
- (B) Two Different Technologies of Digital Right Management Protection: Watermarking and Visual Cryptography
- (C) Visual Cryptography Based Watermarking
- (D) A Survey of Watermarking and Visual Cryptography

(2-b) What is the novel property of visual cryptography? **(3%)**
- (A) It can be easily decoded by superimposing shares
- (B) It can be combined with watermarking
- (C) It can be used for digital right management protection
- (D) It is a technology of watermarking

(2-c) Please choose a word that is the closest in meaning to the "*state-of-the-art*" in some *state-of-the-art* watermarking schemes ... **(3%)**
- (A) Obsolete (B) Newest (C) Better (D) Popular

(2-d) Please choose a word that is the closest in meaning to the "*infringing*" in ... *infringing* the copyrights of the owner. **(3%)**
- (A) Copying (B) Violating (C) Protecting (D) Agreeing

(2-e) What are not the features of watermarking? **(3%)**
- (A) Robustness (B) Imperceptibility (C) Protection of intellectual property (D) Visual Cryptography

3. **[Writing Test]** Please write an abstract (i.e., a brief summary of a research article) for the above article in Problem 2. Your abstract should have at least 100 words. **(24%)**

4. **[Science and Technology Terminology]** Please give a short and simple explanation (in Chinese) for each science and information terminology.
(4-a) 4K TV **(4%)** (4-b) Cloud computing **(4%)** (4-c) RFID **(4%)** (4-d) Big data **(4%)**

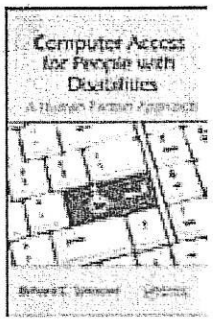
5. **[Computer Engineering Text Book]** The followings (5-a) to (5-c) show a catalog of three text books. Write out the book title (in Chinese), and briefly describe its content (in Chinese).

招生學年度	104	招生類別	碩士班
系所班別	資訊工程學系碩士班（資工乙組）		
科目名稱	英文		
注意事項	以科技英文為主		

(5-a) (7%)

Computer Access for People with Disabilities

A Human Factors Approach



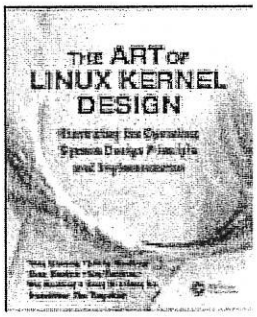
Richard C. Simpson
New York Institute of Technology, New York, USA
Series: Rehabilitation Science in Practice

Providing the information clinicians need to know in order to provide effective alternative computer access solutions to individuals with disabilities, this book presents technology for individuals with physical, cognitive, and sensory impairments, and for older adults. The text covers text entry devices, pointing devices, switch access, automatic speech recognition, and web accessibility. The book draws on research from the fields of rehabilitation engineering, occupational therapy, and human-computer interaction (HCI) and emphasizes fundamental concepts and principles that remain true regardless of which specific operating system or product is being used.

(5-b) (7%)

The Art of Linux Kernel Design

Illustrating the Operating System Design Principle and Implementation

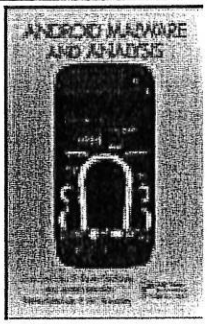


Lixiang Yang
Graduate University of the Chinese Academy of Sciences, Beijing

This book uses the real source code of a multi-process operating system (OS) as the blueprint and its actual running operation as the main thread. It uses the concept of "master-slave mechanism" and provides more than 300 figures, illustrating the complex relationships within the OS. Divided into two sections, it provides detailed insight on the complete process from booting up to system idling. The second part uses a few carefully designed real-life user operations as study cases to explicate important OS concepts.

(5-c) (7%)

Android Malware and Analysis



Ken Dunham
Rampart Research

This book documents the best tools and tactics available for analyzing Android malware. It explains how to use to use dynamic malware analysis to check the behavior of an application/malware as it has been executed in the system. It also describes how to use static analysis to break apart the application/malware using reverse engineering tools and techniques to re-create the actual code and algorithms used. The book includes access to an online library that supplies readers with tools to perform their own analysis of the latest Android malware threats.