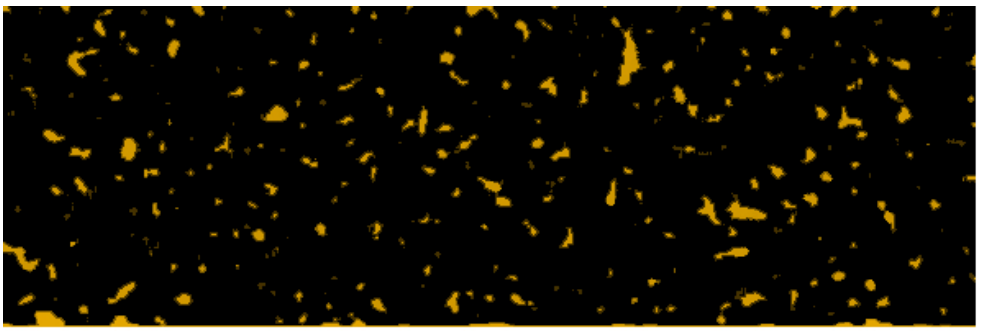


Information Cryptology&
Construction Lab

INFORMATION CRYPTOLOGY AND CONSTRUCTION LAB (ICCL)

http://hera.im.cpu.edu.tw/

Acknowledgement

We would like to express our deep sense of gratitude to Prof. Shiuh-Jeng Wang for his invaluable help and guidance during the course of this project of ICCL brochure. We are highly indebted to him for constantly encouraging us by giving his critics on our work. We are grateful to him for having given us the support and confidence.

This project also owes much to support from all our colleagues and fellow researchers at ICCL, for their wisdom, encouragement, and inspiration over the intended period of our research works in ICCL.

Edited
By
Sajal Bhatia
Saurabh Gupta

Contents	Chapter	Page
About Central Police University	①	5
Introduction to ICCL	②	9
History and Motivation		
Introduction to the Lab.		
Member Tree	③	12
The Director		
The Staff Members		
ICCL Member Tree		
Research Fields	④	17
Computer Forensics		
Multimedia		
Network Security		
Cryptography		
Steganography		
Research Works at ICCL	⑤	22
Steganography		
— Steganography of Capacity Required Using Modulo Operator For Embedding Secret Image		
—Information Hiding at Oblivious Watermarking Scheme upon Alternative Threshold in Spatial Domains		
Cryptography		

—Security Cryptanalysis in High-Order Improved Fast Encryption Algorithm for Multimedia
—Proactive (*k*, *n*) Threshold Secret Sharing Scheme with Variant k and n

Network Security

—A Countermeasure against Frequent Attacks Based on the Blom-scheme in Ad Hoc Sensor Networks
—Mutually Identity Authentications in GSM-based Anonymous Communications

Multimedia

—Visual-based Embedding Systems with Targeted Secret Disclosures and Applications
—Fidelity Colour Multimedia Image with Adaptive Data Hiding on Projection Dimensions

Digital Forensics

—Digital Evidence Seizure in Network Intrusions against Cyber-crime on Internet Systems
—Measures of Retaining Digital Evidence to Prosecute Computer-based Cyber-crime
—Persistence and Desistance: Examining the Impact of Hacker Ethics Observed to Taiwan's Juveniles

---

Recent Publications ⑥ 28

Future Perspectives at ICCL ⑦ 34

Working Environment ⑧ 36

Working Experience of International Students

Projects ⑨ 41

References ⑩ 43

---

1 About CPU

中央警察大學
CENTRAL POLICE UNIVERSITY

中央警官學校
統一警察教育
養現代警官

中央警官學校

Brief history of Central Police University

(summarized from http://cpuweb.cpu.edu.tw/)

The **C**entral **P**olice **U**niversity (CPU) is the highest learning institute for police education in Taiwan, and operates under the Ministry of the Interior, with supervision by the Ministry of Education. Therefore, the education of this university must not only meet the requirements of college education but also the special demands of cadre education.

This university is the institution of the highest learning for police education in our country. On Sept. 1, 1936, by merging Police High School, MOI and Chechiang Provincial Police School, the government established Central Police College in the town of Maqun in Nanjing for the purpose of unifying police educational systems around the country and cultivating police administrative personnel. In this college, two-year education and three-year police education were available. At the breakout of Anti-Japanese War in 1937, the college was moved west to Danzishi in Chongqing. There, special police training courses and special training courses for police officers were added. In order to bring up police administrative personnel taking charge of a department alone, an advanced research course for police administration was organized in Jan. 1944. In order to reserve police cadres after the reoccupation of Taiwan, a lecture course for police cadres was started in Sept. 1944 and the first-class graduates of every period were selected to further their studies in USA.

After the triumph of Anti-Japanese War in 1945, the college was moved back to Nanjing outside Guanghua City-Gate. In accordance with the national policy, the training for army officers turned into police and other specialized trainings were expanded. Besides Nanjing, six more branches were established in Xi'an, Guangchou, Dihua, Chongqing, Beijing and Shenyang, as well as two officer squads in Shanghai and Taiwan. The college flourished for a time with a student body of more than 12,000.

When Civil War broke out in 1949, the college was moved to Guangzhou, then to Chongqing, and finally to Taiwan where it was consolidated with the Training Course for Police Officers in Taipei. In Jan. 1950, the college was closed down under orders, however, the Training Course for Police Officers was still kept for cultivating police in-service.

In May 1954, the college resumed classes and that education of regular courses continued. In 1957, with approval, this college was expanded into a four-year college. At first, two departments of Police Administration and Criminal Investigation were formed, followed by the establishment of other departments, including Public Security, Crime Prevention and Corrections, Household Administration, Fire Service, Traffic Science, Foreign Affairs Police, Military-Service Administration, Administrative Management, Information Management, Border Police, Maritime Police, Forensic Science and Law. In 1970, the graduate school offering MA degree in police administration was established. Since 1974, female students were admitted to enter the college. Besides research institute and education of regular courses, seminars for the promotion of police in-service and professional seminars were held. In order to accelerate international friendship and

cooperation, the college not only admits foreign students, but also cooperates with foreign universities, exchanges teachers and students, holds academic seminars and takes part in international academic organizations and activities. Since its establishment in 1936, CPU has been enjoying a history of over seventy years.

The key-developments of our Lab., ICCL, in Central Police University devote to reinforce high-tech police technology in the face of new crime problems in the emerging information era. In particular, the cyberspace issue in security explorations, information security incident response, and digital forensics studies are the end we are going to.

Academic Departments at CPU

- Dept. of Police Administration the goals of the Department:
  - To cultivate leaders of police administration.
  - To study the law system of policing and public security.

- Dept. of Criminal Investigation
  To train students to be specialized in scientific methods and techniques of criminal investigation and to enhance efficiency in criminal investigation

- Dept. of Forensic Science
  To train students to be specialized in forensic science, to be familiar with relevant theory and research and to develop new forensic skills

- Dept. of Public Security
  To train students to be specialized in national security law enforcement and social security protection.

- Dept. of Crime Prevention & Correction
  To train students to be specialized in crime prevention, corrections, prison administration as well as crime prevention theory and research.

- Dept. of Fire Science
  To train students to be specialized in fire technology and fire science

- Dept. of Traffic Science
  To train students to be specialized in traffic administration and traffic law enforcement as well as traffic safety theory and research.

- **Dept. of Information Management**
  To train students to be specialized in police information technology and management against high-tech computer crime

- Dept. of Foreign Affairs Police
  To train students to be specialized in management of cases involving alien tourists and residents in Taiwan

- Dept. of Border Police
  To train police officers who will maintain border security and also be in charge of immigrant and non-immigrant control upon departure from and entry to Taiwan.

- Dept. of Administrative Management
  To train students in professional knowledge, such as police administration as well as research ability to elevate the academic standards and operational effectiveness in police administration.

- Dept. of Maritime Police
  To train law enforcement officers who will maintain maritime safety, strike on crime at sea, protect oceanic ecology and secure the rights of our fishermen.

- Dept. of Law
  To promote advanced studies on police legal aspects and jurisprudence; to protect human rights and maintain public order.

- General Education Center
  To integrate university education and police education

2
Introduction to ICCL
@
ICCL@B
Forensic Research & development
task force Group

History and Motivation

In any social group, there will always be a handful of people with bad intentions. In the present scenario, the number of the global Internet users has already crossed one hundred million and even if the percentage of the population which performs illegal activities, also known as 'Hackers' is under one percent, the number is alarmingly high. To prevent hackers from invading and insure internet safety, security studies and enforcements are therefore definitely required to establish against the tech-threat in information era.

Because of the change in information technology, it has become more and more important to protect the data and hide the information. No matter whether it is in software or communication, the security issue must be strengthened; and for this reason, studying the concepts of cryptography became an important subject. Due to this reason, Information Cryptology and Construction Lab. (ICCL) was established in 1998.

Realization of the demand for security in future, led its establishment members look for a way that could improve the contemporary technologies in information hiding and make the new developing methods complete. This was the prime motivation that led to the establishment of ICCL which could offer more safe and perfect encryption to solve the information safety problem.

Introduction to ICCL

The **I**nformation **C**ryptology and **C**onstruction **L**ab. (ICCL) is located on the second-floor of Information Building, CPU, Tao Yuan, Taiwan, 333. At present, there are twenty members in this laboratory, and all members are passionate for research in the areas such information security, incident response, digital forensics. The member list consists of the professor (Dr. SHIUH-JENG WANG) and a number of students (graduate/undergraduate) aiming at developing efficient methodologies to get an idea of the crime activities to prevent cyber crime and seize computer-crime suspects in the Cyberspace address. They would like to compass the ends in hope of the most confidence.

With the tremendous growth of Internet in the information technology era, especially in the twenty-first century, the knowledge acquisition has become the foremost demand for all the people around the world. However, there are always some people engaged in misusing the Internet facilities. Their illegitimate behaviors includes invading others OS-systems without getting the owners' permissions, planting the malicious programs onto the disallowed directories in file systems and then to curb, infect, and paralyze the system normal operations. They are even engaged in stealing the software/hardware/other resources that have been registered as authorized in agencies via Internet channels. In particular, the brute-force penetrating methods is probably made use to retrieve illicitly the plaintext-message. Accordingly, a well-designed crypto-mechanism is anxiously required to safeguard the system security and document storage from all the illegitimate attempts. Besides, there is also an urge for studies related to fast data searching techniques, well-organized data structure, high-performance data compression, and high-

capacity/strong-robustness information hiding (steganography/watermarking) on text/image embedding systems. ICCL has proved to be an ideal answer for all of the above mentioned problems.

The projects ICCL has received so far from official commitment include National Science Council ROC, Chung-Shan Institute of Science & Technology under Ministry of National Defense ROC, Academia Sinica ROC, National Security Bureau ROC, Ministry of Economic Affairs ROC, The Institute for Information Industry ROC, and Ministry of Transportation and Communications ROC. Besides, we also received the collaboration requests from industrial enterprises at the implementations of research works.

Over the years, ICCL (popularly called as "Eagle" by its members) has made a tremendous progress in all of the above mentioned areas. It has provided the best of leaning environment to all of its budding researchers and the amount of hard work done by them has paid of by establishing their own brand name. The staff associated vital ICCL has played an indispensable role in its progress, and it is constantly increasing in both quantity and quality.

3
Member Tree

ICCL Staff members:

J.H. Huang who is the vice-chair of ICCL, I (Jeff) became Professor Wang's partner six years ago. I am response for Internet facilities and systems managements of ICCL. Sometimes I help with projects of senior students, keep track their progress and students come to discuss with me when they have problems with their research projects. I really enjoy working with ICCL team members and it is the place where lets me always deepen into professional study field and push myself more forward.
The most special experience at ICCL is to work with international students. Both I and students exchange study experiences and cultures. It is valuable experience I have ever had. I believe that we will continue call students to join ICCL no matter where students are from as long as they are interested in working with us!
ICCL provides the best research environment, and the best facilities, and of course the best leader. It is my honor to be involved with ICCL team.

Ling-Cheng Chien who is the senior secretary of ICCL, I (Lynn) started to work with ICCL team members seven years ago. Professor Wang was the editor-in-chief of "*Communication of the CCISA*," I was his assistant, helped with publication work.
Students here are intelligent and hard working. They are best work partner I have ever had. Two years ago, two Indian students came to ICCL for their internship. They did professional research under Professor Wang's guidance and had co-work with ICCL team members. It was the fabulous opportunity for all of ICCL members of experiencing working with international students. Everyone learned so much through their work.
ICCL regularly provides internship and overseas research opportunities. We welcome international students to join us with open arms. Please check out ICCL websites for detailed information. It is the best place for learning and studying. I believe that students who studied in ICCL would be successful in both their future work and future life.

U.C. Kuo who is the web director of ICCL, I (Unicon) am a staff member of CPU and now in doctoral program of Information Management at Yuan Ze University. My research interests are Data mining, Criminal Linguistics Profiling, and Crime Analysis. I have worked with Prof. Wang for many years. Usually, I deal with the administrative affairs of campus for Prof. Wang and discuss my research with him. Sometimes, I take care of the project progress of senior students in ICCL team. To the best of my knowledge, ICCL team is the best collaborative team. Anyone can learn how to research, how to cooperate with others, and how to enlarge his/ her knowledge under Prof. Wang's guidance.

The Director

Dr. Professor Shiuh-Jeng Wang

PhD. National Taiwan University, Taiwan
Full Professor, Central Police University, Dept. of Information Management
Director Information Crypto and Construction Lab.
Chair of ICCL-FROG (**F**orensic **R**esearch devel**O**pment task force **G**roup)
Director Chinese Cryptography Information Security Association (www.ccisa.org.tw)
Program-chair of SH'08, international (http://www.sersc.org/SH08/)
Program-chair of MPIS'08, international (http://mpis08.ialab.cs.pu.edu.tw/mpis08/)
Program-chair of MPIS'09, international (http://www.ftrg.org/MPIS2009/)
Program-chair of NCS'09, (http://ncs2009.ntpu.edu.tw/CI/CI.htm)
Program-chair of Future Tech 2010, international (http://www.ftrg.org/futuretech2010/)
Visiting Scholar, Comp. Sc. Dept, Florida State University
Visiting Scholar, Comp. Info. Sc & Eng. Dept, University of Florida
Project Study, at Computer School of Carnegie Mellon University

Shiuh-Jeng Wang was born in Taiwan, 1967. He received the M.S. degree in Applied Mathematics from National Chung-Hsing University, Taichung, Taiwan, in 1991. He received his PhD degree in Electrical Engineering at National Taiwan University, Taipei, Taiwan in 1996. He is currently with Dept. of Information Management at Central Police University, Tao-Yuan, Taiwan, where he directs the Information Cryptology and Construction Laboratory (ICCL, http://hera.im.cpu.edu.tw).

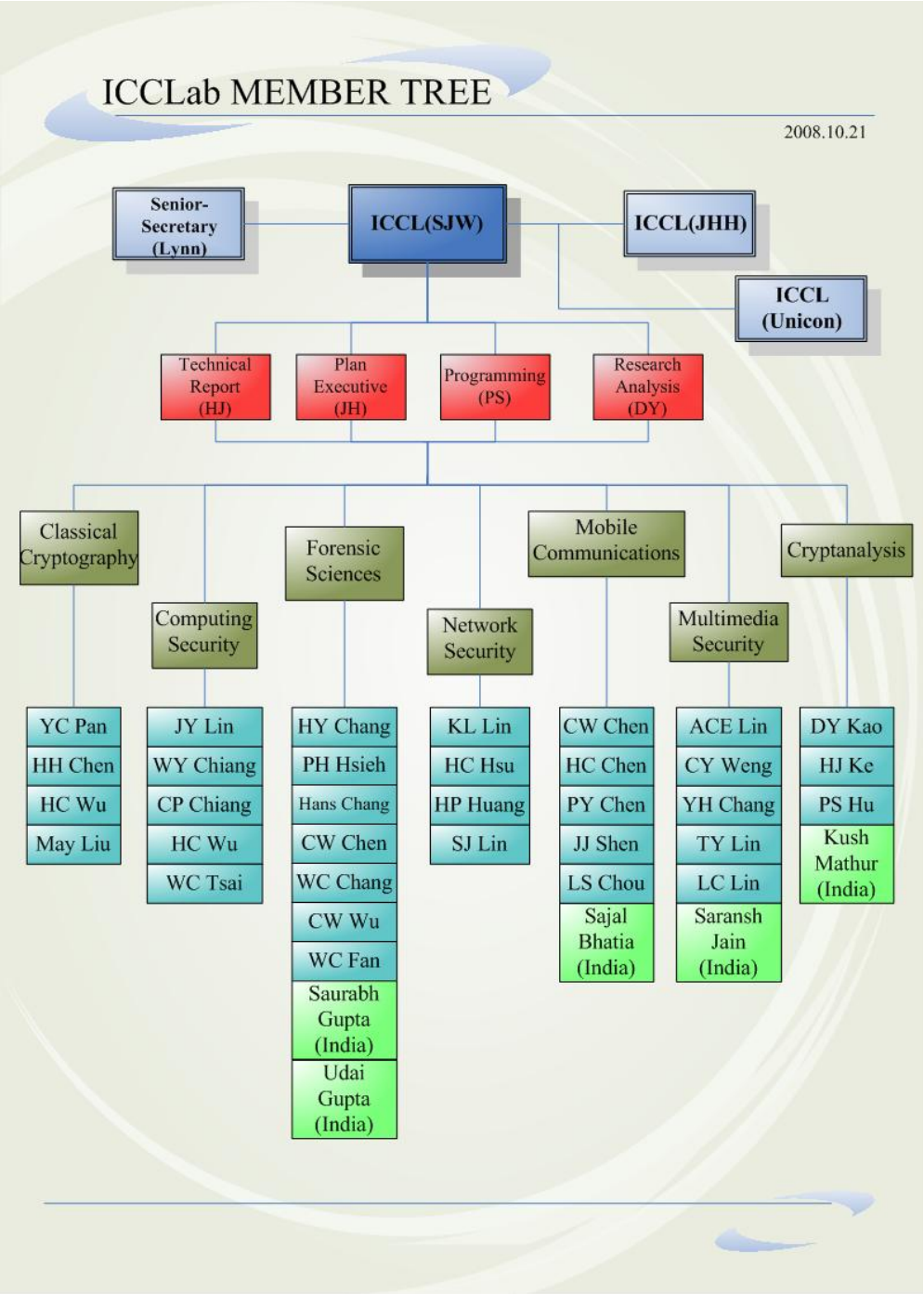
He was a recipient of the 5th Acer Long-Tung Master Thesis Award and the 10th Acer Long-Tung PhD Dissertation Award in 1991 and 1996, respectively. Dr. Wang was a visiting scholar of Computer Science Dept. at Florida State University (FSU), USA in 2002 and 2004. He also was a visiting scholar of Dept. of Computer and Information Science and Engineering at University of Florida (UF) from Aug. 2004 to Feb. 2005. He served the editor-in-chief of the journal of *Communications of the CCISA* in Taiwan from 2000-2006. He has been elected as the Director of Chinese Cryptology and Information Security Association (CCISA) since 2000. Dr. Wang academically toured the CyLab with School of Computer Science in Carnegie Mellon University, USA, in 2007 for international project collaboration inspection.

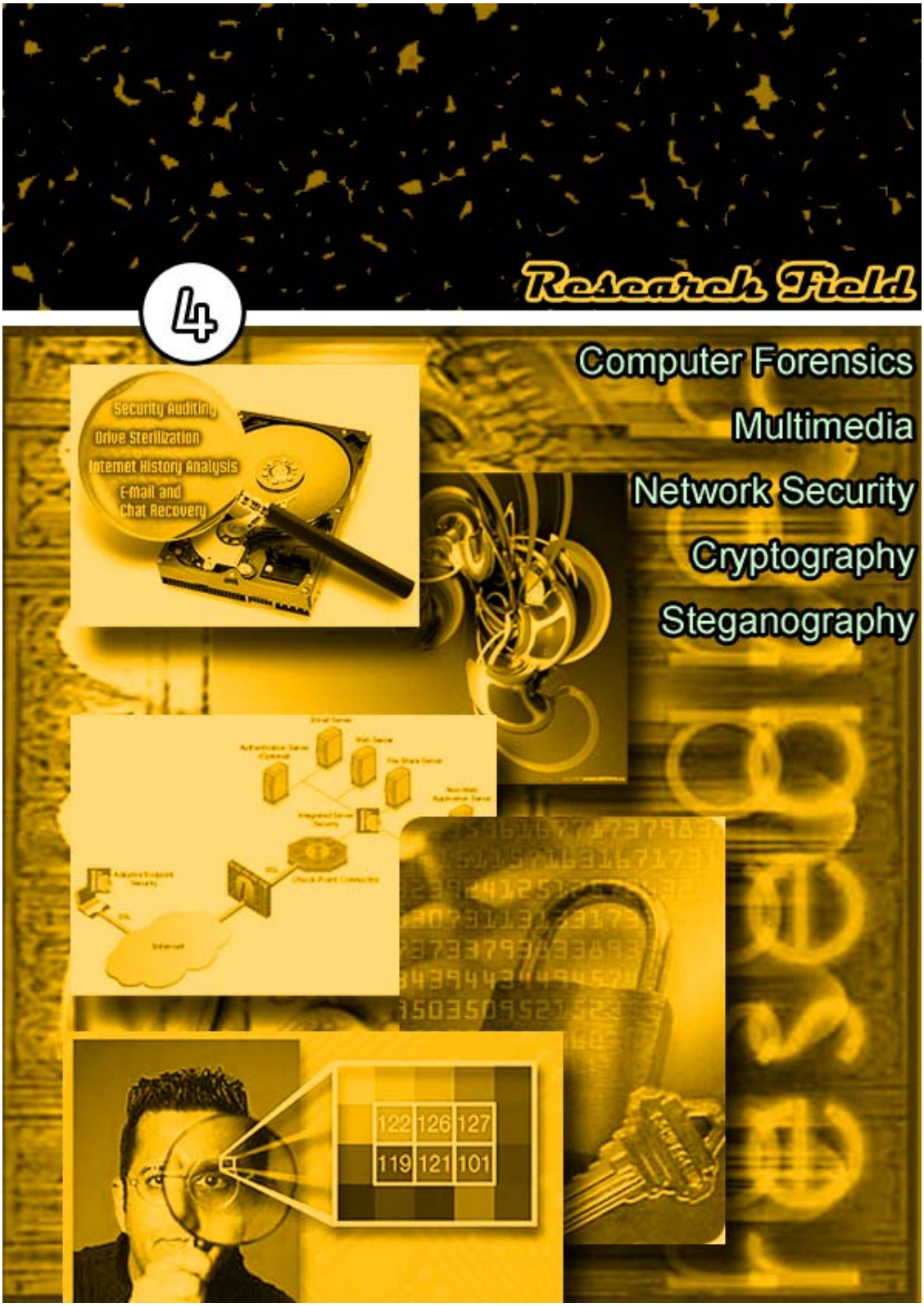
He is also the authors of eight books (in Chinese versions): *Information Security*, *Cryptography and Network Security*, *State of the Art on Internet Security and Digital Forensics, Eyes of Privacy –Information Security and Computer Forensics, Information Multimedia Security, Computer Forensics and Digital Evidence, Computer Forensics and Security Systems,* and *Computer and Network Security in Practice,* published in 2003, 2004, 2006, 2007, and 2009, respectively.

He is also the author/co-author of seven books (in Chinese versions): Information Security, Cryptography and Network Security, State of the Art on Internet Security and Digital Forensics, Eyes of Privacy –Information Security and Computer Forensics, Information Multimedia Security, Computer Forensics and Digital Evidence, and Forensics and Security in Computer Systems published in 2003, 2004, 2006, 2007, and 2009, respectively.

Prof. Wang has published over 200 papers in referred Journals/Conference proceedings/Technique reports so far. He is a full professor and a member of the IEEE, ACM. His current interests include information security, digital investigation and computer forensics, steganography, cryptography, data construction and engineering.

ICCLab Member Tree




Research Field
4
Computer Forensics
Multimedia
Network Security
Cryptography
Steganography
Security Auditing
Drive Sterilization
Internet History Analysis
E-Mail and
Chat Recovery
122 126 127
119 121 101

Computer Forensics

Forensics is the process of using scientific knowledge in the collection, analysis, and presentation of evidence to the courts. The word *forensics* means "to bring to the court." Forensics deals primarily with the recovery and analysis of latent evidence. Forensics takes scientific knowledge and methods and combines them with standards of law for the purpose of recovering and presenting at court evidence related to a crime.

Computer forensics is a generic name that we use for the analysis and reporting of our findings from forensic analysis of all the computer and digital related media in a manner that is admissible in a court of law. The digital media not only includes PC/Laptops or server hard drives but also other storage devices such as USB drives, MP3 players, memory cards, SIM cards and data gathered via network analysis. All types of operating systems can be analyzed, from DOS to Microsoft Windows based through to MAC, UNIX variants, and even those utilizing more obscure systems.

At one time, computer forensics dealt exclusively with *persistent data*—data that is stored on a local hard drive or other medium and is preserved when the computer is powered off—and was the sole domain of law enforcement. In this age of interconnected networks, however, the examination and collection of *volatile data* is becoming more important. Volatile data is any data that is stored in memory, or in transit, that will be lost when the computer loses power or is powered off. Volatile data resides in registries, cache, and random access memory (RAM). Since the nature of volatile data is effervescent, collection of this information will likely need to occur in real or near-real time. Thus we can say that the definition of Computer Forensics applies not only to the collection and examination of archival data but also to real time and latent data. Computer Forensics perfectly merges the disciplines of computer science and the law.

Computer forensics involves three primary activities:

- The gathering and backing up of electronic storage media in proper form and preserving the integrity of the chain of custody in a secure environment.
- The analysis of the electronic storage media (by, for example working copies and not the original images) using court tested protocols and procedures
- The presentation of evidence, either in report form or in court as a recognized expert witness.

Some of the analytical techniques used by computer forensic specialists are the following:

- Building a profile of the target
- Recovering deleted or damaged files
- Identifying user created files
- Using specific search criteria versus performing a full search of the electronic storage media
- Searching the deleted areas of the electronic storage media
- Bypassing or breaking through password protected or encrypted files
- Closely examining cache, temporary Internet and backup files.

Multimedia

Multimedia group of ICCL works in the areas of information security related to multimedia type of data for example digital images, voices etc. and fields related to it. The work is divided into four parts: Information Hiding, Visual Cryptography, Image Detection, and Digital Watermark. Among the areas mentioned above, first and the second uses multimedia characteristic to offer the security application which is different from traditional cryptography. The third cooperates to develop **FROG (F**orensic **R**esearch devel**O**pment Task Force **G**roup), and expand the research into Digital Forensics in multimedia. The fourth is used to solve digital image copyright problems on the internet. Besides the above mentioned areas, we try to constantly incorporate the advances in the field of multimedia into our information security system, and keep us update with the latest development. We wish to contribute our level best in the field of information security field

Network Security

With the explosion of the public Internet and e-commerce, private computers, and computer networks, if not adequately secured, are increasingly vulnerable to damaging attacks. Hackers, viruses, vindictive employees and even human error all represent clear and present dangers to networks. And all computer users, from the most casual Internet surfers to large enterprises, could be affected by network security breaches. However, these security breaches can often be prevented if the network administrator is well acquainted with the prevention methodologies.

Network security consist all activities that organizations undertake to protect the value and ongoing usability of assets and the integrity and continuity of operations. An effective network security strategy requires identifying threats and then choosing the most effective set of tools to combat them. Threats to network security include Viruses, Trojan horse programs, Vandals, Attacks, Data interception. These problems can be countered by using Network security tools which includes Antivirus software packages, secure network infrastructure, Virtual private networks, Identity services**,** Encryption**,** Security management. None of these alone will be sufficient to protect a network, but when they are layered together, they can be highly effective in keeping a network safe from attacks and other threats to security. In addition, well-thought-out corporate policies are critical to determine and control access to various parts of the network.

Cryptography

From the early human age people worked on finding out the ways to keep the information secret. When there is a need of transmitting secure information from one place to another, it's important to protect the information while it is in transit. Cryptography presents various methods for taking legible, readable data, and transforming it into unreadable data for the purpose of secure transmission, and then using a key to transform it back into readable data when it reaches its destination.

The aim of cryptography has come beyond merely making data unreadable, it also extends into user authentication that is, providing the recipient with assurance that the encrypted message originated from a trusted source. Hash functions are sometimes used in conjunction with private key or public key cryptography. This is a type of one-way encryption, which applies an algorithm to a message, such that the message itself cannot be recovered. Unlike key-based cryptography, the goal of the hash function is not to encrypt data for later decryption, but to create a sort of digital fingerprint of a message. The value derived from applying the hash function can be re-calculated at the receiving end, to ensure that the message has not been tampered with during transit. Then, key-based cryptography is applied to decipher the message.

The study of cryptography is becoming deeper day by day, and scientists are rapidly creating mechanisms that are more difficult to break. The most secure type of cryptography yet may be quantum cryptography, a method that has not yet been perfected, which instead of using a key, relies on the basic laws of physics, and the movement and orientation of photons to establish a connection that is absolutely secure and unbreakable.

Steganography

Steganography is a methodology used to hiding information in images. Using stenography, watermarks and copyrights can be placed on an image to shield the rights of its owner without altering the appearance of the image. Almost like magic, images, executable programs, and text messages can hide in images. The cover image does not appear to be altered. People look at the cover image and never suspect something is hidden, but your information is hidden in plain sight.

The word Steganography comes from the Greek and literally means "Hidden writing". People have used Steganography through the centuries to hide messages. The messages are hidden in plain sight in that they are visible to people who know where to look.

Steganography and cryptography are closely related. Cryptography scrambles a message to produce something that looks scrambled. The scrambled appearance usually is a random-string representation; some people see sorting out such a message as a challenge. Steganography instead hides a message in a cover message. The result looks like something innocent, so prying eyes often dismiss it.

5
Research Work at TCCL

Research Works at ICCL

Steganography

Steganography of Capacity Required Using Modulo Operator for Embedding Secret Image

Abstract
A novel mechanism using modulus operations to incorporate secret data (with image form) into a host-image is proposed. The used modulus is a threshold value that indicates how many bits of the secret image are being incorporated into the host-image. In our scheme, there are two kinds of secret images processed. The capacities of these two types are half the size and a quarter the size of the chosen host-image, respectively. As can be seen in the result of our experiment, not only can the secret images be totally embedded, but the extra information, such as the auxiliary table, assisting the secret extraction is released as well. Even then, there is still space remaining after the hiding procedure is completed. The result is a higher capacity exploration for embedding the secret into a host-image. Upon inspection of the quality of the stego-image using the measurement of PSNR it is noted that not only does the image display make the grade of the human vision system, i.e., it is imperceptible by human eyes as far as the embedded secret is concerned, but also the valued results of PSNR remain sufficiently stable for a variety of host-image selections. Therefore, our proposal scheme is notably superior to those in the previous literature. The advantages of this proposed scheme are the higher capacity exploration on secret embedding, and better stability on stego-image displays.

Information Hiding at Oblivious Watermarking Scheme upon Alternative Threshold in Spatial Domains

Abstract
An intellectual property protection mechanism is proposed by means of an oblivious watermarking scheme. The embedding technique adopted in this paper is based on the modular operation. The modulus is a threshold value which determines how the binary pattern of the watermark is to be embedded into an image. In order to create a better fidelity of the image with the embedded watermark against perception by the human vision system, the random bit-string transformed for the watermark is done first. Then there are two classifications required to create the random bit pattern 0/1 during the embedding procedure. Afterwards, several frequent tests of image processing are done, such as JPEG compression, diverse filtering treatments, resampling and requantization, etc., to prove and show off the remarkable result that was achieved. Compared to the literature of LSB-like watermark embedding procedure in [9] and as observed from the experiments, not only the advantages emphasized in original research work remain, but in addition it should be pointed out that it is not necessary to check the original image again to extract the embedded watermark. Therefore, it can be fairly stated that the scheme

explored in this paper is more efficient than the previous one, and that it is a feasible to cope with the protection of intellectual property for digital image recognition.

Cryptography

Security Cryptanalysis in High-Order Improved Fast Encryption Algorithm for Multimedia

Abstract
A rapid multimedia encryption method (Fast Encryption Algorithm for Multimedia, FEA-M) is introduced in this study. This study presents an improved way to increase strength and toughness to improve the security of encryption to make it difficult to break through such attacks. In addition, this paper will refer to the background utilized by FEA-M over the years and its attack methodologies and enhancements.

Proactive (*k, n*) Threshold Secret Sharing Scheme with Variant *k* and *n*

Abstract
A secret sharing scheme protects the secret by distributing it to a group of participants (nodes), and it allows for some groups of participants to collaborate together to reconstruct this secret. With regard to the (k, n) threshold scheme, k out of n or more participants can reconstruct the secret. The proactive secret sharing scheme periodically updates the distributed secret (shadow). Based on such a proactive secret sharing scheme, we propose a completely mobile proactive secret sharing scheme, which not only allows for the changing of participant number n, but arbitrarily changes the threshold k.

Network Security

A Countermeasure against Frequent Attacks Based on the Blom-scheme in Ad Hoc Sensor Networks

Abstract
The security of ad hoc networks is becoming more and more of a serious problem no matter what the usage level of any given ad hoc network is. In this paper, a scheme that

provides a solution for some of the challenging attacks that is currently plaguing ad hoc networks. It is an efficient scheme and secure authentication scheme that sets up more reliable communication links among all the nodes in any ad hoc systems.

Mutually Identity Authentications in GSM-based Anonymous Communications

Abstract
The security of ad hoc networks is becoming more and more of a serious problem no matter what the usage level of any given ad hoc network is. In this paper, a scheme that provides a solution for some of the challenging attacks that is currently plaguing ad hoc networks. It is an efficient scheme and secure authentication scheme that sets up more reliable communication links among all the nodes in any ad hoc systems.

Multimedia

Visual-based Embedding Systems with Targeted Secret Disclosures and Applications

Abstract
A VWC-system (Visual-based Watermarking Concealment System) is proposed to create a watermark embedding procedure for the purpose of protecting intellectual rights. In addition to the feature of watermarking system, the embedded information can hold the secret for the encryption key. This VWC-system uses the frequency-domain watermarking technique together with the concept of visual cryptography in image processing. For the extraction of the watermark, it is categorized as semi-blind. Therefore, the extraction of the embedded share-watermark does not require a host-image. Furthermore, the embedded part is only a share, meaning a portion of the watermark generated from a chosen KFI (Key Feature Image) by visual cryptography. The remaining shares not used in the embedding procedure are kept until the extraction procedure in order to reveal the targeted secret or copyright watermark shown in the message of the watermark image. An extra benefit of using our VWC-system is the secret key delivery. This feature can be easily applied in a symmetric-key cryptosystem for a common key agreement via a public channel. In other words, our proposed VWC-system offers a new application and a novel watermark embedding process, for practical cryptosystem applications, offering improved security.

Fidelity Colour Multimedia Image with Adaptive Data Hiding on Projection Dimensions

Abstract
There have been considerably explored in the spatial domain and frequency domain for information hiding researches. In this paper, we propose a projection-based data hiding scheme in spatial domain for colour images, where the image quality is remarkably enhanced as well as the higher capacity is still guaranteed. In our scheme, we firstly take one pixel in the cover image as the basis, and project it onto a plane. Then, the algorithm of embedding process is proposed in terms of the segment, coding and transformation of location to fulfill the data hiding in the colour image systems. In our paper, not only the size of the cover image remains the same, but also the cover image is no long required in the course of extracting the embedding information. As a result, our paper is to offer an efficient scheme that both achieve the great fidelity and high capacity for the colour multimedia image systems.

Digital Forensics

Digital Evidence Seizure in Network Intrusions against Cyber-crime on Internet Systems

Abstract
With the global trend of internet, many companies set up websites for international recognition and marketing. However, the hackers and potential attackers lurk on internet. More and more web attack methods have invented and threat these vulnerable websites. Recently, the “Code Injection” has become the major problem, such as SQL Injection, ASP Injection, PHP Injection and XSS (Cross Site Scripting) attack. The victims include the biggest Blog “Wrench” in Taiwan and the largest friend’s community website “MySpace” in the world. In this paper, we will analyze the XSS attack and propose a scheme to collect evidence on network systems after XSS attack. We also propose our management strategy against XSS attack.

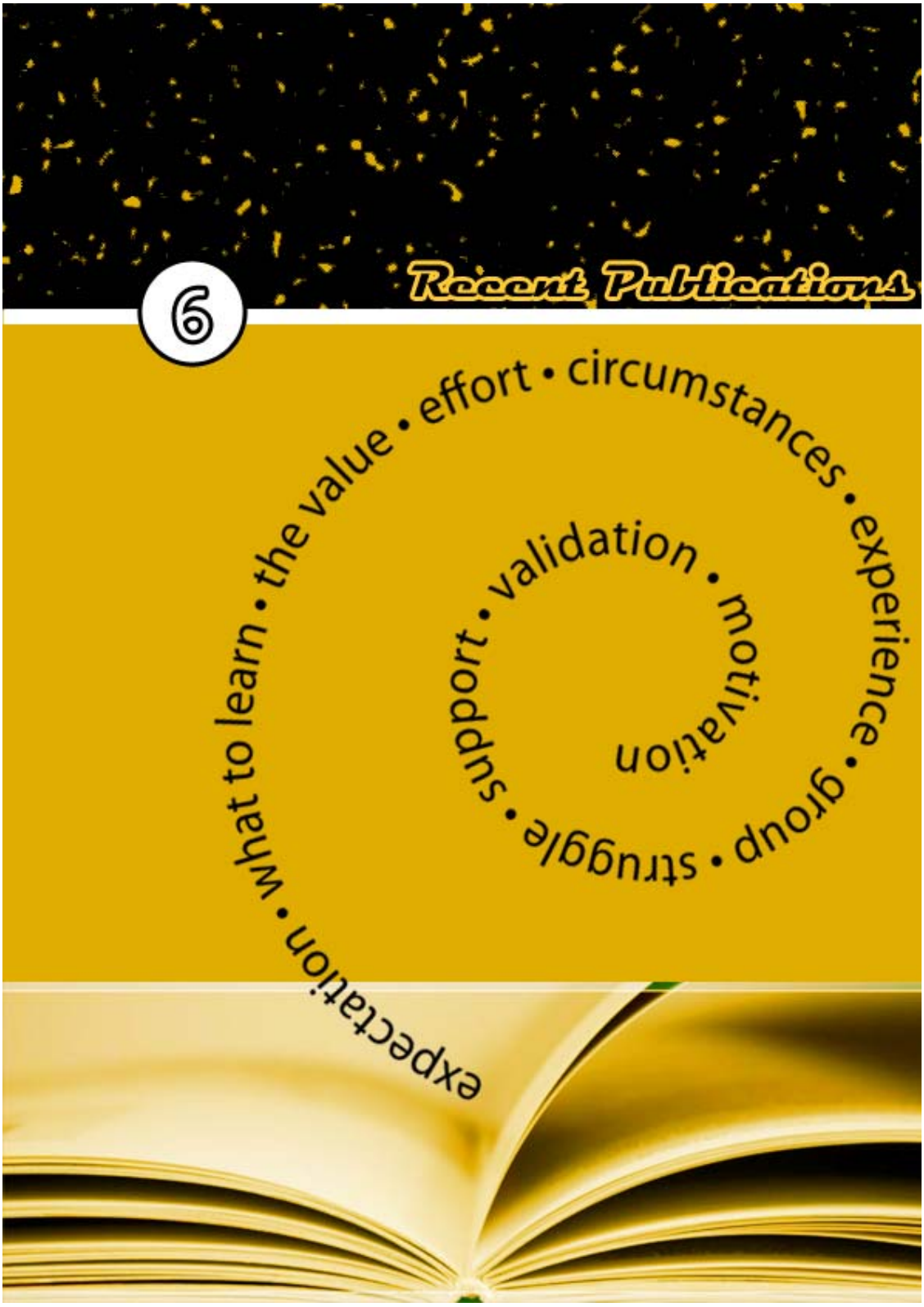
Measures of Retaining Digital Evidence to Prosecute Computer-based Cyber-crime

Abstract
With the rapid growth of computer and network systems in recent years, there has also been a corresponding increase in cyber-crime. Cyber-crime takes many forms and has garnered much attention in the media, making information security a more urgent and important priority. In order to fight cyber-crime, criminal evidence must be gathered from these computer-based systems. This is quite different from the collection of conventional

criminal evidence and can confuse investigators attempting to deal with the forensics of cyber-crime, highlighting the importance of computer forensics. In this paper, we offer solutions to guard against cyber-crime through the implementation of software toolkits for computer-based systems. In this way, those who engage in criminal acts in cyber-space can be more easily apprehended.

Persistence and Desistance: Examining the Impact of Hacker Ethics Observed to Taiwan's Juveniles

Abstract
The internet community has been addressing the unethical behavior of juvenile delinquents for years. Nevertheless, the concepts of hacker shame and ethics have received little empirical study from a theoretical perspective in the field of cyber criminology. Braithwaite's reintegrative shaming theory posits that it can restrain individuals from committing future offenses and, indeed, that those who participate in this shaming process are less likely to consider breaking the law in the first place. Among the abundance of criminological theories, the reintegrative shaming theory may be the most suitable theory to explain hacker activities. This study focuses on the working relationship between nine juvenile delinquents and the shaming mechanism applied to them. However, applying this approach to reduce recidivism among computer hackers in Taiwan requires a great deal of time and effort. It is proposed that the states of shame or remorse are associated with compounded affective processes of hacker ethics. The proposed solution creates a code of ethics for hackers, distinguishes right from wrong, and ensures a greater success for Braithwaite's reintegrative shaming methods. There is an intention to account for shaming issue in recidivism. Problems and solutions related to the shaming theory are discussed, as well as their usefulness in the context of community-based restorative justice. It is argued in this study that reintegrative shaming, without appropriate consideration for the offender's personal code of ethics, is insufficient when handling hacking offenses committed by juveniles. Our main concern is to find out how to help or encourage the offender reintegrate and re-enter into the community, and avoid failure. It is hoped that this strategy can prevent future offending behaviors by these juveniles. Implications drawn from the findings are discussed, and suggestions are offered to ensure the success of this theory when applied to juvenile hackers.


6
Recent Publications
what to learn • the value • effort • circumstances • experience • group • struggle • support • validation • motivation • expectation

Recent (Partial) Publications

1. **"Adaptive Data Hiding in Edged Areas of Images with Spatial LSB Domain Systems,"** *IEEE Transactions on Information Forensics and Security*, Vol. 3, Issue 3. pp. 488-497, Sept. 2008.

Abstract
A new adaptive least-significant-bit (LSB) steganographic method is proposed upon pixel-value differencing (PVD) that provides a larger embedding capacity and imperceptible stego-images. The method exploits the difference value of two consecutive pixels to estimate how many secret bits will be embedded into the two pixels. Pixels located in the edge areas are embedded by *k*-bit LSB substitution method with a larger value of *k* than that of the pixels located in smooth areas. The range of difference values is adaptively divided into lower-level, middle-level, and higher-level. For any pair of consecutive pixels, both pixels are embedded by *k*-bit LSB substitution method. However, the value *k* is adaptive and is decided by the level which the difference value belongs to. In order to remain at the same level to which the difference value of two consecutive pixels belong, before and after embedding, a delicate readjusting phase is used. When compared to Wu et al.'s PVD and LSB replacement method, our experimental results show that our proposed approach provides both larger embedding capacity and higher image quality.

2 **"Genetic Algorithms Highlighting the Target Secret in Visual Cryptography,"** *Journal of Information Management*, April, 2008.

Abstract
Secure concern in visual cryptography is yet another cipher mechanism used in the lower computation requirements. Compared to the text-based cryptography, such as DES and RSA, the time cost in decryption is much saved due to the secret is gained directly by our human vision systems. In secure concerns, how to make visual cryptography practical applying in real cases in the computer systems, there are still open issues in this way. Accordingly, one of the studied literatures, the genetic-based algorithm was proposed to realize the visual cryptography in the shadow/share image generation, in such a way that the size of share image is able to remain the same one of target image showing the secret. It is great research work using the manner of the genetic-based algorithm. In this case, we further observed that the secret shown in the target image can be improved better in order to resolve the misconception in the recognition of critical secret reading. It is conducted the uniform generations of black-pixel and white-pixel in our proposed algorithms. As the experiments given in our scheme, the secret shown in the target image is really undoubtedly visible to make the confusions clear in the recognitions of critical view-points

3. **"Hash Cracking and Aftereffect on Authentication Procedures in Cyberspace,"** *IEEE Aerospace & Electronics Systems Magazine,* Vol. 22, Issue 1, pp. 3-7, Jan. 2007.

Abstract
In 2004, one of the big news was that a fundamental technique in Cryptography – one of the hash algorithms, MD5 (Message Digest 5) had been cracked. Soon after this event, it was announced that the SHA-1 (Secure Hash Algorithm) had been cracked as well. This series of information shocked the researches in the field of cryptography, and raised the attention of every related organization of security application mechanisms. Most agencies are still looking into the impact this may have, and are considering their future responses and solutions in the wake of these developments in the hash structure of cryptanalysis. Based on this information, this paper will discuss in detail the broken MD5 and SHA-1, which both are reported to have been cracked, and will investigate any impact, and propose recommendations for the applications in cyber-space, such as password authentication and forensic software, when using a hash algorithm.

4. "**Internet Forensics on the Basis of Evidence Gathering with Peep Attacks,**" *Computer Standards & Interfaces*, Vol. 29, No. 4, pp. 423-429, 2007.

Abstract
The Peep attack is a variant application of a Botnet. This paper proposes a forensic procedure to analyze the attack behavior and explains how to carry out a computer crime investigation. We also discuss the well-known BotNets engaged in the execution of a Peep attack. In our paper, we describe a Peep attack on the Internet as the paradigm of how a cyber-investigator needs to act in the case of a Cybercrime. When cyber detectives prepare to investigate a break in cyber security, there are some issues they must keep in mind and face up to. It is crucial to swiftly preserve digital evidence and conduct forensic analysis that any useful evidence is seized soon after the cybercrime has been committed. Furthermore, there are two phases of digital forensic analysis to retrieve useful evidence when facing a Cybercrime attack in our scheme. One phase observes the Internet attack action, and the other one introduces how to investigate each case in on-line analysis of sniffing packets and off-line examination of abnormal files. We believe that this analysis model is workable for any other form of BotNets presently being used.

5. "**Two-tier Authentication for Cluster and Individual Sets in Mobile Ad Hoc Networks**," *Computer Networks*, Vol. 51, No. 3, pp. 883-900, 2007.

Abstract
Mobile ad hoc networks (MANETs) have been proposed as an extremely flexible technology for establishing wireless communication. In comparison with fixed networks or traditional mobile cellular networks, some new security issues have arisen with the introduction of MANETs. Routing security, in particular, is an important and complicated issue. In this work, we propose a two-tier authentication scheme for cluster and individual sets, in MANETs. The first tier, based on a hash function and the MAC concept, provides fast message verification and group identification. The second tier, based on secret sharing technology, provides secure user identification. The scenario of two-tier authentication can prevent internal and external attacks, including black holes, impersonation, routing table overflows and energy consummation attacks.

6. "**Key Management of Secret Sharing in Frequent Migrations for Job Environments,**" *Far East journal of Applied Sciences*, Vol. 27, No.2, pp. 153-166, 2007.

Abstract
Secret sharing schemes are convenient to allow shadow holders gain access to a secret in accordance with the threshold scheme. The main benefit of using secret sharing in a dynamic manner is that the shadows can be used repeatedly to work out a common secret. In this paper, a particular secret sharing scheme is proposed aimed at the need of frequently updating a secret, due to the constant migration of the members in a group. In our scheme, the shadow is dynamically distributed and readily changed when required. The advantages proposed in our scheme include: a group member who has migrated will be rejected if s/he intends to reveal the common secret again, the common secret can be changed but the personal key associated with each member remains unchanged, and the shadows can be constantly updated but the common secret remains unchanged in order to increase the flexibility of the key management. Our proposed scheme is suitable for an environment of constant member migration in the secret revelation of real world applications.

7. "**Remote Table-based Log-in Authentication upon Geometric Triangle**", *Computer Standards & Interfaces*, Vol. 26, No. 2, pp. 85-92, 2006

Abstract
In this paper, a mechanism is proposed to realize the table-based log-in authentication of user registrations in a remote network system. The stored table, called the generating key table, exists in a remote server, whose work is to validate whether the

requesting user is legitimate or not. In our scheme, the keys planted in the generating key table are generated by geometric ways upon the triangular property on the two-dimensional coordinate plane, and are used for user authentication later. With our specific arrangements, the attacks of penetrating the stored table are prevented. Without loss of generality, in our scheme, the password can be chosen freely by the registering user, the dynamic operations for a user's insertion, deletion and password change can be conducted, and the verification process is efficiently carried out as well. In addition, an invertible formula is pointed out to address the issue of table-based log-in authentication scheme. It can be the principle of devising such table-based log-in authentication scheme.

8 "**Procedural Response and Digital Evidence Exposure in Information Security Incidents**", *Journal of Discrete Mathematical Sciences & Cryptography*, Vol. 9, No. 3, pp. 417-427, 2006.

Abstract
Electronics records of information systems can be easily altered and duplicate. Information, comprising criminal evidences which can prove guilt, must be gathered at the earliest opportune moment; this is not only critical for the computer criminal law enforcement unit in gathering evidences, but should also direct the victim's behavior when the crime is first discovered. Procedural for dealing with incidents of invasion and attack must be clearly laid out by organization, in advance, through on-going training of personnel. Supervisors must be aware of the most effective moment to deal with contingencies of information security, in order to minimize loss; in this paper, we describe strategies to deal with such contingencies. Our remedies also focus on the functional presentation of ready-to-wear forensic toolkits to secure digital, processing lawful efficacy after the information security incidents has occurred. In this way, an appropriate lawful prosecution can be carried out, the bringing the criminal to justice; demonstration of such vigilance can discourage criminal behavior.

9. "**Vowel-consonant Addressing Mode on Hashing for English Letter-oriented Keys,**" *Journal of Discrete Mathematical Science & Cryptography,* Vol. 8, No. 1, pp. 1-25, April, 2005, Taru publications, India.

Abstract
We propose a scheme using displacement addressing in this paper. The technique is based on a vowel-consonant addressing the English keys of a letter-string. Our scheme is capable of handling thousands of keywords, and enables each keyword to be mapped into a unique address in a continuous space. A set of letter-oriented keywords is technically transformed into a table containing the offset addresses and relevant constants associated with the hashing keywords. For each queried keyword, a

key-pair associated with the keyword is featured first. The physical address of this queried keyword is then pointed out, using the hashing function with the key-pair in conjunction with the utilization of the pre-stored table. With our implementation, not only are the times clearly less than that of the previous one but also the collisions do not significantly increase for a larger set of keywords. Therefore, we conclude that the scheme is quite suitable for the requirements of fast search and minimal space occupation in the data processing of keywords of a letter-string.

10. "**Anonymous Wireless Authentication on a Portable Cellular Mobile System**,"

IEEE Transactions on Computers, Vol. 53, No. 10, Oct., pp. 1317-1329, 2004.

Abstract

A secure and anonymous conference call set-up scheme is proposed for a portable cellular mobile system. The proposed scheme uses an identity-based concept, and enables a mobile unit and a base station to directly authenticate each other by their public identity. It provides mobile subscribers with user identification privacy. Each mobile unit joining in this system can determine whether it is part of a conference call, but it can not derive any further information about who else is also in the conference. That is to say that an anonymous property, accomplished through the aspect of the knapsack-like cipher mechanism, is achieved among the communicating mobiles. Furthermore, re-authentication in the course of hand-off is also discussed, and the re-authentication procedure is performed through a privacy homomorphism mechanism. The time computation with an 8-bit microcontroller handset is acceptable for performing an anonymous conference call in such mobile systems. Therefore, our scheme is feasible and able to be implemented in the existing wireless exploration environment.

7 Future Perspectives

The Future perspectives at ICCL

This Lab. is dedicated in the development of data-transmitting mechanism on the Internet, strengthening the data-transmitting procedure to avoid many kinds of security threats and to establish a connection with trust and security. Besides, it also helps the policeman in developing operations for acquiring digital evidence with effectiveness, transparency, and justice. Based on these targets, the future developing directions should be to develop more secure crypto logical systems and to pursue research in computer forensics for its procedure and application.

8 Working Environment

Working Environment at ICCL

Information Cryptology and Construction Lab. provides an apposite working environment for a Computer Engineer. Equipped with state-of- art facilities, and supported and motivated by some of the best in the field of Information Hiding, this Lab. proves to be an apotheosis place for future researchers.

The Lab. is stocked with all the requisite things for a budding researcher ranging from latest machines to work on to newest editions of books to study from and licensed software's, in addition to a round the clock high bandwidth internet service. The members working here are the masters of their respective fields and prove to an ideal guide whenever required. The separate small room in the Lab. for the students to take some rest while working. This attitude provided to students make them completely comfortable with restrict free approach to broaden their horizon of knowledge. The members of ICCL work in some of the most under-researched but extremely important topics of the contemporary scenario. The main areas of their research are related to Information Hiding and Network Security. This includes topics like Cryptography, Steganography, and Network Digital Forensics.

Working Experiences of the International Students

- **2007**

We (**Sajal Bhatia and Saurabh Gupta**), from LNM IIT, INDIA, were here at ICCL, Central Police University, Taiwan as a research trainee for 11 weeks from May, 14th, 2007 up till July 28, 2007 under Prof S. J. Wang (Director, ICCL). This internship gave us a solid foundation both in terms of the broad spectrum of knowledge. We could grasp as well as the priceless experience of living in this beautiful campus of CPU in the city of Tao-Yuan.

Working in ICCL has been an unforgettable experience for both of us. It has broadened the horizon of our knowledge acquainting us with the latest issues in the field of Cryptography, Steganography and Network Security, which we were unaware off. Being undergraduate students and majoring in Communication and Computers, the work experience at ICCL has imbibed in us the feeling to always aspire for something great and set new goals to achieve.

To accomplish whatever we have done in our internship, there were many people along the way who have been responsible for guiding us, advising us, encouraging us and even reprimanding us. They have been the prefect guide and a nonpareil friend at this crucial stage of our career and have taught us some of the pivotal lessons of life. To them, we are deeply grateful and would like to take this opportunity to offer our heartfelt appreciation. At the outset we would like to thank Prof S. J. Wang who took confidence in us and gave us this wonderful opportunity of coming to ICCL. We had a valuable experience being a part of this prestigious Lab. both academically and otherwise.

We are deeply indebted and thankful to our project leaders Prof. Liao, Kao- Dayu, Unicon, Lynn and Jeff, who irrespective of the situation always helped and supported us. They were a constant source of encouragement which in a long way helped us achieve our goals and develop self confidence. We consider ourselves to be fortunate persons being the students of such eminent personalities. They have been a source of strong inspiration for us and would always be a part of whatever success we achieve.

- **2008**

For the second consecutive year I (**Sajal Bhatia)** got an opportunity to work as a research trainee for 11 weeks at the prestigious Information Crypto and Construction Lab. (ICCL), located in the beautiful campus of Central Police University under the esteemed guidance of Prof. S.J. Wang. This was a special trip for me in the sense that along with the research work that I was involved in I also got a unique opportunity to present my research work done last year in IEEE ISI 2008. Presenting the paper in front of the best in the field of Information Security was an unforgettable experience.

This year I was involved in research on Wireless Sensor Network Security with a PhD student, C.W. Chen, from National Tsing Hua University. I also continued and finished last year work of preparing the ICCL Introduction Brochure. I was also involved in assisting my juniors in various projects assigned to them. Towards the end of my internship I along with one of my junior Udai proposed a new architecture model with novel polling algorithm for wireless sensor networks. We are working on the simulation/ comparison part of our proposed scheme and would be submitting the research work in some reputed conferences/journals. I had an unforgettable experience for the second time in a row and I am grateful to Prof. S.J. Wang for showing the confidence in my abilities and calling me to work again in ICCL. I am also thankful to Jeff, Lynn, H.Y. Chang to immense support which always inspires me to utilize my capabilities to the fullest and achieve the best.

I (**Udai Gupta**) was here at ICCL, Central Police University, Taiwan as a research trainee for 12 weeks from May, 14th, 2008 up till Aug 6, 2008 under Prof S. J. Wang (Director, ICCL). This internship was a pleasant and unforgettable experience. This internship gave me a unique opportunity to work beyond my domain to enhance my skills and improve my practical abilities. It has broadened the horizon of my knowledge acquainting me with the latest issues in the field of Computer Forensic, Cryptography and Network Security. Here I created an implementation for a journal paper which is ready for submission now. I also managed to transfer the website of ICCL from a windows server to a highly secure UNIX (SunOS10) Server (Sun UltraSparc-II) which was configured (including Web Server and FTP Server) by me under the supervision of Jeff. I would like to thank Prof S. J. Wang who believed in my abilities and gave me this wonderful opportunity. I had a valuable experience being a part of this prestigious Lab. both academically and otherwise. I am grateful to Jeff, Lynn, H.Y. Chang, who always encouraged me to achieve my goal and develop self confidence.

I (**Saransh Jain**) came to ICCL, Central Police University, Tao-Yuan, Taiwan for a research internship for 12 weeks from May 13 till August 7. I was assigned research work at Yuan-Ze University too. I am heartily thankful to Prof. S.J Wang who allowed me to be a part of this Lab. This was a great opportunity to me to enhance my skills and prepare myself for hard work. I learned a lot from this Lab. and the environment it provides for research. For me as an undergraduate student, I think it was the best way to utilize my summer vacation. I got to know how the research is done and how to get successful in it. I learned a lot about cultural aspects of Taiwan too. This place is really beautiful situated in the outskirts of Tao-Yuan city.

I worked in the projects assigned by mentors Prof. C.L. Chan, and Ph.D. Candidate D.Y. Kao and W.Y. Chiang. I worked for C4.5 algorithm improvement under Professor Chan, Maritime communication and paper on Cyber-stalking work under D.Y. Kao and steganography work under W.Y. Chiang. I am grateful to them since they always encouraged me to achieve my goal and develop self confidence.

I (**Kush Mathur**) came to ICCL, Central Police University, Tao-Yuan, Taiwan for a research internship for 12 weeks from May 13 till August 7. I was assigned research work at Oriental Institute of Technology(OIT) too. I am thankful to Prof. S.J. Wang who gave me such a great opportunity to be a part of this Lab. This opportunity gave me a platform to prove myself and to enhance my knowledge on the current research topics. I got to know how to write an academic paper and how to proceed in research. I liked the attitude with which all the members of this Lab. worked and I learned a lot from them. Central Police University is in outskirts of Tao-Yuan and the place is really very beautiful.

I worked in the research paper assigned by mentors Prof. M.L. Li and D.Y. Kao. I had done a research on group technology and solving cellular manufacturing problem under Prof M.L. Li in OIT, Taipei. Maritime communication project and paper on Cyber-stalking work under D.Y. Kao. One of the great experiences is to teach English to students of OIT. I came to know about the culture, tradition and history of Taiwan from them. I enjoyed their company a lot since they all are of the same age as mine. The given research topic is new to me but from my mentor Prof. M.L. Li, I learned to be smart and aggressive towards the project. His experience and guidelines directed me towards my goal which gives me self confidence and discipline in my work. I found Taipei as well organized city. It has been connected with MRT stations. I visit many good places in Taipei and interact with many local people. I found people of Taiwan very kind and always ready to help in your needs.

- **2009**

In my summers'09, I (**Aneesh Sharma**) got an opportunity to work as a trainee for 11 weeks at the prestigious lab ICCL, Taiwan. The summer of 2009 was one full of learning. Not only it was one of my most productive summers in a long time but it also proved to be fun. This internship has broadened my horizon by acquainting me with the latest issues in the field of Information Hiding and Computers forensics.

Through all of the things I did that summer I still had the time to enjoy sport, spend time with new friends at school, and also to relax.

During the summer I had two mentors, Prof. S. J. Wang and Prof. Da Yu Kao. Prof. Wang gave me great advice on everything like how to monitor and schedule my own work-day/week and also how to progress with research.
I'm deeply indebted and thankful to Prof. Amy C.F. Lee, Prof. Kao, Chi-Yao Weng, Lynn who irrespective of the situation always helped and supported me. This all around support helped me in accomplishing three conference papers. Out of which two are published in the field of Information Hiding and one is published in Computer Forensics.
As an undergraduate student, I think this was the best way to utilize my summers and get prepared for the journey ahead. I got to know how research is done and how to get successful in it. Also, I made some unforgettable friends during my stay in Taiwan.
With this I can conclude that my internship experience for summers'09 was truly unforgettable and one of the pivotal lesson of my life.

9
Project

(2005-2012)

- Information Protection and Secret Sharing Systems in Digital Image of Steganography (NSC 98-2221-E-015-001-MY3-), National Science Council (NSC), ROC 08/2009~07/2012
- Electronic-trend Cyber-Forensics and Configurations in Web-platform Access to Digital Evidence Analysis (NSC 97-2221-E-015-001-), National Science Council (NSC), ROC 08/2008~07/2009
- Security Studies in 3G Systems, (Grant XC97H84P), Chung-Shan Institute of Science & Technology, Ministry of National Defense, ROC 06/2008~11/2008
- International Collaboration for Advancing Security Technology – International Collaboration of Information Security on Research Capacity and Pivot Technology Development (NSC 96-3114-P-001-001-Y), Academia Sinica, ROC 05/2007~12/2007 (2/3)
- Mobile Secure Transaction Study Based upon Visual-cryptography-oriented Applications (2/2) (NSC 95-2221-E-015-002-MY2), National Science Council (NSC), ROC 08/2007~07/2008
- International Collaboration for Advancing Security Technology – International Collaboration of Information Security on Research Capacity and Pivot Technology Development--- Sub-project #3: Investigation on Advanced Remote Authentication Technologies (1/3) (NSC 94-3114-P-011-001 and NSC 95-3114-P-001-001-Y02), Academia Sinica, ROC 05/2006~04/2007
- Mobile Secure Transaction Study Based upon Visual-cryptography-oriented Applications (1/2) (NSC 95-2221-E-015-002-MY2), National Science Council (NSC), ROC 08/2006~07/2007
- Ad-hoc Sensor Networks with Key-management and Deployments against Compromise Attack and Cyber-crime Behaviors (2/2) (NSC 95-2221-E-015-003-), National Science Council (NSC), ROC 08/2006~07/2007
- Ad-hoc Sensor Networks with Key-management and Deployments against Compromise Attack and Cyber-crime Behaviors (1/2) (NSC 94-2213-E-015-001-), National Science Council (NSC), ROC 08/2005~07/2006

10
References

References

A. Referred Articles

1. C.H. Yang, C.Y. Weng, **S.J. Wang**, and H.M. Sun, "Capacity-raising Steganography Using Multi-Pixel Differencing and Pixel-Value Shifting Operations," Fundamenta Informaticae, accepted in Oct., 2009. (SCI)
2. C.H. Yang, C.Y. Weng, **S.J. Wang**, and H.M. Sun, "Grouping Strategies for Promoting Image Quality of Watermarking on the Basis of Vector Quantization," Journal of Visual Communication and Image Representation, accepted in Oct., 2009. (SCI)
3. **S.J. Wang** and D.Y. Kao, "The IP Address and Time in Cyber-crime Investigation," Policing: An International Journal of Police Strategies & Management, Vol 32. Issue 2, 2009. (SCI).
4. D.Y. Kao, **S.J. Wang,** and Frank F.Y. Huang "' SoTE: Strategy of Triple-E on Solving Trojan Defense of Cyber-crime Case," The Computer Law & Security Review - The International Journal of Technology Law and Practice (Elsevier), www.elsevier.com/locate/clsr, accepted in July 2009. (SCI)
5. C.H. Yang, C.Y. Weng, **S.J. Wang**, and H.M. Sun, "Codebook-linked Watermarking Scheme on Digital Images in Steganography," Fundamenta Informaticae, Vol. 92, pp. 397-409, 2009. (SCI)
6. **S.J. Wang**, D.Y. Kao, and Frank F.Y. Huang, "Procedure Guidance on Internet Forensics Coping with Copyright Arguments of Client-Server-based P2P Models," International Journal Computer Standards & Interfaces, Vol. 31, pp. 795-800, 2009. (SCI)
7. **S.J. Wang**, Y.R. Tsai, P.Y. Chen, and C.C. Shen, "A Scheme of Image-based Signature Verification upon Secret Sharing for Shopping in E-commerce Systems," Journal of Computers, appear in, 2009. (EI)
8. C.W. Chen, **S.J. Wang,** Y.R. Tsai, and H.C. Chen, "FTG-M: Fast-Reacting Tree-Based Group Key Agreement for Mobile Ad Hoc Networks," revised in IEEE Transactions on Wireless Communications, June, 2009. (SCI)
9. J.H. Huang, C.L. Chan, **S.J. Wang,** W.C. Chang, and Udai Gupta, "Intrusion Investigations Using Steganography for Log-file Forensics in Computer Systems," International Journal Computer Standards & Interfaces, revised in March, 2009. (SCI)
10. D.Y. Kao, Frank F.Y. Huang, and **S.J. Wang,** "'Persistence and Desistance: Examining the Impact of Reintegrative Shaming to Ethics in Taiwan Juvenile Hackers'," The Computer Law & Security Review - The International Journal of Technology Law and Practice (Elsevier), www.elsevier.com/locate/clsr, accepted in March. 2009. (SCI)
11. C.H. Yang, C.Y. Weng, **S.J. Wang**, and H.M. Sun, "Varied PVD+LSB Evading Detection Programs to Spatial Domain in Data Embedding Systems," Journal of Systems and Software, revised in March, 2009. (SCI)

12. **S.J. Wang**, Y.R. Tsai, and C.C. Shen, "Verifiable Threshold Scheme in Multi-secret Sharing Distributions upon Extensions of ECC," Wireless Personal Communications, Springer, appear in 2010. (SCI)
13. C.H. Yang and **S.J. Wang**, "Transforming LSB Substitution for Image-based Steganography in Matching Algorithms," Journal of Information Science and Engineering, accepted in Feb. 2009. (SCI)
14. **S.J. Wang,** I.S. Lin, L.C. Lin, and W.Y. Chiang, "A Secret Sharing Authentication Scheme for Digital Images," Journal of Computers, April, 2009. (EI)
15. **S.J. Wang**, J.Y. Lin, H.J. Ke, and S.W. Lin, "Visual-based Embedding Systems with Targeted Secret Disclosures and Applications," International Journal of Ad Hoc and Ubiquitous Computing, Vol. 04, No. 1, pp. 44-53, 2009. (EI)
16. C.H. Yang, C.Y. Weng, **S.J. Wang**, and H.M. Sun, "Adaptive Data Hiding in Edged Areas of Images with Spatial LSB Domain Systems," IEEE Transactions on Information Forensics and Security, Vol. 3, Issue 3. pp. 488-497, Sept. 2008. (SCI)
17. C.W Chen**, S.J. Wang**, and Y.R. Tsai, "TLPKA: Pairwise Key Agreement Based on the Geometrical Property of the Tangent Line in Ad Hoc Network Systems," International Journal of Hybrid Information Technology, Vol.2, No.4, 2008. (EI).
18. H.C. Chen**, S.J. Wang**, and J.H. Wen, "A Cryptographic Key Assignment Scheme with Adaptable Time-token Constraint in a Hierarchy," International Journal of Multimedia and Ubiquitous Computing, Vol. 3, No. 4, 2008. (EI)
19. C.H. Yang, **S.J. Wang,** C.Y. Weng, and H.M. Sun, "Information Hiding Technique Based on Blocked PVD," Journal of Information Management, Vol. 15, No. 3, pp. 29-48, 2008. (TSSCI, Taiwan Social Science Citation Index)
20. **S.J. Wang**, Y.H. Chang, and J.S. Lin, "A Visual-based Authentication Scheme in Wireless Carry-on Laptop Systems," Electronic Commerce Studies, Fall, 2008. (TSSCI, Taiwan Social Science Citation Index)
21. **S.J. Wang**, J.H. Huang, S.Y. Yao and C.L. Chan, "Digital Evidence Seizure in Remote Firewall-based Systems on Internet Forensics," Journal of e-Business, Vol. 10, No. 1, pp. 235-254, March, 2008. (TSSCI, Taiwan Social Science Citation Index)
22. **S.J. Wang,** H.C. Wang, and L.C. Lin, "Genetic Algorithms Highlighting the Target Secret in Visual Cryptography," Journal of Information Management, Vol. 15, No. 2, pp. 85-108, April 2008. (TSSCI, Taiwan Social Science Citation Index)
23. **S.J. Wang,** K.L. Lin, Y.H. Chang, W.Y. Chiang, and J.H. Huang, "Unveiling Controversy of Trojan Defense on Internet Forensics," The Journal of Forensic Sciences, accepted in March. 2008.
24. **S.J. Wang,** Y.H. Chang, H.J. Ke, and W.S. Juang, "Digital Evidence Seizure in Network Intrusions against Cyber-crime on Internet Systems," Journal of Computers, Jan. 2008. (EI)
25. **S.J. Wang,** Y.R. Tsai, and J.W. Chen, "Strategies Averting Sybil-type Attacks Based on the Blom-scheme in Ad Hoc Sensor Networks," Journal of Communications, Vol. 03, Issue 01, pp. 20-26, 2008. (EI)
26. H.C. Chen, **S.J. Wang,** and J.H. Wen, "Packet Construction for Secure Conference Call Request in Ad Hoc Network Systems," Information Sciences, Vol. 177, pp. 5598-5610, 2007. (SCI)

27. **S.J. Wang**, "Information Hiding at Oblivious Watermarking Scheme upon Alternative Threshold in Spatial Domains," Journal of Discrete Mathematical Science & Cryptography, Vol. 10, No. 3, pp. 359-384, 2007, Taru publications, India. (EI)
28. **S.J. Wang,** H.C. Shu, Y.H. Chang, J.H. Hwang, "Immigration E-records in Secure Hierarchical Management upon Forensic Information Demands," The Journal of Forensic Sciences, Accepted in Oct. 2007.
29. **S.J. Wang,** Y.R. Tsai and P.Y. Chen, "Strategies of Proactive (k, n) Threshold Secret Sharing and Applications in a Secure Message Exchange System," Journal of Computers, accepted in Dec. 2007. (EI)
30. H.C. Chen, **S.J. Wang,** and J.H. Wen, "Role-based Proactive Scheme in an Access Control Hierarchy," Journal of Statistics & Management Systems, accepted in June, 2007. (EI)
31. **S.J. Wang** and D.Y. Kao, "Internet Forensics on the Basis of Evidence Gathering with Peep Attacks," International Journal Computer Standards & Interfaces, Vol. 29, pp. 423-429, 2007. (SCI)
32. **S.J. Wang,** H.J. Ke, J.H. Huang, and C.L. Chan, "Hash Cracking and Aftereffect on Authentication Procedures in Cyberspace," IEEE Aerospace & Electronics Systems Magazine, Vol. 22, Issue 1, pp. 3-7, Jan. 2007. (SCI)
33. H.C. Chen, **S.J. Wang,** and J.H. Wen, "A Key Distribution Scheme for Live Multi-session upon Generalized Group-Oriented Cryptography," the Far East Journal of Mathematical Sciences, accepted in April 2007. (EI)
34. **S.J. Wang**, J.Y. Lin, and J.H. Huang, "Internet Forensics with the Digital Evidence Investigations in Cyber-casino Scenarios," Journal of Forensic Sciences, accepted in April 2007.
35. **S.J. Wang,** Y.R. Tsai, L.S. Chiu, and I.S. Lin, "Mutually Identity Authentication in GSM-based Anonymous Communications," Journal of Computers, Vol. 18, No. 2, pp. 33-46, July, 2007. (EI)
36. **S.J. Wang**, "Measures of Retaining Digital Evidence to Prosecute Computer-based Cyber-crime," International Journal Computer Standards & Interfaces (SC&I), Vol. 29, No. 2. pp. 216-223, Jan., 2007. (SCI)
37. Y.R. Tsai and **S.J. Wang**, "Two-tier Authentication for Cluster and Individual Sets in Mobile Ad Hoc Networks," Computer Networks, Vol. 51, pp. 883-900, 2007. (SCI)
38. **S.J. Wang**, "Key Management of Secret Sharing in Frequent Migrations for Job Environments," Far East Journal of Applied Mathematics, Vol. 27, No. 2, 2007. (EI)
39. **S.J. Wang** and P.S. Hu, "Key Management for Pay-TV Broadcast Systems in Hierarchy," Journal of Discrete Mathematical Science & Cryptography, Vol. 9, No. 3, pp. 449-496, Dec. 2006, Taru publications, India. (EI)
40. **S.J. Wang**, "Procedural Response and Digital Evidence Exposure in Information Security Incidents," Journal of Discrete Mathematical Science & Cryptography, Vol. 9, No. 3, pp. 417-427, Dec. 2006, Taru publications, India. (EI)
41. J.H. Huang**, S.J. Wang,** A.C. Chiang and Y.L. Hwang, "Real-time Response against Abnormal Invasion in the case of Applications Using NetKeeper Systems," The Journal of Forensic Sciences, Sept. 2006.
42. **S.J. Wang**, "Fundamental Common Key Establishment in MANETs upon Geometric Mathematics," Far East Journal of Mathematical Sciences, Vol. 23, Issue 1, pp. 127-135, Oct., 2006. (EI)

43. **S.J. Wang** and D.Y. Kao, "Invasions of Malware in Cyber-space and Countermeasures Improving Cyber-security," ACM Operating Systems Review (ACM OSR), Accepted in June, 2006. (EI)
44. **S.J. Wang,** C.C. Wu, and C.Y. Lin, "In View of Completeness and Proof Ability of Digital Photo Evidence upon Watermarking Authentication Schemes in Forensic Sciences," Communications of the CCISA, Vol. 12, No. 2, April, 2006.
45. C.H. Yang and **S.J. Wang**, "Weighted Bipartite Graph for Locating Optimal LSB Substitution for Secret Embedding," Journal of Discrete Mathematical Science & Cryptography, Vol. 9, No. 1, pp. 153-164, April, 2006, Taru publications, India. (EI)
46. **S.J. Wang,** H.J. Ke, J.H. Huang and S.H. Chen, "Evidence Ability Study Based upon Wartermarking KH-scheme in Digital Forensics," The Journal of Forensic Sciences, March 2006.
47. **S.J. Wang,** C.H. Yen, I.S. Lin and H.H. Chen,"Authentication System on the Basis o f Visual-based Recognitions," Journal of Computers, Vol. 16, No. 5, 2005. (EI)
48. C.H. Yang and **S.J. Wang,** "Accelerating VQ-based Codeword Search on the Basis of Partial Search Strategy," International Journal Computer Standards & Interfaces, Vol 28, No. 2, pp. 231-240, 2005. (SCI)
49. **S.J. Wang,** Y.R. Tsai, and James Chen, "Node Communications in View of Security upon Ad Hoc Networks," Communications of the CCISA, Vol. 11, No. 4, Oct., 2005.
50. J.H. Huang, H.J. Ke, **S.J. Wang,** and P. F. Chung, "Linux-based Firewall Mechanism of *iptables* in Information Security District Systems," The Journal of Forensic Sciences, Vol. 59, pp. 63-80, Sept., 2005.
51. **S.J. Wang,** "Steganography of Capacity Required Using Modulo Operator for Embedding Secret Image," Applied Mathematics and Computation, Vol. 164, pp. 99-116, May, 2005. (SCI)
52. **S.J. Wang**, "Vowel-consonant Addressing Mode on Hashing for English Letter-oriented Keys," Journal of Discrete Mathematical Science & Cryptography, Vol. 8, No. 1, pp. 1-25, April, 2005, Taru publications, India. (EI)
53. **S.J. Wang** and C.H. Yang, "Hierarchy-oriented Searching Algorithms Using Alternative Duplicate Codewords for Vector Quantization Mechanism," Applied Mathematics and Computation, Vol. 162, No. 2, pp. 559-576, March, 2005. (SCI)
54. **S.J. Wang** and C.M. Chuang, "Anonymous Message Communications with User Hierarchy in a Multicast System," Applied Mathematics and Computation, Vol. 159, No. 1, pp. 95-112, Nov., 2004. (SCI)
55. **S.J. Wang**, "Anonymous Wireless Authentication on a Portable Cellular Mobile System," IEEE Transactions on Computers, Vol. 53, No. 10, Oct., pp. 1317-1329, 2004.(SCI)
56. H.C. Chen, **S.J. Wang,** and J.H. Wen, "Models for Role-based Hierarchical Access Control Organizations," Communications of the CCISA, Vol. 10, No. 4, Oct., 2004.
57. **S.J. Wang,** "Direct Construction of a Secret in Generalized Group Oriented Cryptography," International Journal Computer Standards & Interfaces, Vol. 26, No. 5, pp. 455-460, Sept., 2004. (SCI)
58. **S.J. Wang,** "Threshold Verification Scheme to a Valid-signature Using Identity Only on Specialized Approval," Applied Mathematics and Computation, Vol. 152, No. 2, pp. 373-383, May, 2004. (SCI)

59. **S.J. Wang** and H.J. Ke, "Curbing Gambling Activities on the Internet," IEEE Aerospace and Electronic Systems Magazine, pp. 33-35, April, 2004. (SCI Extend)
60. **S.J. Wang** and Y.C. Kuo, "A Secure Mechanism for Fine Payment Acting on Internet Transaction," Web Journal of Chinese Management Review (http://www.cmr.tuan.com), Vol. 7, No. 2, pp. 158-171, April, 2004, Hong Kong.
61. **S.J. Wang,** "The High Capacity in Embedding Logo implementing the Intellectual Property Using Tree-oriented Coding Mechanism," Bulletin of the College of Engineering, National Taiwan University, pp. 119-126, Feb, 2004.
62. **S.J. Wang,** "Remote Table-based Log-in Authentication Upon Geometric Triangle," to be appear in International Journal Computer Standards & Interfaces, Vol. 26, No. 2, pp. 85-92, 2004. (SCI)
63. **S.J. Wang,** H.J. Ke and W.C. Kuo, "A Parser Software Platform Setp-up Looking for Specified Web Sites," The Journal of Forensic Sciences, Vol. 56, pp. 123-136, March 2004.
64. **S.J. Wang** and Y.R. Tsai, "Private Communications in Hierarchical Group-Mobile Radio Systems," Journal of Discrete Mathematical Science & Cryptography, Vol. 7, No. 2, pp. 187-201, 2004, Taru publications, India. (EI)
65. **S.J. Wang,** H.J. Ke, and K.L. Ho, "Forensic Tools Study in Response to Information Crisis Incident," Communications of the CCISA, Vol. 10, No. 1, Jan., 2004.
66. **S.J. Wang,** "Yet Another Log-in Authentication Using N-dimensional Construction Based on Circle Property," IEEE Transactions on Consumer Electronics, Vol. 49, pp. 337-341, May, 2003. (SCI)
67. **S.J. Wang** and C.H. Yan, "Fast Access with Certificate Revocation List in PKI Mechanism," Bulletin of the College of Engineering, National Taiwan University, Vol. 88, pp. 97-107, June, 2003.
68. **S.J. Wang** and C.S. Lin, "Prototype System Set-up for Required Real-time Query on Counterfeit Certificate Recognitions," The Journal of Forensic Sciences, Vol. 55, pp. 41-55, March, 2003.
69. **S.J. Wang** and H.J. Ke, "Authentication and Watermarking in Information Hiding," Communications of the CCISA, Vol. 9, No. 2, March, 2003.
70. **S.J. Wang** and C.K. Lu, "A Scheme of Non-sensible Document in Transit with Secret Hiding," Journal of Information Management, Vol. 9, No. 2, pp. 169-182, Jan. 2003 (TSSCI, Taiwan Social Science Citation Index).
71. **S.J. Wang**, "Encryption Packet Broadcast Using Factorial Number Structure," Journal of Computers, Vol. 14, No. 3, pp. 23-31, 2002.
72. **S.J. Wang,** H.J. Ke and C.Y. Yang, "Evidence Investigation for Intruders in Web Systems," Communications of the CCISA, Vol. 8, No. 4, Sept., 2002.
73. **S.J. Wang** and D.Y. Kao, "Security Forensics and Empirical Strategies for Preventing from the Intrusion of Trojan Horse," Journal of Information, Technology and Society, pp. 109-117, Dec. 2001.
74. K.S. Yang, D. Y. Kao and **S.J. Wang,** "A Model Analysis of Information Criminal Whereabouts --- In Case of Illegal Compact Disc on Sale," The Journal of Forensic Sciences, Vol. 51, pp. 91-102, 2001.
75. D. Y. Kao and **S.J. Wang,** "The Planning and Management Strategy for Protecting the Hacker Intruding in Telephone Information Systems," Police Science Quarterly, Vol. 31. No. 5, pp. 161-170, 2001.

76. **S.J. Wang** and Y.C. Lin, "A Scheme of Fast key Recover on Broadcast Network upon the Three-center-location of a Triangle," Journal of Computers, Vol. 12, No. 1, March, 2000.
77. C.H. Yan and **S.J. Wang**, "A New Strategy of Secure-control-card with Software implementation for Police Agency," Police Science Quarterly, Vol. 30, No. 6, May, 2000.
78. **S.J. Wang** and P. S. Hu, "A Dynamic Access Control Scheme with High Security Based on the Square Modular Technique in Hierarchy Structure," Bulletin of the College of Engineering, National Taiwan University, Vol. 78, pp. 61-66, Feb. 2000.
79. D. Y. Kao and **S.J. Wang,** "The Behavior Analysis of Investigating Intruder Activities in Internet Networks," The Journal of Forensic Sciences, Vol. 48, pp.57-70, 1999.
80. **S.J. Wang** and J.K. Jan, "A New Addressing Method for Letter-Oriented Keys, " Journal of Systems & Software, Vol. 46. pp. 77-88, 1999. (SCI)
81. **S.J. Wang**, Y.R. Tsai and J.F. Chang, "A New Two-Way and Location-Secure Authentication Scheme Based on Secret Sharing, " Journal of the Chinese Institute of Electrical Engineering, Vol. 6, No. 4, 1999. (EI)
82. **S. J. Wang** and J. F. Chang, "Smart-Card Based Secure Password Authentication Scheme," Computers & Security, Vol. 15, No. 3, pp. 231-237, 1996. (SCI)
83. **S. J. Wang** and J. F. Chang, "A Hierarchical and Dynamic Group-Oriented Cryptographic Scheme," IEICE Trans. Fundamentals, Vol. E79-A, No.1, pp. 76-85, January 1996. (SCI)
84. H. T. Liaw, **S. J. Wang** and C. L. Lei, "A Dynamic Cryptographic Key Assignment Scheme in a Tree Structure," International Journal of Computers & Mathematics with Applications, Vol. 25, No. 6, pp. 109-114, 1993. (SCI)
85. H. T. Liaw, **S. J. Wang** and C. L. Lei, "Secure Dynamic User Hierarchy Scheme Based on the Knapsack Problem," International Journal of Computer Systems Science & Engineering, Vol. 4, pp.210-216, 1993. (SCI)
86. J. K. Jan and **S. J. Wang**, "A Dynamic Access Control Scheme Based Upon the Knapsack Problem," International Journal of Computers & Mathematics with Applications, Vol. 26, No. 12, pp. 75-86, 1993. (SCI)
87. J. K. Jan, C. C. Chang and **S. J. Wang**, "A New Dynamic Key-Lock-Pair Access Control Scheme," Computers & Security, Vol. 10, No. 2, pp. 129-139, 1991. (SCI)

B. International Conferences/Proceedings

1. D.Y. Kao, **S.J. Wang,** A. Sharma, and Frank F.Y. Huang, "A Case-Oriented Model of Digital Forensics on Infected Zombie Computers," IEEE-PROCEEDINGS, 2009 The Second International Workshop on Multimedia,

Information Privacy and Intelligent Computing Systems (MPIS-2009), Korea, Dec. 2009.
2. H.M. Sun, C.Y. Weng, and **S.J. Wang**, "A Scheme of Modulo-based Capacity-improvement upon EMD Systems," IEEE-PROCEEDINGS, presented in Sept., Japan, 2009.
3. H.C. Chen, **S.J. Wang,** J.H. Wen, and C.W. Chen, "Temporal and Location-based RBAC Model," IEEE-PROCEEDINGS, The 5th International Joint Conference on Networked Computing and Advanced Information Management (NCM-2009), http://www.aicit.org/ncm/ presented in Aug., Seoul, Korea, 2009.
4. C.W. Chen, **S.J. Wang**, Y.R. Tsai, and H.C. Chen, "A Framework of Multicast Key Agreement for Distributed User on 3G-WLAN," IEEE-PROCEEDINGS, The 5th International Joint Conference on Networked Computing and Advanced Information Management (NCM-2009), http://www.aicit.org/ncm/ presented in Aug., Seoul, Korea, 2009.
5. C.F. Lee**,** L.C. Lin**, S.J. Wang,** and C.Y. Weng, "Balancing Capacity and Fidelity in Image Multimedia of Steganographic Systems," 2009 Joint Workshop (Taiwan/Japan/Korea) on Information Security, http://jwis2009.nsysu.edu.tw/index.php/jwis/jwis2009 presented in Aug. 2009.
6. **S.J. Wang,** Y.R. Tsai, C.C. Shen, and P.Y. Chen, "Hierarchical Key Agreement Protocols in Group-user Systems," IEEE-PROCEEDINGS, presented in Aug., China, 2009.
7. C.H. Yang, C.T. Huang, and **S.J. Wang**, "Reversible Steganography Based on Side Match and Hit Pattern for VQ-Compressed Images," IEEE-PROCEEDINGS, presented in Aug., China, 2009.
8. W.Y. Chiang, **S.J. Wang,** C.Y. Weng, and C.H. Yang, "Robustness-set in Watermarking Embedding Systems Using Codebook Classifications," ACM-PROCEEDINGS, The Third International Conference on Ubiquitous Information Management and Communication (ICUIMC-2009), presented in SKKU, Suwon, Korea, Jan. 2009.
9. H.J. Ke, **S.J. Wang**, and W.Y. Chiang, "Watermarking Damage to Risk Multimedia in Intellectual Property Systems," 2008 International Computer Symposium, Taiwan, Nov. 2008.
10. **S.J. Wang**, Y.R. Tsai, and J.J. Shen, "Dynamic Threshold Multi-secret Sharing Scheme Using Elliptic Curve and Bilinear Maps," presented in IEEE-PROCEEDINGS, 2008 The Third International Symposium on Smart Home (SH-2008), Sanya, Hainan Island, China, Dec. 2008.
11. D.Y. Kao, **S.J. Wang,** K. Mathur, S. Jain, Frank F.Y. Huang, "Dataset Analysis of Proxy Logs Detecting to Curb Propagations in Network Attacks," IEEE-PROCEEDINGS, 2008 The First International Workshop on Multimedia, Information Privacy and Intelligent Computing Systems (MPIS-2008), Taiwan, Dec. 2008.
12. **S.J. Wang**, Y.R. Tsai, and P.Y. Chen , "Authentication Scheme in Peer-to-peer Based Live Stream Sharing Management Systems," presented in IEEE-PROCEEDINGS, 2008 The International Conference on Intelligent Systems Design and Applications (ISDA), Taiwan, Nov. 2008.

13. C.H. Yang, S.C. Huang, C.T. Huang, and **S.J. Wang**, "Non-embedded Image Protection Approaches Based on Vector Quantization," presented in IEEE-PROCEEDINGS, 2008 The International Conference on Intelligent Systems Design and Applications (ISDA), Taiwan, Nov. 2008.
14. **S.J. Wang,** I.S. Lin, Y.L. Hsieh, and C.Y. Wen, "Secret Sharing Systems with Authentication-based Steganography," presented in IEEE-PROCEEDINGS, 2008 International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), Harbin, China, Aug. 2008.
15. D.Y. Kao, **S.J. Wang,,** Frank F.Y. Huang**,** S. Bhatia, and S. Gupta "Dataset Analysis of Proxy Logs Detecting to Curb Propagations in Network Attacks," presented in LNCS-PROCEEDINGS, Pacific Asia Workshop on Cybercrime and Computer Forensics (PACCF 2008) in conjunction with ISI 2008, Lecture Notes in Computer Science (LNCS), published in Spring-Verlag, Taipei, Taiwan, June 2008.
16. H.C. Chen**, S.J. Wang**, J.H. Wen, and C.W. Chen, "Flexible Key Assignment for a Time-token Constraint in a Hierarchy," IEEE-PROCEEDINGS, 2008 International Conference on Multimedia and Ubiquitous Engineering, presented in Busan l, Korea, April, 2008.
17. C.W Chen**, S.J. Wang**, and Y.R. Tsai, "Geometrically Reciprocal Authentication Scheme Using Shift Tangent Line in Ad Hoc Network Systems," IEEE-PROCEEDINGS, 2008 International Conference on Multimedia and Ubiquitous Engineering, presented in Busan, Korea, April 2008.
18. H.M. Sun, C.Y. Weng and **S.J. Wang,** "Histogram-based Undetectable Fidelity Image in Steganography as MSB Controller," ACM-Proceedings, The Second International Conference on Ubiquitous Information Management and Communication, presented in SKKU, Suwon, Korea, Jan. 2008.
19. **S.J. Wang,** Y.H. Chang, W.Y. Chiang, and W.S. Juang, "Investigations in Cross-site Script on Web-systems Gathering Digital Evidence against Cyber-Intrusions," IEEE-PROCEEDINGS, Forensics for Future Generation Communication Environments (F2GC) 2007, presented in Korea, Dec. 2007.
20. **S.J. Wang,** H.S. Chen, P.Y. Chen and Y.R. Tsai, "Security Cryptanalysis in High-Order Improved Fast Encryption Algorithm for Multimedia," IEEE-PROCEEDINGS, Future Generation Communication Networking (FGCN) 2007, presented in Korea, Dec. 2007.
21. **S.J. Wang,** Y.R. Tsai and P.Y. Chen, "Proactive (k, n) Threshold Secret Sharing Scheme with Variant k and n," IEEE-PROCEEDINGS, 2007 International Conference on Intelligent Pervasive Computing, will be presented in Korea, Oct. 2007.
22. D.Y. Kao, F.F.Y. Huang**,** and **S.J. Wang,** "Maturity and Shame: Bringing Computer Ethics to Taiwan's Juvenile Delinquents," accepted in Australian and New Zealand Society criminology, the 20th Annual ANZSOC Conference, Adelaide, Australia, Sept. 2007.
23. C.H. Yang, **S.J. Wang**, and C.Y. Weng, **"**Analyses of Pixel-Value-Differencing Schemes with LSB Replacement in Steganography," to present in

IEEE-PROCEEDINGS, the third international Conference on Intelligent Information Hiding and Multimedia Signal Processing, Nov. 2007.

24. T.C. Wu, A. Perrig, W.S. Juang, M. Reiter, **S.J. Wang**, B.Y. Yang, C. Kuo, M. Luk, J. McCune, A. Studer, H.Y. Chen, C.W. Chen, X.Y. Chen, H.C. Chi, C.Y. Fu, Y.C. Lin, K. Tsay, and Z.R. Yang, "Remote authentication and ubiquitous trust establishment: scalable group key establishment," Proceedings of 2007 Second iCAST/CMU/TRUST Joint Conference on Security and Privacy Technologies, pp. 8-10, Taipei, Taiwan, June 2007.
25. **S.J. Wang**, J.Y. Lin, H.J. Ke, and Y.H. Chang "Targeted Secret Disclosures in Visual-based Watermarking Concealment Systems," IEEE-PROCEEDINGS, International Conference on Multimedia and Ubiquitous Engineering (MUE 2007), Seoul, Korea, April 2007.
26. **S.J. Wang**, Y.R. Tsai and J.W Chen, "A Countermeasure Against Frequent Attacks Based on the Blom-scheme in Ad Hoc Sensor Networks," IEEE-PROCEEDINGS, International Symposium on Wireless Pervasive Computing 2007, Puerto Rico, Feb. 2007.
27. D.Y. Kao, **S.J. Wang,** and F.F.Y. Huang, and Y.H. Chang "Inferring Social Network from Forensic Assessment Model of P2P Copyright Infringement," The 3th Asia-Pacific International Conference on Knowledge management (KMAP2006), Hong Kong, Dec. 2006.
28. D.Y. Kao, **S.J. Wang**, and F.F.Y. Huang, "An Information Based Management on the Analysis of Internet Perpetrators," The 3th Asia-Pacific International Conference on Knowledge management (KMAP2006), Hong Kong, Dec. 2006.
29. H.C.H. Ko, **S.J. Wang,** and I.S. Lin, "Flexible Key Management in Required Frequent Migrations upon Secret Sharing Scheme**,"** Proceedings of WISA 2006: The 7th International Workshop on Information Security Applications, Korea, Aug. 2006.
30. D.Y. Kao**, S.J. Wang**, and F.F.Y. Huang, "Digitized Forensic Investigation at P2P Copyright Controversy, Infringement," present in LNCS-PROCEEDINGS, International Conference on Intelligence and Security Informatics (IEEE ISI-2006), Lecture Notes in Computer Science (LNCS), published in Spring-Verlag, USA, May, 2006.
31. **S.J. Wang**, S. Chen and J.H. Hwang, "Survey of Cyber-security and a Fundamental of Geometric Common Key Agreement in MANETs," to be presented in the IASTED International Conference on Networks and Communication Systems (NCS 2006), ISBN: 0-88986-590-6, March, Thailand, 2006. (ACTA Press)
32. **S.J. Wang**, H.J. Ke, and J.H. Hwang, "Concerns and Aftermath of Cracking Hash in Cyber-space," International Forensic Science Symposium (IFS Symposium Taipei 2005), Nov., Taipei, Taiwan, 2005.
33. D.Y. Kao and **S.J. Wang**, "Evidences and Forensics at IP Address Clue in Cyber Crime," present in 17th Meeting of the International Association of Forensic Sciences, Hong-Kong, Aug. 2005.
34. **S.J. Wang** and C.H. Yang, "Gathering Digital Evidence in Response to Information Security Incidents," present in LNCS-PROCEEDINGS, International Conference on Intelligence and Security Informatics (IEEE ISI-

2005), Lecture Notes in Computer Science (LNCS), published in Spring-Verlag, Atlanta, Georgia, USA, May, 2005.
35. **S.J. Wang**, "Multicasting Secret Images using a Knapsack-like Cipher System," to be presented in 17th International Conference on Computer Applications in Industry and Engineering (CAINE-2004), Orlando, Florida, USA, Nov. 2004. (INPEC)
36. Y.R. Tsai and **S.J. Wang**, "Routing Security and Authentication Mechanism for Mobile Ad Hoc Networks," presented in IEEE-PROCEEDINGS, IEEE VTC 2004-Fall with Wireless Technologies for Global Security, Sept. 2004, USA.
37. **S.J. Wang** and H.J. Ke, "Countermeasures in Curbing Gambling Activities on Internet in Taiwan," presented in IEEE-PROCEEDINGS, IEEE Conference of 2003 International Carnahan Conference on Security Technology, Oct. 2003.
38. **S.J. Wang** and K.S. Yang, "Watermark Embedding Mechanism Using Modulus-based for Intellectual Property Protection on Image Data," LNCS-PROCEEDINGS, E-Commerce and Web Technologies, Lecture Notes in Computer Science (LNCS), No. 2455, published by Springer-Verlag, 2002.
39. **S.J. Wang,** Patrick S. Chen and Y.C. Lin, "Log-in Authentication Based on Locating Centers of a Triangle," presented in IEEE-PROCEEDINGS, IEEE TENCON 2002, held in Beijing of China in Sept. 2002.
40. **S.J. Wang** and C.H. Yang, "A Threshold-Verification Scheme to a Valid-signature Using the Identity Check," Workshop Proceedings: The Seventh International Conference on Distributed Multimedia Systems with workshop on Cryptology and Network Security, Taiwan, Sept. 2001.
41. **S.J. Wang** and K.S. Yang, "A Scheme of High Capacity Embedding on Image Data Using Modulo Mechanism," Proceedings of WISA 2001: The Second International Workshop on Information Security Applications, Seoul, Korea, Sept. 2001.
42. **S.J. Wang** and Y.H. Chang, "A Vowel-oriented Retrieval Scheme on Minimal Perfect Hashing Searching," presented in Internal Computer Symposium (ICS-2000), held at Chi-Yi, National Cheng-Chung University, Dec. 6-8, 2000.
43. **Wang,** and J.F. Chang, "A Conference Key Multicasting Scheme Using Knapsack and Secret Sharing," LNCS-PROCEEDINGS, Database and Expert Systems Applications-DEXA'99, Lecture Notes in Computer Science (LNCS), No. 1677, published by Springer Verlag, 1999.
44. **S. J. Wang** and J. F. Chang, "An Efficient Access Control Scheme Based on Arithmetic Coding," International Conference on Wireless Computer Communication: Emerging Business Opportunities (Infocom'94), Tata McGraw-Hill, New Delhi, India; 1995, 1995.
45. **S. J. Wang** and J. F. Chang, "An Efficient Access Control Scheme Based on Arithmetic Coding," to be published in INFOCOM'94 International Conference on Wireless Computer Communication: Emerging Business Opportunities, 1994.

C. Academic Reports/Domestic Conferences

1. **S.J. Wang**, L.C. Lin, and W.C. Chang, "Log-Forensics Detecting Intruders in Steganography," 2008 the 14th Conference of Information Management Research & Practice, Soochow University, Taiwan, Dec., 2008.
2. **S.J. Wang**, and C.W. Wu, "T-Tool: Forensics Tool in Windows Systems for Investigations of Digital Evidence," 2008 the 14th Conference of Information Management Research & Practice, Soochow University, Taiwan, Dec., 2008.
3. **S.J. Wang** and C.W. Chen, "Rootkit Debate in Trojan Defense in Compuer Forensics," 2008 Symposium on Digital Life Technologies: Building a Safe, Secured and Sound (3S) Living Environment, National Cheng-kung University, June, 2008.
4. **S.J. Wang**, H.Y. Chang, and J.S. Lin, "Information Investigations in Network Forensics Using GUI Tools," Proceedings of the 18th National Conference on Information Security R.O.C., Taiwan, May, 2008.
5. J.H. Huang, C.L. Chan and **S.J. Wang**, "Cyber-crime Investigations in the Utilizations of Forensic Tools," Open Forum in Central Police University, May, Taiwan, 2008.
6. W.Y. Chiang, **S.J. Wang,** and J.S. Lin, "Ubiquitous-based RFID Establishing High-tech Society with High Security and Quality," 2007 the 13th Conference of Information Management Research & Practice, Dec., 2007.
7. W.Y. Chiang, **S.J. Wang,** and J.S. Lin, "Fidelity Colour Multimedia Image with Adaptive Data Hiding on Projection Dimensions," presented in National Computer Symposium, Taiwan, Dec., 2007.
8. **S.J. Wang**, H.H. Chen and T.Y. Lin, "Secure Transmission in Networks Using Visual Cryptography Systems," TANET2007, National Taiwan University, Taiwan, Oct., 2007.
9. **S.J. Wang,** Y.H. Chang, and J.S. Lin, "Visual Authentications to User Log-in Mobile Computer Systems," Proceedings of the 10th of Conference of Electronic Commence 2007, Taipei University, Taipei, Taiwan, Oct. 2007.
10. J.H. Hwang, **S.J. Wang,** and P.H. Hsieh, "Cookies Relevance to Digital Evidence and Preservation on Internet Forensics," to be presented in 2007 Symposium on Digital Life Technologies-Building a Safe, Secured and Sound (3S) Living, National Cheng-kung University, June, 2007.
11. W.Y. Chiang, **S.J. Wang,** and J.S. Lin, "Intelligent Information on Secret Sharing Functions in Law Enforcement Systems," to be presented in Proceedings of the 17th National Conference on Information Security R.O.C., Taiwan, June, 2007.
12. **S.J. Wang**, I.S. Lin, and J.S. Lin, **"**Visual Two-way BAN-Logic Authentication in User Identity Systems," Conference of Electronic Commerce and Digital Life 2007 (ECDL 2007), Shih Chien University, Taipei, Taiwan, March 2007.
13. **S.J. Wang**, D.Y. Lin, and J.S. Lin, **"**PRT Authentication in a Secure RFID System Curbing Hybrid Frequent Attacks," Conference of Electronic

Commernce and Digital Life 2007 (ECDL 2007), Shih Chien University, Taipei, Taiwan, March 2007.

14. **S.J. Wang** and S.Y. Yao, **"**Trusted Forensic Reports on the Basis Cross-verification in Tool Utilizations," Conference of Electronic Commerce and Digital Life 2007 (ECDL 2007), Shih Chien University, Taipei, Taiwan, March 2007.
15. **S.J. Wang**, J.Y. Lin, and J.S. Lin, "Integrity Evidence for Chain of Custody in Signature Payload Embedding Systems," 2006 the 12th Conference of Information Management Research & Practice, National Formosa University, Taiwan, Dec., 2006.
16. **S.J. Wang,** Y.H. Chang, and J.S. Lin, "Evidence Gathering to SSL-VPN-conncected Network Systems in Forensics," Taiwan Conference Business and Information 2006, TBI2006), National Taipei Univ., Taipei, Taiwan, Nov. 2006.
17. **S.J. Wang**, C.H. Ko, and J.S. Lin, "Evidence Gathering to Copyright Controversy with Information Broadcast in Cyberspace," Taiwan Conference Business and Information 2006, TBI2006), National Taipei Univ., Taipei, Taiwan, Nov. 2006.
18. **S.J. Wang**, I.S. Lin, and J.S. Lin, **"**Evidence Gathering to Social Engineering of Phishing Fraud in Cyberspace," Taiwan Conference Business and Information 2006, TBI2006), National Taipei Univ., Taipei, Taiwan, Nov. 2006.
19. D.Y. Kao, **S.J. Wang,** and F.F.Y. Huang, "Cyber-crime in Computer-based Systems Increases the Need for Digital Forensic Analysis," the Conference of Crime Investigation and Forensic Sciences, Taiwan, Nov. 2006.
20. **S.J. Wang,** C.C. Wu, and J.Y. Lin, "A Half-tone Scheme Embedding Digital Evidence Proof Ability in Forensic Sciences," presented in Proceedings of the 16th National Conference on Information Security R.O.C., Taiwan, June, 2006.
21. **S.J. Wang,** H.C. Wang, and L.C. Lin, "Genetic Algorithms Highlighting the Stacked Secret in Visual Cryptography," 2006 Symposium on Digital Life Technologies-Building a Safe, Secured and Sound (3S) Living, National Cheng-kung University, June, 2006.
22. **S.J. Wang**, S.H. Chen, H.J. Ke, J.H. Hwang, and Y.H. Chang, "Integrated Forensic Tools Operating in Information Security Incidents," Conference of Electronic Commerce and Digital Life 2006 (ECDL 2006), National Taipei Univ., Taiwan, Feb., 2006.
23. S.Y. Yao and **S.J. Wang**, "Improved Remote Forensics on the Internet Systems," 2005 the 11th Conference of Information Management Research & Practice, Shih Chien University, Taiwan, Dec., 2005.
24. **S.J. Wang** and Da-Yu Kao, "Cybercrime Myths in the Justice Systems," Proceedings of the 15th National Conference on Information Security R.O.C., National Sun Yat-Sen University, Taiwan, June, 2005.
25. **S.J. Wang,** H.J. Ke, S.H. Chen and C.H. Yang, "Proof Ability of Digital Photo Evidence in an Embedding System," 2005 Symposium on Digital Life and Internet Technologies, National Cheng-kung University, June, 2005.
26. **S.J. Wang,** C.H. Kuo and C.H. Yang, "Visual Authentication Scheme to Multiple-Identify User in Computer-based Systems," Proceedings of the 16th

International Conference of Information Management (ICIM'2005), Fu Jen Catholic University, May, 2005.

27. **S.J. Wang** and D.Y. Kao**, "**Strategies to Combat the Invasion of Cyberspace from Within," the Conference of Crime Investigation and Forensic Sciences, Taiwan, Nov. 2004.
28. **S.J. Wang**, S.C. Chen, H.W. Hwang, and J.H. Wen**, "**Adaptive Hierarchical Access Model in a Role-base System," Proceedings of the 14th National Conference on Information Security R.O.C., National Taiwan University of Science and Technology, Taipei, June, 2004.
29. **S.J. Wang,**' C.H. Yang, Y.R. Liao, and C.H. Kuo, "Intellectual Rights Embedding Systems using VQ Coding," Proceedings of the 15th International Conference of Information Management, Chung-Yuan Christian University, Taipei, May, 2004.
30. **S.J. Wang** and H.J. Ke, "Chaotic Watermark against Intellectual Property on Secure Information Hiding," 2003 Symposium on Digital YLife and Internet Technologies, National Cheng-kung University, Oct. 2003.
31. **S.J. Wang,** H.J. Ke, and W.J. Kuo, "Web Parser Design for Specified Web-site Search," 2003 Symposium on Digital Life and Internet Technologies, National Cheng-kung University, Oct. 2003.
32. **S.J. Wang** and S.T. Yeh, "Fast Similar Image Search Based on the Partial Space Computing," Proceedings of the 14th International Conference of Information Management, National Chung-Cheng University, Sept., 2003.
33. **S.J. Wang** and C.H. Lin, "Digital Audit Table on E-payment Systems," Proceedings of the 14th International Conference of Information Management, National Chung-Cheng University, Sept., 2003.
34. **S.J. Wang,** H.J. Ke and C.H. Yen, "User Identification Scheme upon the Visual Cryptography," Proceedings of the 13th National Conference on Information Security R.O.C., Cheng-Gung University, Aug. 2003.
35. C.Y. Yang and **S.J. Wang**, "Data Access Mode and User Authentication in a Enhanced CA system," The 8th Conference of Information Management Research & Practice, Kaoshiung, Taiwan , Nov. 2002.
36. **S.J. Wang** , C.H. Lin and J.S. Lin, "Digital Evidence Investigation on E-payment Systems," The Management of E-Commerce 2002, Taichung, Taiwan, Nov. 2002.
37. C.Y. Yang and **S.J. Wang,** "High-tech Countermeasures against Cybercrime," The 6th Information Management and Law Enforcement Conference, Central Police University, Taoyuan, Taiwan, May, 2002.
38. **S.J. Wang** and H.F. Shih, "Fast Spatial Image Search System with Compact Space Utilization," Proceedings of the 13th International Conference of Information Management (ICIM'2002), Taipei, May, 2002.
39. S.C. Chen, J.H. Wen and **S.J. Wang,** "A New Identity-Based and Generalized Group-Oriented Cryptographic Scheme," Proceedings of the Twelfth National Conference on Information Security R.O.C., Taichung, May, 2002.
40. **S.J. Wang** and I.S. Lin, "High Capacity for Data Embedding Using Quadtree Coding," Proceedings of the 12th National Conference on Information Security R.O.C., Taichung, May, 2002.

41. H.J. Ke, C.H. Lin and **S.J. Wang,** "Intellectual Rights Dispute from On-line Game," Workshop of Relialbe Information System and Environment, National Chaio-Tung University, Taiwan, Dec. 2001.
42. **S.J. Wang** and C.S. Lin, "Efficient Image Search System Using Block-oriented extraction," presented in CSIM2000, The 7th Conference of Information Management Research & Practice, Taipei, Taiwan, Dec. 2001.
43. **S.J. Wang** and D.Y. Kao, "Cybertrace for Digital Evidence," Communications of the CCISA, Vol. 8, No. 1, Dec. 2001.
44. D.Y. Kao and **S.J. W**, "Some Cyber-crime Problems Related to the Law Protection, Violation, Enforcement and Information Forensics in the Information Society,**"** Information Security Newsletter, Vol. 7, No. 3, 2001.
45. **S.J. Wang** and D.Y. Kao, "The Bearing Duty of Network Malicious Programs Writing,", Information Security Newsletter, Vol. 7, No. 1, 2000.
46. **S.J. Wang** and Y.C. Kuo, "A Secure Mechanism for a Small Amount of Fine Payment Acting on Internet Transaction," presented in CSIM2000, The 6th Conference of Information Management Research & Practice, National Chaio-Tung University, Taiwan, Dec., 2000.
47. **S.J. Wang** and P.S. Hu, "The Scheme of Secure Pay-TV System with Cryptographic Key Management," presented in TANET2000, National Chung-Kung University, Oct, 2000.
48. **S.J. Wang** and D.Y. Kao, "The Study of Source Investigation to Network Intruders with Torrential DoS attack," Information and Education, Aug., 2000.
49. **S.J. Wang** and D.Y. Kao, "The Development and Jeopardy of Constraining Network Intrusion and Hacker Behavior," Information Security Newsletter, Vol. 5, No. 3, pp. 97-106,1999.
50. D.Y. Kao and **S.J. Wang**, "The Study of Network Worms and Internet besieging Mechanism," Communications of the Institute of Information and Computing Machinery, Vol. 2, No. 3, pp. 57-64,1999.
51. **S. J. Wang**, Y. R. Tsai and J. F. Chang, 'A Group-Call Cryptographic Multicasting Scheme in Multilevel Trunked Mobile Radio Systems,' Proceedings of the 9th National Conference on Information Security R.O.C., pp. 361-37, 1999.

D. General Magazines/Talks

1. S.J. Wang, (Information Cryptology and Construction Lab.), "Digital Evidence and Forensics on the Computers and Network Systems (XXXXI) －Image-file in case of operations of DD," NetAdmin, http://www.netadmin.com.tw/, PCuSER, Dec., 2009.
2. S.J. Wang, (Information Cryptology and Construction Lab.), "Digital Evidence and Forensics on the Computers and Network Systems (XXXX) －

Watermarking embedding and Camera-forensics," NetAdmin, http://www.netadmin.com.tw/, PCuSER, Nov., 2009.
3. S.J. Wang, (Information Cryptology and Construction Lab.), "Digital Evidence and Forensics on the Computers and Network Systems (IXXXX) －Key door in digital forensics –Image File," NetAdmin, http://www.netadmin.com.tw/, PCuSER, Oct., 2009.
4. S.J. Wang, (Information Cryptology and Construction Lab.), "Digital Evidence and Forensics on the Computers and Network Systems (XXXVIII) － Memory Forensics," NetAdmin, http://www.netadmin.com.tw/, PCuSER, Sept., 2009.
5. S.J. Wang, (Information Cryptology and Construction Lab.), "Digital Evidence and Forensics on the Computers and Network Systems (XXXVII) －Evidence in PDA and Forensic Procedures in Cyber-crime," NetAdmin, http://www.netadmin.com.tw/, PCuSER, Aug., 2009.
6. S.J. Wang, (Information Cryptology and Construction Lab.), "Digital Evidence and Forensics on the Computers and Network Systems (XXXVI) －Evidence Investigations in Mobile handset with Digital Forensics," NetAdmin, http://www.netadmin.com.tw/, PCuSER, July, 2009
7. S.J. Wang, (Information Cryptology and Construction Lab.), "Digital Evidence and Forensics on the Computers and Network Systems (XXXV) －Myths: Show Forensic Power to Vista in Window Systems," NetAdmin, http://www.netadmin.com.tw/, PCuSER, June, 2009.
8. S.J. Wang, (Information Cryptology and Construction Lab.), "Digital Evidence and Forensics on the Computers and Network Systems (IVXXX) －Countering: Steganography vs. Forensic Analysis," NetAdmin, http://www.netadmin.com.tw/, PCuSER, May, 2009.
9. S.J. Wang, (Information Cryptology and Construction Lab.), "Digital Evidence and Forensics on the Computers and Network Systems (XXXIII) －Evidence Investigations in Unix/Linux System Using the Power of TCT," NetAdmin, http://www.netadmin.com.tw/, PCuSER, April, 2009.
10. S.J. Wang, (Information Cryptology and Construction Lab.), "Digital Evidence and Forensics on the Computers and Network Systems (XXXII) －On-line Message and Forensics in Cyber-crime," NetAdmin, http://www.netadmin.com.tw/, PCuSER, March, 2009.
11. **S.J. Wang**, (Information Cryptology and Construction Lab.), "Digital Evidence and Forensics on the Computers and Network Systems **(XXXI)** － New Generation USB: U-Key Applied to Information Security and Forensics," NetAdmin, http://www.netadmin.com.tw/, PCuSER, Feb., 2009.

12. **S.J. Wang**, (Information Cryptology and Construction Lab.), "Digital Evidence and Forensics on the Computers and Network Systems **(XXX)** －Remote Forensics in a Toolkit Operatoin **-**Helix 2.0," NetAdmin, http://www.netadmin.com.tw/, PCuSER, Jan, 2009.
13. **S.J. Wang**, (Information Cryptology and Construction Lab.), "Digital Evidence and Forensics on the Computers and Network Systems **(IXXX)** － Evidence Spider Spreading in Computer Forensics," NetAdmin, http://www.netadmin.com.tw/, PCuSER, Dec., 2008.
14. **S.J. Wang**, (Information Cryptology and Construction Lab.), "Digital Evidence and Forensics on the Computers and Network Systems (**VIIIXX**) －Digital Evidence Investigations in P2P Network Systems," NetAdmin, http://www.netadmin.com.tw/, PCuSER, Nov., 2008.
15. **S.J. Wang**, (Information Cryptology and Construction Lab.), "Digital Evidence and Forensics on the Computers and Network Systems **(VIIXX)** －Perspectives to PDA Forensics," NetAdmin, http://www.netadmin.com.tw/, PCuSER, Oct., 2008.
16. **S.J. Wang**, (Information Cryptology and Construction Lab.), "Digital Evidence and Forensics on the Computers and Network Systems **(VIXX)** －Leading Tool in Forensics: Encase Studies," NetAdmin, http://www.netadmin.com.tw/, PCuSER, Sept., 2008.
17. **S.J. Wang**, (Information Cryptology and Construction Lab.), "Digital Evidence and Forensics on the Computers and Network Systems **(VXX)** －Visual-table Maker in Forensic Analysis against Cyber-criminals,"NetAdmin, http://www.netadmin.com.tw/, PCuSER, Aug, 2008.
18. **S.J. Wang**, (Information Cryptology and Construction Lab.), "Digital Evidence and Forensics on the Computers and Network Systems **(IVXX)** －Rootkit Utilization against Trojan Controversy on Computer Forensics,,"NetAdmin, http://www.netadmin.com.tw/, PCuSER, July, 2008.
19. **S.J. Wang**, (Information Cryptology and Construction Lab.), "Digital Evidence and Forensics on the Computers and Network Systems (**XXIII**) －Watch out Conversation Evidence on Internet Forensics," NetAdmin, http://www.netadmin.com.tw/, PCuSER, June, 2008.
20. **S.J. Wang**, (Information Cryptology and Construction Lab.), "Digital Evidence and Forensics on the Computers and Network Systems (**XXII**) －Audit to Trace the Key-Evidence in Computer Forensics," NetAdmin, http://www.netadmin.com.tw/, PCuSER, May, 2008.
21. **S.J. Wang**, (Information Cryptology and Construction Lab.), "Digital Evidence and Forensics on the Computers and Network Systems (**XXI**) －Accessible Digital Evidence Whereever the Investigation is required: Remote Forensics," NetAdmin, http://www.netadmin.com.tw/, PCuSER, April, 2008.
22. **S.J. Wang**, (Information Cryptology and Construction Lab.), "Digital Evidence and Forensics on the Computers and Network Systems **(XX)** －Helix of Live-CD," NetAdmin, http://www.netadmin.com.tw/, PCuSER, March, 2008.

23. **S.J. Wang**, (Information Cryptology and Construction Lab.), "Digital Evidence and Forensics on the Computers and Network Systems **(IXX)** ─ Digital Forensics in Open Systems with the Operations of TCT-ware," NetAdmin, http://www.netadmin.com.tw/, PCuSER, Feb., 2008.
24. **S.J. Wang**, (Information Cryptology and Construction Lab.), "Digital Evidence and Forensics on the Computers and Network Systems **(XVIII)** ─Encase Guide and Enforcement Studies," NetAdmin, http://www.netadmin.com.tw/, PCuSER, Jan., 2008.
25. **S.J. Wang**, (Information Cryptology and Construction Lab.), "Digital Evidence and Forensics on the Computers and Network Systems **(XVII)** ─FTK Guide and Enforcement Studies," NetAdmin, http://www.netadmin.com.tw/, PCuSER, Dec., 2007.
26. **S.J. Wang**, (Information Cryptology and Construction Lab.), "Digital Evidence and Forensics on the Computers and Network Systems **(XVI)** ─ Remote Forensics to lock the Suspicion in Network Systems," NetAdmin, http://www.netadmin.com.tw/, PCuSER, Nov., 2007.
27. **S.J. Wang**, (Information Cryptology and Construction Lab.), "Digital Evidence and Forensics on the Computers and Network Systems **(XV)** ─ Cyber-trail against Trojan Injection on Internet Forensics," NetAdmin, http://www.netadmin.com.tw/, PCuSER,Oct., 2007.
28. **S.J. Wang**, (Information Cryptology and Construction Lab.), "Digital Evidence and Forensics on the Computers and Network Systems **(IXV)** ─ Evidence Seizure at Cross-site Script (XSS) on Internet Forensics," NetAdmin, http://www.netadmin.com.tw/, PCuSER, Sept., 2007.
29. **S.J. Wang**, (Information Cryptology and Construction Lab.), "State of the Art of Cryptography, Ever, Current and Future: Applications and Trend in Modern Computers & Communications **(IV)** ─ Key-stroke with Crypto-Forensics," NetAdmin, http://www.netadmin.com.tw/, PCuSER, Aug., 2007.
30. **S.J. Wang**, (Information Cryptology and Construction Lab.), "Digital Evidence and Forensics on the Computers and Network Systems **(XIII)** ─ Internet Forensics on Audit Records and Cyber-trails," NetAdmin, http://www.netadmin.com.tw/, PCuSER, July, 2007.
31. **S.J. Wang**, (Information Cryptology and Construction Lab.), "Security and Coding World **(I)** ─ Code History in Oriental and West," Benesse, http://www.benesse.com.tw, Editing Reviews, June, 2007.
32. **S.J. Wang**, (Information Cryptology and Construction Lab.), "Digital Evidence and Forensics on the Computers and Network Systems **(XII)** ─ VPN on Internet Forensics," NetAdmin, http://www.netadmin.com.tw/, PCuSER, June, 2007.
33. **S.J. Wang**, (Information Cryptology and Construction Lab.), "Digital Evidence and Forensics on the Computers and Network Systems **(XI)** ─Categories and Software Developments in Information Forensics," NetAdmin, http://www.netadmin.com.tw/, PCuSER, May, 2007.
34. **S.J. Wang**, (Information Cryptology and Construction Lab.), "Digital Evidence and Forensics on the Computers and Network Systems **(X)** ─Firewall Systems

on Internet Forensics," NetAdmin, http://www.netadmin.com.tw/, PCuSER, April, 2007.
35. **S.J. Wang**, (Information Cryptology and Construction Lab.), "Digital Evidence and Forensics on the Computers and Network Systems **(IX)** －Cookies on the Internet Forensics," NetAdmin, http://www.netadmin.com.tw/, PCuSER, March, 2007.
36. **S.J. Wang**, (Information Cryptology and Construction Lab.), "Digital Evidence and Forensics on the Computers and Network Systems **(VIII)** －Trust it of Cross-verification Forensic Tools," NetAdmin, http://www.netadmin.com.tw/, PCuSER, Feb., 2007.
37. **S.J. Wang**, (Information Cryptology and Construction Lab.), "Steganography of Multimedia for Privacy on the Internet **(XI)** －Genetic Connections to Visual Cryptography," iThome,Vol. 23, PC home Publication Group, http://service.pchome.com.tw, Oct., 2006.
38. **S.J. Wang**, (Information Cryptology and Construction Lab.), "High-tech Cyber-crime on the Computers and Internet (**XI**) －Benefits on the Internet and Tricks at Web-site Visits," iThome,Vol. 22, PC home Publication Group, http://service.pchome.com.tw, July, 2006.
39. **S.J. Wang**, (Information Cryptology and Construction Lab.), "Web Surveillance and Management on the Cyberspace (**V**) －Secure Web-mail Sytems Coping with the User-friendly Trends," CONNECTIMES, The Instit ute for Information Industry, Jan., 2006.
40. **S.J. Wang**, (Information Cryptology and Construction Lab.), "Digital Evidence and Forensics on the Computers and Network Systems **(VII)** － Countermeatures against the Attacks of BotNets in the Cyberspace," CONNECTIMES, The Instit ute for Information Industry, Jan., 2006.
41. **S.J. Wang**, (Information Cryptology and Construction Lab.), "Steganography of Multimedia for Privacy on the Internet **(X)** －Text-based Information Hiding with Secret Transmissions," CONNECTIMES, The Instit ute for Information Industry, Dec., 2005.
42. **S.J. Wang**, (Information Cryptology and Construction Lab.), "Web Surveillance and Management on the Cyberspace (**IV**) －Secure Email in Authentication and Privacy Requirements," CONNECTIMES, The Instit ute for Information Industry, Nov., 2005.
43. **S.J. Wang**, (Information Cryptology and Construction Lab.), "Steganography of Multimedia for Privacy on the Internet **(IX)** － Explore the Secret behind the Multimedia Systems," CONNECTIMES, The Instit ute for Information Industry, Oct., 2005.
44. **S.J. Wang**, (Information Cryptology and Construction Lab.), "Digital Evidence and Forensics on the Computers and Network Systems **(VI)** － Where the Genuine Evidence is in a Digitized System," CONNECTIMES, The Institute for Information Industry, Sep., 2005.
45. **S.J. Wang**, (Information Cryptology and Construction Lab.), "State of the Art of Cryptography, Ever, Current and Future: Applications and Trend in Modern Computers & Communications **(III)** － Code-breaking in

Communication Systems," CONNECTIMES, The Institute for Information Industry, Aug., 2005.
46. **S.J. Wang**, (Information Cryptology and Construction Lab.),"Steganography of Multimedia for Privacy on the Internet **(VIII)**－The Discovery of Genetics on Visual Cryptography," CONNECTIMES, The Institute for Information Industry, to appear in June, 2005.
47. **S.J. Wang**, (Information Cryptology and Construction Lab.),"Web Surveillance and Management on the Cyberspace **(III)** － The Risk Perspectives and Enhancements of Data Accessing to Clients in Network Systems," CONNECTIMES, The Institute for Information Industry, May, 2005.
48. **S.J. Wang**, (Information Cryptology and Construction Lab.),"Digital Evidence and Forensics on the Computers and Network Systems **(V)-** Portable Live-CD Linux Systems on Computer Forensics," CONNECTIMES, The Institute for Information Industry, April, 2005.
49. **S.J. Wang**, (Information Cryptology and Construction Lab.),"Steganography of Multimedia for Privacy on the Internet **(VII)**－The Applications of Visual Cryptography on Gray-Images" CONNECTIMES, The Institute for Information Industry, March, 2005.
50. **S.J. Wang**, (Information Cryptology and Construction Lab.), "Digital Evidence and Forensics on the Computers and Network Systems **(IV)**- Authentication of Digital Evidence on Digital Photo-pictures," CONNECTIMES, The Institute for Information Industry, Feb., 2005.
51. **S.J. Wang**, (Information Cryptology and Construction Lab.), "State of the Art of Cryptography, Ever, Current and Future: Applications and Trend in Modern Computers & Communications **(II)** － Amazing Quantum in the Applications of Cryptography," CONNECTIMES, The Institute for Information Industry, Jan., 2005.
52. **S.J. Wang**, (Information Cryptology and Construction Lab.), "State of the Art of Cryptography, Ever, Current and Future: Applications and Trend in Modern Computers & Communications **(I)** －Art of Cipher in the War," CONNECTIMES, The Institute for Information Industry, Dec., 2004.
53. **S.J. Wang**, (Information Cryptology and Construction Lab.), "Steganography of Multimedia for Privacy on the Internet **(VI)** － Watermarking and Intellectual Rights on Multimedia," CONNECTIMES, The Institute for Information Industry, Nov., 2004.
54. **S.J. Wang**, (Information Cryptology and Construction Lab.), "Steganography of Multimedia for Privacy on the Internet **(V)**－ Secure Concerns on a Variety of Colours in Visual Cryptography, CONNECTIMES, The Institute for Information Industry, Oct., 2004
55. **S.J. Wang**, (Information Cryptology and Construction Lab.), "Wireless Communications on Security Demands, Authentication and Personal Privacy (**II**)－Ad Hoc Wireless Mobile Security, "CONNECTIMES, The Institute for Information Industry, Aug., 2004.

56. **S.J. Wang**, (Information Cryptology and Construction Lab.), "Web Surveillance and Management on the Cyberspace **(II)** ― SPAM at IP Spoofing," CONNECTIMES, The Institute for Information Industry, July, 2004.
57. **S.J. Wang**, (Information Cryptology and Construction Lab.), "Wireless Communications on Security Demands, Authentication and Personal Privacy **(I)** ― Sensor Networks come in the Wake of Network Sensors," CONNECTIMES, The Institute for Information Industry, June, 2004.
58. **S.J. Wang**, (Information Cryptology and Construction Lab.), "Steganography of Multimedia for Privacy on the Internet **(IV)**―Decrypt Secert using Human Visual System,," CONNECTIMES, The Institute for Information Industry, May, 2004.
59. **S.J. Wang**, (Information Cryptology and Construction Lab.), "Steganography of Multimedia for Privacy on the Internet **(III)**―Show up the Cybercrime on Steganography" CONNECTIMES, The Institute for Information Industry, April, 2004.
60. **S.J. Wang**, (Information Cryptology and Construction Lab.), "Steganography of Multimedia for Privacy on the Internet (**II**) **--**The Ways of Embedding Privacy into Multimedia?" CONNECTIMES, The Institute for Information Industry, March, 2004.
61. **S.J. Wang**, (Information Cryptology and Construction Lab.), "Web Surveillance and Management on the Cyberspace **(I)**―The Solutions against SPAM," CONNECTIMES, The Institute for Information Industry, Feb., 2004.
62. **S.J. Wang**, (Information Cryptology and Construction Lab.), "Steganography of Multimedia for Privacy on the Internet (**I**) ― Steganography and Information Hiding," CONNECTIMES, The Institute for Information Industry, Jan., 2004.
63. **S.J. Wang**, (Information Cryptology and Construction Lab.), "Digital Evidence and Forensics on the Computers and Network Systems (**III**)-John the Ripper," Info.Com, The Institute for Information Industry, Dec., 2003.
64. **S.J. Wang**, (Information Cryptology and Construction Lab.), "High-tech Cyber-crime on the Computers and Internet (**X**) ― Virtual Society on the Internet," CONNECTIMES, The Institute for Information Industry, Nov., 2003.
65. **S.J. Wang**, (Information Cryptology and Construction Lab.), "High-tech Cyber-crime on the Computers and Internet (**IX**) ― Cyber-identification," CONNECTIMES, The Institute for Information Industry, Oct., 2003.
66. **S.J. Wang**, (Information Cryptology and Construction Lab.), "Digital Evidence and Forensics on the Computers and Network Systems (**II**)-Intrusion and Incident Response," Information Security, The Institute for Information Industry, Sept., 2003.
67. **S.J. Wang**, (Information Cryptology and Construction Lab.), "High-tech Cyber-crime on the Computers and Internet (**VIII**) ― Cyber-community," CONNECTIMES, The Institute for Information Industry, Sept., 2003.

68. **S.J. Wang**, (Information Cryptology and Construction Lab.), "High-tech Cyber-crime on the Computers and Internet (**VII**) — On-line Game behind Cyber-crime ," CONNECTIMES, The Institute for Information Industry, Aug., 2003.
69. **S. J. Wang** (Information Cryptology and Construction Lab.), "PKI on the Internet（**III**） — Applications," Information Security, The Institute for Information Industry, Aug., 2003.
70. **S.J. Wang** (Information Cryptology and Construction Lab.), "High-tech Cyber-crime on the Computers and Internet (**VI**)- Trick on the on-line Game," CONNECTIMES, The Institute for Information Industry, July, 2003.
71. **S.J. Wang** (Information Cryptology and Construction Lab.), "PKI on the Internet（**II**）-Guideline," Information Security, The Institute for Information Industry, June, 2003.
72. **S.J. Wang** (Information Cryptology and Construction Lab.), "High-tech Cyber-crime on the Computers and Internet (**V**)- Cyber-contraband," CONNECTIMES, The Institute for Information Industry, June, 2003.
73. **S.J. Wang** (Information Cryptology and Construction Lab.), "PKI on the Internet（**I**）- Concept," Information Security, The Institute for Information Industry, May, 2003.
74. **S.J. Wang** (Information Cryptology and Construction Lab.), "Digital Evidence and Forensics on the Computers and Network Systems **(I)-** Honey Pot," Information Security, The Institute for Information Industry, April. 2003.
75. **S.J. Wang** (Information Cryptology and Construction Lab.), "High-tech Cyber-crime on the Computers and Internet (**IV**)-Cyber-pornography," CONNECTIMES, The Institute for Information Industry, May, 2003.
76. **S.J. Wang** (Information Cryptology and Construction Lab.), "High-tech Cyber-crime on the Computers and Internet (**III-2**)-Forum on Intellectual Property Protection," Info.Com, The Institute for Information Industry, Feb. 2003.
77. **S.J. Wang** (Information Cryptology and Construction Lab.), "High-tech Cyber-crime on the Computers and Internet (**III-1**)- Cyber-rumor," Information Security, The Institute for Information Industry, Jan. 2003.
78. **S.J. Wang** (Information Cryptology and Construction Lab.), "High-tech Cyber-crime on the Computers and Internet (**II**)- Cyber-fraud and Cyber-intimidation," Information Security, The Institute for Information Industry, Dec. 2002.
79. **S.J. Wang** (Information Cryptology and Construction Lab.), "High-tech Cyber-crime on the Computers and Internet (Ⅰ)- Money Laundering and Internet Gambling," Information Security, The Institute for Information Industry, Nov. 2002.

E. Textbooks

1. D.C. Lou, **S.J. Wang**, C.F. Lee, and ICCL (Information Cryptology and Construction Lab.), Multimedia Security, scheduled in Dec. , 2009.
2. **S.J. Wang** and ICCL-FROG (Information Cryptology and Construction Lab. – Forensic Research development task force Group), *The Tour of Number, Secret, and Security in Cyber-world*, scheduled in Feb., 2010.
3. **S.J. Wang,** C.H. Yang, C.L. Lei, and ICCL-FROG (Information Cryptology and Construction Lab. –Forensic Research development task force Group), *Computer and Network Security in Practice-* ***Applying to High-Tech Society,*** ISBN: 978-986-201-254-3, DrMaster book Inc. Aug., 2009.
4. **S.J. Wang,** H.M. Sun, C.Y. Weng, and S.P. Hwang, "Steganalysis in Computer Forensics," http://ics.stpi.org.tw/Treatise/, Science and Technology Information Center, National Applied Research Laboratories,, scheduled in Sept., 2009.
5. **S.J Wang**, C.H. Lin and ICCL-FROG (Information Cryptology and Construction Lab. –Forensic Research development task force Group), *Forensics and Security in Computer Systems*, ISBN: 978-986-201-196-6, DrMaster book Inc., March. 2009.
6. **S.J. Wang,** Y.H. Chang, C.W. Chen and T.Y. Lin, "Visual Security Applications in Authentication safeguarding User Identities," http://ics.stpi.org.tw/Treatise/, Science and Technology Information Center, National Applied Research Laboratories, Dec., 2007.
7. H.J. Ke, **S.J. Wang**, J.H. Hwang, and C.L. Chan, "Warfare in Digital Evidence Investigations Reflecting Origination" http://ics.stpi.org.tw/Treatise/, Science and Technology Information Center, National Applied Research Laboratories, Dec., 2007.
8. **S.J Wang**, U.H. Ke, and ICCL-FROG (Information Cryptology and Construction Lab. –Forensic Research development task force Group), *Computer Forensics and Digital Evidence* - ***State of the Art in the Anti-cyber-crime with Security Tactics*** 、***Computer Crime Prevention*** 、***Authentication and Re-construction of Venue***, ISBN: 978-986-201-004-4, DrMaster book Inc., June, 2007.
9. **S.J Wang**, J.S. Ke, and ICCL (Information Cryptology and Construction Lab.), *Information Multimedia Security*--- ***Steganography and Watermarking***, ISBN: 978-957-527-980-6, DrMaster book Inc., July, 2007.
10. **S.J Wang**, D.Y. Kao, and ICCL(Information Cryptology and Construction Lab.), *Information Security*---***State of the Art on Internet Security and Digital Forensics***, ISBN: 978-957-527-946-2, DrMaster book Inc., Jan., 2007.
11. C.H. Yang, **S.J. Wang** and I.S. Lin, "Trends and Managements in Information Multimedia Security,"

http://ics.stpi.org.tw/Treatise/, Science and Technology Information Center, National Applied Research Laboratories, Dec., 2006.

12. **S.J. Wang,** Y.H. Chang, J.H. Huang and D.Y. Kao, "Forensic Lab. Countermeasures in Anti-high-tech Crimes," http://ics.stpi.org.tw/Treatise/, Science and Technology Information Center, National Applied Research Laboratories, Nov., 2006.
13. **S.J. Wang,** J.Y. Lin, D.Y. Kao and C.H. Ke, "Evidence Discrimination under Intelligent Property in P2P Client-server Systems", http://ics.stpi.org.tw/Treatise/, Science and Technology Information Center, National Applied Research Laboratories, July 2006.
14. **S.J. Wang**, H.J. Ke, and ICCL(Information Cryptology and Construction Lab.), *Information and Network Security*---***Eyes of Secret –State of the Art on Internet Security and Digital Forensics***, ISBN: 957-527-890-9, DrMaster book Inc, March, 2006.
15. **S.J. Wang,** D.Y. Kao, C.T. Wu and A.C. Chiang, "Information Security in Evidence and Forensic Science," Special Issue **(I)** in Information and Communications Forum, ISBN: 957-619-130-0, http://ics.stpi.org.tw/Treatise/, Science and Technology Information Center, National Applied Research Laboratories, Dec. 2005.
16. **S.J. Wang**, H.J. Ke, and ICCL (Information Cryptology and Construction Lab.), ***Cryptography and Network Security-development, theory & applications***, ISBN: 957-527-690-6, DrMaster book Inc, May, 2004.
17. D.Y. Kao, **S.J Wang**, and ICCL (Information Cryptology and Construction Lab.), ***Information Security*****,** ISBN: 957-527-605-1, DrMaster book Inc., June, 2003.
18. **S.J. Wang (**Editor), *Information & Communication Security Series* ***(Vol. IV):*** *System Security,* STIC-RSR-091-10, ISBN: 957-619-077-0, Science and Technology Information Center, National Science Council, ROC Dec. 2002.
19. **S.J. Wang,** *Police Technology: Network besieged Mechanism and Information Security,* ISBN: 957-112-418-4, Wu-Nan Book Inc., Taiwan, March, 2001.

資訊密碼暨建構實驗室，http://hera.im.cpu.edu.tw/
(**I**nformation **C**ryptology and **C**onstruction **L**ab., **ICCL**)

主持人：王旭正 (Dr. Professor Shiuh-Jeng Wang), http://hera.im.cpu.edu.tw/sjw_2006/
計畫行政團隊：黃嘉宏、簡羚茜、古永昌

由於資訊科技的快速變遷，對於保護資料、隱藏重要資訊的需求與日俱增，不論在軟體、通訊等方面上的安全性問題實是必須不斷的強化，以防止有心人士乘虛而入。任何的社會群體中，總是有一小撮居心不良的人。如今全球 Internet 的用戶已經突破上億，即使其中只有百分之一不到的人意圖不軌，但這些百分之一人數確也夠嚇人的了，這些就是我們所說的「駭客」。為因應網際網路不斷發展，防止駭客入侵，確保人們於網際網路世界的安全，乃於民國 87 年成立資訊密碼暨建構實驗室(**I**nformation **C**ryptology and **C**onstruction **L**ab., **ICCL**)。

正因為體會到未來對於安全性的需求，我們致力於在現行的技術上尋求可以改進、突破的地方，以及在新興的方法中來加以研究使其更加的完備。透過這兩種方向，我們期望能夠提供更安全更完善的科技技術、應用與管理來因應可能發生的資訊安全問題。本 **ICCL** 位於中央警察大學資訊大樓二樓，目前 **ICCL** 成員共計有二十名皆熱衷於資訊安全、資料隱藏與資料快速搜尋之研究。本實驗室的成員皆致力於研究出更新方法應用在網路安全與資料建構上，使其網際網路更加安全並增快應用資料的搜尋速度。

ICCL 致力於網路傳輸安全機制的開發，目的在於強化資料在整個資訊網路世界的傳遞過程中能避免各式資通安全威脅，達到一個具安全性和互信的連線。另一方面，協助實務界電腦犯罪偵查/鑑識人員進行一套具標準、有效率，且公開、公正的數位證據萃取作業。

基於以上目標，未來發展方向為資訊與網路安全、密碼系統之研究、以及數位鑑識程序和方法論的研究和應用。

Dr. Professor Shiuh-Jeng Wang

PhD. National Taiwan University, Taiwan, 1996
Full Professor, Central Police University, Dept. of Information Management
Director Information Crypto and Construction Lab
Chair of ICCL-FROG (**F**orensic **R**esearch devel**O**pment task force **G**roup)
Director Chinese Cryptography Information Security Association (**www.ccisa.org.tw**)
Guest-editors:

- Journal of Internet Technology (http://jit.ndhu.edu.tw/englisha.php, indexed by SCI/E) Special Issue on Coding, Cryptography, and Multimedia Security in Computer Systems over Cyber-space Communications (published in 2010)
- The Computer Journal (http://comjnl.oxfordjournals.org/ , or http://www.oxfordjournals.org/our_journals/computer_journal/special.html indexed by SCI) Special Issue on Multimedia Security and Privacy (MSP) (published in 2010)
- Telecommunication Systems, (http://www.springer.com/business/business+information+systems/journal/11235 , indexed by SCI/E)Special Issue on Wireless multimedia networks and Security Services, (published in 2010)

Program-chair of SH'08, international **(**http://www.sersc.org/SH08/**)**
Program-chair of MPIS'08, international (http://mpis08.ialab.cs.pu.edu.tw/mpis08/)
Program-chair of MPIS'09, international (http://www.ftrg.org/MPIS2009/)
Program-chair of Future Tech '10, international (http://www.ftrg.org/futuretech2010)
Program chair in Cryptography and information security, National Comp. Symposium 2009,Taiwan http://ncs2009.ntpu.edu.tw/
Visiting Scholar, Comp. Sc. Dept, Florida State University, 2002, 2004
Visiting Scholar, Comp. Info. Sc & Eng. Dept, University of Florida, 2004, 2005
Project Study, at Computer School of Carnegie Mellon University, 2007

Contact Details

Address: Department of Information Management

Central Police University
56,Shu-Jen Road, Ta-Kang
Kuei-Shan, Tao-Yuan, 333, Taiwan

TEL: +886-3-3282321 EXT: 4807

FAX: +886-3-3272038

E-mail:- sjwang@mail.cpu.edu.tw
dopwang@gmail.com

Web site: http://hera.im.cpu.edu.tw/sjw_2006/