出國報告（出國類別：國際會議）

JPEG 2000 運用於可逆式資訊藏密技術

服務機關：國防大學理工學院電機電子系

姓名職稱：中校教師談光雄

派赴國家：日本

出國期間：106/03/29-106/04/2

報告日期：106/03/31

摘要

2017年「第19屆計算機與資訊工程國際研討會」(19th International Conference on Computer and Information Engineering, ICCIE 2017)係由世界科學，工程與技術學院 (World Academy of Science, Engineering and Technology, WASET)舉辦，並於106年3月30日至31日在日本大阪凱悅酒店(Hyatt Regency Osaka)舉行，本人投稿該研討會論文乙篇，論文題目：JPEG 2000運用於可逆式資訊藏密技術，因榮獲刊登及大會議程安排於3月31日上午0800-0945場次進行電子海報發表，故於3月29日搭機前往與會。當日該場次會議中，計有來至南韓、泰國、新加坡、台灣、日本、土耳其、捷克及埃及哥等數篇論文發表，期間發表人均詳細報告其研究成果，報告完後，台下與台上學者討論熱絡，彼此交流受益良多。

目次

頁次

壹、目的：

2017 年「第 19 屆計算機與資訊工程國際研討會」(19th International Conference on Computer and Information Engineering, ICCIE 2017)，由主辦單位 WASET 於 106 年 3 月 30 日至 31 日在日本大阪凱悅酒店(Hyatt Regency Osaka)舉行，該研討會主要提供科學家，研究人員和學者彼此交流和分享有關計算機與資訊工程各方面的研究成果與實務經驗。另外，此研討會亦為研究人員，相關從業人員與教育工作者提供一個跨科學平台，以探討最新與創新趨勢，並為計算機與資訊工程領域所遇到的實際問題提出解決方案。而本次參與發表之專家學者，計有來至台灣、日本、新加坡、南韓及泰國等各國專家學者，合計發表海報與論文達 90 餘篇。藉由參加本次國際研討會，除了獲得創新知識外更能暸解國際研究趨勢與脈動，進而增進研究動力與方向。此外，本會議所投稿之論文均經由國際相關領域之學者、專家審查，因此一旦獲得大會收錄刊登，亦可增加本院的能見度。

貳、過程：

會議議程

March 31, 2017, Session IV: 08:00-09:45

Chair: Robert Grzeszczak

本人發表之論文名稱：

Exploiting JPEG2000 Into Reversible Information

作者：

Te-Jen Chang, I-Hui Pan, Kuang-Hsiung Tan (談光雄), Shan-Jen Cheng, Chien-Wu Lan and Chih-Chan Hu

(Chung Cheng Institute of Technology, National Defense University, ROC)

本次赴日本大阪參加國際研討會，因國人赴日本免簽證及當地交通便利之因素，故僅委託旅行社代訂來回機票，而相關住宿則自行決定住宿東橫 INN 飯店四晚，因本次研討會舉辦地點大阪凱悅酒店在海灣區附近離市區略有相當距離，惟因大阪地鐵網路發達，交通相當便利，因而決定住宿心齋橋附近之東橫 INN 飯店以節省開支。研討會舉行時間為 106 年 3 月 30 日至 31 日，故委由旅行社代訂 3 月 29 日上午 08 時 30 分搭乘長榮航空 BR0132 班機赴日本大阪關西機場，抵達大阪關西機場時已逾當地時間中午 12 時 10 分，辦好出關手續，即自行搭乘南海電鐵抵達南波站，再步行約 10 分鐘後抵達下榻飯店，此時已逾 14 時 20 分，由於飯店仍無法辦理入住，故在辦理寄放行李後，選擇離飯店附近之餐廳用餐並稍作休息，而晚上則在飯店稍作準備與休息。3 月 30 日當日早上 10:30 到達會場並完成報到手續，當日並擇感興趣之場次聆聽相關論文發表。3 月 31 日發表當日早上 07:50 抵達會議地點，電子海報與論文發表場次同為上午 08 時 00 分場次，會議一開始，由會議主持人 Prof. Robert Grzeszczak 主持議程並由發表人逐一開始報告，本會議共發表 18 篇論文及電子海報發表，分別由沙烏地阿拉伯 King Abdulaziz University Saudi Arabia、泰國 Naresuan University Thailand、菲律賓 Technological Institute of the Philippines、新加坡 National University of Singapore、日本 National Institute of Technology, Gifu College Japan 、加拿大 University of Western Ontario Canada 及台灣政治大學、宜蘭大學、嘉義大學等專家學者輪流發表，發表人均詳細報告其研究成果，報告完後，主持人亦提供時間給在場與會專家、學者提問，由於所研究之領域具相關性，因此台下與台上學者討論相當熱絡。本人發表之電子海報為第 2 順位，發表完後，學者亦提出相關見解及寶貴建議，對於本次參加國際研討會，使自身能更瞭解國際研究趨勢與脈動，因此對於未來研究方向將有更多動力。

本人所發表之論文為「Exploiting JPEG2000 Into Reversible Information」，內容報告摘要如下：隨著多媒體網路時代的來臨，為了保護資料避免在網路傳輸中被竄改、破壞及偽造，所以資訊隱藏技術陸續被提出。資訊隱藏技術意指將重要機密資訊，隱藏在隱蔽媒體中，進而產生偽裝媒體。此偽裝媒體具有自然保護色的特色，在不引起懷疑的狀況下，將重要機密資訊傳送出去。此篇研究，我們提出高容量可逆式資訊隱藏技術，此技術以灰階做為隱蔽媒體，利用估測誤差值實施擴張藏密，因此，可達到更高的資訊

隱藏量。根據實驗證明本研究所提出的技術，不論在資訊負載容量及影像品質的整體上表現都能讓人滿意。

3 月 30 日，當日會議旁聽其他專家、學者發表議題，摘錄如下：

(1) All-Silicon Raman Laser with Quasi-Phase-Matched Structures and Resonators：

本研究提出輸出波長為 1.3μm 的全矽拉曼雷射原理，其係採用準相位匹配結構和諧振器來提高全矽拉曼雷射輸出功率。在 FTTH 系統 GE-PON 矽元件產生的 1.3μm 雷射具有舉足輕重之地位，因為此矽元件可與 GE-PON 中使用的矽平面光波電路（Si PLC）單片整合而成，且其與目前常用的 Si PLC 上設置的 1.3μm III-V 半導體雷射相比，可減少 Si PLC 和 Si 雷射光波導之耗損。因此，本文所提出的具有諧振器的準相位匹配的 Si 拉曼雷射可以增益為 20cm ／ GW 的 Si 波導的諧振器和 1.3dB（最大）處的 174 倍的雷射功率，其損耗為 1.2dB / cm，功率為 10mW，波導長度為 3mm，橫截面為（1.5μm^2）。

(2) Analysis of SCR-Based ESD Protection Circuits with Electrical Characteristics for the 5V Power Clamp：

本文分析了具有導通時間特性的矽控整流器（SCR）之靜電放電（ESD）保護電路。其結構是低電壓觸發 SCR（LVTSCR），齊納觸發 SCR（ZTSCR）和 P 基板觸發 SCR（PTSCR）。這三個結構主要用於 5 V 電源。通常，具有低觸發電壓結構之元件具有比其他結構快速開啟之特性。利用 ZTSCR 的齊納二極體結構，可增加 PTSCR 的觸發電流，而本文所提到之保護電路均具有 LVTSCR 低觸發電壓。在利用模擬軟體 Synopsys TCAD 來驗證其效果，LVTSCR 的導通時間為 2.8 ns，ZTSCR 為 2.1 ns，PTSCR 為 2.4 ns。然而，在 HBM 模擬結果，430K PTSCR 較 450K LVTSCR 和 495K ZTSCR 的具有更堅固的元件結構。因此，PTSCR 是 5 V 電源最有效的 ESD 保護電路。

(3) Antioxidant Property and Total Phenol Content of Rice Bran Oil from KDML105 and RD6：

由於米糠油（RBO）具有降低血清膽固醇的功效，且其具有抗氧化和抗癌的特性，因此亦可減緩過敏性症狀。而 RBO 具有酚類化合物等抗氧化合物。因此，本研究的目的是驗證兩種白色泰國大米中之總酚含量（TPC）和抗氧化性能: KDML105 和 RD6。本研究採用溶劑萃取法及 Folin-Ciocalteu 比色法測定 TPC，並採自由基清除率（DPPH）用於測定 EC50 之抗氧化性能。由研究證實，KDML105 具有明顯較高之 TPC，且其具有 9.8 毫克食子酸/毫升。而在兩個 KDML105 和 RD6 中之 RBO 實體間的 EC50 並無顯著差異。

(4) Classification of Traffic Complex Acoustic Space：

在多年的發展，對於景觀的研究已經被細化為城市空間和建築兩種類型。以交通功能為核心者，具有明顯的建築空間組合和流量設計特點。以交通綜合為核心者整合了商務，住宿，娛樂等各種功能。在本研究中，對於各式交通狀況環境中進行了現場錄音，提取和分析了不同的聲音元素，包括聲波變化，頻率分佈，聲源穩定等方面，對於每個不同交通環境進行類比分析。將復雜的交通環境及建築空間從聲學環境的角度以分為幾個典型的聲場空間，主要包括穩定聲場空間，高壓聲場空間，節奏聲場空間和動態聲音

空間。本研究可將該分類進一步深化交通環境聲學環境評價與控制研究。

(5) Color Segmentation of Satellite Imagery to Estimate Total Suspended Solid at Rawa Pening Lake, Central Java, Indonesia：

水是人類和其他生物所需之重大自然資源。在印度尼西亞中的水佔了全國的約 81％，因此其係由內陸、水域和大海組成之國家。本文主要研究對像為湖泊和陸域水庫，並對其中水質進行監測。總懸浮固體（TSS）是水質中要參數之一。大多數早期的研究受利用取水來獲得 TSS 值直接測量。此方法相當耗時，導致成本提高。而遙測感應技術的發明可有效解決水域和淤泥之監測，此外在海岸線變化繪製和天氣分析等諸多問題均可有效解決。本研究的目的是通過使用 Lansat 8 圖像來評估中爪哇的 Rawa Pening 湖中 TSS。由實驗結果證明，該方法成功地監測出 Rawa Pening 的 TSS。

3 月 31 日，當日其他學者、專家發表議題，摘錄如下：

(1) Design of a Remote Radiation Sensing Module Based on Portable Gamma Spectrometer：

可攜式伽瑪光譜儀需具有敏感，可攜帶及便利性。因此，為了滿足這些要求，本文開發了利用 SiPM 之可攜式輻射探測器儀。本文所開發之可攜式輻射探測器儀使用耦合矽 GAGG、光電倍增器和 RF 射頻模組來測量伽瑪光譜，並且透過無線網路或智慧型手機達到相關接收量測數據。本文所開發之可攜式輻射探測器儀消耗功率約 4.4W，重量約 180g（含電池），並能在 662keV 下達到 5.8%的 FWHM 能量分辨率。

(2) Digital Elevation Model Analysis of National Geopark Ciletuh Area as Mitigation of Tsunami Hazard：

Ciletuh 地質公園是印度尼西亞國家地質公園之一，其亦為聯合國教科文組織全球地質公園所認證，Ciletuh 地質公園位於蘇卡布，其直接面向兩塊地質構造活動板塊之的交匯處。Ciletuh 地質公園周圍環繞之懸崖最高達 300 米，因此，該地區容易受到海嘯的襲擊。在 2006 年的案例研究中，龐班達蘭經歷了 7.7 級地震，因而伴隨著強大海嘯。本研究的目是分析海嘯的潛在危害，並預測 Ciletuh 地質公園地區海嘯警報提供裝配點之建議。本文使用的方法為高程度模型分析，地形和衛星圖像之觀測與分析。從數據處理和分析結果，Ciletuh 地質公園海嘯災害風險極高，因此，本研究結果可以提供 Ciletuh 地質公園相關管理單位在未來的發展規劃過程中參考。

(3) Digital Elevation Model Analysis of Potential Prone Flood Disaster Watershed Citarum Headwaters Bandung：

洪水是導致河流平坦化及地區沉沒的主因，由於溢流的河水無法有效控制，將可能導致周邊地區基礎建設造成損害。本文旨在利用數字高程模型（DEM）的數據，以便在易於發生洪水的地區分析與告警，在次級數據分析（ArcGIS）上可驗證 Citarum 上游發生淹水區域之預測，而本文評估淹水分佈圖，係以萬隆地區 13 個縣/區內好發區域為研究目標，其中由分析結果可知最嚴重的地區是 Baleendah-Dayeuhkolot-Bojongsoang-Banjaran 地區。

參、心得報告：

本次赴日本參加國際研討會，看到許多專家學者對於現實所發生之問題提出解決方案，深感佩服，例如:有學者提出米糠油對於人提健康之研究，水質監測及提出數字高程模型來分析可能出現水患的區域等。因此，體會到學者做研究應以解決當前所遇到之問題，以改善或增進人們生活品質。另外，本次研討會在日本大阪舉行，其交通相當便利，因此在研討會期間利用搭乘該地區的各式鐵路系統前往會場，沿途景觀可以充分感受到日本的進步，此外，對於日本龐大的鐵道系統，也深感佩服，雖然其由不同鐵道公司所經營，但其銜接與規劃均相當便利，由其是其具有相當高之準點率。最後，參加國際研討會是一項很有意義的學術活動，也非常感謝科技部經費補助，校院部各級長官的協助，使得此次研討會能順利成行。

肆、參考資料：

圖片為研討會內外場與會議現場等

研討會地點指示牌

註冊報到(1)

註冊報到(2)

研討會場內(1)

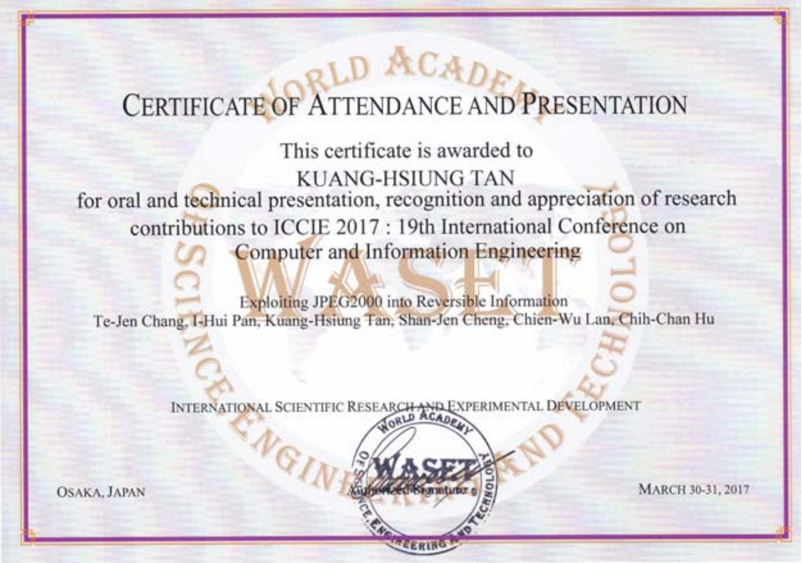
研討會場內(2)

研討會場內(3)

研討會場內(4)

研討會場內(5)

研討會場內(6)



CERTIFICATE OF ATTENDANCE AND PRESENTATION

This certificate is awarded to

KUANG-HSIUNG TAN

for oral and technical presentation, recognition and appreciation of research contributions to ICCIE 2017 : 19th International Conference on Computer and Information Engineering

Exploiting JPEG2000 into Reversible Information

Te-Jen Chang, I-Hui Pan, Kuang-Hsiung Tan, Shan-Jen Cheng, Chien-Wu Lan, Chih-Chan Hu

INTERNATIONAL SCIENTIFIC RESEARCH AND EXPERIMENTAL DEVELOPMENT

WORLD ACADEMY OF SCIENCE, ENGINEERING AND TECHNOLOGY
WASET

OSAKA, JAPAN

Authorized Signature

MARCH 30-31, 2017

出席證明

伍、建議事項：

對於參加國際研討會，將可增進學術交流亦可開闊國際觀，利用參加國際學術研討會，使各國瞭解我們的學術成就。所謂學術無國界，藉由各國的專家學者互相研討，彼此激勵出火花，對於學術而言也是一項寶貴收穫，因此，在經費有限的情況下，期許能鼓勵老師們能多出去走走，瞭解目前各國學術研究方向，增進學校能見度，以提升自己本職學能。最後，感謝科技部的經費提供，使得本次研討會能順利成行。

陸、會議資料：

收錄論文光碟片(論文電子檔 90 餘篇)

Exploiting JPEG2000 into Reversible Information

Te-Jen Chang, I-Hui Pan, Kuang-Hsiung Tan, Shan-Jen Cheng, Chien-Wu Lan and Chih-Chan Hu

***Abstract*—**With the event of multimedia age in order to protect data not to be tampered, damaged, and faked, information hiding technologies are proposed. Information hiding means that important secret information is hidden into cover multimedia, and then camouflaged media is produced. This camouflaged media has the characteristic of natural protection. Under the undoubted situation, important secret information is transmitted out. Reversible information hiding technologies for high capacity is proposed in this paper. The gray images are as cover media in this technology. We compress gray images and compare with the original image to produce the estimated differences. By using the estimated differences, expression information hiding is used and higher information capacity can be achieved. According to experimental results, the proposed technology can be approved. For these experiments, the whole capacity of information payload and image quality can be satisfied.

***Keywords*—**Cover media, camouflaged media, reversible information hiding.

I. Introduction

INFORMATIONis the thing to communicate among people. Information is also called communication. Communication in human life exists everywhere, for example: cell phone, television, computer, Internet, and e-mail, and so on. Secret communication has been heavily needed since ancient times. For military, natural security and military confidentiality depend on the secret communication architecture. A major breakthrough has been achieved in modern cryptographic technologic, so the secret communication architecture can be protected in texture. On the other side, video media in e-generation is replaced with traditional text. Graphical User Interface (GUI) shortens the distance between people with machines. People use computers and Internet more normal. It is a necessity in our life. The computers and Internet are regarded as the target, which will be stolen and broken by hacker. How we protect the multimedia products becomes very important. The function of multimedia products cannot be protected by cryptographic technology. So, information hiding technology can be invented.

Recently, information technology develops very quickly. Internet becomes a public communication path. Therefore, how we transmit secure information from a transmitter to a receiver safely becomes an important topic. Some copyrights are declared, and some secret information is hidden by information hiding. We use cover media to hide confidential information, such as videos, music, texts, or images. We must assume after hiding information, the media (videos, music, texts, or images) do not have obvious changes or after the other non-official people intercept information, they do not doubt the content which has already hidden important secret data. So, the important secret data can be transmitted out and prevented from tampering and damaging by an interested people. It is the purpose of information hiding.

Generally, information hiding is distinguished into: spatial domain and frequency domain. Information hiding in spatial domain is directly to change pixel values in images and to achieve the purpose of information hiding. The advantages in this method are low computational complexity, high payload, and easy-to-achieve. They do not break the quality of images. Everybody usually uses Internet to upload or to download images to transmit message. Therefore, an image is one of the best ways to cover media. In this experiment, “image” is regarded as cover multimedia. The estimated pixel differences are created by compression and secret information is embedded to produce camouflaged images. We implement and verify the efficiency of data hiding.

The study range is limited into technological steganalysis in data hiding. This is reversible data hiding which is refereed the estimated difference [1]. The main content is images in spatial domain. These images use the relationship among pixel values to produce the differences to hide secret information.

The study is referred to the reversible data embedding using a difference expansion and Least Significant Bit (LSB) replacement in this paper. It combines the advantages which are difference expansions and least significant bit replacement. The cover image is proposed in the data hiding process.

We compare the quality difference of data hiding between the proposed method and the other methods [1]–[3] to verify our proposed method. The experimental result is applied in web page. The estimated images are browsed in the outer layer of the web page. The stegoimages are stored in the inner layer of the web page. They can be downloaded and stored by using another file name. Comparing with the estimated difference method [1], there is higher quantity of data hiding, but the estimated differences are larger than those in the other methods.

The estimated images are regarded as reference images of camouflaged image in the proposed method. There are more accurate estimations, but the estimated differences are smaller. The quality of the camouflaged images is promoted.

T. J. Chang is with the Department of Electrical and Electronic Engineering, Chung Cheng Institute of Technology, National Defense University, Taoyuan 335, Taiwan (corresponding author; phone: +886-3-380-9991 ext.363; e-mail: karl591218@gmail.com).

I. H. Pan is with AIR Command and Staff College, National Defense University, Taoyuan334, Taiwan. (e-mail: panchefukui@gmail.com).

K. H. Tan and C. W. Lan are with the Department of Electrical and Electronic Engineering, Chung Cheng Institute of Technology, National Defense University, Taoyuan 335, Taiwan(e-mail: s913115@gmail.com;g941339@gmail.com).

S. J. Cheng is with Department of Aircraft Engineering, Army Academy ROC, Taoyuan320,Taiwan (e-mail: cheng5721@gmail.com).

C. C. Hu is with System Manufacturing Center, National Chung-Shan Institute of Science and Technology, Sanxia District, New Taipei City 23742, Taiwan (e-mail: huchihchan@gmail.com).

II. Discussion of Information Hiding Technology

From now on, along with the progress of human culture, interactions among people are very frequent and "information hiding" is heavily needed; e.g., from personal privacy to national confidentiality. Even in the personal privacy or in the national confidentiality, they need safe and effective method to hide the transmitted information and to prevent secret information from leakage. These technologies of data hiding are the sources of steganography. The earliest reference is traced into 5th Century B.C. In the article "The Histories" which is written by historian Herodotus in ancient Greek, one technology is described. It is to prevent Greek from being conquered by Xerxes which is in Persian. He wrote secret information to engrave on the wood and covered the secret information on the surface by wax, and then prevented Greek Guard from checking. He told the Greeks the attack action, and then the Greeks had enough time to prepare and to resist the invasion of Persia.

The word "steganography" comes from "Steganos" and "Graphy". The original meaning is to hide words. We can extend to transmit information by using secret method. It has a weakness when the data hiding technology is broken. The information can be understood by the third person. Therefore, cryptography is developing. Secret information does not hide itself in cryptography. It hides the meanings of secret information. This process is called encryption. Secret information is transformed into texts or symbols which cannot be understood. Therefore, depending on the rules which have already coordinated by the transmitters and the receivers, the information will be transferred. The receivers only depend on the transferred rules to transfer the secret information, and then the meaning of the secret information can be restored. If the enemies intercept it since they do not understand the transferred rules, the meaning of secret information cannot be obtained. The concept of steganography will be proposed. Steganography is to hide secret information into images, audios, videos, and texts. The media which hide information is called cover media. The action of hiding secret information is called embedding. The cover media in which information is embedded is called stegomedia.

The classification for steganography [4] distinguished the information hiding into four items as shown in Fig. 1. The first is stego channel, the second is anonymity, the third is Steganography, and the last is copyright mark. The descriptions of each item are as follows: stego channel is called the channel where unauthorized information can be transmitted. This channel is usually used to steal the information which is in the computer. Anonymity means to hide our information or use a pretended name to transmit data. Steganography means to hide plaintexts into specific media. Nobody will doubt them. That is, nobody knows about secret information inside message. Copyright mark means that some associated information, which is the name of the company or the symbol included, is stored in specific media. But, there are two methods which are appeared or hidden. This is one of the most representative hiding methods and this is called digital watermark.

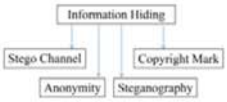


Fig. 1 Classification for Steganography.

Steganography is elaborated in this paper. Steganography is a technology where information is hidden into figures, videos, even voices. When information is hidden into cover media, the cover media does not change itself. Steganography can be extended as watermark; for example, a label in product. Many small figures are used for permutation, and then, a figure which has some meanings is generated. Figures which are drawn by ASCII are used. Some methods can be employed to hide information, such as holography technology, infrared, B. B. call, and HTML code, and so on. Secret information can be hidden by using static figures. It cannot be identified by human eyes. The main purpose of the embedded capacity depends on the quality of stego images. One of the most important facts is that the original image can be restored.

Generally, the following three conditions must be satisfied for a good information hiding technology. The descriptions are as follows: (1) Security means that hiding information must resist to detection and breaking confidentiality. It cannot be removed by unassociated people. Even information which is hidden is known and it can be protected; (2) Imperceptibility means that human eyes cannot find secret information which is hidden in cover media. The quality of cover media is affected to lower the minimum for information hiding. So, unauthorized people will no doubt, and then, the purpose of data hiding will be achieved; (3) High payload means that the larger the hiding capacity of data is, the better the data hiding is. The larger capacity represents higher hiding ability. During the same imperceptible condition, more information will be hidden.

According to different embedding technologies, the technologies of the information hiding can be divided into two classes: spatial domain and frequency domain. They are described as follows in Fig. 2.

1) Spatial domain: Most technologies exploit the media that human eyes can directly sense. Nobody can feel the secret information hiding in the media. Most are established in the human visible system. Mostly. Cover media are directly modified to achieve the purpose of data hiding. There are many advantages which are a lot of positions of data hiding, and easily to hide, and easily to manage in spatial domain. General methods in spatial domain are least significant bit (LSB), difference expansion (DE), and histogram shifting.
2) Frequency domain: Transform the pixel values of images in spatial domain into coefficients in frequency domain, and then secret message is added the specific coefficients. General transformation technologies in frequency domain are discrete Fourier transform (DFT), discrete cosine transform (DCT), or discrete wavelet transform (DWT). Most methods exploit digital watermarking technology. Using DCT, images from spatial domain are transformed

to frequency domain, and then a matching table is made, which is used for a watermark to be hidden inside. The secret information can be hidden inside the message by look-up table, and then a digital watermark system which is image verification can be completed.

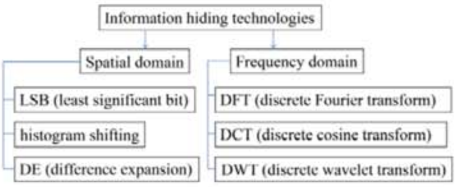

Information hiding technologies
Spatial domain
Frequency domain
LSB (least significant bit)
histogram shifting
DE (difference expansion)
DFT (discrete Fourier transform)
DCT (discrete cosine transform)
DWT (discrete wavelet transform)

Fig. 2 Applications for information hiding technologies.

Comparing with the above two methods (in spatial domain and in frequency domain), data hiding is used in spatial domain. It has many advantages which are simple algorithms, easily to implement. The faults are that tough degrees is not enough resulted for the attacked information. According to the above algorithms, since the information is varied, the visible effect will be affected. Otherwise, in general, if the information hiding is used in frequency domain, a better result will be obtained. Because the hiding information will be distributed into the frequency domain, the original information in spatial domain will not be varied. Then, the visible effect is better and the fault is the information amounts, which can be hidden, are not larger.

The information hiding technologies in spatial domain are LSB, DE, Histogram shifting and those in frequency domain are DFT, DCT, DWT. They are described as follows:

1) Least Significant Bit (LSB): LSB is a general data hiding algorithm in spatial domain. The 8-bit gray pixel is shown in Fig. 3 and this bit is called LSB replacement. The bit is affected largest in Fig. 3 and this bit is called the most significant bit (MSB) replacement. The LSB replacement is that hiding secret information "0" or "1" into the LSB in the figure. The pixel is the smallest for LSB in the figure. After hiding secret information, the pixel value is only changed between "0" and "1". Human eyes almost cannot identify the difference between "0" and "1". The figure, which is implemented by the information hiding, is almost the same as the original figure. Since the imperceptibility is achieved, the data hiding capacity is higher. If the original figure is restored, the secret information of LSB in the pixel value can be retrieved in sequence. The operational processes are very simple and quick.

2) Difference Expansion (DE): The DE method was proposed by [5]. This method is that the adjacent pixels in the cover images are used to hide secret data. Two adjacent pixel values are a set of pixel couple. Two adjacent pixel values are subtracted, and the difference is expanded double. Then, one bit which is secret information is embedded. The data hiding of the difference expansion for the estimated differences is as shown in Fig. 4. The difference expansion which belongs to reversible data hiding needs the position map to record embedding methods for each pixel value and then it can be restored in the original image. If the position map and the secret information is embedded into the cover image together. The embedding capacity will be reduced and the complexity of the algorithm will be increased. In order to solve these faults, one method was proposed by [6]. It is based on that the difference expansion is to promote the capacity for the reversible data hiding. The pixel differences between the cover image and surrounded images are not larger. Since the values of the difference expansion are not larger, the smaller values of the pixel can be embedded. The position map is not needed in this method. It has two advantages: the higher capacity and the lower distortion.

3) Histogram Shifting: The histogram shifting method was proposed by [4]. It is reversible information into the histogram. Find the peak point and zero point in the histogram. The largest amounts for the pixel values are called peak point. The smallest amounts for the pixel values are called zero point. Shift the pixels between the peak point and the zero point. The position aside the peak point will be empty. The secret information can be embedded. Lena and histogram figures are shown in Fig. 5.

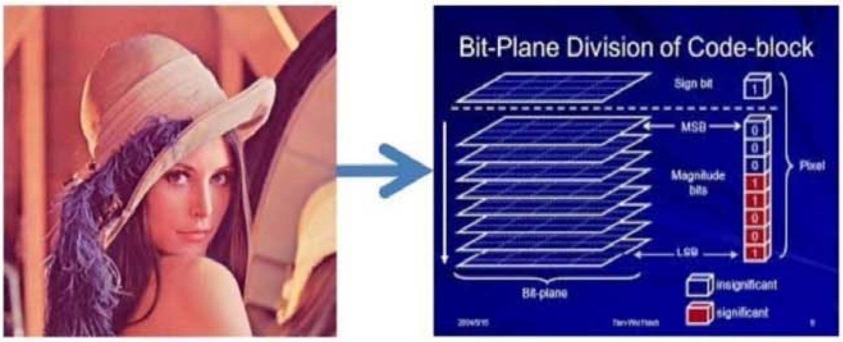


Fig. 38-bits gray pixel

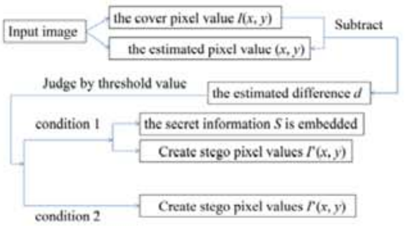

Input image
the cover pixel value $I(x, y)$
the estimated pixel value (x, y)
Subtract
Judge by threshold value
the estimated difference d
condition 1
the secret information S is embedded
Create stego pixel values $I'(x, y)$
Create stego pixel values $I'(x, y)$
condition 2

Fig. 4 Data hiding of the difference expansion for the estimated differences

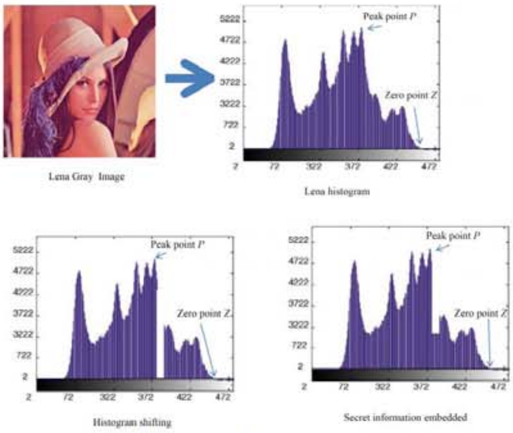


Fig. 5 Lena and histogram figures

The reversible data hiding for quality images using modification of the prediction errors (MPE) method was proposed by [2]. LSB matching is revisited, which was proposed by [4]. Once the peak point and the zero point are selected for Ni's method, whatever the embedded capacity, the gray values of the pixels between the peak point and the zero point will be changed 1 bit. The distortion probability of the images is larger. The largest embedding capacity is the pixel number of the peak point. So, the faults which are high distortion probability are existed in Ni's method which is presented in [3].

The zero point is sharply centered in the histogram of the estimated differences for most natural images. It is decayed by exponentiation way towards two sides. The simple addition and subtraction operations are used in MPE method. It only modifies some estimated differences to embed the secret information. The estimated differences are centered the position "0". This position is the embedding point of the largest amount. Thus, the information is firstly embedded from the estimated difference is equal to 0. The information is recorded to embed the pixel position of the ending image by parameter L, and then the remaining pixel values are remained constant. Hence, after information hiding is implemented, high quality of the images can be remained. In TABLEI, for the same embedding capacity, comparing MPE method with histogram method, the higher the PSNR values are, the higher the qualities of the images.

A high capacity reversible data hiding scheme with edge prediction and difference expansion was proposed in [3]. Some technologies in this scheme are the same as in the MPE method. That is, the estimated pixel values created by using the adjacent pixel values which is the original value X. The scanning methods are also the same. The figure with edge prediction and difference expansion is shown as Fig. 6.

TABLE I
COMPARISON TABLE BETWEEN MPE METHOD WITH HISTOGRAM

Images (512 * 512)	The embedding capacities for information (bit)	Histogram	MPE
		PSNR	PSNR

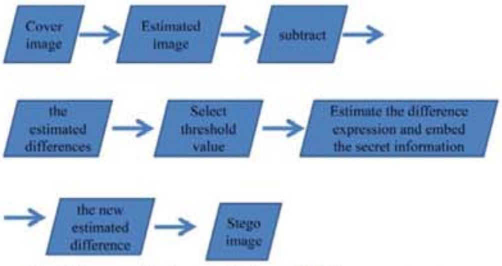

Cover image
Estimated image
subtract
the estimated differences
Select threshold value
Estimate the difference expression and embed the secret information
the new estimated difference
Stego image

Fig. 6 Figure with edge prediction and difference expansion.

One method was proposed by [2]. The estimated differences are used to hide the secret information and the estimated values are established by using the adjacent pixel values. The differences between the estimated values with the values which are in the original pixel values are used to the estimated differences. For the small values "0 or 1" of the estimated differences, the secret information is embedded. Comparing the proposed method with the histogram method which was proposed by [4], there are many advantages which are higher capacity of data hiding and higher quality of images in the proposed method. Improved difference expansion method was proposed by [6]. The secret information can be embedded by using the estimated difference expansion to improve the fault which the position map is resulted in the decreases of data hiding capacity.

Summarize the above advantages. The compressed images are restored by compression software. Because the images are distorted the estimated differences will be created to expand and the secret information is embedded. The samples are produced by two types which are JPEG and JPEG2000 in this experiment. The following discussions by using these samples and the information-embedding algorithms are used into these samples.

1) Information-embedding algorithm:

An original image which is known is called f1. The image is compressed by PhotoImpact software and restored, then to produce the estimated image f2. The difference between f1 with f2 is as the estimated difference *Pe*. The estimated differences are designed into 8 threshold values in this experiment to implement the estimated difference expansion and to embed the secret information. Otherwise, if the estimated differences of the pixel values don't include the 8 threshold values, the pixel-shifting operation will be implemented. Finally, the stego image newf1 will be created. The processes of the embedding algorithm are shown in Fig. 7.

i. Selections of the estimated differences and dynamic threshold values:

Take Lena image for example. The size is 512 * 512. The samples which are two kinds of JPEG and JPEG 2000 are produced by the comparison software. For in or out of the range of the threshold values, there are many methods which are information-embedding and differences-changing. These are distinguished into two categories: the first I the traditional and the second is the difference histogram adjustment. There are two kinds of processes in the first method. One is the difference values are in the range of the threshold values to process difference expansion. The other is the difference values are out of the range of the threshold values to change the method which the information is embedded and record the characteristics in the position map.

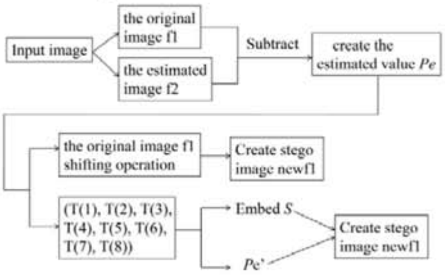


Fig. 7 Processes of embedding algorithm.

There are also two kinds of processes in the second methods. One is the values are in the range of threshold values to process difference expansion. The other is the values are out of the range of the threshold values to process shifting. The advantage in the second method is that the overflow situation will be recorded in the position map. The second method will be exploited in this paper. In the process of information-embedding, the analysis for the selection of the dynamic threshold values is exploited. Set the initial value T(0) = 0 as shown in (1).

$$T(j) = (-1)^{(j-1)}(j-1) + T(j-1), \quad j \in \{1, 2, \ldots, j_E\} \tag{1}$$

In (1), j is represented for the analytic order of the threshold value. j_E is represented for the threshold value for the analysis of the threshold value. The 8 threshold values T(1) ~ T(8) are established in this experiment. The threshold values are represented for the estimated difference values of embedding information as shown in TABLE II. In this experiment, the analysis is executed from the estimated difference equals to be 0 to the positive and the negative sides out of the original point in sequence.

ii. Estimated difference expansion and secret information embedding:

The purpose which information firstly embedded from the estimated difference value T(1) equals to be 0to avoid the image distorting. Because of most natural images, the estimated differences are sharply centered into the zero point and are decade towards two sides by the way of exponentiation. So, the zero point can provide enough space to embed information. The estimated difference P_e in images are scanned from top to bottom, and from left to right by N type. If the estimated difference in that position is equal to the threshold value, the secret information S_k (only one bit) is embedded into the estimated difference P_e . The embedded secret information S which is generated by random in the sample is 0 or 1. The capacity of the secret information depends on the largest capacity of data hiding which can be accommodated in every image. At first, the secret information is embedded into the pixel value which the estimated difference equals to be 0. When the capacity of the pixel value, which the estimated difference equals to be 0, is not enough, there are still more secret information. This secret information is embedded the pixel values which the estimated difference equals to be-1. When the capacity of the pixel value which the estimated difference equals to be -1 is not enough, there are still more secret information, these secret information are embedded the pixel value which the estimated difference equals to be 1, and so on. Until embedding the secret information is finished. The ended point is recorded as the image position of the threshold value T(j). The estimated difference expansion and the embedding information are shown as Fig. 8.

The matching table for the estimated difference P_e is shown in TABLEIII. When the estimated difference for the pixel P_e = T(j), j = 1, 2, 3, …, 8., the operations of the estimated difference expansion and embedding secret information are implemented.

iii. Pixel shifting operation out of the range of threshold value:

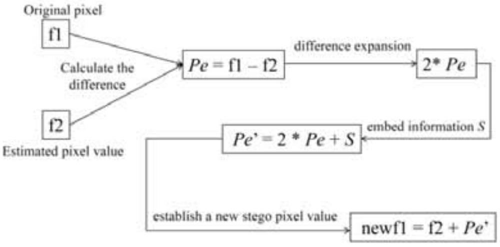


Fig. 8 Estimated difference expansion and embedding information.

TABLE II
THRESHOLD VALUES

T(1)	T(2)	T(3)	T (4)	T(5)	T(6)	T(7)	T(8)
0	-1	1	-2	2	-3	3	-4

TABLE III
MATCHING TABLE FOR ESTIMATED DIFFERENCE P_e

P_e	P_e is implemented the difference expansion and the secret information embed	After data hiding P_e'
T(1) = 0	2 * 0 + S	0 or 1
T(2) = -1	2 * (-1) + S	-2 or -1
T(3) = 1	2 * 1 + S	2 or 3
T(4) = -2	2 * (-2) + S	-4 or -3
T(5) = 2	2 * (2) + S	4 or 5
T(6) = -3	2 * (-3) + S	-6 or -5
T(7) = 3	2 * (3) + S	6 or 7
T(8) = -4	2 * (-4) + S	-8 or -7

During the processes of embedding information, the pixel which in the range of the threshold value is implemented the estimated difference expansion and information embedding operations. In order to avoid these pixels which the information has already been hidden or has not been hidden are created superposition and confused, the extra information must be recorded. The extra information which is not included in the position map is the pixels which are distinguished in the range and out of range of the threshold value. So, the secret information can be correctly got and the original image can be restored during decryption process. But the capacity in the position map will lower sharply the embedding capacity. One method is designed in this experiment: during the processes of embedding information, if the estimated difference P_e of the pixel is out of the range of the threshold value, the pixel value in the original image f1 will do shifting operation. They can be distinguished with the embedded pixel. That is, when $P_e \neq$T(j). The procedure is described as follows:

Step 1: In the process of hiding information until j = 1, if $P_e \neq$ T(1), shifting is implemented:
$P_e > 0$, f1 is shifting right 1, newf1 = f1 + 1
$P_e < 1$, no operation, newf1 = f1

Step 2: In the process of hiding information until j = 2, if $P_e \neq$ T(2), shifting is implemented:
$P_e > 0$, f1 is shifting right 1, newf1 = f1 + 1
P_e = 1, no operation, newf1 = f1, which is in the situation of j = 1
$P_e <$ -1, f1 is shifting left 1, newf1 = f1 - 1

Step 3: In the process of hiding information until j = 3, if $P_e \neq$ T(3), shifting is implemented:
$P_e > 1$, f1 is shifting right 2, newf1 = f1 + 2
P_e = 0, -1, no operation, newf1 = f1, which is in the situation of j = 2
$P_e <$ -1, f1 is shifting left 1, newf1 = f1 - 1

Step 4: In the process of hiding information until j = 4, if $P_e \neq$ T(4), shifting is implemented:
$P_e > 0$, f1 is shifting right 2, newf1 = f1 + 2
P_e = 1, 0, 1, f1, no operation, newf1 = f1, which is in the situation of j = 3
$P_e <$ -2, f1 is shifting left 2, newf1 = f1 - 2

Step 5: In the process of hiding information until j = 5, if $P_e \neq$ T(5), shifting is implemented:
$P_e > 2$, f1 is shifting right 3, newf1 = f1 + 3
P_e = -2, -1, 0, 1, no operation, newf1 = f1, which is in the situation of j = 4
$P_e <$ -2, f1 is shifting left 2, newf1 = f1 - 2

Step 6: In the process of hiding information until j = 6, if $P_e \neq$ T(6), shifting is implemented:
$P_e > 2$, f1 is shifting right 3, newf1 = f1 + 3
P_e = -2, -1, 0, 1, 2, no operation, newf1 = f1, which is in the situation of j = 5
$P_e <$ -3, f1 is shifting left 3, newf1 = f1 - 3

Step 7: In the process of hiding information until j = 7, if $P_e \neq$T(7), shifting is implemented:
$P_e > 3$, f1 is shifting right 4, newf1 = f1 + 4
P_e = -3, -2, -1, 0, 1, 2, no operation, newf1 = f1, which is in the situation of j = 6
$P_e <$ -3, f1 is shifting left 3, newf1 = f1 - 3

Step 8: In the process of hiding information until j = 8, if $P_e \neq$T(8), shifting is implemented:
$P_e > 3$, f1 is shifting right 4, newf1 = f1 + 4
P_e = -3, -2, -1, 0, 1, 2, 3, no operation, newf1 = f1, which is in the situation of j = 7
$P_e <$ -4, f1 is shifting left 4, newf1 = f1 - 4

Step 9: When embedding the secret information is finished, the pixels behind the position don't change and shift.

III. COMPARING WITH OTHER REVERSIBLE DATA HIDING METHODS

Thumbnail out of the web page in the Internet are browsed. Enlarged view inside the web page in the Internet can be downloaded and be stored in another file name. The Thumbnail and the Enlarged view are referenced in this paper. The compression rate is mostly concentrated 10% ~ 20%. The images are compressed 20%, 10%, and 5% by JPEG and JPEG2000 to create 6 samples as the estimated images as shown in TABLEIV. These images are Lena, Barbara, Airplane, Tiffany, Boat, Baboon, Goldhill, Girl, Zelda. For analyzing and comparing, the experimental results are shown from Table 6 to Table 10. The experimental results are between the proposed method with other 5 methods which are proposed by [1]–[3], [5], [7]. The difference expansion was proposed by [5]. The reversible data hiding method based on the estimated difference was proposed by [1]. The reversible data hiding method which the estimated difference can be modified was proposed by [2]. The reversible data hiding method with edge prediction and difference expansion was proposed by [3]. The reversible data hiding method which uses histogram with interleaving predictions was proposed by [7]. The experimental results show that when the capacities of information-embedding are the same, the PSNR values which are obtained by the proposed method are better than those which are obtained by other 5 methods.

TABLE IV
MATCHING TABLE OF ESTIMATED IMAGE SAMPLES

Compression methods Compression probability	JPEG2000	JPEG
20%	A	B
10%	C	D
5%	E	F

IV. CONCLUSIONS

Based on the estimated difference, one reversible data hiding which high capacity of data hiding can be reached is proposed. In this method, after compressing the original image, the micro difference for distortion will be created, the operations of the estimated difference expansion and information-embedding will be preceded. During the processes, the operations of the dynamic threshold value and pixel-shifting will be adopted. This method is simple and direct. When the original images wants to be restored, and the secret information want to be known, the position which the estimated difference of the threshold value will be only known, and then the secret information can be decrypted and the original image can be restored. The capacity of data hiding and the quality of image can be better for the reversible data hiding. According to the experimental results, the image quality of data hiding in spatial domain can be satisfied. Because of low distortion for military application, it can't be imprecated. Except legal participants, nobody can retrieve secret information from data hiding image and good security can be remained.

The results in the experiment show that: the capacity of data hiding in the proposed method is the same as that in other methods [8-10]. The PSNR value in the proposed method is higher than that in other methods. In future works, by using proposed method, when data hiding, for every image, the size of a layer of pixel which the information is embedded is the same as the size of the original image. When the threshold value is over 8, that is, the estimated difference is over out of the range of ± 4. Because the histogram exponentiation for the estimated difference is largely lowered, and after the estimated difference is expanded, more serious distortions and overflow maybe result in. So, in the future, larger space of data hiding is created to achieve higher capacity of data hiding and the necessity is satisfied, but the PSNR value can't be lowered more. For example, by changing the estimated method or using different methods dynamically different image distributions can be adapted. It is a future direction in our study.

Besides, in order to let the image be reversibly restored correctly, avoid the estimated difference superimposing to confuse. Every pixel value in the non-data-hiding image shifts towards left towards right. It takes more time. But if some pixels are recorded that which one has already hidden secret information which one has not hidden by the position map, extra data must be needed to include the position map, and the capacity of data hiding will be lowered. Therefore, we will try to improve this fault in the future. The information will be quickly retrieved and be correctly restored.

In this study, to encrypt the first layer pixel is only implemented. How to modify the data hiding algorithm? It can make the capacity of data hiding larger the information can be hidden into the second, the third, layers), at the same time, the reversible data hiding can be achieved. The quality of images can be remained or be lowered not too much. How to find the trade-off? This is sophisticated purpose in the future.

ACKNOWLEDGMENT

The authors would like to acknowledge the financial support of the Ministry of Science and Technology of Taiwan through its grant MOST 105-2221-E-606-011.

REFERENCES

[1] H. WTesng, and C. P. Hsieh, "Prediction-based reversible data hiding,"*Information Science*, vol. 179, no. 14, pp. 2460-2469, 2009.

[2] W. Hong, T. S. Chen, and C. WShiu, "Reversible data hiding for quality images using modification of prediction errors,"*The Journal of Systems and Software*, vol. 82, pp. 1833-1842, 2009.

[3] H. C. Wu, C. C. Lee, C. S. Tsai, Y. P. Chu, and H. R. Chen, "A high capacity reversible data hiding scheme with edge prediction and difference expansion,"*The Journal of Systems and Software*, vol. 82, pp. 1966-1973, 2009.

[4] N. J.Mielikainen, "LSB matching revisited,"*IEEE Signal Processing Letters*, vol. 13, no. 5, pp. 285-287, 2006.

[5] J.Tian, "Reversible data embedding using a difference expansion," *IEEE Tras. Circuits and Systems for Video Technology*, vol. 13, no. 8, pp. 890-896, 2003.

[6] C. F. Lee, H. L. Chen, and H. K. Tso, "Embedding capacity raising in reversible data hiding based on prediction of difference expansion,"*The Journal of Systems and Software*, vol. 83, pp. 1864-1872, 2010.

[7] C. H. Yang, and M. H. Tsai, "Improving histogram-based reversible data hiding by interleaving predictions,"*IET Image Process,* vol. 4, no. 4, pp. 223-234, 2009.

[8] G.Juhi, G.Priya,and S. C. Gupta, "Reversible data hiding technique using histogram shifting,"2nd*IEEE Conf. Computing for Sustainable Global Development*, pp. 2114-2119, 2015.

[9] Z.Xinpeng, "Separable reversible data hiding in encrypted image,"*IEEE Trans. Information Forensics and Security*, vol. 7, no. 2, pp. 826-832.

[10] Z.Xinpeng, "Reversible data hiding with optimal value transfer,"*IEEE Trans. Multimedia*, vol. 15, no. 2, pp. 316-325, 2013.

T.J. Chang received the B.S., M.S., and Ph.D. degrees in electrical and electronic engineering from Chung Cheng Institute of Technology (CCIT), National Defense University (NDU), Taiwan, ROC in 1993, 2001 and 2008, respectively. He has been a member of the faculty at CCIT, where he is currently an assistant professor in the Department of Electrical and Electronic Engineering. His teaching and research interests include operating system, information security, data structure, computer network.

I. H.Pan received his BS degree in electrical engineering from the School of Defense Science, Chung Cheng Institute of Technology (CCIT), National Defense University (NDU), Taiwan, Republic of China in 2015, and the M.S. degree in electrical engineering from the Chung Cheng Institute of Technology, National Defense University, Taiwan, Republic of China in 2005. Since 2015, he has been with the Air Command and Staff College (ACSC) of National Defense University, where he is currently an assistant professor. His current research interests include statistical pattern recognition, watermarking, information hiding cryptography, and steganography theory.

K. H. Tan received the B.S., M.S., and Ph.D. degrees in electrical and electronic engineering from Chung Cheng Institute of Technology (CCIT), National Defense University (NDU), Taiwan, ROC in 2002, 2007 and 2013, respectively. He has been a member of the faculty at CCIT, where he is currently an assistant professor in the Department of Electrical and Electronic Engineering. His teaching and research interests include power electronics, microgrid system and intelligent control.

S. J. Cheng is an assistant Professor and director in Department of Aircraft Engineering, Army Academy ROC, Taiwan. He received B.S. in electrical engineering from the Republic of China (ROC) Military Academy, Taiwan, ROC (1990-1994); and M.S degree in electrical engineering from the Chung Cheng Institute of Technology (CCIT), National Defense University (NDU), Taiwan, ROC (1999-2001). He received the PhD degree in the School of Defense science at the CCIT, NDU, Taiwan, ROC. (2006-2010). His research interests include optimization, artificial neural network, PEMFC, identification, numerical computation and transformer design.

C. W.Lan was born in Tainan, Taiwan, 1981. He received the B.S., M.S. and Ph.D. degrees from the Department of Electrical and Electronic Engineering, and the School of Defense Science, Chung Cheng Institute of Technology, National Defense University, Taoyuan, Taiwan, in 2003, 2006, and 2013, respectively. He is currently an Assistant Professor of the Department of Electrical and Electronic Engineering of Chung Cheng Institute of Technology, National Defense University. His current research interests include humanoid robot, computer vision, and remote control.

C. C. Hu received the B.S. and M.S. degrees in Electrical and Electronic Engineering from Chung-Cheng Institute of Technology, Taiwan in 2002, and 2007, respectively. He was received the Ph.D. degree in Electrical Engineering from National Central University, Taiwan in 2015. He has been a deputy engineer of the System Manufacturing Center at National Chung-Shan Institute of Science and Technology, and his research interests include nanophotonics, electromagnetic field simulation, near-field optics and plasmonics.