ISSN 2313-1527 (PRINT)
ISSN 2313-1535 (ONLINE)

IJEIE

International Journal of Electronics
and Information Engineering

Vol. 9, No. 1 (Sept. 2018)

INTERNATIONAL JOURNAL OF ELECTRONICS & INFORMATION ENGINEERING

PUBLISHING OFFICE

Min-Shiang Hwang
Department of Computer Science & Information Engineering, Asia University, Taichung 41354, Taiwan, R.O.C.
Email: mshwang@asia.edu.tw

International Journal of Electronics and Information Engineering is published both in traditional paper form (ISSN 2313-1527) and in Internet (ISSN 2313-1535) at http://ijeie.jalaxy.com.tw

PUBLISHER: Candy C. H. Lin

23-75, P.O. Box, Taichung, Taiwan 40199, R.O.C.

International Journal of Electronics and Information Engineering

Vol. 9, No. 1 (Sept. 1, 2018)

Smart Kitchen: Automated Cooker Technique Using IoT

Diaa Salama Abdul Minaam

(Corresponding author: Diaa Salama Abdul Minaam)

Information Systems Department, Faculty of Computers and Information, Benha University, Egypt

(Email: diaa.salama@fci.bu.edu.eg)

(Received Jan. 29, 2018; revised and accepted June 1, 2018)

Abstract

Catering companies around the world suffering from wasting food during cooking it because of a large number of meals preparing at the same time so that the Chef can forget them on the Cooker during preparing another one. The paper discusses the design, implementation, and evaluation of an embedded system using (IoT) technology for improving the control of cooking time of "Basmatio" restaurant in the city of Cairo, Egypt. This system allows the chef to choose between different timers for different meals and all timers can work in parallel which will save a lot of food losses and unnecessary employees, and this system will be an embedded system using avr-atmeg32.

Keywords: Automated Cooker; IoT; Smart Kitchen

1 Introduction

We are living in the Internet of Things (IoT) era. According to the prediction of the International Data Corporation [4], the global IoT market will grow from $655.8 billion in 2014 to 1.7$ trillion in 2020 with an annual growth rate of 16.9% [4, 6, 16].

The Internet of Things (IoT) plays a remarkable role in all aspects of our daily lives (See Figure 1). It covers many fields including healthcare, automobiles, entertainments, industrial appliances, sports, homes, etc. The pervasiveness of IoT eases some everyday activities, enriches the way people interact with the environment and surroundings, and augments our social interactions with other people and objects [?, 12, 21–23]. Developing applications for the IoT could be a challenging task due to several reasons:

1) The high complexity of distributed computing;

2) The lack of general guidelines or frameworks that handle low level communication and simplify high level implementation;

3) Multiple programming languages;

4) Various communication protocols.

It involves developers to manage the infrastructure and handle both software and hardware layers along with preserving all functional and non-functional software requirements [7, 8, 10, 11, 14, 15]. We proposed to design and construction of an embedded system in a kitchen cooker, its interfaced with an Atmega 32 microcontroller programmed in C language.

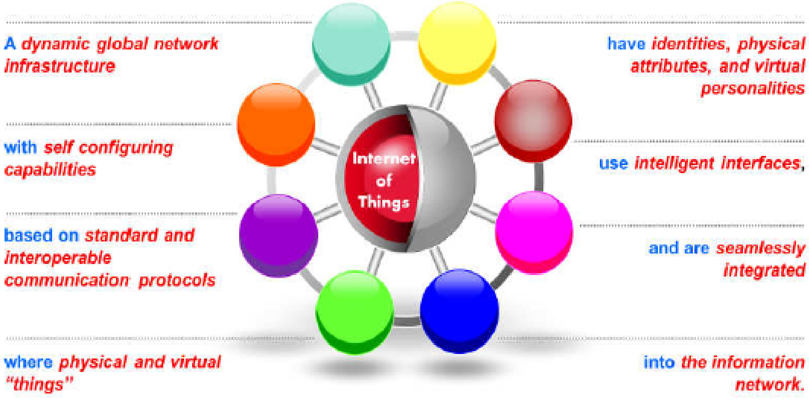

A dynamic global network infrastructure
with self configuring capabilities
based on standard and interoperable communication protocols
where physical and virtual "things"
have identities, physical attributes, and virtual personalities
use intelligent interfaces,
and are seamlessly integrated
into the information network.
Internet of Things

Figure 1: Internet of Things

1.1 Background to IoT

The IoT was envisioned in Mark Weisner's seminal paper on ubiquitous computing in 1991, "The computer of the 21st Century" [9]. However the term "The Internet of Things" wasn't used until 1999 by Kevin Ashton [20] who was working on networked Radio Frequency Identification (RFID) devices. Since then developments in communications and networking technology have fuelled an exponential growth in this area with IoT forecasted to soon become the largest global market sector [5].

Whilst there is concern over data security and intrusion into people's daily routines [18], these connected appliances offer many potentially helpful services, such as food management in the kitchen, remote heating control and health monitoring.

1.2 Role of IoT in Smart Kitchens

There is lot of promotion surrounding the IoT. The basic idea connects objects we use every day to the internet and each other allowing them to communicate in a novel way and make life easier. Many companies are making ventures into the field with internet connected kitchen appliances, clothing, home security systems. The implications of IoT in food industry more specifically making improvements in food safety are highly appreciable. The advancement in Wireless technology and cloud computing the IoT has the potential to make food more safer from the farm to the consumers dinner plate.

The smart kitchen is installed with all computing system to exhibit smart behavior based on sensors, actuators and interactive devices that are built in or embedded within the household articles such as dinning set, refrigerators, cooking range, coffee machine, oven, sink and so on. The integral components of the computing system will sense and model contextual information and apply it for providing smart services for a chosen application. Many other researchers who are recognized in literature on IoT applications such as [1–3, 17] studied the important of IoT application in our life.

2 Related Works

Numerous studies have attempted to explain and discuss smart kitchens with various approaches and methods. Shivaranjini S. Mogali [13] highlights the various aspects of IoT and its role in smart kitchen.

The different technologies such as RFID, WSN, Cloud Computing, Networking Technology and Nanotechnology that support the IoT, and their applications in various fields i.e Smart home, Smart City, Smart Grid, Smart Health and Smart Farming, and she found, and how IoT is significant because it could open new avenues of research and learning. Of course it raises serious concern about privacy, security and data owernership. The different applications of IoT in Kitchen ranks the highest when compared with other domains. Perhaps it may be due to the hi-fi living style and advancement of the applied technology in every walk of life. Ultimately the smooth functioning of the devices and the knowledge for their operation are essential to achieve the expected results. Otherwise the traditional cookware can only save us.

Shirsath *et al.* [17] aimed to design and construction of an SMS based Gas Leakage Alert System to reduce the risks in Kitchen if there is leakage in gas cylinder using Internet of Thing, and thereby leads to a faster response time in the events of a leakage condition. multiregional sensors has been designed, constructed and tested. The result obtained from the tests carried out shows that the system is capable of sending SMS alerts whenever there is gas concentration at the inputs of the gas sensors. For this they are using gas sensors, temperature sensors, weight sensors. Threshold values are set into the room, when it crosses that values it will send a notification to the user, about the leakage of a gas cylinder and leakage of a gas. Server can communicate with the user through android device. Through email and SMS server can sends a notification to the user which will display on the android devices. It can prevent the accident and hazards. It is a cost effective and time consuming solution.

Gaurav *et al.* [19] also focused on the gas leaking problem by designing a gas leaking monitoring system for kitchen and home safety. This system detects the leakage of the LPG and alerts the consumer about the leak by SMS and as an emergency measure the system will turnoff the power supply, while activating the alarm. The additional advantage of the system is that it continuously monitors the level of the LPG present in the cylinder using load sensor and if the gas level reaches below the threshold limit of gas around 2kg so that the user can replace the old cylinder with new in time and automatically books the cylinder using a GSM module .The device ensures safety and prevents suffocation and explosion due to gas leakage and software monitors all the functionality of software.

Lei *et al.* [24] developed an automatic checkout and healthy diet catering system based on lOT technique. By utilizing a new type dishware which embedded RFID tag, the system can mark the diet with IS014443A air protocol and bind it to the consumer. With the automatic checkout feature, it can save labor costs for the catering company and cut down the consumers' waiting time to improve the service quality. The system use a new type dishware which embedded RFID (Radio Frequency Identification) tags, via the uniqueness of the RFID tag's identification, so system can mark every dish the consumer select. When consumer checking out, the system can collect diet data by identify the RFID tags which embedded in dish ware. This system uses the advantage of cluster, providing catering enterprises SaaS (Software as a Service) service. Through the diet data mining, the system can draw the overall spending trend of consumers. On the one hand, the system can improve the efficiency of catering enterprises by the feature of automatic checkout. So the system can reduce the unsalable food to improve the catering enterprises profit.

3 Implementation

In the implementation process we walkthrough many steps, firstly we must specify the Hardware components of the system, and they are will be:

1) Input Unit:
   We have only one input in our device and it is the 4×4 Keypad (See Figure 2) and it‘s role is to make the user choose the meal which he wants to put on the stove that he already choose, and

to generate alarm sequence. The user press on the reset button to reset the stove and terminate the alarm sequence.

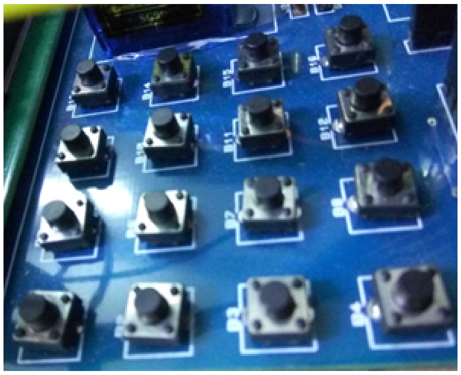


Figure 2: The 4 × 4 Keypad

2) Output Unit:
We used the LCD (LMO 016L 16 × 2 Alphanumeric; See Figure 3) as an output device because it makes the user simply see what he chooses and the changes in the system conditions easily, it is also easy to program and uses less DIOS from my micro controller

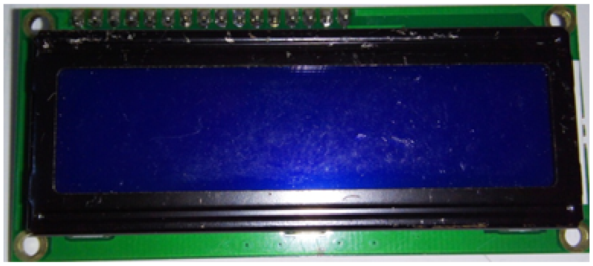


Figure 3: The LCD

3) Microcontroller Unit:
This unit is divided into two parts, hardware part and software part. The hardware is essentially the microcontroller. Microcontroller is a single chip containing a microprocessor, memory (RAM & ROM), input/output ports, timers and serial ports and it is designed for embedded control applications. We know that the main use of microcontroller is the control of a machine or system using a fixed program stored in the ROM and this program does not change over the lifetime of the system [14]. We used ATmega32 microcontroller. ATmega32 is an 8-bit high performance microcontroller of Atmel's Mega AVR family (See Figure 4). ATmega32 is based on enhanced RISC architecture with 131 powerful instructions. Most of the instructions execute in one machine cycle. ATmega32 can work on maximum frequency of 16MHZ. It contains 8-channel 10-bit A/D Converter and a JTAG interface for on-chip debugging. The device supports throughput of 16 MIPS at 16 MHz and operates between 4.5-5.5 volts.

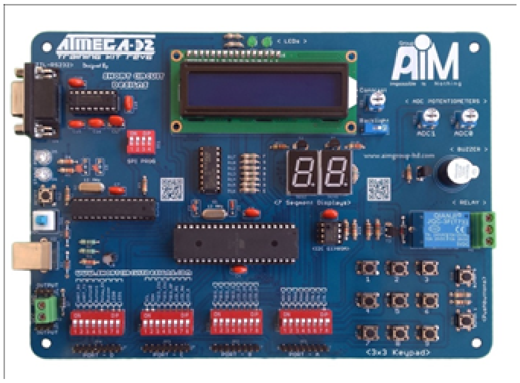


Figure 4: AVR - Atmega 32 Micro controller kit

4) Alarm Unit:
We also need buzzer and led as alarm indications for the user (See Figure 5).

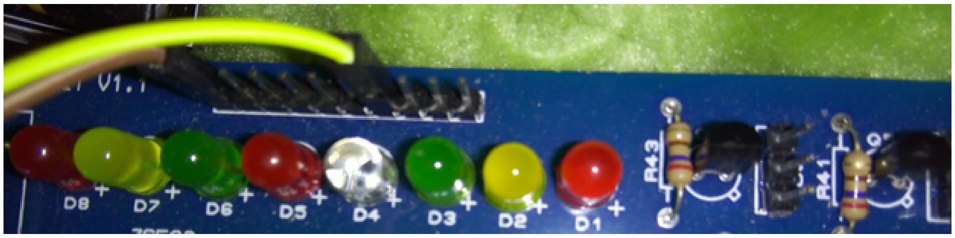


Figure 5: The Led Indicator

5) Burning Tool:
We used the USB asp as an AVR Burning Tool (See Figure 6).

Figure 6: USB ASP

6) Software Development:

The software needed to run the control process of this system was developed using C language in the microC PRO for AVR (See Figure 7). The program code was then written into the chip. Eclipse Neon 0.2 used to write code and burn it in the microcontroller.

We also need to specify Timers to calculate the time for the meals and give us indications when it‘s done, Choose the DIO-S to connect the hardware components (LCD - Keypad - Led - Buzzer), and create the drivers for the microcontroller peripherals (Timers - DIO - ISR ”Interrupt”) and the devices that I used (LCD - Keypad).

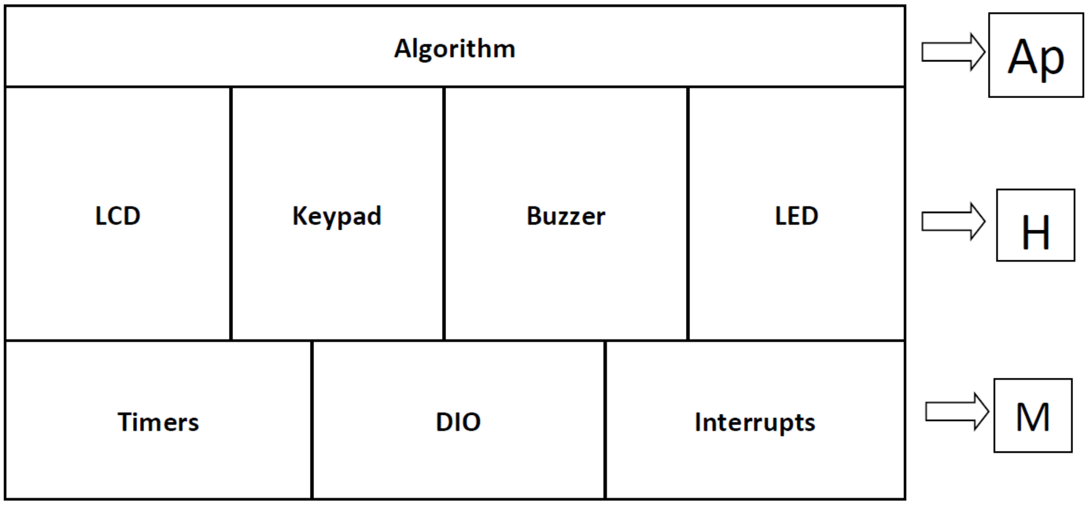


Figure 7: Static design

7) Construction:
The system was constructed in modules as designed and later put together on completion to simplify construction, testing and maintenance. After verifying that all the components are working as expected, we integrated them into a single system. The entire system circuit as shown in Figure 8 was laid out carefully to minimize error and to ease troubleshooting.

4 Results

At the first, the LCD will show the default screen which contains the cooker stoves numbers (See Figure 9).

And then check which button has the user pressed, if it was stove 1 the button waits until he choose the meal. And the same for the other stoves buttons. When the user chooses the meal it appears on the screen the name of the meal next to the stove he chooses (See Figure 10).

The global flag of the meal turns to 1 and when the code goes to the ISR it will check the flag of the meal when it finds the flag equals to 1, it starts the timer logic for this meal.

When the meal counter reaches the desired time, it starts the alarm sequence which is putting voltage on the pins which the buzzer and the led are connected to and they turned on (See Figure 11). And put (*) next to the meal name on the screen to work as indication that this meal has already finished.

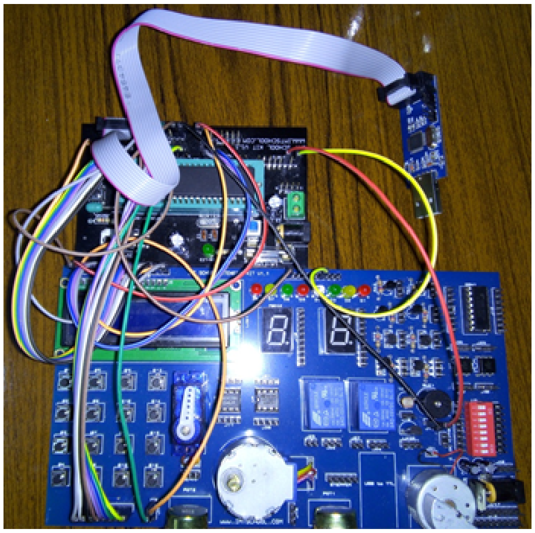


Figure 8: The system construction

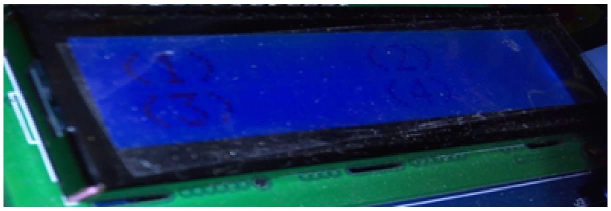


Figure 9: The default screen

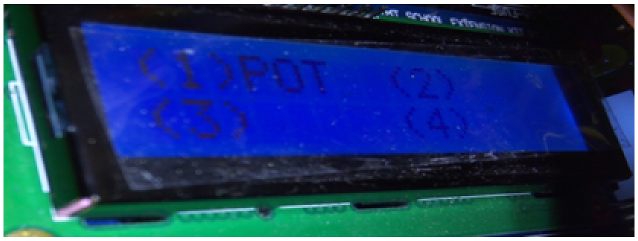


Figure 10: The screen after choosing the meal

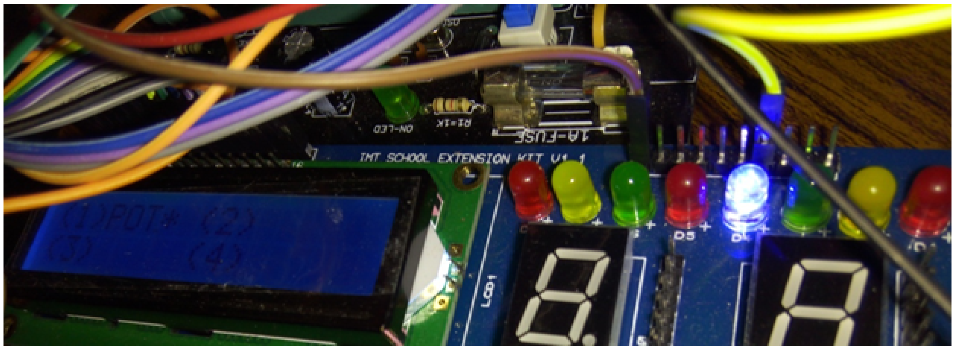


Figure 11: The screen and the led after reaching the desired time

If the user pressed on the reset button of the stove. It deletes the meals name, and the (*) from the LCD and remove the voltage from the pins which the buzzer and the led connected to terminates the alarm sequence for this stove, and return to the default screen (See Figure 12).

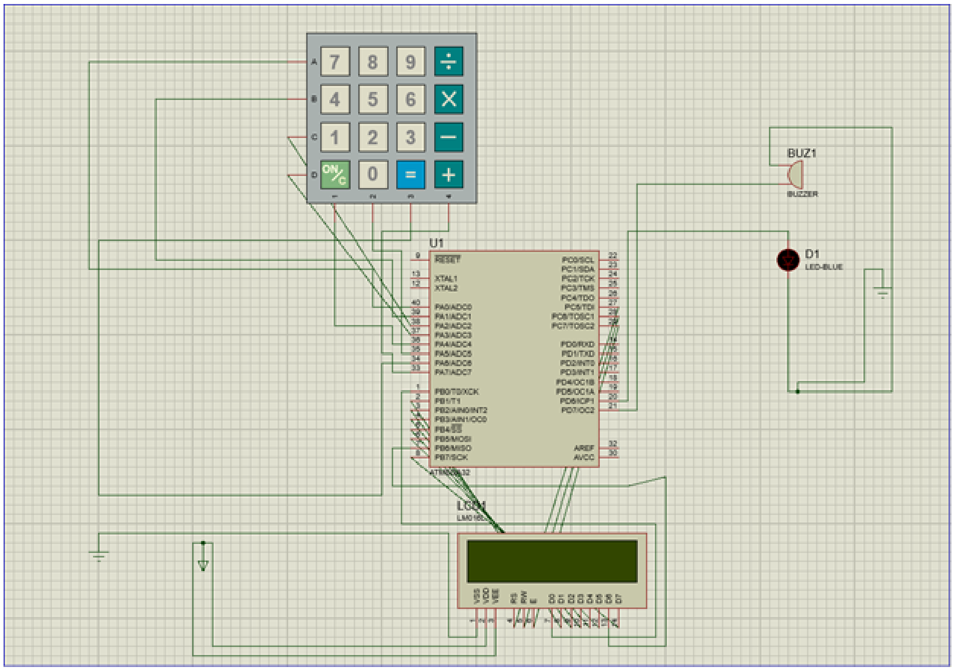


Figure 12: The system layout and the circuit diagram

5 Conclusions and Future Works

The IoT market is growing rapidly and as a consequence the attention has shifted from proposing single IoT elements and protocols towards application platforms in order to identify frameworks supporting the standard IoT suites of regulations and protocols. This study has covered a subset of commercially available frameworks and platforms for developing industrial and consumer based IoT applications. The developed IoT embedded system has partially solved the cooking problems in ”Basmatio” restaurants by allowing the chef to choose between different timers for different meals and the all timers can work in parallel.

One of the modifications is to provide the system with heat sensor for safety if there is undesired fire from the stove. Make the configuration of the meal time generic product. Not for ”Basmatio” only but for any restaurant. And Make a counter using 7 segment to count how many time as he cooked a certain meal, to know which meal is preferred by his clients and the average of each meal‘s ingredients consumption.

References

[1] D. S. Abdul.Elminaam, “Smart Life Saver System for Alzheimer patients, Down Syndromes, and Child Missing Using IoT,” *Asian Journal of Applied Sciences*, vol. 6, no. 1, pp. 21–37, Feb. 2018.

[2] D. S. Abdul.Elminaam, “ SHAS-IoT: Smart Home Automation System (SHAS) Using Internet of Things (IoT) to Improve Safety and Security,” *Research of applied Science*, vol. 13, no. 3, pp. 209–215, Mar. 2018.

[3] D. S. Abdul.Elminaam, T. M. M. Alenezi, “Building Smart Oil and Gas field Using IOT,” *International Journal of Advancements in Computing Technology*, vol. 9, no. 3, pp. 43–56, Dec. 2017.

[4] M. Chiang, T. Zhang, “Fog and IoT: An overview of research opportunities,” *IEEE Internet Things*, vol. 3, no. 6, pp. 854–864, Dec. 2016.

[5] J. Chung, S. Choi, C. J. Kee, E. Song, S. Moon, J. Kim and S. Noh, “A Study on Diagnosing Security Vulnerability Issues of Big Data and Internet of Things under IT Convergence,” *Journal of Engineering and Applied Sciences*, vol. 12, no. 12, pp. 3130–3132, 2017.

[6] J. Gubbia, R. Buyyab, S. Marusica, M. Palaniswamia, “IoT: A vision, architectural elements, and future directions,” *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, Sept. 2013.

[7] J. Huang, Y. Meng, X. Gong, “A novel deployment scheme for green Internet of Things,” *IEEE Internet Things*, vol. 1, no. 2, pp. 196–205, Apr. 2014.

[8] D. Kothandaraman and C. Chellappan, “Human Movement Tracking System with Smartphone Sensing and Bluetooth Low Energy in Internet of Things,” *Asian Journal of Information Technology*, vol. 15, no. 4, pp. 661–669, 2016.

[9] A. M. Kowshalya and M. L. Valarmathi, “Towards Trustworthy and Secure Communications in Social Internet of Things (SIoT),” *Asian Journal of Information Technology*, vol. 15, no. 20, pp. 3957–3964, 2016.

[10] R. Kranenburg and A. Bassi, “IoT challenges,” *Commun. Mobile Comput.*, vol. 1, no. 1, pp. 1–5, 2012.

[11] T. Liu and D. Lu, “The application and development of IoT,” in *Proceedings of International Symposium of Inf. Technol. Med. Educ. (ITME’12)*, vol. 2, pp. 991–994, 2012.

[12] D. Minoli, K. Sohraby, B. Occhiogrosso, “IoT considerations, requirements, and architectures for smart buildings-energy optimization and next-generation building management systems,” *IEEE Internet Things*, vol. 4, no. 1, pp. 269–273, Feb. 2017.

[13] S. S. Mogali, “Internet of Things and its role in Smart Kitchen,” in *4th National Conferrence of Scientometrics and Internet of Things*, Bangalore, Sep. 2015.

[14] C. E. A. Mulligan and M. Olsson, "Architectural implications of smart city business models: An evolutionary perspective," *IEEE Commun. Mag.*, vol. 51, no. 6, pp. 80–85, June 2013.

[15] S. Onofre, P. Sousa, J. P. Pimento, "Geo-referenced Multi-agent Architecture for Surveillance," in *Proceedings of the 16th International Power Electronics and Motion Control Conference and Exposition (PEMC'14)*, pp. 455–460, Sept. 2014.

[16] S. Rani, S. H. Ahmed, R. Talwar, J. Malhotra, H. Song, " IoMT: A reliable cross Layer protocol for internet of multimedia things," *IEEE Internet Things*, vol. 4, no. 3, pp. 832–839, June 2017.

[17] S. Shraddha, S. Snehal, C. Ameya, and T. Rahul, "SMART KITCHEN USING IOT," *International Journal of Advanced Research in Computer Engineering & Technology*, vol. 5, no. 5, pp. 1297–1301, May 2016.

[18] N. Syazarin, N. Abd Aziz, S. M. Daud, S. A. Syarif, H. Abas and A. Azizan, "An Overview on Security Features for Internet of Things (IoT) in Perception Layer," *Journal of Engineering and Applied Sciences*, vol. 12, no. 16, pp. 4132–4137, 2016.

[19] G. V. Tawale-Patil, K. H. Kulkarni, P. U. Kuwad, P. R. Pawar, "Smart Kitchen Using IoT," *International Journal of Research in Advent Technology*, Special Issue National Conference "NCPCI-2016", pp. 205–207, Mar. 2016.

[20] K. Velusamy, D. Venkitaramanan, S. K. Vasudevan, P. Periasamy and B. Arumugam, "Internet of Things in Cloud," *Journal of Engineering and Applied Sciences*, vol. 8, no. 9, pp. 304–313, 2013.

[21] I. Vilajosana, J. Llosa, B. Martinez, M. Domingo-Prieto, A. Angles, and X. Vilajosana, "Bootstrapping smart cities through a self-sustainable model based on big data flows," *IEEE Commun. Mag.*, vol. 51, no. 6, pp. 128–134, June 2013.

[22] K. Yang and Z. Zhang, "Summarize on IoT and exploration into technical system framework," in *Proceedings of IEEE Symposium on Robot. Appl. (ISRA'12)*, pp. 653–656, 2012.

[23] A. Zanella, N. Bui, A. Castellani, "Internet of Things for smart cities," *IEEE Internet Things*, vol. 1, no. 1, pp. 22–32, Feb. 2014.

[24] L. Zhoui, A. Wang, Y. Zhang, and S. Sun, "A Smart Catering System Base on Internet-of-Things Technique," in *IEEE Proceedings of ICCT'15*, pp. 433–436, 2015.

Biography

Diaa Salama Abdul-Minaam was born on November 23, 1982 in KafrSakr, Sharkia, Egypt. He received the B.S from Faculty of Computers & Informatics, Zagazig University, Egypt in 2004 with grade very good with honor, and obtains master degree in information system from faculty of computers and information, menufia university, Egypt in 2009 specializing in Cryptography and network security. He obtained his Ph.D. degree in information system from faculty of computers and information, menufia university,Egypt . He is currently a Lecturer in Information systems department, Faculty of Computers and Information, Benha University, Egypt since 2011. He has worked on a number of research topics .Diaa has contributed more than 20+ technical papers in the areas of wireless networks, wireless network security, Information security and Internet applications, Cloud Computing, Mobile Cloud Computing in international journals, international conferences, local journals and local conferences. He majors in Cryptography, Network Security, IoT, Big Data, Cloud Computing. (Mobile: +20166104747; +201019511000 E-mail: ds_desert@yahoo.com)

An Improvement of One Anonymous Identity-based Encryption Scheme

Lihua Liu[1], Zhenzhen Guo[1], Zhengjun Cao[2], Zhen Chen[2]
(Corresponding author: Zhengjun Cao)

Department of Mathematics, Shanghai Maritime University[1]
Haigang Ave 1550, Shanghai, 201306, China[1]
Department of Mathematics, Shanghai University[2]
Shangda Road 99, Shanghai, 200444, China[2]
(Email: caozhj@shu.edu.cn)

(Received Mar. 8, 2018; revised and accepted June 10, 2018)

Abstract

At PKC'09, Seo *et al.* proposed an anonymous identity-based encryption scheme. The ciphertext consists of (C_1, C_2, C_3, C_4), where C_1 is the blinded message, C_4 is the blinded identity. Both C_2 and C_3 are used as decrypting helpers. To prove its security, they defined five games and introduced a *strong simulator* who was able to select different Setups for those games. In this paper, we improve the scheme by removing one decrypting helper and the strong simulator. We show its security under the ℓ-computational Diffie-Hellman assumption with a normal simulator who requires only a unique Setup. The techniques developed in this paper are helpful to optimize other cryptographic protocols.

Keywords: Anonymous Identity-based Encryption; Decrypting Helper; Strong Simulator; ℓ-computational Diffie-Hellman Assumption

1 Introduction

The concept of identity-based encryption was introduced by Shamir in 1984 [25]. In the scenario, one can encrypt messages using a ure's identity information. Of course, some system public parameters should be involved. In 2002, Horwitz and Lynn [16] defined the notion of hierarchical ID-based encryption (HIBE for short), which can handle IDs hierarchically. In 2005, Abdalla *et al.* [1] introduced the concepts of anonymous IBE and anonymous HIBE. But they did not give a concrete construction of anonymous HIBE. An anonymous IBE requires that the ciphertext does not leak any information about the receiver's identity.

The primitive of anonymous IBE has interested many researchers. In 2006, Gentry [15] proposed a concrete construction of anonymous IBE in the standard model. Boyen and Waters [5] provided a concrete construction of anonymous HIBE. At PKC'09, Seo *et al.* [24] proposed an anonymous HIBE (SKOS for short) that has constant size ciphertexts, *i.e.*, the size of the ciphertext does not depend on the depth of the hierarchy. The SOKS scheme [24] is based on bilinear groups of composite order, which was introduced by Boneh, Goh, and Nissim [4]. The SOKS is inspired by BBG-HIBE [2]. The BBG-HIBE provides constant size ciphertexts but does not satisfy the requirement of anonymity. Recently, Fan *et al.* [14, 27] have proposed some anonymous multi-receiver identity-based encryption schemes. In 2014, Wang [26] pointed out that the improved anonymous multi-receiver identity-based encryption scheme [27] is insecure.

In order to alleviate user's pairing computation burden, Chevallier-Mames *et al.* [13] explored the problem of secure delegation of elliptic-curve pairing. Other algorithms for outsourcing of bilinear pairings were discussed in [6, 9, 12, 20]. In 2016, Hsien *et al.* [17] presented a survey of public auditing for secure data storage in cloud computing. Others discussed the problem of public auditing for shared data storage with user revocation [10, 11, 18, 19, 22].

In the SKOS scheme, the ciphertext consists of (C_1, C_2, C_3, C_4), where C_1 is the blinded message, C_4 is the blinded identity, both C_2 and C_3 are used as decrypting helpers. But the two helpers are *generated and used in parallel*. To reduce its cost, it is better to remove one helper. We also observe that the ciphertext is *repeatedly randomized*. Concretely, in the ciphertext $(ME^s, G^sZ_1, F^sZ_2, (V\prod_{i=1}^{k} H_i^{I_i})^s Z_3)$, the session key s is used for randomizing the message M and the ID as ME^s and $(V\prod_{i=1}^{k} H_i^{I_i})^s$, respectively. The other session keys Z_1, Z_2, Z_3 are used for randomizing $G^s, F^s, (V\prod_{i=1}^{k} H_i^{I_i})^s$, respectively. That means C_2, C_3, C_4 are repeatedly randomized. Apparently, it will incur more computational cost.

To prove the security of SKOS, they defined five games: $\mathrm{CT}_1 = (C_1, C_2, C_3, C_4)$, $\mathrm{CT}_2 = (C_1 \cdot R_p, C_2, C_3, C_4)$, $\mathrm{CT}_3 = (C_1 \cdot R = R_1, C_2, C_3, C_4)$, $\mathrm{CT}_4 = (R_1, R_2, C_3, C_4)$, $\mathrm{CT}_5 = (R_1, R_2, R_3, R_4)$, where R_p is a randomly chosen element from $\mathbb{G}_{T,p}$; R, R_1 are uniformly distributed in $\mathbb{G}_T$; and R_2, R_3, R_4 are uniformly distributed in $\mathbb{G}$ ($\mathbb{G}_{T,p}, \mathbb{G}_T, \mathbb{G}$ are different bilinear groups). To deal with different games, it has to introduce a *strong simulator* who is able to select different Setups for those games.

In this paper, we improve the SKOS scheme by removing one decrypting helper and the strong simulator. We show its security under the ℓ-computational Diffie-Hellman assumption with a normal simulator who only requires a unique Setup. we think that the analysis skills developed in this paper are helpful to optimize other cryptographic protocols.

2 Preliminary

Bilinear groups of composite order [4]. Let $\mathcal{G}$ be a group generation algorithm that takes security parameter 1^λ as input and outputs tuple $(p, q, \mathbb{G}, \mathbb{G}_T, e)$ where p and q are distinct primes, $\mathbb{G}$ and $\mathbb{G}_T$ are cyclic groups of order $n = p\,q$, and $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ is a non-degenerate bilinear map; i.e., e satisfies the following properties:

1) Bilinear: for $\forall\, g_1, h_1 \in \mathbb{G}$ and $\forall\, a, b \in \mathbb{Z}$, $e(g_1^a, h_1^b) = e(g_1, h_1)^{a\,b}$;
2) Non-degenerate: for generator g_1 of $\mathbb{G}$, $e(g_1, g_1)$ generates $\mathbb{G}_T$.

Let $\mathbb{G}_p$ and $\mathbb{G}_q$ denote the subgroups of $\mathbb{G}$ of order p and q, respectively. Then $\mathbb{G} = \mathbb{G}_p \times \mathbb{G}_q$. If g_1 is a generator of $\mathbb{G}$, then g_1^q and g_1^p are generators of $\mathbb{G}_p$ and $\mathbb{G}_q$, respectively. Let g_p and g_q denote generators of $\mathbb{G}_p$ and $\mathbb{G}_q$, respectively. Notice that $e(h_p, h_q) = 1$ for all random elements $h_p \in \mathbb{G}_p$ and $h_q \in \mathbb{G}_q$ because $e(h_p, h_q) = e(g_p^a, g_q^b)$ for some integers a, b, and

$$e(g_p^a, g_q^b) = e(g_1^{q\,a}, g_1^{p\,b}) = e(g_1, g_1)^{p\,q\,a\,b} = 1$$

for some generator g_1 in $\mathbb{G}$.

ℓ-computational Diffie-Hellman assumption. Given a cyclic group $\mathbb{G}$ of prime order p, a random generator g and $(g^a, g^{a^2}, \cdots, g^{a^\ell})$ for some random $a \in \mathbb{Z}_p^*$, it is computationally intractable to compute $g^{a^{\ell+1}}$.

Security definitions of anonymous HIBE. We refer to [1,3] for the formal security definitions of anonymous HIBE, and refer to [7,8] for a weaker notion of security that the adversary commits ahead of time to the public parameters that it will attack.

3 Review of The SKOS Scheme

Setup. Given a security parameter λ and the maximum hierarchy depth L, the algorithm generates $(p, q, \mathbb{G}, \mathbb{G}_T, e)$. Pick random elements $g, f, v, h_1, \cdots, h_L, w \in \mathbb{G}_p$, $R_g, R_f, R_v, R_1, \cdots, R_L \in \mathbb{G}_q$. and compute

$$G = gR_g, F = fR_f, V = vR_v,\ H_1 = h_1R_1, \cdots, H_L = h_LR_L, E = e(g, w).$$

Publish the description of a group $\mathbb{G}$ and public system parameters as $[g_q, G, F, V, H_1, \cdots, H_L, E]$. The master secret key is set as $[p, q, g, f, v, h_1, \cdots, h_L, w]$. The group description contains n but not p, q.

KeyGeneration. Given ID=$[I_1, I_2, \cdots, I_k] \in (\mathbb{Z}_n)^k$, pick random $r_1, r_2, s_1,\ s_2, t_1, t_2 \in \mathbb{Z}_n$ such that $s_1t_2 - s_2t_1 \neq 0 \bmod p$ and $\neq 0 \bmod q$. Output

$$\begin{aligned}\mathrm{Pvk}_{\mathrm{d}}^{\mathrm{ID}} &= [w(v\prod_{i=1}^{k} h_i^{I_i})^{r_1} f^{r_2}, g^{r_1}, g^{r_2}, h_{k+1}^{r_1}, \cdots, h_L^{r_1}],\\ \mathrm{Pvk}_{\mathrm{r}}^{\mathrm{ID}} &= [[(v\prod_{i=1}^{k} h_i^{I_i})^{s_1} f^{s_2}, g^{s_1}, g^{s_2}, h_{k+1}^{s_1}, \cdots, h_L^{s_1}], [(v\prod_{i=1}^{k} h_i^{I_i})^{t_1} f^{t_2}, g^{t_1}, g^{t_2}, h_{k+1}^{t_1}, \cdots, h_L^{t_1}]],\end{aligned}$$

where $\mathrm{Pvk}_{\mathrm{d}}^{\mathrm{ID}}$ is used for decryption and delegation, and $\mathrm{Pvk}_{\mathrm{r}}^{\mathrm{ID}}$ is used for re-randomization.

Derivation. Given a private key for the parent,

$$\begin{aligned}\mathrm{Pvk}^{\mathrm{ID}_{|k-1}} &= [\mathrm{Pvk}_d^{\mathrm{ID}_{|k-1}}, \mathrm{Pvk}_r^{\mathrm{ID}_{|k-1}}]\\ &= [[a_0, a_1, a_2, b_k, \cdots, b_L], [[\alpha_0, \alpha_1, \alpha_2, \beta_k, \cdots, \beta_L], [\alpha'_0, \alpha'_1, \alpha'_2, \beta'_k, \cdots, \beta'_L]]],\end{aligned}$$

pick random $\gamma_1, \gamma_2, \gamma_3, \delta_1, \delta_2, \delta_3 \in \mathbb{Z}_n$ such that $g_p^{\gamma_2\delta_3 - \gamma_3\delta_2} \neq 1$ and $g_q^{\gamma_2\delta_3 - \gamma_3\delta_2} \neq 1$. Output

$$\begin{aligned}\mathrm{Pvk}_d^{\mathrm{ID}_{|k}} &= [\zeta_0\theta_0^{\gamma_1}\theta_0'^{\delta_1}, \zeta_1\theta_1^{\gamma_1}\theta_1'^{\delta_1}, \zeta_2\theta_2^{\gamma_1}\theta_2'^{\delta_1}, \eta_{k+1}\phi_{k+1}^{\gamma_1}\phi_{k+1}'^{\delta_1}, \cdots, \eta_L\phi_L^{\gamma_1}\phi_L'^{\delta_1}],\\ \mathrm{Pvk}_r^{\mathrm{ID}_{|k}} &= [[\theta_0^{\gamma_2}\theta_0'^{\delta_2}, \theta_1^{\gamma_2}\theta_1'^{\delta_2}, \theta_2^{\gamma_2}\theta_2'^{\delta_2}, \phi_{k+1}^{\gamma_2}\phi_{k+1}'^{\delta_2}, \cdots, \phi_L^{\gamma_2}\phi_L'^{\delta_2}],\\ &\qquad [\theta_0^{\gamma_3}\theta_0'^{\delta_3}, \theta_1^{\gamma_3}\theta_1'^{\delta_3}, \theta_2^{\gamma_3}\theta_2'^{\delta_3}, \phi_{k+1}^{\gamma_3}\phi_{k+1}'^{\delta_3}, \cdots, \phi_L^{\gamma_3}\phi_L'^{\delta_3}]]\end{aligned}$$

where

$$\begin{aligned}[\zeta_0, \zeta_1, \zeta_2, \eta_{k+1}, \cdots, \eta_L] &= [a_0 \cdot b_k^{I_k}, a_1, a_2, b_{k+1}, \cdots, b_L]\\ [\theta_0, \theta_1, \theta_2, \phi_{k+1}, \cdots, \phi_L] &= [\alpha_0 \cdot \beta_k^{I_k}, \alpha_1, \alpha_2, \beta_{k+1}, \cdots, \beta_L]\\ [\theta'_0, \theta'_1, \theta'_2, \phi'_{k+1}, \cdots, \phi'_L] &= [\alpha'_0 \cdot \beta_k'^{I_k}, \alpha'_1, \alpha'_2, \beta'_{k+1}, \cdots, \beta'_L].\end{aligned}$$

Encryption. To encrypt message $M \in \mathbb{G}_T$ for a given identity $ID = [I_1, \cdots, I_k] \in (\mathbb{Z}_n)^k$, pick a random $s \in \mathbb{Z}_n$ and random $Z_1, Z_2, Z_3 \in \mathbb{G}_q$. Output the ciphertext

$$(ME^s, G^sZ_1, F^sZ_2, (V\prod_{i=1}^{k} H_i^{I_i})^s Z_3).$$

Decryption. To decrypt ciphertext (C_1, C_2, C_3, C_4) with respect to $ID = [I_1, \cdots, I_k]$, using the first three elements of subkey $\mathrm{Pvk}_d^{\mathrm{ID}} = [a_0, a_1, a_2, b_{k+1}, \cdots, b_L]$, compute the plaintext

$$M = C_1 \cdot e(a_1, C_4) \cdot e(a_2, C_3)/e(a_0, C_2).$$

4 Analysis of The SKOS Scheme

On the doubly randomized key. The ciphertext consists of (C_1, C_2, C_3, C_4), where C_1 is the blinded message, C_4 is the blinded identity, both C_2 and C_3 are decrypting helpers. The reason to set two decrypting helpers is that the authors adopt the doubly randomized key, i.e.,

$$\mathrm{Pvk}_{\mathrm{d}}^{\mathrm{ID}} = [w(v\prod_{i=1}^{k} h_i^{I_i})^{r_1} f^{r_2}, g^{r_1}, g^{r_2}, h_{k+1}^{r_1}, \cdots, h_L^{r_1}].$$

Notice that $a_1 = g^{r_1}$ and $a_2 = g^{r_2}$ are used for decryption in parallel. But we know the setting is unnecessary because it incurs more computational cost. Based on this observation, we can set the decrypting key as

$$\mathrm{Pvk}_{\mathrm{d}}^{\mathrm{ID}} = [w(v\prod_{i=1}^{k} h_i^{I_i})^{r_1}, g^{r_1}, h_{k+1}^{r_1}, \cdots, h_L^{r_1}],$$

and the re-randomizing key as

$$\mathrm{Pvk}_{\mathrm{r}}^{\mathrm{ID}} = [[(v\prod_{i=1}^{k} h_i^{I_i})^{s_1}, g^{s_1}, h_{k+1}^{s_1}, \cdots, h_L^{s_1}], [(v\prod_{i=1}^{k} h_i^{I_i})^{t_1}, g^{t_1}, h_{k+1}^{t_1}, \cdots, h_L^{t_1}]].$$

Correspondingly, the system parameters can be optimized as

$$[G, V, H_1, \cdots, H_L, E], \quad [p, q, g, v, h_1, \cdots, h_L, w]$$

for the public system parameters and the master secret key, respectively.

Taking into account that the *fixed argument* for bilinear map using the Miller algorithm [23] is more efficient than that for unfixed argument, we can further optimize the SKOS-IBE scheme by setting that $w = v$. We will show the change does not endanger its security.

On repeatedly randomizing the ciphertext. To encrypt a message $M \in \mathbb{G}_T$ for a given identity $ID = [I_1, \cdots, I_k] \in (\mathbb{Z}_n)^k$, it randomly picks $s \in \mathbb{Z}_n$, $Z_1, Z_2, Z_3 \in \mathbb{G}_q$, and computes the ciphertext

$$(ME^s, G^s Z_1, F^s Z_2, (V\prod_{i=1}^{k} H_i^{I_i})^s Z_3).$$

We here stress that it is unnecessary to repeatedly randomizing

$$G^s, F^s, (V\prod_{i=1}^{k} H_i^{I_i})^s$$

with Z_1, Z_2, Z_3, respectively. The structure of $(V\prod_{i=1}^{k} H_i^{I_i})^s$ suffices to blind the identity $[I_1, \cdots, I_k]$ because one can not recover the secret exponent s, which is usually called *session key*. Therefore, it is better to remove those redundant blinders Z_1, Z_2, Z_3.

On the strong simulator. To prove its security, the authors defined five games and introduced a *strong simulator* who is able to select different Setups for those games. See Lemma 1, Lemma 3, and Lemma 4 in the Section 3.2 [24] for details. We will show the security of the improvement under the ℓ-computational Diffie-Hellman assumption with a normal simulator who only requires a unique Setup.

5 An Improvement of The SKOS Scheme

5.1 Construction

Setup. Given a security parameter λ and the maximum hierarchy depth L, the algorithm generates $(p, q, \mathbb{G}, \mathbb{G}_T, e)$. Pick random elements $g, v, h_1, \cdots, h_L \in \mathbb{G}_p$, $R_g, R_v, R_1, \cdots, R_L \in \mathbb{G}_q$, and compute

$$G = gR_g, V = vR_v,\ H_1 = h_1R_1, \cdots, H_L = h_LR_L, E = e(g, v).$$

Publish the description of a group $\mathbb{G}$ and public system parameters as $[G, V, H_1, \cdots, H_L, E]$. The master secret key is set as $[p, q, g, v, h_1, \cdots, h_L]$.

KeyGeneration. Given ID=$[I_1, I_2, \cdots, I_k] \in (\mathbb{Z}_n)^k$, pick random $r_1, s_1, t_1 \in \mathbb{Z}_n$, output

$$\mathrm{Pvk}_{\mathrm{d}}^{\mathrm{ID}} = [v(v\prod_{i=1}^{k} h_i^{I_i})^{r_1}, g^{r_1}, h_{k+1}^{r_1}, \cdots, h_L^{r_1}].$$

$$\mathrm{Pvk}_{\mathrm{r}}^{\mathrm{ID}} = [[(v\prod_{i=1}^{k} h_i^{I_i})^{s_1}, g^{s_1}, h_{k+1}^{s_1}, \cdots, h_L^{s_1}], [(v\prod_{i=1}^{k} h_i^{I_i})^{t_1}, g^{t_1}, h_{k+1}^{t_1}, \cdots, h_L^{t_1}]].$$

Derivation. Given a private key for the parent,

$$\mathrm{Pvk}^{\mathrm{ID}_{|k-1}} = [\mathrm{Pvk}_d^{\mathrm{ID}_{|k-1}}, \mathrm{Pvk}_r^{\mathrm{ID}_{|k-1}}] = [[a_0, a_1, b_k, \cdots, b_L],\ [[\alpha_0, \alpha_1, \beta_k, \cdots, \beta_L], [\alpha'_0, \alpha'_1, \beta'_k, \cdots, \beta'_L]]],$$

pick random $\gamma_1, \gamma_2, \gamma_3, \delta_1, \delta_2, \delta_3 \in \mathbb{Z}_n$ such that $g_p^{\gamma_2\delta_3-\gamma_3\delta_2} \neq 1$ and $g_q^{\gamma_2\delta_3-\gamma_3\delta_2} \neq 1$. Output

$$\mathrm{Pvk}_d^{\mathrm{ID}_{|k}} = [\zeta_0\theta_0^{\gamma_1}\theta_0'^{\delta_1}, \zeta_1\theta_1^{\gamma_1}\theta_1'^{\delta_1}, \eta_{k+1}\phi_{k+1}^{\gamma_1}\phi_{k+1}'^{\delta_1}, \cdots, \eta_L\phi_L^{\gamma_1}\phi_L'^{\delta_1}]$$
$$\mathrm{Pvk}_r^{\mathrm{ID}_{|k}} = [[\theta_0^{\gamma_2}\theta_0'^{\delta_2}, \theta_1^{\gamma_2}\theta_1'^{\delta_2}, \phi_{k+1}^{\gamma_2}\phi_{k+1}'^{\delta_2}, \cdots, \phi_L^{\gamma_2}\phi_L'^{\delta_2}], [\theta_0^{\gamma_3}\theta_0'^{\delta_3}, \theta_1^{\gamma_3}\theta_1'^{\delta_3}, \phi_{k+1}^{\gamma_3}\phi_{k+1}'^{\delta_3}, \cdots, \phi_L^{\gamma_3}\phi_L'^{\delta_3}]]$$

where

$$[\zeta_0, \zeta_1, \eta_{k+1}, \cdots, \eta_L] = [a_0 \cdot b_k^{I_k}, a_1, b_{k+1}, \cdots, b_L],$$
$$[\theta_0, \theta_1, \phi_{k+1}, \cdots, \phi_L] = [\alpha_0 \cdot \beta_k^{I_k}, \alpha_1, \beta_{k+1}, \cdots, \beta_L],$$
$$[\theta'_0, \theta'_1, \phi'_{k+1}, \cdots, \phi'_L] = [\alpha'_0 \cdot \beta_k'^{I_k}, \alpha'_1, \beta'_{k+1}, \cdots, \beta'_L].$$

Encryption. To encrypt message $M \in \mathbb{G}_T$ for a given identity $ID = [I_1, \cdots, I_k] \in (\mathbb{Z}_n)^k$, pick a random $s \in \mathbb{Z}_n$ and output the ciphertext $(ME^s, G^s, (V\prod_{i=1}^{k} H_i^{I_i})^s)$.

Decryption. To decrypt ciphertext (C_1, C_2, C_3) with respect to $ID = [I_1, \cdots, I_k]$, using the first two elements of subkey $\mathrm{Pvk}_d^{\mathrm{ID}} = [a_0, a_1, b_{k+1}, \cdots, b_L]$, compute $M = C_1 \cdot e(a_1, C_3)/e(a_0, C_2)$.

Correctness.

$$C_1 \cdot e(a_1, C_3)/e(a_0, C_2) = ME^s \cdot e(a_1, (V \prod_{i=1}^{k} H_i^{I_i})^s)/e(a_0, G^s)$$

$$= Me(g, v)^s \cdot \frac{e\left(g^{r_1}, (vR_v \prod_{i=1}^{k} (h_i R_i)^{I_i})^s\right)}{e\left(v(v \prod_{i=1}^{k} h_i^{I_i})^{r_1}, G^s\right)} = Me(g, v)^s \cdot \frac{e\left(g^{r_1}, (v \prod_{i=1}^{k} h_i^{I_i})^s\right)}{e\left(v(v \prod_{i=1}^{k} h_i^{I_i})^{r_1}, g^s\right)}$$

$$= Me(g, v)^s / e(v, g^s) = M$$

Notice that we here have to use the property that $e(h_p, h_q) = 1$ for all $h_p \in \mathbb{G}_p$ and $h_q \in \mathbb{G}_q$. We refer to Table 1 for the differences between the original scheme and the improvement.

Table 1: The SKOS shceme and its improvement

The SKOS-IBE scheme	The improvement
PK: $g_q, G, F, V, H_1, \cdots, H_L, E$ SK: $p, q, g, f, v, h_1, \cdots, h_L, w$	PK: $G, V, H_1, \cdots, H_L, E$ SK: $p, q, g, v, h_1, \cdots, h_L$
Pick $r_1, r_2 \in \mathbb{Z}_n$, compute $\mathrm{Pvk}_{\mathrm{d}}^{\mathrm{ID}}$ as $a = (w(v \prod_{i=1}^{k} h_i^{I_i})^{r_1} f^{r_2}, g^{r_1}, g^{r_2}, h_{k+1}^{r_1}, \cdots, h_L^{r_1})$	Pick $r_1 \in \mathbb{Z}_n$, compute $\mathrm{Pvk}_{\mathrm{d}}^{\mathrm{ID}}$ as $a = (v(v \prod_{i=1}^{k} h_i^{I_i})^{r_1}, g^{r_1}, h_{k+1}^{r_1}, \cdots, h_L^{r_1})$
Pick $s \in \mathbb{Z}_n$, $Z_1, Z_2, Z_3 \in \mathbb{G}_q$, compute $C = (ME^s, G^s Z_1, F^s Z_2, (V \prod_{i=1}^{k} H_i^{I_i})^s Z_3)$	Pick $s \in \mathbb{Z}_n$, compute $C = (ME^s, G^s, (V \prod_{i=1}^{k} H_i^{I_i})^s)$
$M = C_1 \cdot e(a_1, C_4) \cdot e(a_2, C_3)/e(a_0, C_2)$	$M = C_1 \cdot e(a_1, C_3)/e(a_0, C_2)$

5.2 Security Proof

Theorem 1. *If the Setup and KeyGeneratation algorithms satisfy the $(t, \epsilon)-$ ℓ-computational Diffie-Hellman assumption, then there is no adversary with running time t that succeeds to decrypt a ciphertext with advantage ϵ.*

Proof. We assume there exists adversary $\mathcal{A}$ that succeeds to decrypt a ciphertext with advantage ϵ. We show that there is a simulator $\mathcal{B}$ using $\mathcal{A}$ to solve the ℓ-computational Diffie-Hellman problem with advantage ϵ. The adversary $\mathcal{A}$ and simulator $\mathcal{B}$ run the following game.

Initialization. $\mathcal{A}$ chooses identity $ID = [I_1, I_2, \cdots, I_m]$, and sets $I_{m+1} = \cdots = I_L = 0$. Then $\mathcal{A}$ picks a random $a \in \mathbb{Z}_n$ and sets $A_i = g_p^{a^i}$ for $1 \leq i \leq L$. $\mathcal{A}$ sends ID and A_i $(1 \leq i \leq L)$ to the simulator $\mathcal{B}$, and keeps the secret a.

Setup. $\mathcal{B}$ picks random integers and random elements

$$y, x_1, \cdots, x_L \in \mathbb{Z}_n, \ R_g, R_v, R_{h,1}, \cdots, R_{h,l} \in \mathbb{G}_q.$$

Notice that a random element of $\mathbb{G}_p(\mathbb{G}_q)$ can be chosen by raising g_p (g_q, respectively) to random exponents from $\mathbb{Z}_n$. $\mathcal{B}$ computes $v = g_p^y \prod_{i=1}^{L} (A_{L-i+1})^{I_i}$ and sets

$$G = g_p R_g, V = (g_p^y \prod_{i=1}^{L} (A_{L-i+1})^{I_i}) R_v, E = e(A_1, v),$$

$$H_i = g_p^{x_i}/A_{L-i+1}R_{h,i}, \text{ for } 1 \leq i \leq L.$$

Then $\mathcal{B}$ sends $(v, h_1, \cdots, h_L)$ to $\mathcal{A}$, where

$$h_i = g_p^{x_i}/A_{L-i+1} \text{ for } 1 \leq i \leq L.$$

$\mathcal{B}$ finally publishes these parameters $(G, V, E, H_1, \cdots, H_L)$.

Query. For $ID^* = [I_1^*, I_2^*, \cdots, I_u^*]$, where $u \leq L$ is distinct from ID and all its prefixes, $\mathcal{B}$ chooses random integers $r_1 \in \mathbb{Z}_n$ and sends (r_1, ID^*) to $\mathcal{A}$.

Response. Let k be the smallest integer such that $I_k \neq I_k^*$. $\mathcal{A}$ sets

$$\hat{r}_1 = r_1 + a^k/(I_k^* - I_k)$$

and picks random $s_1, t_1 \in \mathbb{Z}_n$. Then $\mathcal{A}$ computes

$$\text{Pvk}_{\text{d}}^{\text{ID}} = [v(v\prod_{i=1}^{k} h_i^{I_i^*})^{\hat{r}_1}, g^{\hat{r}_1}, h_{k+1}^{\hat{r}_1}, \cdots, h_L^{\hat{r}_1}],$$

$$\text{Pvk}_{\text{r}}^{\text{ID}} = [[(v\prod_{i=1}^{k} h_i^{I_i^*})^{s_1}, g^{s_1}, h_{k+1}^{s_1}, \cdots, h_L^{s_1}], [(v\prod_{i=1}^{k} h_i^{I_i^*})^{t_1}, g^{t_1}, h_{k+1}^{t_1}, \cdots, h_L^{t_1}]],$$

and sends Pvk^{ID} to $\mathcal{B}$.

Output. Denote the first component of $\text{Pvk}_{\text{d}}^{\text{ID}}$ by $\tau = v(v\prod_{i=1}^{k} h_i^{I_i^*})^{\hat{r}_1}$, we then have

$$\begin{aligned}
\tau/v &= (v\prod_{i=1}^{k} h_i^{I_i^*})^{\hat{r}_1} = (v\prod_{i=1}^{k} h_i^{I_i^*})^{r_1} \cdot (v\prod_{i=1}^{k} h_i^{I_i^*})^{a^k/(I_k^*-I_k)} \\
&= (v\prod_{i=1}^{k} h_i^{I_i^*})^{r_1} \cdot \left(g_p^y \prod_{i=1}^{L} (A_{L-i+1})^{I_i} \prod_{i=1}^{k} (g_p^{x_i}/A_{L-i+1})^{I_i^*} \right)^{a^k/(I_k^*-I_k)} \\
&= (v\prod_{i=1}^{k} h_i^{I_i^*})^{r_1} \cdot \left(g_p^y A_{L-k+1}^{I_k-I_k^*} \prod_{i=k+1}^{L} (A_{L-i+1})^{I_i} \prod_{i=1}^{k} g_p^{x_i I_i^*} \right)^{a^k/(I_k^*-I_k)} \\
&= (v\prod_{i=1}^{k} h_i^{I_i^*})^{r_1} \cdot \left(A_k^y A_{L+1}^{I_k-I_k^*} \prod_{i=k+1}^{L} (A_{L+k-i+1})^{I_i} \prod_{i=1}^{k} A_k^{x_i I_i^*} \right)^{1/(I_k^*-I_k)} \\
&= (v\prod_{i=1}^{k} h_i^{I_i^*})^{r_1} \cdot A_{L+1}^{-1} \left(A_k^y \prod_{i=k+1}^{L} (A_{L+k-i+1})^{I_i} \prod_{i=1}^{k} A_k^{x_i I_i^*} \right)^{1/(I_k^*-I_k)}
\end{aligned}$$

Hence,

$$g^{a^{L+1}} = A_{L+1} = \frac{v}{\tau} \cdot (v\prod_{i=1}^{k} h_i^{I_i^*})^{r_1} \cdot \left(A_k^y \prod_{i=k+1}^{L} (A_{L+k-i+1})^{I_i} \prod_{i=1}^{k} A_k^{x_i I_i^*} \right)^{1/(I_k^*-I_k)}.$$

Since $\mathcal{B}$ knows $k, L, \tau, v, y, r_1, x_i, A_i, h_i$, for all $1 \leq i \leq L$, he can compute the right side. Thus, $\mathcal{B}$ can obtain $g^{a^{L+1}}$. That is, $\mathcal{B}$ can solve the ℓ-computational Diffie-Hellman problem. We refer to the following Table 2 for the outline of security proof simulation.

□

Table 2: Simulation for the new construction

$\mathcal{A}$		$\mathcal{B}$
Pick $ID = [I_1, I_2, \cdots, I_m]$ and, set $I_{m+1} = \cdots = I_L = 0$. Pick $a \in \mathbb{Z}_n$ and set $A_i = g_p^{a^i}$, $1 \leq i \leq L$.	$\xrightarrow{ID, A_i, i=1,\cdots,L}$	Pick $y, x_1, \cdots, x_L \in \mathbb{Z}_n$, $R_g, R_v, R_{h,1}, \cdots, R_{h,l} \in \mathbb{G}_q$. Compute $v = g_p^y \prod_{i=1}^{L} (A_{L-i+1})^{I_i}$ and set $G = g_p R_g, E = e(A_1, v)$, $V = (g_p^y \prod_{i=1}^{L} (A_{L-i+1})^{I_i}) R_v$, $H_i = g_p^{x_i} / A_{L-i+1} R_{h,i}, 1 \leq i \leq L$. Set $h_i = g_p^{x_i} / A_{L-i+1}$, $1 \leq i \leq L$.
	$\xleftarrow{(v, h_1, \cdots, h_L)}$	Publish $(G, V, E, H_1, \cdots, H_L)$. For $ID^* = [I_1^*, I_2^*, \cdots, I_u^*]$, $u \leq L$,
	$\xleftarrow{(r_1, ID^*)}$	pick $r_1 \leftarrow \mathbb{Z}_n$.
Set k be the smallest integer such that $I_k \neq I_k^*$. Set $\hat{r}_1 = r_1 + a^k/(I_k^* - I_k)$ and pick $s_1, t_1 \in \mathbb{Z}_n$. Compute $\mathrm{Pvk}_{\mathrm{d}}^{\mathrm{ID}} =$ $[v(v \prod_{i=1}^{k} h_i^{I_i^*})^{\hat{r}_1}, g^{\hat{r}_1}, h_{k+1}^{\hat{r}_1}, \cdots, h_L^{\hat{r}_1}]$, $\mathrm{Pvk}_{\mathrm{r}}^{\mathrm{ID}} =$ $[[(v \prod_{i=1}^{k} h_i^{I_i^*})^{s_1}, g^{s_1}, h_{k+1}^{s_1}, \cdots, h_L^{s_1}]$, $[(v \prod_{i=1}^{k} h_i^{I_i^*})^{t_1}, g^{t_1}, h_{k+1}^{t_1}, \cdots, h_L^{t_1}]]$	$\xrightarrow{\mathrm{Pvk}^{\mathrm{ID}}}$	Output $A_{L+1} = \frac{v}{\tau} \cdot (v \prod_{i=1}^{k} h_i^{I_i^*})^{r_1} \cdot$ $\left(A_k^y \prod_{i=k+1}^{L} (A_{L+k-i+1})^{I_i} \prod_{i=1}^{k} A_k^{x_i I_i^*} \right)^{\frac{1}{(I_k^* - I_k)}}$

6 Conclusion

In this paper, we improve the SKOS scheme and prove its security under ℓ-computational Diffie-Hellman assumption. The problem to determine whether a cryptographic scheme has redundant parameters is very difficult. In our opinion, if the designer of the original scheme can not provide an attack against an obviously simplified scheme, then the original could be of redundancy. By the way, the bilinear groups with a large composite order are very hard to practically implement. We refer to Ref. [21] for the details.

Acknowledgements

We thank the National Natural Science Foundation of China (61303200, 61411146001). We are grateful to the reviewers for their valuable suggestions.

References

[1] M. Abdalla *et al.*, "Searchable encryption revisited: Consistency properties, relation to anonymous ibe, and extensions," in *Proceedings of Annual Cryptology Conference, Advances in Cryptology (CRYPTO'05)*, pp. 205–222, Santa Barbara, California, USA, Aug. 2005.

[2] D. Boneh, X. Boyen, and E.-J. Goh, "Hierarchical identity based encryption with constant size ciphertexts," in *Proceedings of International Conference on the Theory and Application of Cryptographic Techniques, Advances in Cryptology (EUROCRYPT'05)*, pp. 440–456, Aarhus, Denmark, May 2005.

[3] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Proceedings of Annual Cryptology Conference, Advances in Cryptology (CRYPTO'01)*, pp. 213–229, Santa Barbara, California, USA, Aug. 2001.

[4] D. Boneh, E. Goh, and K. Nissim, "Evaluating 2-dnf formulas on ciphertexts," in *Proceedings of Theory of Cryptography (TCC'05)*, pp. 325–341, Cambridge, MA, USA, Feb. 2005.

[5] X. Boyen and B. Waters, "Anonymous hierarchical identity-based encryption (without random oracles)," in *Proceedings of Annual Cryptology Conference, Advances in Cryptology (CRYPTO'06)*, pp. 290–307, Santa Barbara, California, USA, Aug. 2006.

[6] S. Canard, J. Devigne, and O. Sanders, "Delegating a pairing can be both secure and efficient," in *Proceedings of Applied Cryptography and Network Security (ACNS'14)*, pp. 549–565, Lausanne, Switzerland, June 2014.

[7] R. Canetti, S. Halevi, and J. Katz, "A forward-secure public-key encryption scheme," in *Proceedings of International Conference on the Theory and Application of Cryptographic Techniques, Advances in Cryptology (EUROCRYPT'03)*, pp. 255–271, Warsaw, Poland, May 2003.

[8] R. Canetti, S. Halevi, and J. Katz, "Chosen-ciphertext security from identity-based encryption," in *Proceedings of International Conference on the Theory and Application of Cryptographic Techniques, Advances in Cryptology (EUROCRYPT'04)*, pp. 207–222, Interlaken, Switzerland, May 2004.

[9] Z. J. Cao, L. H. Liu, and O. Markowitch, "On two kinds of flaws in some server-aided verification schemes," *International Journal of Network Security*, vol. 18, no. 6, pp. 1054–1059, 2016.

[10] J. S. Chen, C. Y. Yang, and M. S. Hwang, "The capacity analysis in the secure cooperative communication system," *International Journal of Network Security*, vol. 19, no. 6, pp. 863–869, 2017.

[11] T. Y. Chen, C. C. Lee, M. S. Hwang, and J. K. Jan, "Towards secure and efficient user authentication scheme using smart card for multi-server environments," *Journal of Supercomputing*, vol. 66, no. 2, pp. 1008–1032, 2013.

[12] X. F. Chen and et al., "Efficient algorithms for secure outsourcing of bilinear pairings," *Theoretical Computer Science*, no. 562, pp. 112–121, 2015.

[13] B. Chevallier-Mames and et al., "Secure delegation of elliptic-curve pairing," in *Proceedings of Smart Card Research and Advanced Application, 9th IFIP WG 8.8/11.2 International Conference (CARDIS'10)*, pp. 24–35, Passau, Germany, April 2010.

[14] C. Fan, L. Y. Huang, and P. H. Ho, "Anonymous multireceiver identity-based encryption," *IEEE Transaction on Computers*, vol. 59, no. 9, pp. 1239–1249, 2010.

[15] C. Gentry, "Practical identity-based encryption without random oracles," in *Proceedings of International Conference on the Theory and Application of Cryptographic Techniques, Advances in Cryptology (EUROCRYPT'06)*, pp. 445–464, St. Petersburg, Russia, May 2006.

[16] J. Horwitz and B. Lynn, "Towards hierarchical identity-based encryption," in *Proceedings of International Conference on the Theory and Application of Cryptographic Techniques, Advances in Cryptology (EUROCRYPT'02)*, pp. 466–481, Amsterdam, The Netherlands, May 2002.

[17] W. F. Hsien, C. C. Yang, and M. S. Hwang, "A survey of public auditing for secure data storage in cloud computing," *International Journal of Network Security*, vol. 18, no. 1, pp. 133–142, 2016.

[18] C. W. Liu, W. F. Hsien, C. C. Yang, and M. S. Hwang, "A survey of attribute-based access control with user revocation in cloud data storage," *International Journal of Network Security*, vol. 18, no. 5, pp. 900–916, 2016.

[19] C. W. Liu, W. F. Hsien, C. C. Yang, and M. S. Hwang, "A survey of public auditing for shared data storage with user revocation in cloud computing," *International Journal of Network Security*, vol. 18, no. 4, pp. 650–666, 2016.

[20] L. H. Liu and Z. J. Cao, "A note on 'efficient algorithms for secure outsourcing of bilinear pairings'," *International Journal of of Electronics and Information Engineering*, vol. 5, no. 1, pp. 30–36, 2016.

[21] L. H. Liu, Z. J. Cao, W. P. Kong, and J. B. Wang, "On bilinear groups of a large composite order," *International Journal of of Electronics and Information Engineering*, vol. 7, no. 1, pp. 1–9, 2017.

[22] C. Meshram, S. Meshram, and C. C. Lee, "Constructing provably secure id-based beta cryptographic scheme in random oracle," *International Journal of Network Security*, vol. 20, no. 3, pp. 568–574, 2018.

[23] V. Miller, "The weil pairing, and its efficient calculation," *Journal of Cryptology*, no. 17, p. 235261, 2004.

[24] J. Seo, T. Kobayashi, M. Ohkubo, and K. Suzuki, "Anonymous hierarchical identity-based encryption with constant size ciphertexts," in *Proceedings of Public Key Cryptography (PKC'09)*, pp. 215–234, Irvine, CA, USA, Mar. 2009.

[25] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proceedings of Annual Cryptology Conference, Advances in Cryptology (CRYPTO'84)*, pp. 47–53, Santa Barbara, California, USA, Aug. 1984.

[26] H. Q. Wang, "Insecurity of 'improved anonymous multi-receiver identity-based encryption'," *Computer Journal*, vol. 57, no. 4, pp. 636–638, 2014.

[27] J. Zhang and J. Mao, "Comment on anonymous multi-receiver identity-based encryption scheme," *International Journal of Communication Systems*, vol. 28, no. 4, pp. 645–658, 2012.

Biography

Lihua Liu is an associate professor with Department of Mathematics at Shanghai Maritime University. She received her Ph.D. degree in applied mathematics from Shanghai Jiao Tong University. Her research interests include combinatorics, cryptography and information security.

Zhenzhen Guo is currently pursuing her M.S. degree from Department of Mathematics, Shanghai Maritime university. Her research interests include combinatorics and cryptography.

Zhengjun Cao is an associate professor with Department of Mathematics at Shanghai University. He received his Ph.D. degree in applied mathematics from Academy of Mathematics and Systems Science, Chinese Academy of Sciences. He served as a post-doctor in Computer Sciences Department, Université Libre de Bruxelles, from 2008 to 2010. His research interests include cryptography, discrete logarithms and quantum computation.

Zhen Chen is currently pursuing his M.S. degree from Department of Mathematics, Shanghai University. His research interests include information security and cryptography.

Strategic Target Classification with Transfer Learning

Shoulin Yin, Jie Liu, and Lin Teng
(Corresponding author: Jie Liu)

Software College, Shenyang Normal University
Shenyang 110034, China
(Email: ljnan127@163.com)

(Received Mar. 27, 2018; revised and accepted June 12, 2018)

Abstract

Target classification plays an important in target detection, target recognition or target localization. Therefore, finding a common feature representation is crucial to tackle the problem of domain shift where the source domain and target domain have different distribution. Remote sensing technologies develop rapidly, the demand for rapid and accurate extraction of target is higher and higher, especially for military?targets. This paper proposes a transfer learning algorithm for strategic target classification. This work would fine tune a pre-trained network for a new recognition task with faster region convolutional neural network (Faster R-CNN). Then, transfer learning mechanism is adopted to transform the feature extraction in the faster R-CNN training process into strategic target classification. Meanwhile, images are labeled automatically according to the shape, size and texture. A very efficient GPU implementation of the convolution operation is used to make training faster. Finally, we make a model comparison on AlexNet, GoogleNet, and VGG.

Keywords: AlexNet; Faster Region Convolutional Neural Network; Target Classification; Transfer Learning

1 Introduction

Strategic target classification method usually needs to be given sufficient training samples to learn a prediction model, in which the training sample collection is a very important step[1]. And according to these new target classification task, training samples in the sample library is often outdated, they can not satisfy the requirement of the traditional machine learning theory with distribution hypothesis, namely the training sample and classification targets obey the same probability statistical distribution. However, due to the effect of background environment, traditional classification methods will not be able to carry out. It needs to label a large number of new samples in order to satisfy the demands of the current target classification training task [2-3]. Meanwhile, labeling new samples will cost a lot of manpower and material resources. That will seriously decrease the classification effectiveness.

Under the framework of traditional machine learning, the task of learning is to learn a classification model on the basis of given full training data. Then the learning model is used to classify and predict the test data sets. However, there is a key problem in machine learning algorithms that abundant training data is difficult to acquire. Traditional machine learning needs to label a large number of training data for every field, which will cost a lot of manpower and material resources. Without amounts of labeled data, this will not carry out related learning research and application. Additionally, traditional machine learning methods suppose that training data and testing data have the same data distribution, however, in many cases, the distribution hypothesis does not satisfy actual condition. If we re-label new data, it is very expensive.

Transfer Learning(TL) [4-6] goal aims to learn knowledge from an environment to help learning tasks in the new environment. Therefore, the TL cannot make distribution assuming as traditional machine learning. Currently, TL task can be divided into the following three parts: transfer learning with homogeneous space based on the instance; transfer learning with homogeneous space based on the feature; and transfer learning with heterogeneous space; According to researchers study, the first one has stronger knowledge transfer ability. The second one has broader knowledge transfer ability, and the third one has a comprehensive learning and extension ability.

TL can divide data set into source domain $S_D = (\alpha_s^i, \beta_s^i)_{i=1}^m$ and target domain $T_D = (\alpha_t^i, \beta_t^i)_{i=j+1}^n$ (in which includes training set $T_{D-Training}$ and testing set $T_{D-Testing}$). All the data have the same feature space. Namely, α can be described by the feature in the feature space. $T_{D-Training}$ is always acquired by manually labeled, and little $T_{D-Testing}$ data cannot select a better feature sub-set or train a well classifier. In S_D, though there are amount of labeled data, the different data distribution of S_D and T_D leads to a difficult classification. Goal of TL is from existing prior sample data to transfer knowledge. And it is without the traditional machine learning theory to train data and test data. So TL is used in the classification of the new image (target domain), which is suitable for remote sensing data classification and and updating task with dense time.

2 Proposed Method

Faster R-CNN was proposed by Ren in 2015 [7]. Object detection mainly contains four steps: candidate region generation, feature extraction, classification, location refinement in faster RCNN. They are finally unified into a deep network framework.

2.1 Structure of Region Proposal Network

A Region Proposal Network (RPN) [8] takes an image (of any size) as input and outputs a set of rectangular object proposals. With the extracted feature map, all possible candidate boxes are discriminating. The candidate box is relatively sparse due to the subsequent location refinement procedure. Structure of RPN is shown in Figure 1.

Raw feature extraction net includes several ”con+relu” layers. Feature can be seen as a channel image with scale of $51 * 39 * 256$. For each location of this image, it considers nine possible candidate windows (anchors). There are three scales in RPN: raw image scale, normalization scale and network input scale. ”cls+score” is classification layer and ”bbox+pred” is window regression layer.

2.2 Training for RPN

Considering each image in training set, it executes following procedures.

1) For every labeled candidate region of ground truth, the biggest overlap ratio of anchor is regarded as prospect sample;

2) For the rest anchors, if overlap ratio with one labeled region is greater than 0.7, it will be denoted as prospect sample. If it is smaller than 0.3, it will be as background sample.

3) Remove the anchors crossing image box.

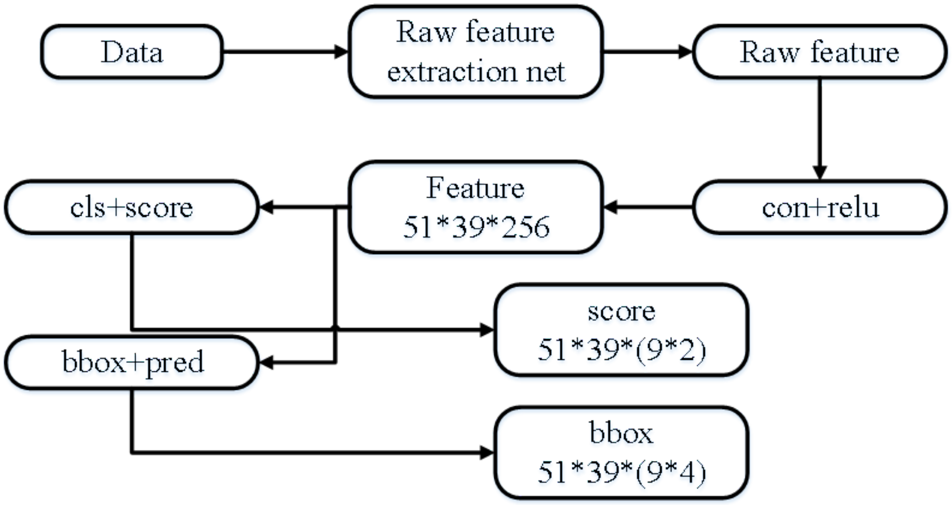


Figure 1: Structure of RPN

4) Repeat the above process.

2.3 Comparison of R-CNN, Fast R-CNN and Faster R-CNN

- R-CNN.

  1) Input test image;
  2) Use selective search method to choose approximately 2000 region proposals from up to down;
  3) Each region proposal will be warped as $227 * 227$ pixel and input CNN. The seventh layer in CNN is as output;
  4) The feature extracted by CNN is input SVM to classify;
  5) Classified region proposals are with bound box regression to generate the predicted window coordinates. Nevertheless, the processes are complex for fine tuning network, training SVM and training bounding box. Training is time consuming, which occupy large disk space; Namely, 5,000 images generate several hundred gigabytes of feature files. It needs 47s to process one image with GPU and VGG16. Each region proposal needs to run the whole feed-forward CNN;

- Fast R-CNN.

  1) Input test image;
  2) Use selective search method to choose approximately 2000 region proposals from up to down;
  3) CNN is used for feature extraction;
  4) Suggestion window is mapped to the last convolution layer feature map of CNN;
  5) Softmax Loss and Smooth L1 Loss are used for training classified probability and Bounding box regression;

Table 1: Image of each class

Class	Resolution	Negative number	Positive number
B52	0.5m	100	100
F15	0.5m	70	65
KC135	0.5m	255	255
CVN	0.5m	36	34
Destroyer	0.5m	196	204

Table 2: Size of each class

Class	B52	F15	KC135	CVN	Destroyer
Size	100 × 100	40 × 40	90 × 90	720 × 720	340 × 50

- Faster R-CNN.

  1) Input test image;
  2) CNN is used for feature extraction.
  3) 300 suggestion windows are produced by RPN.
  4) Suggestion window is mapped to the last convolution layer feature map of CNN.
  5) Each ROI has the same feature map through Roi pooling.
  6) Softmax Loss and Smooth L1 Loss are used for training classified probability and Bounding box regression.

From the above analysis, Faster R-CNN has the better effect.

3 Experiments and Results

In that military target data are difficult to acquire for target classification in remote sensing images, therefore, we downloaded 1315 images from Google Earth. And five target types are labeled including positive samples and negative samples among these images shown in Table 1 with the resolution for each class.

The total number of training images is 1315. There are two vital factors affecting the Faster RCNN training result: size and quality. Known to all, the sample size must be same as in Table 2. From these images, we augmented all the positive samples by translation, scale, and rotation transforms.

Figure 2 is the classification result. And Figure 3 is the training accuracy result. It can obtain the 100% training accuracy, because the sample data is pre-training with matlab platform. The sample number is very big. However, the classification result is better than other method.

We tested three types of models in this paper: AlexNet-finetune model, GoogleNet-finetune model, and VGG-finetune [9-12]. We set the learning rate to 0.01 and set the batch size to 256 for AlexNet, and 32 for GoogleNet, VGG16. The training process was performed using the open source Caffe framework and got the mini-batch comparison result as shown in Table 3.

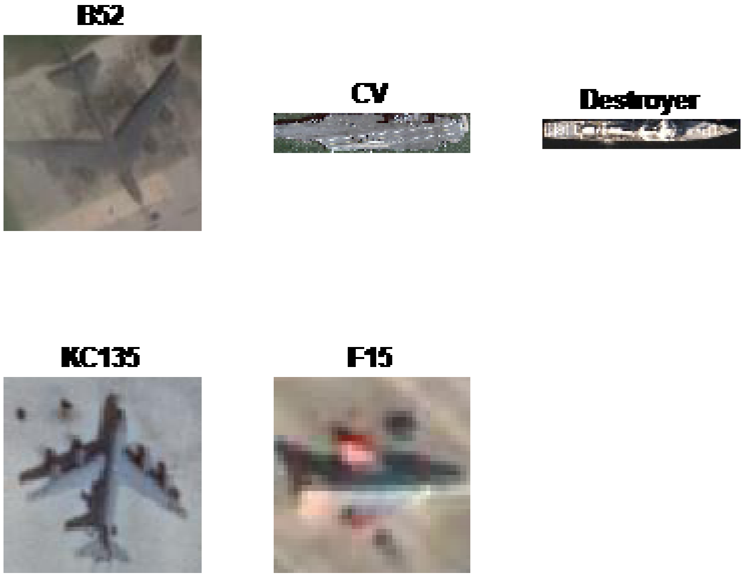


Figure 2: Classification result

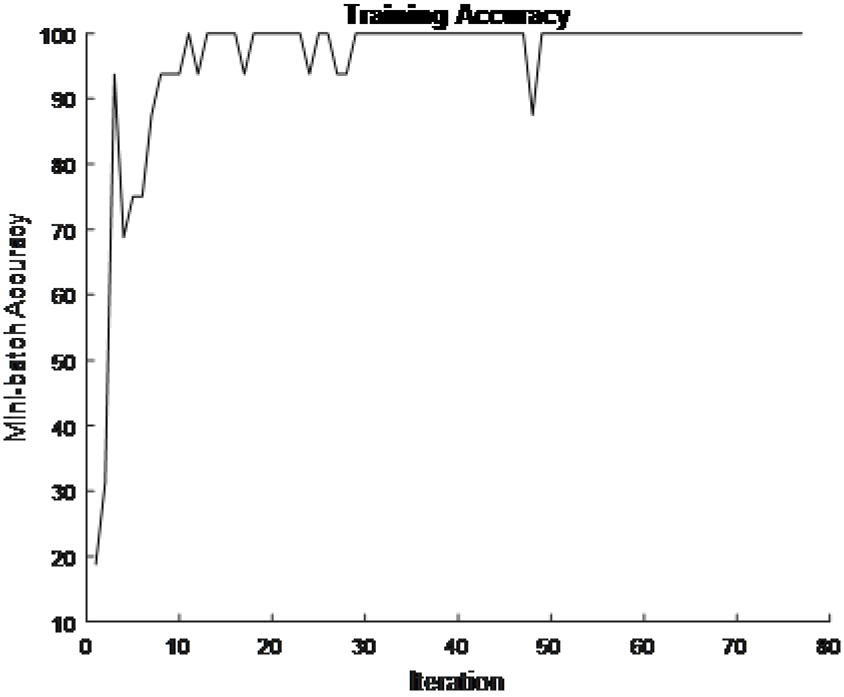


Figure 3: Training accuracy

Table 3: Mini-batch comparison

Model	Mini-batch loss	Mini-batch Accuracy
AlexNet-finetune	2.1284	18.75%
GoogleNet-finetune	2.2356	17.66%
VGG-finetune	2.4527	17.65%

Table 4: Results of ALEXNET+FASTER RCNN

Class	Recall	Precision
B52	0.9576	0.9511
F15	0.9174	0.8742
KC135	0.8659	0.8355
CVN	0.9438	0.9216
Destroyer	0.9157	0.8747

Known to all, CNN models need ample training data sets to learn the essential features of tasks. However, it involves a great deal of effort and time creating a large number of data set examples with labels. We use recall and precision to show the result with this paper's model. Table4 is the result, which shows that the proposed model has a better effect.

4 Conclusions

TIn this paper, we propose a transfer learning algorithm for strategic target classification. This work would fine tune a pre-trained network for a new recognition task with Faster R-CNN. Then, transfer learning mechanism is adopted to transform the feature extraction in the faster R-CNN training process into strategic target classification. Meanwhile, images are labeled automatically according to the shape, size and texture. In the further, the next work is that we will continue to enhance this framework and apply it into detection and localization works.

Acknowledgments

The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] H. Du, Z. Liu, H. Song, *et al.*, "Improving RGBD saliency detection using progressive region classification and saliency fusion," *IEEE Access*, PP(99): 1-1, 2016.

[2] M. M. Ghazi, B. Yanikoglu, E. Aptoula, "Plant identification using deep neural networks via optimization of transfer learning parameters," *Neurocomputing*, vol. 235, pp. 228–235, 2017.

[3] J. Long, E. Shelhamer, T. Darrell, "Fully convolutional networks for semantic segmentation," *IEEE Transactions on Pattern Analysis & Machine Intelligence*, vol. 39, no. 4, pp. 640, 2017.

[4] Y. Long, Y. Gong, Z. Xiao, *et al.*, "Accurate object localization in remote sensing images based on convolutional neural networks," *IEEE Transactions on Geoscience & Remote Sensing*, vol. 55, no. 5, pp. 2486–2498, 2017.

[5] G. K. Ouzounis, L. Gueguen, "Interactive collection of training samples from the Max-Tree structure," in *IEEE International Conference on Image Processing*, pp. 449–1452, 2011.

[6] P. Peng, T. Xiang, Y. Wang, *et al.*, "Unsupervised cross-dataset transfer learning for person reidentification," in *IEEE Computer Vision and Pattern Recognition*, pp. 1306–1315, 2016.

[7] S. Ren, K. He, R. Girshick, *et al.*, "Faster R-CNN: Towards real-time object detection with region proposal networks," in *International Conference on Neural Information Processing Systems*, MIT Press, pp. 91–99, 2015.

[8] D. Sarikaya, J. Corso, K. Guru, "Detection and localization of robotic tools in robot-assisted surgery videos using deep neural networks for region proposal and detection," *IEEE Transactions on Medical Imaging*, PP(99): 1-1, 2017.

[9] L. Teng, H. Li, S. Yin, "Modified pyramid dual tree direction filter-based image denoising via curvature scale and nonlocal mean multigrade remnant filter," *International Journal of Communication Systems*, 2017.

[10] M. Xie, N. Jean, M. Burke, *et al.*, "Transfer learning from deep features for remote sensing and poverty mapping," in *13th AAAI Conference on Artificial Intelligence*, pp. 3929–3935, 2016.

[11] S. Yin, Y. Zhang, S. Karim, "Large scale remote sensing image segmentation based on fuzzy region competition and Gaussian mixture model," in *IEEE Access*, vol. 6, pp. 26069–26080, 2018.

[12] B. Zoph, D. Yuret, J. May, *et al.*, "Transfer learning for low-resource neural machine translation," in *International Conference on Empirical Methods in Natural Language Processing*, pp. 1568–1575, 2016.

Biography

Shoulin Yin received the B.Eng. and M.Eng. degree from Shenyang Normal University, Shenyang , Liaoning province, China in 2016 and 2013 respectively. Now, he is a doctor in Harbin Institute of Technology. His interests are Network Security, image processing and Data Mining. Email:910675024@qq.com.

Jie Liu obtained his Ph.D. degree in Information Science and Engineering from Harbin Institute of Technology. Jie Liu is a full professor of the software college at Shenyang Normal University. His interests are wireless networks, mobile computing, cloud computing, social networks, network security and quantum cryptography. Prof. Liu had published more than 30 international journal and international conference papers on the above research fields. Email:ljnan127@163.com.

Lin Teng received the B.Eng. degree from Shenyang Normal University, Shenyang, Liaoning province, China in 2016. Now, she is a laboratory assistant in Shenyang Normal University. Her research interests include Multimedia Security, Network Security, Filter Algorithm and Data Mining. She had published more than 10 international journal papers on the above research fields. Email:1532554069@qq.com.

A Note on One Outsourcing Scheme for Big Data Access Control in Cloud

Lihua Liu[1], Zhengjun Cao[2], Chong Mao[2]
(Corresponding author: Zhengjun Cao)

Department of Mathematics, Shanghai Maritime University[1]
Haigang Ave 1550, Shanghai 201306, China[1]
Department of Mathematics, Shanghai University[2]
Shangda Road 99, Shanghai 200444, China[2]
(Email: caozhj@shu.edu.cn)

(Received May 21, 2018; revised and accepted July 8, 2018)

Abstract

We analyze Yang *et al.*'s outsourcing scheme [IEEE TPDS, 2015, 3461-3470] for big data access control in the cloud, and remark that the scheme is flawed because it brings the data owner a new challenge for protecting the session keys with more memory overhead. To the best of our knowledge, it is the first time to find such a shortcoming in outsourcing schemes.

Keywords: Access Matrix; Big Data Access Control; Cloud Computing; Embedding Degree; Weil Pairing

1 Introduction

Cloud computing benefits scientific and engineering applications such as computational financing, data mining, and many other data-intensive activities by supporting a paradigm shift from local to network-centric computing and network-centric content [22]. It enables customers with limited computational resources to outsource large-scale computational tasks to the cloud, and facilitates big data access control.

The problem of big data access control in the cloud is a hot topic. In 2016, Hsien *et al.* [10, 16, 17] presented three surveys of public auditing for secure data storage in cloud computing. In 2017, Chao *et al.* [8] put forth an improved key-management scheme for hierarchical access control.

Attribute-based encryption has attracted much attentions [1, 11–15, 23]. In 2015, Yang *et al.* [25] proposed a scheme for attribute-based access control with dynamic policy updating for big data. The scheme avoids the transfer of encrypted data back and forth between the data owner and the cloud server. It makes use of the previously encrypted data under old access policies, and enables the data owner to send only policy updating key to the cloud server. Upon receiving the updating key, the cloud server can directly update the policies of encrypted data without the need for decryption.

In this note, we would like to stress that Yang *et al.*'s scheme is unpractical because the data owner has to store session keys in local memory for the later updating when a message is encrypted and outsourced to the cloud. Concretely, the data owner has to generate and store more data in local memory which are to be kept confidentially when he wants to store securely a message in the cloud. To the best of our knowledge, it is the first time to find such a shortcoming in outsourcing schemes, which is different from the flaws found in [3–7, 18, 20, 21].

2 Preliminaries

Definition 1. *An elliptic curve E over a finite field $\mathbb{F}_q$ is defined by an equation $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, where $a_1, a_2, a_3, a_4, a_6 \in \mathbb{F}_q$ and $\triangle \neq 0$, $\triangle$ is the discriminant of E and is defined as follows: $\triangle = -d_2^2d_8 - 8d_4^3 - 27d_6^2 + 9d_2d_4d_6$, $d_2 = a_1^2 + 4a_2, d_4 = 2a_4 + a_1a_3, d_6 = a_3^2 + 4a_6, d_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$.*

If L is any extension field of $\mathbb{F}_q$, then the set of L-rational points on E is $E(L) = \{(x, y) \in L \times L : y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0\} \cup \{\infty\}$, where ∞ is the point at infinity.

The number of points in the group $E(\mathbb{F}_q)$, denoted by $\#E(\mathbb{F}_q)$, is called the order of E over $\mathbb{F}_q$.

Let n be a prime and coprime to the characteristic of $\mathbb{F}_q$. Suppose n divides $\#E(\mathbb{F}_q)$. Then there exists a n-torsion group $E(\mathbb{F}_{q^k})[n] := \{P \in E(\mathbb{F}_q^k) \mid nP = \mathcal{O}\}$, where the number k is called the *embedding degree* [9, 24], which is the smallest positive integer such that n divides $q^k - 1$, and nP denotes the sum of n copies of P.

Theorem 1. *(Balasubramanian and Koblitz [2]). Let E be an elliptic curve over $\mathbb{F}_q$ and n be a prime dividing $\#E(\mathbb{F}_q)$. Suppose that n does not divide $q-1$ and that $\gcd(n, q) = 1$. Then the n-torsion group $E[n] \subset E(\mathbb{F}_{q^k})$ if and only if n divides $q^k - 1$.*

The structure of n-torsion group $E(\mathbb{F}_{q^k})[n]$ is described by the following relation

$$E(\mathbb{F}_{q^k})[n] \cong (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}),$$

which means $\#E(\mathbb{F}_{q^k})[n] = n^2$. The Weil pairing is defined on the n-torsion group $E(\mathbb{F}_{q^k})[n]$, not on any n-order group $G \subset E(\mathbb{F}_q)$.

Let μ_n be the group of nth roots of unity. Clearly, $\mu_n \subset \mathbb{F}_{q^k}$, but $\mu_n \not\subset \mathbb{F}_{q^j}$ for $j = 1, \cdots, k-1$.

Definition 2. *The Weil pairing is a map $e_n : E(\mathbb{F}_{q^k})[n] \times E(\mathbb{F}_{q^k})[n] \to \mu_n$ with the following properties:*

1. *Linearity: If $P, Q, R \in E(\mathbb{F}_{q^k})[n]$, then*

$$e_n(P + Q, R) = e_n(P, R)e_n(Q, R),$$

$$e_n(P, Q + R) = e_n(P, Q)e_n(P, R).$$

2. *Alternating: If $P \in E(\mathbb{F}_{q^k})[n]$, then $e_n(P, P) = 1$. This, along with linearity, implies that if $P, Q \in E(\mathbb{F}_{q^k})[n]$, then $e_n(Q, P) = e_n(Q, P)^{-1}$.*

3. *Non-degeneracy: If $\mathcal{O} \neq P \in E(\mathbb{F}_{q^k})[n]$, there exists $Q \in E(\mathbb{F}_{q^k})[n]$ such that $e_n(P, Q) \neq 1$.*

Most literatures use the notation $E[n]$ to denote the n-torsion group [19], which does not specify that the representation of points, the computation of functions, and the evaluation of functions related to Weil/Tate pairings, should be performed in the extension field $\mathbb{F}_{q^k}$, instead of the base field $\mathbb{F}_q$.

3 Review of Yang *et al.*'s Scheme

The scheme [25] involves the following entities: authorities, cloud server, data owners and data consumers. Every authority is responsible for managing attributes of users in its domain and generating a public/secret key pair for each attribute and a secret key for each user according to his attributes. The cloud server stores the data for data owners and provides data access service to users.

The data owners define access policies and encrypt data under these policies. Each user is assigned with a global user identity and can freely get the ciphertexts from the server. The user can decrypt a ciphertext only when its attributes satisfy the access policy defined in the ciphertext.

The scheme consists of the following phases.

GlobalSetup. Set the global parameters as $(p, g, e, \mathbb{G}, \mathbb{G}_T, H)$, where $\mathbb{G}$ and $\mathbb{G}_T$ are two multiplicative groups with prime order p, g is a generator of $\mathbb{G}$,

$$e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$$

is a bilinear map, and H is a random oracle which maps global identities GID to elements of $\mathbb{G}$.

AuthoritySetup. Let S_{AID} denote the set of all the attributes managed by the authority AID. For each attribute $x \in S_{AID}$, the authority chooses two random exponents $\alpha_x, \beta_x \in \mathbb{Z}_p$ and publishes its public key as

$$PK_{AID} = \{e(g,g)^{\alpha_x}, g^{\beta_x}\}_{\forall x \in S_{AID}}.$$

Keep $SK_{AID} = \{\alpha_x, \beta_x\}_{\forall x \in S_{AID}}$ in secret.

KeyGeneration. For each user GID, each authority AID assigns a set of attributes $S_{GID,AID}$ to this user and generates the secret key

$$SK_{GID,AID} = \{K_{x,GID} = g^{\alpha_x} H(GID)^{\beta_x}\}_{\forall x \in S_{GID,AID}}.$$

Encryption. For the message m, a set of public keys $\{PK\}$ and an $n \times l$ access matrix M with ρ mapping its rows to attributes, the data owner picks

$$\overrightarrow{v} = (s, y_2, \cdots, y_l) \in \mathbb{Z}_p^l,$$

$$\overrightarrow{w} = (0, z_2, \cdots, z_l) \in \mathbb{Z}_p^l,$$

$$\overrightarrow{r} = (r_1, r_2, \cdots, r_n) \in \mathbb{Z}_p^n,$$

and computes $\lambda_i = M_i \overrightarrow{v}^T, w_i = M_i \overrightarrow{w}^T, i = 1, \cdots, n$, where M_i is the vector corresponding to the ith row of M. Set the ciphertext $\mathbf{CT}$ as

$$C = m \cdot e(g,g)^s, \ C_{1,i} = e(g,g)^{\lambda_i} e(g,g)^{\alpha_{\rho(i)} r_i},$$
$$C_{2,i} = g^{r_i}, \ C_{3,i} = g^{\beta_{\rho(i)} r_i} g^{w_i}$$

where $i = 1, \cdots, n$. Store $\mathbf{CT}, M, \rho$ and $\overrightarrow{r}$ in the cloud (r will be invoked in the later updating phase).

◇ *Notice that encrypting two different message $m, \hat{m}$ with the same session key s is insecure.*

DataDecryption. Given $\mathbf{CT}, M, \rho$, the user, equipped with secret keys $\{K_{\rho(i),GID}\}$ for a subset of rows i of M such that $(1, 0, \cdots, 0)$ is in the span of these rows, computes

$$\frac{C_{1,i} \cdot e(H(GID), C_{3,i})}{e(K_{\rho(i),GID}, C_{2,i})} = e(g,g)^{\lambda_i} e(H(GID), g)^{w_i}$$

for each such i. The user then chooses $c_i \in \mathbb{Z}_p$ such that $\sum_i c_i M_i = (1, 0, \cdots, 0)$ and computes

$$\prod_i \left(e(g,g)^{\lambda_i} e(H(GID), g)^{w_i}\right)^{c_i} = e(g,g)^s,$$
$$m = C/e(g,g)^s.$$

PolicyUpdating. If the data owner wants to update the ciphertext $\{\mathbf{CT}, M, \rho, \overrightarrow{r}\}$ from the previous access policy $\mathbb{A}$ to the new access policy $\mathbb{A}'$, he generates an update key UK_m and sends it to the cloud server. The server then runs the ciphertext updating algorithm to update the ciphertext. We refer to the original description [25] for different cases (updating a Boolean formula, or a LSSS structure, or a threshold gate).

4 Analysis of Yang *et al.*'s Scheme

Suppose that E is the underlying elliptic curve over the finite field $\mathbb{F}_q$, the message m must be in the set $\mathbb{G}_T \subset \mathbb{F}_{q^k}$, where $\mathbb{G}_T$ is the group of pth roots of unity and the positive integer k is the embedding degree. Therefore, the message is eventually expressed as

$$m = (m_1, \cdots, m_k) \in \mathbb{F}_q^k.$$

Yang *et al.*'s scheme specifies three DynamicPolicyUpdating cases.

1) In the case of updating a Boolean formula (see Section 4.1.2 [25]), the data owner has to randomly pick $a_m, \lambda', w', r_{n+1} \in \mathbb{Z}_p$ such that

$$\lambda'_j = \lambda_j + \lambda', \ \lambda_{n+1} = a_m \cdot \lambda',$$
$$w'_j = w_j + w', \ w_{n+1} = a_m \cdot w',$$

where $\lambda_i = M_i \overrightarrow{v}^T, w_i = M_i \overrightarrow{w}^T, i = 1, \cdots, n$, and M_i is the vector corresponding to the ith row of M.

2) In the case of updating a LSSS structure (see Section 4.2.1 [25]), the data owner has to randomly pick

$$\overrightarrow{v}' = (s, y'_2, \cdots, y'_{l'}) \in \mathbb{Z}_p^{l'},$$
$$\overrightarrow{w}' = (0, z'_2, \cdots, z'_{l'}) \in \mathbb{Z}_p^{l'}$$

and compute

$$\lambda_i = M_i \overrightarrow{v}^T, \ w_i = M_i \overrightarrow{w}^T,$$
$$\lambda'_i = M'_i \overrightarrow{v'}^T, \ w'_i = M'_i \overrightarrow{w'}^T.$$

3) In the case of updating a threshold gate (see Section 4.3 [25]), the data owner has to transform the threshold gate into a LSSS structure and apply the above method of updating a LSSS structure.

Apparently, in all cases *the data owner has to invoke the session key* $\overrightarrow{v}$.

Since $C = m \cdot e(g,g)^s$ where m is the message to be encrypted and $e(g,g)$ is a global public parameter, the session key

$$\overrightarrow{v} = (s, y_2, \cdots, y_l) \in \mathbb{Z}_p^l$$

Table 1: Outsourced data versus incurred data

Outsourced data	message	$m = (m_1, \cdots, m_k) \in \mathbb{F}_q^k, \ \ k \leq 6$
Incurred data	session key	$\overrightarrow{v} = (s, y_2, \cdots, y_l) \in \mathbb{Z}_p^l, \ \ l = (t-1)C_n^t + 1$

must be kept in secret. If the session key $\overrightarrow{v}$ is encrypted and outsourced to the cloud, then it leads to a vicious circle. Thus, the data owner has to store $\overrightarrow{v} = (s, y_2, \cdots, y_l) \in \mathbb{Z}_p^l$ in local memory. See Table 1 for the comparisons between outsourced data and locally generated and stored data.

To avoid the Weil and Tate pairing attacks [9], one should ensure that the size of p is approximately equal to the size of q. So, we assume that both p and q are of ψ bits.

To facilitate the computation of pairings, one should ensure that $k \leq 6$. Thus, the binary length of m is not greater than 6ψ while the binary length of $\overrightarrow{v}$ is $l\psi$. Notice that $l = (t-1)C_n^t + 1$ where t is the threshold value and n is the size of the set of attributes (see Page 3467 [25]).

In general, we have $l > 6$. That means the data owner has to store more data in local memory when he wants to store securely a message in the cloud. Thus, the scheme does risk big things for the sake of small ones. To the best of our knowledge, it is the first time to find such a shortcoming in outsourcing schemes.

5 Conclusion

We show that Yang *et al.*'s scheme is unpractical because it brings the data owner a new challenge for protecting the session keys with more memory overhead. We would like to stress that the structure of group $\mathbb{G}_T$ is still unfamiliar to some researchers, which leads to such an unreasonable scheme. In the scenario of cloud computing one should carefully balance the data storage requirement for the outsourced data and that for the locally stored data.

Acknowledgements

We thank the National Natural Science Foundation of China (61303200, 61411146001). We are grateful to the reviewers for their valuable suggestions.

References

[1] N. Attrapadung and *et al.*, "Attribute-based encryption schemes with constant-size ciphertexts," *Theoritical Computer Science*, no. 422, pp. 15–38, 2012.

[2] R. Balasubramanian and N. Koblitz, "The improbability that an elliptic curve has sub-exponential discrete log problem under the menezes-okamoto-vanstone algorithm," *Journal of Cryptology*, no. 11, pp. 141–145, 1998.

[3] Z. J. Cao and L. H. Liu, "Comment on 'harnessing the cloud for securely outsourcing large-scale systems of linear equations'," *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 5, pp. 1551–1552, 2016.

[4] Z. J. Cao and L. H. Liu, "A note on two schemes for secure outsourcing of linear programming," *International Journal of Network Security*, vol. 19, no. 2, pp. 323–326, 2017.

[5] Z. J. Cao, L. H. Liu, and O. Markowitch, "Analysis of one scheme for enabling cloud storage auditing with verifible outsourcing of key updates," *International Journal of Network Security*, vol. 19, no. 6, pp. 950–954, 2017.

[6] Z. J. Cao, L. H. Liu, and O. Markowitch, "Comment on 'highly efficient linear regression outsourcing to a cloud'," *IEEE Transactions on Cloud Computing (10.1109/TCC.2017.2709299)*, 2017.

[7] Z. J. Cao, C. Mao, and L. H. Liu, "Analysis of one secure anti-collusion data sharing scheme for dynamic groups in the cloud," *International Journal of of Electronics and Information Engineering*, vol. 5, no. 2, pp. 65–68, 2016.

[8] W. Y. Chao, C. Y. Tsai, and M. S. Hwang, "An improved key-management scheme for hierarchical access control," *International Journal of Network Security*, vol. 19, no. 4, pp. 639–643, 2017.

[9] D. Hankerson, A. Menezes, and S. Vanstone, *Guide to Elliptic Curve Cryptography.* USA: Springer-Verlag, 2004.

[10] W. F. Hsien, C. C. Yang, and M. S. Hwang, "A survey of public auditing for secure data storage in cloud computing," *International Journal of Network Security*, vol. 18, no. 1, pp. 133–142, 2016.

[11] A. Lewko, A. Sahai, and B. Waters, "Revocation systems with very small private keys," in *Proceedings of 2010 IEEE Symposium on Security and Privacy*, pp. 273–285, Claremont Resort, Berkeley, CA., May 2010.

[12] A. Lewko and *et al.*, "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption," in *Proceedings of the 29th Annual Eurocrypt Conference (EUROCRYPT 2010)*, pp. 62–91, Monaco and Nice, French Riviera, June 2010.

[13] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in *Proceedings of the 30th Annual Eurocrypt Conference (EUROCRYPT 2011)*, pp. 568–588, Tallinn, Estonia, May 2011.

[14] A. Lewko and B. Waters, "Unbounded hibe and attribute-based encryption," in *Proceedings of the 30th Annual Eurocrypt Conference (EUROCRYPT 2011)*, pp. 547–567, Tallinn, Estonia, May 2011.

[15] A. Lewko and B. Waters, "New proof methods for attribute-based encryption: Achieving full security through selective techniques," in *Proceedings of the 32nd International Cryptology Conference (CRYPTO 2012)*, pp. 180–198, University of California, Santa Barbara, August 2012.

[16] C. W. Liu, W. F. Hsien, C. C. Yang, and M. S. Hwang, "A survey of attribute-based access control with user revocation in cloud data storage," *International Journal of Network Security*, vol. 18, no. 5, pp. 900–916, 2016.

[17] C. W. Liu, W. F. Hsien, C. C. Yang, and M. S. Hwang, "A survey of public auditing for shared data storage with user revocation in cloud computing," *International Journal of Network Security*, vol. 18, no. 4, pp. 650–666, 2016.

[18] L. H. Liu and Z. J. Cao, "A note on 'efficient algorithms for secure outsourcing of bilinear pairings'," *International Journal of of Electronics and Information Engineering*, vol. 5, no. 1, pp. 30–36, 2016.

[19] L. H. Liu, Z. J. Cao, W. P. Kong, and J. B. Wang, "On bilinear groups of a large composite order," *International Journal of of Electronics and Information Engineering*, vol. 7, no. 1, pp. 1–9, 2017.

[20] L. H. Liu, Z. J. Cao, C. Mao, and J. B. Wang, "Computational error analysis of two schemes for outsourcing matrix computations," *International Journal of Electronics and Information Engineering*, vol. 7, no. 1, pp. 23–31, 2017.

[21] L. H. Liu, W. P. Kong, Z. J. Cao, and J. B. Wang, "Analysis of one certificateless encryption for secure data sharing in public clouds," *International Journal of Electronics and Information Engineering*, vol. 6, no. 2, pp. 108–113, 2017.

[22] D. Marinescu, *Cloud Computing Theory and Practice.* USA: Elsevier, 2013.

[23] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proceedings of the 24th Annual Eurocrypt Conference (EUROCRYPT 2005)*, pp. 457–473, Aarhus, Denmark, May 2005.

[24] J. Silverman, *The Arithmetic of Elliptic Curves*. USA: Springer-Verlag, 1986.

[25] K. Yang, X. H. Jia, and K. Ren, "Secure and verifiable policy update outsourcing for big data access control in the cloud," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 12, pp. 3461–3470, 2015.

Biography

Lihua Liu is an associate professor with Department of Mathematics at Shanghai Maritime University. She received her Ph.D. degree in applied mathematics from Shanghai Jiao Tong University. Her research interests include combinatorics, cryptography and information security.

Zhengjun Cao is an associate professor with Department of Mathematics at Shanghai University. He received his Ph.D. degree in applied mathematics from Academy of Mathematics and Systems Science, Chinese Academy of Sciences. He served as a post-doctor in Computer Sciences Department, Université Libre de Bruxelles, from 2008 to 2010. His research interests include cryptography, discrete logarithms and quantum computation.

Chong Mao is currently pursuing his M.S. degree from Department of Mathematics, Shanghai University. His research interests include information security and cryptography.

Cryptanalysis of Knapsack Cipher Using Genetic Swarm Optimization

Anto Merline M and Vimalathithan Rathinasabapathy

(Corresponding author: Anto Merline M)

Department of Electronics and Communication Engineering, Karpagam College of Engineering
Coimbatore, Tamil Nadu 641032, India
(Email: merlinemanoharan@gmail.com)

(Received Apr. 12, 2018; revised and accepted June 20, 2018)

Abstract

Cryptanalysis is a baffling problem in cryptography. Knapsack problem was one of the NP complete problems, to break the knapsack cipher it is necessary to solve this instance of the knapsack problem, which is hard of course, instead Computational Intelligence can solve the problem easily. In this paper, a newer technique called Genetic Swarm Optimization (GSO) in attacking the Knapsack cipher is proposed. This Combined technique combine the goodness of Genetic Algorithm (GA) and Particle Swarm Optimization (PSO) is used in the field of cryptanalysis in attacking Knapsack Ciphers and thereby reductive the search space by an order of '1.8' and '1.6' when compared to GA and PSO respectively. GSO is put-upon for the first in the field of public key cryptanalysis.

Keywords: Cryptanalysis; Genetic Algorithm; Particle Swarm Optimization; Genetic Swarm Optimization; Fitness

1 Introduction

Cryptography is a science of protecting the information into an unreadable format (ciphertext) and method of transmitting the same in a form that can be read and processed by only by the intended users. The Encryption is the process of making the information into an unreadable format and the reverse of that is called decryption. Cryptanalysis is a mathematical technique which is used to break cryptographic algorithms and attack the encrypted text, without having the secret key [1,11,23]. Cryptography is the art of making encrypted text while Cryptanalysis is the art of breaking that encrypted text. Nowadays Computational Intelligence (CI) finds lot of interest in a cryptanalysis of ciphers.

CI is the study of adaptive mechanisms that enable savvy behavior of a system in convoluted and dynamic environs like Genetic Algorithms (GA) and Particle Swarm Optimization (PSO) [15,16]. A population based optimization algorithms like GA and PSO can be used to solve optimization problems. The basic difference between GA and PSO: Crossover and Mutation operations present in GA which is not in PSO but it contains fast Convergence which is the main strength of PSO, compares favorably with global optimization algorithm like GA. The Similarity between these two algorithms: Both are initializing a population and evaluate a fitness function in identical way. At last both are generational. The advantage of both GA and PSO were combined to form a new evolutionary algorithm known as Genetic Swarm Optimization (GSO) is proposed in the field of cryptanalysis. The hybrid GSO algorithm is developed to mitigate the premature convergence problem in Cryptanalysis. Jain and Chaudiri demonstrated the improved knapsack cipher proposed by Pham prevents brute force attack [7]. Rajaram Ramasamy et.al proposed a new digital signature scheme with message recovery using knapsack based ECC [18]. Zhengping Jin used known message attack, and showed that Su and Tsai's encryption scheme doesn't provide confidentiality [8]. Rajaram Ramasamy proposed ECC and knapsack to generate the signature thereby claiming that the scheme is more secure against current attacking mechanisms [19].

Different Cryptanalysis researches have been carried out in attacking the knapsack cipher using Evolutionary Algorithms (EA) like GA, PSO, and hill climbing. But very few reports have been reported on combining the EA. Spillman (1993), for the first time presented a GA technique for the cryptanalysis of knapsack cipher [22]. This paper has gives the possible ways of discovering the key for a Knapsack cipher. The comments by Frank(1994) on [22] says that , if the problem size increases GA may decrease the portion of the search space and suspects that the search time may increases exponentially [2]. Garg, Aditya, Agarwal (2007) used Genetic algorithm to attack knapsack ciphers [3]. Their result says that by properly selecting the initial parameters of GA, the performance of GA can be improved when compared to [22]. Raghavan, Divya, and Parthiban (2009) used parallel Evolutionary computing to break Knapsack Cipher [17]. As already reported that very few research works carried out by combining the EA. This paper is the one that combines the Evolutionary algorithms, hill climbing and GA. Hill climbing works mainly on the mutation. If crossover operator is combined with Hill climbing then the algorithm is equivalent to GA. Also from the results, there is no improvement in key search space. Mayada, Baraa, Sarab (2008) used Binary PSO for attacking the knapsack ciphers [12]. From their result, PSO has effectively reduced the search space in attacking the knapsack ciphers when compared to GA. Supravo Saptarshi, Mostafiz, Atreyee, Malay (2011) used Binary Firefly algorithm (FA) in attacking the Knapsack cipher and their results say that algorithm perform better when compared to GA [24]. Firefly algorithm may trap into local optima and they do not change with time. Also they do not keep the track of its previous better solution [21].

Vimalathithan and Valarmathi [25, 26] applied GSO in the field of cryptanalysis and succeeded in breaking symmetrically encrypted S-DES ciphers and DES ciphers. Ashish Jain [7] identifies and characterizes the practical knapsack cipher 0/f requirement and also they demonstrate that the computational complexity of the knapsack cipher 0/f and knapsack cipher 0/1 is equal. In this paper, GSO (which combines the advantages of GA and PSO) is applied to cryptanalyst the Knapsack cipher (asymmetric encryption) and our result says that GSO is meliorated than GA and PSO and it is an effective tool which can be used in the field of public key cryptanalysis. The GSO reduces the search space at least by the order of '1.8' and '1.6' when compared to GA and PSO respectively.

The remaining part of the paper is organized as follows: Section 2 gives the brief overview about Knapsack crypto system and section 3 describes about Computational Intelligence. Section 4 describes about how fitness function calculated and how to cryptanalysis the knapsack cipher by using CI. Section 5 gives the Experimental results and at last Section 6 concludes the research work.

2 Basics of Knapsack Cipher

This subsection defines Knapsack problem. Suppose two k-tuples, $a = [a_1, a_2, \cdots, a_k]$ and $x = [x_1, x_2, \cdots, x_k]$ are given, the first tuple is the predefined set and the second tuple x_i takes either 0 or 1 only. The sum of elements in the knapsack is given by

$$s = knapsackSum(a, x) = x_1a_1 + x_2a_2 + \cdots + x_ka_k. \tag{1}$$

If 'a' and 'x' are known then it is easy to calculate s, instead, if 's' and 'a' are known then it is difficult to compute 'x'. The function knapsackSum is a one-way function if 'a' general k-tuple. But it is easy to compute knapsackSum and inv_knapsackSum if the k-tuple is super increasing. Such that

$a_i \geq a_1 + a_2 + \cdots + a_i - 1$ is known as super increasing tuple. In other words, each element (except a_1) is greater than or equal to the sum of a_{ll} previous elements. The super increasing knapsack can be easily recovered and thereby the security to the message is very low. If the super increasing knapsack is known, then the bit pattern thereby the message can be easily recovered. Instead of using super increasing knapsack, Merkle and Hellman proposed an idea of Trapdoor knapsack which is hard to break [13]. Algorithms 1, 2, 3 show the algorithm for key generation and encryption/decryption using Knapsack cryptosystem.

Algorithm 1 Knapsack cipher algorithm: Key Generation

```
Super increasing: K-tuple $b = [b_1, b_2, \cdots, b_k]$ is created.
Choose a modulus $n$, such that $n > b_1 + b_2 + \cdots + b_k$;
Select a random integer $r$ that is relatively prime with $n$ and $1 \leq r \leq n - 1$;
Create a temporary k-tuple $t = [t_1, t_2, \cdots, t_k]$ in which $t_i = r.b_i \bmod n$.
Select a permutation of $k$ objects and find a new tuple $a =$ permute $(t)$;
Public key: (k-tuple a.); Private key: $(n, r, k - tupleb)$.
```

Algorithm 2 Knapsack cipher algorithm: Encryption

```
Converts the message to a k-tuple $x = [x_1, x_2, \cdots, x_k]$ in which $x_i$ is either 0 or 1. The tuple $x$ is the plaintext.
Use the knapsackSum routine to calculate $s$.
Display's' as ciphertext.
```

Algorithm 3 Knapsack cipher algorithm: Decryption

```
Receive the ciphertext $s$;
Find $s` = (r - 1.s) \bmod n$;
Use inv_knapsackSum to create $x'$. Permute $x'$ to find $x$. The tuple $x$ is the recovered plaintext.
```

3 Computational Intelligence

The Cryptanalysis techniques such as GA, PSO and GSO are briefly explained in this section.

3.1 Genetic Algorithm

GA mimics biological evolution to solve constrained as well as unconstrained problems. A simple genetic algorithm represent savvy development of random search that yield good results in optimization of real problems.GA uses three operators namely: Selection (Reproduction), Crossover and Mutation [5,6,14, 20]. To optimize a given problem GA takes a set called chromosomes and a metric unit called fitness function which allows each chromosome to be quantitatively evaluated. The set of chromosomes is called population. Fitness value is computed for each chromosome. Based on these values chromosomes are selected for a subsequent process. Once the chromosomes are selected crossover is applied which selects and create new offspring. Mutation is performed after crossover where one or more bits in the chromosome are changed randomly. In each generation GA produces a new set of possible solutions for a given problem. The algorithm is continued till optimum solution is found.

3.2 Particle Swarm Optimization

Swarm Intelligence is a path breaking paradigm used for solving the perplex problems. PSO is a population based optimization tool which could be implemented in cryptanalysis. For continuous variable optimization problems canonical PSO may be applied. Since the cryptographic operation used in our case is processed '0's and '1's, the canonical PSO cannot be applied directly. In case of Binary PSO, the particle position takes either '0's or '1's but the real value as in case of canonical PSO. Hence Binary PSO is preferred. In the Binary PSO particle's position and velocity in terms of changes of probabilities that will be in one state or the other are defined [9, 10]. The binary swarms are initialized with an initial population of random candidates. The particles move iteratively through the d-dimension problem space to hunt the new solutions where the fitness is be compute as the quality measure. Each particle has a position-vector x_i (i is the index of the particle)and velocity vector v_i. Each particle commemorates its own fess position so far in the vector $x_i^{\#}$ (p_{best}) and its j-th dimensional value is $x_{ij}^{\#}$. The sample position vector among the swarm so far is then stored in a vector $x*$ (g_{best}) and its j-th dimensional value is x_j*. Previous velocity ($v_{ij}(t)$) is which is updated to the new velocity ($v_{ij}(t+1)$) for each iteration. Particles updates its velocity and moves to a new position according to the Equations (2) and (3):

$$\begin{aligned} v_{ij}(t+1) &= w.v_{ij}(t) + c_1r_1(x_{ij}^{\#}(t) - x_{ij}(t)) + c_2r_2(x_j*(t) - x_{ij}(t)) && (2)\\ x_i(t+1) &= 1 \text{ if } \rho \leq S(v_i(t)), \\ &= 0 \text{ otherwise.} && (3) \end{aligned}$$

Where 'w' is the inertia factor, r_1 and r_2 are the random numbers, uniformly distributed in the interval [0, 1]. r_1 and r_2 are used to exert the diversity of the population for the jth dimension of the ith particle. It is used maintain the population diversity. c_1 and c_2 are called as coefficient of the self-recognition component, social component respectively. 'ρ' is a random function in the closed interval [0, 1], and the $S(V_i(t))$ is given by

$$S(V_i(t)) = \frac{1}{1+e^{-V_i}}. \quad (4)$$

3.3 Genetic Swarm Optimization

Genetic Swarm Optimization is an optimization technique which is used to cryptanalysis the knapsack problem. It is the combination of vantages characteristics of both GA and PSO technique. GSO maintains the cooperation between GA and PSO. The effectiveness and efficiency of GSO is higher than the GA and PSO technique because it having the combination effectiveness and advantage of both of the algorithms.

The working principle of GSO is given: In this first the selection of population process is carried out from the given problem. It uses fitness function as a main parameter to find the optimal solution to break the knapsack cipher. After the population selection, the population is split into two parts according to the parameter known as hybrid coefficient h_{coeff}. This parameter determines the percentage of the total population to be processed by GA and the remaining $(1 - h_{coeff})$ percentage of the total population is to be processed by PSO. For example, if $h_{coeff} = 0$, then the algorithm becomes purely PSO because the whole population is processed by PSO operators and if $h_{coeff} = 1$, then the algorithm becomes purely GA because the whole population is processed by GA operators. The criteria for h_{coeff} is $0 < h_{coeff} < 1$. The rudiments of GSO can be found in [4, 25]. According to h_{coeff} the population is processed by GA and PSO and the fitness function is calculated. The population undergoes many numbers of iterations until the optimum solution is finding. After each iteration the population is recombined to form a new population which is again split into two parts according to h_{coeff}. The process flowchart of GSO operation is shown in Fig.1. The hybrid coefficient may be static or dynamic. If it is static, h_{coeff} is constant for all iterations. If it is dynamic, h_{coeff} takes random values for each iteration. The iterations continue until optimum solution is obtained.

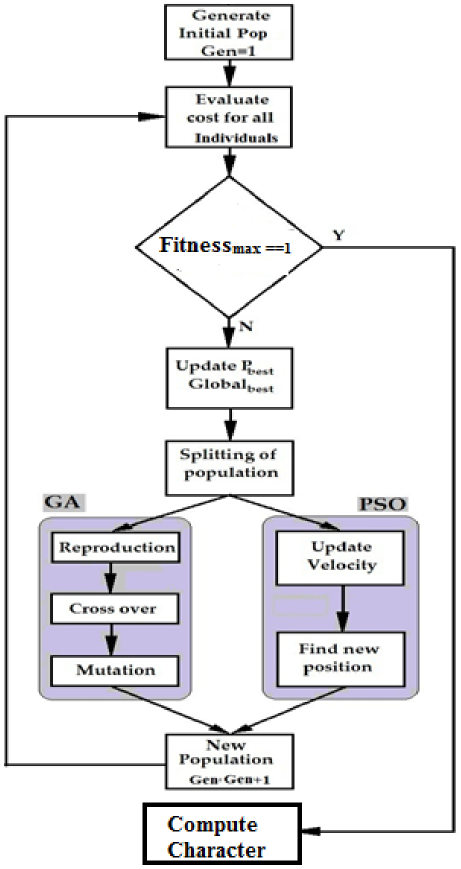


Figure 1: A GSO cycle for breaking Knapsack cipher

4 Attacking Knapsack Cipher Using GSO

The fitness function is to be defined in order to evaluate the performance of GSO,. We use the fitness function used by Spillman [22]. The fitness function illustrated in Equation (8) is used to evaluated each particle i. Let $M = \{m_1, m_2, \cdots, m_n\}$, $m_i \in \{0, 1\}$ be n arbitrary solution and the public key

$A = \{a_1, a_2, \cdots, a_n\}$, then

$$\begin{aligned} Sum &= \sum_{j=1}^{n} a_j m_j & (5) \\ Target &= \sum_{j} a_j & (6) \\ Full\ Sum &= \sum_{j=1}^{n} a_j. & (7) \end{aligned}$$

Where Full sum is the sum of the components in Knapsack and Target is the sum of particular components in the Knapsack.

$$\begin{aligned} Maxdiff &= \max(Target, Full\ Sum - Target) \\ Fitness &= 1 - \sqrt{(}|Sum - Target|/Target)\text{If Sum} \leq \text{Target} \\ Fitness &= 1 - 6^{th\ root}(|Sum - Target|/Maxdiff)\text{otherwise} & (8) \end{aligned}$$

The fitness function takes the value in the range (0, 1). The goal is to maximize the fitness function. Next we describe our proposed research approach, how to attack Knapsack cipher using our algorithm. In order to combine the GA and PSO, initialize the parameters for GA and PSO. Also initialize the hybrid coefficient for GSO. Generate the initial population randomly, fitness value for the entire population has to be compute and check for the fitness value. Here we take $h_{coeff} = 0.3$; i.e., GA processed 30% of the population and PSO processed the remaining 70% of the population to generate new population. Figure 1 shows how the Key is computed in each generation. The evolution process is continued using GSO algorithm until the essential criteria are met. The algorithm is shown in Algorithm 4.

Algorithm 4 Algorithm for attacking knapsack cipher

```
1: Initialize POPGSO Randomly;
2: Select $h_{coeff}$: i.e., Static or Dynamic
3: If Static:
4:     Case 1: $h_{coeff}(k) = 0$ for all $k$;
5:     Case 2: $h_{coeff}(k) = 0.2$ for all $k$;
6:     Case 3: $h_{coeff}(k) = 0.3$ for all $k$;
7:     Case 4: $h_{coeff}(k) = 1.0$ for all $k$.
8: If dynamic: $h_{coeff}(k) = rand()$
9: $POP_{GA} = h_{coeff}(k) \times P_{GSO}$ individuals for GA;
10: $POP_{PSO} = h_{coeff}(k) \times POP_{GSO}$ individuals for PSO;
11: For $POP_{GA}$: Generate new population by Applying GA;
12: For $POP_{PSO}$: Generate new population by applying PSO;
13: Update New population: $POP_{GSO} = POP_{GA} + POP_{PSO}$;
14: Compute the fitness for POPGSO;
15: Check for Fitness == 1: Repeat Steps 2-13 until Fitness takes Unity.
16: if fitness=1 is met then
17:     convert the corresponding bit pattern to ASCII character. Repeat Steps 1-15 until all the characters were recovered.
18: end if
19: End
```

5 Experimental Setup and Results

The effectiveness of our GSO algorithm should be verified therefore, we implemented the algorithm using Matlab 7.5 in an Intel Corei5 (2.4GHz) System.

The easy knapsack used is (1, 3, 7, 13, 26, 65, 119, 267), *i.e.*, the super increasing tuple b. The parameters 'n' and 'r' takes the value 65423 and 21031 respectively. Using these values the tuple 'a' is computed and it is given by (21031, 63093, 16371, 23422, 16615, 54322). Here we considered the messages "MACRO' and 'CRYPTO', it is encrypted using the Knapsack encryption algorithm. The Knapsack cipher for the message considered is given in Table 1.

In order to break the knapsack cipher, GSO parameters is to be initialized where initial settings for GA and PSO parameters were shown in Table 2. 10 is the population size taken for the experiment and the number of generation is set to 10 so that the total search space is restricted to 100.

Table 1: Knapsack cipher for the messages

Message	Cipher Target Sum	Message	Cipher Target Sum
M	65728	C	100739
A	37646	R	103130
C	10739	Y	72779
R	103130	P	40037
O	128821	T	56408

Table 2: GA and PSO parameters for GSO GA parameters PSO parameters

GA parameters	PSO parameters
Mating Scheme - BMW (BMW- Best Mate Worst) Crossover Type - Random Mutation Rate - 0.015	Self-Recognition Parameter $c_1 = 1$ Social Parameter $c_2 = 4 - c_1$ Constriction parameter $C = 1$ Inertia weight (w) $0 < w < 0.99$

As already said in Section 3 the hybrid coefficient can be taken as static and dynamic. For instance, if h_{coeff} takes 0.3 then for each iteration 3 chromosomes undergo GA operations and 7 particles undergo PSO operation. In case of dynamic hybrid coefficient then h_{coeff} takes different value for each iteration thereby the splitting of population also varies in each iteration in accordance with h_{coeff}.

After setting these parameters, select the hybrid coefficient, then the algorithm was run and obtained results were shown in Table 3 for the message MACRO and for the message CRYPT is shown in Table 4. Garg, Aditya, Agarwal (2009) used GA to attack the knapsack cipher 'MACRO' and obtained the message in 115 populations [3] and Mayada, Baraa, Sarab (2008) used PSO to attack the same cipher and obtained the result in 86 populations [12]. By properly selecting the parameters of GA and PSO (as shown in Table 2), the same cipher (MACRO) is attacked with 81 populations (search space) using GSO with $h_{coeff} = 0$ (GA) and 68 search space using GSO with $h_{coeff} = 1$ (PSO). By hybrid the favorable characteristics of GA and PSO the search space can be further reduced. The GSO algorithm performs better if the hybrid coefficient lies between 0 and 0.5 than the hybrid coefficient lies between 0.5 and 1. Since the GA dominates the PSO in the second case and the convergence rate is slow. The

Table 3: Results for attacking the message Macro

Text	GSO with									
	$h_{coeff} = 0$		$h_{coeff} = 0.2$		$h_{coeff} = 0.3$		$h_{coeff} = 1$		$h_{coeff} = rand$	
	NS	NG	NS	NG	NS	NG	NS	NG	NS	NG
M	92	10	55	6	44	5	45	5	43	5
A	75	8	39	4	32	4	76	8	47	5
C	72	8	45	5	24	3	54	6	19	2
R	84	9	27	3	49	5	78	8	35	4
O	81	9	76	8	64	7	87	9	33	4
μ	80.8	8.8	48.4	5.2	42.6	4.8	68	7.2	35.4	4

NS: Number of Searches; NG: Number of Generations. μ: Average.

Table 4: Results for attacking the message Crypt

Text	GSO with									
	$h_{coeff} = 0$		$h_{coeff} = 0.2$		$h_{coeff} = 0.3$		$h_{coeff} = 1$		$h_{coeff} = rand$	
	NS	NG	NS	NG	NS	NG	NS	NG	NS	NG
C	72	8	64	7	62	7	64	7	42	5
R	65	7	42	5	49	5	59	6	47	5
Y	82	9	54	6	65	7	55	5	51	6
P	74	8	49	5	34	4	87	9	34	4
T	68	7	54	6	46	5	73	8	37	4
μ	72.2	7.8	52.6	5.8	51.2	5.6	67.6	7	42.2	4.8

search space can be even further reduced if dynamic hybrid coefficient is used, where at least 1.2 times the search space should be reduced when compared to static coefficients ($h_{coeff} = 0.3$). This can be observed from Table 3 and Table 4.

6 Conclusion

In this paper, knapsack cipher is attacked using GSO which combines the advantages of GA and PSO algorithm. The experimental result shows that GSO effectively breaks that knapsack cipher. The complexity of the algorithm lies in selecting the fitness function. From the analysis we came to know that, by properly initializing the GA and PSO parameters the result can be improved. The search space has been reduced by the order of 1.8 and 1.6 when compared to GA and PSO respectively. Also the Computational Complexity is reduced by at least 1.2 times compared to the static coefficient. By varying the parameters of GA, PSO and GSO i.e., hybrid coefficient the algorithm is to be fine tuned will be the future research. Also by analyzing and taking the vantage characteristics of other evolutionary algorithms, a new hybrid evolutionary algorithm is to be developed and apply the same in the cryptanalysis of knapsack cipher, block ciphers and stream ciphers.

References

[1] B. A. Forouzan, *Cryptography and Network Security*, Tata Mc Graw hill Education, 2nd edition, 2009.

[2] R. Frank, Comments on cryptanalysis of Knapsack ciphers using genetic algorithms", *Cryptologia*, vol. 18, no. 2, pp. 153 -154, 1994.

[3] P. Gaarg, S. Aditya, D. C. Agarwal, "An enhanced cryptanalytic attack on knapsack cipher using genetic algorithm", in *World Academy of science Engineering and Technology*, pp. 815-818, 2007.

[4] Gandelli, F. Grimaccia, M. Mussetta, P. Pirinoli, R. E. Zich, Development and validation of different hybridization strategies between GA and PSO, in *Proceedings of IEEE Congress on Evolutionary Computation*, Singapore, pp. 2782-2787, 2007.

[5] D. E. GoldBerg, *Genetic Algorithm in Search, Optimization and Machine Learning*, Boston, Addision-Wesley, 1999.

[6] R. L. Haupt, S. E. Haupt, *Practical Genetic Algorithms*, 2nd ed., Wiley, 2004.

[7] A. Jain, N. S. Chaudhari, "Analysis of the improved knapsack cipher," in *8th International Conference on Contemporary Computing*, pp. 537-541, 2015.

[8] Z. Jin, H. Zhang, and Z. Li, "Security on a Knapsack-type encryption scheme based upon hybrid-model assumption," *International Journal of Network Security*, vol. 19, no. 4, pp. 644-647, July 2017.

[9] J. Kennedy, R. Eberhart, "Particle swarm optimization," in *IEEE International Conference on Neural Networks*, pp. 1942-1948, 1995.

[10] J. Kennedy, R. Eberhart, "A discrete binary version of the particle swarm algorithm," in *International Conference on Neural Network*, pp. 4104-4108, 1997.

[11] N. Koblitz, *A Course in Number Theory and Cryptography*, Springer International Edition, 2008.

[12] F. A. Mayada, A. A. Baraa, M. H. Sarab, "A binary particle swarm optimization for attacking knapsacks cipher algorithm", in *Proceedings of the International Conference on Computer and Communication Engineering*, pp.77-81, 2008.

[13] R. C. Merkle, M. E. Hellman, "Hiding information and signatures in trapdoor knapsacks," *IEEE Transactions on Information Theory*, vol. IT-24, pp. 525-530, 1978.

[14] M. Mitchell, *An Introduction to Genetic Algorithms*, First MIT Press Paperback edition, 1998.

[15] N. Nedjah, A. Abraham, L. de M. Mourelle, "Swarm intelligent systems," *Studies in Computational Intelligence*, vol. 26, 2006.

[16] N. Nedjah, A. Abraham, L. de M. Mourelle, "Computational intelligence in information assurance and security," *Studies in Computational Intelligence*, vol. 57, pp. 8-13, 2007.

[17] M. Raghavan, V. Divya, R. Parthiban, "Cryptanalysis of Knapsack cipher using parallel evolutionary computing", *International Journal of Recent Trends in Engineering*, pp.260-263, 2009.

[18] R. R. Ramasamy, M. A. Prabakar, M. I. Devi, and M. Suguna, "Knapsack based ECC encryption and decryption," *International Journal of Network Security*, vol. 9, no. 3, pp. 218-226, Nov. 2009.

[19] R. Ramasamy and M. A. Prabakar, "Digital signature scheme with message recovery using Knapsack-based ECC," *International Journal of Network Security*, vol. 12, no. 1, pp. 7-12, Jan. 2011.

[20] C. R. Reeves, J. E. Rowe, *Genetic Algorithms-Principles and Perspectives. A Guide to GA Theory*, Kluwer Academic Publishers, 2002.

[21] K. P. Saibal, C. S. Rai, P. S. Amrit, "Comparitive study of firefly algorithm and particle swarm optimization for noisy non-linear optimization problems," *International Journal of Intelligent Systems and Applications*, vol. 10, pp. 50-57, 2012.

[22] R. Spillman, Cryptanalysis of knapsack ciphers using genetic algorithms, *Cryptologia*, vol. 17, no. 4, pp. 367-377, 1993.

[23] W. Stallings, *Cryptography and Network Security Principles and Practices*, Pearson Education, 2004.

[24] P. Supravo, N. S. Saptarshi, A. M. Mostafiz, K. Atreyee, K. Malay, "A cryptanalytic attack on the knapsack cryptosystem using binary firefly algorithm," in *International Conference on Computer & Communication Technology*, pp. 428-432, 2011.

[25] R. Vimalathithan, M. L. Valarmathi, "Cryptanalysis of simplified-DES using computational intelligence," *WSEAS Transactions on Computers*, vol. 10, no. 7, pp. 210-219, 2011.

[26] R. Vimalathithan, M. L. Valarmathi, "Cryptanalysis of DES using computational intelligence," *European Journal of Scientific Research*, vol. 55, no. 2, pp. 237-244, 2011.

Biography

Anto Merline M is a Ph.D- Research Scholar in the Department of Electronics and Communication, Karpagam College of Engineering, Coimbatore, Tamilnadu, India. She received her B.E. Degree in Electronics and Communication Engineering from University College of Engineering, Panruti and M.E. Degree in Communication Systems from K.Ramakrishnan College of Engineering, Trichy. Her Area of interests is Communication Network Security, Cryptography, IOT, LoRa and Machine Learning. E-mail: merlinemanoharan@gmail.com

Vimalathithan Rathinasabapathy is working as a Professor in the Department of Electronics and Communication, Karpagam College of Engineering, Coimbatore, Tamilnadu, India. He received his B.E. degree in Electronics and Communication Engineering from Kongu Engineering College, Perundurai, M.E. Degree from Government College of Technology, Coimbatore and Ph.D. in Information and Communication Engineering, Anna University, Chennai. He completed his Post Doctorate at University of Padua, Italy. Also he is a member of Cryptology Research Society of India, Computer Society of India, and IEI. His Area of interests is Cryptography, Cryptanalysis, Electromagnetic Interference and Compatibility, LoRa, IOT, Machine Learning. E-mail: athivimal@gmail.com

Visual Exploration Using Improved Moving Average Methods for Time Series Datasets

Cheng-Hung Chuang[1,2], Wei-Fu Lu[1], Ying-Chen Lin[1], and Jui-Chi Chen[1]
(Corresponding author: Jui-Chi Chen)

Department of Computer Science and Information Engineering, Asia University[1]
500, Lioufeng Rd., Wufeng, Taichung 41354, Taiwan
(Email: rikki@asia.edu.tw)
Department of Medical Research, China Medical University Hospital[2]

(Received May 24, 2018; revised and accepted Aug. 14, 2018)

Abstract

Recently, Taiwan government has voluntarily opened up various data sets to provide the public for analysis and application in order to find potential problems and help solve some public issues. A common way of using the data sets to initially explore potential issues is to visualize the miscellaneous data and present useful information represented by readily available statistical charts. In this process, the most often encountered problem is the fluctuations of the data changes in the time series of the statistical chart, so it is not easy to visually compare the trends of the source data among different factors. Therefore, we use the concept of moving average to smooth short-term fluctuations. The moving average can clearly show the difference or impact of the data on different factors. However, when using some of the traditional moving average methods to draw charts, we found that the moving averages lag behind the values of the source data, making the data visual delay in comparison. To solve this problem, this study proposes two improved moving average methods, which are compared with the traditional moving average methods in terms of smoothness and lag results to see if we can find a better one, which can more accurately analyze time series datasets to determine the trends of the past problems and the possible future trends, and then lead the follow-up study.

Keywords: Data Visualization; Moving Average; Open Data; Time Series Datasets

1 Introduction

In recent years, in order to enhance participation in public policy issues, Taiwan government has voluntarily opened up a large amount of government data to provide the public and businesses with a variety of data sets. In this way, the quality of people's life can be improved, and the demand of the industry can be met, which is also helpful to the decision making of all levels of government [9].

According to the definition of the World Health Organization (WHO), Taiwan has entered the ageing society because the elderly population exceeded 7% of national population since 1993. Last year, the National Development Council (NDC) estimated that Taiwan will enter the aged society with an elderly population ratio of 14% in 2018. It is estimated that the elderly population will have more than 20% of national population and officially enter the super-aged society in 2026. [1] Aging leads to an increase in the prevalence of cancer and chronic diseases [6]. Facing with such a severe test of cancer and chronic diseases, studying the related problems, and exploring the potential risk factors and the possible causes can prevent diseases earlier and promote people's health in our country.

In Taiwan Open Government Data (TOGD), there are 40 groups of related datasets on the issue of cancer currently provided by the Executive Yuan, Taiwan. Among them, the datasets with a relatively large amount of secondary data include "Statistics on Cause of Cancer Deaths" provided by the Department of Statistics, Ministry of Health and Welfare (MHW), and "Statistics on Cancer Incidence" provided by the Health Promotion Administration, MHW [9]. Those secondary data have been converted into structured datasets through long-term data collection and data cleansing by government agencies. We follow up data selection and data integration based on research topics, followed by data exploration [3, 4, 13]. The most common step in using secondary data to explore problems is data visualization, which presents the useful information transformed from, or hidden in, miscellaneous data using readily available statistical charts or stereoscopic models [5, 8].

In the visualization processes, the most often encountered problem is the fluctuations of the data changes in the time series of the statistical chart, so it is not easy to visually compare the trends of the source data among different factors. As shown in Figure 1 based on 22 different cities and counties in Taiwan, we drew the line chart of the age-standardized cancer incidence per 100,000 population standardized by WHO 2000's global population. The horizontal axis represents the diagnostic year of the cancer incidence drawn from 1979 to 2014, and the vertical axis indicates the age-standardized incidence. The trends of the annual cancer incidence of 22 cities and counties in Taiwan, as shown in Figure 1, seem to be chaotic and disorderly with ups and downs. It is not easy to distinguish the difference among different regions and point out the long-term trends in a short time. Therefore, we use the concept of Moving Average (MA) [7], a technique commonly used in investment technical analysis, to smooth the short-term sharp fluctuations, to reflect long-term trends, and to clearly show the difference among different geographic regions.

Preliminary studies have shown that using the traditional Arithmetic Moving Average (AMA) method to draw a statistical chart does easily compare the difference in cancer incidence or mortality among different geographic regions. Nevertheless, closer examination reveals that AMA has a numerical lag problem. The larger the sliding window size, the smoother the AMA curve, but the more severe the lag behind the annual incidence or mortality. The lag gives some degree of errors in the observation of annual numerical changes. Weighted MA (WMA) is another way to deal with the lag problem, but the WMA averages are getting less smooth, losing the goal of using the moving average to smooth drastic fluctuations in the curve. Therefore, we propose two improved MA methods to try to compare with the traditional AMA and WMA methods according to the smoothness and lag results to see if we can find another better solution. Subsequently, the results of this study for data visualization will be used to lead the follow-up study.

2 Materials and Methods

The NDC manages the government open data platform [9] to provide all kinds of data sets of various agencies voluntarily. This study complies with the guidelines of the Open Government Data License - Version 1 [10] to use the TOGD datasets for non-profit academic research.

The "Statistics on Cancer Incidence" dataset offers the source data of cancer incidence provided by the Health Promotion Administration, MHW, Taiwan [9]. All of the data were recorded for download in a single file of a total of 82,848 records from 1979 to 2014. The dataset was updated on May 16, 2017, which is a plain text file (".csv" extension) with fields separated by commas and the text encoded with UTF-8. The fields in the dataset include year, sex, city or county name, type of cancer, number of cancer patients, mean age at diagnosis, median age at diagnosis, crude incidence (per 100,000 population) and the age-standardized cancer incidence (per 100,000 population) standardized by WHO 2000's global

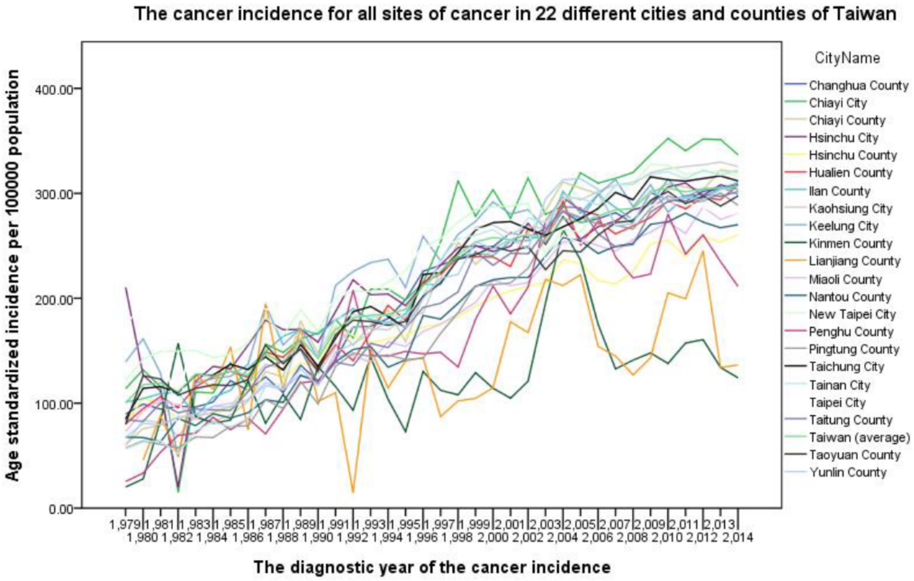


Figure 1: The line chart for the cancer incidence of 22 cities and counties in Taiwan over the past decades.

population.

The "Statistics on Cause of Cancer Deaths" datasets offer the source data of the cause of cancer deaths provided by the Department of Statistics, MHW, Taiwan [9]. The data were organized into one file (namely a dataset) per year, so there are 26 files from 1991 to 2016, with a total of 592,721 records, including 44 records with the township code 1202 (unknown) in 1991. The datasets were updated on June 5, 2017, which are plain text files (".txt" extension) encoded with UTF-8. All of the 26 files were compressed into a single package in a ZIP format for download. The main fields in each dataset are year, sex, age code, township code, cause of death, and number of deaths.

To calculate the cancer mortality, we also need to download the "Profile of Population - Stratified by Sex and Region" dataset, which records the population of cities and counties in Taiwan, provided by the Department of Statistics, Ministry of the Interior (MOI) [9]. The dataset was updated on Sept. 4, 2017, which is a plain text file (".csv" extension) with fields separated by commas and the text encoded with UTF-8. All data are recorded in a single file, providing statistical data of the population of the cities and counties from 1982 to 2014. The total population in Taiwan at the ends of 2015 and 2016 can be obtained from "Weekly Bulletin of Interior Statistics, Week 10 2017" by the Department of Statistics, MOI [1]. This study uses the SPSS Statistics 20.0, Excel 2013, and RStudio 2017 for statistical analysis and/or making charts and tables.

When we initially explore the cancer-related issues in cities and counties of Taiwan, the most common problem with using statistical charts is the case of fluctuations of the polylines drawn from the cancer incidence or mortality data in the time-series charts, making the data trends less obvious and inter-regional comparisons more difficult. In the long-term market research and investment analysis, the concept of moving average is often used to continuously analyze the average investment cost over a period of time. The characteristics of the moving average can smooth the short-term fluctuating curve. Therefore, we first calculate the n-year AMA of the cancer incidence or mortality in different geographical regions in the year (y) and decide whether it reflects the long-term trend. The formula of the n-year AMA is as follows:

$$nAMA(y) = (\sum_{j=0}^{n-1} I_{y-j})/n, \tag{1}$$

where window size $n \in N$, and I_{y-j} is incidence or mortality in the year $(y - j)$. And $nAMA(y + 1)$ could be calculated using

$$nAMA(y + 1) = nAMA(y) + (I_{y+1} - I_{y-n+1})/n. \tag{2}$$

Equation (2) is more efficient for calculating the consecutive nAMA values than Equation (1).

Unfortunately, nAMA has a lag problem, that is, the larger the sliding window size (n) is, the more the nAMA value falling behind the cancer incidence or mortality in the year (y) becomes. The lag problem often leads to a time lag in years. Figure 2 illustrates the 5- to 20-year AMAs of the annual crude mortality of liver cancer per 100,000 population in Taiwan over the past decades. The y-axis of Figure 2 indicates the death year of liver cancer, which is drawn from 1992 to 2016, and x-axis measures the annual crude mortality. As shown in Figure 2, the larger the number of years (n) for moving average, the more serious the lag problem in mortality. For example, 10AMA lags more behind source mortality than 5AMA in the same year. Weighted MA (WMA) is another way to solve the lag problem, so we try the various WMA formulas for comparison in the following.

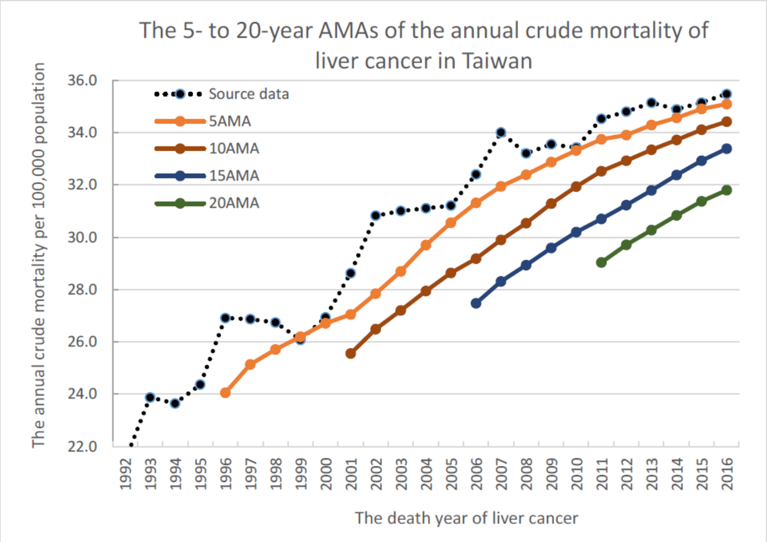


Figure 2: Arithmetic moving averages of the crude mortality (including both sexes) for liver and intrahepatic bile ducts of cancer in Taiwan from 1992 to 2016.

The first common type of WMA is the n-year Linear WMA (nLWMA) of the cancer incidence or mortality in the year (y), and its formula is shown below [2,14]:

$$\begin{aligned} nLWMA(y) &= [\sum_{j=0}^{n-1}(n-j)(I_{y-j})]/\sum_{i=1}^{n} i) \\ &= 2 \cdot [\sum_{j=0}^{n-1}(n-j)(I_{y-j})]/[n(n+1)], \end{aligned} \tag{3}$$

where $n \in N$, and I_{y-j} is incidence or mortality in the year $(y-j)$.

The second type of WMA is the n-year Squared WMA (nSWMA) of the cancer incidence or mortality in the year (y), and its formula is as follows:

$$nSWMA(y) = [\sum_{j=0}^{n-1}(n-j)^2(I_{y-j})]/(\sum_{i=1}^{n} i^2), \tag{4}$$

where $n \in N$, and I_{y-j} is incidence or mortality in the year $(y-j)$.

The third type of WMA is the n-year Cubic WMA (nCWMA) of the cancer incidence or mortality in the year (y), and its formula can be written as

$$nCWMA(y) = [\sum_{j=0}^{n-1}(n-j)^3(I_{y-j})]/(\sum_{i=1}^{n} i^3), \tag{5}$$

where $n \in N$, and I_{y-j} is incidence or mortality in the year $(y-j)$.

The fourth type of WMA is the n-year Quartic WMA (nQWMA) of the cancer incidence or mortality in the year (y), and its formula is shown below:

$$nQWMA(y) = [\sum_{j=0}^{n-1}(n-j)^4(I_{y-j})]/(\sum_{i=1}^{n} i^4), \tag{6}$$

where $n \in N$, and I_{y-j} is incidence or mortality in the year $(y-j)$.

The general formula for WMA described above is the k-th power of the n-year WMA, nWMAPk, of the cancer incidence or mortality in the year (y), which can be written as

$$nWMAP_k(y) = [\sum_{j=0}^{n-1}(n-j)^k(I_{y-j})]/(\sum_{i=1}^{n} i^k), \tag{7}$$

where $k, n \in N$, and I_{y-j} is incidence or mortality in the year $(y-j)$.

The fifth type of WMA is the n-year Exponential WMA (nEWMA) of the cancer incidence or mortality in the year (y), and its formula is as follows [2,11,14]:

$$nEWMA(y) = [\sum_{j=0}^{n-1}(1-\alpha)^j(I_{y-j})]/\sum_{i=0}^{n-1}(1-\alpha)^i, \tag{8}$$

where $\alpha = 2/(n+1)$, $n \in N$, and I_{y-j} is incidence mortality in the year $(y-j)$.

Therefore, if nEWMA is calculated yearly and sequentially, the formula for the next year can be rewritten as

$$nEWMA(y+1) = \alpha \cdot (I_{y+1}) + (1-\alpha) \cdot nEWMA(y), \tag{9}$$

where $\alpha = 2/(n+1)$, $n \in N$, and I_y is incidence or mortality in the year (y). Preliminary experimental observations show that the lag value decreasing, as the power of nWMA increasing, and the nWMA value is closer to the annual incidence or mortality. However, the higher power the WMA curves have, the less smooth the curves are, which loses the objective of smoothing the curves. In this paper, we propose two improved MA models which take both the lag and the smoothness into account to obtain the better solution of moving average. The first proposed model is the n-year Balanced AMA (nBAMA) of the cancer incidence or mortality in the year (y), which calculates the average of the incidence or mortality from the $(n/2)$-th year before the year (y) to the $(n/2)$-th year after the year (y), instead of the n years before the year (y). Thus, the smoothness of BAMA is very close to that of AMA, while the BAMA value is closer to the source incidence or mortality of the year (y), and also better than the AMA value. In other words, BAMA can also improve the lag problem. The formula of the first proposed model is as follows:

$$nBAMA(y) = (\sum_{j=0}^{n-1} I_{y-j+\lfloor \frac{n}{2} \rfloor})/n, \tag{10}$$

where $n \in N$, and I_y is incidence or mortality in the year (y). If nBAMA is calculated yearly and sequentially, the formula for the next year will be equal to:

$$nBAMA(y+1) = nBAMA(y) + (I_{y+\lfloor \frac{n}{2} \rfloor+1} - I_{y-\lceil \frac{n}{2} \rceil+1})/n. \tag{11}$$

The second proposed model is the k-th power of the n-year Balanced WMA, nBWMAPk, of the cancer incidence or mortality in the year (y), and its general formula is shown below:

$$nBWMAP_k(y) = \frac{\lfloor n/2+1 \rfloor^k \cdot I_y + \sum_{j=1}^{\lfloor n/2 \rfloor} (\lfloor n/2+1 \rfloor - j)^k (I_{y-j} + I_{y+j})}{\lfloor n/2+1 \rfloor^k + 2 \cdot \sum_{i=1}^{\lfloor n/2 \rfloor} i^k}, \tag{12}$$

where $k, n \in N$, $ngeq2$, and I_y is incidence or mortality in the year (y). Naturally, BWMAPk includes Balanced LWMA (BLWMA) when $k = 1$, Balanced SWMA (BSWMA) when $k = 2$, Balanced CWMA (BCWMA) when $k = 3$, and Balanced QWMA (BQWMA) when $k = 4$.

Subsequently, we compare the above formulas based on the lag problem and the curve smoothness mentioned above. To observe how much the numerical differences between the source data (I_j) and the n-year averages (nXMA(j)) derived from moving average methods (XMAs), we define σ^n_{XMA} by Equation (13). The larger σ^n_{XMA} is, the more serious the lag problem becomes.

$$\sigma^n_{XMA} = \sqrt{\sum_{j=t}^{t+m-1} [I_j - nXMA(j)]^2/m}, \tag{13}$$

where $m, n \in N$, $m, n \geq 2$, m is number of evaluation years, t is the first evaluation year, and I_j is incidence or mortality in the year (j). For comparing different Moving Average methods (XMA), the lag value of n-year XMA can be normalized to [0, 1], denoted by the Lag Index (LI), as shown below:

$$LI^n_{XMA} = \frac{\sigma^n_{XMA} - \min(\{All\ \sigma^n_{XMA}\})}{\max(\{All\ \sigma^n_{XMA}\}) - \min(\{All\ \sigma^n_{XMA}\})} \tag{14}$$

where $\min(\{All\ \sigma^n_{XMA}\}$ is the minimum value of all σ^n_{XMA}, and $\max(\{All\ \sigma^n_{XMA}\}$ is the maximum value of all σ^n_{XMA}.

Let δ be the smoothness of XMA, which shows how much the numerical difference between the n-year XMA value of the year (j) and that of year $(j+1)$. Then we calculate the root mean square of the numerical differences over the evaluation years. The smaller the value δ, the smoother the moving average curve. The evaluation formula for the smoothness is as follows:

$$\delta^n_{XMA} = \sqrt{\sum_{j=t}^{t+m-2} [nXMA(j+1) - nXMA(j)]^2/(m-1)} \tag{15}$$

where $m, n \in N$, $m, n \geq 2$, m is number of evaluation years, and t is the first evaluation year. Similarly, the smoothness of any n-year XMA can be normalized to [0, 1], which is the Smooth Index (SI) as shown below:

$$SI^n_{XMA} = \frac{\delta^n_{XMA} - \min(\{All\ \delta^n_{XMA}\})}{\max(\{All\ \delta^n_{XMA}\}) - \min(\{All\ \delta^n_{XMA}\})} \tag{16}$$

where $\min(\{All\ \delta^n_{XMA}\})$ is the minimum value of all δ^n_{XMA} and $\min(\{All\ \delta^n_{XMA}\})$ is the maximum value of all δ^n_{XMA}.

To evaluate the overall effect of a moving average XMA with both lag and smoothness, we multiply the mean square of lag $(\sigma^n_{XMA})^2$ by the mean square of smoothness $(\delta^n_{XMA})^2$ to obtain a composite score which is called Product of Mean Squares (PMS). Meanwhile, the power k, the smooth weighted parameter, is introduced as the adjustment of the smoothness. When a better smooth effect is considered, the value k must be increased. Therefore, the following composite score for the overall effect of XMA is written as:

$$PMS^{n,k}_{XMA} = \ln((\sigma^n_{XMA})^2 \cdot (\delta^n_{XMA})^{2k}), \tag{17}$$

where $n, k \in N$, and $n \geq 2$.

3 Results and Discussion

The trends of the annual cancer incidence of 22 cities and counties in Taiwan, as shown in Figure 1, seem to be chaotic and disorderly with ups and downs. It is not easy to distinguish the differences among different regions, and point out the long-term trends in a short time. Using Equation (1) or (2), we calculated the 12-year arithmetic moving average (12AMA) of cancer incidence (including both sexes) for all sites in Taipei and Kaohsiung over the past three decades. The 12AMA trends for the cancer incidence of the two cities are shown in Figure 3, where x-axis is the diagnostic year of the cancer, and y-axis indicates the age-standardized incidence. The dotted lines in the figure represent the source data of the incidence of the two cities, while the solid lines show the 12AMA averages. The trend of the annual cancer incidence is obvious because the shape of the 12AMA curve is smooth. However, there is a serious numerical gap between 12AMA and the annual incidence in the same city, which is the lag problem. The problem makes the intersection of two 12AMA curves lagging behind the intersection of the annual incidence curves of the two cities in Figure 3, which indirectly results in judgment with a delayed error. For example, the 12AMA curve of Taipei intersected with the 12AMA curve of Kaohsiung at 2006. In fact, the intersection of the original curves of the two cities took place as early as 1999.

To solve the lag problem, we use Equations (3) through (9) to calculate the 9-year WMA curves of the cancer incidence (including both sexes) in Chiayi City over the past three decades. As shown in Figure 4, the lagged effects and smoothing differences among various 9-year WMAs are compared. Although the 9AMA curve is the smoothest, its lag is the most. The 9EWMA has the smallest lag, of which curve is the closest to the line of the source data, but it is the least smooth. However, the lag

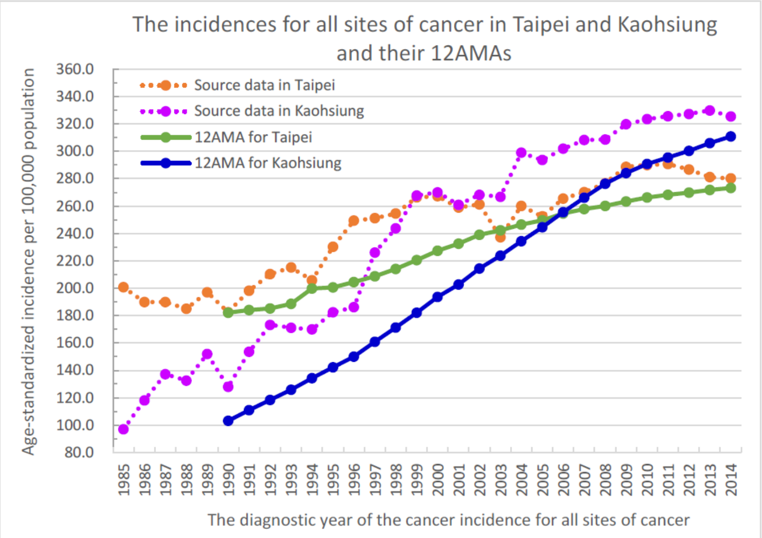


Figure 3: The line chart for the cancer incidence (including both sexes) and the 12AMA curves of Taipei and Kaohsiung over the past three decades.

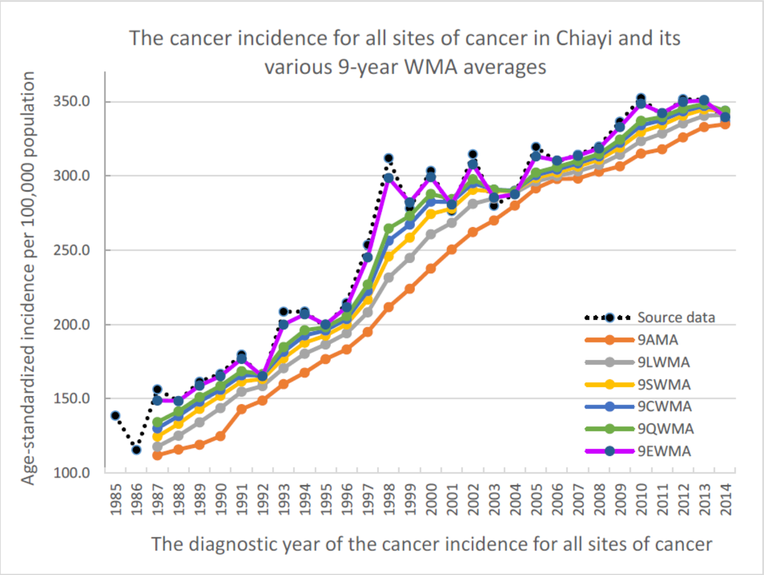


Figure 4: The cancer incidence (including both sexes) and various 9-year WMA curves of Chiayi City over the past three decades.

and the smoothness of various 9-year WMAs are all different, and the trade-offs between pros and cons are presented. That is, the smoother the curve is, the more the average lags behind.

As illustrated in Figure 4, the larger the power k of 9WMA, the more the lag improvement; nevertheless, the curves of 9WMA with high order of power become less smooth, losing the original goal of smoothing the curves with moving averages. Thus, two improved MA models, Equations (10) and (12), are proposed in this study, and are called Balanced AMA (BAMA) and Balanced WMA (BWMA), respectively. To compare the differences among the proposed and traditional MA models, we use the Microsoft Excel random generator to produce a simulated fluctuation time-series dataset with a bell-shaped distribution for calculating and comparing all the 9-year moving averages mentioned above. After excluding the least smooth 9EWMA and 9QWMA in Figure 4, we plot the visual comparison of the 9-year moving averages in Figure 5. The simulated data are represented by the black dotted line, and the other lines are illustrated for the 9-year moving averages, respectively. Roughly, 9BLWMA (green line) and 9BSWMA (blue line) proposed in this study appear to be similar in smoothness to the traditional moving average (9AMA), and they also greatly improve the lag problems, which can be improved further by using another simulated time-series dataset with a smooth bell-shaped distribution as shown in Figure 6. Basically, all the balanced moving averages can improve the lag problems.

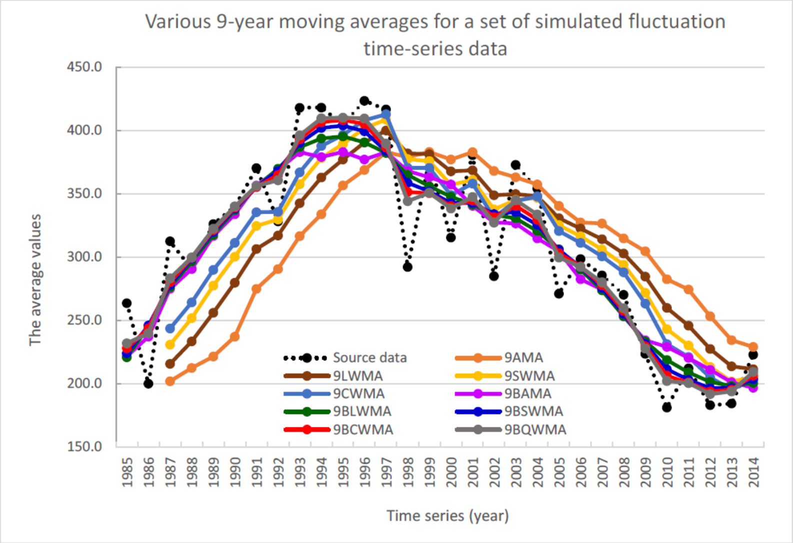


Figure 5: Various 9-year moving averages for a simulated fluctuation time-series dataset with a bell-shaped distribution.

To objectively evaluate the lag and the curve smoothness of the moving averages mentioned above, we propose Equations (13) through (16) to represent lag σ^n_{XMA}, lag index LI^n_{XMA}, smoothness δ^n_{XMA}, and smoothness index SI^n_{XMA}, respectively. The smaller the LI^n_{XMA} value, the less the lag. The smaller the SI^n_{XMA} value, the smoother the moving average curve. Therefore, if a moving average makes these two indices smaller than others do, it is the most suitable for representing a time series trend of the source data. Based on the same simulated fluctuation dataset above, the lag index (Table 1) and the smoothness index (Table 2) of various n-year moving averages (nXMAs) are obtained according to Equations (13) and (14). Consequently, the following results are observed: a) No matter what type of moving average is used, the larger the sliding window size (n), the larger the lag index, and the smaller the smoothness index. b) Most of the balanced MAs have smaller lag indices than the traditional MAs do, especially, when the sliding window size is large. c) AMA has the least smoothness index, i.e., the best smoothing effect. The smoothness indices of all MA methods are affected by the sliding window size and the simulated fluctuation data. In general, if the smoothness indices are sorted in increasing order, then AMA < BAMA < BLWMA < BSWMA < LWMA < SWMA < BWWMA < CWMA < BQWMA < QWMA. The smoothing effects of BAMA and BLWMA proposed are almost equal to those of the best AMA, followed by BSWMA proposed in this study.

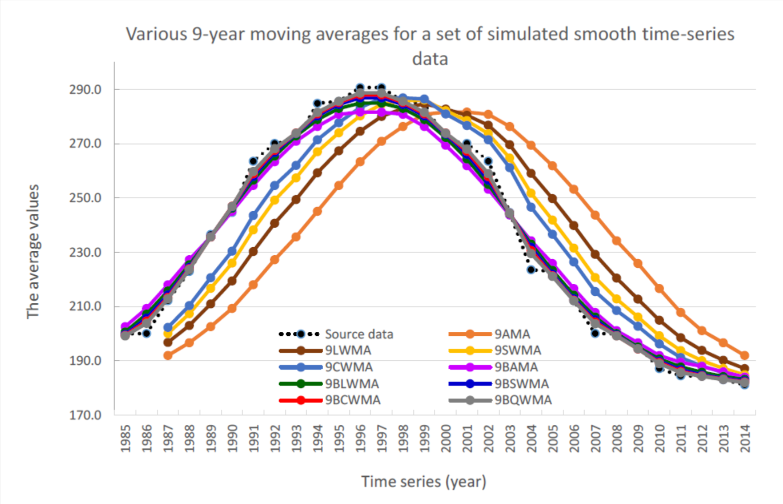


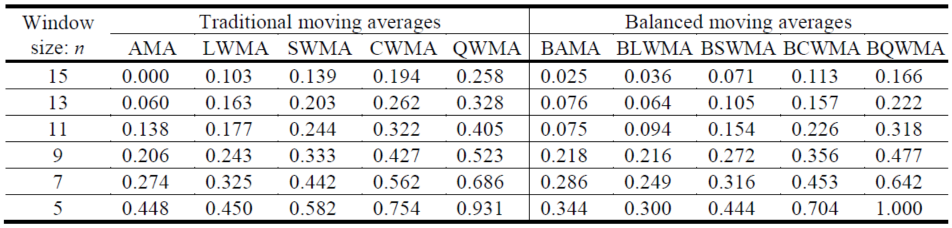
Figure 6: Various 9-year moving averages for a simulated smooth time-series dataset with a bell-shaped distribution.

Table 1: The lag index LI^n_{XMA} for various n-year moving averages (nXMAs) using the simulated fluctuation time-series dataset.

Window	Traditional moving averages					Balanced moving averages				
size: n	AMA	LWMA	SWMA	CWMA	QWMA	BAMA	BLWMA	BSWMA	BCWMA	BQWMA
15	1.000	0.692	0.508	0.401	0.332	0.386	0.307	0.263	0.231	0.204
13	0.941	0.646	0.466	0.360	0.289	0.343	0.279	0.238	0.207	0.179
11	0.823	0.553	0.400	0.307	0.242	0.313	0.251	0.212	0.180	0.148
9	0.754	0.519	0.376	0.282	0.216	0.273	0.242	0.207	0.169	0.130
7	0.602	0.409	0.288	0.207	0.146	0.272	0.223	0.176	0.127	0.078
5	0.434	0.289	0.187	0.115	0.058	0.236	0.192	0.132	0.064	0.000

Based on the same simulated smooth dataset above, the lag index (Table 3) and the smoothness index (Table 4) of various n-year moving averages (nXMAs) are obtained according to Equations (15) and (16), respectively. Consequently, the following results are observed: a) No matter what type of moving average is used, the larger the sliding window size, the larger the lag index, but the smaller the smoothness index. b) When the source data tend to be smooth, all of the balanced MAs have smaller lag indices than the traditional MAs do. If the lag indices are sorted in increasing order, then BQWMA < BCWMA < BSWMA < BLWMA < BAMA < QWMA < CWMA < SWMA < LWMA < AMA. c) The AMA and BAMA have the best smoothing effect. If the smoothness indices are sorted in increasing

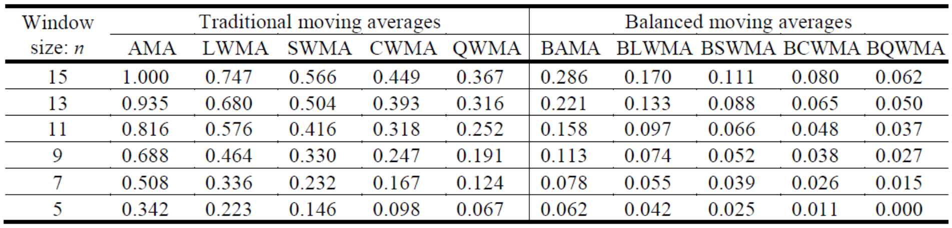
Table 2: The smoothness index SI^{n}_{XMA} for various n-year moving averages (nXMAs) using the simulated fluctuation time-series dataset.



Window	Traditional moving averages					Balanced moving averages				
size: *n*	AMA	LWMA	SWMA	CWMA	QWMA	BAMA	BLWMA	BSWMA	BCWMA	BQWMA
15	0.000	0.103	0.139	0.194	0.258	0.025	0.036	0.071	0.113	0.166
13	0.060	0.163	0.203	0.262	0.328	0.076	0.064	0.105	0.157	0.222
11	0.138	0.177	0.244	0.322	0.405	0.075	0.094	0.154	0.226	0.318
9	0.206	0.243	0.333	0.427	0.523	0.218	0.216	0.272	0.356	0.477
7	0.274	0.325	0.442	0.562	0.686	0.286	0.249	0.316	0.453	0.642
5	0.448	0.450	0.582	0.754	0.931	0.344	0.300	0.444	0.704	1.000

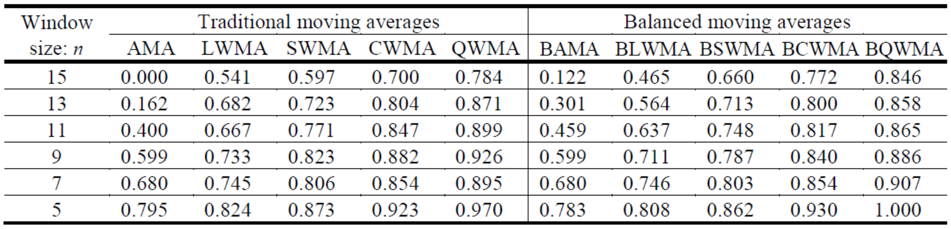
order, then AMA $\fallingdotseq$ BAMA $<$ BLWMA $<$ LWMA $<$ BSWMA $\fallingdotseq$ SWMA $<$ BCWMA $\fallingdotseq$ CWMA $<$ BQWMA $\fallingdotseq$ QWMA. Generally, the smoothing effects of the balanced MAs are close to those of the traditional MAs when the source data tend to be smooth.

Table 3: The lag index LI^{n}_{XMA} for various n-year moving averages (nXMAs) using the simulated smooth time-series dataset.



Window	Traditional moving averages					Balanced moving averages				
size: *n*	AMA	LWMA	SWMA	CWMA	QWMA	BAMA	BLWMA	BSWMA	BCWMA	BQWMA
15	1.000	0.747	0.566	0.449	0.367	0.286	0.170	0.111	0.080	0.062
13	0.935	0.680	0.504	0.393	0.316	0.221	0.133	0.088	0.065	0.050
11	0.816	0.576	0.416	0.318	0.252	0.158	0.097	0.066	0.048	0.037
9	0.688	0.464	0.330	0.247	0.191	0.113	0.074	0.052	0.038	0.027
7	0.508	0.336	0.232	0.167	0.124	0.078	0.055	0.039	0.026	0.015
5	0.342	0.223	0.146	0.098	0.067	0.062	0.042	0.025	0.011	0.000

Table 4: The smoothness index SI^{n}_{XMA} for various n-year moving averages (nXMAs) using the simulated smooth time-series dataset.

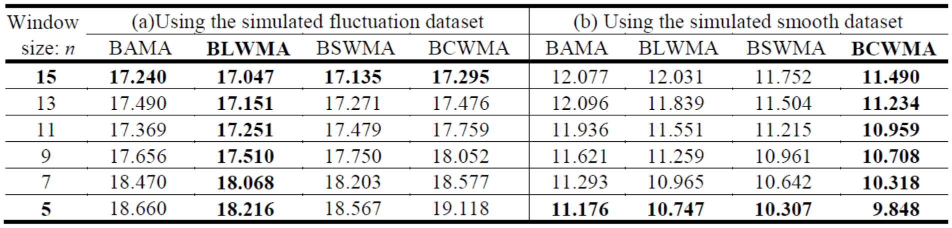


Window	Traditional moving averages					Balanced moving averages				
size: *n*	AMA	LWMA	SWMA	CWMA	QWMA	BAMA	BLWMA	BSWMA	BCWMA	BQWMA
15	0.000	0.541	0.597	0.700	0.784	0.122	0.465	0.660	0.772	0.846
13	0.162	0.682	0.723	0.804	0.871	0.301	0.564	0.713	0.800	0.858
11	0.400	0.667	0.771	0.847	0.899	0.459	0.637	0.748	0.817	0.865
9	0.599	0.733	0.823	0.882	0.926	0.599	0.711	0.787	0.840	0.886
7	0.680	0.745	0.806	0.854	0.895	0.680	0.746	0.803	0.854	0.907
5	0.795	0.824	0.873	0.923	0.970	0.783	0.808	0.862	0.930	1.000

If the lag and the smoothness are taken into account simultaneously, Equation (17) is used to calculate the composite score $PMS^{n,2}_{XMA}$ for evaluating the overall effect of a moving average. The lower the composite score, the better the overall effect. To compare nBAMA, nBLWMA, nBSWMA, and nBCWMA all together, we use six sets of sample data to obtain the composite scores listed in Tables 5 through 7, assuming that the smooth weighted parameter $k = 2$. First, the simulated fluctuation time-series dataset are used to calculate various nXMA composite scores as shown in Table 5(a). The

15BLWMA obtains the lowest score, i.e., it has the best performance. In particular, the larger the sliding window size, the better the overall effect. BLWMA has a great contribution to improve the lag problem and the smoothness. Second, Table 5(b) shows various nXMA composite scores derived from the simulated smooth time-series dataset. BAMA and BLWMA, which have better smoothing effects although, are not significantly different from the other MA methods in terms of smoothness. When the data is smooth, and even a large sliding window size is used, it no longer increases the composite scores. On the contrary, the small sliding window size and BCWMA used can get the high score on the degree of lag so that 5BCWMA performs the best.

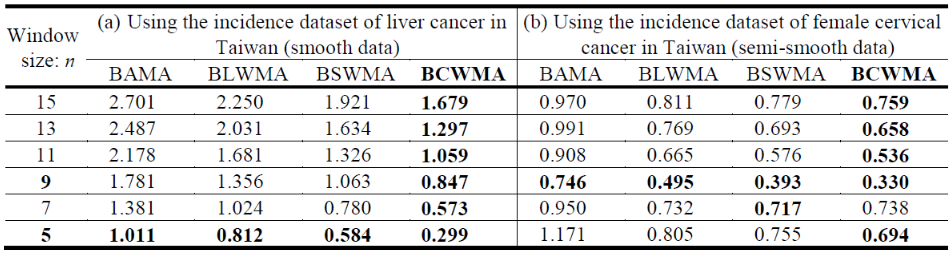
Table 5: The composite scores $PMS^{n,2}_{XMA}$ in terms of lag and smoothness using the two simulated datasets aforementioned for examples.



Window	(a)Using the simulated fluctuation dataset				(b) Using the simulated smooth dataset			
size: *n*	BAMA	**BLWMA**	BSWMA	BCWMA	BAMA	BLWMA	BSWMA	**BCWMA**
15	**17.240**	**17.047**	**17.135**	**17.295**	12.077	12.031	11.752	**11.490**
13	17.490	**17.151**	17.271	17.476	12.096	11.839	11.504	**11.234**
11	17.369	**17.251**	17.479	17.759	11.936	11.551	11.215	**10.959**
9	17.656	**17.510**	17.750	18.052	11.621	11.259	10.961	**10.708**
7	18.470	**18.068**	18.203	18.577	11.293	10.965	10.642	**10.318**
5	18.660	**18.216**	18.567	19.118	**11.176**	**10.747**	**10.307**	**9.848**

Tables 6 and 7 show the results of the other four examples in Taiwan based on the age-standardized cancer incidence for some sites per 100,000 population standardized by WHO 2000's global population. The overall effects of nXMAs were evaluated from 1981 to 2014. Table 6(a) shows the composite scores of nXMAs for the incidence (including both sexes) of liver cancer over the evaluation years. Because the source data is smooth, the conclusion is the same as that in Table 5(b). Table 6(b) takes the incidence of female cervical cancer over the evaluation years for an example. The source data of the cervical cancer incidence are semi-smooth, so the scoring results are similar to Table 6(a). However, when the sliding window size (n) is 9 in Table 6(b), it performs better. Two more examples are for the cancer incidence in Hsinchu City (male) and Chiayi City (both sexes), Taiwan. The source data of the two examples are relatively fluctuant, which are used to score nXMAs for comparison in Tables 7(a) and 7(b), respectively. Generally, when the sliding window size (n) is 9 or 11, the method BLWMA or BSWMA performs better.

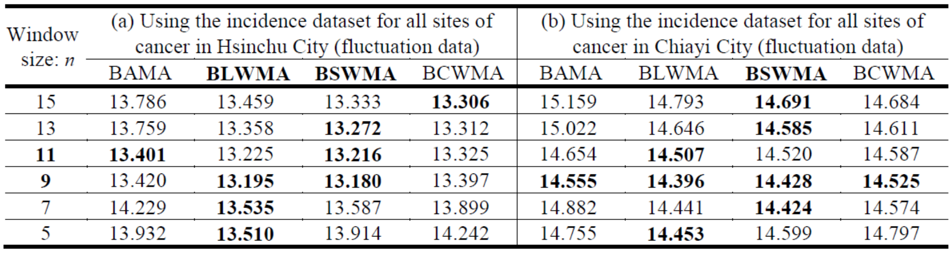
Table 6: The composite scores $PMS^{n,2}_{XMA}$ in terms of lag and smoothness using the incidence datasets of liver cancer (both sexes) and cervical cancer (female) in Taiwan for examples.



Window size: *n*	(a) Using the incidence dataset of liver cancer in Taiwan (smooth data)				(b) Using the incidence dataset of female cervical cancer in Taiwan (semi-smooth data)			
	BAMA	BLWMA	BSWMA	**BCWMA**	BAMA	BLWMA	BSWMA	**BCWMA**
15	2.701	2.250	1.921	**1.679**	0.970	0.811	0.779	**0.759**
13	2.487	2.031	1.634	**1.297**	0.991	0.769	0.693	**0.658**
11	2.178	1.681	1.326	**1.059**	0.908	0.665	0.576	**0.536**
9	1.781	1.356	1.063	**0.847**	**0.746**	**0.495**	**0.393**	**0.330**
7	1.381	1.024	0.780	**0.573**	0.950	0.732	**0.717**	0.738
5	**1.011**	**0.812**	**0.584**	**0.299**	1.171	0.805	0.755	**0.694**

Based on the above discussions, the proposed BLWMA and BSWMA methods in this study obtain

Table 7: The composite scores $PMS^{n,2}_{XMA}$ in terms of lag and smoothness using the incidence datasets for all sites of cancer in Hsinchu City (male) and Chiayi City (both sexes) for examples.



Window size: *n*	(a) Using the incidence dataset for all sites of cancer in Hsinchu City (fluctuation data)				(b) Using the incidence dataset for all sites of cancer in Chiayi City (fluctuation data)			
	BAMA	**BLWMA**	**BSWMA**	BCWMA	BAMA	BLWMA	**BSWMA**	BCWMA
15	13.786	13.459	13.333	**13.306**	15.159	14.793	**14.691**	14.684
13	13.759	13.358	**13.272**	13.312	15.022	14.646	**14.585**	14.611
11	**13.401**	13.225	**13.216**	13.325	14.654	**14.507**	14.520	14.587
9	13.420	**13.195**	**13.180**	13.397	**14.555**	**14.396**	**14.428**	**14.525**
7	14.229	**13.535**	13.587	13.899	14.882	14.441	**14.424**	14.574
5	13.932	**13.510**	13.914	14.242	14.755	**14.453**	14.599	14.797

good smoothness in most cases, and also greatly contribute to the lag improvement, which are well suited for visualizing the data of the cancer incidence and mortality in Taiwan. On the selection of the sliding window size, it appears from many examples that $n = 9$ or 11 can be applied to the general case of semi-smooth source data without fluctuation. Finally, we use the same source data in Figure 3 to plot the moving averages of the cancer incidence for all sites in Taipei and Kaohsiung over the past three decades, as shown in Figure 7, by using 9BLWMA. The dotted lines in Figure 7 represent the source data of the cancer incidence of the two cities, while the solid lines represent the 9BLWMA averages of the cancer incidence of the two cities, respectively. Comparing 9BLWMA in Figure 7 with 12AMA in Figure 3, it is observed that the smoothness of both two moving lines is good, but the 9BLWMA method greatly improves the severe lag problem of 12AMA, avoiding the error caused by the delay judgment. As shown in Figure 7, Taipei's 9BLWMA has a cross with Kaohsiung's 9BLWMA at 2000, six years earlier than the intersection of the 12AMAs of the two cities in Figure 3. The cross is at most one-year far from the intersection of the source data of the two cities at 1999. In future research, the results of this study combined with the Autoregressive Integrated Moving Average (ARIMA) model [12,15] may be applied to predict more accurately the likely changes in the incidence and mortality of a specific cancer in a given geographical area in the coming years.

4 Conclusion

Some common traditional MA methods to draw charts used in this study found that the moving averages lag behind the values of the source data, making the data visual delay in comparison. This study proposes two improved balanced MA methods to compare with the traditional MA methods in terms of lag and smoothness. The following conclusions are acquired: a) No matter what type of moving average is used, the larger the sliding window size, the better the smoothness, but the more serious the lag. b) Most of balanced MAs have less lags than traditional MAs do, especially, when the sliding window size is large. c) In most cases, the proposed BLWMA and BSWMA methods obtain very good smoothness, and also have a significant contribution to improve the lag problem, which are very suitable for the visual exploration of time-series datasets.

Acknowledgements

The various datasets used in this study were released by the NDC and related authorities in Taiwan, and were licensed to academic research according to the Open Government Data License - Version 1.

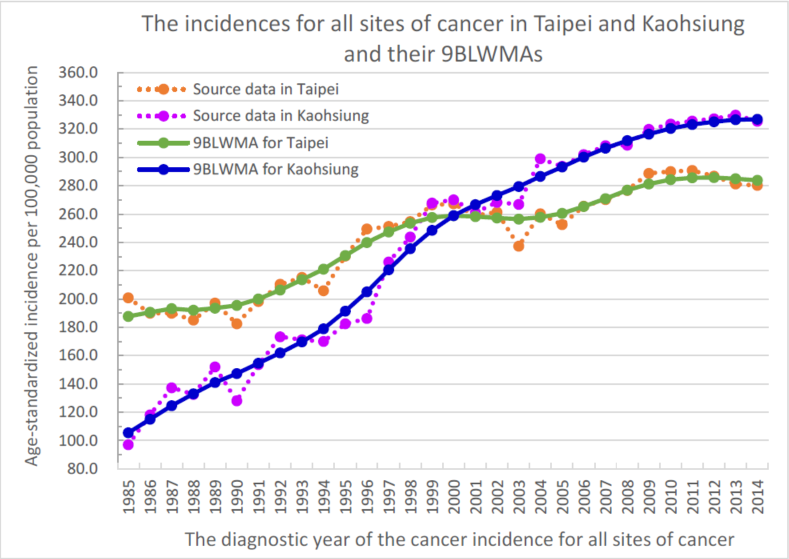


Figure 7: The cancer incidence (including both sexes) and the 9BLWMAs of Taipei and Kaohsiung over the past three decades.

The authors also gratefully acknowledge the financial support from the Taiwan Ministry of Science and Technology (MOST 105-2221-E-468-021-).

References

[1] Department of Statistics, Ministry of the Interior, Executive Yuan, Taiwan, *Weekly Bulletin of Interior Statistics*, Week 10 2017. (`http://www.moi.gov.tw/stat/news_content.aspx?sn=11735andhttp://www.moi.gov.tw/files/news_file/week10610_1.pdf`)

[2] J. D. Hamilton, *Time Series Analysis (1st Edition)*, Publisher: Princeton University Press, Jan. 11, 1994.

[3] J. Han, M. Kamber, J. Pei, *Data Mining: Concepts and Techniques (Third Edition)*, Publisher: Morgan Kaufmann, July 6, 2011.

[4] A. P. Javier, C. Y. P. Carmen, D. M. Robert, T. C. W. Stephen, and G. Z. Yang, "Big data for health," *IEEE Journal of Biomedical and Health Informatics*, vol. 19, no. 4, pp. 1193–1208, 2015.

[5] D. A. Keim, "Information visualization and visual data mining," *IEEE Transactions on Visualization and Computer Graphics*, vol. 8, no. 1, pp. 1–8, 2002.

[6] T. Y. Lan, "Population aging in Taiwan: Future health implications," *Taiwan Journal of Public Health*, vol. 22, nO. 3, pp. 237–244, 2003.

[7] X. Liu, H. An, L. Wang, Q. Guan, "Quantified moving average strategy of crude oil futures market based on fuzzy logic rules and genetic algorithms," *Physica A: Statistical Mechanics and its Applications*, vol. 482, pp. 444–457, 2017..

[8] L. Meloncon, E. Warner, "Data visualizations: A literature review and opportunities for technical and professional communication," in *IEEE International Professional Communication Conference (ProComm'17)*, pp. 1–9, 2017.

[9] National Development Council, Executive Yuan, Taiwan, *Taiwan Open Government Data*, 2017. (https://data.gov.tw/)

[10] National Development Council, Executive Yuan, Taiwan, *Open Government Data License - Version 1.0*, July 27, 2015. (https://data.gov.tw/license)

[11] National Institute of Standards and Technology, U.S. Department of Commerce, *NIST/SEMATECH e-Handbook of Statistical Methods: 6.3.2.4. EWMA Control Charts*, Apr. 2012. (http://www.itl.nist.gov/div898/handbook/)

[12] F. Nhita, D. Saepudin, U. N. Wisesty, "Comparative study of moving average on rainfall time series data for rainfall forecasting based on evolving neural network classifier," in *The 3rd International Symposium Computational and Business Intelligence (ISCBI'15)*, pp. 112–116, 2015.

[13] M. S. Viktor, K. Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think*, Publisher: Eamon Dolan/Mariner Books, Mar. 4, 2014.

[14] W. W. S. Wei, *Time Series Analysis: Univariate and Multivariate Methods (2nd Edition)*, Publisher: Pearson, July 17, 2005.

[15] Wikipedia, *Autoregressive-moving-average (ARMA) Model*, 2017. (https://en.wikipedia.org/wiki/Autoregressive-moving-average_model)

Biography

Cheng-Hung Chuang is an associate professor in the Department of Computer Science and Information Engineering, Asia University, Taiwan. He is also a research scholar in the Department of Medical Research, China Medical University Hospital, Taiwan. His research interests include medical image processing, video processing, optical signal processing, and artificial neural networks. (Email: chchuang@asia.edu.tw)

Wei-Fu Lu is an assistant professor in the Department of Computer Science and Information Engineering, Asia University, Taiwan. His research interests include computational biology, bioinformatics, algorithm design and analysis, and discrete mathematics. (Email: weifu@asia.edu.tw)

Ying-Chen Lin is a student in the Department of Computer Science and Information Engineering, Asia University, Taiwan. (Email: 106021010@live.asia.edu.tw)

Jui-Chi Chen is an associate professor in the Department of Computer Science and Information Engineering, Asia University, Taiwan. His research interests include data mining, biomedical informatics, biomedical communications, and wireless communications. (Email: rikki@asia.edu.tw)

Guide for Authors

International Journal of Electronics and Information Engineering

International Journal of Electronics and Information Engineering (IJEIE) will be committed to the timely publication of very high-quality, peer-reviewed, original papers that advance the state-of-the art and applications of Electronics and Information Engineering. Topics will include, but not be limited to, the following: Algorithms, Bioinformatics, Computation Theory, AI, Fuzzy Systems, Embedded Systems, VLSI/EDA, Computer Networks, Information Security, Database, Data Mining, and Information Retrieval, Digital Content, Digital Life, and Human Computer Interaction, Image Processing, Computer Graphics, and Multimedia Technologies, Information Literacy, e-Learning, and Social Media, Mobile Computing, Wireless Communications, and Vehicular Technologies, Parallel, Peer-to-peer, Distributed, and Cloud Computing, Semiconductor, Software Engineering and Programming Languages, Telecommunication, etc.

1. Submission Procedure

Authors are strongly encouraged to submit their papers electronically by using online manuscript submission at http://ijeie.jalaxy.com.tw/.

2. General

Articles must be written in good English. Submission of an article implies that the work described has not been published previously, that it is not under consideration for publication elsewhere. It will not be published elsewhere in the same form, in English or in any other language, without the written consent of the Publisher.

2.1 Length Limitation:

All papers should be concisely written and be no longer than 30 double-spaced pages (12-point font, approximately 26 lines/page) including figures.

2.2 Title page

Title page should contain the article title, author(s) names and affiliations, address, an abstract not exceeding 100 words, and a list of three to five keywords.

2.3 Corresponding author

Clearly indicate who is willing to handle correspondence at all stages of refereeing and publication. Ensure that telephone and fax numbers (with country and area code) are provided in addition to the e-mail address and the complete postal address.

2.4 References

References should be listed alphabetically, in the same way as follows:

For a paper in a journal: M. S. Hwang, C. C. Chang, and K. F. Hwang, ``An ElGamal-like cryptosystem for enciphering large messages," *IEEE Transactions on Knowledge and Data Engineering*, vol. 14, no. 2, pp. 445--446, 2002.

For a book: Dorothy E. R. Denning, *Cryptography and Data Security*. Massachusetts: Addison-Wesley, 1982.

For a paper in a proceeding: M. S. Hwang, C. C. Lee, and Y. L. Tang, ``Two simple batch verifying multiple digital signatures," in *The Third International Conference on Information and Communication Security (ICICS2001)*, pp. 13--16, Xian, China, 2001.

In text, references should be indicated by [number].

2.5 Author benefits

No page charge is made.

Subscription Information

Individual subscriptions to IJEIE are available at the annual rate of US$ 200.00 or NT 6,000 (Taiwan). The rate is US$1000.00 or NT 30,000 (Taiwan) for institutional subscriptions. Price includes surface postage, packing and handling charges worldwide. Please make your payment payable to "Jalaxy Technique Co., LTD." For detailed information, please refer to http://ijeie.jalaxy.com.tw or Email to ijeieoffice@gmail.com.